Algebra & Number Theory

Volume 14
2020
No. 8

msp

Algebra & Number Theory

msp.org/ant

PRODUCTION

production@msp.org
Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2020 is US $415/year for the electronic version, and $620/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

ALGEBRA AND NUMBER THEORY 14:8 (2020)
https://doi.org/10.2140/ant.2020.14.2001

Toroidal orbifolds, destackification, and Kummer blowings up

Dan Abramovich, Michael Temkin and Jarosław Włodarczyk

With an appendix by David Rydh

We show that any toroidal DM stack X with finite diagonalizable inertia possesses a maximal toroidal coarsening X_{tcs} such that the morphism $X \to X_{\mathrm{tcs}}$ is logarithmically smooth.

Further, we use torification results of Abramovich and Temkin (2017) to construct a destackification functor, a variant of the main result of Bergh (2017), on the category of such toroidal stacks X. Namely, we associate to X a sequence of blowings up of toroidal stacks $\widetilde{\mathcal{F}}_X : Y \to X$ such that Y_{tcs} coincides with the usual coarse moduli space Y_{cs}. In particular, this provides a toroidal resolution of the algebraic space X_{cs}.

Both X_{tcs} and $\widetilde{\mathcal{F}}_X$ are functorial with respect to strict inertia preserving morphisms $X' \to X$.

Finally, we use coarsening morphisms to introduce a class of nonrepresentable birational modifications of toroidal stacks called Kummer blowings up.

These modifications, as well as our version of destackification, are used in our work on functorial toroidal resolution of singularities.

1. Introduction

We study the birational geometry of toroidal orbifolds, aiming towards applications in resolution of singularities and semistable reduction, as initiated in our paper [Abramovich et al. 2020].

Throughout this paper a noetherian logarithmically regular logarithmic DM stack X will be referred to as a *toroidal DM stack*, and if its inertia is finite and diagonalizable then we say that X is a *toroidal orbifold*. Finally, X is called *simple* if its inertia groups I_x act trivially on the sharpened stalks $\overline{M}_x$ of the

This research is supported by BSF grant 2014365.

MSC2010: primary 14A20; secondary 14E05, 14E15.

Keywords: algebraic stacks, toroidal geometry, logarithmic schemes, birational geometry, resolution of singularities.

logarithmic structure. The coarse moduli space is denoted X_{cs}. For such objects we prove the following destackification result:

Theorem 1 (see Theorem 4.1.5). *Let $\mathcal{C}$ be the category of simple toroidal orbifolds. Then to any object X in $\mathcal{C}$ one can associate a* **destackifying blowing up** *of toroidal stacks $\mathcal{F}_X : X' \to X$ along a nowhere zero ideal I_X and a* **coarse destackifying blowing up** *$\mathcal{F}_X^0 : X_0 \to X_{\mathrm{cs}}$ along a nowhere zero ideal J_X so that*

(i) *$X_0 = (X')_{\mathrm{cs}}$ and X_0 inherits from X' a logarithmic structure making it a toroidal algebraic space such that the morphism $X' \to X_0$ is logarithmically smooth*;

(ii) *the blowings up are compatible with any surjective logarithmically smooth inert morphism $f : Y \to X$ from $\mathcal{C}$*:

$$I_X\mathcal{O}_Y = I_Y, \quad J_X\mathcal{O}_{Y_{\mathrm{cs}}} = J_Y, \quad Y' = X' \times_X Y, \quad Y_0' = X_0' \times_{X_{\mathrm{cs}}} Y_{\mathrm{cs}}.$$

Moreover, *the last two isomorphisms hold even without assuming that f is surjective.*

In addition, we remove the assumption on the triviality of the inertia action in Theorem 4.1.4. In this case, destackification is achieved by a sequence of blowings up, which is only compatible with strict inert morphisms.

The theorem above is a variant of the main result of [Bergh 2017]. It is tuned for different purposes and uses different methods. First, we restrict to diagonalizable inertia. In this case, Theorem 4.1.5 generalizes the main result of [Bergh 2017] in that we allow arbitrary toroidal singularities. Our method is also different from Bergh's, in that we use the *torific ideal* of [Abramovich and Temkin 2017] which produces the destackification result in one step. Unlike Bergh's result we do not describe the destackification in terms of a sequence of well-controlled operations such as blowings up and root stacks. In particular, applications to factorization of birational maps must use [Bergh 2017] rather than our theorems.

Our study of destackification requires understanding the degree to which one may remove stack structure while keeping logarithmic smoothness. For this purpose we introduce and study the properties of coarsening morphisms of Deligne–Mumford stacks in general in Section 2. A full classification of Deligne–Mumford coarsenings and in particular their existence, generalizing the Keel–Mori theorem, is a question we believe is of independence interest. This task, as well as a discussion of key cases, is provided in Appendix A written by David Rydh.

We then specialize to toroidal stacks in Section 3. We associate to a toroidal Deligne–Mumford stack X its *total toroidal coarsening* X_{tcs}, whose existence follows from Appendix A, and prove:

Theorem 2 (see Theorem 3.4.7). *Let $\widetilde{\mathcal{C}}$ be the 2-category of toroidal orbifolds and let X be an object of $\widetilde{\mathcal{C}}$. Then*

(i) *the total toroidal coarsening $X \to X_{\mathrm{tcs}}$ exists*;

(ii) *for any geometric point $x \to X$, we have $(I_{X/X_{\mathrm{tcs}}})_x = G_x^{\mathrm{tor}}$, where $(I_{X/X_{\mathrm{tcs}}})_x$ is the relative stabilizer and $G_x^{\mathrm{tor}} \subset G_x$ the maximal subgroup of inertia acting toroidally*;

(iii) *any logarithmically flat morphism $h : Y \to X$ in $\widetilde{\mathcal{C}}$ induces a morphism $h_{\mathrm{tcs}} : Y_{\mathrm{tcs}} \to X_{\mathrm{tcs}}$ with a 2-commutative diagram*

$$\begin{tikzcd} Y \arrow[r, "\phi_Y"] \arrow[d, "h"'] & Y_{\mathrm{tcs}} \arrow[d, "h_{\mathrm{tcs}}"] \arrow[dl, phantom, "\alpha"] \\ X \arrow[r, "\phi_X"'] \arrow[ur, Rightarrow] & X_{\mathrm{tcs}} \end{tikzcd}$$

and the pair $(h_{\mathrm{tcs}}, \alpha)$ is unique in the 2-categorical sense;

(iv) *assume in addition that Y is simple and h is logarithmically smooth and inert. Then the diagram in* (*iii*) *is 2-cartesian.*

We emphasize that in this paper the theorem above is only used in Theorems 4.1.4 and 4.1.5, and only tangentially. Our original treatment of Theorem 3 below used toroidal coarsenings, but our current formalism requires a relative coarsening over $B\mathbb{G}_m$.

Apart from destackification, our treatment of coarsening morphisms figures in our study of a collection of nonrepresentable birational modifications which is essential in our work [Abramovich et al. 2020] on resolution of singularities. This is detailed in Section 5, which is mostly independent of Sections 3 and 4. We define in Section 5.4.1 the notion of a *permissible Kummer center I* on a toroidal scheme, and in Section 5.4.4 we define its blowing up $[\mathrm{Bl}_I(X)] \to X$, which is in general a toroidal DM stack. Furthermore, in Section 5.5 we extend these notions to the case when X itself is a toroidal DM stack. The key properties of Kummer blowings up are as follows:

Theorem 3 (see Theorems 5.4.5 and 5.4.16, Lemmas 5.4.21, 5.4.19 and 5.4.18, and Section 5.5). *Let X be a toroidal DM stack and let I be a permissible Kummer ideal on X with the associated Kummer blowing up $f : [\mathrm{Bl}_I(X)] \to X$. Then*

(i) (*$V(I)$-modification*) *f is proper and an isomorphism over $X \smallsetminus V(I)$*;

(ii) (*principalization property*) *$f^{-1}(I)$ is an invertible ideal*;

(iii) (*universal property*) *f is the universal morphism of toroidal DM stacks $h : Z \to X$ such that $h^{-1}(I)$ is an invertible ideal*;

(iv) (*orbifold property*) *the relative inertia $I_{[\mathrm{Bl}_I(X)]/X}$ is finite diagonalizable, and it acts trivially on the monoids $\overline{M}_X$. If X is a simple toroidal orbifold then $[\mathrm{Bl}_I(X)]$ is a simple toroidal orbifold as well*;

(v) (*functoriality*) *let $f : Y \to X$ be a logarithmically smooth morphism of toroidal orbifolds and $J = I\mathcal{O}_Y$. Then $[\mathrm{Bl}_J(Y)] = [\mathrm{Bl}_I(X)] \times_X Y$, where the product is taken in the category of fs logarithmic stacks*;

(vi) (*coarse blowing up*) *assume $Z \hookrightarrow X$ is a strict closed logarithmic subscheme. Let $Z' \to Z$ be the strict transform* (*i.e., the closure of $Z \smallsetminus V(I)$ in $[\mathrm{Bl}_I(X)]$*). *Set $J_n = I^{n!} \cap \mathcal{O}_X$. Then the relative coarse moduli space $Z'_{\mathrm{cs}/X}$ is the blowing up of Z along the saturated ideal $((J_n)^m)^{\mathrm{nor}}\mathcal{O}_Z$ for large enough n and m*;

(vii) (*strict transform*) *assume further in* (vi) *that $J = I\mathcal{O}_Z$ is a permissible Kummer ideal on Z. Then the morphism $Z' \to Z$ factors through a unique isomorphism $Z' = [\mathrm{Bl}_J(Z)]$.*

Remark 4. We expect some of our statements to apply in greater generality: it is natural to allow X to be an Artin stack, where the stabilizer at any $x \in X$ acts discretely on the monoid $\overline{M}_x$, and where the kernel of this action is linearly reductive. With this generality, permissible Kummer centers (Section 5.4.1) may have index d divisible by the characteristic of the residue field at x.

2. Coarsening morphisms and inertia

2.1. *Inertia stack.*

2.1.1. *Basic properties of inertia.* Recall that the inertia stack $I_{X/Y}$ of a morphism $f : X \to Y$ of Artin stacks is the second diagonal stack $I_{X/Y} = X \times_{X \times_Y X} X$, where both structure arrows $X \to X \times_Y X$ are the diagonal. It is a representable group object over X.

The absolute inertia stack of X is $I_X = I_{X/\mathbb{Z}}$. Recall that by [Stacks, Tag 04Z6]

$$I_{X/Y} = I_X \times_{I_Y} X. \tag{1}$$

In other words, $I_{X/Y} = \operatorname{Ker}(I_X \to f^*(I_Y))$, where $f^*(I_Y) = I_Y \times_Y X$.

In fact, the inertia stack is a group functor in the following sense: given a morphism $f : X \to Y$ a natural morphism $I_f : I_X \to I_Y$ arises, and the induced morphism $I_X \to f^*(I_Y)$ is a homomorphism. In addition, the inertia functor is defined as a 2-limit and hence it respects 2-limits, including fiber products. So, given $T = X \times_Z Y$ with projections $f : T \to X$, $g : T \to Y$ and $h : T \to Z$, one has that

$$I_{X \times_Z Y} = I_X \times_{I_Z} I_Y = f^*(I_X) \times_{h^*(I_Z)} g^*(I_Y). \tag{2}$$

Similar facts hold for relative inertia over a fixed stack S.

2.1.2. *Inert morphisms.* We say that a morphism $f : X \to Y$ is *inert* or *inertia-preserving* if it respects the inertia in the sense that $I_X = f^*(I_Y)$. In particular, $I_{X/Y} = X$ and hence f is representable (see [Stacks, Tag 04SZ] for the absolute case, the relative case follows easily). Inert morphisms are preserved by base changes. Finally, inert morphisms have no nontrivial automorphisms.

2.1.3. *Inert groupoids.* In general, one runs into 2-categorical issues when trying to define groupoids in stacks or their quotients. This is addressed, using the theory of higher stacks and their truncations, in [Harper 2017, Definition 3.10, Proposition 3.11], where groupoids with representable projection arrows are considered. We sketch the situation here in the case of inert groupoids, suppressing the specification of a number of 2-arrows that the theory of higher stacks provides. The treatment here is thus a restatement of [Stacks, Tag 044U] in the situation of inert groupoids. By *an inert groupoid* in stacks we mean a usual datum $(p_{1,2} : X_1 \rightrightarrows X_0, m, i, \delta)$ as in [Stacks, Tag 0231], where X_i are stacks and all morphisms are inert.

Let $f : X_0 \to Y$ be a morphism. An isomorphism $\phi : f \circ p_1 \to f \circ p_2$ is said to *satisfy the cocycle condition* on

$$X_2 := X_1 \times_{p_2, X_0, p_1} X_1 \overset{\pi_{1,2}}{\rightrightarrows} X_1$$

if $\pi_2^*\phi \circ \pi_1^*\phi = m^*\phi$.

Lemma 2.1.4. *Assume that $p_{1,2} : X_1 \rightrightarrows X_0$ is a smooth inert groupoid in Artin stacks. Then there exists a representable smooth morphism of stacks $q : X_0 \to X$ such that $X_1 = X_0 \times_X X_0$, with a 2-isomorphism $q \circ p_1 \to q \circ p_2$ satisfying the cocycle condition on X_2, and moreover*

1. *X is the quotient $[X_0/X_1]$ in the sense that any morphism $f : X_0 \to Y$ with a 2-isomorphism $f \circ p_1 \to f \circ p_2$ satisfying the cocycle condition on X_2 are induced by q from a morphism $X \to Y$, which is unique up to a unique 2-isomorphism*;
2. *if $Z \to X$ is a morphism from an algebraic space, inducing a smooth inert groupoid in algebraic spaces $p^Z_{1,2} : Z_1 \rightrightarrows Z_0$, then $[Z_0/Z_1] \to Z$ is an isomorphism*;
3. *if $Y_1 \rightrightarrows Y_0$ is another inert groupoid with quotient Y, and a given smooth morphism $X_0 \to Y_0$ extends to a cartesian morphism of groupoids, then there is a smooth morphism $X \to Y$, unique up to unique isomorphism, with $X_i = Y_i \times_Y X$.*

Sketch of proof. Let $U \to X_0$ be a smooth covering by a scheme and set

$$R = U \times_{X_0, p_1} X_1 \times_{p_2, X_0} U.$$

Since inert morphisms are representable, R is an algebraic space and we obtain a smooth groupoid $R \rightrightarrows U$ in algebraic spaces. So the quotient $X = [U/R]$ is an Artin stack, and a (mostly 1-categorical) diagram chase shows that X is as required and satisfies (1) and (2). The existence of a morphism $X \to Y$ in part (3) follows from (1), and its properties follow from (2) by taking compatible smooth covers $Z_X \to X$ and $Z_Y \to Y$. □

2.1.5. *Inertia of special types.* We say that a stack X has *finite inertia* if the morphism $I_X \to X$ is finite, and we say that X has *diagonalizable inertia* if the geometric fibers of $I_X \to X$ are diagonalizable groups. For example, both conditions are satisfied when X admits an étale inert covering of the form $[Z/G] \to X$, where Z is a separated scheme acted on by a finite diagonalizable group G.

2.2. *Coarse spaces.*

2.2.1. *Coarse moduli spaces and their basic properties.* Recall that by the Keel–Mori theorem, a stack X with finite inertia possesses a coarse moduli space X_{cs}; see [Keel and Mori 1997] and more generally [Rydh 2013, pp. 630–631]. Rydh's treatment removes all but necessary assumptions; here the morphism $\pi : X \to X_{\mathrm{cs}}$ is a separated universal homeomorphism with $\pi_*\mathcal{O}_X = \mathcal{O}_{X_{\mathrm{cs}}}$, but cannot be assumed proper unless X is of finite type over a scheme.

In the sequel, we will say that X_{cs} is the *coarse space* of X and $X \to X_{\mathrm{cs}}$ is the *total coarsening morphism* of X. Recall that for any flat morphism of algebraic spaces $Z \to X_{\mathrm{cs}}$, the base change morphism $Y = X \times_{X_{\mathrm{cs}}} Z \to Z$ is a total coarsening morphism and the projection $Y \to X$ is flat and inert. As a partial converse, a morphism $Y \to X$ which is either inert and étale [Rydh 2013, Theorem 6.10], or inert and flat with X tame [Rydh 2020] is the base change of $h_{\mathrm{cs}} : Y_{\mathrm{cs}} \to X_{\mathrm{cs}}$.

2.2.2. *The universal property.* The coarse space of X is initial among morphisms $X \to Z$ to algebraic spaces, and we will extend this, under appropriate assumptions, to morphisms $X \to Z$ of stacks. We say that an inertia map $I_X \to I_Z$ is *trivial* if it factors through the unit $Z \to I_Z$. This happens if and only if $I_{X/Z} = I_X$.

Theorem 2.2.3. *Assume that $\phi : X \to Z$ is a morphism of Artin stacks and the inertia of X is finite.*

(i) *Assume either X is tame or Z is a Deligne–Mumford stack. Then the inertia map $I_\phi : I_X \to I_Z$ is trivial if and only if ϕ factors through the coarse space $f : X \to X_{\text{cs}}$: there exists $\psi : X_{\text{cs}} \to Z$ and a* 2*-isomorphism $\alpha : \phi \xrightarrow{\sim} \psi \circ f$.*

(ii) *A factorization in* (i) *is unique in the sense of* 2*-categories: if ψ' and α' form another such datum then there exists a unique* 2*-isomorphism $\psi = \psi'$ making the whole diagram* 2*-commutative.*

Proof. If ϕ factors through f then I_ϕ factors through the inertia $I_{X_{\text{cs}}}$, which is trivial. Conversely, assume that I_ϕ is trivial.

- Assume Z is Deligne–Mumford. Choose an étale covering of Z by a scheme Z_0 and set $Z_1 = Z_0 \times_Z Z_0$ and $X_i = X \times_Z Z_i$, as in the left part of following diagram, which is cartesian:

$$\begin{tikzcd}
Z_1 \arrow[d, shift left] \arrow[d, shift right] & X_1 \arrow[l] \arrow[r] \arrow[d, shift left] \arrow[d, shift right] & Y_1 \arrow[d, shift left] \arrow[d, shift right] \\
Z_0 \arrow[d] & X_0 \arrow[l] \arrow[r] \arrow[d] & Y_0 \\
Z & X \arrow[l] &
\end{tikzcd}$$

  Since I_{Z_i} and I_ϕ are trivial, equations (1) and (2) imply that $I_{X_i} = I_X \times_X X_i$, and we obtain that the étale surjective morphisms $X_i \to X$ are inert.

  It follows that each X_i has finite inertia, in particular, coarse spaces $Y_i = (X_i)_{\text{cs}}$ are defined as in the right-hand side of the diagram above.

  Since the arrows $X_1 \to X_0$ are both étale and inert, [Rydh 2013, Theorem 6.10] applies (with $\mathcal{W} \to \mathcal{X}$ there replaced by $X_1 \to X_0$). Thus the left-hand diagram above is cartesian and the morphisms $Y_1 \to Y_0$ are étale. Now $Y_1 \rightrightarrows Y_0$ is an étale groupoid with quotient X_{cs}. For $i = 0, 1$ the map $X_i \to Z_i$ factors through Y_i uniquely, and the induced morphism of groupoids

$$(Y_1 \rightrightarrows Y_0) \to (Z_1 \rightrightarrows Z_0)$$

  gives rise to the unique morphism $\psi : X_{\text{cs}} \to Z$ as required.

- Assume instead X is tame. The same argument as in the Deligne–Mumford case above holds, replacing the reference [Rydh 2013] with [Rydh 2020]. Here we present another argument valid when both X and Z are tame. By [Abramovich et al. 2011, Theorem 3.1] the morphism $X \to Z$ factors through its relative coarse moduli space $X_{\text{cs}/Z}$, hence it suffices to replace Z by $X_{\text{cs}/Z}$ and show that $X_{\text{cs}/Z} \to X_{\text{cs}}$ is an isomorphism. The problem is local in the étale topology of X_{cs}, hence we may assume $X = [V/G]$ with V a scheme and G finite linearly reductive, in which case the result follows from [Abramovich et al. 2011, Proposition 3.6].

For (ii), consider a diagram

$$\begin{tikzcd} X \arrow[r] & X_{\mathrm{cs}} \arrow[r, shift left, "\psi"] \arrow[r, shift right, "\psi'"'] & Z \end{tikzcd}$$

with isomorphisms $\alpha : \phi \xrightarrow{\sim} \psi \circ f$, $\alpha' : \phi \xrightarrow{\sim} \psi' \circ f$. Given a presentation $Z_0 \to Z$, the isomorphisms α, α' provide a commutative base change diagram

$$\begin{tikzcd} & (X_{\mathrm{cs}})_0 \arrow[dd, dotted] \arrow[dr, "\psi_0"] & \\ X_0 \arrow[ur] \arrow[dr] & & Z_0. \\ & (X_{\mathrm{cs}})'_0 \arrow[ur, "\psi'_0"'] & \end{tikzcd}$$

Since $(X_{\mathrm{cs}})_0, (X_{\mathrm{cs}})'_0 \to X_{\mathrm{cs}}$ are flat, both $X_0 \to (X_{\mathrm{cs}})_0, (X_{\mathrm{cs}})'_0$ are coarse moduli spaces, giving a unique $(X_{\mathrm{cs}})_0 \to (X_{\mathrm{cs}})'_0$ making the diagram commutative. The same holds with Z_0 replaced by $Z_1 = Z_0 \times_Z Z_0$, providing a unique isomorphism of ψ with ψ'. □

Remark 2.2.4. We note that further results are provided in [Abramovich and Temkin 2018; Romagny et al. 2018; Rydh 2020]. Part (i) does not hold without restrictions; see the example in Section A.2.3.

2.3. *General coarsening morphisms.*

2.3.1. *Coarsening morphisms.* We say that a morphism of stacks $\pi : X \to Y$ is a *coarsening morphism* if the inertia $I_{X/Y}$ is finite and for any flat morphism $Z \to Y$ with Z an algebraic space the base change $X \times_Y Z \to Z$ is a total coarsening morphism as discussed in Section 2.2. It follows, see Lemma 2.3.4, that these are separated universal homeomorphisms with $\pi_* \mathcal{O}_X = \mathcal{O}_Y$. It is easy to see that coarsening morphisms are preserved by composition and arbitrary flat base change, not necessarily representable. In addition, being a coarsening morphism is a flat-local property on the target. In fact, one can show that this is the smallest class of morphisms containing total coarsening morphisms and closed under flat base changes and descent.

Remark 2.3.2. We use a new terminology and definition, but the object is not new. We refer to [Abramovich et al. 2011, Section 3] for the definition of relative coarse moduli space $X_{\mathrm{cs}/S}$ of a morphism of stacks $X \to S$ with finite relative inertia. It is easy to see that $X \to X_{\mathrm{cs}/S}$ is a coarsening morphism and, conversely, for every coarsening morphism $X \to Y$ one has that $Y = X_{\mathrm{cs}/Y}$.

2.3.3. *Basic properties.* In view of Remark 2.3.2, the following lemma is essentially covered by [Abramovich et al. 2011, Theorem 3.2], but we provide a proof for completeness.

Lemma 2.3.4. *Let X be an Artin stack with finite inertia and let $f : X \to Y$ be a coarsening morphism. Then*

(i) *there exists a unique morphism $g : Y \to X_{\mathrm{cs}}$ such that $g \circ f$ is isomorphic to the total coarsening morphism $h : X \to X_{\mathrm{cs}}$*;

(ii) *f is a separated universal homeomorphism*;

(iii) $Y_{\mathrm{cs}} = X_{\mathrm{cs}}$, *i.e., g is the total coarsening morphism.*

Proof. (i) Choose an atlas $Y_1 \rightrightarrows Y_0$ of Y and set $X_i = Y_i \times_Y X$. Then $Y_i = (X_i)_{\mathrm{cs}}$ and hence the composed morphisms $X_i \to X \to X_{\mathrm{cs}}$ factor uniquely through morphisms $g_i : Y_i \to X_{\mathrm{cs}}$. The uniqueness implies that g_1 coincides with both pullbacks of g_0, hence f descends to a morphism $g : Y \to X_{\mathrm{cs}}$, which is unique.

(ii) Continuing with the notation above, since the projections $f_i : X_i \to Y_i$ are total coarsening morphisms (Section 2.2.1), they are separated universal homeomorphisms, and hence the same is true for f by descent.

(iii) We should prove that a morphism $Y \to T$ with T an algebraic space factors uniquely through X_{cs}. The composed morphism $X \to Y \to T$ factors through X_{cs} uniquely, hence the morphisms $X_i \to X \to T$ factor through X_{cs}. Since $Y_i = (X_i)_{\mathrm{cs}}$ we obtain that the morphisms $Y_i \to T$ factor through X_{cs} in a compatible way, and hence they descend to a morphism $Y \to X_{\mathrm{cs}}$ through which $Y \to T$ factors. □

2.3.5. *The universal property.* Similarly to coarse spaces, with appropriate assumptions, coarsening morphisms can be described by a universal property.

Theorem 2.3.6. *Let $\phi : X \to Z$ be a morphism of Artin stacks and let $f : X \to Y$ be a coarsening morphism.*

(i) *Assume either X is tame or Z is a Deligne–Mumford stack. Then the following conditions are equivalent*:

  (a) *ϕ factors through f.*

  (b) *$I_\phi : I_X \to \phi^*(I_Z)$ factors through $I_f : I_X \to f^*(I_Y)$.*

  (c) *The map $I_{X/Y} \to \phi^* I_Z$ is trivial.*

  (d) *$I_{X/Y} \subseteq I_{X/Z}$.*

(ii) *A factoring of ϕ through f in* (*i*) *is unique in the 2-categorical sense* (*see Theorem 2.2.3*(ii)). *In other words*, *f is a 2-categorical epimorphism.*

(iii) *In particular*, *the 2-category of coarsening morphisms of X is equivalent to a partially ordered set and the total coarsening morphism h is its final object.*

Proof. The implications (a)⇒(b)⇒(c)⇔(d) in (i) follow from the definitions and the base change property of inertia, see (1) in Section 2.1.1. So assume that the map $I_{X/Y} \to I_Z$ is trivial and let us prove (a). Consider a smooth covering of Y by a scheme Y_0 and set $Y_1 = Y_0 \times_Y Y_0$ and $X_i = Y_i \times_X Y$. Since $I_{X_i} = I_X \times_{I_Y} I_{Y_i}$ and I_{Y_i} is trivial, we obtain that I_{X_i} is the pullback of $I_{X/Y}$, and hence the morphisms $I_{X_i} \to I_Z$ are trivial. By Theorem 2.2.3, the morphisms $X_i \to Z$ factor through $Y_i = (X_i)_{\mathrm{cs}}$ uniquely. We obtain a morphism of groupoids $(Y_1 \rightrightarrows Y_0) \to Z$, which gives rise to a required morphism $Y \to Z$.

In the same way, part (ii) reduces to Theorem 2.2.3(ii) using that the question is smooth-local on Y. Part (iii) follows from part (ii). □

Remark 2.3.7. The implication (c)⇒(b) in the theorem is nontrivial. Informally, it indicates that $f^*(I_Y) = I_X / I_{X/Y}$. (To prove that this is indeed a group scheme quotient we should have tested it with all group schemes over X, while (b) only uses group schemes which are a pullback of some I_Z.)

Note that again the example in Section A.2.3 shows that part (i) does not hold without appropriate assumptions.

Remark 2.3.8. A full classification of Deligne–Mumford coarsenings, as well as a discussion of key cases, is provided in Appendix A.

3. Toroidal stacks and moduli spaces

3.1. *Toroidal schemes.*

3.1.1. *References.* We adopt the terminology of [Abramovich and Temkin 2017] concerning toroidal schemes and their morphisms with the only difference that we replace Zariski fine and saturated logarithmic structures by the étale fine and saturated logarithmic structures. In other words, in this paper we extend the class of toroidal schemes so that it contains "toroidal embeddings with self-intersections" in the terminology of [Kempf et al. 1973].

Note that when Kato [1994] introduced logarithmically regular logarithmic schemes, he worked with Zariski logarithmic schemes for simplicity. However, étale locally any fine logarithmic scheme is a Zariski logarithmic scheme, and this allows to easily extend all results about logarithmic regularity to general fs logarithmic schemes; see [Niziol 2006].

We will make use of Kummer logarithmically étale morphisms; see [Niziol 2008] and Section 5.3.5.

3.1.2. *Toroidal schemes.* Now, let us recall the main points quickly. In this paper, a *toroidal scheme* X is a logarithmically regular logarithmic scheme (X, M_X) in the sense of [Niziol 2006]. Alternatively, one can represent X by a pair (X, U), where the open subscheme U is the locus where the logarithmic structure is trivial. One reconstructs the monoid by $M_X = \mathcal{O}_{X_{\text{ét}}} \cap i_*(\mathcal{O}^\times_{U_{\text{ét}}})$, where $i : U \hookrightarrow X$ is the open immersion. Usually, we will denote a toroidal scheme X or (X, U).

3.1.3. *Fans.* Recall that the logarithmic stratum $X(n)$ of a logarithmic scheme $(X, \mathcal{M}_X)$ consists of all points $x \in X$ with $\operatorname{rank}(\overline{M}_x) = n$. Here and in the sequel we use the convention that $\overline{M}_x$ denotes $\overline{M}_{\bar{x}}$ for a geometric point $\bar{x} \to X$ over x. In particular, $\overline{M}_x$ is defined up to an automorphism, but its rank is well defined.

If X is a toroidal scheme then, by logarithmic regularity, each stratum $X(n)$ is regular of pure codimension n. By the *fan* of a toroidal scheme X we mean the set $\operatorname{Fan}(X)$ of all generic points of the logarithmic strata of X. Also, let $\eta : X \to \operatorname{Fan}(X)$ denote the contraction map sending a point x to the generic point of the connected component of the logarithmic stratum containing x.

3.1.4. *Morphisms.* A morphism of toroidal schemes $(Y, V) \to (X, U)$ is a morphism of the associated logarithmic schemes. Equivalently one can describe it as a morphism $f : Y \to X$ such that $f(V) \subseteq U$. *Logarithmically smooth morphisms* form an important class of morphisms (called *toroidal morphisms* in [Abramovich and Temkin 2017]). *Strict morphisms* form another important class: these are the morphisms that induce an isomorphism $f^*\mathcal{M}_X \xrightarrow{\sim} \mathcal{M}_Y$.

3.2. *Toroidal actions.*

3.2.1. *Definitions.* A *diagonalizable group* G is a $\mathbb{Z}$-flat group scheme of the form $\boldsymbol{D}_L$ for a finitely generated group L; see [Abramovich and Temkin 2018, Section 3.2]. An action of G on a scheme X is *relatively affine* if there is a scheme Z and an affine G-invariant morphism $X \to Z$; see [Abramovich and Temkin 2018, Section 5.1]. This will be a running assumption throughout. It implies the existence of schemes of fixed points and a good inertia stratification. We also assume that X is toroidal and G acts on it in the sense of [Abramovich and Temkin 2017, Section 3.1]: $p^*M_X \xrightarrow{\sim} m^*M_X$, where $p, m : X \times G \rightrightarrows X$ are the projection and the action morphisms, but in this paper M_X is an étale sheaf. In particular $G_{\eta(x)} \subseteq G_x$. The action is *simple* at a point $x \in X$ if the stabilizer G_x acts trivially on $\overline{M}_x$, and the action is *toroidal* at x if it is simple at x and $G_x = G_{\eta(x)}$. Note that the latter happens if and only if G_x acts trivially on the connected component of the logarithmic stratum through x; see [Abramovich and Temkin 2017, Sections 3.1.4, 3.1.7].

Remark 3.2.2. (i) By [Abramovich and Temkin 2017, Corollary 3.2.18], the set of points $x \in X$, at which the action is toroidal or simple, is open.

(ii) Let us temporary say that the action is quasitoroidal at x is $G_x = G_{\eta(x)}$. This notion is not so meaningful due to the following examples:

(1) The openness property fails for quasitoroidality. For example, let $G = \mathbb{Z}/2\mathbb{Z}$ act on $X = \operatorname{Spec}(k[x, y])$ by switching the coordinates. Then the action is quasitoroidal at the origin, but it is not quasitoroidal at other points of the line X^G, which is given by $x = y$. Note that this action is not simple at the origin, so the example is consistent with the openness result for the toroidal locus.

(2) Let $G = \mathbb{Z}/4\mathbb{Z}$ with a generator g act on $X = \operatorname{Spec}(k[x, y])$ by $gx = y$ and $gy = -x$. Then the action is quasitoroidal everywhere but is not simple at the origin.

(iii) We note, as in Remark 4 of the introduction, that while the restrictions imposed here are sufficient for the immediate applications we have in mind, we expect some of our statements to hold in greater and more natural generality.

3.2.3. *The groups G_x^{tor}.* Let $G_{\overline{M}_x}$ be the subgroup of G_x that stabilizes $\overline{M}_x$. By the *toroidal stabilizer* at x we mean the subgroup $G_x^{\mathrm{tor}} = G_{\eta(x)} \cap G_{\overline{M}_x}$ of the stabilizer G_x. Thus G_x^{tor} is the maximal subgroup of G_x that acts toroidally at x.

Lemma 3.2.4. *If a diagonalizable group G acts in a relatively affine manner on a toroidal scheme X then any point $x \in X$ possesses a neighborhood X' such that $G_x^{\mathrm{tor}} \cap G_{x'} = G_{x'}^{\mathrm{tor}}$ for any point $x' \in X'$.*

Proof. Let X' be obtained by removing from X the Zariski closures of all points $\varepsilon \in \operatorname{Fan}(X)$ which are not generizations of x. Thus, $\eta(x')$ is a generization of $\eta(x)$ for any $x' \in X'$. Note that $\overline{M}_{x'} = \overline{M}_{\eta(x')}$ since $\overline{M}_X$ is locally constant along logarithmic strata. Therefore $G_{x'}^{\mathrm{tor}} = G_{\eta(x')}^{\mathrm{tor}}$, and it suffices to deal with the case when $x, x' \in \operatorname{Fan}(X)$. Then x' specializes to x and our claim reduces to the check that $G_{\overline{M}_x} \cap G_{x'} = G_{\overline{M}_{x'}}$. Since any cospecialization $\phi : \overline{M}_x \to \overline{M}_{x'}$ is surjective, $G_{\overline{M}_x} \cap G_{x'} \subseteq G_{\overline{M}_{x'}}$. Conversely, we need to show $G_{\overline{M}_{x'}} \subset G_{\overline{M}_x}$.

Let $F \subset \overline{M}_x$ be a face associated to the closed stratum $Y = \overline{\{x'\}}$ and cospecialization ϕ, so that $\overline{M}_{x'} = \overline{M}_x/F$ and ϕ is the quotient homomorphism. The normalization Y^{nor} of Y is itself toroidal, having characteristic monoid F at a point x^{nor} over x (and trivial monoid at the generic point x'). Since $G_{\overline{M}_{x'}}$

fixes x' it acts trivially on Y^{nor} and hence on F. Since $G_{\overline{M}_{x'}}$ also acts trivially on $\overline{M}_{x'} = \overline{M}_x/F$ it acts trivially on $\overline{M}_x$, as needed. □

3.2.5. *The quotients.* Toroidal stabilizers can also be characterized in terms of the quotient morphisms. To obtain a nice picture we restrict to étale groups.

Lemma 3.2.6. *Assume that an* ***étale*** *diagonalizable group G acts in a relatively affine manner on a toroidal scheme (X, U) and $x \in X$ is a point. Then G_x^{tor} is the maximal subgroup H of the stabilizer G_x such that if $q : X \to X/H$ is the quotient morphism then the pair $(X/H, U/H)$ is toroidal at $q(x)$ and the morphism $(X, U) \to (X/H, U/H)$ is Kummer logarithmically étale at x.*

Proof. If $H \subseteq G_x^{\mathrm{tor}}$, that is H acts toroidally at x, then the quotient is as asserted by [Abramovich and Temkin 2017, Theorem 3.3.12]. Conversely, assume that H is such that q is Kummer logarithmically étale at x. Then $\overline{M}_{q(x)}$ contains $n\overline{M}_x$ for a large enough n, and since H acts trivially on $\overline{M}_{q(x)}$, it acts trivially on $\overline{M}_x$. So the action of H is simple in a neighborhood of x. Let C be the connected component of the logarithmic stratum containing x. If $H \nsubseteq G_\eta$ then the induced morphism $C \to q(C)$ is ramified at x because η is the generic point of C. But we assumed that q is logarithmically étale, and hence $C \to q(C)$ is étale at x. This shows that $H \subseteq G_\eta$, and hence $H \subseteq G_\eta \cap G_{\overline{M}_x} = G_x^{\mathrm{tor}}$, as required. □

3.2.7. *Functoriality.* Assume that toroidal schemes X and Y are provided with relatively affine actions of diagonalizable groups G and H, respectively, $\lambda : H \to G$ is a homomorphism, and $f : Y \to X$ is a λ-equivariant morphism. We want to study when the toroidal inertia groups are functorial in the sense that $H_y^{\mathrm{tor}} \hookrightarrow \lambda^{-1}(G_x^{\mathrm{tor}})$ for any $y \in Y$ with $x = f(y)$. By [Abramovich and Temkin 2017, Lemma 3.1.6(i)], strict morphisms respect simplicity of the action. The toroidal property is more subtle: the functoriality of toroidal inertia may fail even for surjective fix-point reflecting strict morphisms.

Example 3.2.8. Let $X = \mathrm{Spec}(k[x, y])$ with the toroidal structure (x) and $G = \mathbb{Z}/2\mathbb{Z}$ acting by the sign both on x and y. Then the action is not toroidal at the origin O, so $G_{X,O}^{\mathrm{tor}} = 1$. Let Y be the x-axis $\mathrm{Spec}(k[x])$ with the toroidal structure (x). Then Y embeds G-equivariantly into X, but the action is toroidal on Y and hence $G_{Y,O}^{\mathrm{tor}} = G$ is not mapped into $G_{X,O}^{\mathrm{tor}}$. Furthermore, if $X_0 = X \setminus \{O\}$ then $X_0 \coprod Y \to X$ is a surjective fix-point reflecting strict morphism which is not functorial for the toroidal inertia.

Remark 3.2.9. As this example shows, the statement in [Abramovich and Temkin 2017, Lemma 3.1.9(ii)] needs to be corrected to read "and the converse is true if f is *étale* and surjective", and the proof should read "Hence (ii) follows from (i), Lemma 3.1.6(i) and *étale descent*". This does not affect other results of that paper, since only the direct implication was used.

The problem in Example 3.2.8 is that O is in the fan of Y but not in the fan of X, and the stabilizer drops at $\eta_X(O)$. To avoid such examples we will restrict to logarithmically flat morphisms.

Lemma 3.2.10. *Assume that $f : Y \to X$ is a logarithmically flat morphism of toroidal schemes. Then for any point $y \in Y$ with $x = f(y)$ one has that $f(\eta_Y(y)) = \eta_X(x)$. In particular,* $f(\mathrm{Fan}(Y)) \subseteq \mathrm{Fan}(X)$.

Proof. It suffices to prove that each connected component C of a logarithmic stratum on Y goes to the same logarithmic stratum $X(n)$, and the induced morphism $f : C \to X(n)$ is flat. The claim is étale local, hence we can assume that f splits into a composition of a strict flat morphism $Y \to X_P[Q]$ and the projection $X_P[Q] \to X$, where $P \hookrightarrow Q$ and $X_P[Q] = X \times_{\mathrm{Spec}(\mathbb{Z}[P])} \mathrm{Spec}(\mathbb{Z}[Q])$. The first case is clear, and in the second case the maps of the strata are easily seen to be flat. □

Lemma 3.2.11. *Let $f : Y \to X$ be a λ-equivariant morphism as in Section 3.2.7, and let $y \in Y$ be a point with $x = f(y)$ and the induced homomorphism $\lambda_y : H_y \to G_x$ such that f is logarithmically flat at y. Then*

(i) $\lambda_y(H_y^{\mathrm{tor}}) \subseteq G_x^{\mathrm{tor}}$;

(ii) *if, in addition, f is fix-point reflecting and either f is strict at y, or the action of H is simple at y, then $\lambda_y : H_y^{\mathrm{tor}} \xrightarrow{\sim} G_x^{\mathrm{tor}}$.*

Proof. Claim (i) follows from the following two observations: by logarithmic flatness $\overline{M}_x \subset \overline{M}_y$ so the inclusion $\lambda_y(H_{\overline{M}_y}) \subseteq G_{\overline{M}_x}$ holds, and the inclusion $\lambda_y(H_{\eta(y)}) \subseteq G_{\eta(x)}$ holds because $f(\eta(y)) = \eta(x)$ by Lemma 3.2.10.

In part (ii), strictness or simplicity assumption implies that $H_{\overline{M}_y} \xrightarrow{\sim} G_{\overline{M}_x}$. It remains to note that $H_{\eta(y)} \xrightarrow{\sim} G_{\eta(x)}$ because $f(\eta_Y(y)) = \eta_X(x)$ by Lemma 3.2.10 and f is fix-point reflecting. □

3.2.12. *Toroidal inertia.* For the sake of completeness we note that the groups G_x^{tor} glue to a *toroidal inertia* group scheme I_X^{tor} over the G-scheme X. Namely, if $\bar{\varepsilon}$ denotes the Zariski closure of ε then

$$I_X^{\mathrm{tor}} := \bigcup_{\varepsilon \in \mathrm{Fan}(X)} G_\varepsilon^{\mathrm{tor}} \times \bar{\varepsilon}$$

is a subgroup of $G \times X$, which is obviously contained in I_X. Since G is discrete there is no ambiguity about the scheme structure: $G \times X = \coprod_{g \in G} X$ and $I_X = \coprod_{g \in G} X^g$, where X^g is the closed subscheme fixed by g. The functoriality results of Lemma 3.2.11 extend to the toroidal inertia schemes in the obvious way.

3.3. *Toroidal stacks.* Using descent, the notions of toroidal schemes and morphisms can easily be extended to Artin stacks; see [Olsson 2003, Section 5]. We will stick to the case of DM stacks, since only they show up in our applications. A minor advantage of this restriction is that one can work with the étale topology instead of the lisse-étale topology.

3.3.1. *Logarithmic structures on stacks.* By a logarithmic structure on an DM stack X we mean a sheaf of monoids M_X on the étale site $X_{\text{ét}}$ and a homomorphism $\alpha_X : M_X \to \mathcal{O}_{X_{\text{ét}}}$ inducing an isomorphism $M_X^\times \xrightarrow{\sim} \mathcal{O}_{X_{\text{ét}}}^\times$. If $p_{1,2} : X_1 \rightrightarrows X_0$ is an atlas of X then giving a logarithmic structure M is equivalent to giving compatible logarithmic structures M_{X_i} in the sense that $p_i^{-1} M_{X_0} = M_{X_1}$ for $i = 1, 2$. We say that (X, M_X) is fine, saturated, etc., if (X_0, M_{X_0}) is so. We use here that these properties of M_{X_0} are étale local on X_0, and hence are independent of the choice of the atlas.

3.3.2. *Logarithmic stacks and atlases.* By a logarithmic stack (X, M_X) we mean a stack provided with a logarithmic structure. In this case, for any smooth atlas $X_1 \rightrightarrows X_0$ of X we provide X_0 and X_1 with the pullbacks of M_X and say that $(X_1, M_{X_1}) \rightrightarrows (X_0, M_{X_0})$ is an atlas of (X, M_X). Indeed, $\alpha_X : M_X \to \mathcal{O}_{X_{\text{ét}}}$ is uniquely determined by this datum.

3.3.3. *Toroidal stacks.* A logarithmic stack (X, M_X) is *logarithmically regular* or *toroidal* if it admits an atlas such that (X_0, M_{X_0}) is toroidal. In this case any atlas is toroidal because logarithmic regularity is a smooth-local property; see [Gabber and Ramero 2004, Proposition 12.5.46].

Furthermore, the triviality loci $U_i \subseteq X_i$ of M_{X_i} are compatible with respect to the strict morphisms $p_{1,2}$, hence U_0 descends to an open substack $i : U \hookrightarrow X$ that we call the triviality locus of M_X. Furthermore, when (X, M_X) is logarithmically regular, U determines the logarithmic structure by $M_X = \mathcal{O}_{X_{\text{ét}}} \cap i_*(\mathcal{O}^\times_{U_{\text{ét}}})$ because the same formulas reconstruct M_{X_i}. In the sequel, we will often view toroidal stacks as pairs (X, U). Again, a morphism $(Y, V) \to (X, U)$ of toroidal stacks is nothing else but a morphism $f : Y \to X$ of stacks such that $V \hookrightarrow f^{-1}(U)$.

3.4. ***Total toroidal coarsening.*** Let (X, U) be a toroidal DM stack.

3.4.1. *Toroidal coarsening morphisms.* Let $f : X \to Y$ be a coarsening morphism and $V \hookrightarrow Y$ the open substack corresponding to the open subset $f(|U|)$. We say that $f : X \to Y$ is *toroidal* if the pair (Y, V) is a toroidal stack, and the morphism $(X, U) \to (Y, V)$ is Kummer logarithmically étale. If it exists, the final object of the category of toroidal coarsening morphisms of X will be called the *total toroidal coarsening* of X and denoted $\phi_X : X \to X_{\text{tcs}}$.

Our next goal is to construct X_{tcs}. By Theorem A.1.3, ϕ_X is determined by the geometric points of its inertia, so our plan is as follows. First, we will extend the notion of toroidal stabilizers from Section 3.2.3 to geometric points of stacks, and then we will use them to construct ϕ_X so that, indeed, $(I_{\phi_X})_x$ is the toroidal stabilizer of x. In this context, I_{ϕ_X} is the generalization to toroidal stacks of the toroidal inertia I^{tor}_X from Section 3.2.12.

3.4.2. *Toroidal inertia.* Let $Z = X_{\text{cs}}$. By [Abramovich and Vistoli 2002, Lemma 2.2.3], a geometric point $x \to X$ possesses an étale neighborhood $X' = X \times_Z Z'$ of the form $[X'_0/G_x]$, in particular $X' \to X$ is inert. Pulling back the toroidal structure of X we obtain a G_x-equivariant toroidal structure on X'_0 and we take $G^{\text{tor}}_{X'_0,x}$ to be the maximal subgroup of G_x acting toroidally along x. By the following lemma, we can denote this group simply G^{tor}_x. It will be called the *toroidal stabilizer* at x. Note also that $\overline{M}_{X,x} = \overline{M}_{X'_0,x}$, and hence we obtain an action of G_x on $\overline{M}_x$. We say that X is *simple* if for any point $x \to X$ the group G_x acts on $\overline{M}_x$ trivially.

The toroidal stabilizer is related to the previous paragraph: by Lemma 3.2.6 a coarsening morphism $f : X \to Y$ is toroidal if and only if $\operatorname{Ker}(G_x \to G_{f(x)}) \subset G^{\text{tor}}_x$.

Lemma 3.4.3. *With the above notation, the group $G^{\text{tor}}_{X'_0,x}$ and the action of G_x on $\overline{M}_x$ are independent of the choices of neighborhood X' and quotient presentation $X' = [X'_0/G_x]$.*

Proof. Given a finer étale neighborhood $Z'' \to Z'$ of the image of x in Z, set $X'' = X \times_Z Z''$ and $X''_0 = X'_0 \times_{X'} X''$. In particular, $X'' = [X''_0/G_x]$. It suffices to check that $G^{\mathrm{tor}}_{X'_0,x} = G^{\mathrm{tor}}_{X''_0,x}$. Being a base change of a morphism of algebraic spaces, the morphism $X'' \to X'$ is inert, and it follows that the strict étale G_x-equivariant morphism $X''_0 \to X'_0$ is inert. Therefore, $G^{\mathrm{tor}}_{X'_0,x} = G^{\mathrm{tor}}_{X''_0,x}$ by [Abramovich and Temkin 2017, Lemma 3.1.9(ii)] and Remark 3.2.9. Also, it is clear that $\overline{M}_{X'_0,x} = \overline{M}_{X''_0,x}$ as G_x-sets.

It remains to consider two different presentations $X' = [X'_0/G_x] \simeq [X''_0/G_x]$ over the same étale $Z' \to Z$. Write $Y = X'_0 \times_{X'} X''_0$, so that $X' \simeq [Y/(G_x \times G_x)]$. One checks that $Y \to X'_0$ and $Y \to X''_0$ are inert. Lemma 3.2.11 implies $G^{\mathrm{tor}}_{X'_0,x} = G^{\mathrm{tor}}_{X''_0,x}$, giving the result. □

Functoriality properties from Lemma 3.2.11 extend to stacks straightforwardly.

Lemma 3.4.4. *Let $f : Y \to X$ be a morphism of toroidal stacks, and $y \to Y$ a point with $x = f(y)$ and the induced homomorphism $\lambda_y : G_y \to G_x$.*

(i) *If f is étale, strict and inert, then $\lambda_y : G^{\mathrm{tor}}_y \xrightarrow{\sim} G^{\mathrm{tor}}_x$.*

(ii) *If f is logarithmically flat at y, then $\lambda_y(G^{\mathrm{tor}}_y) \subseteq G^{\mathrm{tor}}_x$. If, in addition, f is inert and Y is simple at y, then $\lambda_y : G^{\mathrm{tor}}_y \xrightarrow{\sim} G^{\mathrm{tor}}_x$.*

Proof. If $Y_0 \to X_0$ is a λ_y-equivariant morphism of affine schemes inducing $f : Y = [Y_0/G_y] \to X = [X_0/G_x]$ then the toroidal stabilizers equal to the toroidal stabilizers of the actions of G_y and G_x on Y_0 and X_0, respectively. In this case, (i) follows from [Abramovich and Temkin 2017, Lemma 3.1.9(ii)] and Remark 3.2.9, and (ii) follows from Lemma 3.2.11.

The general case is reduced to this by local work on the coarse moduli spaces: first we base change both stacks with respect to an étale morphism $Z' \to X_{\mathrm{cs}}$ such that we can present $X = [X_0/G_x]$. Then we replace Y further by an appropriate étale neighborhood of y induced from an étale neighborhood of its image in Y_{cs}, so that we can present $Y = [Y_0/G_y]$. Now the G_x-torsors associated to $Y \to BG_y \to BG_x$ and $Y \to X \to BG_x$ agree on the residual gerbe $BG_y \subset Y$, so that after further inert localization of Y they agree on Y. This provides a λ-equivariant morphism $Y_0 \to X_0$ as needed. □

3.4.5. *Toroidal orbifolds.* In the sequel, by a *toroidal orbifold* we mean a toroidal DM stack X with finite diagonalizable inertia (but note Remarks 4 and 3.2.2(iii)). We allow the generic stabilizer to be nontrivial.

3.4.6. *The construction.* Now we can construct the total toroidal coarsening.

Theorem 3.4.7. *Let $\widetilde{\mathcal{C}}$ be the 2-category of toroidal orbifolds with the subcategory $\mathcal{C}$ of simple objects. Then*

(i) *for any object X of $\widetilde{\mathcal{C}}$, the total toroidal coarsening X_{tcs} exists;*

(ii) *for any geometric point $x \to X$, we have $(I_{X/X_{\mathrm{tcs}}})_x = G^{\mathrm{tor}}_x$, where $(I_{X/X_{\mathrm{tcs}}})_x$ is the relative stabilizer and G^{tor}_x the toroidal inertia group;*

(iii) *any logarithmically flat morphism $h : Y \to X$ in $\widetilde{\mathcal{C}}$ induces a morphism $h_{\mathrm{tcs}} : Y_{\mathrm{tcs}} \to X_{\mathrm{tcs}}$ with a 2-commutative diagram*

$$\begin{tikzcd} Y \arrow[r, "\phi_Y"] \arrow[d, "h"'] & Y_{\mathrm{tcs}} \arrow[d, "h_{\mathrm{tcs}}"] \arrow[dl, phantom, "\overset{\alpha}{\nearrow}"] \\ X \arrow[r, "\phi_X"'] & X_{\mathrm{tcs}} \end{tikzcd}$$

and the pair $(h_{\mathrm{tcs}}, \alpha)$ is unique in the 2-categorical sense: if $(h'_{\mathrm{tcs}}, \alpha')$ is another such pair then there exists a unique 2-isomorphism $h'_{\mathrm{tcs}} = h_{\mathrm{tcs}}$ making the whole diagram 2-commutative;

(iv) *assume that h is logarithmically smooth and inert, and Y is simple. Then the diagram in (iii) is 2-cartesian.*

The present proof of (i) and (ii) was suggested by David Rydh.

Proof. We first show that there is an open and closed subgroup $I_X^{\mathrm{tor}} \subset I_X$ with fibers G_x^{tor}.

Fix x and write $G = G_x$. By [Abramovich and Vistoli 2002, Lemma 2.3.3] there is a neighborhood $Z_0 \to Z := X_{\mathrm{cs}}$ and a G_x-scheme W_0 with isomorphism $X_0 := [W_0/G] \simeq X \times_Z Z_0$. By Lemma 3.4.3 we may replace X by X_0. Since $|X_0| = |Z_0|$, by Lemma 3.2.4 we can shrink Z_0 so that $G_w^{\mathrm{tor}} = G_x^{\mathrm{tor}} \cap G_w$ for any $w \in W_0$. Since $G_x^{\mathrm{tor}} \subset G$ are discrete groups this defines an open and closed subgroup $I_X^{\mathrm{tor}} \subset I_X$.

Theorem A.1.3 provides a coarsening morphism $X \to X_{\mathrm{tcs}}$ satisfying (i), (ii).

To prove (iii) we should prove that the morphism $Y \to X_{\mathrm{tcs}}$ factors through Y_{tcs} uniquely. So, by Theorem 2.3.6 we should prove that $I_{Y/Y_{\mathrm{tcs}}}$ is mapped to zero in $I_{X_{\mathrm{tcs}}}$. We claim that, moreover, the map $I_Y \to I_X$ takes $I_{Y/Y_{\mathrm{tcs}}}$ to $I_{X/X_{\mathrm{tcs}}}$. It suffices to check this on the geometric points, since the inertia are étale for DM stacks. But the latter is covered by Lemma 3.4.4(ii).

Let us prove (iv). Let Q denote the square diagram from (iii). Choose an étale covering $f : Z \to X_{\mathrm{tcs}}$ with Z a scheme. It suffices to show that the base change square $f^*(Q) := Q \times_{X_{\mathrm{tcs}}} Z$ is 2-cartesian. For any point $y \to Y$ with $x = h(y)$ we have that $G_y^{\mathrm{tor}} \xrightarrow{\sim} G_x^{\mathrm{tor}}$ by Lemma 3.4.4(ii). Hence $I_{\phi_Y(y)} = I_{\phi_X(x)}$, and we obtain that the morphism h_{tcs} is inert. It follows that $Z \times_{X_{\mathrm{tcs}}} Y_{\mathrm{tcs}}$ is an algebraic space. Thus, the morphisms $f^*(\phi_X)$ and $f^*(\phi_Y)$ are coarsening morphisms whose targets are algebraic spaces, and hence both are usual coarse spaces. We can now apply Lemma B.2.6 to conclude that the square $f^*(Q)$ is 2-cartesian. □

4. Destackification

4.1. *The main result.*

4.1.1. *Blowings up of toroidal stacks.* We say that a morphism $f : (X', U') \to (X, U)$ of toroidal stacks is the *blowing up along* a closed substack $Z \hookrightarrow X$ if $f : X' \to X$ is a blowing up along Z and $U' = f^{-1}(U) \setminus f^{-1}(Z)$. For example, a blowing up of toroidal schemes is a blowing up of usual schemes $f : X' \to X$ such that the toroidal divisor $X' \setminus U'$ of (X', U') is the union of the preimage of the toroidal divisor of (X, U) and the exceptional divisor of f. We use the same definition for normalized blowings up.

4.1.2. *Torification.* Our destackification results are based on and can be viewed as stack-theoretic enhancements of torification theorems of [Abramovich and Temkin 2017]. In Appendix B we recall these results and slightly upgrade them according to the needs of this paper.

4.1.3. *Destackification theorem.* Let us first formulate our main results on destackification. Their proof will occupy the rest of Section 4. Using the torification functors $\mathcal{T}$ and $\widetilde{\mathcal{T}}$ we will construct two destackification functors: $\mathcal{F}$ and $\widetilde{\mathcal{F}}$. The former one has stronger functoriality properties, but only applies to toroidal stacks with inertia acting *simply*.

Theorem 4.1.4. *Let $\widetilde{\mathcal{C}}$ be the category of toroidal orbifolds.*

(i) *For any object X of $\widetilde{\mathcal{C}}$ there exists a sequence of birational blowings up of toroidal stacks $\widetilde{\mathcal{F}}_X : X_n \to \cdots \to X$ such that $(X_n)_{\mathrm{tcs}} = (X_n)_{\mathrm{cs}}$.*

(ii) *In addition, one can choose $\widetilde{\mathcal{F}}$ compatible with surjective smooth strict inert morphisms $f : X' \to X$ from $\widetilde{\mathcal{C}}$ in the sense that for any such f the sequence $\widetilde{\mathcal{F}}_{X'}$ is the pullback of $\widetilde{\mathcal{F}}_X$. Compatibility on the level of morphisms holds even without assuming that f is surjective.*

Theorem 4.1.5. *Let $\mathcal{C}$ be the category of simple toroidal orbifolds. Then to any object X in $\mathcal{C}$ one can associate a birational blowing up of toroidal stacks $\mathcal{F}_X : X_1 \to X$ along an ideal I_X and a blowing up $\mathcal{F}^0_X : X_0 \to X_{\mathrm{cs}}$ along an ideal J_X so that*

(i) $(X_1)_{\mathrm{tcs}} = (X_1)_{\mathrm{cs}} = X_0$;

(ii) *if $f : X' \to X$ is a surjective logarithmically smooth inert morphism in $\mathcal{C}$, then $\mathcal{F}_{X'}$ and $\mathcal{F}^0_{X'}$ are the pullbacks of $\mathcal{F}_X$ and $\mathcal{F}^0_X$, respectively. Compatibility on the level of morphisms holds even without assuming that f is surjective.*

For the sake of completeness, we note that claim (ii) of the two theorems is also satisfied for strict morphisms f which are strongly equivariant in the sense that $f : X' \to X$ is the pullback of $f_{\mathrm{cs}} : X'_{\mathrm{cs}} \to X_{\mathrm{cs}}$. For these versions of Theorem 4.1.4(ii) (resp. Theorem 4.1.5(ii)) the proof is the same, but the reference to Corollary B.2.7 should be replaced by a reference to Theorem B.2.2 (resp. Theorem B.2.4). In both cases birationality follows from Proposition B.1.4.

4.2. ***The proof.*** We will work with Theorem 4.1.5 for concreteness. The proof of Theorem 4.1.4 is similar and involves less details; the main difference is that one should use Theorem B.2.2 as the torification input instead of Corollary B.2.7. (Recall that smooth inert morphisms are strongly equivariant by [Abramovich and Temkin 2018, Theorem 1.3.1(ii)(b)].)

We will construct the functor $\mathcal{F}$ by showing that the torification functor $\mathcal{T}$ descends to stacks. This will be done in two stages: first we will establish its descent to global quotients $[W/G]$ and then will use étale descent with respect to inert morphisms.

4.2.1. *Step 1: the global quotient case.* We will first prove the theorem for the subcategory $\mathcal{C}'$ of $\mathcal{C}$ whose objects X are of the form $[W/G]$, where G is an étale diagonalizable group acting on a toroidal quasiaffine scheme W.

Since the blowing up and the center of $\mathcal{T}'_{W,G}$ are G-equivariant, they descend to X. Namely, there exists a unique blowing up of toroidal stacks $\mathcal{F}_{X,W}: X_1 \to X$ whose pullback to W is $\mathcal{T}'_{W,G}: W_1 \to W$. Since $[W/G]_{\mathrm{cs}} = W/G$, we simply set $\mathcal{F}^0_{X,W} = \mathcal{T}'^0_{W,G}$. We claim that these $\mathcal{F}_{X,W}$ and $\mathcal{F}^0_{X,W}$ are independent of the choice of the covering W.

Suppose that $X = [W'/G']$ is another such representation. Note that $X = [W''/G'']$, where $W'' = W \times_X W'$ and $G'' = G \times G'$, and it suffices to compare the blowings up induced from W and W''. In this case the projection $W'' \to W$ is inert and λ-equivariant for the projection $\lambda : G'' \twoheadrightarrow G$, and hence $\mathcal{T}'_{W'',G''}$ and $\mathcal{T}'^0_{W'',G''}$ are the pullbacks of $\mathcal{T}'_{W,G}$ and $\mathcal{T}'^0_{W,G}$ by Corollary B.2.7. It follows that $\mathcal{F}_{X,W} = \mathcal{F}_{X,W''}$ and $\mathcal{F}^0_{X,W} = \mathcal{F}^0_{X,W''}$, and in the sequel we can safely write $\mathcal{F}_X$ and $\mathcal{F}^0_X$.

The properties of $\mathcal{F}$ and $\mathcal{F}^0$ are checked similarly, so we will only discuss $\mathcal{F}$. The action of G on W_1 is toroidal, hence $G_w = G^{\mathrm{tor}}_w$ for any $w \in W_1$. Since $X_1 = [W_1/G]$, the definition of toroidal stabilizers in Section 3.4.2 implies that $G_x = G^{\mathrm{tor}}_x$ for any geometric point $x \to X_1$. Therefore, $(X_1)_{\mathrm{tcs}} = (X_1)_{\mathrm{cs}}$ by Theorem 3.4.7. Assume that $f : X' \to X$ is a logarithmically smooth inert morphism in $\mathcal{C}'$. Choose presentations $X = [W/G]$ and $X' = [W'/G']$. Replacing the latter presentation by $[W' \times_X W/G \times G']$, we can assume that there is a homomorphism $\lambda : G' \to G$ such that f lifts to a λ-equivariant morphism $h : W' \to W$. Since f is inert, the same is true for h, and $\mathcal{T}'_{W,G}$ and $\mathcal{T}'_{W',G'}$ are compatible by Corollary B.2.7. By the definition of $\mathcal{F}$ on $\mathcal{C}'$, we obtain that $\mathcal{F}_X$ and $\mathcal{F}_{X'}$ are compatible too.

4.2.2. *Step 2: inert étale descent.* Assume now that X is an arbitrary toroidal orbifold. By [Abramovich and Vistoli 2002, Lemma 2.2.3], the coarse moduli space $Z = X_{\mathrm{cs}}$ possesses an étale covering

$$Z' = \coprod_{i=1}^{l} Z_i \to Z$$

such that each Z_i is affine and each $X_i = X \times_Z Z_i$ lies in $\mathcal{C}'$, say $X_i = [W_i/G_i]$. Note that $X' = \coprod_{i=1}^{l} X_i$ is also in $\mathcal{C}'$, for example, $X' = W'/G'$ for $W' = \coprod_i (X_i \times \prod_{j \neq i} G_j)$ and $G' = \prod_j G_j$. Furthermore, $X'' = X' \times_X X'$ is also in $\mathcal{C}'$ since $X'' = [W''/G'']$ for $W'' = W' \times_X W'$ and $G'' = G' \times G'$. (Although $I_X \to X$ is finite, X does not have to be separated, so W'' can be quasiaffine even though we started with an affine W'.)

By Section 4.2.1 $\mathcal{F}$ was defined for X' and X'' and $\mathcal{F}_{X''}$ is the pullback of $\mathcal{F}_{X'}$ with respect to either of the projections $X'' \rightrightarrows X'$. By étale descent, $\mathcal{F}_{X'}$ is the pullback of a blowing up $\mathcal{F}_{X,X'}: X_1 \to X$ of the toroidal stack X. In the same fashion, the blowings up $\mathcal{F}^0_{X'}$ and $\mathcal{F}^0_{X''}$ of Z' and $Z'' = Z' \times_Z Z'$ descend to a blowing up $\mathcal{F}^0_{X,X'}: Z_1 \to Z$, and by descent $(X_1)_{\mathrm{cs}} = Z_1$. Independence of the covering $X' \to X$ is proved as usual: given another such covering one passes to their fiber product, which is also a global quotient of a quasiaffine scheme, and then uses that $\mathcal{F}$ is compatible with inert morphisms.

We have now constructed $\mathcal{F}_X$ and $\mathcal{F}^0_X$ for an arbitrary object of $\mathcal{C}$. Their properties are established by étale descent via a covering $f : X' \to X$ as above. For example, for any geometric point $x \to X_1$ choose a lifting $x' \to X'_1$. Then $G_x = G_{x'}$ because f is inert, and hence $f_1 : X'_1 \to X_1$ is inert too. In addition, $G^{\mathrm{tor}}_x = G^{\mathrm{tor}}_{x'}$ by Lemma 3.4.4(i), and $G_{x'} = G^{\mathrm{tor}}_{x'}$ by Step 1. Thus, $G_x = G^{\mathrm{tor}}_x$, and hence $(X_1)_{\mathrm{tcs}} = (X_1)_{\mathrm{cs}}$.

5. Kummer blowings up

5.1. *Permissible centers.*

5.1.1. *Toroidal subschemes.* Let X be a toroidal scheme. We say that a closed subscheme Y of X is *toroidal* if $(Y, \mathcal{M}_X|_Y)$ is toroidal. Thus toroidal closed subschemes correspond to strict closed immersions of toroidal schemes. We stress that this differs from the terminology of [Abramovich and Temkin 2017, §2.3.12], in that toroidal subschemes are not defined by monomial ideals. Rather, they are locally described as follows:

Lemma 5.1.2. *Let X be a toroidal scheme and Y a closed subscheme of X. Then Y underlies a toroidal subscheme if and only if locally at any point $y \in Y$ there exist elements $t_1, \dots, t_n \in \mathcal{O}_{X,y}$ restricting to regular parameters on the stratum $X(d)$ of X through y, and $m \le n$ such that $Y = V(t_1, \dots, t_m)$ locally at y.*

Elements $t_1, \dots, t_n \in \mathcal{O}_{X,y}$ as in the statement will be called *regular coordinates*.

Proof. The inverse implication follows from the formal-local description of toroidal schemes; see [Kato 1994, Theorem 3.2]. Assume that Y is toroidal and let us construct required coordinates at y. We can assume that X and Y are local with closed point y. Let d be the rank of $\overline{M}_{X,y} = \overline{M}_{Y,y}$, and let n and $n-m$ be the dimensions of the closed logarithmic strata $X(d)$ and $Y(d)$. Since $X(d)$ and $Y(d)$ are regular, $\mathcal{O}_{X(d),y}$ possesses a regular family of parameters $t'_1, \dots, t'_n$ such that $V(t'_1, \dots, t'_m) = Y(d)$. Lift them to coordinates $t_1, \dots, t_n \in \mathcal{O}_{X,y}$. Since $Y(d) = X(d) \times_X Y$, we can also achieve that $t_1, \dots, t_m$ vanish on Y. The scheme $V(t_1, \dots, t_m)$ is integral (even toroidal) by the inverse implication, and $\dim(X) = d + n$ and $\dim(Y) = d + n - m$, hence the closed immersion $Y \hookrightarrow V(t_1, \dots, t_m)$ is an isomorphism. □

5.1.3. *Permissible centers.* Let X be a toroidal scheme. An ideal $J \subset \mathcal{O}_X$ is *monomial* if it is the image of a monoid ideal in M_X. A closed subscheme $Z = \operatorname{Spec}_X(\mathcal{O}_X/I)$ is called a *permissible center* if locally at any point $z \in Z$ it is the intersection of a toroidal subscheme and a monomial subscheme, that is, there exists a regular family of parameters $t_1, \dots, t_n$ and a monomial ideal J such that $I = (t_1, \dots, t_l, J)$ for $l \le n$.

5.1.4. *Playing with the toroidal structure.* A standard method used in toroidal geometry is to enlarge/decrease the toroidal structure by adding/removing components to/from $X \setminus U$. For example, see [Abramovich and Temkin 2017, §§3.4, 3.5]. We will use this method, and here is a first step.

Lemma 5.1.5. *Assume that (X, U) is a local toroidal scheme, C is the closed logarithmic stratum and $t_1, \dots, t_n$ a regular family of parameters of $\mathcal{O}_{C,x}$. Let W be obtained from U by removing the divisors $V(t_1), \dots, V(t_l)$, where $0 \le l \le n$. Then (X, W) is toroidal and $\overline{M}_{(X,W),x} = \overline{M}_{(X,U),x} \oplus \mathbb{N}^l$.*

Proof. The equality of the monoids is clear. Since the intersection of C with $V(t_1, \dots, t_l)$ is regular of codimension l we obtain that (X, W) is toroidal at x and hence toroidal. □

Corollary 5.1.6. *Assume that (X, U) is a toroidal scheme and $Z \hookrightarrow X$ is a permissible center. Then locally on X one can enlarge the toroidal structure of X so that Z is a monomial subscheme of the new toroidal scheme (X, W).*

Proof. Locally at $x \in X$ the center is given by $(t_1, \dots, t_l, J)$, where J is monomial. Set $W = U \setminus \bigcup_{i=1}^{l} V(t_i)$ and use Lemma 5.1.5. □

5.1.7. *Functoriality.* Permissible centers are respected by logarithmically smooth morphisms.

Lemma 5.1.8. *Assume that $f : Y \to X$ is a logarithmically smooth morphism of toroidal schemes and $Z \hookrightarrow X$ is a permissible center* (*resp. a toroidal subscheme*). *Then $Z \times_X Y$ is a permissible center* (*resp. a toroidal subscheme*) *in Y.*

Proof. Note that f induces smooth morphisms between logarithmic strata of Y and X. It follows that if $t_1, \dots, t_n$ are regular coordinates at $x \in X$ then their pullbacks form a part of a family of regular coordinates at a point $y \in f^{-1}(x)$. In view of Lemma 5.1.2, this implies the claim about toroidal subschemes. Since pullback of a monomial subscheme is obviously monomial, we also obtain the claim about permissible centers. □

5.2. *Permissible blowings up.*

5.2.1. *The model case.* We will prove that permissible centers give rise to normalized blowings up of toroidal schemes in the sense of Section 4.1.1. This can be done very explicitly in the model case when $X = \boldsymbol{A}^n_M = \operatorname{Spec}(B[M, t_1, \dots, t_n])$, where B is an arbitrary regular ring, M is a toric monoid, and $I = (t_1, \dots, t_n, m_1, \dots, m_r)$ for $m_i \in M$. For the sake of illustration we consider this case separately. Let $X' = \mathrm{Bl}_I(X)^{\mathrm{nor}}$ be the normalized blowing up of X along I. We have two types of charts:

(1) The t_i-chart is $\boldsymbol{A}^{n-1}_N = \operatorname{Spec}(B[N, t_1/t_i, \dots, t_n/t_i])$, where N is the saturation of the submonoid of $M \oplus \mathbb{Z}t_i$ generated by M, t_i and the elements $m_1 - t_i, \dots, m_r - t_i$. In particular, for any point x' of the chart with image $x \in X$ one has that $\operatorname{rk}(\overline{M}_{x'}) \le \operatorname{rk}(\overline{M}_x) + 1$. The monoid N is still sharp.

(2) The m_j-chart is $\boldsymbol{A}^n_P = \operatorname{Spec}(B[P, t_1/m_j, \dots, t_n/m_j])$, where P is the saturation of the submonoid of M^{gp} generated by M and the elements $m_1 - m_j, \dots, m_r - m_j$. In particular, the rank does not increase on this chart: $\operatorname{rk}(\overline{M}_{x'}) \le \operatorname{rk}(\overline{M}_x)$ for any point x' sitting over $x \in X$. The monoid P need not be sharp.

5.2.2. *The general case.* One can deal with the general case similarly by reducing to formal charts, but this is slightly technical, especially in the mixed characteristic case. A faster way is to play with the toroidal structure, reducing to the known properties of toroidal blowings up.

Lemma 5.2.3. *Assume that (X, U) is a toroidal scheme and $f : X' \to X$ is the normalized blowing up along a permissible center $Z \hookrightarrow X$, and set $U' = f^{-1}(U \setminus Z)$. Then (X', U') is a toroidal scheme and hence f underlies a normalized blowing up of toroidal schemes.*

Proof. The question is étale local on X, so we can assume that $X = \operatorname{Spec}(A)$ is a strictly henselian scheme with closed point x. Then $Z = V(t_1, \dots, t_l, m_1, \dots, m_r)$, where m_i are monomials and $t_1, \dots, t_n$ is a family of regular parameters of the logarithmic stratum through x. Set $W = U \setminus \bigcup_{i=1}^{l} V(t_i)$. Then (X, W) is toroidal by Lemma 5.1.5 and Z is a monomial subscheme of (X, W). Set $W' = f^{-1}(W \setminus Z)$.

Then (X', W') is toroidal and the toroidal blowing up $(X', W') \to (X, W)$ is logarithmically smooth; see [Nizioł 2006, Section 4] for proofs or [Abramovich and Temkin 2017, Lemma 4.3.3] for a summary. Furthermore, $X' \setminus U'$ is obtained from $X' \setminus W'$ by removing the strict transforms D'_i of $D_i = V(t_i)$, so we should prove that this operation preserves the toroidal property. By [Abramovich and Temkin 2017, Theorem 2.3.15] it suffices to prove that each D'_i is a Cartier divisor.

Now choose $y \in \{t_1, \dots, t_l, m_1, \dots, m_r\}$ and let us study the situation on the y-chart X'_y. We claim that the inclusion $D'_i|_{X'_y} \hookrightarrow V(t_i/y)$ is an equality and hence D'_i is Cartier, as required. If $y = t_i$ there is nothing to prove, so assume that $y \neq t_i$. It suffices to show that $V(t_i/y)$ is integral. So, for any $x' \in X'_y$ it suffices to prove that $\overline{M}_{x'}$ splits as $Q \oplus (t_i - y)\mathbb{N}$. To compute $\overline{M}_{x'}$ we recall that toroidal blowings up are base changes of toric blowings up of the charts. In particular, $X' \to X$ is the base change of the blowing up of $\operatorname{Spec}(\mathbb{Z}[M, t_1, \dots, t_l])$ along the ideal generated by $(t_1, \dots, t_l, m_1, \dots, m_r)$. The latter was computed in Section 5.2.1, and we saw that, indeed, its charts are of the form $\operatorname{Spec}(\mathbb{Z}[Q, t_i/y])$. □

5.2.4. *Functoriality.* In the sequel, by a *permissible blowing up* we mean the normalized blowing up along a permissible center. To simplify the notation, we will omit the normalization and will simply write $\mathrm{Bl}_I(X)$ or $\mathrm{Bl}_Z(X)$. Naturally, permissible blowings up are compatible with logarithmically smooth morphisms.

Lemma 5.2.5. *Let X be a toroidal scheme and let $Z \hookrightarrow X$ be a permissible center. Then for any logarithmically smooth morphisms $f : Y \to X$ of toroidal schemes, the pullback $T = Z \times_X Y$ is a permissible center and $\mathrm{Bl}_T(Y) = \mathrm{Bl}_Z(X) \times_X Y$ in the category of fs logarithmic schemes.*

Proof. We know that T is permissible by Lemma 5.1.8. The problem is local on X hence we can assume that X is local. As in the proof of Lemma 5.2.3, $Z = V(t_1, \dots, t_l, m_1, \dots, m_r)$ and Z becomes monomial once we replace $U = X(0)$ by $U' = U \setminus \bigcup_{i=1}^l V(t_i)$. Since the pullbacks of t_i form a subfamily of a regular family at any point of $f^{-1}(x)$, we also have that $V' = Y(0) \setminus \bigcup_{i=1}^l f^{-1}(V(t_i))$ defines a toroidal structure and T is monomial on (Y, V'). We omit the easy check that the morphism $(Y, V') \to (X, U')$ is logarithmically smooth. The lemma now follows from the fact that toroidal blowings up are compatible with logarithmically smooth morphisms; see [Nizioł 2006, Corollary 4.8]. □

5.3. ***Kummer ideals.*** Let X be a logarithmic scheme. In [Abramovich et al. 2020] we also use a generalization of permissible blowings up that we are going to define now. Informally speaking, we will blow up "ideals" of the form $(t_1, \dots, t_n, m_1^{1/d}, \dots, m_r^{1/d})$. Our next aim is to formalize such objects, and the main task is to define "ideals" $(m^{1/d})$.

5.3.1. *Ideals $I^{[1/d]}$.* First, let us describe the best approximation to extracting roots on the logarithmic scheme itself. For any monomial ideal I and $d \geq 1$ let $I^{[1/d]}$ denote the monomial ideal J generated by monomials m with $m^d \in I$. Recall that monomial ideals are in a one-to-one correspondence with the ideals of $\overline{M}_X$. If I corresponds to $J \subseteq \overline{M}_X$ then $I^{[1/d]}$ corresponds to $(1/d)J \cap \overline{M}_X$. So, extracting the root is a purely monomial operation, and hence it is compatible with strict morphisms $f : Y \to X$ in the sense that

$$(f^{-1}(I))^{[1/d]} = f^{-1}(I_X^{[1/d]}).$$

Remark 5.3.2. It may happen that I is invertible but $I^{[1/d]}$ is not. On the level of monoids this can be constructed as follows: take $M \subset \mathbb{N}^2$ given by (x, y) with $x + y \in 3\mathbb{Z}$ and $I = (3, 3) + M$. Then $I^{[1/3]}$ is generated by $(1, 2)$ and $(2, 1)$ and it is not principal.

5.3.3. *Kummer monomials.* By a *Kummer monomial* on a logarithmic scheme X we mean a formal expression $m^{1/d}$ where m is a monomial on X and $d \geq 1$ is an integer which is invertible on X. In order to view $m^{1/d}$ as an actual function we should work locally with respect to a certain log-étale topology. For example, $X[m^{1/d}] := (X \otimes_{k[m]} k[m^{1/d}])^{\text{sat}}$ is the universal fs logarithmic scheme over X on which $m^{1/d}$ is defined, and $X[m^{1/d}] \to X$ is logarithmically étale by our assumption on d.

Remark 5.3.4. One can also consider roots with a noninvertible d but then the morphism $X[m^{1/d}] \to X$ is only logarithmically syntomic, i.e., logarithmically flat and lci. We prefer to exclude such cases because we will later consider only toroidal schemes, and logarithmic regularity is not local with respect to the log-syntomic topology.

5.3.5. *Kummer topology.* In order to define operations on different monomials one has to pass to larger covers of X, and there are two ways to do this uniformly. The first one is to consider the pro-finite coverings and work with structure sheaves on nonnoetherian schemes; see [Talpo and Vistoli 2018]. Another possibility is to work with the structure sheaf of a topology generated by finite coverings. The two approaches are equivalent. We adopt the second one using the Kummer logarithmically étale topology defined by Niziol [2008]. For brevity, it will be called the Kummer topology.

Recall that a logarithmically étale morphism $f : Y \to X$ is called *Kummer* if for any point $y \in Y$ with $x = f(y)$ the homomorphism $\overline{M}_x^{\text{gp}} \to \overline{M}_y^{\text{gp}}$ is injective with finite cokernel, and $\overline{M}_y$ is the saturation of $\overline{M}_x$ in $\overline{M}_y^{\text{gp}}$. Setting surjective Kummer morphisms to be coverings, we obtain a *Kummer topology* on the category of fs logarithmic schemes. The site of Kummer logarithmic schemes over X will be denoted $X_{\text{két}}$. The following lemma shows that when working with the Kummer topology it suffices to consider two special types of coverings. The proof is simple, and we refer to [Niziol 2008, Corollary 2.17] for details.

Lemma 5.3.6. *The topology of $X_{\text{két}}$ is generated by two types of coverings: strict étale morphisms $Z \to Y$ and morphisms of the form $Y[m^{1/d}] \to Y$, with d invertible in $\mathcal{O}_Y$.*

5.3.7. *The structure sheaf.* The rule $Y \mapsto \Gamma(\mathcal{O}_Y)$ defines a presheaf of rings $\mathcal{O}_{X_{\text{két}}}$ on $X_{\text{két}}$.

Lemma 5.3.8. *The presheaf $\mathcal{O}_{X_{\text{két}}}$ is a sheaf.*

Proof. A more general claim is proved in [Niziol 2008, Proposition 2.18]. Let us outline a simple argument that works in our case. It suffices to check the sheaf condition for the two coverings from Lemma 5.3.6. The first case is clear since $\mathcal{O}_{X_{\text{ét}}}$ is a sheaf. In the second case we note that μ_d acts on $Y' = Y[m^{1/d}]$ and Y is the quotient, in particular, $\mathcal{O}_Y(Y')^{\mu_d} = \mathcal{O}_Y(Y)$. The saturated fiber product $Y'' = (Y' \times_Y Y')^{\text{sat}}$ equals $\mu_d \times Y'$, and hence the equalizer of $\mathcal{O}_Y(Y') \rightrightarrows \mathcal{O}_Y(Y'')$ equals $\mathcal{O}_Y(Y')^{\mu_d}$, that is, $\mathcal{O}_Y$ satisfies the sheaf condition with respect to the covering $Y' \to Y$. □

5.3.9. *Kummer ideals.* By a Kummer ideal we mean an ideal $I \subseteq \mathcal{O}_{X_{\text{két}}}$ which is coherent in the following sense: there exists a Kummer covering $Y \to X$ and a coherent ideal $I_Y \subseteq \mathcal{O}_Y$ such that $I|_{Y_{\text{két}}}$ is generated by I_Y in the sense that $\Gamma(Z, I) = \Gamma(Z, I_Y \mathcal{O}_Z)$ for any Kummer morphism $Z \to Y$.

Example 5.3.10. (i) If I_X is a monomial ideal on X let I be the associated ideal on $X_{\text{két}}$ and for Y Kummer over X let I_Y denote restrictions of I onto Y. Given $d \geq 1$ define $J = I^{1/d}$ by $J_Y = (I_Y)^{[1/d]}$. Note that the projections $p_{1,2}$ of $Z = (Y \times_X Y)^{\text{sat}}$ onto Y are strict. Hence $p_i^{-1}(J_Y) = J_Z$ for $i = 1, 2$, and we obtain that the pullbacks are naturally isomorphic, that is, J is an ideal in $\mathcal{O}_{X_{\text{két}}}$. Moreover, J is coherent because one can construct a covering $Y \to X$ such that $I_Y = J_Y^d$ and then $J_Z = J_Y \mathcal{O}_Z$ for any Kummer morphism $Z \to Y$. For example, choose an étale covering $\bigcup_i X_i \to X$ such that the ideals $I|_{X_i} = (\{m_{ij}\})$ are globally generated by monomials, let $Y_i = (X_i[m_{i1}^{1/d}, m_{i2}^{1/d}, \dots])^{\text{sat}}$, and take $Y = \coprod_i Y_i$.

(ii) One can produce more ideals using addition and multiplication, ideals coming from $\mathcal{O}_X$, and Kummer ideals from (i). For example, if $t_i \in \Gamma(\mathcal{O}_X)$ and m_j are global monomials then the ideal $J = (t_1, \dots, t_n, m_1^{1/d}, \dots, m_r^{1/d})$ is a well-defined coherent Kummer ideal, as well as its powers J^l.

Remark 5.3.11. (i) It is essential that we are working with saturated logarithmic schemes and the Kummer topology. For example, if $X = \operatorname{Spec}(k[t])$ and X_{fl} denotes the small flat site of X then by the usual flat descent $\mathcal{O}_{X_{\text{fl}}}$ is a sheaf in which any coherent ideal comes from a coherent ideal of $\mathcal{O}_X$. In particular, the ideal $t\mathcal{O}_{X_{\text{fl}}}$ is not a square. This happens for the following reason: although $(t) = (y^2)$ on the double covering $Y = \operatorname{Spec}(k[y]) \to X$ with $y^2 = t$, the fiber product $Z = Y \times_X Y$ equals to $\operatorname{Spec}(k[y_1, y_2]/(y_1^2 - y_2^2))$ and the two pullbacks of (y) to Z are different: $(y_1) \neq (y_2)$. In other words, the root $(y) = \sqrt{(t)}$ is not unique locally on X_{fl} and hence does not give rise to an ideal.

(ii) The sheaf $\mathcal{O}_{X_{\text{két}}}$ also has noncoherent ideals. For example, for $X = \operatorname{Spec}(k[m])$ the maximal monomial ideal $\sum_{d=1}^{\infty}(m^{1/d})$. In fact, it is not even quasicoherent because it is not generated by an ideal on a Kummer étale cover of X.

5.4. ***Blowings up of permissible Kummer ideals.*** This section provides the key construction of a Kummer blowing up of a toroidal scheme. It was pointed out by David Rydh that Kummer blowings up have an elegant construction using stack-theoretic $\mathcal{P}roj$ constructions and specifically stack-theoretic blowings up. Rydh's forthcoming foundational paper on these notions will simplify this entire section significantly.

5.4.1. *Permissible Kummer centers.* We restrict our consideration to toroidal schemes. Permissible centers extend to Kummer ideals straightforwardly: we say that a Kummer ideal I on a toroidal scheme X is *permissible* if it is generated by the ideal of a toroidal subscheme and a monomial Kummer ideal. In other words, for any geometric point $\bar{x} \to X$ one has that $I_{\bar{x}} = (t_1, \dots, t_n, m_1^{1/d}, \dots, m_r^{1/d})$, where $t_1, \dots, t_n$ is a part of a regular sequence of parameters, and $m_1, \dots, m_r$ are monomials. We impose the additional assumption that d is invertible on X, which is sufficient for our characteristic 0 applications but not optimal; see Remark 4. By $V(I)$ we denote the set of points of X where I is not the unit ideal; it is a closed subset of X.

5.4.2. *Kummer blowings up: global quotient case.* Let I be a permissible Kummer center on X. The idea of defining $\mathrm{Bl}_I(X)$ is to blow up a sufficiently fine Kummer covering of X and then descend it to a modification of X.

Assume first that there exists a G-Galois Kummer covering $Y \to X$ such that I is generated by I_Y. Note that $X = Y/G$. Locally, I_Y is generated by monomials and elements coming from I. Since G acts by characters on monomials and preserves elements coming from I, the ideal I_Y and the blowing up $Y' = \mathrm{Bl}_{I_Y}(Y) \to Y$ are G-equivariant. Moreover, using these generators we see that the blowing up Y' is covered by G-equivariant affine charts. In particular, the algebraic space Y'/G is a scheme, which we denote X'_{cs}, and $X'_{\mathrm{cs}} \to X$ is a W-modification, where $W = X \smallsetminus V(I)$. Here a *$W$-modification* $X'_{\mathrm{cs}} \to X$ is a modification restricting to the identity over the dense open $W \subset X$.

Note that X'_{cs} is the coarse space $[Y'/G]_{\mathrm{cs}}$ of the stack quotient $[Y'/G]$. We will show that X'_{cs} depends only on X and I, but it may happen that X'_{cs} with the quotient logarithmic structure is not toroidal: see Section 5.4.6 below for a general explanation and Example 5.4.12(ii) for a concrete example. On the other hand, $[Y'/G]$ is too close to Y': the morphism $Y' \to [Y'/G]$ is étale hence $[Y'/G]$ is toroidal, but it is ramified over the same points of X'_{cs} over which Y' is ramified, and hence depends on the choice of the covering $Y \to X$. Finally, we would like to ensure that the exceptional divisor E on $[Y'/G]$ remains Cartier, in other words, we would like the morphism $[Y'/G] \to B\mathbb{G}_m$ corresponding to the line bundle $\mathcal{O}(E)$ to descend to our modification. For these reasons the main player in the sequel will be the relative coarsening $[Y'/G]_{\mathrm{cs}/B\mathbb{G}_m}$ (see Section 2.3 and Remark 2.3.2). In particular, we will see that it is toroidal and independent of the choice of the covering $Y \to X$.

Lemma 5.4.3. *With the above notation, the X-stack $X' = [Y'/G]_{\mathrm{cs}/B\mathbb{G}_m}$ and its coarse space $X'_{\mathrm{cs}} = Y'/G$ depend on X and I only, but not on the Kummer covering $Y \to X$.*

Proof. It suffices to deal with X', since X'_{cs} is obtained from it. We should prove that if $Z \to X$ is another Kummer covering with Galois group H and $Z' = \mathrm{Bl}_{I_Z}(Z)$ then $[Z'/H]_{\mathrm{cs}/B\mathbb{G}_m} = X'$. The family of Kummer coverings is filtered, hence it suffices to consider the case when Z dominates Y. In this case, $Z/K = Y$ where K is a subgroup of H with $H/K = G$.

Since $I_Z = I_Y\mathcal{O}_Z$, the charts of both $\mathrm{Bl}_{I_Y}(Y)$ and $\mathrm{Bl}_{I_Z}(Z)$ can be given by the same elements. It follows that $Z' \to Y$ factors through a finite morphism $Z' \to Y'$. Since Y' is normal, this implies that $Z'/K = Y'$, and we obtain a coarsening morphism $h : [Z'/H] \to [Y'/G]$. Clearly, the exceptional divisor on $[Z'/H]$ is the pullback of the exceptional divisor on $[Y'/G]$. Therefore the morphism $[Z'/H] \to B\mathbb{G}_m$ factors through the morphism $[Y'/G] \to B\mathbb{G}_m$, and this implies that $[Z'/H]_{\mathrm{cs}/B\mathbb{G}_m} = [Y'/G]_{\mathrm{cs}/B\mathbb{G}_m}$, as required. □

5.4.4. *Kummer blowings up: the general case.* In the general case, the Kummer blowing up of X along I is defined by gluing. Namely, X has an étale covering $\sqcup X_i \to X$ such that $I_i = I|_{X_i}$ is generated by global functions and roots of global monomials, and then each X_i has a G_i-Kummer Galois covering $Y_i \to X_i$ such that $J_i = I_{Y_i}$ generates $I|_{Y_i}$. By Lemma 5.4.3 the stack $X'_i = [\mathrm{Bl}_{J_i}(Y_i)/G_i]_{\mathrm{cs}/B\mathbb{G}_m}$ and its coarse space $(X'_i)_{\mathrm{cs}} = \mathrm{Bl}_{J_i}(Y_i)/G_i$ depend on X_i and I_{X_i} only.

Over $X_{ij} := X_i \times_X X_j$ the stacks $(X'_i)_{X_{ij}}$ and $(X'_j)_{X_{ij}}$ are isomorphic by Lemma 5.4.3. Indeed the isomorphism over X is unique: the stacks are birational, normal, separated and Deligne–Mumford; hence [Fantechi et al. 2010, Proposition A.1] applies. This implies that X'_i glue uniquely over the intersections X_{ij}. Thus, we obtain morphisms $X' \to X$ and $X'_{\mathrm{cs}} \to X$ depending only on X and I. We say that $X'_{\mathrm{cs}} := \mathrm{Bl}_I(X)$ is the *coarse Kummer blowing up* of X along I and $X' = [\mathrm{Bl}_I(X)]$ is the *Kummer blowing up* of X along I. Here are two basic properties of this operation.

Theorem 5.4.5. *Assume that (X, U) is a toroidal scheme and I is a permissible Kummer center, and let $W = X \smallsetminus V(I)$. Then*

(i) *$f : [\mathrm{Bl}_I(X)] \to X$ and $\mathrm{Bl}_I(X) \to X$ are W-modifications of X;*

(ii) *$([\mathrm{Bl}_I(X)], f^{-1}(U))$ is a simple toroidal orbifold.*

Proof. The claims are local on X, so we can assume that X possesses a G-Galois Kummer covering Y such that I_Y generates $I|_{Y_{\text{két}}}$. Then $[\mathrm{Bl}_{I_Y}(Y)/G]$ is proper over X and the preimage of W is dense, and hence the same is true for the partial coarse spaces $[\mathrm{Bl}_I(X)]$ and $\mathrm{Bl}_I(X)$. Furthermore, the constructions are compatible with localizations and $I|_W = 1$, hence both are W-modifications of X.

The fact that $([\mathrm{Bl}_I(X)], f^{-1}(U))$ is a toroidal orbifold is shown in Lemma 5.4.7 below, using the explicit charts described in Section 5.4.6. Its simplicity follows from the observation that G acts simply on Y, and hence it also acts simply on $\mathrm{Bl}_{I_Y}(Y)$. □

5.4.6. *Charts of Kummer blowings up.* Next, let us describe explicit charts of Kummer blowings up. Assume that $X = \mathrm{Spec}(A)$ and $I = (t_1, \dots, t_n, m_1^{1/d}, \dots, m_r^{1/d})$ is a permissible Kummer ideal, where $(t_1, \dots, t_n)$ defines a toroidal subscheme and m_i are global monomials. Then $X' = [\mathrm{Bl}_I(X)]$ is of the form $[\mathrm{Bl}_J(Y)/G]_{\mathrm{cs}/B\mathbb{G}_m}$, where

$$B = A \otimes_{\mathbb{Z}[m_1,\dots,m_r]} \mathbb{Z}[m_1^{1/d}, \dots, m_r^{1/d}],$$

$Y = \mathrm{Spec}(B^{\mathrm{sat}})$, $G = (\boldsymbol{\mu}_d)^r$, and $J = I\mathcal{O}_Y$. Note that $\mathrm{Bl}_J(Y)$ is covered by the charts

$$Y'_y = \mathrm{Spec}(B[t'_1, \dots, t'_n, u'_1, \dots, u'_r]^{\mathrm{sat}}),$$

where $y \in \{t_1, \dots, t_n, m_1^{1/d}, \dots, m_r^{1/d}\}$, $t'_i = t_i/y$ and $u'_j = m_i^{1/d}/y$. Hence X' is covered by the charts $X'_y = [Y'_y/G]_{\mathrm{cs}/B\mathbb{G}_m}$.

Let us describe X'_y locally at the image of a point $q \in Y'_y$. The stabilizer G_q is the inertia group of $[Y'_y/G]$ at the image of q. Hence the morphism $[Y'_y/G] \to B\mathbb{G}_m$ induces a homomorphism $G_q \to \mathbb{G}_m$, whose kernel $G_{q/B\mathbb{G}_m}$ is the relative stabilizer of $[Y'_y/G]$ over $\mathbb{G}_m$ at the image of q. In particular, $X'_y = [(Y'_y/G_{q/B\mathbb{G}_m})/(G/G_{q/B\mathbb{G}_m})]$ locally at the image of q. To complete the picture it remains to observe that the relative stabilizer $G_{q/B\mathbb{G}_m}$ is the subgroup of G_q acting trivially on y, that is, G_q acts on y through its image in $\mathbb{G}_m$. To show this explicitly consider two cases:

(1) The t_i-chart. Since G acts trivially on t_i we have that $G_{q/B\mathbb{G}_m} = G_q$ and hence $X'_y = Y'_y/G$ is a scheme.

(2) The $m_i^{1/d}$-chart. In this case, $G_{q/B\mathbb{G}_m}$ contains $G_q \cap \boldsymbol{\mu}_d^{r-1}$ and $G_q/G_{q/B\mathbb{G}_m} = \boldsymbol{\mu}_e$, where e is the minimal divisor of d such that $m_i \in \mathcal{M}_x^{d/e}$, where $x \in X$ is the image of q; in particular, G_q acts through $\boldsymbol{\mu}_e$ on the image of $m_i^{1/d}$ in $\mathcal{M}_q$.

Lemma 5.4.7. *Keep the above notation. Then the group $G_{q/B\mathbb{G}_m}$ acts toroidally at q. In particular, the coarsening $[Y'/G] \to [\mathrm{Bl}_I(X)]$ is toroidal and $[\mathrm{Bl}_I(X)] = [Y'/G]_{\mathrm{cs}/\mathbb{G}_m} = [Y'/G]_{\mathrm{tcs}/B\mathbb{G}_m}$.*

Proof. The regular coordinates on Y'_y are of the form $t'_i = t_i/y$. Since $G_{q/B\mathbb{G}_m}$ acts trivially on t_i and y, it acts trivially on t'_i. Thus, its action at q is toroidal. □

We will not need the following remark, so its justification is left to the interested reader.

Remark 5.4.8. (i) The whole group G_q can act nontrivially on $m_i^{1/d}$-charts, see Example 5.4.12(ii) below. So, one may wonder what is the maximal toroidal coarsening $[Y'/G]_{\mathrm{tcs}}$. By the above lemma, we have a natural morphism $f : [\mathrm{Bl}_I(X)] \to [Y'/G]_{\mathrm{tcs}}$. It turns out that in the nonmonomial case (i.e., there exists at least one regular parameter t_1), f is an isomorphism. On the other hand, in the monomial case the action of the whole G_q is automatically toroidal, and hence $[Y'/G]_{\mathrm{tcs}} = Y'/G$. In this case, f can be a nontrivial coarsening; see Example 5.4.12(i).

(ii) In an early version of the paper, we defined $[\mathrm{Bl}_I(X)]$ to be equal to $[Y'/G]_{\mathrm{tcs}}$. This definition possesses worse functorial properties and often required to distinguish the monomial and nonmonomial cases. It seems that the new definition is the "right" one.

5.4.9. *The coarse blowing up.* The coarse blowing up can be computed directly.

Lemma 5.4.10. *Assume given a toroidal affine scheme $X = \mathrm{Spec}(A)$ with a positive number $e \in d\mathbb{Z}$ and a Kummer ideal $I = (t_1, \dots, t_n, m_1^{1/d}, \dots, m_r^{1/d})$. Then $\mathrm{Bl}_I(X)$ is the normalized blowing up of X along either of the following ideals: $J_e = (t_1^e, \dots, t_n^e, m_1^{e/d}, \dots, m_r^{e/d})$, $\widetilde{J}_e = I^e \cap \mathcal{O}_X$.*

Proof. Set $Y = \mathrm{Spec}(B)$ with $B = A[m_1^{1/d}, \dots, m_r^{1/d}]$. It suffices to check that $\mathrm{Bl}_{I_Y}(Y)$ is finite over both $\mathrm{Bl}_{J_e}(X)$ and $\mathrm{Bl}_{\widetilde{J}_e}(X)$. Indeed, in this case $\mathrm{Bl}_I(X) = \mathrm{Bl}_{I_Y}(Y)/\boldsymbol{\mu}_d^r$ is a finite modification of both $\mathrm{Bl}_{J_e}(X)^{\mathrm{nor}}$ and $\mathrm{Bl}_{\widetilde{J}_e}(X)^{\mathrm{nor}}$, and since the latter are normal we are done.

We will check the finiteness on charts. Let $y \in \{t_1, \dots, t_n, m_1^{1/d}, \dots, m_r^{1/d}\}$ and $x = y^e$. It suffices to show that $B[I/y]$ is finite over both $A[J_e/x]$ and $A[\widetilde{J}_e/x]$. But this is clear because $B[I/y]$ is integral over both $B[J_eB/x]$ and $B[\widetilde{J}_eB/x]$. □

5.4.11. *Examples.* Let us consider two basic examples of Kummer blowings up.

Example 5.4.12. (i) Let $X = \mathrm{Spec}(k[\pi])$ with the logarithmic structure given by π, and let $I = (\pi^{1/d})$. Then $[\mathrm{Bl}_I(X)] = [\mathrm{Spec}(k[\pi^{1/d}])/\mu_d]$ has stabilizer μ_d at the origin.

(ii) Let $X = \mathrm{Spec}(k[t, \pi])$ with the logarithmic structure given by π, and let $I = (t, \pi^{1/2})$. By Lemma 5.4.10, the coarse blow up $X'_{\mathrm{cs}} = \mathrm{Bl}_I(X)$ coincides with $\mathrm{Bl}_J(X)^{\mathrm{nor}}$, where $J = (t^2, \pi)$. In fact, $\mathrm{Bl}_J(X)$ is already normal and covered by two charts: $(X'_1)_{\mathrm{cs}} = \mathrm{Spec}(k[t, \pi, t^2/\pi])$ and $(X'_2)_{\mathrm{cs}} =$

$\mathrm{Spec}(k[t, \pi/t^2])$. The chart $(X'_2)_{\mathrm{cs}}$ is regular, but the chart $(X'_1)_{\mathrm{cs}}$ has an orbifold singularity O_X at the origin. Moreover, the natural logarithmic structure on $(X'_1)_{\mathrm{cs}}$ is generated by π only, and $(X'_1)_{\mathrm{cs}}$ is not toroidal with this logarithmic structure. (Though $(X'_1)_{\mathrm{cs}}$ can be made toroidal by increasing the toroidal structure, for example, by adding the divisor (t).)

Now let us consider the finer stack-theoretic picture. The Kummer blowing up $X' = [\mathrm{Bl}_I(X)]$ can be computed using the Kummer covering $Y = \mathrm{Spec}(k[t, \pi^{1/2}])$ with $G = \boldsymbol{\mu}_2$. This can be done directly, but for the sake of comparison we will first compute $X'' = [Y'/G]_{\mathrm{tcs}}$, where $Y' = \mathrm{Bl}_{(t,\pi^{1/2})}(Y)$. Cover Y' by two charts: $Y'_1 = \mathrm{Spec}(k[t/\pi^{1/2}, \pi^{1/2}])$ and $Y'_2 = \mathrm{Spec}(k[t, \pi^{1/2}/t])$. Then X'' is covered by the charts $X''_i = [Y'_i/G]_{\mathrm{tcs}}$. The action of G on Y'_2 is toroidal, and hence $X''_2 = Y'_2/G = (X'_2)_{\mathrm{cs}}$. The action of G at the origin O_Y of Y'_1 is not toroidal because G acts via the nontrivial character on both parameters. Therefore the stabilizer at the image $O_{X''} \in X''$ of O_Y is G. In particular, the coarse moduli space $X'' \to X'_{\mathrm{cs}}$ is an isomorphism over $X'_{\mathrm{cs}} \smallsetminus \{O_{X'_{\mathrm{cs}}}\}$, and the preimage of $O_{X'_{\mathrm{cs}}}$ is the point $O_{X''}$ with a nontrivial stack structure. Furthermore, it is easy to see that the exceptional divisor is Cartier on X'', and hence the morphism $X' \to X''$ admits a section. Thus, $X' = X''$ is the cone orbifold.

5.4.13. *Enlarging the toroidal structure.* As in the proof of Lemma 5.2.3, enlarging the toroidal structure any Kummer blowing up can be made into a logarithmically smooth morphism.

Lemma 5.4.14. *Let $X = (X, U)$ be a toroidal scheme, I be a permissible Kummer ideal on X and $f : X' = [\mathrm{Bl}_I(X)] \to X$ be the associated Kummer blowing up. Assume that $X_1 = (X, U_1)$ is a toroidal scheme obtained by enlarging the toroidal structure so that I is monomial on X_1 (see Corollary 5.1.6). Then $X'_1 = (X', f^{-1}(U_1))$ is a toroidal orbifold and the morphism $X'_1 \to X_1$ is logarithmically smooth.*

Proof. The claim is local on X, hence we can assume that there exists a G-Galois Kummer covering $Y \to X$ such that $J = I\mathcal{O}_Y$ is a permissible ideal. Let $Y' = \mathrm{Bl}_J(Y)$ and let Y'_1 and Y_1 be the toroidal schemes with the toroidal structure induced from U_1. Since J is monomial on Y_1, we have that $Y'_1 \to Y_1$ is a toroidal blowing up. By Section 5.4.6 the action of G on Y'_1 is toroidal (it acts trivially on all regular coordinates). Therefore, any subgroup $H \subseteq G$ acts toroidally and hence the morphism $Y'_1/H \to X_1$ is logarithmically smooth. It follows that for any coarsening T of $[Y'_1/G]$ the morphism $T \to Y_1/G = X_1$ is logarithmically smooth. It remains to recall that, by definition, X' is a coarsening of $[Y'/G]$, namely the relative coarse space with respect to the morphism $[Y'/G] \to B\mathbb{G}_m$ induced by the exceptional divisor. □

5.4.15. *The universal property.* Kummer blowings up can be characterized by a universal property which extends the classical characterization of blowings up.

Theorem 5.4.16. *Let X be a toroidal scheme and let I be a permissible Kummer ideal with the associated Kummer blowing up $f : [\mathrm{Bl}_I(X)] \to X$. Then $f^{-1}(I)$ is an invertible ideal and f is the universal morphism of toroidal DM stacks $h : Z \to X$ such that $h^{-1}(I)$ is an invertible ideal.*

Proof. All claims are local on X, so we can use the description of charts from Section 5.4.6: choosing a G-Galois Kummer covering $Y \to X$, such that I_Y is an ordinary ideal, and setting $Y' = \mathrm{Bl}_{I_Y}(Y)$ we have that $[\mathrm{Bl}_I(X)] = [Y'/G]_{\mathrm{cs}/B\mathbb{G}_m}$. Now, the first claim is obtained by unraveling the definition of

$X' := [\mathrm{Bl}_I(X)]$. Indeed, the exceptional divisor on Y', and hence also on Y'/G, is Cartier. Furthermore, the induced morphism $[Y'/G] \to B\mathbb{G}_m$ factors through X', that is the exceptional divisor on X' is also Cartier.

Now, let us check the universal property. So, assume that $h : Z \to X$ is such that $h^{-1}(I)$ is an invertible ideal, and let us show that it factors through $[\mathrm{Bl}_I(X)]$ uniquely up to a unique 2-isomorphism. Set $T = Z \times_X Y$ as an fs logarithmic scheme. From the factorization $T \to Z \to X$, the pullback of I to T is an invertible Kummer ideal. From the factorization $T \to Y \to X$, the pullback of I to T is the usual ideal $I_Y \mathcal{O}_T$. Therefore $I_Y \mathcal{O}_T$ is an invertible ideal, and by the universal property of blowings up, $T \to Y$ factors through a morphism $T \xrightarrow{\phi} Y' = \mathrm{Bl}_{I_Y}(Y)$ in a unique way. The exceptional divisors on T and Y' are compatible, hence induce compatible morphisms to $B\mathbb{G}_m$.

Note that $T \to Z$ is Kummer étale with Galois group $G = \boldsymbol{\mu}_d^r$ equal to the Galois group of $Y \to X$. Taking the stack quotient by G, the exceptional divisors remain Cartier, hence morphisms $[T/G] \to [Y'/G] \to B\mathbb{G}_m$ arise. Passing to the relative coarse moduli spaces yields a morphism $[T/G]_{\mathrm{cs}/B\mathbb{G}_m} \to X'$. It remains to recall that the exceptional divisor on $Z = T/G$ is already Cartier, hence $[T/G]_{\mathrm{cs}/B\mathbb{G}_m} = Z$ and we obtain the required morphism $Z \to X'$. □

5.4.17. *Strict transforms.* By a classical observation, the universal property of blowings up implies that if $X' \to X$ is the blowing up along an ideal I then the strict transform Z' of a closed subscheme $Z \hookrightarrow X$ is the blowing up of Z along $I\mathcal{O}_Z$. The same reasoning applies to Kummer blowings up as well.

Lemma 5.4.18. *Assume that X is a toroidal scheme, $Z \hookrightarrow X$ is a closed toroidal subscheme, and $I \subseteq \mathcal{O}_X$ is a permissible Kummer ideal whose restriction $J = I\mathcal{O}_Z$ is a permissible Kummer ideal on Z. Let $X' \to X$ be the Kummer blowing up along I and let Z' be the strict transform of Z (i.e., the closure of $Z \smallsetminus V(I)$ in X'). Then the morphism $Z' \to Z$ factors through a unique isomorphism $Z' = [\mathrm{Bl}_J(Z)]$.*

Proof. On the one hand, since $Z' \to X$ factors through X', the ideal $I\mathcal{O}_{Z'} = J\mathcal{O}_{Z'}$ is invertible. So, $Z' \to Z$ factors through a morphism $h : Z' \to Y = [\mathrm{Bl}_J(Z)]$ by Theorem 5.4.16. On the other hand, $J\mathcal{O}_Y$ is an invertible ideal, and since $J\mathcal{O}_Y = I\mathcal{O}_Y$, we obtain by Theorem 5.4.16 that the morphism $Y \to X$ factors through X'. Furthermore, $Y \to X$ factors through Z' because $Z \smallsetminus V(J)$ is dense in Y. This provides a morphism $Y \to Z'$, which is easily seen to be the inverse of h by the uniqueness of the factorization in Theorem 5.4.16. □

Since Kummer blowings up were only defined for toroidal schemes, we cannot extend the above theorem to the case when Z is an arbitrary closed logarithmic subscheme of X. However, in this case we can at least describe the strict transform on the level of the coarse space.

Lemma 5.4.19. *Assume that X is a toroidal scheme, $Z \hookrightarrow X$ is a strict closed logarithmic subscheme, and $I \subseteq \mathcal{O}_X$ is a permissible Kummer ideal. Let $X' \to X$ be the Kummer blowing up along I and let $Z' \to Z$ be the strict transform. Set $J_n = I^{n!} \cap \mathcal{O}_X$. Then Z'_{cs} is the blowing up of Z along $((J_n)^m)^{\mathrm{nor}}\mathcal{O}_Z$ for large enough n and m.*

Proof. The claim is local on X, hence by Lemma 5.4.14 we can enlarge the logarithmic structure on X making I monomial. Recall that by Lemma 5.4.10, $X'_{\mathrm{cs}} \to X$ is the normalized blowing up along J_n for a large enough n. Clearly J_n is monomial, hence by [Abramovich and Temkin 2017, Corollary 5.3.6] $X'_{\mathrm{cs}} \to X$ is the blowing up along $((J_n)^m)^{\mathrm{nor}}$ for a large enough m. Note that Z'_{cs} is the closed subscheme of X'_{cs} coinciding with the image of Z'. It follows that Z'_{cs} is the strict transform of Z and hence it is the blowing along $((J_n)^m)^{\mathrm{nor}}\mathcal{O}_Z$ by the usual theory of strict transforms. □

5.4.20. *Functoriality.* The universal property can also be used to show that, as most other constructions of this paper, Kummer blowings up are compatible with logarithmically smooth morphisms.

Lemma 5.4.21. *Let $f : Y \to X$ be a logarithmically smooth morphisms of toroidal schemes, I a permissible Kummer center on X, and $J = f^{-1}(I)$. Then* $[\mathrm{Bl}_J(Y)] = [\mathrm{Bl}_I(X)] \times_X Y$, *where the product is taken in the category of fs logarithmic schemes.*

Proof. Recall that J is permissible by Lemma 5.2.5. Set $X' = [\mathrm{Bl}_I(X)]$ and $Y' = [\mathrm{Bl}_J(Y)]$. Since $J\mathcal{O}_{Y'} = I\mathcal{O}_{Y'}$, the morphism $Y' \to X$ factors through X' by Theorem 5.4.16, and we obtain a morphism $Y' \to X' \times_X Y$. Conversely, since $X' \times_X Y$ is logarithmically smooth over X', the pullback of the invertible ideal $I\mathcal{O}_{X'}$ to $X' \times_X Y$ is also invertible. The latter coincides with the pullback of J to $X' \times_X Y$, and using Theorem 5.4.16 again we obtain a morphism $X' \times_X Y \to Y'$. It follows from the uniqueness of the factorizations that these two morphisms are inverse, implying the lemma. □

5.5. ***Kummer blowings up of stacks.*** It is also desirable to work with compositions of Kummer blowings up. For example, such sequences will be our main tool in constructing logarithmic desingularization in [Abramovich et al. 2020]. For this one should at least extend the construction to the case when X itself is a toroidal orbifold. We will see that, in fact, everything works fine when X is a toroidal DM stack.

5.5.1. *Kummer ideals.* The Kummer topology naturally extends to logarithmic stacks, giving rise to the notion of Kummer ideals. Permissibility of Kummer ideals is an étale-local notion and hence it extends to toroidal DM stacks too. Also, Lemma 5.2.3, which concerns usual coherent ideals, generalizes as follows:

> A permissible blowing up of a toroidal DM stack (resp. simple toroidal orbifold) is again a toroidal DM stack (resp. simple toroidal orbifold).

To combine the two notions and form the *Kummer* blowing up of a toroidal DM stack we must check that 2-categorical issues do not arise.

5.5.2. *Kummer blowings up.* Assume now that X is a toroidal DM stack and I is a permissible Kummer ideal on $X_{\text{két}}$. Find a strict étale covering of X by a toroidal scheme X_0 and set $X_1 = X_0 \times_X X_0$. The pullback I_i of I to X_i is a permissible Kummer ideal, and we set $Y_i = [\mathrm{Bl}_{I_i}(X_i)]$. Since $[X_1 \rightrightarrows X_0]$ is an étale groupoid whose projections and the multiplication morphism are strict, we obtain by Lemma 5.4.21 that $Y_1 \rightrightarrows Y_0$ is an étale groupoid *of stacks* whose projections are strict and *inert*. By Lemma 2.1.4 the quotient $Y = [Y_0/Y_1]$ exists as a toroidal DM stack and satisfies $Y_i = X_i \times_X Y$. We call Y the Kummer blowing up of X along I and denote it $[\mathrm{Bl}_I(X)] := Y$. A straightforward verification using Lemma 5.4.21 shows:

(1) The X-stack $Y = [\mathrm{Bl}_I(X)]$ is independent of the presentation $X = [X_0/X_1]$ and depends only on X and I. The uniqueness of Y is understood up to an isomorphism of X-stacks, which is unique up to a unique 2-isomorphism, again by [Fantechi et al. 2010, Proposition A.1]. If X is simple then Y is simple.

(2) If $f : X' \to X$ is a logarithmically smooth morphism and $I' = f^{-1}(I)$ then $[\mathrm{Bl}_{I'}(X')] = [\mathrm{Bl}_I(X)] \times_X X'$, the product taken in the fs category.

5.5.3. *Proof of Theorem 3.* If X is a toroidal scheme, then parts (i) and (iv) were proved in Theorem 5.4.5, parts (ii) and (iii) in Theorem 5.4.16, part (v) in Lemma 5.4.21, part (vi) in Lemma 5.4.19, and part (vii) in Lemma 5.4.18. In general, part (v) holds by (2) above, and this allows to reduce all other claims to the case of schemes. Namely, choose a strict étale covering $f : X' \to X$ of X by a toroidal scheme X', set $I' = f^{-1}(I)$, and consider the Kummer blowing up $Y' = [\mathrm{Bl}_{I'}(X')]$. Then $Y' = Y \times_X X'$, and all assertions for $Y \to X$ follow from the case of $Y' \to X'$ by étale descent. For example, $I_{Y/X} \times_X X' = I_{Y'/X'} = I_{Y'}$ is finite diagonalizable and acts trivially on the monoids $\overline{M}_{x'} = \overline{M}_{f(x')}$, hence the same is true for $I_{Y/X}$.

Appendix A: Existence of coarsenings

by David Rydh

A.1. *Classification of Deligne–Mumford coarsenings.*

A.1.1. *The category of coarsenings.* Recall that a *coarsening* is a morphism $f : X \to Y$ of Artin stacks such that Y is the coarse space of X relative to Y (Section 2.3.1). Equivalently, for any flat morphism $Y' \to Y$ from an algebraic space Y', the base change $f' : X' \to Y'$ is a coarse space. Equivalently, f is a universal homeomorphism with finite diagonal and $f_*\mathcal{O}_X = \mathcal{O}_Y$.

A priori, coarsenings $f : X \to Y$ of a fixed Artin stack X constitute a 2-category $\mathcal{C}_X$ where a 1-morphism from $f_1 : X \to Y_1$ to $f_2 : X \to Y_2$ is a 1-morphism $h : Y_1 \to Y_2$ together with a 2-morphism $\alpha : h \circ f_1 \Rightarrow f_2$; and a 2-morphism $(h_1, \alpha_1) \Rightarrow (h_2, \alpha_2)$ is a 2-morphism $\gamma : h_1 \Rightarrow h_2$ such that $\alpha_2 \circ \gamma = \alpha_1$. The 2-category $\mathcal{C}_X$ is, however, always equivalent to a partially ordered set (Theorem 2.3.6(iii)). The initial object of $\mathcal{C}_X$ is id_X. If X has finite inertia, then the final object of $\mathcal{C}_X$ is the usual coarse space, or *total coarsening*, $f : X \to X_{\mathrm{cs}}$ (Section 2.2.1).

A.1.2. *The main theorem.* Let $\mathcal{C}_X^{\mathrm{DM}} \subseteq \mathcal{C}_X$ denote the full 2-subcategory of DM-coarsenings, that is, coarsenings $X \to Y$ with Y a Deligne–Mumford stack. The purpose of this appendix is to prove the following classification result for DM-coarsenings.

Theorem A.1.3. *Let X be an Artin stack with finite inertia. The 2-category $\mathcal{C}_X^{\mathrm{DM}}$ is equivalent to the partially ordered set of open and closed subgroups $N \subseteq I_X$. A DM-coarsening $X \to Y$ corresponds to the subgroup $I_{X/Y} \subseteq I_X$.*

A morphism $\phi : X \to Z$, with Z Deligne–Mumford, factors uniquely through a given DM-coarsening $f : X \to Y$ if and only if the induced map on inertia $I_{X/Y} \to \phi^* I_Z$ is trivial (Theorem 2.3.6(i)). It follows that the map $(X \to Y) \mapsto I_{X/Y}$ is injective on DM-coarsenings.

If $f : X \to Y$ is a DM-coarsening, then $I_Y \to Y$ is finite and unramified so the unit section of I_Y is an open and closed immersion. Since $I_{X/Y} = \ker(I_X \to f^*I_Y)$ it follows that $I_{X/Y} \subseteq I_X$ is an open and closed subgroup.

It remains to prove that every open and closed subgroup N of I_X gives rise to a DM-coarsening. Note that any subgroup $N \subseteq I_X$ is necessarily normal: if T is a scheme, $\xi : T \to X$ is a morphism and s is a section of $\xi^*I_X \to T$, then s corresponds to a 2-morphism $u : \xi \Rightarrow \xi$ and the induced isomorphism $\xi^*N \to \xi^*N$ is conjugation by s (see the discussion in [Abramovich et al. 2008, Appendix A] right before Theorem A.1). The final object, corresponding to $N = I_X$, is the total coarsening morphism $X \to X_{\mathrm{cs}}$. Theorem A.1.3 is thus a generalization of the Keel–Mori theorem on the existence of total coarsenings.

A.1.4. *Étale neighborhoods with desired inertia.* The key step in the proof of the Keel–Mori theorem is the existence of a suitable étale neighborhood $h : W \to X$; see [Keel and Mori 1997, §4; Rydh 2013, Proposition 6.11]. Specifically, h should be inert, that is, $I_W = h^*I_X$, and W should admit a finite flat presentation by a scheme (this is the basic case where we know how to construct a coarse space). We give the following variant of this result.

Proposition A.1.5. *Let X be an Artin stack with finite inertia and let $N \subseteq I_X$ be an open and closed subgroup. Then there is a representable, separated, étale and surjective morphism $h : W \to X$ such that $I_W = h^*N$ as subgroups of h^*I_X.*

Proof. Let $p : U \to X$ be a locally quasifinite flat presentation [Rydh 2011, Theorem 7.1] (or [Stacks, Tag 04N0] if X is not quasiseparated). Note that p is separated. The relative Hilbert functor $\mathrm{Hilb}(U/X) \to X$ is thus representable, separated and locally of finite presentation. Indeed, if T is a scheme and $T \to X$ is a morphism, then $U \times_X T$ is an algebraic space, separated and locally of finite presentation over T, and hence so is $\mathrm{Hilb}(U/X) \times_X T = \mathrm{Hilb}(U \times_X T/T)$, by Artin's representability theorem [1969, Corollary 6.2].

Let $W' \subset \mathrm{Hilb}(U/X)$ be the open substack parametrizing open and closed subschemes along the fibers, namely, the restriction of the universal closed subscheme to W' is open in $\mathrm{Hilb}(U/X) \times_X U$. Let $h' : W' \to X$ be the structure map. It is representable, separated, étale and surjective, but allows for all possible open and closed subgroups of inertia. Over W' we have two open and closed subgroups $I_{W'} \subseteq h'^*I_X$ and $h'^*N \subseteq h'^*I_X$. The locus $W \subseteq W'$ where these coincide is open since $h'^*I_X \to W'$ is closed. It remains to verify that $h : W \to X$ is surjective which can be done on points.

Let $x : \operatorname{Spec} k \to X$ be a point with k algebraically closed. Then the stabilizer G_x acts freely on the finite k-scheme x^*U. Let $Z \subseteq x^*U$ be an open and closed subscheme such that x^*N acts set-theoretically transitively on Z, that is, Z is the preimage of a connected component of x^*U/x^*N. Then the stabilizer of $[Z]$ in W' is x^*N so $[Z]$ is a point in W lifting x. □

As in [Rydh 2013, Proposition 6.11], by construction the stacks W and W' admit finite flat presentations by AF-schemes.

A.1.6. *Proof of Theorem A.1.3.* Two Deligne–Mumford coarsenings $f_i : X \to Y_i$ with the same subgroups I_{X/Y_i} are uniquely isomorphic by Theorem 2.3.6. Given an open and closed subgroup $N \subseteq I_X$, take an étale neighborhood $h : W \to X$ as in Proposition A.1.5. Note that $I_{W \times_X W} = I_W \times_N I_W = I_W \times_X W$, hence the étale projections $W \times_X W \to W$ are inert. It follows from [Rydh 2013, Theorem 6.10] that the two induced maps $(W \times_X W)_{\mathrm{cs}} \to W_{\mathrm{cs}}$ are also étale morphisms and give rise to an étale groupoid. The quotient stack Y thus admits a morphism $X \to Y$ and, tautologically, $W = X \times_Y W_{\mathrm{cs}}$ and $h^* I_{X/Y} = I_W = h^* N$. The morphism $X \to Y$ is thus a Deligne–Mumford coarsening with $I_{X/Y} = N$.

A.2. *Examples of coarsenings.*

A.2.1. *Characteristic zero.* In characteristic zero, every stack with finite inertia is Deligne–Mumford and Theorem A.1.3 gives a full classification of all coarsenings.

A.2.2. *Tame Deligne–Mumford stacks.* If X is tame and Deligne–Mumford, then every coarsening is Deligne–Mumford. This is an immediate consequence of Theorem 2.3.6(i). Thus we obtain a full classification of all coarsenings in this case as well.

A.2.3. *Wild Deligne–Mumford stacks.* When X is Deligne–Mumford but not tame, then there may exist coarsenings that are not Deligne–Mumford. The following example is given in [Romagny et al. 2018, §4.5].

Let $U = \operatorname{Spec} \mathbb{F}_p[\epsilon, x]/(\epsilon^2)$ and let $G = \mathbb{Z}/p\mathbb{Z}$ act via $t.(\epsilon, x) = (\epsilon, x + t\epsilon)$. Let $X = [U/G]$. There is a p-torsion line bundle $\mathcal{L}$ on X corresponding to the trivial line bundle $\mathcal{O}_U \cdot e$ on U with action $t.e = (1 + t\epsilon)e$. The classifying map $\phi : X \to B\boldsymbol{\mu}_p$ induces a trivial map $I_X \to \boldsymbol{\mu}_p$ on inertia. Nevertheless, ϕ does not factor through the coarse space $f : X \to X_{\mathrm{cs}}$. If we let $Z = X_{\mathrm{cs}/B\boldsymbol{\mu}_p}$, then $X \to Z$ is a coarsening that is not Deligne–Mumford and $I_{X/Z} = I_X$.

A.2.4. *Tame Artin stacks.* When X is tame, then its coarsenings correspond to subgroups of inertia by Theorem 2.3.6(i). These subgroups are closed but not necessarily open as in the following example.

Let $U = \operatorname{Spec} \mathbb{F}_p[x]$ and let $G = \boldsymbol{\mu}_{2p} = \boldsymbol{\mu}_p \times \mathbb{Z}/2\mathbb{Z}$ act on U via $t.x = tx$. Let $X = [U/G]$ and $Y = [V/\boldsymbol{\mu}_p]$ where $V = \operatorname{Spec} \mathbb{F}_p[x^2]$ and the action is $t.x^2 = t^2 x^2$. The inertia stack of X is trivial except for a $\boldsymbol{\mu}_{2p}$ over the origin. The natural map $f : X \to Y$ is a coarsening and the closed subgroup $I_{X/Y} \subset I_X$ is not open: it is trivial except for a $\mathbb{Z}/2\mathbb{Z}$ over the origin.

A.2.5. *Initial DM-coarsening.* There is always an initial DM-coarsening of X corresponding to the intersection of all open and closed subgroups of I_X. This initial DM-coarsening need not commute with restrictions to open substacks though. The reason is that the identity component $(I_X)^0$ need not be open. For example, this happens if $X = BG$ where G is a 1-parameter deformation of $\mathbb{Z}/p\mathbb{Z}$ to $\boldsymbol{\mu}_p$ in mixed characteristic p or from $\mathbb{Z}/p\mathbb{Z}$ to $\boldsymbol{\alpha}_p$ in equal characteristic p. One can, however, show that $(I_X)^0$ is open and closed if X is a tame Artin stack in equal characteristic.

A.2.6. *Rigidifications.* When X is any Artin stack and $N \subseteq I_X$ is a *flat* subgroup, then there is a *rigidification* $f : X \to X \mathbin{/\!\!/} N$ [Abramovich et al. 2008, Appendix A]. This is a coarsening that also is an fppf-gerbe. It has the universal property that for any Artin stack Z, a morphism $\phi : X \to Z$ factors through f if and only if the induced map $N \to \phi^* I_Z$ is trivial. The universal property does not require Z to be Deligne–Mumford or X to be tame.

Appendix B: Torification

B.1. *The torification functors.*

B.1.1. *The general case.* Let W be a toroidal scheme acted on by a diagonalizable group G in a relatively affine way. For example, any action of G on a quasiaffine scheme is relatively affine. The main results of [Abramovich and Temkin 2017] establish a so-called torification $\widetilde{\mathcal{T}}_{W,G} : W^{\mathrm{tor}} \to W$, which is a composition of two G-equivariant morphisms of toroidal schemes: the barycentric subdivision and the normalized blowing up of a so-called torifying ideal, see [op. cit., Theorem 4.6.5], such that the action on W^{tor} is toroidal. The barycentric subdivision is naturally a composition of blowings up, see [op. cit., §4.1.2]. The resulting sequence of normalized blowings up is compatible with strict strongly G-equivariant morphisms $f : W' \to W$ in the sense that $\widetilde{\mathcal{T}}_{W',G'}$ is the *contracted pullback* of $\widetilde{\mathcal{T}}_{W,G}$, i.e., $f^*(\widetilde{\mathcal{T}}_{W,G})$ with all empty blowings up removed. Furthermore, it is shown in [op. cit., Theorem 5.4.5] that the normalized blowing up of a torifying ideal I_W can also be realized as a blowing up of another ideal I'_W, in particular, $\widetilde{\mathcal{T}}_{W,G}$ is a projective modification even when W is not qe and it is not obvious a priori that normalizations are finite. However, the resulting realization of $W^{\mathrm{tor}} \to W$ as a sequence of blowings up, that we denote $\widetilde{\mathcal{T}}'_{W,G}$, is only compatible with surjective morphisms $f : W' \to W$ as above.

B.1.2. *Simple actions.* If the action is simple then slightly stronger results are available; see [Abramovich and Temkin 2017, Theorems 4.6.3 and 5.4.2]. In particular, torification is achieved by a single G-equivariant normalized blowing up $\mathcal{T}_{W,G} : W^{\mathrm{tor}} \to W$, and the quotient morphism $\mathcal{T}^0_{W,G} : W^{\mathrm{tor}} /\!\!/ G \to W /\!\!/ G$ has a natural structure of a normalized blowing up. This is compatible with strict strongly G-equivariant morphisms $f : W' \to W$. In addition, both morphisms can be enhanced to blowings up, that we denote $\mathcal{T}'_{W,G}$ and $\mathcal{T}'^0_{W,G}$. This involves the choice of a large enough threshold n — their centers are obtained from the centers of $\mathcal{T}_{W,G}$ and $\mathcal{T}^0_{W,G}$ by raising them to the n-th powers and applying the integral closure operation. As a result, $\mathcal{T}'_{W,G}$ and $\mathcal{T}'^0_{W,G}$ are only compatible with surjective morphisms.

B.1.3. *Birationality.* In [Abramovich and Temkin 2017, Theorems 4.6.3, 4.6.5, 5.4.2, and 5.4.5] it was shown that the torification functors used here are birational modifications only under a technical assumption that the action is *full*. For the purpose of this article we note the following:

Proposition B.1.4. *Assume G is finite. Then the torification morphisms are birational.*

Proof. For a point $w \in W$ write $\eta(w)$ for the generic point specializing to w — it is unique since W is normal. The subset $U_1 \subset W$ where the logarithmic structure is trivial and the subset $U_2 \subset W$ where $G_w = G_{\eta(w)}$ are both open, invariant, and dense, hence the same is true for $U = U_1 \cap U_2$. Since G is finite the strict embedding $U \hookrightarrow W$ is strongly equivariant, hence the torific ideal restricts to $\mathcal{O}_U$ and the torification morphisms are trivial on U. □

We note that, when G is infinite, some assumption on the action is necessary: the standard action of $\mathbb{G}_m$ on $\mathbb{A}^1$ has $\sigma_x = \{1\}$, which cannot be balanced since $\mathcal{I}_{-1} = 0$.

B.2. ***Stronger functoriality.*** Using the methods of [Abramovich and Temkin 2018] one can easily show that the functors $\widetilde{\mathcal{T}}$ and $\mathcal{T}$ possess stronger functoriality properties than asserted there. Let us discuss this strengthening.

B.2.1. *λ-equivariance.* We start with an aspect that holds for both algorithms. Recall that a G-morphism $f : W' \to W$ is *strongly equivariant* if f is the base change of the GIT quotient $f /\!\!/ G$. Some criteria of strong equivariance and related properties can be found in [Abramovich and Temkin 2018, Theorem 1.3.1 and Lemma 5.6.2; Rydh 2020]. More generally, assume that G' acts on W', G acts on W, and f is λ-equivariant for a homomorphism $\lambda : G' \to G$. We say that f is *strongly λ-equivariant* if it is fix-point reflecting and the G-morphism

$$W' \times^{G'} G = (W' \times G)/G' \to W$$

is strongly equivariant. Recall that the fixed-point reflecting condition means that f induces an isomorphism $G'_x = G_{f(x)}$ for any $x \in W'$, and hence G' acts freely on $W' \times G$.

Theorem B.2.2. *Assume that toroidal schemes W and W' are provided with relatively affine actions of diagonalizable groups G and G', respectively. Further assume that $\lambda : G' \to G$ is a homomorphism, and $f : W' \to W$ is a strict and strongly λ-equivariant morphism. Then $\widetilde{\mathcal{T}}_{W',G'}$ is the contracted pullback of $\widetilde{\mathcal{T}}_{W,G}$. In addition, $\widetilde{\mathcal{T}}'_{W',G'}$ is the contracted pullback of $\widetilde{\mathcal{T}}'_{W,G}$ if f is surjective.*

Proof. This happens because $\widetilde{\mathcal{T}}$ is defined in terms of local combinatorial data $(\overline{M}_x, G_x, \sigma_x)$, see [Abramovich and Temkin 2017, Section 3.6.8], and the latter only depends on G_x rather than on the entire G. □

B.2.3. *Weakening the strictness assumption.* A finer observation is that the strictness assumption is not so essential for the functoriality of $\mathcal{T}$. For comparison, note that $\widetilde{\mathcal{T}}$ is constructed using barycentric subdivisions which depend on the monoids $\overline{M}_x$, hence it is not functorial with respect to nonstrict morphisms.

Theorem B.2.4. *Assume that toroidal schemes W and W' are provided with relatively affine and simple actions of diagonalizable groups G and G', respectively, $\lambda : G' \to G$ is a homomorphism, and $f : W' \to W$ is a strongly λ-equivariant morphism. Further assume that for any point $x' \in W'$ with $x = f(x')$ the restriction $f_S : S' \to S$ of f to the logarithmic strata through x' and x is strongly λ-equivariant. Then the normalized blowings up $\mathcal{T}_{W',G'}$ and $\mathcal{T}^0_{W',G'}$ are the pullbacks of $\mathcal{T}_{W,G}$ and $\mathcal{T}^0_{W,G}$, respectively. If f is also surjective, then the same is true for the blowings up $\mathcal{T}'_{W',G'}$, $\mathcal{T}'^0_{W',G'}$ and $\mathcal{T}'_{W,G}$, $\mathcal{T}'^0_{W,G}$.*

Proof. Note that a reference to [Abramovich and Temkin 2017, Lemma 4.2.13(ii)] is the only place in the proof of [op. cit., Theorem 4.6.3], where one uses the assumption that f is strict. The lemma asserts that f respects the reduced signatures: $f^*(\sigma_x) = \sigma_{x'}$. Recall that the latter are defined as the multisets of nontrivial characters through which G_x acts on the cotangent spaces to S and S' at x and x', respectively. But we assume that f_S is strongly G_x-equivariant, hence $f^*(\sigma_x) = \sigma_{x'}$ by [op. cit., Lemma 3.6.4], and we avoid the use of [op. cit., Lemma 4.2.13(ii)]. □

B.2.5. *Logarithmically smooth morphisms.* The assumption that $f : W' \to W$ is strong can be omitted when f is logarithmically smooth. For this we need the following instance of Luna's fundamental lemma.

Lemma B.2.6. *Assume that Y and X are toroidal schemes provided with relatively affine actions of étale diagonalizable groups, the action on Y is simple, $\lambda : H \to G$ is a homomorphism, and $f : Y \to X$ is a logarithmically smooth λ-equivariant inert morphism. Then f is strongly λ-equivariant.*

Proof. Replacing Y by $Y \times^H G$ we can assume that $G = H$. In addition, it suffices to work locally on $Y /\!\!/ G$ and $X /\!\!/ G$, hence we can assume that these schemes are local and f is surjective. Since f is logarithmically smooth and inert, simplicity of the action on Y implies that the action on X is simple too.

In addition, let $\widetilde{G}$ denote the stabilizer of the closed orbits of Y and X. Then $f /\!\!/ \widetilde{G}$ is strongly $G/\widetilde{G}$-equivariant because $G/\widetilde{G}$ acts freely on $Y /\!\!/ \widetilde{G}$ and $X /\!\!/ \widetilde{G}$. Therefore, it suffices to prove that f is strongly $\widetilde{G}$-equivariant, and replacing G by $\widetilde{G}$ and localizing again, we can assume that $G = \widetilde{G}$.

Note that if f is strict, then it is a smooth morphism and the claim was proved in Luna's lemma [Abramovich and Temkin 2018, Theorem 1.3.1(2b)]. We will deduce the lemma from this particular case. In particular, using this claim we can replace X and Y by their equivariant étale covers, hence by [Abramovich and Temkin 2017, Proposition 3.2.10(i); Illusie and Temkin 2014, Proposition 1.2] we can assume that there exist an equivariant chart $P \to Q$, $X \to \boldsymbol{A}_P$, $Y \to \boldsymbol{A}_Q$ of f, where $\boldsymbol{A}_M = \operatorname{Spec}(\mathbb{Z}[M])$ and the actions are trivial on P and Q. Then the morphism $g : Y_P[Q] = Y \times_{\boldsymbol{A}_P} \boldsymbol{A}_Q \to Y$ is strong as both g and $g /\!\!/ G$ are pullbacks of $\boldsymbol{A}_Q \to \boldsymbol{A}_P$. In addition, $Y \to Y_P[Q]$ is strict and hence smooth. It remains to observe that $Y \to Y_P[Q]$ is also fix-points preserving, and hence it is strongly smooth by the above case. □

As an application we obtain:

Corollary B.2.7. *Assume that toroidal schemes W and W' are provided with relatively affine and simple actions of étale diagonalizable groups G and G', respectively, $\lambda : G' \to G$ is a homomorphism, and $f : W' \to W$ is a logarithmically smooth, fix-point reflecting, λ-equivariant morphism. Then the normalized blowings up $\mathcal{T}_{W',G'}$ and $\mathcal{T}^0_{W',G'}$ are the pullbacks of $\mathcal{T}_{W,G}$ and $\mathcal{T}^0_{W,G}$, respectively. If f is also surjective, then the same is true for the blowings up $\mathcal{T}'_{W',G'}$, $\mathcal{T}'^0_{W',G'}$ and $\mathcal{T}'_{W,G}$, $\mathcal{T}'^0_{W,G}$.*

Proof. Since f is strongly equivariant by Lemma B.2.6, the claim will follow from Theorem B.2.4 once we prove that the induced morphisms $f_S : S' \to S$ between the logarithmic strata are strongly equivariant. Since f_S is logarithmically smooth, f_S is smooth. Clearly, f_S is fix-point reflecting. Since the groups are finite, all orbits are special and hence f_S is inert [Abramovich and Temkin 2018, §5.1.8 and §5.5.3]. Thus, f_S is strongly equivariant (even strongly smooth) by [Abramovich and Temkin 2018, Theorem 1.1.3(ii)]. □

Acknowledgements

We are thankful to David Rydh for detailed and precise suggestions and criticism, reaching almost every page of this manuscript, as well as for Appendix A.

References

[Abramovich and Temkin 2017] D. Abramovich and M. Temkin, "Torification of diagonalizable group actions on toroidal schemes", *J. Algebra* **472** (2017), 279–338. MR Zbl

[Abramovich and Temkin 2018] D. Abramovich and M. Temkin, “Luna’s fundamental lemma for diagonalizable groups”, *Algebr. Geom.* **5**:1 (2018), 77–113. MR Zbl

[Abramovich and Vistoli 2002] D. Abramovich and A. Vistoli, “Compactifying the space of stable maps”, *J. Amer. Math. Soc.* **15**:1 (2002), 27–75. MR Zbl

[Abramovich et al. 2008] D. Abramovich, M. Olsson, and A. Vistoli, “Tame stacks in positive characteristic”, *Ann. Inst. Fourier* (*Grenoble*) **58**:4 (2008), 1057–1091. MR Zbl

[Abramovich et al. 2011] D. Abramovich, M. Olsson, and A. Vistoli, “Twisted stable maps to tame Artin stacks”, *J. Algebraic Geom.* **20**:3 (2011), 399–477. Correction in **24**:2 (2015), 399–400. MR Zbl

[Abramovich et al. 2020] D. Abramovich, M. Temkin, and J. Włodarczyk, “Principalization of ideals on toroidal orbifolds”, *J. Eur. Math. Soc.* (*JEMS*) (online publication August 2020).

[Artin 1969] M. Artin, “Algebraization of formal moduli, I”, pp. 21–71 in *Global analysis*, edited by D. C. Spencer and S. Iyanaga, Univ. Tokyo Press, 1969. MR Zbl

[Bergh 2017] D. Bergh, “Functorial destackification of tame stacks with abelian stabilisers”, *Compos. Math.* **153**:6 (2017), 1257–1315. MR Zbl

[Fantechi et al. 2010] B. Fantechi, E. Mann, and F. Nironi, “Smooth toric Deligne–Mumford stacks”, *J. Reine Angew. Math.* **648** (2010), 201–244. MR Zbl

[Gabber and Ramero 2004] O. Gabber and L. Ramero, “Foundations for almost ring theory”, preprint, 2004. Release 7.5. arXiv

[Harper 2017] A. Harper, “Factorization for stacks and boundary complexes”, preprint, 2017. arXiv

[Illusie and Temkin 2014] L. Illusie and M. Temkin, “Gabber’s modification theorem (log smooth case)”, pp. 167–212 in *Travaux de Gabber sur l’uniformisation locale et la cohomologie étale des schémas quasi-excellents*, edited by L. Illusie et al., Astérisque **363-364**, Soc. Math. France, Paris, 2014. MR Zbl

[Kato 1994] K. Kato, “Toric singularities”, *Amer. J. Math.* **116**:5 (1994), 1073–1099. MR Zbl

[Keel and Mori 1997] S. Keel and S. Mori, “Quotients by groupoids”, *Ann. of Math.* (2) **145**:1 (1997), 193–213. MR Zbl

[Kempf et al. 1973] G. Kempf, F. F. Knudsen, D. Mumford, and B. Saint-Donat, *Toroidal embeddings, I*, Lecture Notes in Math. **339**, Springer, 1973. MR Zbl

[Nizioł 2006] W. Nizioł, “Toric singularities: log-blow-ups and global resolutions”, *J. Algebraic Geom.* **15**:1 (2006), 1–29. MR Zbl

[Nizioł 2008] W. Nizioł, “K-theory of log-schemes, I”, *Doc. Math.* **13** (2008), 505–551. MR

[Olsson 2003] M. C. Olsson, “Logarithmic geometry and algebraic stacks”, *Ann. Sci. École Norm. Sup.* (4) **36**:5 (2003), 747–791. MR Zbl

[Romagny et al. 2018] M. Romagny, D. Rydh, and G. Zalamansky, “The complexity of a flat groupoid”, *Doc. Math.* **23** (2018), 1157–1196. MR Zbl

[Rydh 2011] D. Rydh, “Étale dévissage, descent and pushouts of stacks”, *J. Algebra* **331** (2011), 194–223. MR Zbl

[Rydh 2013] D. Rydh, “Existence and properties of geometric quotients”, *J. Algebraic Geom.* **22**:4 (2013), 629–669. MR Zbl

[Rydh 2020] D. Rydh, “A generalization of Luna’s fundamental lemma for stacks with good moduli spaces”, preprint, 2020. arXiv

[Stacks] P. Belmans, A. J. de Jong, et al., “The Stacks project”, electronic reference, available at http://stacks.math.columbia.edu.

[Talpo and Vistoli 2018] M. Talpo and A. Vistoli, “Infinite root stacks and quasi-coherent sheaves on logarithmic schemes”, *Proc. Lond. Math. Soc.* (3) **116**:5 (2018), 1187–1243. MR Zbl

Communicated by Hélène Esnault
Received 2018-04-07 Revised 2020-02-01 Accepted 2020-03-25

abrmovic@math.brown.edu *Brown University, Providence, RI, United States*

michael.temkin@mail.huji.ac.il *The Hebrew University of Jerusalem, Jerusalem, Israel*

wlodar@math.purdue.edu *Purdue University, West Lafayette, IN, United States*

dary@math.kth.se *KTH Royal Institute of Technology, Stockholm, Sweden*

ALGEBRA AND NUMBER THEORY 14:8 (2020)
https://doi.org/10.2140/ant.2020.14.2037

Auslander correspondence for triangulated categories

Norihiro Hanihara

We give analogues of the Auslander correspondence for two classes of triangulated categories satisfying certain finiteness conditions. The first class is triangulated categories with additive generators and we consider their endomorphism algebras as the Auslander algebras. For the second one, we introduce the notion of [1]-additive generators and consider their graded endomorphism algebras as the Auslander algebras. We give a homological characterization of the Auslander algebras for each class. Along the way, we also show that the algebraic triangle structures on the homotopy categories are unique up to equivalence.

1. Introduction

The main concern in representation theory of algebras is to understand the module categories. Among such categories, those with *finitely many* indecomposable objects, or equivalently the *representation-finite* algebras, are most fundamental. Let us recall the following famous theorem due to Auslander [1971]:

Theorem 1.1 (Auslander correspondence). *There exists a bijection between the set of Morita equivalence classes of finite dimensional algebras* Λ *of finite representation type and the set of Morita equivalence classes of finite dimensional algebras* Γ *such that* $\operatorname{gl.dim}\Gamma \leq 2$ *and* $\operatorname{dom.dim}\Gamma \geq 2$.

This theorem states that a categorical property (=representation-finiteness) of $\mathsf{mod}\,\Lambda$ can be characterized by homological invariants (=gl. dim and dom. dim) of Γ, called the *Auslander algebra* of $\mathsf{mod}\,\Lambda$. There are many results of this type giving the relationships between categorical properties of those appearing naturally in representation theory, and homological properties of their "Auslander algebras", for example, [Iyama 2005; 2007; Enomoto 2018].

The aim of this paper is to find an analogue of these results for triangulated categories [Neeman 2001]. Let k be an arbitrary field and $\mathcal{T}$ be a k-linear, Hom-finite, idempotent-complete triangulated category. We consider two kinds of finiteness conditions on triangulated categories.

The first one is a direct analogue of representation-finiteness: $\mathcal{T}$ is *finite*, that is, $\mathcal{T}$ has finitely many indecomposable objects up to isomorphism. In this case, $\mathcal{T}$ has an additive generator M. We call $\mathsf{End}_{\mathcal{T}}(M)$ the *Auslander algebra* of $\mathcal{T}$, which is uniquely determined by $\mathcal{T}$ up to Morita equivalence. The first main result of this paper is the following homological characterization of the Auslander algebras of triangulated categories. We say that a finite dimensional algebra A is *twisted* n*-periodic* if it is self-injective and there

This work is supported by JSPS KAKENHI Grant Number JP19J21165.
MSC2010: primary 18E30; secondary 16E05, 16E65, 16G70.
Keywords: triangulated category, Auslander correspondence, periodic algebra, Cohen–Macaulay module.

exists an automorphism α of A such that $\Omega^n \simeq (-)_\alpha$ as functors on $\underline{\mathsf{mod}}\,A$. We refer to Corollary 2.2 for equivalent characterizations.

Theorem 1.2. *Let k be a perfect field. The following are equivalent for a basic finite dimensional k-algebra A:*

(1) *A is the Auslander algebra of a k-linear*, Hom-*finite*, *idempotent-complete triangulated category which is finite.*

(2) *A is twisted* 3*-periodic.*

This result shows a close connection between periodic algebras [Erdmann and Skowroński 2008] and triangulated categories. Our proof depends on Amiot's result (Proposition 3.2). This is a complement of Heller's classical observation [1968, 16.4] which gives a parametrization of pretriangle structures on a pretriangulated category $\mathcal{T}$ in terms of isomorphisms $\Omega^3 \simeq [-1]$ on $\underline{\mathsf{mod}}\,\mathcal{T}$. Later practice of this property of the third syzygy in representation theory can be seen in [Auslander and Reiten 1996; Yoshino 2005; Amiot 2007; Iyama and Oppermann 2013].

Moreover, with some additional assumptions on $\mathcal{T}$, we give a bijection between finite triangulated categories and certain algebras, which is a more precise form of the above theorem; see Theorem 3.4. Furthermore, after submitting this article, a similar result by Muro [2020] appeared. His main result enables us to state Theorem 3.4 with less additional assumptions; see Remark 3.5.

The second finiteness condition is the following:

(S1) There is an object $M \in \mathcal{T}$ such that $\mathcal{T} = \mathsf{add}\{M[n] \mid n \in \mathbb{Z}\}$.

(S2) For any $X, Y \in \mathcal{T}$, $\mathsf{Hom}_{\mathcal{T}}(X, Y[n]) = 0$ holds for almost all n.

If these conditions are satisfied, we say $\mathcal{T}$ is [1]-*finite* and call M as in (S1) a [1]-*additive generator*. For example, the bounded derived categories of representation-finite hereditary algebras are [1]-finite, and additive generators for module categories are [1]-additive generators for the derived categories. There are various studies on [1]-finite triangulated categories, for example [Rouquier 2008; Xiao and Zhu 2005; Amiot 2007]. Note that [1]-finite triangulated categories have infinitely many indecomposable objects unless $\mathcal{T} = 0$.

For a [1]-finite triangulated category $\mathcal{T}$ with a [1]-additive generator M, we call

$$C = \bigoplus_{n\in\mathbb{Z}} \mathsf{Hom}_{\mathcal{T}}(M, M[n])$$

the [1]-*Auslander algebra* of $\mathcal{T}$, which is naturally a $\mathbb{Z}$-graded algebra and is uniquely determined by $\mathcal{T}$ up to graded Morita equivalence. Thanks to our condition (S2), C is finite dimensional. To study it, we prepare some results on "graded projectivization" in Section 4 (see Proposition 4.2). Such constructions of graded algebras appear naturally in various contexts [Artin and Zhang 1994; Asashiba 2017].

Our second main result is the Auslander correspondence for [1]-finite triangulated categories. To state it, we have to restrict to a nice class of triangulated categories called *algebraic*. Recall that they are the stable categories of Frobenius categories [Happel 1988, I.2.6]. Algebraic triangulated categories are enhanced by differential graded categories [Keller 2006], and play a central role in tilting theory [Angeleri Hügel et al. 2007].

Now we can formulate the following second main result of this paper in terms of algebraic triangulated categories and graded algebras. We say that a finite dimensional $\mathbb{Z}$-graded algebra A is *(a)-twisted n-periodic* if it is self-injective and there exists a graded automorphism α of A such that $P_\alpha \simeq P$ for all $P \in \mathsf{proj}^{\mathbb{Z}} A$ and $\Omega^n \simeq (-)_\alpha(a)$ as functors on $\underline{\mathsf{mod}}^{\mathbb{Z}} A$. We refer to Corollary 2.4 for equivalent conditions.

Theorem 1.3. *Let k be an algebraically closed field. There exists a bijection between the following*:

(1) *The set of triangle equivalence classes of k-linear*, Hom*-finite*, *idempotent-complete*, *algebraic triangulated categories $\mathcal{T}$ which are* [1]*-finite.*

(2) *The graded Morita equivalence classes* (*see Definition* 4.3) *of finite dimensional graded k-algebra C which are* (-1)*-twisted* 3*-periodic.*

(3) *A disjoint union of Dynkin diagrams of type A*, *D*, *and E.*

The correspondences are given as follows:

- *From* (1) *to* (2): *Taking the* [1]*-Auslander algebra of $\mathcal{T}$.*
- *From* (1) *to* (3): *Taking the tree type of the AR-quiver of $\mathcal{T}$.*
- *From* (2) *to* (1): $C \mapsto \mathsf{proj}^{\mathbb{Z}} C$.
- *From* (3) *to* (1): $Q \mapsto k(\mathbb{Z}Q)$, *where $k(\mathbb{Z}Q)$ is the mesh category associated with $\mathbb{Z}Q$.*

Moreover, we have the following explicit descriptions of (1) and (2) in the above theorem.

Theorem 1.4 (Theorem 5.3, Proposition 6.1). *The classes* (1) *and* (2) *in Theorem 1.3 are the same as* $(1')$ *and* $(2')$, *respectively*:

$(1')$ *The set of triangle equivalence classes of the bounded derived categories* $\mathsf{D}^{\mathsf{b}}(\mathsf{mod}\, kQ)$ *of the path algebra kQ for a disjoint union Q of Dynkin quivers of type A*, *D*, *and E.*

$(2')$ *The orbit algebras $k(\mathbb{Z}Q)/[1]$ for a disjoint union Q of Dynkin quivers of type A*, *D*, *and E.*

Compared to Theorem 1.2, Theorem 1.3 is more strict in the point that the Auslander algebras C correspond *bijectively* to the triangulated categories. This can be done by the classification of [1]-finite triangulated categories as is stated in $(1')$. These results suggest that [1]-finite triangulated categories are easier than finite ones in controlling their triangle structures as well as their additive structures.

Our classification is deduced from the following uniqueness of the triangle structures on the homotopy categories, which is somehow surprising; compare [Keller 2018].

Theorem 1.5 (Theorem 5.1). *Let Λ be a ring such that* $\mathsf{K}^{\mathsf{b}}(\mathsf{proj}\,\Lambda)$ *is a Krull–Schmidt category and Λ does not have a semisimple ring summand*, *and let $\mathcal{C}$ be an algebraic triangulated category. If $\mathcal{C}$ and* $\mathsf{K}^{\mathsf{b}}(\mathsf{proj}\,\Lambda)$ *are equivalent as additive categories*, *then they are equivalent as triangulated categories.*

For example, $\mathsf{K}^{\mathrm{b}}(\mathsf{proj}\,\Lambda)$ is Krull–Schmidt if Λ is a module-finite algebra over a complete Noetherian local ring. We actually see that the possible triangle structure on a given Krull–Schmidt additive category is unique in the sense that the suspensions and the mapping cones are uniquely determined as objects, see Proposition 5.5 for details.

As an application of our classification Theorem 1.4 of [1]-finite triangulated categories, we recover the main result of [Chen et al. 2008] stating that any finite dimensional algebra over an algebraically closed field with derived dimension 0 is piecewise hereditary of Dynkin type.

We also apply Theorem 1.4 to Cohen–Macaulay representation theory. A rich source of [1]-finite triangulated categories is given by CM-finite Iwanaga–Gorenstein algebras [Curtis and Reiner 1981; 1987; Leuschke and Wiegand 2012; Simson 1992; Yoshino 1990], for example, simple singularities and trivial extension algebras of representation-finite hereditary algebras. We consequently obtain the following result, which states that $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ is triangle equivalent to the derived category of a Dynkin quiver under some mild assumptions.

Corollary 1.6 (Theorem 7.3). *Let k be an algebraically closed field and $\Lambda = \bigoplus_{n\geq 0}\Lambda_n$ be a positively graded* CM*-finite Iwanaga–Gorenstein algebra such that each Λ_n is finite dimensional over k and Λ_0 has finite global dimension. Then, the stable category $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ is* [1]*-finite and therefore, it is triangle equivalent to $\mathsf{D}^{\mathrm{b}}(\mathsf{mod}\,kQ)$ for a disjoint union Q of some Dynkin quivers of type A, D, and E.*

This partially recovers [Kajiura et al. 2007; Buchweitz et al. 2020, 2.2] in a quite different way. Note that our result is more general, but less explicit in the sense that Corollary 1.6 does not give the type of Q from given Λ.

As this application suggests, our classification shows that the "easiest" triangulated categories are very likely to be the derived category of Dynkin quivers, and provides a completely different method (from a direct construction of tilting objects) of giving a triangle equivalence for such categories.

Notations and conventions. We denote by k a field. For a category $\mathcal{C}$, we denote by $\mathsf{Hom}_{\mathcal{C}}(-,-)$ or simply $\mathcal{C}(-,-)$ the Hom-spaces between the objects and by $J_{\mathcal{C}}(-,-)$ the Jacobson radical of $\mathcal{C}$. A $\mathcal{C}$-module is a contravariant functor from $\mathcal{C}$ to the category of abelian groups. A $\mathcal{C}$-module M is finitely presented if there is an exact sequence

$$\mathcal{C}(-,X) \to \mathcal{C}(-,Y) \to M \to 0$$

for some $X, Y \in \mathcal{C}$. We denote by $\mathsf{mod}\,\mathcal{C}$ the category of finitely presented $\mathcal{C}$-modules. If $\mathcal{C}$ is graded by a group G, the category of finitely presented graded functor is denoted by $\mathsf{mod}^G\mathcal{C}$, and its projectives by $\mathsf{proj}^G\mathcal{C}$. The morphism space in $\mathsf{mod}^G\mathcal{C}$ is denoted by $\mathsf{Hom}_{\mathcal{C}}(-,-)_0$ or $\mathcal{C}(-,-)_0$. The category $\mathsf{mod}^G\mathcal{C}$ is endowed with the grade shift functor (g) for each $g \in G$, defined by $M(g) = M$ as an ungraded module and $(M(g)(X))_h = (MX)_{gh}$ for each $X \in \mathcal{C}$.

Similarly, for a k-algebra A, the Jacobson radical of A is denoted by J_A. A module over A means a finitely generated right module. We denote by $\mathsf{mod}\,A$ (resp. $\mathsf{proj}\,A$) the category of (projective) A-modules. If A is graded, the category of graded (projective) A-modules is denoted by $\mathsf{mod}^G A$ (resp. $\mathsf{proj}^G A$).

2. Periodicity of syzygies

Let A be a k-algebra. We denote by A^e the enveloping algebra $A^{\mathrm{op}} \otimes_k A$ and by Ω_A (resp. Ω_{A^e}) the syzygy, that is, the kernel of the projective cover in $\operatorname{mod} A$ (resp. $\operatorname{mod} A^e$). In this section, we generalize for our purpose the result of Green, Snashall and Solberg [Green et al. 2003] which relates the periodicity of syzygy of simple A-modules and that of A considered as a bimodule over itself. The following theorem and its proof is a graded and twisted version of [loc. cit., 1.4].

Theorem 2.1. *Let G be an abelian group and A be a finite dimensional, ring-indecomposable, non-semisimple G-graded k-algebra. Assume that $J_A = J_{A_0} \oplus (\bigoplus_{i \neq 0} A_i)$ and that A/J_A is separable over k. Then, the following are equivalent for $a \in G$ and $n > 0$:*

1. *$\Omega_A^n(A/J_A) \simeq A/J_A(a)$ in $\operatorname{mod}^G A$.*
2. *A is self-injective and there exists a graded algebra automorphism α of A such that $\Omega^n \simeq (-)_\alpha(a)$ as functors on $\underline{\operatorname{mod}}^G A$.*
3. *There exists a graded algebra automorphism α of A such that $\Omega_{A^e}^n(A) \simeq {}_1A_\alpha(a)$ in $\operatorname{mod}^G A^e$.*

Proof. By the original case, we have that A is self-injective under the assumption (3). Then the implication (3) $\Rightarrow$ (2) follows. Also, (2) $\Rightarrow$ (1) is clear.

It remains to prove (1) implies (3). Note that by our assumption on J_A, it is graded and any simple object in $\operatorname{mod}^G A$ is simple in $\operatorname{mod} A$. Assume (1) holds and set $B = \Omega_{A^e}^n(A)$. This is a projective A-module on each side.

Step 1: *$S \otimes_A B$ is simple for all graded simple (right) A-modules S.*

Let S be a graded simple A-module. Then, applying $S \otimes_A -$ to the minimal projective resolution $P\colon \cdots \to P_i \xrightarrow{d_i} P_{i-1} \to \cdots \to P_0$ of A in $\operatorname{mod}^G A^e$ yields the minimal projective resolution of S in $\operatorname{mod}^G A$. Indeed, since A/J_A is separable over k, we have $J_{A^e} = J_A \otimes_k A + A \otimes_k J_A$. Then, $\operatorname{Im} d_i \subset P_{i-1} J_{A^e} = J_A P_{i-1} + P_{i-1} J_A$ by the minimality of P and therefore, $\operatorname{Im}(S \otimes d_i) \subset S \otimes_A P_{i-1} J_A$ by $S \otimes_A J_A P_{i-1} = 0$. This shows $S \otimes_A P$ is minimal. Therefore we have $S \otimes_A B \simeq \Omega_A^n(S)$, which is simple by assumption (1).

It follows by induction that the exact functor $- \otimes_A B$ preserves length.

Step 2: *$B \simeq A(a)$ in $\operatorname{mod}^G A$.*

Consider the exact sequence $0 \to J_A \to A \to A/J_A \to 0$ in $\operatorname{mod}^G A$. Applying $- \otimes_A B$ yields $B \to A/J_A(a) \to 0$. This shows that the module B contains $A/J_A(a)$ in its top. But since B is a projective (right) A-module having the same length as A by the remark following Step 1, we see that $B \simeq A(a)$ in $\operatorname{mod}^G A$.

Step 3: *There exists a graded algebra automorphism α of A such that $\Omega_{A^e}^n(A) \simeq {}_1A_\alpha(a)$.*

By Step 2, there exists a graded algebra endomorphism α of A such that $B \simeq {}_\alpha A_1(a)$ in $\operatorname{mod}^G A^e$. Indeed, fix an isomorphism $\varphi\colon A(a) \to B$ in $\operatorname{mod}^G A$, put $x = \varphi(1)$, and set $\alpha(u) = \varphi^{-1}(ux)$ for $u \in A$. Then, α is of degree 0, since x and φ are, and it is easily checked that α is an algebra endomorphism and that $\varphi\colon {}_{\alpha}A_1(a) \to B$ is an isomorphism in $\mathsf{mod}^G A^e$. Now we show that α is an isomorphism. Let I be the kernel of α. Since $B \simeq {}_{\alpha}A$ is a projective left A-module, the inclusion $I \subset A$ in $\mathsf{mod}^G A$ stays injective by applying $- \otimes_A {}_{\alpha}A$. But since the map $I \otimes_A {}_{\alpha}A \to {}_{\alpha}A$ is zero, we have $I \otimes_A {}_{\alpha}A = 0$, and we conclude that $I = 0$ by the remark following Step 1.

This finishes the proof of (1) ⇒ (3). □

We need the following two particular cases. The first one, which we will use in Section 3 is the following result for $G = \{1\}$, where the special case "$\Omega^n(S) \simeq S$ for all simples" is [Green et al. 2003, 1.4].

Corollary 2.2. *Let A be a ring-indecomposable, nonsemisimple finite dimensional k-algebra such that A/J_A is separable over k. Then, the following are equivalent for $n > 0$:*

(1) $\Omega^n_A(A/J_A) \simeq A/J_A$.

(2) *A is self-injective and there exists an automorphism α of A such that $\Omega^n \simeq (-)_\alpha$ as functors on $\underline{\mathsf{mod}}\, A$.*

(3) *There exists an automorphism α of A such that $\Omega^n_{A^e}(A) \simeq {}_1A_\alpha$ in $\mathsf{mod}\, A^e$.*

We name such algebras as follows:

Definition 2.3. A finite dimensional algebra is *twisted n-periodic* if it is a direct product of simple algebras or algebras satisfying the equivalent conditions in Corollary 2.2.

The second one is the following for $G = \mathbb{Z}$ and the permutation of simples is the identity, which will be used in Section 6.

Corollary 2.4. *Let A be a finite dimensional, ring-indecomposable, nonsemisimple $\mathbb{Z}$-graded k-algebra such that A/J_A is separable over k. Then, the following are equivalent for $a \in \mathbb{Z}$ and $n > 0$:*

(1) *$\Omega^n_A(S) \simeq S(a)$ in $\mathsf{mod}^{\mathbb{Z}} A$ for any simple objects in $\mathsf{mod}^{\mathbb{Z}} A$.*

(2) *A is self-injective and there exists a graded algebra automorphism α of A such that $\Omega^n \simeq (-)_\alpha(a)$ as functors on $\underline{\mathsf{mod}}^{\mathbb{Z}} A$ and $P_\alpha \simeq P$ in $\mathsf{mod}^{\mathbb{Z}} A$ for all $P \in \mathsf{proj}^{\mathbb{Z}} A$.*

(3) *There exists a graded algebra automorphism α of A such that $\Omega^n_{A^e}(A) \simeq {}_1A_\alpha(a)$ in $\mathsf{mod}^{\mathbb{Z}} A^e$ and $P_\alpha \simeq P$ in $\mathsf{mod}^{\mathbb{Z}} A$ for all $P \in \mathsf{proj}^{\mathbb{Z}} A$.*

Similarly, we name these algebras as follows:

Definition 2.5. A finite dimensional graded algebra is *(a)-twisted n-periodic* if it is a direct product of simple algebras or algebras satisfying the equivalent conditions in Corollary 2.4.

3. Auslander correspondence

We now prove the first main result Theorem 1.2 of this paper, which gives a homological characterization of the Auslander algebras of finite triangulated categories.

First, we give the properties of the endomorphism algebra of a basic additive generator for a finite triangulated category, proving Theorem 1.2(1) ⇒ (2).

Proposition 3.1. *Let $\mathcal{T}$ be a k-linear*, Hom-*finite idempotent-complete triangulated category. Assume $\mathcal{T}$ has an additive generator M. Take M to be basic and set $C = \mathsf{End}_{\mathcal{T}}(M)$. Let α be the automorphism of C induced by* $[1]$; *precisely, fix an isomorphism $a\colon M \to M[1]$ and define α by $\alpha(f) = a^{-1} \circ f[1] \circ a$ for $f \in \mathsf{End}_{\mathcal{T}}(M)$. Then, C is a finite dimensional algebra which is twisted* 3*-periodic.*

Proof. Since $\mathsf{mod}\,\mathcal{T} \simeq \mathsf{mod}\,C$ and $\mathsf{mod}\,\mathcal{T}$ is a Frobeniuis category (see [Krause 2007, 4.2]), C is self-injective. Also, since the triangles in $\mathcal{T}$ yield projective resolutions of C-modules, the third syzygy is induced by the automorphism α, that is, we have $\Omega^3 \simeq (-)_\alpha$ on $\underline{\mathsf{mod}}\,C$. Then C is twisted 3-periodic by Corollary 2.2. □

For the converse implication, we need the following result due to Amiot, which allows one to introduce a triangle structure on the category of projectives in a Frobenius category.

Proposition 3.2 [Amiot 2007, 8.1]. *Let $\mathcal{P}$ be an idempotent complete k-linear category such that the functor category* $\mathsf{mod}\,\mathcal{P}$ *is naturally a Frobenius category. Let S be an autoequivalence of $\mathcal{P}$ and extend this to* $\mathsf{mod}\,\mathcal{P} \to \mathsf{mod}\,\mathcal{P}$. *Assume there exists an exact sequence of exact functors from* $\mathsf{mod}\,\mathcal{P}$ *to* $\mathsf{mod}\,\mathcal{P}$

$$0 \to 1 \to X^0 \to X^1 \to X^2 \to S \to 0,$$

where X^i take values in $\mathcal{P} = \mathsf{proj}\,\mathcal{P}$. Then, $\mathcal{P}$ has a structure of a triangulated category with suspension S. The triangles are ones isomorphic to $X^0M \to X^1M \to X^2M \to SX^0M$ for $M \in \mathsf{mod}\,\mathcal{P}$.

Combining this with Corollary 2.2, we can prove Theorem 1.2(2) ⇒ (1). Let us summarize the proof below.

Proof of Theorem 1.2. (1) ⇒ (2) is Proposition 3.1.

(2) ⇒ (1) Since A is self-injective, Ω^3 permutes the simples, so by Corollary 2.2, there exists an exact sequence

$$0 \to A \to P^0 \to P^1 \to P^2 \to {}_1A_\alpha \to 0$$

of (A, A)-bimodules, with P^i's projective and α is an automorphism of A. Then, we can apply Proposition 3.2 for $\mathcal{P} = \mathsf{proj}\,A$, $S = - \otimes_A A_\alpha$, and $X^i = - \otimes_A P^i$. □

Applying a recent result of Keller [2018], we can formulate Theorem 1.2 in terms of bijection between triangulated categories and algebras under some assumptions on triangulated categories. Let us recall the relevant definitions. Let $\mathcal{T}$ be a k-linear triangulated category with Auslander–Reiten triangles, and Γ its AR-quiver. Then Γ together with the AR-translation τ forms a translation quiver. For each pair of vertices $x, y \in \Gamma$, we denote by $\{x \to y\}$ the set of arrows from x to y. Fix a bijection $\sigma\colon \{y \to x\} \to \{\tau x \to y\}$, and define $m_x = \sum_{a \in \{y \to x\}} \sigma(a)a$ which is a morphism in the path category $k\Gamma$. Let I be the ideal of $k\Gamma$ generated by $\{m_x \mid x \in \Gamma\}$.

Definition 3.3 [Riedtmann 1980; Happel 1988]. In the above setting, we call the category $k\Gamma/I$ the *mesh category* of the translation quiver Γ. We say that $\mathcal{T}$ is *standard* if it is k-linearly equivalent its mesh category of the AR-quiver.

We have the following version of Theorem 1.2 under the standardness of $\mathcal{T}$.

Theorem 3.4. *Let k be an algebraically closed field. Then, there exists a bijection between the following*:

(1) *The set of triangle equivalence classes of k-linear*, Hom-*finite*, *idempotent-complete triangulated categories which are finite*, *algebraic*, *and standard.*

(2) *The set of isomorphism classes of finite dimensional mesh algebras over k.*

The correspondence from (1) *to* (2) *is given by taking the basic Auslander algebra*, *and from* (2) *to* (1) *by taking the category of projective modules.*

Proof. We first check that each map is well-defined.

Let $\mathcal{T}$ be a triangulated category as in (1). Then, the standardness of $\mathcal{T}$ implies that its basic Auslander algebra is a mesh algebra.

Suppose next that A is a finite dimensional mesh algebra. We want to show that $\mathsf{proj}\,A$ has the unique structure of an algebraic triangulated category up to equivalence. Since the third syzygy of simple A-modules are simple, $\mathcal{T} = \mathsf{proj}\,A$ has a structure of a triangulated category by Theorem 1.2. Also, this is standard since A is a mesh algebra. We claim that $\mathsf{proj}\,A$ admits a triangle structure which is algebraic. Since $\mathcal{T}$ is a finite, standard triangulated category, there exists a Dynkin quiver Q, a k-linear automorphism F of $\mathsf{D}^{\mathrm{b}}(\mathsf{mod}\,kQ)$, and a k-linear equivalence $\mathsf{D}^{\mathrm{b}}(\mathsf{mod}\,kQ)/F \simeq \mathsf{proj}\,A$ [Riedtmann 1980]. As in the proof of [Keller 2018], F is isomorphic to $- \otimes^{L}_{kQ} X$ for some (kQ, kQ)-bimodule complex X. Then by [Keller 2005], $\mathsf{D}^{\mathrm{b}}(\mathsf{mod}\,kQ)/F$ admits an algebraic triangle structure as a triangulated orbit category, hence so does $\mathsf{proj}\,A$. This finishes the proof of the claim. Now, this algebraic triangle structure is unique up to equivalence by the main result of [Keller 2018]. This shows the well-definedness.

It is clear that these maps are mutually inverse. □

Remark 3.5. One can show that using the main result of [Muro 2020], the assumption "standardness" can be dropped.

4. Graded projectivization

In this section, we formulate the method of realizing certain additive categories, which we call *G-finite* additive categories on which a group G acts with some finiteness conditions, as the category of graded projective modules over a G-graded algebra. This generalizes the classical "projectivization" [Auslander et al. 1995, II.2], which realizes a finite additive category as the category of projectives over an algebra.

Let $\mathcal{A}$ be an additive category with an action of a group G. Precisely, an automorphism F_g of $\mathcal{A}$ is given for each $g \in G$ so that $F_{gh} = F_h \circ F_g$ for all $g, h \in G$. Then the action of G extends to an automorphism of $\mathsf{mod}\,\mathcal{A}$ by $F_g M = M \circ F_g^{-1}$. For example, the action on the representable functors is $F_g \mathcal{A}(-, X) = \mathcal{A}(-, F_g X)$.

Recall that the orbit category $\mathcal{A}/G$ has the same objects as $\mathcal{A}$ and the morphism space

$$(\mathcal{A}/G)(X, Y) = \bigoplus_{g \in G} \mathcal{A}(X, F_g Y)$$

and the composition $b \circ a$ of $a \in \mathcal{T}(X, F_gY)$ and $b \in \mathcal{T}(Y, F_hZ)$ is given by $b \circ a = F_g(b)a$, where the right hand side is the composition in $\mathcal{A}$. Then, $\mathcal{A}/G$ is naturally a G-graded category whose degree g part is $\mathcal{A}(X, F_gY)$.

Proposition 4.1. *Let $\mathcal{A}$ be an additive category with an action of a group G. Consider the orbit category $\mathcal{C} = \mathcal{A}/G$. Then, the following assertions hold*:

(1) *The Yoneda embedding $\mathcal{A} \to \mathsf{proj}^G\mathcal{C}$ is fully faithful. It is an equivalence if $\mathcal{A}$ is idempotent-complete.*

(2) *There exists an equivalence $\mathsf{mod}\,\mathcal{A} \simeq \mathsf{mod}^G\mathcal{C}$ such that the action of F_g on $\mathsf{mod}\,\mathcal{A}$ corresponds to the grade shift (g) on $\mathsf{mod}^G\mathcal{C}$, that is, we have the following commutative diagram of functors*:

$$\begin{tikzcd}
\mathsf{mod}\,\mathcal{A} \arrow[r, "\simeq"] \arrow[d, "F_g"'] & \mathsf{mod}^G\mathcal{C} \arrow[d, "(g)"] \\
\mathsf{mod}\,\mathcal{A} \arrow[r, "\simeq"] & \mathsf{mod}^G\mathcal{C}
\end{tikzcd}$$

Proof. (1) We have the Yoneda lemma for graded functors: $\mathsf{Hom}_{\mathsf{mod}^G\mathcal{C}}(\mathcal{C}(-, X), M) = (MX)_0$. It follows that the Yoneda embedding $\mathcal{A} \to \mathsf{proj}^G\mathcal{C}$ is fully faithful. Also, if $\mathcal{A}$ is idempotent-complete, the projectives in $\mathsf{mod}^G\mathcal{C}$ are representable, and therefore the Yoneda embedding is dense.

(2) It is clear that the functor in (1) induces an equivalence $\mathsf{mod}\,\mathcal{A} \simeq \mathsf{mod}^G\mathcal{C}$. Also, the degree h part of the functor $\mathcal{C}(-, F_gX)$ is $\mathcal{A}(-, F_hF_gX) = \mathcal{A}(-, F_{gh}X)$, which is equal to the same degree part of $\mathcal{C}(-, X)(g)$. Thus we have the commutative diagram. □

Now we impose the following finiteness conditions on the G-action:

(G1) There is $M \in \mathcal{A}$ such that $\mathcal{A} = \mathsf{add}\{F_gM \mid g \in G\}$.

(G2) For any $X, Y \in \mathcal{A}$, $\mathsf{Hom}_{\mathcal{A}}(X, F_gY) = 0$ for almost all $g \in G$.

If these conditions are satisfied, we say that an additive category $\mathcal{A}$ with an action of G is *G-finite*. If $\mathcal{A}$ is a G-finite additive category, we say $M \in \mathcal{A}$ as in (G1) is a *G-additive generator*. If G is generated by a single element F, we use the term *F-finite* for G-finiteness, and *F-additive generator* for G-additive generator. Note that if G is the trivial group, G-finiteness is nothing but finiteness, and a G-additive generator is an additive generator.

Let us reformulate Proposition 4.1 in terms of the graded endomorphism algebra below. Note that this generalizes the classical "projectivization" for finite additive categories, which is the case G is trivial, to "graded projectivization" for G-finite categories. Although this is rather formal, it will be useful in the sequel.

Proposition 4.2. *Let $\mathcal{A}$ be a k-linear*, Hom-*finite*, *idempotent-complete category with an action of G, which is G-finite. Let $M \in \mathcal{A}$ be a G-additive generator and set $C = \mathsf{End}_{\mathcal{A}/G}(M)$. Then, the following assertions hold*:

(1) *C is a finite dimensional G-graded algebra.*

(2) *The functor $\mathcal{A} \to \mathsf{proj}^G C$, $X \mapsto \bigoplus_{g\in G} \mathsf{Hom}_{\mathcal{A}}(M, F_g X)$ is an equivalence.*

(3) *There exists an equivalence $\mathsf{mod}\,\mathcal{A} \simeq \mathsf{mod}^G C$ such that the action of g on $\mathsf{mod}\,\mathcal{A}$ corresponds to the grade shift (g) on $\mathsf{mod}^G C$.*

Proof. (1) C is finite dimensional by (G2).

(2) Since we have an equivalence $\mathsf{proj}^G \mathcal{A}/G \to \mathsf{proj}^G C$ by substituting M, the assertion follows from Proposition 4.1(1).

(3) This is the same as Proposition 4.1(2). □

Definition 4.3. G-Graded rings A and B are *graded Morita equivalent* if there is an equivalence $\mathsf{mod}^G A \simeq \mathsf{mod}^G B$ which commutes with grade shift functors (g) for all $g \in G$.

Let us note the following remark.

Proposition 4.4. *Assume* (G1) *is satisfied and set $C = \mathsf{End}_{\mathcal{A}/G}(M)$.*

(1) *The ungraded algebra C does not depend on the choice of M up to Morita equivalence.*

(2) *The graded algebra C does not depend on the choice of M up to graded Morita equivalence.*

Proof. (1) Since C is the endomorphism algebra of an additive generator of the category $\mathcal{A}/G$, the assertion follows.

(2) This follows from Proposition 4.2(3). □

As a direct application of this graded projectivization, we present as an example the following graded version of the Auslander correspondence. For simplicity, we consider $\mathbb{Z}$-graded algebras. A graded algebra Λ is *representation-finite* if $\mathsf{mod}^{\mathbb{Z}}\Lambda$ has finitely many indecomposables up to grade shift. This is equivalent to the representation-finiteness of the ungraded algebra Λ [Gordon and Green 1982].

Proposition 4.5. *There exists a bijection between the following*:

(1) *The set of graded Morita equivalence classes of finite dimensional $\mathbb{Z}$-graded algebras Λ of finite representation type.*

(2) *The set of graded Morita equivalence classes of finite dimensional $\mathbb{Z}$-graded algebras Γ with* $\mathrm{gl.\,dim}\,\Gamma \leq 2 \leq \mathrm{dom.\,dim}\,\Gamma$.

The correspondence is given as follows:

- *From* (1) *to* (2): $\Gamma = \mathsf{End}_\Lambda(M) = \bigoplus_{n\in\mathbb{Z}} \mathsf{Hom}_\Lambda(M, M(n))_0$ *for a* (1)*-additive generator M for* $\mathsf{mod}^{\mathbb{Z}}\Lambda$.
- *From* (2) *to* (1): $\Lambda = \mathsf{End}_\Gamma(Q) = \bigoplus_{n\in\mathbb{Z}} \mathsf{Hom}_\Gamma(Q, Q(n))_0$ *for a* (1)*-additive generator Q for the category of graded projective-injective Γ-modules.*

Proof. Note that Γ (resp. Λ) does not depend on the choice of M (resp. Q) by Proposition 4.4(2). The rest of the proof follows by the same argument as in Theorem 1.1; see [Auslander et al. 1995, VI.5]. □

Notice that this correspondence $\Lambda \leftrightarrow \Gamma$ is the same as the ungraded case, thus it is a refinement of Theorem 1.1 on how much grading Λ or Γ have up to graded Morita equivalence.

5. Uniqueness of triangle structures

The aim of this section is to prove some results which state the uniqueness of triangle structures on certain additive categories. We say that an additive category $\mathcal{C}$ *has a unique algebraic triangle structure up to equivalence* if $\mathcal{C}_1 = (\mathcal{C}, [1], \triangle)$ and $\mathcal{C}_2 = (\mathcal{C}, [1]', \triangle')$ are algebraic triangle structures on $\mathcal{C}$, then there exists a triangle equivalence $F\colon \mathcal{C}_1 \xrightarrow{\sim} \mathcal{C}_2$ such that $F(X) \simeq X$ in $\mathcal{C}$ for all $X \in \mathcal{C}$.

The following is the main result of this section.

Theorem 5.1. *Let Λ be a ring with no simple ring summands such that $\mathsf{K}^{\mathrm{b}}(\operatorname{proj} \Lambda)$ is Krull–Schmidt. Then, the additive category $\mathsf{K}^{\mathrm{b}}(\operatorname{proj} \Lambda)$ has a unique algebraic triangle structure up to equivalence.*

We give applications of Theorem 5.1. For a quiver Q, let $\mathbb{Z}Q$ be the associated infinite translation quiver [Assem et al. 2006; Happel 1988], and let $k(\mathbb{Z}Q)$ be its mesh category [Happel 1988].

Corollary 5.2. *Let Q be a disjoint union of Dynkin quivers which does not contain A_1. Then, the mesh category $k(\mathbb{Z}Q)$ has a unique algebraic triangle structure up to equivalence.*

As a consequence, we have the classification of [1]-finite algebraic triangulated categories.

Theorem 5.3. *Let k be an algebraically closed field. Any [1]-finite algebraic triangulated category over k is triangle equivalent to the bounded derived category $\mathsf{D}^{\mathrm{b}}(\operatorname{mod} kQ)$ of the path algebra kQ for a disjoint union Q of Dynkin quivers of type A, D, and E.*

Now we start the preparations for the proofs of the above results. Recall that an additive category is *Krull–Schmidt* if any object is a finite direct sum of objects whose endomorphism rings are local. This is the case if the category is idempotent-complete and Hom-finite over a complete Noetherian local ring. A Krull–Schmidt category $\mathcal{C}$ is *purely nonsemisimple* if for each $X \in \mathcal{C}$, $J_{\mathcal{C}}(-, X) \neq 0$ or $J_{\mathcal{C}}(X, -) \neq 0$ holds. Note that these conditions are equivalent if $\mathcal{C}$ is triangulated.

First we observe that the suspension and the terms appearing in triangles in a triangulated category are determined by its additive structure under some Krull–Schmidt assumptions. Recall from [Auslander et al. 1995, I.2] that a morphism $f\colon X \to Y$ in a Krull–Schmidt category is *right minimal* if for any direct summand X' of X, the restriction $f|_{X'}$ is nonzero. We dually define left minimality.

Lemma 5.4. *Let $\mathcal{C}$ be a Krull–Schmidt additive category. Assume $\mathcal{C}$ has a structure of a triangulated category. Let $f\colon X \to Y$ be a right minimal morphism in $J_{\mathcal{C}}$:*

(1) *The mapping cone of f is the minimal weak cokernel of f.*

(2) *$X[1]$ is the minimal weak cokernel of the minimal weak cokernel of f.*

Proof. Complete f to a triangle $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} X[1]$.

(1) We have to show that g is the minimal weak cokernel of f. We only have to show the left minimality of g. If this is not the case, then h has a summand $W \xrightarrow{1_W} W$ for a common nonzero summand W of Z and $X[1]$. This contradicts the right minimality of f.

(2) We want to show that h is the minimal weak cokernel of g. Again, we only have to show the left minimality of h. If this is not the case, then $f[1]$ has a summand $V \xrightarrow{1_V} V$ for a common nonzero summand V of $X[1]$ and $Y[1]$. This contradicts $f \in J_{\mathcal{C}}(X, Y)$. □

We deduce that the possible triangle structures on a given purely nonsemisimple Krull–Schmidt additive category is roughly unique in the following sense. We denote by $\mathrm{cone}_{\triangle}(f)$ the mapping cone of f in a triangle structure $\triangle$.

Proposition 5.5. *Let $\mathcal{C}$ be a purely nonsemisimple Krull–Schmidt additive category. If $(\mathcal{C}, [1], \triangle)$ and $(\mathcal{C}, [1]', \triangle')$ are triangle structures on $\mathcal{C}$, then we have the following*:

(1) *$X[1] \simeq X[1]'$ for all objects $X \in \mathcal{C}$.*

(2) *$\mathrm{cone}_{\triangle}(f) \simeq \mathrm{cone}_{\triangle'}(f)$ in $\mathcal{C}$ for all morphisms f in $\mathcal{C}$.*

Proof. (1) Let $X \in \mathcal{C}$ be an indecomposable object. Since $\mathcal{C}$ is purely nonsemisimple, there exists a nonzero morphism $f : X \to Y$ in $J_{\mathcal{C}}$. Then, f is a right minimal radical map, and hence the assertion follows from Lemma 5.4(2).

(2) Let $f : X \to Y$ be an arbitrary morphism in $\mathcal{C}$. By removing the summands isomorphic to $W \xrightarrow{1} W$, which does not affect the mapping cone, we may assume $f \in J_{\mathcal{C}}$. Then, f has a decomposition $X_1 \oplus X_2 \xrightarrow{(f_1,0)} Y$ with right minimal $f_1 \in J_{\mathcal{C}}$ and the mapping cone of f is the direct sum of that of f_1 and $X_2[1]$. Now the mapping cone of f_1 is determined by Lemma 5.4(1) and since $\mathcal{C}$ is purely nonsemisimple, $[1]$ is determined by the additive structure by (1). This proves the assertion. □

For Theorem 5.1, we need the following result of Keller on algebraic triangulated categories.

Proposition 5.6 [Keller 1994, 4.3]. *Let $\mathcal{T}$ be an algebraic triangulated category and $T \in \mathcal{T}$ be a tilting object. Then, there exists a triangle equivalence $\mathcal{T} \simeq \mathsf{K}^{\mathrm{b}}(\mathsf{proj}\,\mathsf{End}_{\mathcal{T}}(T))$.*

Note that we have the following observation, which will be crucial for the proof.

Lemma 5.7. *Let $\mathcal{C}$ be a purely nonsemisimple Krull–Schmidt additive category. Assume $\mathcal{C}_1 = (\mathcal{C}, [1], \triangle)$ and $\mathcal{C}_2 = (\mathcal{C}, [1]', \triangle')$ are triangle structures on $\mathcal{C}$. Then, an object $T \in \mathcal{C}$ is a tilting object in $\mathcal{C}_1$ if and only if it is a tilting object in $\mathcal{C}_2$.*

Proof. Indeed, we have $\mathcal{C}_1(T, T[n]) = \mathcal{C}_2(T, T[n]')$ by Proposition 5.5(1), which shows that the vanishing of extensions does not depend on the triangle structure. Also, by Proposition 5.5(2), T generates $\mathcal{C}_1$ if and only if T generates $\mathcal{C}_2$. This shows the assertion. □

Now we are ready to prove our results.

Proof of Theorem 5.1. Let $\mathcal{C}$ be the underlying additive category of $\mathcal{K} = \mathsf{K}^{\mathrm{b}}(\operatorname{proj} \Lambda)$. Assume $\mathcal{C}$ is triangulated. We show that $\mathcal{C}$ is triangle equivalent to $\mathcal{K}$ by finding a tilting object whose endomorphism ring is Λ. Note that $\mathcal{C} = \mathcal{K}$ is purely nonsemisimple and Krull–Schmidt by our assumption on Λ. Let $T \in \mathcal{C}$ be the object corresponding to $\Lambda \in \mathcal{K}$. Then, T is a tilting object by Lemma 5.7 and clearly $\mathsf{End}_{\mathcal{C}}(T) = \Lambda$. By our assumption that $\mathcal{C}$ is algebraic, we deduce that $\mathcal{C}$ is triangle equivalent to $\mathcal{K}$ by Proposition 5.6. □

For the proof of Corollary 5.2, let us recall the following standardness theorem of Riedtmann.

Proposition 5.8 [Riedtmann 1980]. *Let k be a field and $\mathcal{T}$ be a k-linear*, Hom*-finite idempotent-complete triangulated category whose AR-quiver is $\mathbb{Z}Q$ for some acyclic quiver Q. Assume the endomorphism algebra of an indecomposable object of $\mathcal{T}$ is k. Then, $\mathcal{T}$ is k-linearly equivalent to the mesh category $k(\mathbb{Z}Q)$.*

A well known application of this result is an equivalence $\mathsf{K}^{\mathrm{b}}(\operatorname{proj} kQ) \simeq k(\mathbb{Z}Q)$ for a Dynkin quiver Q [Happel 1988, I.5.6].

Proof of Corollary 5.2. Since $k(\mathbb{Z}Q) \simeq \mathsf{K}^{\mathrm{b}}(\operatorname{proj} kQ)$ as additive categories, Theorem 5.1 gives the result. □

A k-linear triangulated category $\mathcal{T}$ is *locally finite* [Xiao and Zhu 2005] if for each indecomposable $X \in \mathcal{T}$, we have $\sum_{Y:\text{indec.}} \dim_k \mathsf{Hom}_{\mathcal{T}}(X, Y) < \infty$. This condition is equivalent to its dual [loc. cit.]. Clearly, our [1]-finite triangulated categories are locally finite. The classification of [1]-finite triangulated category depends on the following result.

Proposition 5.9 [Xiao and Zhu 2005, 2.3.5]. *Let k be an algebraically closed field and $\mathcal{T}$ be a locally finite triangulated category which does not contain a nonzero finite triangulated subcategory. Then, the AR-quiver of $\mathcal{T}$ is $\mathbb{Z}Q$ for a disjoint union Q of Dynkin quivers of type A, D, and E.*

Proof of Theorem 5.3. The AR-quiver of a [1]-finite triangulated category is $\mathbb{Z}Q$ for some Dynkin quiver Q by Proposition 5.9. Moreover, it is equivalent to $k(\mathbb{Z}Q)$ by Proposition 5.8. Thus Corollary 5.2 applies. □

We end this section by noting the following lemma, which we use later. This lemma states in particular, that for mesh categories, the suspension is unique up to isomorphism of functors

Lemma 5.10. *Let Q be a Dynkin quiver and α be an automorphism of the mesh category $k(\mathbb{Z}Q)$ such that $\alpha X \simeq X$ for all $X \in k(\mathbb{Z}Q)$. Then, α is isomorphic as functors to the identity functor.*

Proof. Since Q is Dynkin, we can inductively construct a natural isomorphism between α and id. □

6. [1]-Auslander correspondence

In this section, we prove the second main result, Theorem 1.3, of this paper. In the first subsection, we give the correspondence from triangulated categories to algebras, and the converse one in the second subsection. We will prove the main theorem in the final subsection.

6A. ***From triangulated categories to algebras.*** We apply the graded projectivization prepared in Section 4 to triangulated categories. Let $\mathcal{T}$ be a k-linear, Hom-finite, idempotent-complete triangulated category. Consider the action on $\mathcal{T}$ of $G = \mathbb{Z}$, generated by the suspension [1]. Then, the G-finiteness in this case are:

(S1) There is $M \in \mathcal{T}$ such that $\mathcal{T} = \mathsf{add}\{M[n] \mid n \in \mathbb{Z}\}$.

(S2) For any $X, Y \in \mathcal{T}$, $\mathsf{Hom}_{\mathcal{T}}(X, Y[n]) = 0$ for almost all n.

According to the terminology in Section 4, we say $\mathcal{T}$ is [1]-*finite*, and call M as in (S1) a [1]-*additive generator.*

The following proposition gives the correspondence from triangulated categories to algebras.

Proposition 6.1. *Let $\mathcal{T}$ be a k-linear*, Hom-*finite*, *idempotent-complete*, *triangulated category which is* [1]-*finite. Let $M \in \mathcal{T}$ be a* [1]-*additive generator and set $C = \mathsf{End}_{\mathcal{T}/[1]}(M)$. Then*, *$C$ is a finite-dimensional graded self-injective algebra such that $\Omega^3 L \simeq L(-1)$ for any graded C-module L.*

Proof. C is finite dimensional by (S2). Also, since $\mathsf{mod}\,\mathcal{T} \simeq \mathsf{mod}^{\mathbb{Z}} C$ by Proposition 4.2(2) and $\mathsf{mod}\,\mathcal{T}$ is Frobenius, C is self-injective. It remains to show the statement on the third syzygy. Let L be a graded C-module and let $Q \to R \to L \to 0$ be a projective presentation of L in $\mathsf{mod}^{\mathbb{Z}} C$. Take the map $X \to Y$ in $\mathcal{T}$ corresponding to $Q \to R$ and complete it to a triangle $W \to X \to Y \to W[1]$. Put $P_Z = \bigoplus_{n\in\mathbb{Z}} \mathsf{Hom}_{\mathcal{T}}(M, Z[n])$ for each $Z \in \mathcal{T}$. This is the graded projective C-module corresponding to Z. Note that $P_{Z[1]} = P_Z(1)$, where (1) is the grade shift functor on $\mathsf{mod}^{\mathbb{Z}} C$. The triangle above yields an exact sequence $P_X(-1) \to P_Y(-1) \to P_W \to P_X \to P_Y \to P_W(1)$. Since $P_X = Q$ and $P_Y = R$, we see that $\Omega^3 L \simeq L(-1)$. □

Example 6.2. Let Q be a Dynkin quiver and $\mathcal{T} = \mathsf{D}^{\mathsf{b}}(\mathsf{mod}\,kQ)$. Let M be an additive generator for $\mathsf{mod}\,kQ$. Then, M is a [1]-additive generator for $\mathcal{T}$ and we have $C = \mathsf{End}_{kQ}(M) \oplus \mathsf{Ext}^1_{kQ}(M, M)$. The degree 0 part of C is the Auslander algebra of $\mathsf{mod}\,kQ$.

Let Q' be another Dynkin quiver with the same underlying graph Δ as Q. Since kQ and kQ' are derived equivalent, we have $\mathsf{D}^{\mathsf{b}}(\mathsf{mod}\,kQ') = \mathcal{T}$. Similarly as above, an additive generator M' for $\mathsf{mod}\,kQ'$ is a [1]-additive generator for $\mathcal{T}$. The corresponding graded algebra C' is $\mathsf{End}_{kQ'}(M') \oplus \mathsf{Ext}^1_{kQ'}(M', M')$, with the Auslander algebra of $\mathsf{mod}\,kQ'$ in the degree 0 part.

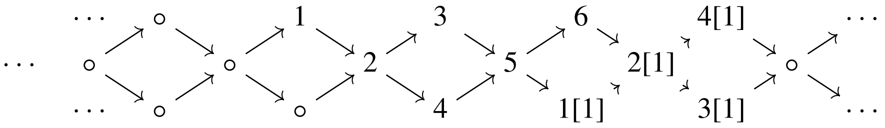
By Proposition 4.4, C and C' are isomorphic as ungraded algebras (but not as graded algebras). In this way, $C \simeq C'$ contains the Auslander algebras of module categories over Δ for any orientation of Δ.

Let us give a more specific example.

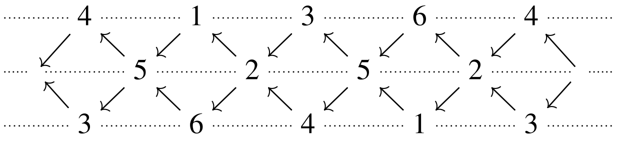
Example 6.3. Let Q be the following Dynkin quiver of type A_3, and $\mathcal{T}$ be its derived category $\mathsf{D}^{\mathsf{b}}(\mathsf{mod}\,kQ)$.

$$a \leftarrow b \leftarrow c.$$

Then, the AR-quiver of $\mathcal{T}$ is as follows:



where $1, \dots, 6$ denotes the objects from $\operatorname{mod} kQ$. Take $M = \bigoplus_{i=1}^{6} M_i$, where M_i is the indecomposable kQ-module corresponding to the vertex i. Then, $C = \operatorname{End}_{kQ}(M) \oplus \operatorname{Ext}^1_{kQ}(M, M)$. It is easily verified that C is presented by the quiver $\mathbb{Z}A_3/[1]$ and the mesh relations. The quiver of C looks as follows:



where the vertices with the same number are identified, with mesh relations along the dotted lines. The arrows $1 \to 5$ and $2 \to 6$ have degree 1 and all the others have degree 0.

Now, let Q' be the quiver obtained by reflecting Q at vertex a:

$$a \to b \leftarrow c.$$

Fix an equivalence $\mathsf{D}^{\mathrm{b}}(\operatorname{mod} kQ') \simeq \mathsf{D}^{\mathrm{b}}(\operatorname{mod} kQ)$ so that $M' = M_2 \oplus \cdots \oplus M_6 \oplus M_1[1]$ is an additive generator for $\operatorname{mod} kQ'$. Then, $C' = \operatorname{End}_{kQ'}(M') \oplus \operatorname{Ext}^1_{kQ'}(M', M')$ is presented by the same quiver with relations as C, with arrows $2 \to 1$ and $2 \to 6$ having degree 1 and all the others degree 0. Thus $C \simeq C'$ as ungraded algebras but not as graded algebras.

Nevertheless, C and C' are graded Morita equivalent. Here we give a direct equivalence $\operatorname{mod}^{\mathbb{Z}} C \to \operatorname{mod}^{\mathbb{Z}} C'$. Let e_i be the idempotent of C corresponding to M_i $(1 \le i \le 6)$ and set $P = e_2C \oplus \cdots \oplus e_6C \oplus e_1C(1)$. Then, we have $\operatorname{End}_C(P) \simeq C'$ as graded algebras and $\operatorname{Hom}_C(P, -)$ gives a desired equivalence.

6B. ***From algebras to triangulated categories.*** We can give the converse correspondence as in Section 3. Setting $a = -1$ in the following proposition gives the result.

Proposition 6.4. *Let A be a finite dimensional graded algebra such that A/J_A is separable over k and $\Omega^3 S \simeq S(a)$ for any graded simple module S. Then, $\operatorname{proj}^{\mathbb{Z}} A$ has a structure of a triangulated category. If k is algebraically closed and $a \neq 0$, then the suspension is isomorphic to $(-a)$ and the algebraic triangle structure on $\operatorname{proj}^{\mathbb{Z}} A$ is unique up to equivalence.*

Proof. By Corollary 2.4, A is self-injective and there exists an exact sequence

$$0 \to A \to P^0 \to P^1 \to P^2 \to {}_1A_\alpha(-a) \to 0$$

in $\operatorname{mod}^{\mathbb{Z}} A^e$, where P^i, $i = 0, 1, 2$ are projectives, and α is a graded algebra automorphism of A such that $P_\alpha \simeq P$ for all $P \in \operatorname{proj}^{\mathbb{Z}} A$. Then, we can apply Proposition 3.2 for $\mathcal{P} = \operatorname{proj}^{\mathbb{Z}} A$, $X^i = - \otimes_A P^i$ and $S = (-)_\alpha(-a)$ to see that $\operatorname{proj}^{\mathbb{Z}} A$ is triangulated with suspension $(-)_\alpha(-a)$. Now assume k is algebraically closed and $a \neq 0$. Since we have $\mathsf{Hom}_{\mathsf{proj}^{\mathbb{Z}} A}(X, Y(-na)) = 0$ for almost all $n \in \mathbb{Z}$ for each $X, Y \in \mathsf{proj}^{\mathbb{Z}} A$, the triangulated category $\mathsf{proj}^{\mathbb{Z}} A$ is [1]-finite, and therefore, it is equivalent to the mesh category $k(\mathbb{Z}Q)$ for some Dynkin diagram Q by Propositions 5.9 and 5.8. Then, by changing the triangle structure if necessary, $\mathsf{proj}^{\mathbb{Z}} A$ has a structure of an algebraic triangulated category, which is unique up to equivalence by Corollary 5.2. Also, $(-)_\alpha(-a)$ and $(-a)$ are isomorphic as functors by Lemma 5.10. □

6C. *Proof of Theorem 1.3.* Combining the previous results, we can now prove the second main result of this paper.

Proof of Theorem 1.3. For M as in (1), C is as stated in (2) by Proposition 6.1. Also, the graded Morita equivalence class of C does not depend on the choice of M by Proposition 4.4. This shows the well-definedness of (1) to (2).

For the map from (2) to (1), it is well-defined since $\mathsf{proj}^{\mathbb{Z}} C$ has the unique structure of an algebraic triangulated category up to equivalence by Proposition 6.4.

It is easily checked that these maps are mutually inverse.

The bijection between (1) and (3) is Proposition 5.9 and Theorem 5.3. □

Remark 6.5. The algebra C in Theorem 1.3 satisfies $[3] \simeq (1)$ as functors on $\underline{\mathsf{mod}}^{\mathbb{Z}} C$ by Proposition 6.1.

7. Applications to Cohen–Macaulay modules

Applying our classification in Theorem 5.3 of [1]-finite triangulated categories, we show that the stable categories $\underline{\mathsf{CM}}^{\mathbb{Z}} \Lambda$ of some CM-finite Iwanaga–Gorenstein algebras, in particular, of (commutative) graded simple singularities are triangle equivalent to the derived categories of Dynkin quivers.

A Noetherian algebra Λ is *Iwanaga–Gorenstein* if $\mathrm{id}_\Lambda \Lambda = \mathrm{id}_{\Lambda^{\mathrm{op}}} \Lambda < \infty$. A typical example of Iwanaga–Gorenstein algebra is given by commutative Gorenstein rings of finite Krull dimension. For an Iwanaga–Gorenstein algebra Λ, we have the category

$$\mathsf{CM}\,\Lambda = \{X \in \mathsf{mod}\,\Lambda \mid \mathsf{Ext}^i_\Lambda(X, \Lambda) = 0 \text{ for all } i > 0\}$$

of *Cohen–Macaulay* Λ-modules. It is naturally a Frobenius category and we have a triangulated category $\underline{\mathsf{CM}}\,\Lambda$.

Now consider the case Λ is graded: let $\Lambda = \bigoplus_{n \geq 0} \Lambda_n$ is a positively graded Noetherian algebra such that each Λ_n is finite dimensional over a field k. If Λ is a graded Iwanaga–Gorenstein algebra, we similarly have the category

$$\mathsf{CM}^{\mathbb{Z}} \Lambda = \{X \in \mathsf{mod}^{\mathbb{Z}} \Lambda \mid \mathsf{Ext}^i_\Lambda(X, \Lambda) = 0 \text{ for all } i > 0\}$$

of graded Cohen–Macaulay modules. It is again Frobenius and hence the stable category $\underline{\mathsf{CM}}^{\mathbb{Z}} \Lambda$ is triangulated. A graded Iwanaga–Gorenstein algebra is *CM-finite* if $\mathsf{CM}^{\mathbb{Z}}\,\Lambda$ has finitely many indecomposable objects up to grade shift.

We now show that CM-finite Iwanaga–Gorenstein algebras give a large class of examples of [1]-finite triangulated categories.

Proposition 7.1. *Let Λ be a positively graded CM-finite Iwanaga–Gorenstein algebra with* $\operatorname{gl.dim}\Lambda_0 < \infty$. *Then, the triangulated category* $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ *is* $[1]$*-finite.*

To prove this, we need an observation for general Noetherian algebras, which is motivated by [Yamaura 2013, 3.5]. Let us fix some notations. We denote by $\mathsf{Ext}^i_\Lambda(-,-)_0$ the Ext groups on $\mathsf{mod}^{\mathbb{Z}}\Lambda$. Note that for $M, N \in \mathsf{mod}^{\mathbb{Z}}\Lambda$, the Ext groups on $\mathsf{mod}\,\Lambda$ are graded k-vector spaces: $\mathsf{Ext}^i_\Lambda(M,N) = \bigoplus_{n\in\mathbb{Z}}\mathsf{Ext}^i_\Lambda(M,N(n))_0$, $(i \geq 0)$. For each $M \in \mathsf{mod}^{\mathbb{Z}}\Lambda$ and $n \in \mathbb{Z}$, we denote by $M_{\geq n}$ the Λ-submodule of M consisting of components of degree $\geq n$.

Lemma 7.2. *Let Λ be a positively graded Noetherian algebra with* $\operatorname{gl.dim}\Lambda_0 < \infty$. *Then, for any* $X, Y \in \mathsf{mod}^{\mathbb{Z}}\Lambda$, *we have* $\mathsf{Hom}_\Lambda(X, \Omega^n Y)_0 = 0$ *for sufficiently large n.*

Proof. Take a minimal graded projective resolution of Y: $\cdots \to P_2 \to P_1 \to P_0 \to Y \to 0$. We will show that for each $i \in \mathbb{Z}$, $P_n = (P_n)_{\geq i}$ holds for $n \gg 0$. For this, it suffices to show that $P_n = (P_n)_{\geq 1}$ for $Y = Y_{\geq 0}$. Note that the degree 0 part of the minimal projective resolution of Y yields a Λ_0-projective resolution of Y_0. By our assumption that $\operatorname{gl.dim}\Lambda_0 < \infty$, we have $(P_n)_0 = 0$, hence $(P_n)_{\geq 1} = P_n$ for sufficiently large n. Now, we have $\mathsf{Hom}_\Lambda(X, \Lambda(-n))_0 = \mathsf{Hom}_\Lambda(X,\Lambda)_{-n} = 0$ for $n \gg 0$. Indeed, this is certainly true if X is projective. For general X, take a surjection $P \twoheadrightarrow X$ from a projective module P. Then we have an injection $\mathsf{Hom}_\Lambda(X,\Lambda) \hookrightarrow \mathsf{Hom}_\Lambda(P,\Lambda)$ and our assertion follows from the case X is projective. Therefore, we conclude that $\mathsf{Hom}_\Lambda(X, P_n)_0 = 0$, thus $\mathsf{Hom}_\Lambda(X, \Omega^{n+1}Y)_0 = 0$ for sufficiently large n. □

Proof of Proposition 7.1. We verify the conditions (S1) and (S2) found in Section 6A.

First we show (S2): $\underline{\mathsf{Hom}}_\Lambda(X, \Omega^n Y)_0 = 0$ for almost all n for each $X, Y \in \underline{\mathsf{CM}}^{\mathbb{Z}}(\Lambda)$. The case $n \gg 0$ is done in Lemma 7.2, so it remains to prove the case $n \ll 0$. Since Λ is CM-finite, $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ has the AR duality, and we have $D\,\underline{\mathsf{Hom}}(X, \Omega^n Y)_0 \simeq \underline{\mathsf{Hom}}(Y, \Omega^{-n-1}\tau X)_0$, hence the assertion follows from the case of $n \gg 0$.

Next we show (S1): $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ has only finitely many indecomposables up to suspension. Since Λ is of finite CM type, there exists $0 \neq n \in \mathbb{Z}$ such that $\Omega^n X \simeq X$ up to grade shift for any indecomposable $X \in \underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$. By (S2), $\Omega^n X$ and X are not actually isomorphic in $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$. Therefore, $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ has only finitely many indecomposables up to Ω^n, in particular up to Ω^{-1}.

These assertions show that $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ is $[1]$-finite. □

As an application of Theorem 5.3, we immediately obtain the following result.

Theorem 7.3. *Let k be algebraically closed and let $\Lambda = \bigoplus_{n\geq 0}\Lambda_n$ is a positively graded Iwanaga–Gorenstein algebra such that each Λ_n is finite dimensional over k. Suppose Λ is CM-finite and* $\operatorname{gl.dim}\Lambda_0 < \infty$. *Then, the AR-quiver of $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ is $\mathbb{Z}\Delta$ for a disjoint union Δ of some Dynkin diagrams of type A, D and E. Moreover, $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ is triangle equivalent to* $\mathsf{D}^{\mathsf{b}}(\mathsf{mod}\,kQ)$ *for any orientation Q of Δ.*

Proof. The statement for the AR-quiver follows from Propositions 7.1 and 5.9. The triangle equivalence follows from Proposition 7.1 and Theorem 5.3. □

A well-known class of commutative Gorenstein rings of finite representation type is given by simple singularities. Here we assume that k is algebraically closed of characteristic 0. Then, they are classified up to isomorphism by the Dynkin diagrams for each $d = \dim \Lambda$ and have the form $k[x, y, z_2, \dots, z_d]/(f)$ with

(A_n) $f = x^2 + y^{n+1} + z_2^2 + \cdots + z_d^2, \quad (n \geq 1),$

(D_n) $f = x^2y + y^{n-1} + z_2^2 + \cdots + z_d^2, \quad (n \geq 4),$

(E_6) $f = x^3 + y^4 + z_2^2 + \cdots + z_d^2,$

(E_7) $f = x^3 + xy^3 + z_2^2 + \cdots + z_d^2,$

(E_8) $f = x^3 + y^5 + z_2^2 + \cdots + z_d^2;$

see [Leuschke and Wiegand 2012, Chapter 9]. We admit any grading on Λ so that each variable and f are homogeneous of positive degrees. Then, Λ is CM-finite (in the graded sense) since its completion $\hat{\Lambda}$ at the maximal ideal $\Lambda_{>0}$ is CM-finite, that is, $\mathsf{CM}\,\hat{\Lambda}$ has only finitely many indecomposable objects [Yoshino 1990, Chapter 15].

Corollary 7.4. *Let k be an algebraically closed field of characteristic zero and $\Lambda = k[x, y, z_2, \dots, z_d]/(f)$ with f one of the above. Give a grading on Λ so that each variable and f are homogeneous of positive degrees. Then, the stable category $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ is triangle equivalent to the derived category $\mathsf{D}^{\mathrm{b}}(\mathsf{mod}\, kQ)$ of the path algebra kQ of a disjoint union Q of Dynkin quivers.*

We give several more examples. First we consider the case Λ is finite dimensional.

Example 7.5. Let

$$\Lambda = \Lambda_n = k[x]/(x^n)$$

with $\deg x = 1$. Then, Λ is a finite dimensional self-injective algebra. In this case we have $\mathsf{CM}^{\mathbb{Z}}\Lambda = \mathsf{mod}^{\mathbb{Z}}\Lambda$. It is of finite representation type with indecomposable Λ-modules Λ_i $(1 \leq i \leq n)$, and $\Lambda_0 = k$ has finite global dimension. We can easily compute its AR-quiver (for $n = 4$) to be

$$\begin{tikzcd}[column sep=tiny]
 & \cdots & \circ \arrow[dr] & & \Lambda_3(-1) \arrow[dr] & & \Lambda_3 \arrow[dr] & & \Lambda_3(1) \arrow[dr] & & \circ \arrow[dr] & & \cdots \\
\cdots & \circ \arrow[ur] \arrow[dr] & & \Lambda_2(-2) \arrow[ur] \arrow[dr] & & \Lambda_2(-1) \arrow[ur] \arrow[dr] & & \Lambda_2 \arrow[ur] \arrow[dr] & & \Lambda_2(1) \arrow[ur] \arrow[dr] & & \circ \arrow[ur] \arrow[dr] & \\
 & \cdots & \circ \arrow[ur] & & \Lambda_1(-2) \arrow[ur] & & \Lambda_1(-1) \arrow[ur] & & \Lambda_1 \arrow[ur] & & \Lambda_1(1) \arrow[ur] & & \cdots,
\end{tikzcd}$$

where the top of Λ_i is in degree 0. We see that the AR-quiver of $\underline{\mathsf{mod}}^{\mathbb{Z}}\Lambda$ is $\mathbb{Z}A_{n-1}$. Consequently, we have a triangle equivalence $\underline{\mathsf{mod}}^{\mathbb{Z}}\Lambda \simeq \mathsf{D}^{\mathrm{b}}(\mathsf{mod}\, kQ)$ for a quiver Q of type A_{n-1}.

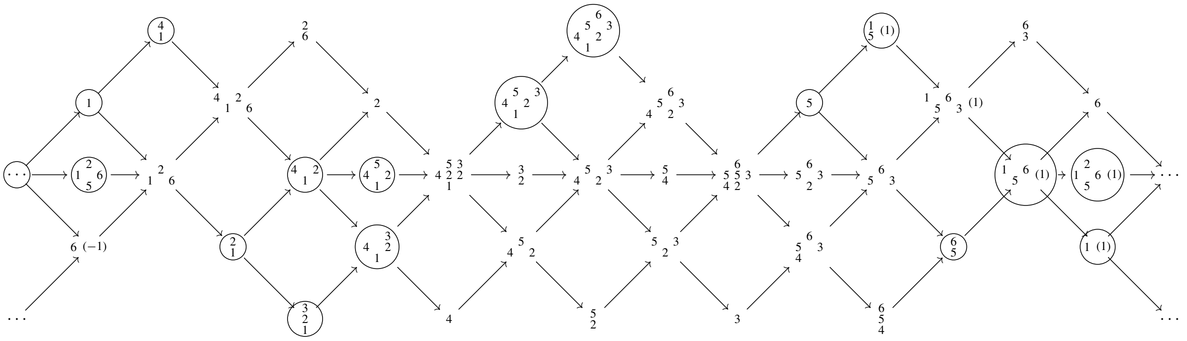
The next one is a finite dimensional Iwanaga–Gorenstein algebra.

Example 7.6. Let Λ be the algebra presented by the following quiver with relations:

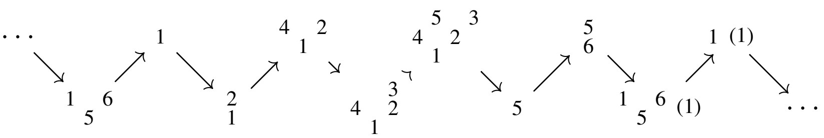
$$\begin{tikzcd}
1 \arrow[dr, "x"] & 2 \arrow[l, "a"'] \arrow[dr, "y"] & 3 \arrow[l, "b"'] \\
4 \arrow[u, "c"] & 5 \arrow[l, "f"] \arrow[u, "d"'] & 6 \arrow[l, "g"] \arrow[u, "e"']
\end{tikzcd}$$

$$da = fc,\ eb = gd,$$
$$ax = yg,$$
$$cx = 0,\ xd = 0,\ xf = 0,\ dy = 0,\ by = 0,\ ye = 0,$$

with $\deg x = \deg y = 1$ and all other arrows having degree 0. Then, it is an Iwanaga–Gorenstein algebra of dimension 1. (In fact, this is the 3-preprojective algebra [Iyama and Oppermann 2013] of its degree 0 part.) We can compute the AR-quiver of $\mathsf{mod}^{\mathbb{Z}}\Lambda$ to be the following:



Here, each module is graded so that its top is concentrated in degree 0, or equivalently, its lowest degree is at 0. We then compute the category $\mathsf{CM}^{\mathbb{Z}}\Lambda$ to be the circled modules and it is verified that the AR-quiver of $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ is



We see that this is $\mathbb{Z}A_2$ and consequently $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda \simeq \mathsf{D}^{\mathrm{b}}(\mathsf{mod}\, kQ)$ for a quiver Q of type A_2.

We consider as a final example a *Gorenstein order*: let $R = k[x_1, \dots, x_d]$ be a polynomial ring. A Noetherian R-algebra Λ is an *R-order* if it is projective as an R-module. An R-order Λ is *Gorenstein* if $\mathsf{Hom}_R(\Lambda, R)$ is projective as a Λ-module. In this case, Cohen–Macaulay Λ-modules are Λ-modules which are projective as R-modules.

Example 7.7. Let $R = k[x]$ be a graded polynomial ring with $\deg x = 1$ and let

$$\Lambda = \begin{pmatrix} R & R \\ (x^n) & R \end{pmatrix}.$$

This is a Gorenstein R-order of dimension 1. Its indecomposable CM modules up to grade shift are given by the row vectors $M_i = \big((x^i)\ \ R\big)$ for $0 \le i \le n$, and M_0 and M_n are the projectives. We define the gradings on the M_i so that their top $\begin{pmatrix}0 & k\end{pmatrix}$ is in degree 0. Then, the AR-quiver of $\mathsf{CM}^{\mathbb{Z}}\Lambda$ (for $n=4$) is computed to be

$$\begin{tikzcd}[column sep=small]
\cdots \arrow[dr] & & \circ \arrow[dr] & & M_0(-1) \arrow[dr] & & M_0 \arrow[dr] & & \cdots \\
& \circ \arrow[ur] \arrow[dr] \arrow[rr, dotted, no head] & & M_1(-1) \arrow[ur] \arrow[dr] \arrow[rr, dotted, no head] & & M_1 \arrow[ur] \arrow[dr] \arrow[rr, dotted, no head] & & M_1(1) \arrow[ur] \arrow[dr] & \\
\cdots \arrow[ur] \arrow[dr] \arrow[rr, dotted, no head] & & M_2(-1) \arrow[ur] \arrow[dr] \arrow[rr, dotted, no head] & & M_2 \arrow[ur] \arrow[dr] \arrow[rr, dotted, no head] & & M_2(1) \arrow[ur] \arrow[dr] \arrow[rr, dotted, no head] & & \cdots \\
& M_3(-1) \arrow[ur] \arrow[dr] \arrow[rr, dotted, no head] & & M_3 \arrow[ur] \arrow[dr] \arrow[rr, dotted, no head] & & M_3(1) \arrow[ur] \arrow[dr] \arrow[rr, dotted, no head] & & \circ \arrow[ur] \arrow[dr] & \\
\cdots \arrow[ur] & & M_4 \arrow[ur] & & M_4(1) \arrow[ur] & & \circ \arrow[ur] & & \cdots ,
\end{tikzcd}$$

where the upgoing arrows are natural inclusions, the downgoing arrows are the multiplications by x, and the dotted lines indicate the AR-translations. By deleting the projective vertices, we see that the AR-quiver of $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda$ is $\mathbb{Z}A_{n-1}$, and consequently $\underline{\mathsf{CM}}^{\mathbb{Z}}\Lambda \simeq \mathsf{D}^{\mathsf{b}}(\mathsf{mod}\, kQ)$ for a quiver Q of type A_{n-1}.

Acknowledgement

The author is deeply grateful to his supervisor Osamu Iyama for many helpful suggestions and careful instructions.

References

[Amiot 2007] C. Amiot, "On the structure of triangulated categories with finitely many indecomposables", *Bull. Soc. Math. France* **135**:3 (2007), 435–474. MR Zbl

[Angeleri Hügel et al. 2007] L. Angeleri Hügel, D. Happel, and H. Krause (editors), *Handbook of tilting theory*, Lond. Math. Soc. Lect. Note Ser. **332**, Cambridge Univ. Press, 2007. MR Zbl

[Artin and Zhang 1994] M. Artin and J. J. Zhang, "Noncommutative projective schemes", *Adv. Math.* **109**:2 (1994), 228–287. MR Zbl

[Asashiba 2017] H. Asashiba, "A generalization of Gabriel's Galois covering functors, II: 2-categorical Cohen–Montgomery duality", *Appl. Categ. Structures* **25**:2 (2017), 155–186. MR Zbl

[Assem et al. 2006] I. Assem, D. Simson, and A. Skowroński, *Elements of the representation theory of associative algebras, I: Techniques of representation theory*, Lond. Math. Soc. Student Texts **65**, Cambridge Univ. Press, 2006. MR Zbl

[Auslander 1971] M. Auslander, "Representation dimension of Artin algebras", lecture notes, Queen Mary College, 1971.

[Auslander and Reiten 1996] M. Auslander and I. Reiten, "*D*Tr-periodic modules and functors", pp. 39–50 in *Representation theory of algebras* (Cocoyoc, Mexico, 1994), edited by R. Bautista et al., CMS Conf. Proc. **18**, Amer. Math. Soc., Providence, RI, 1996. MR Zbl

[Auslander et al. 1995] M. Auslander, I. Reiten, and S. O. Smalø, *Representation theory of Artin algebras*, Cambridge Stud. Adv. Math. **36**, Cambridge Univ. Press, 1995. MR Zbl

[Buchweitz et al. 2020] R.-O. Buchweitz, O. Iyama, and K. Yamaura, "Tilting theory for Gorenstein rings in dimension one", *Forum Math. Sigma* **8** (2020), Paper No. e36, 37. MR

[Chen et al. 2008] X.-W. Chen, Y. Ye, and P. Zhang, "Algebras of derived dimension zero", *Comm. Algebra* **36**:1 (2008), 1–10. MR Zbl

[Curtis and Reiner 1981] C. W. Curtis and I. Reiner, *Methods of representation theory with applications to finite groups and orders, I*, Wiley, New York, 1981. MR Zbl

[Curtis and Reiner 1987] C. W. Curtis and I. Reiner, *Methods of representation theory with applications to finite groups and orders, II*, Wiley, New York, 1987. MR Zbl

[Enomoto 2018] H. Enomoto, "Classifications of exact structures and Cohen–Macaulay-finite algebras", *Adv. Math.* **335** (2018), 838–877. MR Zbl

[Erdmann and Skowroński 2008] K. Erdmann and A. Skowroński, "Periodic algebras", pp. 201–251 in *Trends in representation theory of algebras and related topics*, edited by A. Skowroński, Eur. Math. Soc., Zürich, 2008. MR Zbl

[Gordon and Green 1982] R. Gordon and E. L. Green, "Representation theory of graded Artin algebras", *J. Algebra* **76**:1 (1982), 138–152. MR Zbl

[Green et al. 2003] E. L. Green, N. Snashall, and Ø. Solberg, "The Hochschild cohomology ring of a selfinjective algebra of finite representation type", *Proc. Amer. Math. Soc.* **131**:11 (2003), 3387–3393. MR Zbl

[Happel 1988] D. Happel, *Triangulated categories in the representation theory of finite-dimensional algebras*, Lond. Math. Soc. Lect. Note Ser. **119**, Cambridge Univ. Press, 1988. MR Zbl

[Heller 1968] A. Heller, "Stable homotopy categories", *Bull. Amer. Math. Soc.* **74** (1968), 28–63. MR Zbl

[Iyama 2005] O. Iyama, "The relationship between homological properties and representation theoretic realization of Artin algebras", *Trans. Amer. Math. Soc.* **357**:2 (2005), 709–734. MR Zbl

[Iyama 2007] O. Iyama, "Auslander correspondence", *Adv. Math.* **210**:1 (2007), 51–82. MR Zbl

[Iyama and Oppermann 2013] O. Iyama and S. Oppermann, "Stable categories of higher preprojective algebras", *Adv. Math.* **244** (2013), 23–68. MR Zbl

[Kajiura et al. 2007] H. Kajiura, K. Saito, and A. Takahashi, "Matrix factorizations and representations of quivers, II: Type ADE case", *Adv. Math.* **211**:1 (2007), 327–362. MR Zbl

[Keller 1994] B. Keller, "Deriving DG categories", *Ann. Sci. École Norm. Sup.* (4) **27**:1 (1994), 63–102. MR Zbl

[Keller 2005] B. Keller, "On triangulated orbit categories", *Doc. Math.* **10** (2005), 551–581. MR Zbl

[Keller 2006] B. Keller, "On differential graded categories", pp. 151–190 in *International Congress of Mathematicians, II* (Madrid, 2006), edited by M. Sanz-Solé et al., Eur. Math. Soc., Zürich, 2006. MR Zbl

[Keller 2018] B. Keller, "A remark on a theorem by Claire Amiot", *C. R. Math. Acad. Sci. Paris* **356**:10 (2018), 984–986. MR Zbl

[Krause 2007] H. Krause, "Derived categories, resolutions, and Brown representability", pp. 101–139 in *Interactions between homotopy theory and algebra* (Chicago, 2004), edited by L. L. Avramov et al., Contemp. Math. **436**, Amer. Math. Soc., Providence, RI, 2007. MR Zbl

[Leuschke and Wiegand 2012] G. J. Leuschke and R. Wiegand, *Cohen–Macaulay representations*, Math. Surv. Monogr. **181**, Amer. Math. Soc., Providence, RI, 2012. MR Zbl

[Muro 2020] F. Muro, "Enhanced finite triangulated categories", *Journal of the Institute of Mathematics of Jussieu* (2020), 1–43.

[Neeman 2001] A. Neeman, *Triangulated categories*, Ann. of Math. Stud. **148**, Princeton Univ. Press, 2001. MR Zbl

[Riedtmann 1980] C. Riedtmann, "Algebren, Darstellungsköcher, Überlagerungen und zurück", *Comment. Math. Helv.* **55**:2 (1980), 199–224. MR Zbl

[Rouquier 2008] R. Rouquier, "Dimensions of triangulated categories", *J. K-Theory* **1**:2 (2008), 193–256. MR Zbl

[Simson 1992] D. Simson, *Linear representations of partially ordered sets and vector space categories*, Algebra Logic Appl. **4**, Gordon and Breach, Montreux, Switzerland, 1992. MR Zbl

[Xiao and Zhu 2005] J. Xiao and B. Zhu, "Locally finite triangulated categories", *J. Algebra* **290**:2 (2005), 473–490. MR Zbl

[Yamaura 2013] K. Yamaura, "Realizing stable categories as derived categories", *Adv. Math.* **248** (2013), 784–819. MR Zbl

[Yoshino 1990] Y. Yoshino, *Cohen–Macaulay modules over Cohen–Macaulay rings*, Lond. Math. Soc. Lect. Note Ser. **146**, Cambridge Univ. Press, 1990. MR Zbl

[Yoshino 2005] Y. Yoshino, "A functorial approach to modules of G-dimension zero", *Illinois J. Math.* **49**:2 (2005), 345–367. MR Zbl

Communicated by Michel Van den Bergh
Received 2018-09-28 Revised 2019-12-01 Accepted 2020-04-23

m17034e@math.nagoya-u.ac.jp *Graduate School of Mathematics, Nagoya University, Furocho, Chikusa-ku, Nagoya, Japan*

ALGEBRA AND NUMBER THEORY 14:8 (2020)
https://doi.org/10.2140/ant.2020.14.2059

Supersingular locus of Hilbert modular varieties, arithmetic level raising and Selmer groups

Yifeng Liu and Yichao Tian

This article has three goals: First, we generalize the result of Deuring and Serre on the characterization of supersingular locus to all Shimura varieties given by totally indefinite quaternion algebras over totally real number fields. Second, we generalize the result of Ribet on arithmetic level raising to such Shimura varieties in the inert case. Third, as an application to number theory, we use the previous results to study the Selmer group of certain triple product motive of an elliptic curve, in the context of the Bloch–Kato conjecture.

1. Introduction

The study of special loci of moduli spaces of abelian varieties starts from Deuring and Serre. Let $N \geq 4$ be an integer and p a prime not dividing N. Let $Y_0(N)$ be the coarse moduli scheme over $\mathbb{Z}_{(p)}$ parametrizing elliptic curves with a cyclic subgroup of order N. Let $Y_0(N)^{\mathrm{ss}}_{\mathbb{F}_p}$ denote the supersingular locus of the special fiber $Y_0(N)_{\mathbb{F}_p}$, which is a closed subscheme of dimension zero. Deuring and Serre proved the following deep result (see, for example [Serre 1996]) characterizing the supersingular locus:

$$Y_0(N)^{\mathrm{ss}}_{\mathbb{F}_p}(\mathbb{F}_p^{\mathrm{ac}}) \cong B^\times\backslash\hat{B}^\times/\hat{R}^\times. \tag{1-1}$$

Here, B is the definition quaternion algebra over $\mathbb{Q}$ ramified at p, and $R \subseteq B$ is any Eichler order of level N. Moreover, the induced action of the Frobenius element on $B^\times\backslash\hat{B}^\times/\hat{R}^\times$ coincides with the Hecke action given by the uniformizer of $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$.

One main application of the above result is to study congruence of modular forms. Let $f = q + a_2q^2 + a_3q^3 + \cdots$ be a normalized cusp new form of level $\Gamma_0(N)$ and weight 2. Let $\mathfrak{m}_f$ be the ideal of the away-from-Np Hecke algebra generated by $\mathrm{T}_v - a_v$ for all primes $v \nmid Np$. We assume that f is not

MSC2010: primary 14G35; secondary 11G05, 11R34.
Keywords: Hilbert modular varieties, supersingular locus, automorphic forms, level raising, Selmer groups.

dihedral. Take a sufficiently large prime ℓ, not dividing $Np(p^2-1)$. Using the isomorphism (1-1) and the Abel–Jacobi map (over $\mathbb{F}_{p^2}$), one can construct a map

$$\Gamma(B^\times\backslash\hat{B}^\times/\hat{R}^\times,\mathbb{F}_\ell)/\mathfrak{m}_f\to \mathrm{H}^1(\mathbb{F}_{p^2},\mathrm{H}^1(Y_0(N)\otimes\mathbb{F}_p^{\mathrm{ac}},\mathbb{F}_\ell(1))/\mathfrak{m}_f) \tag{1-2}$$

where $\Gamma(B^\times\backslash\hat{B}^\times/\hat{R}^\times,\mathbb{F}_\ell)$ denotes the space of $\mathbb{F}_\ell$-valued functions on $B^\times\backslash\hat{B}^\times/\hat{R}^\times$. [Ribet 1990] proved that the map (1-2) is surjective. Note that the right-hand side is nonzero if and only if $\ell\mid a_p^2-(p+1)^2$, in which case the dimension is 1. From this, one can construct a normalized cusp new form g of level $\Gamma_0(Np)$ and weight 2 such that $f\equiv g \mod \ell$ when $\ell\mid a_p^2-(p+1)^2$.

This article has three goals: First, we generalize the result of Deuring and Serre to all Shimura varieties given by totally indefinite quaternion algebras over totally real number fields. Second, we generalize Ribet's result to such Shimura varieties in the inert case. Third, as an application to number theory, we use the previous results to study Selmer groups of certain triple product motives of elliptic curves, in the context of the Bloch–Kato conjecture.

For the rest of Introduction, we denote F a totally real number field, and B a *totally indefinite* quaternion algebra over F. Put $G:=\mathrm{Res}_{F/\mathbb{Q}}B^\times$ as a reductive group over $\mathbb{Q}$.

1A. ***Supersingular locus of Hilbert modular varieties.*** Let p be a rational prime that is unramified in F. Denote by Σ_p the set of all places of F above p, and put $g_\mathfrak{p}:=[F_\mathfrak{p}:\mathbb{Q}_p]$ for every $\mathfrak{p}\in\Sigma_p$. Assume that B is unramified at all $\mathfrak{p}\in\Sigma_p$. Fix a maximal order $\mathcal{O}_B$ in B. Let $K^p\subseteq G(\mathbb{A}^\infty)$ be a neat open compact subgroup in the sense of Definition 2.6. We have a coarse moduli scheme $\mathbf{Sh}(G,K^p)$ over $\mathbb{Z}_{(p)}$ parametrizing abelian varieties with real multiplication by $\mathcal{O}_B$ and K^p-level structure (see Section 2E for details). Its generic fiber is a Shimura variety; in particular, we have the following well-known complex uniformization:

$$\mathbf{Sh}(G,K^p)(\mathbb{C})\cong G(\mathbb{Q})\backslash(\mathbb{C}-\mathbb{R})^{[F:\mathbb{Q}]}\times G(\mathbb{A}^\infty)/K^pK_p,$$

where K_p is a hyperspecial maximal subgroup of $G(\mathbb{Q}_p)$. The supersingular locus of $\mathbf{Sh}(G,K^p)$, that is, the maximal closed subset of $\mathbf{Sh}(G,K^p)\otimes\mathbb{F}_p^{\mathrm{ac}}$ on which the parametrized abelian variety (over $\mathbb{F}_p^{\mathrm{ac}}$) has supersingular p-divisible group, descends to $\mathbb{F}_p$, denoted by $\mathbf{Sh}(G,K^p)^{\mathrm{ss}}_{\mathbb{F}_p}$. Our first result provides a global description of the subscheme $\mathbf{Sh}(G,K^p)^{\mathrm{ss}}_{\mathbb{F}_p}$.

To state our theorem, we need to introduce another Shimura variety. Let $B^\dagger$ be the quaternion algebra over F, unique up to isomorphism, such that the Hasse invariants of $B^\dagger$ and B differ exactly at all archimedean places and all $\mathfrak{p}\in\Sigma_p$ with $g_\mathfrak{p}$ odd. Similarly, put $G^\dagger:=\mathrm{Res}_{F/\mathbb{Q}}(B^\dagger)^\times$ and identify $G^\dagger(\mathbb{A}^{\infty,p})$ with $G(\mathbb{A}^{\infty,p})$. We put

$$\mathbf{Sh}(G^\dagger,K^p)(\mathbb{F}_p^{\mathrm{ac}}):=G^\dagger(\mathbb{Q})\backslash G^\dagger(\mathbb{A}^\infty)/K^pK_p^\dagger,$$

where $K_p^\dagger$ is a maximal open compact subgroup of $G^\dagger(\mathbb{Q}_p)$. We denote by $\mathbf{Sh}(G^\dagger,K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$ the corresponding scheme over $\mathbb{F}_p^{\mathrm{ac}}$, that is, copies of $\mathrm{Spec}\,\mathbb{F}_p^{\mathrm{ac}}$ indexed by $\mathbf{Sh}(G^\dagger,K^p)(\mathbb{F}_p^{\mathrm{ac}})$.

Theorem 1.1 (Theorem 3.13). *Let h be the least common multiple of $(1+g_{\mathfrak{p}}-2\lfloor g_{\mathfrak{p}}/2\rfloor)g_{\mathfrak{p}}$ for $\mathfrak{p}\in\Sigma_p$. We have*[1]

$$\mathbf{Sh}(G,K^p)^{\mathrm{ss}}_{\mathbb{F}_p}\otimes\mathbb{F}_{p^h}=\bigcup_{\mathfrak{a}\in\mathfrak{B}}W(\mathfrak{a}).$$

Here

- *$\mathfrak{B}$ is a set of cardinality $\prod_{\mathfrak{p}\in\Sigma_p}\binom{g_{\mathfrak{p}}}{\lfloor g_{\mathfrak{p}}/2\rfloor}$ equipped with a natural action by* $\mathrm{Gal}(\mathbb{F}_{p^h}/\mathbb{F}_p)$;
- *the base change $W(\mathfrak{a})\otimes\mathbb{F}_p^{\mathrm{ac}}$ is a $\bigl(\sum_{\mathfrak{p}\in\Sigma_p}\lfloor g_{\mathfrak{p}}/2\rfloor\bigr)$-th iterated $\mathbb{P}^1$-fibration over $\mathbf{Sh}(G^\dagger,K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$, equivariant under prime-to-p Hecke correspondences.*[2]

In particular, $\mathbf{Sh}(G,K^p)^{\mathrm{ss}}_{\mathbb{F}_p}$ is proper and of equidimension $\sum_{\mathfrak{p}\in\Sigma_p}\lfloor g_{\mathfrak{p}}/2\rfloor$.

If p is inert in F of degree 2 and B is the matrix algebra, then the result was first proved in [Bachmat and Goren 1999]. If p is inert in F of degree 4 and B is the matrix algebra, then the result was due to Yu [2003]. Assume that p is inert in F of even degree. Then the strata $W(\mathfrak{a})$ have already been constructed in [Tian and Xiao 2019], and the authors proved there that, under certain genericity conditions on the Satake parameters of a fixed automorphic cuspidal representation π, the cycles $W(\mathfrak{a})$ give all the π-isotypic Tate cycles on $\mathbf{Sh}(G,K^p)_{\mathbb{F}_p}$.

Similarly, one can define the superspecial locus $\mathbf{Sh}(G,K^p)^{\mathrm{sp}}_{\mathbb{F}_p}$ of $\mathbf{Sh}(G,K^p)$, that is, the maximal closed subset of $\mathbf{Sh}(G,K^p)\otimes\mathbb{F}_p^{\mathrm{ac}}$ on which the parametrized abelian variety has superspecial p-divisible group. It is a reduced scheme over $\mathbb{F}_p$ of dimension zero. We have the following result:

Theorem 1.2 (Theorem 3.16). *Assume that $g_{\mathfrak{p}}$ is odd for every $\mathfrak{p}\in\Sigma_p$. For each $\mathfrak{a}\in\mathfrak{B}$ as in the previous theorem, $W(\mathfrak{a})$ contains the superspecial locus $\mathbf{Sh}(G,K^p)^{\mathrm{sp}}_{\mathbb{F}_p}\otimes\mathbb{F}_{p^h}$, and the iterated $\mathbb{P}^1$-fibration $\pi_{\mathfrak{a}}\colon W(\mathfrak{a})\otimes\mathbb{F}_p^{\mathrm{ac}}\to\mathbf{Sh}(G^\dagger,K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$ induces an isomorphism*

$$\mathbf{Sh}(G,K^p)^{\mathrm{sp}}_{\mathbb{F}_p^{\mathrm{ac}}}\xrightarrow{\sim}\mathbf{Sh}(G^\dagger,K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$$

compatible with prime-to-p Hecke correspondences.

In fact, Theorem 3.16(2) shows that the $\mathbb{F}_{p^2}$-scheme structure on $\mathbf{Sh}(G^\dagger,K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$ induced from the isomorphism in the above theorem is independent of $\mathfrak{a}$. In other words, we have a canonical $\mathbb{F}_{p^2}$-scheme structure on $\mathbf{Sh}(G^\dagger,K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$, which we denote by $\mathbf{Sh}(G^\dagger,K^p)$. Then it is easy to see that the iterated $\mathbb{P}^1$-fibration $\pi_{\mathfrak{a}}$ descends to a morphism of $\mathbb{F}_{p^h}$-schemes

$$\pi_{\mathfrak{a}}\colon W(\mathfrak{a})\to\mathbf{Sh}(G^\dagger,K^p)_{\mathbb{F}_p^h}.$$

A main application of the global description of the supersingular locus is to study the level raising phenomenon, as we will explain in the next section.

[1] The notation here is simplified. In fact, in the main text and particularly Theorem 3.13, $B^\dagger$, $G^\dagger$, $\mathfrak{B}$, $\mathfrak{a}$ and $W(\mathfrak{a})$ are denoted by $B_{\mathtt{S}_{\max}}$, $G_{\mathtt{S}_{\max}}$, $\mathfrak{B}_{\varnothing}$, $\underline{\mathfrak{a}}$ and $W_{\varnothing,\varnothing}(\underline{\mathfrak{a}})$, respectively.

[2] One should consider $\mathbf{Sh}(G^\dagger,K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$ as the $\mathbb{F}_p^{\mathrm{ac}}$-fiber of a Shimura variety attached to $G^\dagger$. However, it seems impossible to define the correct Galois action on $\mathbf{Sh}(G^\dagger,K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$ using the formalism of Deligne homomorphisms when $g_{\mathfrak{p}}$ is odd for at least one $\mathfrak{p}\in\Sigma_p$. When $g_{\mathfrak{p}}$ is odd for all $\mathfrak{p}\in\Sigma_p$, we will define the correct Galois action by $\mathrm{Gal}(\mathbb{F}_p^{\mathrm{ac}}/\mathbb{F}_p)$ using superspecial locus. See the discussion after Theorem 1.2.

1B. ***Arithmetic level raising for Hilbert modular varieties.*** We suppose that $g=[F:\mathbb{Q}]$ is odd. Fix an irreducible cuspidal automorphic representation Π of $\mathrm{GL}_2(\mathbb{A}_F)$ of parallel weight 2 defined over a number field $\mathbb{E}$. Let B, G be as in the previous section; and let K be a neat open compact subgroup of $G(\mathbb{A}^\infty)$. Then we have the Shimura variety $\mathrm{Sh}(G,K)$ defined over $\mathbb{Q}$. Let $\mathtt{R}$ be a finite set of places of F away from which Π is unramified and K is hyperspecial maximal.

Let p be a rational prime inert in F such that the unique prime $\mathfrak{p}$ of F above p is not in $\mathtt{R}$. Then $K=K^pK_p$ and $\mathrm{Sh}(G,K)$ has a canonical integral model $\mathbf{Sh}(G,K^p)$ over $\mathbb{Z}_{(p)}$ as in the previous section. We also choose a prime λ of $\mathbb{E}$ and put $k_\lambda:=\mathcal{O}_{\mathbb{E}}/\lambda$.

Let $\mathbb{Z}[\mathbb{T}^{\mathtt{R}}]$ (resp. $\mathbb{Z}[\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}]$) be the (abstract) spherical Hecke algebra of $\mathrm{GL}_{2,F}$ away from $\mathtt{R}$ (resp. $\mathtt{R}\cup\{\mathfrak{p}\}$). Then Π induces a homomorphism

$$\phi_{\Pi,\lambda}\colon \mathbb{Z}[\mathbb{T}^{\mathtt{R}}]\to\mathcal{O}_{\mathbb{E}}\to k_\lambda$$

via Hecke eigenvalues. Put $\mathfrak{m}:=\ker(\phi_{\Pi,\lambda}|_{\mathbb{Z}[\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}]})$.

The Hecke algebra $\mathbb{Z}[\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}]$ acts on the (étale) cohomology group $\mathrm{H}^\bullet(\mathbf{Sh}(G,K^p)\otimes\mathbb{F}_p^{\mathrm{ac}},k_\lambda)$. Let $\Gamma(\mathfrak{B}\times\mathbf{Sh}(G^\dagger,K^p)(\mathbb{F}_p^{\mathrm{ac}}),*)$ be the abelian group of $*$-valued functions on $\mathfrak{B}\times\mathbf{Sh}(G^\dagger,K^p)(\mathbb{F}_p^{\mathrm{ac}})$, which admits the Hecke action of $\mathbb{Z}[\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}]$ via the second factor. We have a Chow cycle class map

$$\Gamma(\mathfrak{B}\times\mathbf{Sh}(G^\dagger,K^p)(\mathbb{F}_p^{\mathrm{ac}}),\mathbb{Z})\to\mathrm{CH}^{(g+1)/2}(\mathbf{Sh}(G,K^p)_{\mathbb{F}_p^{\mathrm{ac}}})$$

sending a function f on $\mathfrak{B}\times\mathbf{Sh}(G^\dagger,K^p)(\mathbb{F}_p^{\mathrm{ac}})$ to the Chow class of $\sum_{\mathfrak{a},s}f(\mathfrak{a},s)\pi_{\mathfrak{a}}^{-1}(s)$, which is $\mathbb{Z}[\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}]$-equivariant. We will show that under certain "large image" assumption on the mod-λ Galois representation attached to Π, the above Chow cycle class map (eventually) induces the following Abel–Jacobi map

$$\Gamma(\mathfrak{B}\times\mathbf{Sh}(G^\dagger,K^p)(\mathbb{F}_p^{\mathrm{ac}}),k_\lambda)/\mathfrak{m}\to\mathrm{H}^1(\mathbb{F}_{p^{2g}},\mathrm{H}^g(\mathbf{Sh}(G,K^p)_{\mathbb{F}_p^{\mathrm{ac}}},k_\lambda((g+1)/2))/\mathfrak{m}).\tag{1-3}$$

See Section 4A for more details. The following theorem is what we call *arithmetic level raising*:

Theorem 1.3 (Theorem 4.7). *Suppose that p is a λ-level raising prime in the sense of Definition 4.5. In particular, we have the following equalities in k_λ*:

$$\phi_{\Pi,\lambda}(\mathrm{T}_{\mathfrak{p}})^2=(p^g+1)^2,\quad \phi_{\Pi,\lambda}(\mathrm{S}_{\mathfrak{p}})=1,$$

where $\mathrm{T}_{\mathfrak{p}}$ (resp. $\mathrm{S}_{\mathfrak{p}}$) is the (spherical) Hecke operator at $\mathfrak{p}$ represented by $\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)\in\mathrm{GL}_2(F_{\mathfrak{p}})$ (resp. $\left(\begin{smallmatrix}p&0\\0&p\end{smallmatrix}\right)\in\mathrm{GL}_2(F_{\mathfrak{p}})$). Then the map (1-3) *is surjective.*

As we will point out in Remarks 4.2 and 4.6, if there exist rational primes inert in F, and Π is not dihedral and not isomorphic to a twist by a character of any of its internal conjugates, then for all but finitely many prime λ, there are infinitely many (with positive density) rational primes p that are λ-level raising primes.

Suppose that the Jacquet–Langlands transfer of Π to B exists, say Π_B. If $(\Pi_B^{\infty,p})^{K^p}$ has dimension 1 and there is no other automorphic representation of $B^\times(\mathbb{A}_F)$ (of parallel weight 2, unramified at $\mathfrak{p}$, and with nontrivial K^p-invariant vectors) congruent to Π_B modulo λ, then the target of (1-3) has dimension $\binom{g}{(g-1)/2}$ over k_λ.

Remark 1.4. In principle, our method can be applied to prove a theorem similar to Theorem 1.3 when B is not necessarily totally indefinite but the "supersingular locus", defined in an *ad hoc* way if B is not totally indefinite, still appears in the near middle dimension. In fact, the proof of Theorem 1.3 will be reduced to the case where B is indefinite at only one archimedean place (that is, the corresponding Shimura variety $\mathrm{Sh}(B)$ is a curve). However, we decide not to pursue the most general scenario as that would make the exposition much more complicated and technical. On the other hand, we would like to point out that arithmetic level raising when $1 < \dim \mathrm{Sh}(B) < [F : \mathbb{Q}]$ has arithmetic application as well, for example, to bound the triple product Selmer group (see the next section) with respect to a cubic extension $F/F^\flat$ of totally real number fields with $F^\flat \neq \mathbb{Q}$.

Let us explain the meaning of Theorem 1.3. Suppose that Π admits Jacquet–Langlands transfer, say Π_B, to $B^\times$ such that $\Pi_B^K \neq \{0\}$. Then the right-hand side of (1-3) is *nonzero*. In particular, under the assumption of Theorem 1.3, the left-hand side of (1-3) is nonzero as well. One can then deduce that there is an (algebraic) automorphic representation Π' of $G^\dagger(\mathbb{A}) = (B^\dagger)^\times(\mathbb{A}_F)$ (trivial at ∞) such that the associated Galois representations of Π' and Π with coefficient $\mathcal{O}_{\mathbb{E}}/\lambda$ are isomorphic. However, it is obvious that Π' cannot be the Jacquet–Langlands transfer of Π, as $B^\dagger$ is ramified at $\mathfrak{p}$ while Π is unramified at $\mathfrak{p}$. In this sense, Theorem 1.3 reveals certain level raising phenomenon. Moreover, this theorem not only proves the existence of level raising, but also provides an explicit way to realize the congruence relation behind the level raising through the Abel–Jacobi map (1-3). As this process involves cycle classes and local Galois cohomology, we prefer to call Theorem 1.3 *arithmetic level raising*. This is crucial for our later arithmetic application. Namely, we will use this arithmetic level raising theorem to bound certain Selmer groups, as we will explain in the next section.

1C. *Selmer group of triple product motive.*

In this section, we assume that $g = [F : \mathbb{Q}] = 3$; in other words, F is a totally real cubic number field.

Let E be an elliptic curve over F. We have the $\mathbb{Q}$-motive $\otimes \mathrm{Ind}_{\mathbb{Q}}^F \mathsf{h}^1(E)$ (with coefficient $\mathbb{Q}$) of rank 8, which is the multiplicative induction of the F-motive $\mathsf{h}^1(E)$ to $\mathbb{Q}$. The *cubic-triple product motive* of E is defined to be

$$\mathsf{M}(E) := (\otimes \mathrm{Ind}_{\mathbb{Q}}^F \mathsf{h}^1(E))(2).$$

It is canonically polarized. For every prime p, the p-adic realization of $\mathsf{M}(E)$, denoted by $\mathsf{M}(E)_p$, is a Galois representation of $\mathbb{Q}$ of dimension 8 with $\mathbb{Q}_p$-coefficients. In fact, up to a twist, it is the multiplicative induction from F to $\mathbb{Q}$ of the rational p-adic Tate module of E.

Now we assume that E is modular. Then it gives rise to an irreducible cuspidal automorphic representation Π_E of $(\mathrm{Res}_{F/\mathbb{Q}} \mathrm{GL}_{2,F})(\mathbb{A}) = \mathrm{GL}_2(\mathbb{A}_F)$ with trivial central character. Denote by $\tau : {}^L G \to \mathrm{GL}_8(\mathbb{C})$ the triple product L-homomorphism [Piatetski-Shapiro and Rallis 1987, Section 0], and $L(s, \Pi_E, \tau)$ the triple product L-function, which has a meromorphic extension to the complex plane by [Garrett 1987;

Piatetski-Shapiro and Rallis 1987]. Moreover, we have a functional equation

$$L(s,\Pi_E,\tau)=\epsilon(\Pi_E,\tau)C(\Pi_E,\tau)^{1/2-s}L(1-s,\Pi_E,\tau)$$

for some $\epsilon(\Pi_E,\tau)\in\{\pm 1\}$ and positive integer $C(\Pi_E,\tau)$. The global root number $\epsilon(\Pi_E,\tau)$ is the product of local ones: $\epsilon(\Pi_E,\tau)=\prod_v \epsilon(\Pi_{E,v},\tau)$, where v runs over all places of $\mathbb{Q}$. Here, we have $\epsilon(\Pi_{E,v},\tau)\in\{\pm 1\}$ and that it equals 1 for all but finitely many v. Put

$$\Sigma(\Pi_E,\tau):=\{v\mid \epsilon(\Pi_{E,v},\tau)=-1\}.$$

In particular, the set $\Sigma(\Pi_E,\tau)$ contains ∞. We have $L(s,\mathsf{M}(E))=L\bigl(s+\frac{1}{2},\Pi_E,\tau\bigr)$.

Now we assume that E satisfies Assumption 5.1. In particular, $\Sigma(\Pi_E,\tau)$ has odd cardinality. Let $B^\flat$ be the indefinite quaternion algebra over $\mathbb{Q}$ with the ramification set $\Sigma(\Pi_E,\tau)-\{\infty\}$, and put $B:=B^\flat\otimes_{\mathbb{Q}}F$. Put $G:=\operatorname{Res}_{F/\mathbb{Q}}B^\times$ as before. We will define neat open compact subgroups $K_{\mathfrak{r}}\subseteq G(\mathbb{A})$, indexed by certain integral ideals $\mathfrak{r}$ of F. We have the Shimura threefold $\mathrm{Sh}(G,K_{\mathfrak{r}})$ over $\mathbb{Q}$. Put $G^\flat:=(B^\flat)^\times$ and let $K_{\mathfrak{r}}^\flat\subseteq G^\flat(\mathbb{A})$ be induced from $K_{\mathfrak{r}}$. Then we have the Shimura curve $\mathrm{Sh}(G^\flat,K_{\mathfrak{r}}^\flat)$ over $\mathbb{Q}$ with a canonical finite morphism to $\mathrm{Sh}(G,K_{\mathfrak{r}})$. Using this 1-cycle, we obtain, under certain conditions, a cohomology class

$$\Theta_{p,\mathfrak{r}}\in \mathrm{H}^1_f(\mathbb{Q},\mathsf{M}(E)_p)^{\oplus a(\mathfrak{r})},$$

where $\mathrm{H}^1_f(\mathbb{Q},\mathsf{M}(E)_p)$ is the *Bloch–Kato Selmer group* (Definition 5.6) of the Galois representation $\mathsf{M}(E)_p$ (with coefficient $\mathbb{Q}_p$), and $a(\mathfrak{r})>0$ is some integer depending on $\mathfrak{r}$. See Section 5A for more details of this construction. We have the following theorem on bounding the Bloch–Kato Selmer group using the class $\Theta_{p,\mathfrak{r}}$.

Theorem 1.5 (Theorem 5.7). *Let E be a modular elliptic curve over F satisfying Assumption 5.1. For a rational prime p, if there exists a perfect pair $(p,\mathfrak{r})$ such that $\Theta_{p,\mathfrak{r}}\neq 0$, then we have*

$$\dim_{\mathbb{Q}_p}\mathrm{H}^1_f(\mathbb{Q},\mathsf{M}(E)_p)=1.$$

See Definition 5.4 for the meaning of perfect pairs, and also Remark 5.8.

The above theorem is closely related to the Bloch–Kato conjecture. We refer readers to the Introduction of [Liu 2016] for the background of this conjecture, especially how Theorem 1.5 can be compared to the seminal work of Kolyvagin [1990] and the parallel result [Liu 2016, Theorem 1.5] for another triple product case. In particular, we would like to point out that under the (conjectural) triple product version of the Gross–Zagier formula and the Beilinson–Bloch conjecture on the injectivity of the Abel–Jacobi map, the following two statements should be equivalent:

- $L'(0,\mathsf{M}(E))\neq 0$ (note that $L(0,\mathsf{M}(E))=0$).
- There exists some $\mathfrak{r}_0$ such that for every other $\mathfrak{r}$ contained in $\mathfrak{r}_0$, we have $\Theta_{p,\mathfrak{r}}\neq 0$ as long as $(p,\mathfrak{r})$ is a perfect pair.

Assuming this, then Theorem 1.5 implies that if $L'(0, \mathsf{M}(E)) \neq 0$, that is, $\mathrm{ord}_{s=0} L(s, \mathsf{M}(E)) = 1$, then $\dim_{\mathbb{Q}_p} \mathrm{H}^1_f(\mathbb{Q}, \mathsf{M}(E)_p) = 1$ for all but finitely many p. This is certainly evidence toward the Bloch–Kato conjecture for the motive $\mathsf{M}(E)$.

At this point, it is not clear how the arithmetic level raising, Theorem 1.3, is related to Theorem 1.5. We will briefly explain this in the next section.

1D. ***Structure and strategies.*** There are four sections in the main part. In short words, Section 2 is responsible for the basics on Shimura varieties that we will use later; Section 3 is responsible for Theorems 1.1 and 1.2; Section 4 is responsible for Theorem 1.3; and Section 5 is responsible for Theorem 1.5.

In Section 2, we study certain Shimura varieties and their integral models attached to both unitary groups of rank 2 and quaternion algebras, and compare them through Deligne's recipe of connected Shimura varieties. The reason we have to study unitary Shimura varieties is the following: In the proof of Theorems 1.1, 1.2 and 1.3, we have to use an induction process to go through certain quaternionic Shimura varieties associated to B that are *not* totally indefinite. Those Shimura varieties are not (coarse) moduli spaces but we still want to carry the information from the moduli interpretation through the induction process. Therefore, we use the technique of changing Shimura data by studying closely related unitary Shimura varieties, which are of PEL-type. Such argument is coherent with [Tian and Xiao 2016] in which the authors study Goren–Oort stratification on quaternionic Shimura varieties.

In Section 3, we first construct candidates for the supersingular locus in Theorem 1.1 via Goren–Oort strata, which were studied in [Tian and Xiao 2016], and then prove that they exactly form the entire supersingular locus, both through an induction argument. As we mentioned previously, during the induction process, we need to compare quaternionic Shimura varieties to unitary ones. At last, we identify and prove certain properties for the superspecial locus, in some special cases.

In Section 4, we state and prove the arithmetic level raising result. Using the nondegeneracy of certain intersection matrices proved in [Tian and Xiao 2019], we can reduce Theorem 1.3 to establishing a similar isomorphism on certain quaternionic Shimura curves. Then we use the well-known argument of Ribet together with Ihara's lemma in this context to establish such isomorphism on curves.

In Section 5, we focus on the number theoretical application of the arithmetic level raising established in the previous section. The basic strategy to bound the Selmer group follows the same line as in [Kolyvagin 1990; Liu 2016; 2019]. Namely, we construct a family of cohomology classes $\Theta^{\nu}_{p,\mathfrak{r},\underline{\ell}}$ to serve as annihilators of the Selmer group after quotient by the candidate class $\Theta_{p,\mathfrak{r}}$ in rank 1 case. In the case considered here, those cohomology classes are indexed by an integer ν as the depth of congruence, and a pair of rational primes $\underline{\ell} = (\ell, \ell')$ that are "p^{ν}-level raising primes" (see Definition 5.10 for the precise terminology and meaning). The key idea is to connect $\Theta_{p,\mathfrak{r}}$ and various $\Theta^{\nu}_{p,\mathfrak{r},\underline{\ell}}$ through some objects in the middle, that is, some mod-p^{ν} modular forms on a certain Shimura set. Following past literature, the link between $\Theta_{p,\mathfrak{r}}$ and those mod-p^{ν} modular forms is called the *second explicit reciprocity law*; while the link between $\Theta^{\nu}_{p,\mathfrak{r},\underline{\ell}}$ and those mod-p^{ν} modular forms is called the *first explicit reciprocity law*. The first law in this context has already been established by one of us in [Liu 2019]. To establish the second law, we use Theorem 1.3; namely, we have to compute the corresponding element in the left-hand side in the isomorphism of Theorem 1.3 of the image of $\Theta_{p,\mathfrak{r}}$ in the right-hand side.

1E. ***Notation and conventions.*** The following list contains basic notation and conventions we fix throughout the article. We will usually not recall them when we use, as most of them are common:

- Let Λ be an abelian group and S a finite set. We denote by $|S|$ the cardinality of S and $\Gamma(S, \Lambda)$ the abelian group of Λ-valued functions on S.
- If a base is not specified in the tensor operation $\otimes$, then it is $\mathbb{Z}$. For an abelian group A, put $\hat{A} := A \otimes (\varprojlim_n \mathbb{Z}/n)$. In particular, we have $\hat{\mathbb{Z}} = \prod_l \mathbb{Z}_l$, where l runs over all rational primes. For a fixed rational prime p, we put $\hat{\mathbb{Z}}^{(p)} := \prod_{l \neq p} \mathbb{Z}_l$.
- We denote by $\mathbb{A}$ the ring of adèles over $\mathbb{Q}$. For a set $\Box$ of places of $\mathbb{Q}$, we denote by $\mathbb{A}^{\Box}$ the ring of adèles away from $\Box$. For a number field F, we put $\mathbb{A}^{\Box}_F := \mathbb{A}^{\Box} \otimes_{\mathbb{Q}} F$. If $\Box = \{v_1, \dots, v_n\}$ is a finite set, we will also write $\mathbb{A}^{v_1,\dots,v_n}$ for $\mathbb{A}^{\Box}$.
- For a field K, denote by K^{ac} the algebraic closure of K and put $\mathrm{G}_K := \mathrm{Gal}(K^{\mathrm{ac}}/K)$. Denote by $\mathbb{Q}^{\mathrm{ac}}$ the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. When K is a subfield of $\mathbb{Q}^{\mathrm{ac}}$, we take G_K to be $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ac}}/K)$ hence a subgroup of $\mathrm{G}_{\mathbb{Q}}$.
- For a number field K, we denote by $\mathcal{O}_K$ the ring of integers in K. For every finite place v of $\mathcal{O}_K$, we denote by $\mathcal{O}_{K,v}$ the ring of integers of the completion of K at v.
- If K is a local field, then we denote by $\mathcal{O}_K$ its ring of integers, $\mathrm{I}_K \subseteq \mathrm{G}_K$ the inertia subgroup. If v is a rational prime, then we simply write G_v for $\mathrm{G}_{\mathbb{Q}_v}$ and I_v for $\mathrm{I}_{\mathbb{Q}_v}$.
- Let K be a local field, Λ a ring, and N a $\Lambda[\mathrm{G}_K]$-module. We have an exact sequence of Λ-modules
$$0 \to \mathrm{H}^1_{\mathrm{unr}}(K, N) \to \mathrm{H}^1(K, N) \xrightarrow{\partial} \mathrm{H}^1_{\mathrm{sing}}(K, N) \to 0,$$
where $\mathrm{H}^1_{\mathrm{unr}}(K, N)$ is the submodule of unramified classes.
- Let Λ be a ring and N a $\Lambda[\mathrm{G}_{\mathbb{Q}}]$-module. For each prime power v, we have the localization map $\mathrm{loc}_v \colon \mathrm{H}^1(\mathbb{Q}, N) \to \mathrm{H}^1(\mathbb{Q}_v, N)$ of Λ-modules.
- Denote by $\mathbb{P}^1$ the projective line scheme over $\mathbb{Z}$, and $\mathbb{G}_m = \mathrm{Spec}\,\mathbb{Z}[T, T^{-1}]$ the multiplicative group scheme.
- Let X be a scheme. The cohomology group $\mathrm{H}^\bullet(X, -)$ will always be computed on the étale site of X. If X is of finite type over a subfield of $\mathbb{C}$, then $\mathrm{H}^\bullet(X(\mathbb{C}), -)$ will be understood as the Betti cohomology of the associated complex analytic space $X(\mathbb{C})$.

2. Shimura varieties and moduli interpretations

In this section, we study certain Shimura varieties and their integral models attached to both unitary groups of rank 2 and quaternion algebras, and compare them through Deligne's recipe of connected Shimura varieties.

Let F be a totally real number field, and $p \geq 3$ a rational prime unramified in F. Denote by $\Sigma_\infty = \mathrm{Hom}_{\mathbb{Q}}(F, \mathbb{C})$ the set of archimedean places of F, and Σ_p the set of p-adic places of F above p. We fix throughout Sections 2 and 3 an isomorphism $\iota_p \colon \mathbb{C} \xrightarrow{\sim} \mathbb{Q}_p^{\mathrm{ac}}$. Via ι_p, we identify Σ_∞ with the set of p-adic embeddings of F via ι_p. For each $\mathfrak{p} \in \Sigma_p$, we put $g_{\mathfrak{p}} := [F_{\mathfrak{p}} : \mathbb{Q}_p]$ and denote by $\Sigma_{\infty/\mathfrak{p}}$ the subset of p-adic embeddings that induce $\mathfrak{p}$, so that we have

$$\Sigma_\infty = \coprod_{\mathfrak{p} \in \Sigma_p} \Sigma_{\infty/\mathfrak{p}}.$$

Since p is unramified in F, the Frobenius, denoted by σ, acts as a cyclic permutation on each $\Sigma_{\infty/\mathfrak{p}}$.

We fix also a totally indefinite quaternion algebra B over F such that B splits at all places of F above p.

2A. ***Quaternionic Shimura varieties.*** Let $\mathtt{S}$ be a subset of $\Sigma_\infty \cup \Sigma_p$ of even cardinality, and put $\mathtt{S}_\infty := \mathtt{S} \cap \Sigma_\infty$. For each $\mathfrak{p} \in \Sigma_p$, we put $\mathtt{S}_{\mathfrak{p}} := \mathtt{S} \cap (\Sigma_{\infty/\mathfrak{p}} \cup \{\mathfrak{p}\})$ and $\mathtt{S}_{\infty/\mathfrak{p}} = \mathtt{S} \cap \Sigma_{\infty/\mathfrak{p}}$. We suppose that $\mathtt{S}_{\mathfrak{p}}$ satisfies the following assumptions.

Assumption 2.1. Take $\mathfrak{p} \in \Sigma_p$:

(1) If $\mathfrak{p} \in \mathtt{S}$, then $g_{\mathfrak{p}}$ is odd and $\mathtt{S}_{\mathfrak{p}} = \Sigma_{\infty/\mathfrak{p}} \cup \{\mathfrak{p}\}$.

(2) If $\mathfrak{p} \notin \mathtt{S}$, then $\mathtt{S}_{\infty/\mathfrak{p}}$ is a disjoint union of chains of even cardinality under the Frobenius action on $\Sigma_{\infty/\mathfrak{p}}$, that is, either $\mathtt{S}_{\mathfrak{p}} = \Sigma_{\infty/\mathfrak{p}}$ has even cardinality or there exist $\tau_1, \dots, \tau_r \in \Sigma_{\infty/\mathfrak{p}}$ and integers $m_1, \dots, m_r \geq 1$ such that

$$\mathtt{S}_{\mathfrak{p}} = \coprod_{i=1}^{r} \{\tau_i, \sigma^{-1}\tau_i, \dots, \sigma^{-2m_i+1}\tau_i\} \tag{2-1}$$

and $\sigma\tau_i, \sigma^{-2m_i}\tau_i \notin \mathtt{S}_{\mathfrak{p}}$.

Let $B_{\mathtt{S}}$ denote the quaternion algebra over F whose ramification set is the union of $\mathtt{S}$ with the ramification set of B. We put $G_{\mathtt{S}} := \mathrm{Res}_{F/\mathbb{Q}}(B_{\mathtt{S}}^\times)$. For $\mathtt{S} = \varnothing$, we usually write $G = G_\varnothing$. Then $G_{\mathtt{S}}$ is isomorphic to G over F_v for every place $v \notin \mathtt{S}$, and we fix an isomorphism

$$G_{\mathtt{S}}(\mathbb{A}^{\infty,p}) \cong G(\mathbb{A}^{\infty,p}).$$

Let $\mathtt{T}$ be a subset of $\mathtt{S}_\infty$, and $\mathtt{T}_{\mathfrak{p}} = \mathtt{S}_{\infty/\mathfrak{p}} \cap \mathtt{T}$ for each $\mathfrak{p} \in \Sigma_p$. Throughout this paper, we will always assume that $|\mathtt{T}_{\mathfrak{p}}| = \#\mathtt{S}_{\mathfrak{p}}/2$. Consider the Deligne homomorphism

$$\begin{aligned} h_{\mathtt{S},\mathtt{T}} \colon \mathbb{S}(\mathbb{R}) = \mathbb{C}^\times &\to G_{\mathtt{S}}(\mathbb{R}) \cong \mathrm{GL}_2(\mathbb{R})^{\Sigma_\infty - \mathtt{S}_\infty} \times (\mathbb{H}^\times)^{\mathtt{T}} \times (\mathbb{H}^\times)^{\mathtt{S}_\infty - \mathtt{T}} \\ x + \sqrt{-1}y &\mapsto \left(\begin{pmatrix} x & y \\ -y & x \end{pmatrix}^{\Sigma_\infty - \mathtt{S}_\infty}, (x^2+y^2)^{\mathtt{T}}, 1^{\mathtt{S}_\infty - \mathtt{T}} \right) \end{aligned}$$

where $\mathbb{H}$ denotes the Hamiltonian algebra over $\mathbb{R}$. Then $G_{\mathtt{S},\mathtt{T}} := (G_{\mathtt{S}}, h_{\mathtt{S},\mathtt{T}})$ is a Shimura datum, whose reflex field $F_{\mathtt{S},\mathtt{T}}$ is the subfield of the Galois closure of F in $\mathbb{C}$ fixed by the subgroup stabilizing both $\mathtt{S}_\infty$ and $\mathtt{T}$. For instance, if $\mathtt{S}_\infty = \varnothing$, then $\mathtt{T} = \varnothing$ and $F_{\mathtt{S}} = \mathbb{Q}$. Let $\wp$ denote the p-adic place of $F_{\mathtt{S},\mathtt{T}}$ via the embedding $F_{\mathtt{S},\mathtt{T}} \hookrightarrow \mathbb{C} \xrightarrow{\sim} \mathbb{Q}_p^{\mathrm{ac}}$. By abuse of notation, we will often write $G = G_{\varnothing,\varnothing}$ in what follows.

In this article, we fix an open compact subgroup $K_p = \prod_{\mathfrak{p}\in\Sigma_p} K_{\mathfrak{p}} \subseteq G_{\mathtt{S}}(\mathbb{Q}_p) = \prod_{\mathfrak{p}\in\Sigma_p}(B_{\mathtt{S}} \otimes_F F_{\mathfrak{p}})^{\times}$, where

- $K_{\mathfrak{p}}$ is a hyperspecial subgroup if $\mathfrak{p} \notin \mathtt{S}$, and
- $K_{\mathfrak{p}} = \mathcal{O}_{B_{\mathfrak{p}}}^{\times}$ is the unique maximal open compact subgroup of $(B_{\mathtt{S}} \otimes_F F_{\mathfrak{p}})^{\times}$ if $\mathfrak{p} \in \mathtt{S}$.

For a sufficiently small open compact subgroup $K^p \subseteq G(\mathbb{A}^{\infty,p}) \cong G_{\mathtt{S}}(\mathbb{A}^{\infty,p})$, we have the Shimura variety $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)$ defined over $F_{\mathtt{S}}$ whose $\mathbb{C}$-points are given by

$$\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)(\mathbb{C}) = G_{\mathtt{S}}(\mathbb{Q})\backslash(\mathfrak{H}^{\pm})^{\Sigma_\infty - \mathtt{S}_\infty} \times G_{\mathtt{S}}(\mathbb{A}^{\infty})/K^pK_p$$

where $K = K^pK_p \subseteq G(\mathbb{A}^{\infty})$, and $\mathfrak{H}^{\pm} = \mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R})$ is the union of upper and lower half-planes. Note that the scheme $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)_{\mathbb{Q}^{\mathrm{ac}}}$ over $\mathbb{Q}^{\mathrm{ac}}$ is independent of $\mathtt{T}$, but different choices of $\mathtt{T}$ will give rise to different actions of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ac}}/F_{\mathtt{S},\mathtt{T}})$ on $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)_{\mathbb{Q}^{\mathrm{ac}}}$.

When $\mathtt{S}_\infty = \Sigma_\infty$, the action of $\Gamma_{F_{\mathtt{S},\mathtt{T}}} := \mathrm{Gal}(\mathbb{Q}^{\mathrm{ac}}/F_{\mathtt{S},\mathtt{T}})$ on the set $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)(\mathbb{Q}^{\mathrm{ac}})$ is given as follows. Note that the Deligne homomorphism $h_{\mathtt{S},\mathtt{T}}$ factors through the center $T_F = \mathrm{Res}_{F/\mathbb{Q}}(\mathbb{G}_m) \subseteq G_{\mathtt{S}}$, and the action of $\Gamma_{F_{\mathtt{S},\mathtt{T}}}$ factors thus through its maximal abelian quotient $\Gamma^{\mathrm{ab}}_{F_{\mathtt{S},\mathtt{T}}}$. Let $\mu\colon \mathbb{G}_{m,F_{\mathtt{S},\mathtt{T}}} \to T_F \otimes_{\mathbb{Q}} F_{\mathtt{S},\mathtt{T}}$ be the Hodge cocharacter (defined over the reflex field $F_{\mathtt{S},\mathtt{T}}$) associated with $h_{\mathtt{S},\mathtt{T}}$. Let $\mathrm{Art}\colon \mathbb{A}^{\infty,\times}_{F_{\mathtt{S},\mathtt{T}}} \to \Gamma^{\mathrm{ab}}_{F_{\mathtt{S},\mathtt{T}}}$ denote the Artin reciprocity map that sends uniformizers to geometric Frobenii. Then the action of $\mathrm{Art}(g)$ on $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)(\mathbb{Q}^{\mathrm{ac}})$ is given by the multiplication by the image of g under the composite map

$$\mathbb{A}^{\infty,\times}_{F_{\mathtt{S},\mathtt{T}}} \xrightarrow{\mu} T_F(\mathbb{A}^{\infty}_{F_{\mathtt{S},\mathtt{T}}}) = (F \otimes_{\mathbb{Q}} \mathbb{A}^{\infty}_{F_{\mathtt{S},\mathtt{T}}})^{\times} \xrightarrow{\mathrm{N}_{F_{\mathtt{S},\mathtt{T}}/\mathbb{Q}}} \mathbb{A}^{\infty,\times}_{F} \subseteq G_{\mathtt{S}}(\mathbb{A}^{\infty}).$$

If $\tilde{F}$ denotes the Galois closure of F in $\mathbb{C}$, then the restriction of the action of $\Gamma_{F_{\mathtt{S},\mathtt{T}}}$ to $\Gamma_{\tilde{F}}$ depends only on $\#\mathtt{T}$.

We put $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}}) := \varprojlim_{K^p} \mathrm{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)$. Let $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}})^{\circ}$ be the neutral geometric connected component of $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}}) \otimes_{F_{\mathtt{S}}} \mathbb{Q}^{\mathrm{ac}}$, that is, the one containing the image of point

$$(i^{\Sigma_\infty - \mathtt{S}_\infty}, 1) \in (\mathfrak{H}^{\pm})^{\Sigma_\infty - \mathtt{S}_\infty} \times G_{\mathtt{S}}(\mathbb{A}^{\infty}).$$

Then $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}})^{\circ} \otimes_{\mathbb{Q}^{\mathrm{ac}},\iota_p} \mathbb{Q}_p^{\mathrm{ac}}$ descends to $\mathbb{Q}_p^{\mathrm{ur}}$, the maximal unramified extension of $\mathbb{Q}_p$ in $\mathbb{Q}_p^{\mathrm{ac}}$. Moreover, by Deligne's construction [1979], $\mathrm{Sh}_{K_p}(G_{\mathtt{S},\mathtt{T}})$ can be recovered from the connected Shimura variety $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}})^{\circ}$ together with its Galois and Hecke actions (see [Tian and Xiao 2016, 2.11] for details in our particular case).

2B. ***An auxiliary CM extension.*** Choose a CM extension E/F such that

- E/F is inert at every place of F where B is ramified,
- for $\mathfrak{p} \in \Sigma_p$, E/F is split (resp. inert) at $\mathfrak{p}$ if $g_{\mathfrak{p}}$ is even (resp. if $g_{\mathfrak{p}}$ is odd).

Let $\Sigma_{E,\infty}$ denote the set of complex embeddings of E, identified also with the set of p-embeddings of E by composing with ι_p. For $\tilde{\tau} \in \Sigma_{E,\infty}$, we denote by $\tilde{\tau}^c$ the complex conjugation of $\tilde{\tau}$. For $\mathfrak{p} \in \Sigma_p$, we denote by $\Sigma_{E,\infty/\mathfrak{p}}$ the subset of p-adic embeddings of E inducing $\mathfrak{p}$. Similarly, for a p-adic place $\mathfrak{q}$ of E, we have the subset $\Sigma_{E,\infty/\mathfrak{q}} \subseteq \Sigma_{E,\infty}$ consisting of p-adic embeddings that induce $\mathfrak{q}$.

Assumption 2.2. Consider a subset $\tilde{\mathtt{S}}_\infty \subseteq \Sigma_{E,\infty}$ satisfying the following:

(1) For each $\mathfrak{p} \in \Sigma_p$, the natural restriction map $\Sigma_{E,\infty/\mathfrak{p}} \to \Sigma_{\infty/\mathfrak{p}}$ induces a bijection $\tilde{\mathtt{S}}_{\infty/\mathfrak{p}} \xrightarrow{\sim} \mathtt{S}_{\infty/\mathfrak{p}}$, where $\tilde{\mathtt{S}}_{\infty/\mathfrak{p}} = \tilde{\mathtt{S}}_\infty \cap \Sigma_{E,\infty/\mathfrak{p}}$.

(2) For each p-adic place $\mathfrak{q}$ of E above a p-adic place $\mathfrak{p}$ of F, the cardinality of $\tilde{\mathtt{S}}_{\infty/\mathfrak{q}}$ is half of the cardinality of the preimage of $\mathtt{S}_{\infty/\mathfrak{p}}$ in $\Sigma_{E,\infty/\mathfrak{q}}$.

For instance, if $\mathfrak{p}$ splits in E into two places $\mathfrak{q}$ and $\mathfrak{q}^c$ and $\mathtt{S}_\mathfrak{p}$ is given by (2-1), then the subset

$$\tilde{\mathtt{S}}_{\infty/\mathfrak{p}} = \coprod_{i=1}^{r} \{\tilde{\tau}_i, \sigma^{-1}\tilde{\tau}_i^c, \dots, \sigma^{-2m_i+2}\tilde{\tau}_i, \sigma^{-2m_i+1}\tilde{\tau}_i^c\}$$

satisfies the requirement. Here, $\tilde{\tau}_i \in \Sigma_{E,\infty/\mathfrak{p}}$ denotes the lift of τ_i inducing the p-adic place $\mathfrak{q}$. The choice of such a $\tilde{\mathtt{S}}_\infty$ determines a collection of numbers $s_{\tilde{\tau}} \in \{0, 1, 2\}$ for $\tilde{\tau} \in \Sigma_{E,\infty}$ by the following rules:

$$s_{\tilde{\tau}} = \begin{cases} 0 & \text{if } \tilde{\tau} \in \tilde{\mathtt{S}}_\infty, \\ 2 & \text{if } \tilde{\tau}^c \in \tilde{\mathtt{S}}_\infty, \\ 1 & \text{otherwise.} \end{cases}$$

Our assumption on $\tilde{\mathtt{S}}_\infty$ implies that, for every prime $\mathfrak{q}$ of E above p, the set $\{\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{q}} \mid s_{\tilde{\tau}} = 0\}$ has the same cardinality as $\{\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{q}} \mid s_{\tilde{\tau}} = 2\}$.

Put $\tilde{\mathtt{S}} := (\mathtt{S}, \tilde{\mathtt{S}}_\infty)$ and $T_E := \operatorname{Res}_{E/\mathbb{Q}}(\mathbb{G}_m)$. Consider the Deligne homomorphism

$$\begin{aligned} h_{E,\tilde{\mathtt{S}},\mathtt{T}} \colon \mathbb{S}(\mathbb{R}) = \mathbb{C}^\times \to T_E(\mathbb{R}) = \prod_{\tau \in \Sigma_\infty} (E \otimes_{F,\tau} \mathbb{R})^\times \cong (\mathbb{C}^\times)^{\mathtt{S}_\infty - \mathtt{T}} \times (\mathbb{C}^\times)^{\mathtt{T}} \times (\mathbb{C}^\times)^{\mathtt{S}^c_\infty} \\ z = x + \sqrt{-1}y \mapsto ((\bar{z}, \dots, \bar{z}), (z^{-1}, \dots, z^{-1}), (1, \dots, 1)). \end{aligned}$$

where, for each $\tau \in \mathtt{S}_\infty$, we identify $E \otimes_{\tau,F} \mathbb{R}$ with $\mathbb{C}$ via the embedding $\tilde{\tau} \colon E \hookrightarrow \mathbb{C}$ with $\tilde{\tau} \in \tilde{\mathtt{S}}_\infty$ lifting τ. We write $T_{E,\tilde{\mathtt{S}},\mathtt{T}} = (T_E, h_{E,\tilde{\mathtt{S}},\mathtt{T}})$ and put $K_{E,p} := (\mathcal{O}_E \otimes \mathbb{Z}_p)^\times \subseteq T_E(\mathbb{Q}_p)$, the unique maximal open compact subgroup of $T_E(\mathbb{Q}_p)$. For each open compact subgroup $K_E^p \subseteq T_E(\mathbb{A}^{\infty,p})$, we have the zero-dimensional Shimura variety $\operatorname{Sh}(T_{E,\mathtt{S},\mathtt{T}}, K_E)$ whose $\mathbb{Q}^{\mathrm{ac}}$-points are given by

$$\operatorname{Sh}(T_{E,\tilde{\mathtt{S}},\mathtt{T}}, K_E)(\mathbb{Q}^{\mathrm{ac}}) = E^\times \backslash T_E(\mathbb{A}^\infty)/K_E^p K_{E,p}.$$

2C. *Unitary Shimura varieties.* Put $T_F := \operatorname{Res}_{F/\mathbb{Q}}(\mathbb{G}_{m,F})$. Then the reduced norm on $B_\mathtt{S}$ induces a morphism of $\mathbb{Q}$-algebraic groups

$$\nu_\mathtt{S} \colon G_\mathtt{S} \to T_F.$$

Note that the center of $G_\mathtt{S}$ is isomorphic to T_F. Let $G''_{\tilde{\mathtt{S}},\mathtt{T}}$ denote the quotient of $G_\mathtt{S} \times T_E$ by T_F via the embedding

$$T_F \hookrightarrow G_\mathtt{S} \times T_E, \quad z \mapsto (z, z^{-1}),$$

and let $G'_{\tilde{\mathtt{S}}}$ be the inverse image of $\mathbb{G}_m \subseteq T_F$ under the norm map

$$\operatorname{Nm} \colon G''_{\tilde{\mathtt{S}}} = (G_\mathtt{S} \times T_E)/T_F \to T_F, \quad (g, t) \mapsto \nu_\mathtt{S}(g) \operatorname{Nm}_{E/F}(t).$$

Here, the subscript $\tilde{\mathtt{S}}$ is to emphasize that we will take the Deligne homomorphism $h''_{\tilde{\mathtt{S}}}\colon \mathbb{C}^\times \to G''_{\tilde{\mathtt{S}}}(\mathbb{R})$ induced by $h_{\mathtt{S},\mathtt{T}} \times h_{E,\tilde{\mathtt{S}},\mathtt{T}}$, which is independent of $\mathtt{T}$. Note that the image of $h''_{\tilde{\mathtt{S}}}$ lies in $G'_{\tilde{\mathtt{S}}}(\mathbb{R})$, and we denote by $h'_{\tilde{\mathtt{S}}}\colon \mathbb{C}^\times \to G'_{\tilde{\mathtt{S}}}(\mathbb{R})$ the induced map.

As for the quaternionic case, we fix the level at p of the Shimura varieties for $G''_{\tilde{\mathtt{S}}}$ and $G'_{\tilde{\mathtt{S}}}$ as follows. Let $K''_p \subseteq G''_{\tilde{\mathtt{S}}}(\mathbb{Q}_p)$ be the image of $K_p \times K_{E,p}$, and put $K'_p := K''_p \cap G'_{\tilde{\mathtt{S}}}(\mathbb{Q}_p)$. Note that K''_p (resp. K'_p) is not a maximal open compact subgroup of $G''_{\tilde{\mathtt{S}}}(\mathbb{Q}_p)$ (resp. $G'_{\tilde{\mathtt{S}}}(\mathbb{Q}_p)$), if $\mathtt{S}$ contains some p-adic place $\mathfrak{p} \in \Sigma_p$. For sufficiently small open compact subgroups $K''^p \subseteq G''_{\tilde{\mathtt{S}}}(\mathbb{A}^{\infty,p})$ and $K'^p \subseteq G'_{\tilde{\mathtt{S}}}(\mathbb{A}^{\infty,p})$, we get Shimura varieties with $\mathbb{C}$-points given by

$$\mathrm{Sh}(G''_{\tilde{\mathtt{S}}}, K''^p)(\mathbb{C}) = G''_{\tilde{\mathtt{S}}}(\mathbb{Q})\backslash(\mathfrak{H}^\pm)^{\Sigma_\infty - \mathtt{S}_\infty} \times G''_{\tilde{\mathtt{S}}}(\mathbb{A}^\infty)/K''^p K''_p,$$
$$\mathrm{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)(\mathbb{C}) = G'_{\tilde{\mathtt{S}}}(\mathbb{Q})\backslash(\mathfrak{H}^\pm)^{\Sigma_\infty - \mathtt{S}_\infty} \times G'_{\tilde{\mathtt{S}}}(\mathbb{A}^\infty)/K'^p K'_p.$$

We put

$$\mathrm{Sh}(G''_{\tilde{\mathtt{S}}}) := \varprojlim_{K''^p} \mathrm{Sh}(G''_{\tilde{\mathtt{S}}}, K''^p), \quad \mathrm{Sh}(G'_{\tilde{\mathtt{S}}}) = \varprojlim_{K'^p} \mathrm{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p).$$

The common reflex field $E_{\tilde{\mathtt{S}}}$ of $\mathrm{Sh}(G'_{\tilde{\mathtt{S}}})$ and $\mathrm{Sh}(G''_{\tilde{\mathtt{S}}})$ is a subfield of the Galois closure of E in $\mathbb{C}$. The isomorphism $\iota_p\colon \mathbb{C} \xrightarrow{\sim} \mathbb{Q}_p^{\mathrm{ac}}$ defines a p-adic embedding of $E_{\tilde{\mathtt{S}}} \hookrightarrow \mathbb{Q}_p^{\mathrm{ac}}$, hence a p-adic place $\tilde{\wp}$ of $E_{\tilde{\mathtt{S}}}$. Then $E_{\tilde{\mathtt{S}}}$ is unramified at $\tilde{\wp}$. Let $\mathrm{Sh}(G''_{\tilde{\mathtt{S}}})^\circ$ (resp. $\mathrm{Sh}(G'_{\tilde{\mathtt{S}}})^\circ$) denote the neutral geometric connected component of $\mathrm{Sh}(G''_{\tilde{\mathtt{S}}}) \otimes_{E_{\tilde{\mathtt{S}}}} \mathbb{Q}^{\mathrm{ac}}$ (resp. $\mathrm{Sh}(G'_{\tilde{\mathtt{S}}}) \otimes_{E_{\tilde{\mathtt{S}}}} \mathbb{Q}^{\mathrm{ac}}$). Then both $\mathrm{Sh}(G''_{\tilde{\mathtt{S}}})^\circ \otimes_{\mathbb{Q}^{\mathrm{ac}},\iota_p} \mathbb{Q}_p^{\mathrm{ac}}$ and $\mathrm{Sh}(G'_{\tilde{\mathtt{S}}})^\circ \otimes_{\mathbb{Q}^{\mathrm{ac}},\iota_p} \mathbb{Q}_p^{\mathrm{ac}}$ can be descended to $\mathbb{Q}_p^{\mathrm{ur}}$.

In summary, we have a diagram of morphisms of algebraic groups

$$G_{\mathtt{S}} \leftarrow G_{\mathtt{S}} \times T_E \to G''_{\tilde{\mathtt{S}}} = (G_{\mathtt{S}} \times T_E)/T_F \leftarrow G'_{\tilde{\mathtt{S}}}$$

compatible with Deligne homomorphisms, such that the induced morphisms on the derived and adjoint groups are isomorphisms. By Deligne's theory of connected Shimura varieties (see [Tian and Xiao 2016, Corollary 2.17]), such a diagram induces canonical isomorphisms between the neutral geometric connected components of the associated Shimura varieties:

$$\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}})^\circ \xleftarrow{\sim} \mathrm{Sh}(G''_{\tilde{\mathtt{S}}})^\circ \xrightarrow{\sim} \mathrm{Sh}(G'_{\tilde{\mathtt{S}}})^\circ. \tag{2-2}$$

Since a Shimura variety can be recovered from its neutral connected component together with its Hecke and Galois actions, one can transfer integral models of $\mathrm{Sh}(G'_{\tilde{\mathtt{S}}})$ to integral models of $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}})$ (see [Tian and Xiao 2016, Corollary 2.17]).

2D. ***Moduli interpretation for unitary Shimura varieties.*** Note that $\mathrm{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)$ is a Shimura variety of PEL-type. To simplify notation, let $\mathcal{O}_{\tilde{\wp}}$ be the ring of integers of the completion of $E_{\tilde{\mathtt{S}}}$ at $\tilde{\wp}$. We recall the integral model of $\mathrm{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)$ over $\mathcal{O}_{\tilde{\wp}}$ defined in [Tian and Xiao 2016] as follows.

Let $K'^p \subseteq G'_{\tilde{\mathtt{S}}}(\mathbb{A}^{\infty,p})$ be an open compact subgroup such that $K'^p K'_p$ is neat (for PEL-type Shimura data). We put $D_{\mathtt{S}} := B_{\mathtt{S}} \otimes_F E$, which is isomorphic to $\mathrm{Mat}_2(E)$ by assumption on E. Denote by $b \mapsto \bar{b}$ the involution on $D_{\mathtt{S}}$ given by the product of the canonical involution on $B_{\mathtt{S}}$ and the complex conjugation on E/F. Write $E = F(\sqrt{\mathfrak{d}})$ for some totally negative element $\mathfrak{d} \in F$ that is a $\mathfrak{p}$-adic unit for every $\mathfrak{p} \in \Sigma_p$.

We choose also an element $\delta \in D_{\mathtt{S}}^{\times}$ such that $\bar{\delta} = \delta$ as in [Tian and Xiao 2016, Lemma 3.8]. Then the conjugation by δ^{-1} defines a new involution $b \mapsto b^* = \delta^{-1}\bar{b}\delta$. Consider $W = D_{\mathtt{S}}$ as a free left $D_{\mathtt{S}}$-module of rank 1, equipped with an $*$-hermitian alternating pairing

$$\psi\colon W \times W \to \mathbb{Q}, \quad \psi(x, y) = \mathrm{Tr}_{E/\mathbb{Q}}(\mathrm{Tr}^{\circ}_{D_{\mathtt{S}}/E}(\sqrt{\mathfrak{d}}x\bar{y}\delta)), \tag{2-3}$$

where $\mathrm{Tr}^{\circ}_{D_{\mathtt{S}}/E}$ denotes the reduced trace of $D_{\mathtt{S}}/E$. Then $G'_{\tilde{\mathtt{S}}}$ can be identified with the unitary similitude group of (W, ψ).

We choose an order $\mathcal{O}_{D_{\mathtt{S}}} \subseteq D_{\mathtt{S}}$ that is stable under $*$ and maximal at p, and an $\mathcal{O}_{D_{\mathtt{S}}}$-lattice $L \subseteq W$ such that $\psi(L, L) \subseteq \mathbb{Z}$ and $L \otimes \mathbb{Z}_p$ is self-dual under ψ. Assume that K'^p is a sufficiently small open compact subgroup of $G'_{\tilde{\mathtt{S}}}(\mathbb{A}^{\infty,p})$ which stabilizes $L \otimes \hat{\mathbb{Z}}^{(p)}$.

Consider the moduli problem $\underline{\mathbf{Sh}}(G'_{\tilde{\mathtt{S}}}, K'^p)$ that associates to each locally noetherian $\mathcal{O}_{\tilde{\wp}}$-scheme S the set of isomorphism classes of tuples $(A, \iota, \lambda, \bar{\alpha}_{K'^p})$, where:

- A is an abelian scheme over S of dimension $4[F : \mathbb{Q}]$.
- $\iota\colon \mathcal{O}_{D_{\mathtt{S}}} \hookrightarrow \mathrm{End}_S(A)$ is an embedding such that the induced action of $\iota(b)$ for $b \in \mathcal{O}_E$ on $\mathrm{Lie}(A/S)$ has characteristic polynomial
$$\det(T - \iota(b) | \,\mathrm{Lie}(A/S)) = \prod_{\tilde{\tau} \in \Sigma_{E,\infty}} (x - \tilde{\tau}(b))^{2s_{\tilde{\tau}}}.$$
- $\lambda\colon A \to A^{\vee}$ is a polarization of A such that
  - the Rosati involution defined by λ on $\mathrm{End}_S(A)$ induces the involution $b \mapsto b^*$ on $\mathcal{O}_{D_{\mathtt{S}}}$,
  - if $\mathfrak{p} \notin \mathtt{S}$, λ induces an isomorphism of p-divisible groups $A[\mathfrak{p}^{\infty}] \xrightarrow{\sim} A^{\vee}[\mathfrak{p}^{\infty}]$, and
  - if $\mathfrak{p} \in \mathtt{S}$, then $(\ker \lambda)[\mathfrak{p}^{\infty}]$ is a finite flat group scheme contained in $A[\mathfrak{p}]$ of rank $p^{4g_{\mathfrak{p}}}$ and the cokernel of induced morphism $\lambda_*\colon \mathrm{H}_1^{\mathrm{dR}}(A/S) \to \mathrm{H}_1^{\mathrm{dR}}(A^{\vee}/S)$ is a locally free module of rank two over $\mathcal{O}_S \otimes_{\mathbb{Z}_p} \mathcal{O}_E/\mathfrak{p}$. Here, $\mathrm{H}_1^{\mathrm{dR}}(-/S)$ denotes the relative de Rham homology.
- $\bar{\alpha}_{K'^p}$ is a K'^p level structure on A, that is, a K'^p-orbit of $\mathcal{O}_{D_{\mathtt{S}}}$-linear isomorphisms of étale sheaves $\alpha\colon L \otimes \hat{\mathbb{Z}}^{(p)} \xrightarrow{\sim} \hat{T}^p(A)$ such that the alternating pairing $\psi\colon L \otimes \hat{\mathbb{Z}}^{(p)} \times L \otimes \hat{\mathbb{Z}}^{(p)} \to \hat{\mathbb{Z}}^{(p)}$ is compatible with the λ-Weil pairing on $\hat{T}^p(A)$ via some isomorphism $\hat{\mathbb{Z}}^{(p)} \cong \hat{\mathbb{Z}}^{(p)}(1)$. Here, $\hat{T}^p(A) = \prod_{l \neq p} T_l(A)$ denotes the product of prime-to-p Tate modules.

Remark 2.3. Sometimes it is convenient to formulate the moduli problem $\underline{\mathbf{Sh}}(G'_{\tilde{\mathtt{S}}}, K'^p)$ in terms of isogeny classes of abelian varieties: one associates to each locally noetherian $\mathcal{O}_{\tilde{\wp}}$-scheme S the equivalence classes of tuples $(A, \iota, \lambda, \bar{\alpha}^{\mathrm{rat}}_{K'^p})$, where

- (A, ι) is an abelian scheme *up to prime-to-p isogeny* of dimension $4[F : \mathbb{Q}]$ equipped with an action $\mathcal{O}_{D_{\mathtt{S}}}$ satisfying the determinant conditions as above;
- λ is a polarization on A satisfying the condition as above;

- $\bar{\alpha}^{\mathrm{rat}}_{K'^p}$ is a rational K'^p-level structure on A, that is, a K'^p-orbit of $\mathcal{O}_{D_{\mathtt{S}}} \otimes \mathbb{A}^{\infty,p}$-linear isomorphisms of étale sheaves on S:

$$\alpha\colon W \otimes_{\mathbb{Q}} \mathbb{A}^{\infty,p} \xrightarrow{\sim} \hat{V}^p(A) := \hat{T}^p(A) \otimes \mathbb{Q}$$

such that the pairing ψ on $W \otimes_{\mathbb{Q}} \mathbb{A}^{\infty,p}$ is compatible with the λ-Weil pairing on $\hat{V}^p(A)$ *up to a scalar in* $\mathbb{A}^{\infty,p,\times}$.

For the equivalence of these two definitions, see [Lan 2013].

Theorem 2.4. *The moduli problem* $\underline{\mathbf{Sh}}(G'_{\tilde{\mathtt{S}}}, K'^p)$ *is representable by a quasiprojective and smooth scheme* $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)$ *over* $\mathcal{O}_{\tilde{\wp}}$ *such that*

$$\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p) \otimes_{\mathcal{O}_{\tilde{\wp}}} E_{\tilde{\mathtt{S}},\tilde{\wp}} \cong \mathrm{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p) \otimes_{E_{\tilde{\mathtt{S}}}} E_{\tilde{\mathtt{S}},\tilde{\wp}}.$$

Moreover, the projective limit $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}) := \varprojlim_{K'^p} \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)$ *is an integral canonical model of* $\mathrm{Sh}(G'_{\tilde{\mathtt{S}}})$ *over* $\mathcal{O}_{\tilde{\wp}}$ *in the sense that* $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}})$ *satisfies the following extension property over* $\mathcal{O}_{\tilde{\wp}}$*: if* S *is a smooth scheme over* $\mathcal{O}_{\tilde{\wp}}$*, any morphism* $S \otimes_{\mathcal{O}_{\tilde{\wp}}} E_{\tilde{\mathtt{S}},\tilde{\wp}} \to \mathbf{Sh}(G'_{\tilde{\mathtt{S}}})$ *extends uniquely to a morphism* $S \to \mathbf{Sh}(G'_{\tilde{\mathtt{S}}})$.

Proof. This follows from [Tian and Xiao 2016, 3.14, 3.19]. □

Let $\mathbb{Z}_p^{\mathrm{ur}}$ be the ring of integers of $\mathbb{Q}_p^{\mathrm{ur}}$. The closure of $\mathrm{Sh}(G'_{\tilde{\mathtt{S}}})^\circ$ in $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}) \otimes_{\mathcal{O}_{\tilde{\wp}}} \mathbb{Z}_p^{\mathrm{ur}}$, denote by $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}})^\circ_{\mathbb{Z}_p^{\mathrm{ur}}}$, is a smooth integral canonical model of $\mathrm{Sh}(G'_{\tilde{\mathtt{S}}})^\circ$ over $\mathbb{Z}_p^{\mathrm{ur}}$. By (2-2), this can also be regarded as an integral canonical model of $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}})^\circ$ over $\mathbb{Z}_p^{\mathrm{ur}}$. This induces a smooth integral canonical model $\mathbf{Sh}(G_{\mathtt{S},\mathtt{T}})$ of $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}})$ over $\mathcal{O}_{F_{\mathtt{S},\mathtt{T}},\wp}$ by Deligne's recipe (see [Tian and Xiao 2016, Corollary 2.17]). For any open compact subgroup $K^p \subseteq G_{\mathtt{S}}(\mathbb{A}^{\infty,p})$, we define $\mathbf{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)$ as the quotient of $\mathbf{Sh}(G_{\mathtt{S},\mathtt{T}})$ by K^p. If K^p is sufficiently small, then $\mathbf{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)$ is a quasiprojective smooth scheme over $\mathcal{O}_{F_{\mathtt{S},\mathtt{T}},\wp}$, and it is an integral model for $\mathrm{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)$.

2E. ***Moduli interpretation for totally indefinite quaternionic Shimura varieties.*** When $\mathtt{S} = \varnothing$, then $\mathtt{T} = \varnothing$ and the Shimura variety $\mathrm{Sh}(G, K^p) := \mathrm{Sh}(G_{\varnothing,\varnothing}, K^p)$ has another moduli interpretation in terms of abelian varieties with real multiplication by $\mathcal{O}_B$. Using this moduli interpretation, one can also construct another integral model of $\mathrm{Sh}(G, K^p)$. The aim of this part is to compare this integral canonical model of $\mathrm{Sh}(G, K^p)$ with $\mathbf{Sh}(G, K^p)$ constructed in the previous subsection using unitary Shimura varieties.

We choose an element $\gamma \in B^\times$ such that

- $\bar{\gamma} = -\gamma$;
- $b \mapsto b^* := \gamma^{-1}\bar{b}\gamma$ is a positive involution;
- $\nu(\gamma)$ is a $\mathfrak{p}$-adic unit for every p-adic place $\mathfrak{p}$ of F, where $\nu\colon B^\times \to F^\times$ is the reduced norm map.

Put $V := B$ viewed as a free left B-module of rank 1, and consider the alternating pairing

$$\langle\,\cdot\,,\,\cdot\,\rangle_F\colon V \times V \to F, \quad \langle x, y\rangle_F = \mathrm{Tr}^\circ_{B/F}(x\bar{y}\gamma),$$

where $\mathrm{Tr}^{\circ}_{B/F}$ is the reduced trace of B. Note that $\langle bx, y\rangle_F = \langle x, b^*y\rangle_F$ for $x, y \in V$ and $b \in B$. We let $G = B^{\times}$ act on V via $g \cdot v = vg^{-1}$ for $g \in G$ and $v \in V$. One has an isomorphism

$$G \cong \mathrm{Aut}_B(V).$$

Fix an order $\mathcal{O}_B \subseteq B$ such that

- $\mathcal{O}_B$ contains $\mathcal{O}_F$, and it is stable under $*$;
- $\mathcal{O}_B \otimes \mathbb{Z}_p$ is a maximal order of $B \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathrm{GL}_2(F \otimes_{\mathbb{Q}} \mathbb{Q}_p)$.

Let $K^p \subseteq G(\mathbb{A}^{\infty,p})$ be an open compact subgroup. Consider the moduli problem $\underline{\mathbf{Sh}}(G, K^p)$ that associates to every $\mathbb{Z}_{(p)}$-scheme T the equivalence classes of tuples $(A, \iota, \bar{\lambda}, \bar{\alpha}_{K^p})$ where

- A is a projective abelian scheme over T up to prime-to-p isogeny;
- ι is a real multiplication by $\mathcal{O}_B$ on A, that is, a ring homomorphism $\iota\colon \mathcal{O}_B \to \mathrm{End}(A)$ satisfying

$$\det(T - \iota(b) | \operatorname{Lie}(A)) = \mathrm{N}_{F/\mathbb{Q}}(\mathrm{N}^{\circ}_{B/F}(T - b)), \quad b \in \mathcal{O}_B,$$

  where $\mathrm{N}^{\circ}_{B/F}$ is the reduced norm of B/F;
- $\bar{\lambda}$ is an $F_+^{p,\times}$-orbit of $\mathcal{O}_F$-linear prime-to-p polarizations $\lambda\colon A \to A^{\vee}$ such that $\iota(b)^{\vee} \circ \lambda = \lambda \circ \iota(b^*)$ for all $b \in \mathcal{O}_B$, where $F_+^{p,\times} \subseteq F^{\times}$ is the subgroup of totally positive elements that are $\mathfrak{p}$-adic units for all $\mathfrak{p} \in \Sigma_p$;
- $\bar{\alpha}_{K^p}$ is a K^p-level structure on (A, ι), that is, $\bar{\alpha}_{K^p}$ is a K^p-orbit of $B \otimes_{\mathbb{Q}} \mathbb{A}^{\infty,p}$-linear isomorphisms of étale sheaves on T:

$$\alpha\colon V \otimes_{\mathbb{Q}} \mathbb{A}^{\infty,p} \xrightarrow{\sim} \hat{V}^p(A).$$

Remark 2.5. By [Zink 1982, Lemma 3.8], there exists exactly one $F_+^{p,\times}$ orbit of prime-to-p polarizations on A that induces the given positive involution $*$ on B. Hence, one may omit $\bar{\lambda}$ from the definition of the moduli problem $\underline{\mathbf{Sh}}(G, K^p)$. This is the point of view in [Liu 2019]. Here, we choose to keep $\bar{\lambda}$ in order to compare it with unitary Shimura varieties.

By [Zink 1982, page 27], one has a bijection

$$\underline{\mathbf{Sh}}(G, K^p)(\mathbb{C}) \cong G(\mathbb{Q})\backslash(\mathfrak{H}^{\pm})^{\Sigma_\infty} \times G(\mathbb{A}^{\infty})/K^pK_p = \mathrm{Sh}(G, K^p)(\mathbb{C}).$$

Note that an object $(A, \iota, \bar{\lambda}, \bar{\alpha}_{K^p}) \in \underline{\mathbf{Sh}}(G, K^p)(T)$ admits automorphisms $\mathcal{O}_F^{\times} \cap K^p$, which is always nontrivial if $F \neq \mathbb{Q}$. Here, $\mathcal{O}_F^{\times}$ is considered as a subgroup of $G(\mathbb{A}^{\infty,p})$ via the diagonal embedding. Thus, the moduli problem $\underline{\mathbf{Sh}}(G, K^p)$ can not be representable. However, Zink shows [1982, Satz 1.7] that $\underline{\mathbf{Sh}}(G, K^p)$ admits a coarse moduli space $\mathbf{Sh}(G, K^p)$, which is a projective scheme over $\mathbb{Z}_{(p)}$. This gives an integral model of the Shimura variety $\mathrm{Sh}(G, K^p)$ over $\mathbb{Z}_{(p)}$.

We recall briefly Zink's construction of $\mathbf{Sh}(G, K^p)$. Take $(A, \iota, \bar{\lambda}, \bar{\alpha}_{K^p}) \in \underline{\mathbf{Sh}}(G, K^p)(T)$ for some $\mathbb{Z}_{(p)}$-scheme T. Choose a polarization $\lambda \in \bar{\lambda}$, and an isomorphism $\alpha \in \bar{\alpha}_{K^p}$. Then λ induces a Weil pairing

$$\hat{\Psi}^{\lambda}\colon \hat{V}^p(A) \times \hat{V}^p(A) \to \mathbb{A}^{\infty,p}(1),$$

and there exists a unique F-linear alternating pairing

$$\hat{\Psi}^{\lambda}_{F}\colon \hat{V}^{p}(A)\times\hat{V}^{p}(A)\to\mathbb{A}^{\infty,p}_{F}(1)$$

such that $\hat{\Psi}^{\lambda}=\mathrm{Tr}_{F/\mathbb{Q}}\circ\hat{\Psi}^{\lambda}_{F}$. We fix an isomorphism $\mathbb{Z}\cong\mathbb{Z}(1)$, and view $\langle\cdot\,,\cdot\rangle$ as a pairing with values in $F(1)$. Then by [Zink 1982, 1.2], there exists an element $c\in\mathbb{A}^{\infty,p,\times}_{F}$ such that

$$\hat{\Psi}^{\lambda}_{F}(\alpha(x),\alpha(y))=c\langle x,y\rangle_{F},\quad x,y\in V\otimes_{\mathbb{Q}}\mathbb{A}^{\infty,p}.$$

The class of c in $\mathbb{A}^{\infty,p,\times}_{F}/\nu(K^{p})$, denoted by $c(A,\iota,\lambda,\bar{\alpha}_{K^{p}})$, is independent of the choice of $\alpha\in\bar{\alpha}_{K^{p}}$. If $F^{\times}_{+}\subseteq F^{\times}$ is the subgroup of totally positive elements, then the image of $c(A,\iota,\lambda,\bar{\alpha}_{K^{p}})$ in

$$\mathbb{A}^{\infty,p,\times}_{F}/F^{p,\times}_{+}\nu(K^{p})\cong\mathbb{A}^{\infty,\times}_{F}/F^{\times}_{+}\nu(K)$$

is independent of the choices of both λ and α.

We choose representatives $c_{1},\dots,c_{r}\in\mathbb{A}^{\infty,p,\times}_{F}/\nu(K^{p})$ of the finite quotient $\mathbb{A}^{\infty,p,\times}_{F}/F^{p,\times}_{+}\nu(K^{p})$, and consider the moduli problem $\underline{\widetilde{\mathbf{Sh}}}(G,K^{p})$ that associates to every $\mathbb{Z}_{p}$-scheme T equivalence classes of tuple $(A,\iota,\lambda,\bar{\alpha}_{K^{p}})$, where

- (A,ι) is an abelian scheme over T up to prime-to-p isogeny equipped with real multiplication by $\mathcal{O}_{B}$;
- $\lambda\colon A\to A^{\vee}$ is a prime-to-p polarization such that $\iota(b)^{\vee}\circ\lambda=\lambda\circ\iota(b^{*})$ for all $b\in\mathcal{O}_{B}$;
- $\bar{\alpha}_{K^{p}}$ is a K^{p}-level structure on A such that $c(A,\iota,\lambda,\bar{\alpha}_{K^{p}})=c_{i}$ for some $i=1,\dots,r$.

To study the representability of $\underline{\widetilde{\mathbf{Sh}}}(G,K^{p})$, we need the following notion of neat subgroups.

Definition 2.6. Let $\mathtt{R}$ be the ramification set of B. For every $g_{v}\in(B\otimes_{F}F_{v})^{\times}$ with $v\notin\mathtt{R}$, let $\Gamma_{g_{v}}$ denote the subgroup of $F^{\mathrm{ac},\times}_{v}$ generated by the eigenvalues of g_{v}. Choose an embedding $\mathbb{Q}^{\mathrm{ac}}\hookrightarrow F^{\mathrm{ac}}_{v}$. Then $(\Gamma_{g_{v}}\cap\mathbb{Q}^{\mathrm{ac}})^{\mathrm{tor}}$ is the subgroup of $\Gamma_{g_{v}}$ consisting of roots of unity, and it is independent of the embedding $\mathbb{Q}^{\mathrm{ac}}\hookrightarrow F^{\mathrm{ac}}_{v}$.

Let $\square$ be a finite set of places of $\mathbb{Q}$ containing the archimedean place, and let $\square_{F}$ be the set of places of F above $\square$. An element $g\in G(\mathbb{A}^{\square})=(B\otimes_{\mathbb{Q}}\mathbb{A}^{\square})^{\times}$ is called *neat* if $\bigcap_{v\in\square_{F}-\mathtt{R}}(\Gamma_{g_{v}}\cap\mathbb{Q}^{\mathrm{ac}})^{\mathrm{tor}}=\{1\}$. We say a subgroup $U\subseteq G(\mathbb{A}^{\square})$ is *neat* if every element $g=g^{\mathtt{R}}g_{\mathtt{R}}\in U$ with $\nu(g^{\mathtt{R}})=1$ is neat. Here, $g^{\mathtt{R}}\in(B\otimes_{F}\mathbb{A}^{\square_{F}\cup\mathtt{R}}_{F})^{\times}$ (resp. $g_{\mathtt{R}}\in\prod_{v\in\mathtt{R}-\square_{F}}(B\otimes_{F}F_{v})^{\times}$) is the prime-to-$\mathtt{R}$ component (resp. $\mathtt{R}$-component) of g.

Assume from now on that $K^{p}\subseteq G(\mathbb{A}^{\infty,p})$ is neat. It is easy to see that each object of $\underline{\widetilde{\mathbf{Sh}}}(G,K^{p})$ has no nontrivial automorphisms. By a well-known result of Mumford, $\underline{\widetilde{\mathbf{Sh}}}(G,K^{p})$ is representable by a quasiprojective smooth scheme $\widetilde{\mathbf{Sh}}(G,K^{p})$ over $\mathbb{Z}_{(p)}$. If B is a division algebra, then $\widetilde{\mathbf{Sh}}(G,K^{p})$ is even projective over $\mathbb{Z}_{(p)}$ (see [Zink 1982, Lemma 1.8]).

Let $\mathcal{O}^{\times}_{F,+}$ be the group of totally positive units of F. There is a natural action by $\mathcal{O}^{\times}_{F,+}\cap\nu(K^{p})$ on $\widetilde{\mathbf{Sh}}(G,K^{p})$ given by $\xi\cdot(A,\iota,\lambda,\bar{\alpha}_{K^{p}})=(A,\iota,\xi\cdot\lambda,\bar{\alpha}_{K^{p}})$ for $\xi\in\mathcal{O}^{\times}_{F,+}$, and the quotient is the moduli problem $\underline{\mathbf{Sh}}(G,K^{p})$. Note that the subgroup $(\mathcal{O}^{\times}_{F}\cap K^{p})^{2}$ acts trivially on $\widetilde{\mathbf{Sh}}(G,K^{p})$. Here, $\mathcal{O}^{\times}_{F}$ is considered as a subgroup in the center of $G(\mathbb{A}^{\infty,p})$. Indeed, if $\xi = \eta^2$ with $\eta \in \mathcal{O}_F^\times \cap K^p$, then the multiplication by η on A defines an isomorphism $(A, \iota, \lambda, \bar{\alpha}_{K^p}) \xrightarrow{\sim} (A, \iota, \xi \cdot \lambda, \bar{\alpha}_{K^p})$. Put

$$\Delta_{K^p} := (\mathcal{O}_{F,+}^\times \cap \nu(K^p))/(\mathcal{O}_F^\times \cap K^p)^2.$$

Proposition 2.7. *Assume that K^p is neat. Let $(A, \iota, \bar{\lambda}, \bar{\alpha}_{K^p})$ be a T-valued point of $\underline{\mathbf{Sh}}(G, K^p)$. Then the group of automorphisms of $(A, \iota, \bar{\lambda}, \bar{\alpha}_{K^p})$ is $\mathcal{O}_F^\times \cap K^p$. Here, $\mathcal{O}_F^\times$ is viewed as a subgroup of $G(\mathbb{A}^{\infty,p})$ via the diagonal embedding.*

Proof. This is a slight generalization of [Zink 1982, Korollar 3.3]. Take $\eta \in \mathrm{End}_{\mathcal{O}_B}(A)_{\mathbb{Q}}$ that preserves $\bar{\lambda}$ and $\bar{\alpha}_{K^p}$. Then there exists $\xi \in F_+{}^\times$ such that $\eta\hat{\eta} = \xi$, where $\hat{\eta}$ is the Rosati involution of η induced by $\bar{\lambda}$. By [Zink 1982, Satz 3.2], it is enough to show that $\hat{\eta} = \eta$. Choose $\alpha \in \bar{\alpha}_{K^p}$, which induces an embedding

$$(\mathrm{End}_{\mathcal{O}_B}(A) \otimes \mathbb{Q})^\times \to (\mathrm{End}_B(V) \otimes_{\mathbb{Q}} \mathbb{A}^{\infty,p})^\times \cong G(\mathbb{A}^{\infty,p}).$$

Then the image of η under this embedding lies in K^p. Consider the endomorphism $\eta^2\xi^{-1} \in \mathrm{End}_{\mathcal{O}_B}(A) \otimes \mathbb{Q}$. Its image in $G(\mathbb{A}^{\infty,p})$ lies in K^p and has reduced norm equal to 1. Since K^p is neat, all the eigenvalues of $\eta^2\xi^{-1}$ are 1. So $\eta^2\xi^{-1}$ must be trivial, hence $\eta = \hat{\eta}$. □

Corollary 2.8. *Assume that K^p is neat. Then the action of Δ_{K^p} on $\widetilde{\mathbf{Sh}}(G, K^p)$ is free.*

Proof. The same argument for [Zink 1982, Korollar 3.4] shows that it follows from the above proposition. □

We put

$$\mathbf{Sh}(G, K^p) := \widetilde{\mathbf{Sh}}(G, K^p)/\Delta_{K^p}, \tag{2-4}$$

which exists as a quasiprojective smooth scheme over $\mathbb{Z}_{(p)}$ by [SGA 1 2003, Exposé VIII, Corollaire 7.7]. Then $\mathbf{Sh}(G, K^p)$ is the coarse moduli space of the moduli problem $\underline{\mathbf{Sh}}(G, K^p)$, and $\widetilde{\mathbf{Sh}}(G, K^p)$ is a finite étale cover of $\mathbf{Sh}(G, K^p)$ with Galois group Δ_{K^p}. For each $i = 1, \dots, r$, we denote by $\widetilde{\mathbf{Sh}}^{c_i}(G, K^p)$ the subscheme of $\widetilde{\mathbf{Sh}}(G, K^p)$ consisting the tuples $(A, \iota, \lambda, \bar{\alpha}_{K^p})$ with $c(A, \iota, \lambda, \bar{\alpha}_{K^p}) = c_i$. It is clear that each $\widetilde{\mathbf{Sh}}^{c_i}(G, K^p)$ is stable under the action of Δ_{K^p}. Let $\mathbf{Sh}^{c_i}(G, K^p) \subseteq \mathbf{Sh}(G, K^p)$ be the image of $\widetilde{\mathbf{Sh}}^{c_i}(G, K^p)$ under the morphism (2-4). Note that each $\mathbf{Sh}^{c_i}(G, K^p)$ is not necessarily defined over $\mathbb{Z}_{(p)}$. Actually, using the strong approximation theorem, one sees easily that $\mathbf{Sh}^{c_i}(G, K^p)(\mathbb{C})$ is a connected component of $\mathbf{Sh}(G, K^p)(\mathbb{C})$.

Remark 2.9. Assume that K^p is neat:

(1) Let $(\widetilde{\mathcal{A}}, \tilde{\iota})$ be the universal abelian scheme with real multiplication by $\mathcal{O}_B$ over $\widetilde{\mathbf{Sh}}(G, K^p)$. Then $\widetilde{\mathcal{A}}$ is equipped with a natural descent data relative to the projection $\widetilde{\mathbf{Sh}}(G, K^p) \to \mathbf{Sh}(G, K^p)$, since the action of Δ_{K^p} modifies only the polarization. By [SGA 1 2003, Exposé VIII, Corollaire 7.7], the descent data on $\widetilde{\mathcal{A}}$ is effective. This means that, even though $\mathbf{Sh}(G, K^p)$ is not a fine moduli space, there exists still a universal family $\mathcal{A}$ over $\mathbf{Sh}(G, K^p)$. Moreover, by étale descent, $\tilde{\iota}$ descends to a real multiplication ι by $\mathcal{O}_B$ on the universal family $\mathcal{A}$ over $\mathbf{Sh}(G, K^p)$.

(2) In general, Δ_{K^p} is nontrivial. However, for any open compact subgroup $K^p \subseteq G(\mathbb{A}^{\infty,p})$, there exists a smaller open compact subgroup $K'^p \subseteq K^p$ such that $\Delta_{K'^p}$ is trivial.

We give an interpretation of $\widetilde{\mathbf{Sh}}(G, K^p)$ in terms of Shimura varieties. Let $G^\star \subseteq G$ be the preimage of $\mathbb{G}_{m,\mathbb{Q}} \subseteq T_F = \mathrm{Res}_{F/\mathbb{Q}}(\mathbb{G}_{m,F})$ via the reduced norm map $\nu\colon G \to T_F$. The Deligne homomorphism $h_\varnothing\colon \mathbb{S}(\mathbb{R}) = \mathbb{C}^\times \to G(\mathbb{R})$ factors through $G^\star(\mathbb{R})$, hence induces a map

$$h_{G^\star}\colon \mathbb{S}(\mathbb{R}) \to G^\star(\mathbb{R}).$$

We put $K_p^\star := G^\star(\mathbb{Q}_p) \cap K_p$, which will be the fixed level at p for Shimura varieties attached to $G^\star$. For a sufficiently small open compact subgroup $K^{\star p} \subseteq G^\star(\mathbb{A}^{\infty,p})$, we have the associated Shimura variety $\mathrm{Sh}(G^\star, K^{\star p})$ defined over $\mathbb{Q}$, whose $\mathbb{C}$-points are given by

$$\mathrm{Sh}(G^\star, K^{\star p})(\mathbb{C}) = G^\star(\mathbb{Q})\backslash((\mathfrak{H}^\pm)^{\Sigma_\infty} \times G^\star(\mathbb{A}^\infty)/K^{\star p}K_p^\star).$$

Put $\mathrm{Sh}(G^\star) := \varprojlim_{K^{\star p}} \mathrm{Sh}(G^\star, K^{\star p})$ as usual.

There is a natural action of $\mathbb{A}^{\infty,p,\times}$ on $\mathbb{A}_F^{\infty,p,\times}/F_+^{p,\times}\nu(K^p)$ by multiplication. Let $\mathfrak{c}_1, \dots, \mathfrak{c}_h$ denote the equivalence classes modulo $F_+^{p,\times}\mathbb{A}^{\infty,p,\times}$ of the chosen set $\{c_1, \dots, c_r\} \subseteq \mathbb{A}_F^{\infty,p,\times}/\nu(K^p)$. We may and do assume that all the c_i's in one equivalence class differ from each other by elements in $\mathbb{A}^{\infty,p,\times}$. For each $\mathfrak{c} \in \{\mathfrak{c}_1, \dots, \mathfrak{c}_h\}$, we put

$$\widetilde{\mathbf{Sh}}^{\mathfrak{c}}(G, K^p) := \coprod_{c_i \in \mathfrak{c}} \widetilde{\mathbf{Sh}}^{c_i}(G, K^p)$$

and similarly $\mathbf{Sh}^{\mathfrak{c}}(G, K^p) = \coprod_{c_i \in \mathfrak{c}} \mathbf{Sh}^{c_i}(G, K^p)$.

Proposition 2.10. *Suppose that $K^p \subseteq G(\mathbb{A}^{\infty,p})$ is a neat open compact subgroup. For every $\mathfrak{c} \in \{\mathfrak{c}_1, \dots, \mathfrak{c}_h\}$, there exists an element $g^p \in G(\mathbb{A}^{\infty,p})$ such that if $K_{\mathfrak{c}}^{\star,p} := G^\star \cap g^p K^p g^{p,-1}$, then we have an isomorphism of schemes over $\mathbb{Q}$*

$$\widetilde{\mathbf{Sh}}^{\mathfrak{c}}(G, K^p) \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q} \xrightarrow{\sim} \mathrm{Sh}(G^\star, K_{\mathfrak{c}}^{\star,p}).$$

Proof. Let $X \cong (\mathfrak{H}^\pm)^{\Sigma_\infty}$ denote the set of conjugacy classes of $h_{G^\star}\colon \mathbb{S}(\mathbb{R}) \to G^\star(\mathbb{R})$. We fix a base point $(A_0, \iota_0, \lambda_0, \bar{\alpha}_{K^p,0}) \in \widetilde{\mathbf{Sh}}^{\mathfrak{c}}(G, K^p)(\mathbb{C})$. Put $V_{\mathbb{Q}}(A_0) := \mathrm{H}_1(A_0(\mathbb{C}), \mathbb{Q})$. We fix an isomorphism $\eta_0\colon V_{\mathbb{Q}}(A_0) \xrightarrow{\sim} V$ of left B-modules and a choice of $\alpha_0 \in \bar{\alpha}_{K^p}$. Then the composite map

$$(\eta_0 \otimes 1) \circ \alpha_0\colon V \otimes_{\mathbb{Q}} \mathbb{A}^{\infty,p} \to \hat{V}^p(A_0) \cong V_{\mathbb{Q}}(A_0) \otimes_{\mathbb{Q}} \mathbb{A}^{\infty,p} \to V \otimes_{\mathbb{Q}} \mathbb{A}^{\infty,p}$$

defines an element $g^p \in G(\mathbb{A}^{\infty,p})$. Now let $(A, \iota, \lambda, \bar{\alpha}_{K^p}) \in \widetilde{\mathbf{Sh}}^{c_i}(G, K^p)(\mathbb{C})$ be another point. There exists also an isomorphism $\eta\colon V_{\mathbb{Q}}(A) \xrightarrow{\sim} V$ as B-modules, and the Hodge structure on $V_{\mathbb{Q}}(A) \otimes_{\mathbb{Q}} \mathbb{R} = \mathrm{H}_1(A(\mathbb{C}), \mathbb{R})$ defines an element $x_\infty \in X$. By the definition of $\mathbf{Sh}^{\mathfrak{c}}(G, K^p)$, there exists an element $\alpha \in \bar{\alpha}_{K^p}$ such that the isomorphism

$$h^p := (\eta \otimes 1) \circ \alpha \circ \alpha_0^{-1}(\eta_0 \otimes 1)^{-1} \in G(\mathbb{A}^{\infty,p})$$

preserves the alternating pairing $\langle\,\cdot\,,\,\cdot\,\rangle_F$ on $V \otimes_{\mathbb{Q}} \mathbb{A}^{\infty,p}$ up to a scalar in $\mathbb{A}^{\infty,p,\times}$. Such an element α is unique up to right multiplication by elements in K^p, and it follows that h^p is well defined up to right multiplication by elements of $K_{\mathfrak{c}}^{\star,p} := g^p K^p g^{p,-1} \cap G^\star(\mathbb{A}^{\infty,p})$. Viewing h^p as an element of $G^\star(\mathbb{A}^\infty)$ with p-component equal to 1, then $(A, \iota, \lambda, \bar{\alpha}_{K^p}) \mapsto [x_\infty, h^p]$ defines a map

$$f : \widetilde{\mathbf{Sh}}^{\mathfrak{c}}(G, K^p)(\mathbb{C}) \to \mathrm{Sh}(G^\star, K^{\star,p})(\mathbb{C}) \cong G^\star(\mathbb{Q})\backslash(X \times G^\star(\mathbb{A}^\infty)/K_{\mathfrak{c}}^{\star,p} K_p^\star).$$

By the complex uniformization of abelian varieties, it is easy to see that f is bijective, and f descends to an isomorphism of schemes over $\mathbb{Q}$ by the theory of canonical models. □

Remark 2.11. In general, there is no canonical choice for g^p in the above proposition. Different choices of g^p will result in different $K_{\mathfrak{c}}^{\star,p}$, which are conjugate to each other in $G^\star(\mathbb{A}^{\infty,p})$. Consequently, the corresponding $\mathbf{Sh}(G^\star, K_{\mathfrak{c}}^{\star,p})$ are isomorphic to each other by the Hecke action of some elements in $G^\star(\mathbb{A}^{\infty,p})$. However, if $\mathfrak{c} = \mathfrak{c}^{\mathrm{tri}}$ is the trivial equivalence class, g^p has a canonical choice, namely $g^p = 1$. In the sequel, we will always take $g^p = 1$ if $\mathfrak{c} = \mathfrak{c}^{\mathrm{tri}}$. Applying Proposition 2.10 to this case, one obtains a moduli interpretation of $\mathrm{Sh}(G^\star, K^{\star,p})$ as well as an integral model $\mathbf{Sh}(G^\star, K^{\star,p})$ over $\mathbb{Z}_{(p)}$ of $\mathrm{Sh}(G^\star, K^{\star,p})$. Explicitly, the integral model $\mathbf{Sh}(G^\star, K^{\star,p})$ parametrizes equivalence classes of tuples $(A, \iota, \lambda, \bar{\alpha}_{K^{\star,p}})$, where (A, ι, λ) is the same data as in $\widetilde{\mathbf{Sh}}(G, K^p)$, and $\alpha_{K^{\star,p}}$ is a $K^{\star,p}$-level structure on A, that is, an $K^{\star,p}$-orbit of isomorphisms $\alpha\colon V \otimes \mathbb{A}^{\infty,p} \xrightarrow{\sim} \hat{V}^p(A)$ such that $\langle\,\cdot\,,\,\cdot\,\rangle_F$ is compatible with $\hat{\Psi}_F^\lambda$ up to a scalar in $\mathbb{A}^{\infty,p,\times}$.

Example 2.12. Fix a lattice $\Lambda \subseteq V$ stable under $\mathcal{O}_B$ such that $\langle \Lambda, \Lambda\rangle_F \subseteq \mathfrak{d}_F^{-1}$, where $\mathfrak{d}_F$ is the different of $F/\mathbb{Q}$, and that $\Lambda \otimes \mathbb{Z}_p$ is self-dual under $\langle\,\cdot\,,\,\cdot\,\rangle_F$.

Let $\mathfrak{M}$, $\mathfrak{N}$ be two ideals of $\mathcal{O}_F$ such that they are mutually coprime, both prime to p and the ramification set $\mathtt{R}$ of B, and that $\mathfrak{N}$ is contained in $N\mathcal{O}_F$ for some integer $N \geq 4$. Let $K_{0,1}(\mathfrak{M}, \mathfrak{N})^p$ be a subgroup of $\gamma \in G(\mathbb{A}^{\infty,p})$ such that there exists $v \in \Lambda$ with $\gamma v \in (\mathcal{O}_F v + \mathfrak{M}\Lambda) \cap (v + \mathfrak{N}\Lambda)$; put $K_{0,1}(\mathfrak{M}, \mathfrak{N}) := K_{0,1}(\mathfrak{M}, \mathfrak{N})^p K_p$. Then $K_{0,1}(\mathfrak{M}, \mathfrak{N})^p$ is neat and $\nu(K_{0,1}(\mathfrak{M}, \mathfrak{N})) = \widehat{\mathcal{O}}_F^\times$. We have thus isomorphisms

$$\mathbb{A}_F^{\infty,p,\times}/F_+^{p,\times}\nu(K_{0,1}(\mathfrak{M}, \mathfrak{N})^p) \cong \mathbb{A}_F^{\infty,\times}/F_+^\times \widehat{\mathcal{O}}_F^\times \cong \mathrm{Cl}^+(F),$$

where $\mathrm{Cl}^+(F)$ is the strict ideal class group of F; and the action of $\mathbb{A}^{\infty,\times}$ on $\mathrm{Cl}^+(F)$ is trivial. We choose prime-to-p fractional ideals $\mathfrak{c}_1, \ldots, \mathfrak{c}_h$ that form a set of representatives of $\mathrm{Cl}^+(F)$. Then for each $\mathfrak{c} \in \{\mathfrak{c}_1, \ldots, \mathfrak{c}_h\}$, the moduli scheme $\widetilde{\mathbf{Sh}}^{\mathfrak{c}}(G, K_{0,1}(\mathfrak{M}, \mathfrak{N})^p)$ classifies tuples $(A, \iota, \lambda, C_{\mathfrak{M}}, \alpha_{\mathfrak{N}})$, where

- (A, ι) is a projective abelian scheme equipped with real multiplication by $\mathcal{O}_B$;
- $\lambda\colon A \to A^\vee$ is an $\mathcal{O}_F$-linear polarization such that $\iota(b)^\vee \circ \lambda = \lambda \circ \iota(b^*)$ for $b \in \mathcal{O}_B$, and the induced map of abelian fppf-sheaves

$$A^\vee \xrightarrow{\sim} A \otimes_{\mathcal{O}_F} \mathfrak{c}$$

  is an isomorphism;
- $C_{\mathfrak{M}}$ is a finite flat subgroup scheme of $A[\mathfrak{M}]$ that is $\mathcal{O}_B$-cyclic of order $(\mathrm{Nm}\,\mathfrak{M})^2$;

- $\alpha_{\mathfrak{N}}\colon (\mathcal{O}_F/\mathfrak{N})^{\oplus 2} \hookrightarrow A[\mathfrak{N}]$ is an embedding of finite étale group schemes equivariant under the action of $\mathcal{O}_B \otimes_{\mathcal{O}_F} \mathcal{O}_F/\mathfrak{N} \cong \mathrm{GL}_2(\mathcal{O}_F/\mathfrak{N})$.

Let $g_{\mathfrak{c}}^p \in G(\mathbb{A}^{\infty,p})$ be such that the fractional ideal attached to the idèle $\nu(g_{\mathfrak{c}}^p) \in \mathbb{A}_F^{\infty,p,\times}$ represents the strict ideal class $\mathfrak{c}$. Put

$$K_{\mathfrak{c}_i}^{\star,p} := g_{\mathfrak{c}}^p K_{0,1}(\mathfrak{M},\mathfrak{N})^p g_{\mathfrak{c}}^{p,-1} \cap G^\star(\mathbb{A}^{\infty,p}).$$

Then we have

$$\widetilde{\mathbf{Sh}}^{\mathfrak{c}}(G, K_{0,1}(\mathfrak{M},\mathfrak{N})^p) \otimes \mathbb{Q} \cong \mathrm{Sh}(G^\star, K_{\mathfrak{c}_i}^{\star,p}).$$

More explicitly, if $\Gamma_{0,1}^{\mathfrak{c}}(\mathfrak{M},\mathfrak{N}) := G^\star(\mathbb{Q})_+ \cap K_{\mathfrak{c}}^{\star,p}$, where $G^\star(\mathbb{Q})_+ \subseteq G^\star(\mathbb{Q})$ is the subgroup of elements with totally positive reduced norms, then

$$\widetilde{\mathbf{Sh}}^{\mathfrak{c}}(G, K_{0,1}(\mathfrak{M},\mathfrak{N})^p)(\mathbb{C}) \cong \mathrm{Sh}(G^\star, K_{\mathfrak{c}}^{\star,p})(\mathbb{C}) \cong \Gamma_{0,1}^{\mathfrak{c}}(\mathfrak{M},\mathfrak{N}) \backslash (\mathfrak{H}^+)^{\Sigma_\infty}.$$

In particular, $\widetilde{\mathbf{Sh}}^{\mathfrak{c}}(G, K_{0,1}(\mathfrak{M},\mathfrak{N})^p) \otimes \mathbb{Q}$ is geometrically connected for every $\mathfrak{c}$. In this case, one has $\Delta_{K_{0,1}(\mathfrak{M},\mathfrak{N})^p} = \mathcal{O}_{F,+}^\times / \mathcal{O}_{F,\mathfrak{N}}^{\times,2}$, where $\mathcal{O}_{F,\mathfrak{N}}^\times$ denotes the subgroup of $\xi \in \mathcal{O}_F^\times$ with $\xi \equiv 1 \mod \mathfrak{N}$. It is clear that the action of $\Delta_{K_{0,1}(\mathfrak{M},\mathfrak{N})^p}$ preserves $\widetilde{\mathbf{Sh}}^{\mathfrak{c}}(G, K_{0,1}(\mathfrak{M},\mathfrak{N})^p)$, and one obtains an isomorphism

$$\mathbf{Sh}(G, K_{0,1}(\mathfrak{M},\mathfrak{N})^p) \cong \coprod_{i=1}^{h} \mathbf{Sh}^{\mathfrak{c}_i}(G, K_{0,1}(\mathfrak{M},\mathfrak{N})^p)$$

with $\mathbf{Sh}^{\mathfrak{c}_i}(G, K_{0,1}(\mathfrak{M},\mathfrak{N})^p) = \widetilde{\mathbf{Sh}}^{\mathfrak{c}_i}(G, K_{0,1}(\mathfrak{M},\mathfrak{N})^p)/\Delta_{K_{0,1}(\mathfrak{M},\mathfrak{N})^p}$. Since $\Delta_{K_{0,1}(\mathfrak{M},\mathfrak{N})^p}$ acts freely on $\widetilde{\mathbf{Sh}}(G, K_{0,1}(\mathfrak{M},\mathfrak{N})^p)$, each $\mathbf{Sh}^{\mathfrak{c}_i}(G, K_{0,1}(\mathfrak{M},\mathfrak{N})^p)$ is a smooth quasiprojective scheme over $\mathbb{Z}_{(p)}$.

2F. ***Comparison of quaternionic and unitary moduli problems.*** We now compare the integral model $\mathbf{Sh}(G, K^p)$ defined in (2-4) and the one constructed using the unitary Shimura variety $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)$ with $\mathtt{S} = \varnothing$. Note that when $\mathtt{S} = \varnothing$, there is only one choice for $\tilde{\mathtt{S}}$, so we write simply G' for $G'_{\tilde{\mathtt{S}}}$. By the universal extension property of $\mathbf{Sh}(G) := \varprojlim_{K^p} \mathbf{Sh}(G, K^p)$, these two integral canonical models are necessarily isomorphic. However, for later applications to the supersingular locus of $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}$, one needs a more explicit comparison between the universal family of abelian varieties over $\mathbf{Sh}(G)$ (as in Remark 2.9(1)) with that over $\mathbf{Sh}(G')$. It suffices to compare the universal objects over the neutral connected components via the isomorphism

$$\mathbf{Sh}(G)^\circ_{\mathbb{Z}_p^{\mathrm{ur}}} \xrightarrow{\sim} \mathbf{Sh}(G')^\circ_{\mathbb{Z}_p^{\mathrm{ur}}}$$

induced by (2-2). Here, $\mathbf{Sh}(G)^\circ_{\mathbb{Z}_p^{\mathrm{ur}}}$ is defined similarly as $\mathbf{Sh}(G')^\circ_{\mathbb{Z}_p^{\mathrm{ur}}}$; in other words, it is the closure of $\mathrm{Sh}(G)^\circ$ in $\mathbf{Sh}(G) \otimes \mathbb{Z}_p^{\mathrm{ur}}$.

The natural inclusion $G^\star \hookrightarrow G$ induces also an isomorphism of derived and adjoint groups, and is compatible with Deligne homomorphisms. By Deligne's theory of connected Shimura varieties, it induces an isomorphism of neutral connected components $\mathbf{Sh}(G^\star)^\circ \cong \mathbf{Sh}(G)^\circ$. Therefore, we are reduced to comparing the universal family over $\mathbf{Sh}(G^\star)$ and $\mathbf{Sh}(G')$.

Recall that we have chosen an element $\gamma \in B^\times$ to define the pairing $\langle\,\cdot\,,\,\cdot\,\rangle_F$ on $V = B$. We take the symmetric element $\delta \in D_{\mathtt{S}}^\times$ in Section 2D to be $\delta = \gamma/(2\sqrt{\mathfrak{d}})$. One has $W = V \otimes_F E$, and

$$\psi(x \otimes 1, y \otimes 1) = \langle x, y\rangle$$

for any $x, y \in V$. Put $\langle\,\cdot\,,\,\cdot\,\rangle := \mathrm{Tr}_{F/\mathbb{Q}} \circ \langle\,\cdot\,,\,\cdot\,\rangle_F$. Then $G^\star$ (resp. G') can be viewed as the similitude group of $(V, \langle\,\cdot\,,\,\cdot\,\rangle)$ (resp. (W, ψ) (2-3)); and there exists a natural injection $G^\star \hookrightarrow G$ compatible with Deligne homomorphisms that induces isomorphisms on the associated derived and adjoint groups.

We take $\mathcal{O}_{D_\varnothing} = \mathcal{O}_B \otimes_{\mathcal{O}_F} \mathcal{O}_E$. Let $K^{\star p} \subseteq G^\star(\mathbb{A}^{\infty,p})$ and $K'^p \subseteq G'(\mathbb{A}^{\infty,p})$ be sufficiently small open compact subgroups with $K^{\star p} \subseteq K'^p$. To each point $(A, \iota, \lambda, \bar{\alpha}_{K^{\star,p}})$ of $\mathbf{Sh}(G^\star, K^{\star,p})$ with values in a $\mathbb{Z}_p$-scheme S, we attach the tuple $(A', \iota', \lambda', \bar{\alpha}^{\mathrm{rat}}_{K'^p})$, where

- $A' = A \otimes_{\mathcal{O}_F} \mathcal{O}_E$;
- $\iota' \colon \mathcal{O}_{D_\varnothing} \to \mathrm{End}_S(A')$ is the action induced by ι;
- $\lambda' \colon A' \to A'^\vee$ is the prime-to-p polarization given by
$$A' = A \otimes_{\mathcal{O}_F} \mathcal{O}_E \xrightarrow{\lambda\otimes 1} A^\vee \otimes_{\mathcal{O}_F} \mathcal{O}_E \xrightarrow{1\otimes i} A^\vee \otimes_{\mathcal{O}_F} \mathfrak{d}_{E/F}^{-1} \cong A'^\vee,$$
where $\mathfrak{d}_{E/F}^{-1}$ is the inverse of the relative different of E/F and $i \colon \mathcal{O}_E \to \mathfrak{d}_{E/F}^{-1}$ is the natural inclusion;
- $\bar{\alpha}^{\mathrm{rat}}_{K'^p}$ is a rational K'^p-level structure on A' induced by $\bar{\alpha}_{K^{\star,p}}$ by the compatibility of alternating forms $(V, \langle\,\cdot\,,\,\cdot\,\rangle)$ and (W, ψ). Here, we use the moduli interpretation of $\mathbf{Sh}(G', K'^p)$ in terms of isogeny classes of abelian varieties (See Remark 2.3).

This defines a morphism

$$\mathbf{Sh}(G^\star, K^{\star p}) \to \mathbf{Sh}(G', K'^p)$$

over $\mathbb{Z}_p$ extending the morphism $\mathrm{Sh}(G^\star, K'^{\star p}) \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \mathrm{Sh}(G', K'^p) \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Taking the projective limit on the prime-to-p levels, one gets a morphism of schemes over $\mathbb{Z}_p$

$$f \colon \mathbf{Sh}(G^\star) \to \mathbf{Sh}(G')$$

such that one has an isomorphism of abelian schemes

$$f^*\mathcal{A}' \cong \mathcal{A} \otimes_{\mathcal{O}_F} \mathcal{O}_E,$$

where $\mathcal{A}$ (resp. $\mathcal{A}'$) is the universal abelian scheme over $\mathbf{Sh}(G^\star)$ (resp. over $\mathbf{Sh}(G'_{\mathtt{S}})$). By the extension property of the integral canonical model, the map f induces an isomorphism

$$f^\circ \colon \mathbf{Sh}(G^\star)^\circ \xrightarrow{\sim} \mathbf{Sh}(G')^\circ$$

which extends the isomorphism $\mathrm{Sh}(G^\star)^\circ \xrightarrow{\sim} \mathrm{Sh}(G')^\circ$ induced by the morphism of Shimura data on the generic fibers. Thus the two universal families over $\mathbf{Sh}(G)^\circ$ induced from $\mathbf{Sh}(G^\star)$ and $\mathbf{Sh}(G')$ respectively are related by the relation

$$f^{\circ,*}(\mathcal{A}'|_{\mathbf{Sh}(G')^\circ}) \cong \mathcal{A}|_{\mathbf{Sh}(G)^\circ} \otimes_{\mathcal{O}_F} \mathcal{O}_E. \tag{2-5}$$

3. Goren–Oort cycles and supersingular locus

In this section, we study the supersingular locus and the superspecial locus of certain Shimura varieties established in the previous section.

3A. ***Notation and conventions.*** Let k be a perfect field containing all the residue fields of the auxiliary field E in Section 2B at p-adic places, and $W(k)$ be the ring of Witt vectors. Then $\Sigma_{E,\infty}$ is in natural bijection with $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{O}_E, W(k))$, and we have a canonical decomposition

$$\mathcal{O}_{D_{\mathrm{S}}} \otimes_{\mathbb{Z}} W(k) \cong \mathrm{Mat}_2(\mathcal{O}_E \otimes_{\mathbb{Z}} W(k)) = \bigoplus_{\tilde\tau \in \Sigma_{E,\infty}} \mathrm{M}(W(k)).$$

Let S be a $W(k)$-scheme, and N a coherent $\mathcal{O}_S \otimes \mathcal{O}_{D_{\mathrm{S}}}$-module. Then one has a canonical decomposition

$$N = \bigoplus_{\tilde\tau \in \Sigma_{E,\infty}} N_{\tilde\tau},$$

where $N_{\tilde\tau}$ is a left $\mathrm{Mat}_2(\mathcal{O}_S)$-module on which $\mathcal{O}_E$ acts via the composite map $\mathcal{O}_E \xrightarrow{\tilde\tau} W(k) \to \mathcal{O}_S$. We also denote by $N^\circ_{\tilde\tau}$ the direct summand $\mathfrak{e} \cdot N_{\tilde\tau}$ with $\mathfrak{e} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in \mathrm{Mat}_2(\mathcal{O}_S)$, and we call $M^\circ_{\tilde\tau}$ the *reduced* $\tilde\tau$*-component* of M.

Let G be a p-divisible group over a k-scheme S. We say that G is *supersingular* if, for every geometric point $\bar s$ of S, the Newton polygon of $G \times_S \bar s$ has only slope $\frac{1}{2}$. An abelian variety A over S is called supersingular if $A[p^\infty]$ is a supersingular p-divisible group over S, or equivalently for every geometric point $\bar s$ of S, $A \times_S \bar s$ is isogenous to a product of supersingular elliptic curves.

Consider a quaternionic Shimura variety $\mathrm{Sh}(G_{\mathrm{S,T}}, K^p)$ of type considered in Section 2A, and let $\mathbf{Sh}(G'_{\tilde{\mathrm{S}}}, K'^p)$ be the associated unitary Shimura variety over $\mathcal{O}_{\tilde\wp}$ as constructed in Section 2D for a certain choice of auxiliary CM extension E/F. Let k_0 be the smallest subfield of $\mathbb{F}_p^{\mathrm{ac}}$ containing all the residue fields of characteristic p of E. Then we have $k_0 \cong \mathbb{F}_{p^h}$ with h equal to the least common multiple of $\{(1 + g_{\mathfrak{p}} - 2\lfloor g_{\mathfrak{p}}/2 \rfloor) g_{\mathfrak{p}} \mid \mathfrak{p} \in \Sigma_p\}$. Put

$$\mathbf{Sh}(G'_{\tilde{\mathrm{S}}}, K'^p)_{k_0} := \mathbf{Sh}(G'_{\tilde{\mathrm{S}}}, K'^p) \otimes_{\mathcal{O}_{\tilde\wp}} k_0.$$

The universal abelian scheme over $\mathbf{Sh}(G'_{\tilde{\mathrm{S}}}, K'^p)_{k_0}$ is usually denoted by $\mathcal{A}'_{\tilde{\mathrm{S}}}$.

3B. ***Hasse invariants.*** We recall first the definition of essential invariant on $\mathbf{Sh}(G'_{\tilde{\mathrm{S}}}, K'^p)_{k_0}$ defined in [Tian and Xiao 2016, Section 4.4]. Let $(A, \iota, \lambda, \bar\alpha_{K'^p})$ be an S-valued point of $\mathbf{Sh}(G'_{\tilde{\mathrm{S}}}, K'^p)_{k_0}$ for some k_0-scheme S. Recall that $\mathrm{H}_1^{\mathrm{dR}}(A/S)$ is the relative de Rham homology of A. Let $\omega_{A^\vee}$ be the module of invariant differential 1-forms on $A^\vee$. Then for each $\tilde\tau \in \Sigma_{E,\infty}$, $\mathrm{H}_1^{\mathrm{dR}}(A/S)^\circ_{\tilde\tau}$ is a locally free $\mathcal{O}_S$-module on S of rank 2, and one has a Hodge filtration

$$0 \to \omega^\circ_{A^\vee,\tilde\tau} \to \mathrm{H}_1^{\mathrm{dR}}(A/S)^\circ_{\tilde\tau} \to \mathrm{Lie}(A/S)^\circ_{\tilde\tau} \to 0.$$

We defined, for each $\tilde\tau \in \Sigma_{E,\infty}$, the essential Verschiebung

$$V_{\mathrm{es},\tilde\tau} : \mathrm{H}_1^{\mathrm{dR}}(A/S)^\circ_{\tilde\tau} \to \mathrm{H}_1^{\mathrm{dR}}(A^{(p)}/S)^\circ_{\tilde\tau} \cong \mathrm{H}_1^{\mathrm{dR}}(A/S)^{\circ,(p)}_{\sigma^{-1}\tilde\tau},$$

to be the usual Verschiebung map if $s_{\sigma^{-1}\tilde{\tau}}=0$ or 1, and to be the inverse of Frobenius if $s_{\tilde{\tau}}=2$. This is possible since for $s_{\tilde{\tau}}=2$, the Frobenius map $F\colon \mathrm{H}_1^{\mathrm{dR}}(A^{(p)}/S)^\circ_{\tilde{\tau}}\to \mathrm{H}_1^{\mathrm{dR}}(A/S)^\circ_{\tilde{\tau}}$ is an isomorphism. For every integer $n\geq 1$, we denote by

$$V_{\mathrm{es}}^n\colon \mathrm{H}_1^{\mathrm{dR}}(A/S)^\circ_{\tilde{\tau}}\to \mathrm{H}_1^{\mathrm{dR}}(A^{(p^n)}/S)^\circ_{\tilde{\tau}}\cong \mathrm{H}_1^{\mathrm{dR}}(A/S)^{\circ,(p^n)}_{\sigma^{-n}\tilde{\tau}}$$

the n-th iteration of the essential Verschiebung.

Similarly, if $S=\operatorname{Spec} k$ is the spectrum of a perfect field k containing k_0, then one can define the essential Verschiebung

$$V_{\mathrm{es}}\colon \tilde{\mathcal{D}}(A)^\circ_{\tilde{\tau}}\to \tilde{\mathcal{D}}(A)^\circ_{\sigma^{-1}\tilde{\tau}}\quad \text{for all } \tilde{\tau}\in\Sigma_{E,\infty},$$

as the usual Verschiebung on Dieudonné modules if $s_{\tilde{\tau}}=0,1$ and as the inverse of the usual Frobenius if $s_{\tilde{\tau}}=2$. Here, $\tilde{\mathcal{D}}(A)$ denote the covariant Dieudonné module of $A[p^\infty]$. This is a σ^{-1}-semilinear map of $W(k)$-modules. For any integer $n\geq 1$, we denote also by

$$V_{\mathrm{es}}^n\colon \tilde{\mathcal{D}}(A)^\circ_{\tilde{\tau}}\to \tilde{\mathcal{D}}(A)^\circ_{\sigma^{-n}\tilde{\tau}}$$

the n-th iteration of the essential Verschiebung.

Now return to a general base S over k_0. For $\tau\in\Sigma_\infty-\mathrm{S}_\infty$, let $n_\tau=n_\tau(\mathrm{S})$ denote the smallest integer $n\geq 1$ such that $\sigma^{-n}\tau\in\Sigma_\infty-\mathrm{S}_\infty$. Assumption 2.1 implies that n_τ is odd. Then for each $\tilde{\tau}\in\Sigma_{E,\infty}$ with $s_{\tilde{\tau}}=1$, or equivalently each $\tilde{\tau}\in\Sigma_{E,\infty}$ lifting some $\tau\in\Sigma_\infty-\mathrm{S}_\infty$, the restriction of $V_{\mathrm{es}}^{n_\tau}$ to $\omega^\circ_{A^\vee,\tilde{\tau}}$ defines a map

$$h_{\tilde{\tau}}(A)\colon \omega^\circ_{A^\vee,\tilde{\tau}}\to \omega^{\circ,(p^{n_\tau})}_{A^\vee,\sigma^{-n_\tau}\tilde{\tau}}\cong (\omega^\circ_{A^\vee,\sigma^{-n_\tau}\tilde{\tau}})^{\otimes p^{n_\tau}}.$$

Applying this construction to the universal object, one gets a global section

$$h_{\tilde{\tau}}\in\Gamma(\mathbf{Sh}(G'_{\tilde{\mathrm{S}}},K'^p)_{k_0},(\omega^\circ_{\mathcal{A}'^\vee_{\tilde{\mathrm{S}}},\sigma^{-n_\tau}\tilde{\tau}})^{\otimes p^{n_\tau}}\otimes(\omega^\circ_{\mathcal{A}'^\vee_{\tilde{\mathrm{S}}},\tilde{\tau}})^{\otimes -1}). \tag{3-1}$$

called the *τ-th partial Hasse invariant.*

Proposition 3.1. *Let $x=(A,\iota,\lambda,\bar{\alpha}_{K'^p})$ be an $\mathbb{F}_p^{\mathrm{ac}}$-point of $\mathbf{Sh}(G'_{\tilde{\mathrm{S}}},K'^p)_{k_0}$, and $\mathfrak{p}$ a p-adic place of F such that $\mathrm{S}_{\infty/\mathfrak{p}}\neq\Sigma_{\infty/\mathfrak{p}}$. Assume that $h_{\tilde{\tau}}(A)\neq 0$ for all $\tilde{\tau}\in\Sigma_{E,\infty/\mathfrak{p}}$ with $s_{\tilde{\tau}}=1$. Then the p-divisible group $A[\mathfrak{p}^\infty]$ is not supersingular.*

Proof. The covariant Dieudonné module $\tilde{\mathcal{D}}(A)$ of $A[p^\infty]$ is a free $W(\mathbb{F}_p^{\mathrm{ac}})\otimes_{\mathbb{Z}}\mathcal{O}_{D_{\mathrm{S}}}$-module of rank 1. Then the covariant Dieudonné module of $A[\mathfrak{p}^\infty]$ is given by

$$\tilde{\mathcal{D}}(A[\mathfrak{p}^\infty])=\bigoplus_{\tilde{\tau}\in\Sigma_{E,\infty/\mathfrak{p}}}\tilde{\mathcal{D}}(A)^{\circ,\oplus 2}_{\tilde{\tau}},$$

and there exists a canonical isomorphism

$$\tilde{\mathcal{D}}(A)^\circ_{\tilde{\tau}}/p\tilde{\mathcal{D}}(A)^\circ_{\tilde{\tau}}\cong \mathrm{H}_1^{\mathrm{dR}}(A/\mathbb{F}_p^{\mathrm{ac}})^\circ_{\tilde{\tau}}.$$

By assumption, for all $\tilde{\tau}\in\Sigma_{E,\infty/\mathfrak{p}}$ lifting some $\tau\in\Sigma_{\infty/\mathfrak{p}}-\mathrm{S}_{\infty/\mathfrak{p}}$, the map

$$h_{\tilde{\tau}}(A)\colon \omega^\circ_{A^\vee,\tilde{\tau}}\to \omega^{\circ,(p^{n_\tau})}_{A^\vee,\sigma^{-n_\tau}\tilde{\tau}}$$

is nonvanishing. Thus it is an isomorphism, as both the source and the target are one-dimensional $\mathbb{F}_p^{\mathrm{ac}}$-vector spaces. For each $\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{p}}$ lifting some $\tau \in \Sigma_{\infty/\mathfrak{p}} - \mathtt{S}_{\infty/\mathfrak{p}}$, choose a basis $e_{\tilde{\tau}}$ for $\omega^{\circ}_{A^\vee,\tilde{\tau}}$, and extend it to a basis $(e_{\tilde{\tau}}, f_{\tilde{\tau}})$ of $\mathrm{H}_1^{\mathrm{dR}}(A/\mathbb{F}_p^{\mathrm{ac}})^{\circ}_{\tilde{\tau}}$. If we consider V_{es} as a σ^{-1}-linear map on $\mathrm{H}_1^{\mathrm{dR}}(A/\mathbb{F}_p^{\mathrm{ac}})^{\circ}_{\tilde{\tau}}$, then one has

$$V_{\mathrm{es}}^{n_\tau}(e_{\tilde{\tau}}, f_{\tilde{\tau}}) = (e_{\sigma^{-n_\tau}\tilde{\tau}}, f_{\sigma^{-n_\tau}\tilde{\tau}}) \begin{pmatrix} u_{\tilde{\tau}} & 0 \\ 0 & 0 \end{pmatrix}$$

with $u_{\tilde{\tau}} \in \mathbb{F}_p^{\mathrm{ac},\times}$.

Let $\mathfrak{q}$ be a p-adic place of E above $\mathfrak{p}$. By our choice of E, $g_{\mathfrak{q}} := [E_{\mathfrak{q}} : \mathbb{Q}_p]$ is always even no matter whether $\mathfrak{p}$ is split or inert in E. To prove the proposition, it suffices to show that the p-divisible group $A[\mathfrak{q}^\infty]$ is not supersingular. By composing the essential Verschiebung maps on all $\mathrm{H}_1^{\mathrm{dR}}(A/S)^{\circ}_{\tilde{\tau}}$ with $\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{q}}$, we get

$$V_{\mathrm{es}}^{g_{\mathfrak{q}}}(e_{\tilde{\tau}}, f_{\tilde{\tau}}) = (e_{\tilde{\tau}}, f_{\tilde{\tau}}) \begin{pmatrix} \bar{a}_{\tilde{\tau}} & 0 \\ 0 & 0 \end{pmatrix}$$

with $\bar{a}_{\tilde{\tau}} \in \mathbb{F}_p^{\mathrm{ac},\times}$ for all $\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{q}}$ with $s_{\tilde{\tau}} = 1$. Now, note that $V_{\mathrm{es}}^{g_{\mathfrak{q}}}$ on $\mathrm{H}_1^{\mathrm{dR}}(A/\mathbb{F}_p^{\mathrm{ac}})^{\circ}_{\tilde{\tau}}$ is nothing but the reduction modulo p of the $\sigma^{-g_{\mathfrak{q}}}$-linear map

$$V^{g_{\mathfrak{q}}}/p^m : \tilde{\mathcal{D}}(A)^{\circ}_{\tilde{\tau}} \to \tilde{\mathcal{D}}(A)^{\circ}_{\tilde{\tau}},$$

where m is the number of $\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{q}}$ with $s_{\tilde{\tau}} = 2$. If $(\tilde{e}_{\tilde{\tau}}, \tilde{f}_{\tilde{\tau}})$ is a lift of $(e_{\tilde{\tau}}, f_{\tilde{\tau}})$ to a basis of $\tilde{\mathcal{D}}(A)^{\circ}_{\tilde{\tau}}$ over $W(\mathbb{F}_p^{\mathrm{ac}})$, then $V^{g_{\mathfrak{q}}}/p^m$ on $\tilde{\mathcal{D}}(A)^{\circ}_{\tilde{\tau}}$ is given by

$$\frac{V^{g_{\mathfrak{q}}}}{p^m}(\tilde{e}_{\tilde{\tau}}, \tilde{f}_{\tilde{\tau}}) = (\tilde{e}_{\tilde{\tau}}, \tilde{f}_{\tilde{\tau}}) \begin{pmatrix} a_{\tilde{\tau}} & pb_{\tilde{\tau}} \\ pc_{\tilde{\tau}} & pd_{\tilde{\tau}} \end{pmatrix}$$

for some $a_{\tilde{\tau}} \in W(\mathbb{F}_p^{\mathrm{ac}})^\times$ lifting $\bar{a}_{\tilde{\tau}}$ and $b_{\tilde{\tau}}, c_{\tilde{\tau}}, d_{\tilde{\tau}} \in W(\mathbb{F}_p^{\mathrm{ac}})$. Put

$$L := \bigcap_{n \geq 1} \left(\frac{V^{g_{\mathfrak{q}}}}{p^m} \right)^n \tilde{\mathcal{D}}(A)^{\circ}_{\tilde{\tau}}.$$

It is easy to see that L is a $W(\mathbb{F}_p^{\mathrm{ac}})$-direct summand of $\tilde{\mathcal{D}}(A)^{\circ}_{\tilde{\tau}}$ of rank one, on which $V^{g_{\mathfrak{p}}}/p^m$ acts bijectively. It follows that $1 - m/g_{\mathfrak{q}}$ is a slope of the p-divisible group $A[\mathfrak{q}^\infty]$. By our choice of the $s_{\tilde{\tau}}$ in Section 2B, the two sets $\{\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{q}} \mid s_{\tilde{\tau}} = 2\}$ and $\{\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{q}} \mid s_{\tilde{\tau}} = 0\}$ have the same cardinality, hence $2m < g_{\mathfrak{q}}$, that is, $1 - m/g_{\mathfrak{q}} > \frac{1}{2}$. Therefore, $A[\mathfrak{q}^\infty]$ hence $A[\mathfrak{p}^\infty]$, are not supersingular. □

3C. *Goren–Oort divisors.* For each $\tau \in \Sigma_\infty - \mathtt{S}_\infty$, let $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\tau}$ be the closed subscheme of $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0}$ defined by the vanishing of $h_{\tilde{\tau}}$ for some $\tilde{\tau} \in \Sigma_{E,\infty}$ lifting τ. By [Tian and Xiao 2016, Lemma 4.5], $h_{\tilde{\tau}}$ vanishes at a point x of $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0}$ if and only if $h_{\tilde{\tau}^c}$ vanishes at x. In particular, $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\tau}$ does not depend on the choice of $\tilde{\tau}$ lifting τ. We call $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\tau}$ the τ-th *Goren–Oort divisor* of $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0}$. For a nonempty subset $\Delta \subseteq \Sigma_\infty - \mathtt{S}_\infty$, we put

$$\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\Delta} := \bigcap_{\tau \in \Delta} \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\tau}.$$

According to [Tian and Xiao 2016, Proposition 4.7], $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\Delta}$ is a proper and smooth closed subvariety of $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0}$ of codimension $\#\Delta$; in other words, the union $\bigcup_{\tau\in\Sigma_\infty-\mathtt{S}_\infty}\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\tau}$ is a strict normal crossing divisor of $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0}$.

In [Tian and Xiao 2016], we gave an explicit description of $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\tau}$ in terms of another unitary Shimura variety of type in Section 2D. To describe this, let $\mathfrak{p}\in\Sigma_p$ denote the p-adic place induced by τ. Set

$$\mathtt{S}_\tau=\begin{cases}\mathtt{S}\cup\{\tau,\sigma^{-n_\tau}\tau\} & \text{if } \Sigma_{\infty/\mathfrak{p}}\neq\mathtt{S}_{\infty/\mathfrak{p}}\cup\{\tau\},\\ \mathtt{S}\cup\{\tau,\mathfrak{p}\} & \text{if } \Sigma_{\infty/\mathfrak{p}}=\mathtt{S}_{\infty/\mathfrak{p}}\cup\{\tau\}.\end{cases}\tag{3-2}$$

We fix a lifting $\tilde{\tau}\in\Sigma_{E,\infty}$ of τ, and take $\tilde{\mathtt{S}}_{\tau,\infty}$ to be $\tilde{\mathtt{S}}_\infty\cup\{\tilde{\tau},\sigma^{-n_\tau}\tilde{\tau}^c\}$ if $\Sigma_{\infty/\mathfrak{p}}\neq\mathtt{S}_{\infty/\mathfrak{p}}\cup\{\tau\}$, and to be $\tilde{\mathtt{S}}_\infty\cup\{\tilde{\tau}\}$ if $\Sigma_{\infty/\mathfrak{p}}=\mathtt{S}_{\infty/\mathfrak{p}}\cup\{\tau\}$. This choice of $\tilde{\mathtt{S}}_{\tau,\infty}$ satisfies Assumption 2.2. We note that both $D_{\mathtt{S}}$ and $D_{\mathtt{S}_\tau}$ are isomorphic to $\mathrm{Mat}_2(E)$. We fix an isomorphism $D_{\mathtt{S}}\cong D_{\mathtt{S}_\tau}$, and let $\mathcal{O}_{D_{\mathtt{S}_\tau}}$ denote the order of $D_{\mathtt{S}_\tau}$ corresponding to $\mathcal{O}_{D_{\mathtt{S}}}$ under this isomorphism.

Proposition 3.2. *Under the above notation, there exists a canonical projection*

$$\pi'_\tau\colon \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\tau}\to\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\tau}, K'^p)_{k_0}$$

where:

(1) *If $\Sigma_{\infty/\mathfrak{p}}\neq\mathtt{S}_{\infty/\mathfrak{p}}\cup\{\tau\}$, then π'_τ is a $\mathbb{P}^1$-fibration over $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\tau}, K'^p)_{k_0}$ such that the restriction of π'_τ to $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\{\tau,\sigma^{-n_\tau}\tau\}}$ is an isomorphism.*

(2) *If $\Sigma_{\infty/\mathfrak{p}}=\mathtt{S}_{\infty/\mathfrak{p}}\cup\{\tau\}$, then π'_τ is an isomorphism.*

Moreover, π'_τ is equivariant under prime-to-p Hecke correspondences when K'^p varies, and there exists a p-quasiisogeny

$$\phi\colon \mathcal{A}'_{\tilde{\mathtt{S}}}|_{\mathbf{Sh}(G'_{\tilde{\mathtt{S}}},K'^p)_{k_0,\tau}}\to\pi'^*_\tau\mathcal{A}'_{\tilde{\mathtt{S}}_\tau}$$

that is compatible with polarizations and K'^p-level structures on both sides, and that induces an isomorphism of relative de Rham homology groups

$$\phi_{*,\tau}:\mathrm{H}^{\mathrm{dR}}_1(\mathcal{A}'_{\tilde{\mathtt{S}}}|_{\mathbf{Sh}(G'_{\tilde{\mathtt{S}}},K'^p)_{k_0,\tau}}/\,\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\tau})^\circ_{\tilde{\tau}'}\cong\mathrm{H}^{\mathrm{dR}}_1(\mathcal{A}'_{\tilde{\mathtt{S}}_\tau}/\,\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\tau}, K'^p))^\circ_{\tilde{\tau}'}$$

for any $\tilde{\tau}'\in\Sigma_{E,\infty/\mathfrak{p}}$ lifting some $\tau'\in\Sigma_\infty-\mathtt{S}_{\tau,\infty/\mathfrak{p}}$.

Proof. This is [Tian and Xiao 2016, Theorem 5.2]. □

Here, we are content with explaining the map π'_τ and the quasiisogeny ϕ on $\mathbb{F}_p^{\mathrm{ac}}$-points. Take $x=(A,\iota_A,\lambda_A,\alpha_A)\in\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\tau}(\mathbb{F}_p^{\mathrm{ac}})$. Denote by $\tilde{\mathcal{D}}(A)^\circ=\bigoplus_{\tilde{\tau}'\in\Sigma_{E,\infty}}\tilde{\mathcal{D}}(A)^\circ_{\tilde{\tau}'}$ the reduced covariant Dieudonné module as usual. For each $\tilde{\tau}'\in\Sigma_{E,\infty}$, define the essential Frobenius

$$F_{\mathrm{es}}\colon\tilde{\mathcal{D}}^\circ_{\sigma^{-1}\tilde{\tau}'}\to\tilde{\mathcal{D}}^\circ_{\tilde{\tau}'}$$

as the usual Frobenius map if $s_{\tilde{\tau}'}=1,2$ and as the inverse of Verschiebung map if $s_{\tilde{\tau}'}=0$. Consider a $W(\mathbb{F}_p^{\mathrm{ac}})$-lattice $M^\circ=\bigoplus_{\tilde{\tau}'\in\Sigma_{E,\infty}}M_{\tilde{\tau}'}$ of $\tilde{\mathcal{D}}(A)^\circ[1/p]$ such that

$$M^\circ_{\tilde{\tau}'}=\begin{cases}F_{\mathrm{es}}^{n_\tau-\ell}\tilde{\mathcal{D}}(A)^\circ_{\sigma^{-n_\tau}\tilde{\tau}} & \text{if } \tilde{\tau}'=\sigma^{-\ell}\tilde{\tau} \text{ with } 0\le\ell\le n_\tau-1,\\ \frac{1}{p}F_{\mathrm{es}}^{n_\tau-\ell}\tilde{\mathcal{D}}(A)^\circ_{\sigma^{-n_\tau}\tilde{\tau}^c} & \text{if } \tilde{\tau}'=\sigma^{-\ell}\tilde{\tau}^c \text{ with } 0\le\ell\le n_\tau-1 \text{ and } \Sigma_{\infty/\mathfrak{p}}\neq\mathtt{S}_{\infty/\mathfrak{p}}\cup\{\tau\},\\ \tilde{\mathcal{D}}(A)^\circ_{\tilde{\tau}'} & \text{otherwise.}\end{cases}$$

Note that the condition $h_{\tilde{\tau}}(A)=0$ is equivalent to $\tilde{\omega}^\circ_{A^\vee,\tilde{\tau}}=F_{\mathrm{es}}^{n_\tau}(\tilde{\mathcal{D}}(A)^\circ_{\sigma^{-n_\tau}\tilde{\tau}})$, where $\tilde{\omega}^\circ_{A^\vee,\tilde{\tau}}$ denotes the preimage of $\omega^\circ_{A^\vee,\tilde{\tau}}$ under the natural reduction map

$$\tilde{\mathcal{D}}(A)^\circ_{\tilde{\tau}}\to\tilde{\mathcal{D}}(A)^\circ_{\tilde{\tau}}/p\tilde{\mathcal{D}}(A)^\circ_{\tilde{\tau}}\cong\mathrm{H}_1^{\mathrm{dR}}(A/\mathbb{F}_p^{\mathrm{ac}})^\circ_{\tilde{\tau}}.$$

Using this property, one checks easily that M° is a Dieudonné submodule of $\tilde{\mathcal{D}}(A)^\circ[1/p]$. Put $M:=M^{\circ,\oplus 2}$ equipped with the natural action of $\mathcal{O}_{D_{\mathtt{S}}}\otimes\mathbb{Z}_p\cong\mathrm{Mat}_2(\mathcal{O}_E\otimes\mathbb{Z}_p)$. Then M corresponds to a p-divisible group G equipped with an $\mathcal{O}_{D_{\mathtt{S}}}$-action and an $\mathcal{O}_{D_{\mathtt{S}}}$-linear isogeny $\phi_p\colon A[p^\infty]\to G$. Thus there exists an abelian variety B over $\mathbb{F}_p^{\mathrm{ac}}$ with $B[p^\infty]=G$ and a p-quasiisogeny $\phi\colon A\to B$ such that ϕ_p is obtained by taking the p^∞-torsion of ϕ. Moreover, by construction, it is easy to see that

$$\dim\mathrm{Lie}(B)^\circ_{\tilde{\tau}'}=\begin{cases}\dim(\mathrm{Lie}(A)^\circ_{\tilde{\tau}'}) & \text{if } \tilde{\tau}'\neq\tilde{\tau},\sigma^{-n_\tau}\tilde{\tau},\\ 0 & \text{if } \tilde{\tau}'=\tilde{\tau},\sigma^{-n_\tau}\tilde{\tau}^c,\\ 2 & \text{if } \tilde{\tau}'=\tilde{\tau}^c,\sigma^{-n_\tau}\tilde{\tau}.\end{cases}$$

In other words, the $\mathcal{O}_E$-action on B satisfies Kottwitz' condition for $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\tau},K'^p)$. Moreover, λ_A and α_A induce an $\mathcal{O}_{D_{\mathtt{S}_\tau}}$-linear prime-to-$p$ polarization λ_B via the fixed isomorphism $\mathcal{O}_{D_{\mathtt{S}}}\simeq\mathcal{O}_{D_{\mathtt{S}_\tau}}$ and a K'^p-level structure α_B on B, respectively, such that $(B,\iota_B,\lambda_B,\bar{\alpha}_B)$ is an $\mathbb{F}_p^{\mathrm{ac}}$-point of $\mathbf{Sh}(G_{\tilde{\mathtt{S}}_\tau},K'^p)$. The resulting map $(A,\iota_A,\lambda_A,\bar{\alpha}_A)\mapsto(B,\iota_B,\lambda_B,\bar{\alpha}_B)$ is nothing but π'_τ.

If $\Sigma_{\infty/\mathfrak{p}}\neq\mathtt{S}_{\infty/\mathfrak{p}}\cup\{\tau\}$, then $\sigma^{-n_\tau}\tau\neq\tau$ and we have $\tilde{\mathcal{D}}(B)^\circ_{\sigma^{-n_\tau}\tilde{\tau}}=\tilde{\mathcal{D}}(A)^\circ_{\sigma^{-n_\tau}\tilde{\tau}}$ by construction. To recover A from B, it suffices to "remember" the line $\omega^\circ_{A^\vee,\sigma^{-n_\tau}\tilde{\tau}}$ inside the two dimensional $\mathbb{F}_p^{\mathrm{ac}}$-vector space

$$\tilde{\mathcal{D}}(A)^\circ_{\sigma^{-n_\tau}\tilde{\tau}}/p\tilde{\mathcal{D}}(A)^\circ_{\sigma^{-n_\tau}\tilde{\tau}}=\tilde{\mathcal{D}}(B)^\circ_{\sigma^{-n_\tau}\tilde{\tau}}/p\tilde{\mathcal{D}}(B)^\circ_{\sigma^{-n_\tau}\tilde{\tau}}.$$

This means that the fiber of π'_τ over a point $(B,\iota_B,\lambda_B,\bar{\alpha}_B)\in\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\tau},K'^p)$ is isomorphic to $\mathbb{P}^1$. On the other hand, if $\Sigma_{\infty/\mathfrak{p}}=\mathtt{S}_{\infty/\mathfrak{p}}\cup\{\tau\}$ then $n_\tau=[F_{\mathfrak{p}}:\mathbb{Q}_p]$ is odd, one can completely recover A from B, and thus π'_τ induces a bijection on closed points.[3] The moreover part of the statement follows from the construction of π'_τ.

3D. ***Periodic semimeanders.*** Following [Tian and Xiao 2019], we iterate the construction of Goren–Oort divisors to produce some closed subvarieties called Goren–Oort cycles. To parametrize those cycles, one need to recall some combinatorial data introduced in [loc. cit., Section 3.1].

For a prime $\mathfrak{p}\in\Sigma_p$, put $d_{\mathfrak{p}}(\mathtt{S}):=g_{\mathfrak{p}}-\#\mathtt{S}_{\infty/\mathfrak{p}}$. If there is no confusion, we write $d_{\mathfrak{p}}=d_{\mathfrak{p}}(\mathtt{S})$ for simplicity. Consider the cylinder $C\colon x^2+y^2=1$ in 3-dimensional Euclidean space, and let C_0 be the section with

[3] To show that π'_τ is indeed an isomorphism, one has to check also that π'_τ induces isomorphisms of tangent spaces to each closed point. This is the most technical part of [Tian and Xiao 2016]. For more details, see [loc. cit., Lemma 5.20].

$z = 0$. We write $\Sigma_{\infty/\mathfrak{p}} = \{\tau_0, \dots, \tau_{g_\mathfrak{p}-1}\}$ such that $\tau_j = \sigma\tau_{j-1}$ for $j \in \mathbb{Z}/g_\mathfrak{p}\mathbb{Z}$. For $0 \le j \le g_\mathfrak{p} - 1$, we use τ_j to label the point $(\cos 2\pi j/g_\mathfrak{p}, \sin 2\pi j/g_\mathfrak{p}, 0)$ on C_0. If $\tau_j \in \mathtt{S}_{\infty/\mathfrak{p}}$, then we put a plus sign at τ_j; otherwise, we put a node at τ_j. We call such a picture *the band* associated to $\mathtt{S}_{\infty/\mathfrak{p}}$. We often draw the picture on the 2-dimensional xy-plane by thinking of x-axis modulo $g_\mathfrak{p}$. We put the points $\tau_0, \dots, \tau_{g_\mathfrak{p}-1}$ on the x-axis with coordinates $x = 0, \dots, g_\mathfrak{p} - 1$ respectively. For example, if $g_\mathfrak{p} = 6$ and $\mathtt{S}_{\infty/\mathfrak{p}} = \{\tau_1, \tau_3, \tau_4\}$, then we draw the band as

● + ● + + ● .

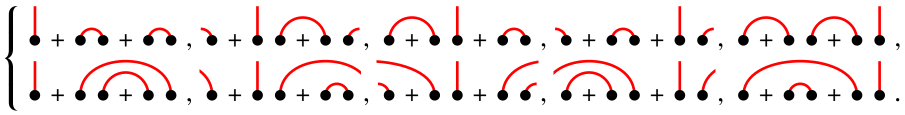
A *periodic semimeander* for $\mathtt{S}_{\infty/\mathfrak{p}}$ is a collection of curves (called *arcs*) that link two nodes of the band for $\mathtt{S}_{\infty/\mathfrak{p}}$, and straight lines (called *semilines*) that links a node to the infinity (that is, the direction $y \to +\infty$ in the 2-dimensional picture) subject to the following conditions:

(1) All the arcs and semilines lie on the cylinder above the band (that is to have positive y-coordinate in the 2-dimensional picture).

(2) Every node of the band for $\mathtt{S}_{\infty/\mathfrak{p}}$ is exactly one end point of an arc or a semiline.

(3) There are no intersection points among these arcs and semilines.

The number of arcs is denoted by r (so $r \le d_\mathfrak{p}/2$), and the number of semilines $d_\mathfrak{p} - 2r$ is called the *defect* of the periodic semimeander. Two periodic semimeanders are considered as the same if they can be continuously deformed into each other while keeping the above three properties in the process. We use $\mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, r)$ denote the set of semimeanders for $\mathtt{S}_{\infty/\mathfrak{p}}$ with r arcs (up to continuous deformations). For example, if $g_\mathfrak{p} = 7$, $r = 2$, and $\mathtt{S}_{\infty/\mathfrak{p}} = \{\tau_1, \tau_4\}$, then we have $d_\mathfrak{p} = 5$ and

$\mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, 2) =$


It is easy to see that the cardinality of $\mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, r)$ is $\binom{d_\mathfrak{p}}{r}$. In fact, the map that associates to each element $\mathfrak{a} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, r)$ the set of right end points of arcs in $\mathfrak{a}$ establishes a bijection between $\mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, r)$ and the subsets with cardinality r of the $d_\mathfrak{p}$-nodes in the band of $\mathtt{S}_{\infty/\mathfrak{p}}$.

3E. ***Goren–Oort cycles and supersingular locus.*** We fix a lifting $\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{p}}$ for each $\tau \in \Sigma_{\infty/\mathfrak{p}} - \mathtt{S}_{\infty/\mathfrak{p}}$.

For a periodic semimeander $\mathfrak{a} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, r)$ with $r \ge 1$, we put

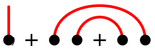
$$\mathtt{S}_\mathfrak{a} := \mathtt{S} \cup \{\tau \in \Sigma_{\infty/\mathfrak{p}} \mid \tau \text{ is an end point of some arc in } \mathfrak{a}\}. \tag{3-3}$$

For an arc δ in $\mathfrak{a}$, we use τ_δ^+ and τ_δ^- to denote its right and left end points respectively. We take

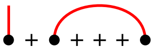
$$\tilde{\mathtt{S}}_{\mathfrak{a},\infty} = \tilde{\mathtt{S}}_\infty \cup \{\tilde{\tau}_\delta^+, \tilde{\tau}_\delta^{-,c} \mid \delta \text{ is an arc of } \mathfrak{a}\}.$$

Here, $\tilde{\tau}_\delta^+$ denotes the fixed lifting of τ_δ^+, and $\tilde{\tau}_\delta^{-,c}$ the conjugate of the fixed lifting $\tilde{\tau}_\delta^-$ of τ_δ^-. We fix an isomorphism $G'_{\tilde{\mathtt{S}}_\mathfrak{a}}(\mathbb{A}^\infty) \cong G'_{\tilde{\mathtt{S}}}(\mathbb{A}^\infty)$, and consider K'^p as an open compact subgroup of $G'_{\tilde{\mathtt{S}}_\mathfrak{a}}(\mathbb{A}^{\infty,p})$. We may thus speak of the unitary Shimura variety $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\mathfrak{a}}, K'^p)$.

Following [Tian and Xiao 2019, Section 3.7], for every $\mathfrak{a}\in\mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, r)$, we construct a closed subvariety $Z'_{\tilde{\mathtt{S}}}(\mathfrak{a})\subseteq\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0}$ of codimension r, which is an r-th iterated $\mathbb{P}^1$-fibration over $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}, K'^{p})_{k_0}$. We proceed by induction on $r\geq 0$. When $r=0$, we put simply $Z'_{\tilde{\mathtt{S}}}(\mathfrak{a}):=\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0}$. Assume now $r\geq 1$. An arc in $\mathfrak{a}$ is called *basic*, if it does not lie above any other arcs. Choose such a basic arc δ, and put $\tau:=\tau_\delta^+$ and $\tau^-:=\tau_\delta^-$ for simplicity. We note that $\tau^-=\sigma^{-n_\tau}\tau$. Consider the Goren–Oort divisor $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0,\tau}$, and let $\pi'_\tau\colon\ \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0,\tau}\to\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\tau}, K'^{p})_{k_0}$ be the $\mathbb{P}^1$-fibration given by Proposition 3.2. Let $\mathfrak{a}_\delta\in\mathfrak{B}(\mathtt{S}_{\mathfrak{a},\infty/\mathfrak{p}}, r-1)$ be the periodic semimeander for $\mathtt{S}_{\mathfrak{a}}$ obtained from $\mathfrak{a}$ by replacing the nodes at τ, τ^- with plus signs and removing the arc δ. For instance, if



then $\mathtt{S}_{\mathfrak{a}}=\mathtt{S}\cup\{\tau_2,\tau_3,\tau_5,\tau_6\}$, and the arc δ connecting τ_3 and τ_5 is the unique basic arc in $\mathfrak{a}$, and



By the induction hypothesis, we have constructed a closed subvariety $Z'_{\tilde{\mathtt{S}}_\tau}(\mathfrak{a}_\delta)\subseteq\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\tau}, K'^{p})_{k_0}$ of codimension $r-1$. Then we define $Z'_{\tilde{\mathtt{S}}}(\mathfrak{a})$ as the preimage of $Z'_{\tilde{\mathtt{S}}_\tau}(\mathfrak{a}_\delta)$ via π'_τ. We denote by

$$\pi'_{\mathfrak{a}}\colon\ Z'_{\tilde{\mathtt{S}}}(\mathfrak{a})\to\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}, K'^{p})_{k_0}$$

the canonical projection. In summary, we have a diagram

$$\begin{tikzcd}
Z'_{\tilde{\mathtt{S}}}(\mathfrak{a}) \arrow[r, hook] \arrow[d] \arrow[dd, bend right, "\pi'_{\mathfrak{a}}"'] & \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0,\tau} \arrow[r, hook] \arrow[d, "\pi'_\tau"] & \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0} \\
Z'_{\tilde{\mathtt{S}}_\tau}(\mathfrak{a}_\delta) \arrow[r, hook] \arrow[d, "\pi'_{\mathfrak{a}_\delta}"] & \mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\tau}, K'^{p})_{k_0} & \\
\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}, K'^{p})_{k_0} & &
\end{tikzcd}$$

where the square is cartesian. By induction hypothesis, the morphism $\pi'_{\mathfrak{a}_\delta}$ is an $(r-1)$-th iterated $\mathbb{P}^1$-fibration. It follows that $\pi'_{\mathfrak{a}}$ is an r-th iterated $\mathbb{P}^1$-fibration.

We explain the relationship between Goren–Oort cycles and the $\mathfrak{p}$-supersingular locus of $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0}$. Take $\mathfrak{a}\in\mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, \lfloor d_{\mathfrak{p}}/2\rfloor)$. If $d_{\mathfrak{p}}$ is even, then we put $W'_{\tilde{\mathtt{S}}}(\mathfrak{a}):=Z'_{\tilde{\mathtt{S}}}(\mathfrak{a})$. If $d_{\mathfrak{p}}$ is odd, then we let $\tau(\mathfrak{a})\in\Sigma_{\infty/\mathfrak{p}}$ denote the end point of the unique semiline in $\mathfrak{a}$, and define $W'_{\tilde{\mathtt{S}}}(\mathfrak{a})$ by the following Cartesian diagram:

$$\begin{tikzcd}
W'_{\tilde{\mathtt{S}}}(\mathfrak{a}) \arrow[r, hook] \arrow[d] & Z'_{\tilde{\mathtt{S}}}(\mathfrak{a}) \arrow[d, "\pi'_{\mathfrak{a}}"] \\
\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}, K'^{p})_{k_0,\tau(\mathfrak{a})} \arrow[r, hook] & \mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}, K'^{p})_{k_0}
\end{tikzcd}$$

We put

$$\tilde{\mathtt{S}}^*_{\mathfrak{a}} := \begin{cases} \tilde{\mathtt{S}}_{\mathfrak{a}} = (\mathtt{S}_{\mathfrak{a}}, \tilde{\mathtt{S}}_{\mathfrak{a},\infty}) & \text{if } d_{\mathfrak{p}} \text{ is even,} \\ (\mathtt{S}_{\mathfrak{a}} \cup \{\tau(\mathfrak{a}), \mathfrak{p}\}, \tilde{\mathtt{S}}_{\mathfrak{a},\infty} \cup \{\tilde{\tau}(\mathfrak{a})\}) & \text{if } d_{\mathfrak{p}} \text{ is odd.} \end{cases} \tag{3-4}$$

Note that the underlying set $\mathtt{S}^*_{\mathfrak{a}}$ of $\tilde{\mathtt{S}}^*_{\mathfrak{a}}$ is independent of $\mathfrak{a} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, \lfloor d_{\mathfrak{p}}/2 \rfloor)$, namely all $\mathtt{S}^*_{\mathfrak{a}}$ are equal to

$$\mathtt{S}(\mathfrak{p}) := \begin{cases} \mathtt{S} \cup \Sigma_{\infty/\mathfrak{p}} & \text{if } d_{\mathfrak{p}} \text{ is even,} \\ \mathtt{S} \cup \Sigma_{\infty/\mathfrak{p}} \cup \{\mathfrak{p}\} & \text{if } d_{\mathfrak{p}} \text{ is odd.} \end{cases} \tag{3-5}$$

If $d_{\mathfrak{p}}$ is odd, then we have an isomorphism

$$\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}, K'^p)_{k_0, \tau(\mathfrak{a})} \cong \mathbf{Sh}(G'_{\tilde{\mathtt{S}}^*_{\mathfrak{a}}}, K'^p)_{k_0}$$

by Proposition 3.2. Thus, regardless of the parity of $d_{\mathfrak{p}}$, one has a $\lfloor d_{\mathfrak{p}}/2 \rfloor$-th iterated $\mathbb{P}^1$-fibration equivariant under prime-to-p Hecke correspondences:

$$\pi'_{\mathfrak{a}}|_{W'_{\tilde{\mathtt{S}}}(\mathfrak{a})} \colon W'_{\tilde{\mathtt{S}}}(\mathfrak{a}) \to \mathbf{Sh}(G'_{\tilde{\mathtt{S}}^*_{\mathfrak{a}}}, K'^p)_{k_0}.$$

Theorem 3.3. *Under the notation above, the union*

$$\bigcup_{\mathfrak{a} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, \lfloor d_{\mathfrak{p}}/2 \rfloor)} W'_{\tilde{\mathtt{S}}}(\mathfrak{a})$$

is exactly the $\mathfrak{p}$*-supersingular locus of* $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0}$, *that is, the maximal closed subset where the universal* $\mathfrak{p}$*-divisible group* $\mathcal{A}'_{\tilde{\mathtt{S}}}[\mathfrak{p}^\infty]$ *is supersingular.*

Proof. We proceed by induction on $d_{\mathfrak{p}} \geq 0$. If $d_{\mathfrak{p}} = 0$, then $\mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, 0)$ consists only of the trivial periodic semimeander (that is, the one without any arcs or semilines). In this case, one has to show that the whole $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0}$ is $\mathfrak{p}$-supersingular. First, we have $s_{\tilde{\tau}} \in \{0, 2\}$ for all $\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{p}}$, and Assumption 2.2(2) implies that the number of $\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{p}}$ with $s_{\tilde{\tau}} = 2$ equals exactly to the number of $\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{p}}$ with $s_{\tilde{\tau}} = 0$. Now consider a point $x = (A, \iota, \lambda, \alpha) \in \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)(\mathbb{F}_p^{\mathrm{ac}})$. Then, for every $\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{p}}$, the $2g_{\mathfrak{p}}$-th iterated essential Verschiebung

$$V_{\mathrm{es}}^{2g_{\mathfrak{p}}} = \frac{V^{2g_{\mathfrak{p}}}}{p^{g_{\mathfrak{p}}}} \colon \tilde{\mathcal{D}}(A)^\circ_{\tilde{\tau}} \to \tilde{\mathcal{D}}(A)^\circ_{\sigma^{-2g_{\mathfrak{p}}}\tilde{\tau}} = \tilde{\mathcal{D}}(A)^\circ_{\tilde{\tau}}$$

is bijective, no matter whether $\mathfrak{p}$ is split or inert in E. It follows immediately that $\frac{1}{2}$ is the only slope of the Dieudonné module $\bigoplus_{\tilde{\tau} \in \Sigma_{E,\infty/\mathfrak{p}}} \tilde{\mathcal{D}}(A)_{\tilde{\tau}} = \tilde{\mathcal{D}}(A[\mathfrak{p}^\infty])$, so that $A[\mathfrak{p}^\infty]$ is supersingular.

Assume now $d_{\mathfrak{p}} \geq 1$. We prove first that the union $\bigcup_{\mathfrak{a} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, \lfloor d_{\mathfrak{p}}/2 \rfloor)} W'_{\tilde{\mathtt{S}}}(\mathfrak{a})$ is contained in the $\mathfrak{p}$-supersingular locus of $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0}$. Fix $\mathfrak{a} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, \lfloor d_{\mathfrak{p}}/2 \rfloor)$. Then one has a projection

$$\pi'_{\mathfrak{a}}|_{W'_{\tilde{\mathtt{S}}}(\mathfrak{a})} \colon W'_{\tilde{\mathtt{S}}}(\mathfrak{a}) \to \mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}, K'^p)_{k_0}$$

and a p-quasiisogeny

$$\phi_{\mathfrak{a}} \colon \mathcal{A}'_{\tilde{\mathtt{S}}}|_{W'_{\tilde{\mathtt{S}}}(\mathfrak{a})} \to \pi'^*_{\mathfrak{a}} \mathcal{A}'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}$$

by the construction of $\pi'_{\mathfrak{a}}$ and Proposition 3.2. Note that $d_{\mathfrak{p}}(\mathtt{S}_{\mathfrak{a}})=0$, and by the discussion above, $\mathcal{A}'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}[\mathfrak{p}^{\infty}]$ is supersingular over the entire $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}, K'^{p})_{k_0}$. It follows that $\mathcal{A}'_{\tilde{\mathtt{S}}}[\mathfrak{p}^{\infty}]$ is supersingular over $W_{\tilde{\mathtt{S}}}(\mathfrak{a})$.

To complete the proof, it remains to show that if $x \in \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})(\mathbb{F}_p^{\mathrm{ac}})$ is a $\mathfrak{p}$-supersingular point, then $x \in W'_{\tilde{\mathtt{S}}}(\mathfrak{a})(\mathbb{F}_p^{\mathrm{ac}})$ for some $\mathfrak{a} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, \lfloor d_{\mathfrak{p}}/2 \rfloor)$. By Proposition 3.1, there exists $\tau \in \Sigma_{\infty/\mathfrak{p}}$ such that $x \in \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0,\tau}(\mathbb{F}_p^{\mathrm{ac}})$. Consider the $\mathbb{P}^1$-fibration $\pi'_{\tau}\colon\ \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0,\tau} \to \mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\tau}}, K'^{p})_{k_0}$. Since $\mathcal{A}'_{\tilde{\mathtt{S}},x}$ is p-quasiisogenous to $\mathcal{A}'_{\tilde{\mathtt{S}}_{\tau},\pi'_{\tau}(x)}$, we see that $\pi'_{\tau}(x)$ lies in the $\mathfrak{p}$-supersingular locus of $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\tau}}, K'^{p})_{k_0}$. By the induction hypothesis, $\pi'_{\tau}(x) \in W'_{\tilde{\mathtt{S}}_{\tau}}(\mathfrak{b})(\mathbb{F}_p^{\mathrm{ac}})$ for some periodic semimeander $\mathfrak{b} \in \mathfrak{B}(\mathtt{S}_{\tau,\infty/\mathfrak{p}}, \lfloor d_{\mathfrak{p}}/2-1 \rfloor)$. Now let $\mathfrak{a}$ be the periodic semimeander obtained from $\mathfrak{b}$ by adjoining an arc δ connecting $\sigma^{-n_{\tau}}\tau$ and τ so that τ is the right end point of δ. Then $\mathfrak{a} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, \lfloor d_{\mathfrak{p}}/2 \rfloor)$, and δ is a basic arc of $\mathfrak{a}$ such that $\mathfrak{b}=\mathfrak{a}_{\delta}$. To finish the proof, it suffices to note that $W'_{\tilde{\mathtt{S}}}(\mathfrak{a}) = \pi'^{-1}_{\tau}(W'_{\tilde{\mathtt{S}}_{\tau}}(\mathfrak{b}))$ by definition. □

Definition 3.4. We put

$$\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0}^{\mathfrak{p}-\mathrm{sp}} := \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0,\Sigma_{\infty/\mathfrak{p}}},$$

and call it the $\mathfrak{p}$-*superspecial locus* of $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0}$.

We have the following proposition that characterizes the $\mathfrak{p}$-superspecial locus.

Proposition 3.5. *Let $\mathfrak{p} \in \Sigma_p$ be such that $d_{\mathfrak{p}}$ is odd, and take $\mathfrak{a} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, (d_{\mathfrak{p}}-1)/2)$. Then $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0}^{\mathfrak{p}-\mathrm{sp}}$ is contained in $W'_{\tilde{\mathtt{S}}}(\mathfrak{a})$, and the restriction of $\pi'_{\mathfrak{a}}$ to $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0}^{\mathfrak{p}-\mathrm{sp}}$ induces an isomorphism*

$$\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0}^{\mathfrak{p}-\mathrm{sp}} \xrightarrow{\sim} \mathbf{Sh}(G'_{\tilde{\mathtt{S}}^{*}_{\mathfrak{a}}}, K'^{p})_{k_0},$$

which is equivariant under prime-to-p Hecke correspondences.

Proof. We proceed by induction on $d_{\mathfrak{p}} \geq 1$. If $d_{\mathfrak{p}}=1$, then all the $\mathfrak{p}$-supersingular locus is $\mathfrak{p}$-superspecial, and the $\mathfrak{p}$-supersingular locus consists of only one stratum $W'_{\tilde{\mathtt{S}}}(\mathfrak{a})$. So the statement is clear.

Assume now $d_{\mathfrak{p}}>1$. Choose a basic arc δ of $\mathfrak{a}$. Let τ (resp. τ^{-}) be the right (resp. left) node of δ, and $\mathfrak{a}_{\delta}$ be the semimeander obtained from $\mathfrak{a}$ by removing the arc δ. Then one has a commutative diagram

$$\begin{tikzcd}
W'_{\tilde{\mathtt{S}}}(\mathfrak{a}) \arrow[r] \arrow[d] & Z'_{\tilde{\mathtt{S}}}(\mathfrak{a}) \arrow[r] \arrow[d] & \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^{p})_{k_0,\tau} \arrow[d, "\pi'_{\tau}"] \\
W'_{\tilde{\mathtt{S}}_{\tau}}(\mathfrak{a}_{\delta}) \arrow[r] \arrow[d] & Z'_{\tilde{\mathtt{S}}_{\tau}}(\mathfrak{a}_{\delta}) \arrow[r] \arrow[d, "\pi'_{\mathfrak{a}_{\delta}}"] & \mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\tau}}, K'^{p})_{k_0} \\
\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}, K'^{p})_{k_0,\tau(\mathfrak{a})} \arrow[r] \arrow[d, "\cong"] & \mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\mathfrak{a}}}, K'^{p})_{k_0} & \\
\mathbf{Sh}(G'_{\tilde{\mathtt{S}}^{*}_{\mathfrak{a}}}, K'^{p})_{k_0} & &
\end{tikzcd}$$

where all the squares are cartesian; all horizontal maps are closed immersions; and all vertical arrows are iterated $\mathbb{P}^1$-bundles. By the induction hypothesis, the $\mathfrak{p}$-superspecial locus $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_{\tau}}, K'^{p})_{k_0}^{\mathfrak{p}-\mathrm{sp}}$ is contained in $W'_{\tilde{\mathtt{S}}_\tau}(\mathfrak{a}_\delta)$ and the restriction of $\pi'_{\mathfrak{a}_\delta}$ induces an isomorphism

$$\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\tau}, K'^p)_{k_0}^{\mathfrak{p}-\mathrm{sp}} \xrightarrow{\sim} \mathbf{Sh}(G'_{\tilde{\mathtt{S}}^*_{\mathfrak{a}}}, K'^p)_{k_0}. \tag{3-6}$$

Now by Proposition 3.2, the restriction of π'_τ induces an isomorphism

$$\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0,\{\tau,\tau^-\}} \xrightarrow{\sim} \mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\tau}, K'^p)_{k_0}$$

compatible with the construction of Goren–Oort divisors. Thus, π'_τ sends $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0}^{\mathfrak{p}-\mathrm{sp}}$ isomorphically to $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}_\tau}, K'^p)_{k_0}^{\mathfrak{p}-\mathrm{sp}}$. The statement now follows immediately by composing with the isomorphism (3-6). □

3F. ***Total supersingular and superspecial loci.*** We will now study the total supersingular locus of $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0}$, that is, the maximal closed subset where the universal p-divisible group $\mathcal{A}'_{\tilde{\mathtt{S}}}[p^\infty]$ is supersingular. Put

$$\mathfrak{B}_{\mathtt{S}} := \{\underline{\mathfrak{a}} = (\mathfrak{a}_\mathfrak{p})_{\mathfrak{p}\in\Sigma_p} \mid \mathfrak{a}_\mathfrak{p} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, \lfloor d_\mathfrak{p}/2\rfloor)\},$$

and $r := \sum_{\mathfrak{p}\in\Sigma_p}\lfloor d_\mathfrak{p}/2\rfloor$. We attach to each $\underline{\mathfrak{a}}$ an r-dimensional closed subvariety $W'_{\tilde{\mathtt{S}}}(\underline{\mathfrak{a}}) \subseteq \mathbf{Sh}_{K'}(G'_{\tilde{\mathtt{S}}})_{k_0}$ as follows. We write $\Sigma_p = \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$, that is, we choose an order for the elements of Σ_p. We put $\mathtt{S}_1 := \mathtt{S}_{\mathfrak{a}_{\mathfrak{p}_1}}$ and $\tilde{\mathtt{S}}^*_1 := \tilde{\mathtt{S}}^*_{\mathfrak{a}_{\mathfrak{p}_1}}$ (see (3-4)); put inductively $\mathtt{S}_{i+1} := (\mathtt{S}_i)_{\mathfrak{a}_{\mathfrak{p}_{i+1}}}$, $\tilde{\mathtt{S}}^*_{i+1} = (\tilde{\mathtt{S}_i})^*_{\mathfrak{a}_{\mathfrak{p}_{i+1}}}$ for $1 \le i \le m-1$; and finally put $\mathtt{S}_{\underline{\mathfrak{a}}} := \mathtt{S}_m$ and $\tilde{\mathtt{S}}^*_{\underline{\mathfrak{a}}} := \tilde{\mathtt{S}}^*_m$. For $\mathfrak{a}_{\mathfrak{p}_1} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, \lfloor d_{\mathfrak{p}_1}/2\rfloor)$, we have constructed a $\lfloor d_{\mathfrak{p}_1}/2\rfloor$-th iterated $\mathbb{P}^1$-fibration

$$\pi'_{\mathfrak{a}_{\mathfrak{p}_1}}|_{W'_{\tilde{\mathtt{S}}}(\mathfrak{a}_{\mathfrak{p}_1})} : W'_{\tilde{\mathtt{S}}}(\mathfrak{a}_{\mathfrak{p}_1}) \to \mathbf{Sh}(G'_{\tilde{\mathtt{S}}^*_1}, K'^p)_{k_0}.$$

Now, applying the construction to $\mathfrak{a}_{\mathfrak{p}_2} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}_2}, \lfloor d_{\mathfrak{p}_2}/2\rfloor)$ and $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}^*_1}, K'^p)_{k_0}$, we have a closed subvariety $W'_{\tilde{\mathtt{S}}^*_1}(\mathfrak{a}_{\mathfrak{p}_2}) \subseteq \mathbf{Sh}(G'_{\tilde{\mathtt{S}}^*_1}, K'^p)_{k_0}$ of codimension $\lceil d_{\mathfrak{p}_2}/2\rceil$. We put

$$W'_{\tilde{\mathtt{S}}}(\mathfrak{a}_{\mathfrak{p}_1}, \mathfrak{a}_{\mathfrak{p}_2}) := (\pi'_{\mathfrak{a}_{\mathfrak{p}_1}})^{-1}(W'_{\tilde{\mathtt{S}}^*_1}(\mathfrak{a}_{\mathfrak{p}_2})).$$

Then there exists a canonical projection

$$\pi'_{\mathfrak{a}_{\mathfrak{p}_1},\mathfrak{a}_{\mathfrak{p}_2}} : W'_{\tilde{\mathtt{S}}}(\mathfrak{a}_{\mathfrak{p}_1}, \mathfrak{a}_{\mathfrak{p}_2}) \xrightarrow{\pi'_{\mathfrak{a}_{\mathfrak{p}_1}}|_{W'_{\tilde{\mathtt{S}}}(\mathfrak{a}_{\mathfrak{p}_1},\mathfrak{a}_{\mathfrak{p}_2})}} W'_{\tilde{\mathtt{S}}^*_1}(\mathfrak{a}_{\mathfrak{p}_2}) \xrightarrow{\pi'_{\mathfrak{a}_{\mathfrak{p}_2}}|_{W'_{\tilde{\mathtt{S}}^*_1}(\mathfrak{a}_{\mathfrak{p}_2})}} \mathbf{Sh}(G'_{\tilde{\mathtt{S}}^*_2}, K'^p)_{k_0}.$$

Repeating this construction, we finally get a closed subvariety $W'_{\tilde{\mathtt{S}}}(\underline{\mathfrak{a}}) \subseteq \mathbf{Sh}(G'_{\tilde{\mathtt{S}}}, K'^p)_{k_0}$ of codimension $\sum_{\mathfrak{p}\in\Sigma}\lceil d_\mathfrak{p}/2\rceil$ together with a canonical projection

$$\pi'_{\underline{\mathfrak{a}}} : W'_{\tilde{\mathtt{S}}}(\underline{\mathfrak{a}}) \to \mathbf{Sh}(G'_{\tilde{\mathtt{S}}^*_{\underline{\mathfrak{a}}}}, K'^p)_{k_0}.$$

Note that the underlying set $\mathtt{S}^*_{\underline{\mathfrak{a}}}$ of $\tilde{\mathtt{S}}^*_{\underline{\mathfrak{a}}}$ is independent of $\underline{\mathfrak{a}} \in \mathfrak{B}_{\mathtt{S}}$, namely all of them are equal to

$$\mathtt{S}_{\max} := \Sigma_\infty \cup \{\mathfrak{p} \in \Sigma_p \mid g_\mathfrak{p} := [F_\mathfrak{p} : \mathbb{Q}_p] \text{ is odd}\}. \tag{3-7}$$

Thus $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}^*_{\underline{\mathfrak{a}}}}, K'^p)_{k_0}$ is a Shimura variety of dimension 0, and $\pi'_{\underline{\mathfrak{a}}}$ is by construction an r-th iterated $\mathbb{P}^1$-fibration over $\mathbf{Sh}(G'_{\tilde{\mathtt{S}}^*_{\underline{\mathfrak{a}}}}, K'^p)_{k_0}$. We note that $W'_{\tilde{\mathtt{S}}}(\underline{\mathfrak{a}})$ does not depend on the order $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ of the places of F above p.

Theorem 3.6. *The total supersingular locus of* $\mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)_{k_0}$ *is given by*

$$\mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)^{\mathrm{ss}}_{k_0} := \bigcup_{\underline{\mathfrak a}\in\mathfrak B_{\mathtt S}} W'_{\tilde{\mathtt S}}(\underline{\mathfrak a}),$$

where each $W'_{\tilde{\mathtt S}}(\underline{\mathfrak a})$ *is a* $\sum_{\mathfrak p\in\Sigma_p}\lfloor d_{\mathfrak p}/2\rfloor$*-th iterated* $\mathbb P^1$*-fibration over some discrete Shimura variety* $\mathbf{Sh}(G'_{\tilde{\mathtt S}^*_{\underline{\mathfrak a}}}, K'^p)_{k_0}$*. In particular,* $\mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)^{\mathrm{ss}}_{k_0}$ *is proper and of equidimension* $\sum_{\mathfrak p\in\Sigma_p}\lfloor d_{\mathfrak p}/2\rfloor$.

Proof. This follows immediately from Theorem 3.3 by induction on the number of p-adic places $\mathfrak p\in\Sigma_p$ such that $d_{\mathfrak p}\neq 0$. □

Remark 3.7. It is clear that the total supersingular locus is the intersection of all $\mathfrak p$-supersingular loci for $\mathfrak p\in\Sigma_p$. It follows that

$$W'_{\tilde{\mathtt S}}(\underline{\mathfrak a}) = \bigcap_{\mathfrak p\in\Sigma_p} W'_{\tilde{\mathtt S}}(\mathfrak a_{\mathfrak p}),$$

and the intersection is transversal.

Similarly to Definition 3.4, we define the total superspecial locus of $\mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)_{k_0}$ as

$$\mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)^{\mathrm{sp}}_{k_0} := \mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)_{k_0,\Sigma_\infty} = \bigcap_{\mathfrak p\in\Sigma_p} \mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)^{\mathfrak p-\mathrm{sp}}_{k_0}.$$

We have the following analogue of Proposition 3.5.

Proposition 3.8. *Suppose that* $d_{\mathfrak p}$ *is odd for all* $\mathfrak p\in\Sigma_p$*. Then for each* $\underline{\mathfrak a}\in\mathfrak B_{\mathtt S}$*,* $W'_{\tilde{\mathtt S}}(\underline{\mathfrak a})$ *contains* $\mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)^{\mathrm{sp}}_{k_0}$*, and each geometric irreducible component of* $W'_{\tilde{\mathtt S}}(\underline{\mathfrak a})$ *contains exactly one point of* $\mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)^{\mathrm{sp}}_{k_0}$*. In other words, the restriction of* $\pi'_{\underline{\mathfrak a}}$ *induces an isomorphism*

$$\mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)^{\mathrm{sp}}_{k_0} \xrightarrow{\sim} \mathbf{Sh}(G'_{\tilde{\mathtt S}^*_{\underline{\mathfrak a}}}, K'^p)_{k_0}.$$

Proof. This follows immediately from Proposition 3.5. □

3G. ***Applications to quaternionic Shimura varieties.*** Denote by $\mathbf{Sh}(G_{\mathtt S,\mathtt T}, K^p)$ the integral model of $\mathrm{Sh}(G_{\mathtt S,\mathtt T}, K^p)$ over $\mathcal O_{F_{\mathtt S,\mathtt T},\wp}$ induced by $\mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)$. We assume that the residue field of $\mathcal O_{F_{\mathtt S,\mathtt T},\wp}$ is contained in k_0 (e.g., $\mathtt S=\mathtt T=\varnothing$), and put $\mathbf{Sh}(G_{\mathtt S,\mathtt T}, K^p)_{k_0} := \mathbf{Sh}(G_{\mathtt S,\mathtt T}, K^p)\otimes_{\mathcal O_{F_{\mathtt S,\mathtt T},\wp}} k_0$. As in [Tian and Xiao 2016; 2019], the construction of Goren–Oort divisors can be transferred to $\mathbf{Sh}(G_{\mathtt S,\mathtt T}, K^p)_{k_0}$ for a sufficiently small open compact subgroup $K^p\subseteq G_{\mathtt S}(\mathbb A^{\infty,p})$.

Consider first the connected Shimura variety $\mathbf{Sh}(G_{\mathtt S,\mathtt T})^\circ_{\mathbb F_p^{\mathrm{ac}}} := \mathbf{Sh}(G_{\mathtt S,\mathtt T})^\circ_{\mathbb Z_p^{\mathrm{ur}}}\otimes_{\mathbb Z_p^{\mathrm{ur}}}\mathbb F_p^{\mathrm{ac}}$. For each $\tau\in\Sigma_\infty$, the Goren–Oort divisor $\mathbf{Sh}(G'_{\tilde{\mathtt S}})_{k_0,\tau} = \varprojlim_{K'^p}\mathbf{Sh}(G'_{\tilde{\mathtt S}}, K'^p)_{k_0,\tau}$ induces a divisor $\mathbf{Sh}(G'_{\tilde{\mathtt S}})^\circ_{\mathbb F_p^{\mathrm{ac}},\tau}$ on $\mathbf{Sh}(G'_{\tilde{\mathtt S}})^\circ_{\mathbb F_p^{\mathrm{ac}}}$. By the canonical isomorphism

$$\mathbf{Sh}(G_{\mathtt S,\mathtt T})^\circ_{\mathbb F_p^{\mathrm{ac}}} \cong \mathbf{Sh}(G'_{\tilde{\mathtt S}})^\circ_{\mathbb F_p^{\mathrm{ac}}}$$

from Section 2F and Deligne's recipe of recovering $\mathbf{Sh}(G_{\mathtt S,\mathtt T})_{\mathbb F_p^{\mathrm{ac}}}$ from $\mathbf{Sh}(G_{\mathtt S,\mathtt T})^\circ_{\mathbb F_p^{\mathrm{ac}}}$ [Tian and Xiao 2016, Corollary 2.13], the divisor $\mathbf{Sh}(G_{\mathtt S,\mathtt T})^\circ_{\mathbb F_p^{\mathrm{ac}},\tau}$ induces a divisor $\mathbf{Sh}(G_{\mathtt S,\mathtt T})_{\mathbb F_p^{\mathrm{ac}},\tau}$ on $\mathbf{Sh}(G_{\mathtt S,\mathtt T})_{\mathbb F_p^{\mathrm{ac}}}$. By Galois descent, one gets a divisor $\mathbf{Sh}(G_{\mathtt S,\mathtt T})_{k_0,\tau}$ on $\mathbf{Sh}(G_{\mathtt S,\mathtt T})_{k_0}$, which is stable under prime-to-p Hecke action.

Finally, we define the Goren–Oort divisors on $\mathbf{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)_{k_0}$ as the image of Goren–Oort divisors on $\mathbf{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)_{k_0}$ via the natural projection $\mathbf{Sh}(G_{\mathtt{S},\mathtt{T}})_{k_0} \to \mathbf{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)_{k_0}$.

Proposition 3.9. *Take $\tau \in \Sigma_{\infty/\mathfrak{p}}$ for some $\mathfrak{p} \in \Sigma_p$, and put $\mathtt{T}_\tau := \mathtt{T} \cup \{\tau\}$. There exists a morphism of k_0-schemes*

$$\pi_\tau \colon \mathbf{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)_{k_0,\tau} \to \mathbf{Sh}(G_{\mathtt{S}_\tau,\mathtt{T}_\tau}, K^p)_{k_0},$$

where $\mathtt{S}_\tau$ was defined in (3-2), *such that*

(1) *it is compatible with π'_τ in Proposition 3.2 on neutral geometric connected components*;

(2) *it is an isomorphism if $\Sigma_{\infty/\mathfrak{p}} = \mathtt{S}_{\infty/\mathfrak{p}} \cup \{\tau\}$; and*

(3) *it is a $\mathbb{P}^1$-fibration.*

Proof. This follows immediately from Proposition 3.2 and [Tian and Xiao 2019, Construction 2.12]. □

Now, the construction of Goren–Oort cycles can be transferred to the quaternionic Shimura variety $\mathbf{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)_{k_0}$. For a periodic semimeander $\mathfrak{a} \in \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, \lfloor d_\mathfrak{p}/2 \rfloor)$, we construct inductively in the same way as $Z'_{\underline{\mathtt{S}}}(\mathfrak{a})$ a closed k_0-subvariety $Z_{\mathtt{S},\mathtt{T}}(\mathfrak{a}) \subseteq \mathbf{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)_{k_0}$ such that there exists a $\lfloor d_\mathfrak{p}/2 \rfloor$-th iterated $\mathbb{P}^1$-fibration

$$\pi_\mathfrak{a} \colon Z_{\mathtt{S},\mathtt{T}}(\mathfrak{a}) \to \mathbf{Sh}(G_{\mathtt{S}_\mathfrak{a},\mathtt{T}_\mathfrak{a}}, K^p)_{k_0}$$

according to Proposition 3.9, where $\mathtt{S}_\mathfrak{a}$ is defined in (3-3) and

$$\mathtt{T}_\mathfrak{a} = \mathtt{T} \cup \{\tau \in \Sigma_\infty \mid \tau \text{ is the right end point of an arc in } \mathfrak{a}\}. \tag{3-8}$$

We define similarly

$$W_{\mathtt{S},\mathtt{T}}(\mathfrak{a}) = \begin{cases} Z_{\mathtt{S},\mathtt{T}}(\mathfrak{a}) & \text{if } d_\mathfrak{p} \text{ is even,} \\ \pi_\mathfrak{a}^{-1}(\mathbf{Sh}(G_{\mathtt{S}_\mathfrak{a},\mathtt{T}_\mathfrak{a}}, K^p)_{k_0,\tau(\mathfrak{a})}) & \text{if } d_\mathfrak{p} \text{ is odd,} \end{cases} \tag{3-9}$$

where $\tau(\mathfrak{a}) \in \Sigma_{\infty/\mathfrak{p}}$ is the end point of the unique semiline of $\mathfrak{a}$. Then $\pi_\mathfrak{a}$ induces a $\lfloor d_\mathfrak{p}/2 \rfloor$-th iterated $\mathbb{P}^1$-fibration

$$\pi_\mathfrak{a}|_{W_{\mathtt{S},\mathtt{T}}(\mathfrak{a})_{\mathbb{F}_p^{\mathrm{ac}}}} \colon W_{\mathtt{S},\mathtt{T}}(\mathfrak{a})_{\mathbb{F}_p^{\mathrm{ac}}} \to \mathbf{Sh}(G_{\mathtt{S}(\mathfrak{p}),\mathtt{T}^*_\mathfrak{a}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$$

where $\mathtt{S}(\mathfrak{p}) = \mathtt{S}^*_\mathfrak{a}$ is defined in (3-5), and

$$\mathtt{T}^*_\mathfrak{a} = \begin{cases} \mathtt{T}_\mathfrak{a} & \text{if } d_\mathfrak{p} \text{ is even,} \\ \mathtt{T}_\mathfrak{a} \cup \{\tau(\mathfrak{a})\} & \text{if } d_\mathfrak{a} \text{ is odd.} \end{cases}$$

Of course, when $d_\mathfrak{p}$ is even, the morphism $\pi_\mathfrak{a}|_{W_{\mathtt{S},\mathtt{T}}(\mathfrak{a})_{\mathbb{F}_p^{\mathrm{ac}}}}$ is simply the base change to $\mathbb{F}_p^{\mathrm{ac}}$ of $\pi_\mathfrak{a}$.

Similarly, for $\underline{\mathfrak{a}} = (\mathfrak{a}_\mathfrak{p})_{\mathfrak{p} \in \Sigma_p} \in \mathfrak{B}_\mathtt{S} = \prod_{\mathfrak{p} \in \Sigma_p} \mathfrak{B}(\mathtt{S}_{\infty/\mathfrak{p}}, \lfloor d_\mathfrak{p}/2 \rfloor)$, we can define a closed subvariety $W_{\mathtt{S},\mathtt{T}}(\underline{\mathfrak{a}}) \subseteq \mathbf{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)_{k_0}$ of dimension $r = \sum_{\mathfrak{p} \in \Sigma_p} \lfloor d_\mathfrak{p}/2 \rfloor$ together with an r-th iterated $\mathbb{P}^1$-fibration

$$\pi_{\underline{\mathfrak{a}}} \colon W_{\mathtt{S},\mathtt{T}}(\underline{\mathfrak{a}})_{\mathbb{F}_p^{\mathrm{ac}}} \to \mathbf{Sh}(G_{\mathtt{S}_{\max},\mathtt{T}^*_{\underline{\mathfrak{a}}}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}},$$

where $\mathtt{S}_{\max}$ was defined in (3-7), and $\mathtt{T}^*_{\underline{\mathfrak{a}}} := \bigcup_{\mathfrak{p} \in \Sigma_p} \mathtt{T}^*_{\mathfrak{a}_\mathfrak{p}}$.

Notation 3.10. In what follows, we will write the $\mathbb{F}_p^{\mathrm{ac}}$-schemes $\mathbf{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p) \otimes_{\mathcal{O}_{F_{\mathtt{S},\mathtt{T}},\wp}} \mathbb{F}_p^{\mathrm{ac}}$ and the sets $\mathbf{Sh}(G_{\mathtt{S},\mathtt{T}}, K^p)(\mathbb{F}_p^{\mathrm{ac}})$, which are independent of $\mathtt{T}$, simply by $\mathbf{Sh}(G_{\mathtt{S}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$ and $\mathbf{Sh}(G_{\mathtt{S}}, K^p)(\mathbb{F}_p^{\mathrm{ac}})$, respectively.

Then the target of $\pi_{\underline{\mathfrak{a}}}$ is simply $\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$ for every $\underline{\mathfrak{a}} \in \mathfrak{B}_{\mathtt{S}}$. In particular, the set of geometric irreducible components of $W_{\mathtt{S},\mathtt{T}}(\mathfrak{a})$ is in bijection with $\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)(\mathbb{F}_p^{\mathrm{ac}})$. Moreover, we have an isomorphism

$$\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)(\mathbb{F}_p^{\mathrm{ac}}) \cong B_{\mathtt{S}_{\max}}^{\times} \backslash \hat{B}_{\mathtt{S}_{\max}}^{\times} / K^p \prod_{\mathfrak{p} \in \Sigma_p} K_{\mathfrak{p}}^{\max},$$

where $K_{\mathfrak{p}}^{\max}$ is the unique maximal open compact subgroups of $(B_{\mathtt{S}_{\max}} \otimes_F F_{\mathfrak{p}})^{\times}$ for each $\mathfrak{p} \in \Sigma_p$. Note that $B_{\mathtt{S}_{\max}}$ splits (resp. ramifies) at $\mathfrak{p}$ if $g_{\mathfrak{p}}$ is even (resp. odd).

3H. ***Totally indefinite quaternionic Shimura varieties.*** We consider the case $\mathtt{S} = \varnothing$ (hence $\mathtt{T} = \varnothing$), and we write $G = G_{\varnothing} = G_{\varnothing,\varnothing}$ and $G' = G'_{\tilde{\varnothing}}$ for simplicity as usual. Recall that $\mathbf{Sh}(G, K^p)$ classifies tuples $(A, \iota, \bar{\lambda}, \bar{\alpha}_{K^p})$ as defined in Section 2E. Even though it is only a coarse moduli space, there still exists a universal abelian scheme $\mathcal{A}$ over $\mathbf{Sh}(G, K^p)$ (See Remark 2.9(1)).

Definition 3.11. Put $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p} := \mathbf{Sh}(G, K^p) \otimes \mathbb{F}_p$:

(1) For each $\mathfrak{p} \in \Sigma_p$, we define the $\mathfrak{p}$-*supersingular locus* of $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}$ as the maximal reduced closed subscheme of $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}$ where the universal $\mathfrak{p}$-divisible group $\mathcal{A}[\mathfrak{p}^\infty]$ is supersingular.

(2) We define the *total supersingular locus* of $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}$ as the intersection of the $\mathfrak{p}$-supersingular locus for all $\mathfrak{p} \in \Sigma_p$.

Theorem 3.12. *For* $\mathfrak{p} \in \Sigma_p$, *put* $g_{\mathfrak{p}} := [F_{\mathfrak{p}} : \mathbb{Q}_p]$. *Then the* $\mathfrak{p}$-*supersingular locus of* $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}$, *after base change to* k_0, *is*

$$\bigcup_{\mathfrak{a} \in \mathfrak{B}(\varnothing_{\infty/\mathfrak{p}}, \lfloor g_{\mathfrak{p}}/2 \rfloor)} W_{\varnothing,\varnothing}(\mathfrak{a}),$$

where $\mathfrak{B}(\varnothing_{\infty/\mathfrak{p}}, \lfloor g_{\mathfrak{p}}/2 \rfloor)$ *is the set of periodic semimeanders of* $g_{\mathfrak{p}}$-*nodes and* $\lfloor g_{\mathfrak{p}}/2 \rfloor$-*arcs, and each* $W_{\varnothing,\varnothing}(\mathfrak{a})$ *is defined in* (3-9) *and* $W_{\varnothing,\varnothing}(\mathfrak{a})_{\mathbb{F}_p^{\mathrm{ac}}}$ *is a* $\lfloor g_{\mathfrak{p}}/2 \rfloor$-*th iterated* $\mathbb{P}^1$-*fibration over* $\mathbf{Sh}(G_{\varnothing(\mathfrak{p})}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$.

Proof. According to the discussion of Section 2F, the definition of the $\mathfrak{p}$-supersingular locus of $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}$ using the universal family $\mathcal{A}$ coincides with the one induced from the $\mathfrak{p}$-supersingular locus of the unitary Shimura variety $\mathbf{Sh}(G', K'^p)_{\mathbb{F}_p}$. The statement then follows from Theorem 3.3. □

Theorem 3.13. *Denote by* $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}^{\mathrm{ss}}$ *the total supersingular locus of* $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}$. *Then we have*

$$\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}^{\mathrm{ss}} \otimes k_0 = \bigcup_{\underline{\mathfrak{a}} \in \mathfrak{B}_{\varnothing}} W_{\varnothing,\varnothing}(\underline{\mathfrak{a}}),$$

where $\mathfrak{B}_{\varnothing}$ *is the set of tuples* $(\mathfrak{a}_{\mathfrak{p}})_{\mathfrak{p} \in \Sigma_p}$ *with* $\mathfrak{a}_{\mathfrak{p}} \in \mathfrak{B}(\varnothing_{\infty/\mathfrak{p}}, \lfloor g_{\mathfrak{p}}/2 \rfloor)$. *The base change* $W_{\varnothing,\varnothing}(\mathfrak{a})_{\mathbb{F}_p^{\mathrm{ac}}}$ *of* $W_{\varnothing,\varnothing}(\underline{\mathfrak{a}})$ *to* $\mathbb{F}_p^{\mathrm{ac}}$ *is a* $\left(\sum_{\mathfrak{p} \in \Sigma_p} \lfloor g_{\mathfrak{p}}/2 \rfloor\right)$-*th iterated* $\mathbb{P}^1$-*fibration over* $\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$, *equivariant under prime-to-p Hecke correspondences, where* $\mathtt{S}_{\max}$ *was defined in* (3-7). *In particular*, $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}^{\mathrm{ss}}$ *is proper and of equidimension* $\sum_{\mathfrak{p} \in \Sigma_p} \lfloor g_{\mathfrak{p}}/2 \rfloor$.

Proof. This follows from Theorem 3.12 by induction on the number of p-adic places $\mathfrak{p} \in \Sigma_p$. □

Remark 3.14. The above theorem is known in the following cases:

(1) If p is inert in F of degree 2 and B is the matrix algebra, then the theorem was first proved in [Bachmat and Goren 1999].

(2) If p is inert in F of degree 4 and B is the matrix algebra, then the results was due to [Yu 2003].

(3) Assume that p is inert in F of even degree. Then the strata $W_{\varnothing,\varnothing}(\underline{\mathfrak{a}})$ have already been constructed in [Tian and Xiao 2019], and the authors proved there that, under certain genericity conditions on the Satake parameters of a fixed automorphic cuspidal representation π, the cycles $W_{\varnothing,\varnothing}(\underline{\mathfrak{a}})$ give all the π-isotypic Tate cycles on the quaternionic Shimura variety $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}$.

We define an action of $\mathrm{G}_{\mathbb{F}_p} = \mathrm{Gal}(\mathbb{F}_p^{\mathrm{ac}}/\mathbb{F}_p)$ on the set $\mathfrak{B}_\varnothing$ as follows. For each periodic semimeander $\mathfrak{a}_\mathfrak{p} \in \mathfrak{B}(\varnothing_{\infty/\mathfrak{p}}, \lfloor g_\mathfrak{p}/2 \rfloor)$, let $\sigma(\mathfrak{a}_\mathfrak{p})$ be the Frobenius translate of $\mathfrak{a}_\mathfrak{p}$, that is, there is an arc in $\sigma(\mathfrak{a}_\mathfrak{p})$ linking two nodes x, y if and only if there is an arc in $\mathfrak{a}_\mathfrak{p}$ linking $\sigma^{-1}(x), \sigma^{-1}(y)$. For $\underline{\mathfrak{a}} = (\mathfrak{a}_\mathfrak{p})_\mathfrak{p}$, we put $\sigma(\underline{\mathfrak{a}}) := (\sigma(\mathfrak{a}_\mathfrak{p}))_{\mathfrak{p}\in\Sigma_p}$. It is clear that the subgroup $\mathrm{Gal}(\mathbb{F}_p^{\mathrm{ac}}/k_0)$ of $\mathrm{Gal}(\mathbb{F}_p^{\mathrm{ac}}/\mathbb{F}_p)$ stabilizes each $\underline{\mathfrak{a}} \in \mathfrak{B}_\varnothing$. Then the action of $\mathrm{Gal}(\mathbb{F}_p^{\mathrm{ac}}/\mathbb{F}_p)$ on $\mathbf{Sh}(G, K^p)^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}$ sends the stratum $W_{\varnothing,\varnothing}(\underline{\mathfrak{a}})$ to $W_{\varnothing,\varnothing}(\sigma(\underline{\mathfrak{a}}))$.

Definition 3.15. We define the *superspecial locus* of $\mathbf{Sh}(G, K^p)_{\mathbb{F}_p}$, denoted by $\mathbf{Sh}(G, K^p)^{\mathrm{sp}}_{\mathbb{F}_p}$, to be the maximal reduced closed subscheme S such that for any geometric point $\bar{x} \to S$ the abelian variety $\mathcal{A}_{\bar{x}}$ is superspecial, that is, $\mathcal{A}_{\bar{x}}$ is isomorphic to a product of supersingular elliptic curves.

Using the universal family of abelian varieties $\mathcal{A}$ over $\mathbf{Sh}(G, K^p)$, one can define, for each $\tau \in \Sigma_\infty$, a partial Hasse invariant h_τ on $\mathbf{Sh}(G, K^p)_{k_0}$ similarly to (3-1). We can also define the Goren–Oort divisor $\mathbf{Sh}(G, K^p)_{k_0,\tau}$ of $\mathbf{Sh}(G, K^p)_{k_0}$ as being the vanishing locus of h_τ. By the relation of universal abelian schemes (2-5), this definition of Goren–Oort divisor coincides with the one defined by transferring to the unitary Shimura variety $\mathbf{Sh}(G', K'^p)_{k_0}$. It is easy to see that

$$\mathbf{Sh}(G, K^p)^{\mathrm{sp}}_{\mathbb{F}_p} \otimes k_0 = \bigcap_{\tau\in\Sigma_\infty} \mathbf{Sh}(G, K^p)_{k_0,\tau}.$$

Theorem 3.16. *Assume that $g_\mathfrak{p}$ is odd for every $\mathfrak{p} \in \Sigma_p$:*

(1) *For each $\underline{\mathfrak{a}} \in \mathfrak{B}_\varnothing$ as in Theorem 3.13, $W_{\varnothing,\varnothing}(\underline{\mathfrak{a}})$ contains the superspecial locus $\mathbf{Sh}(G, K^p)^{\mathrm{sp}}_{\mathbb{F}_p} \otimes k_0$, and the morphism $\pi_{\underline{\mathfrak{a}}} \colon W_{\varnothing,\varnothing}(\underline{\mathfrak{a}})_{\mathbb{F}_p^{\mathrm{ac}}} \to \mathbf{Sh}(G_{\mathrm{S}_{\max}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$ induces a bijection*

$$\mathbf{Sh}(G, K^p)^{\mathrm{sp}}(\mathbb{F}_p^{\mathrm{ac}}) \xrightarrow{\sim} \mathbf{Sh}(G_{\mathrm{S}_{\max}}, K^p)(\mathbb{F}_p^{\mathrm{ac}}) \simeq B^\times_{\mathrm{S}_{\max}} \backslash \hat{B}^\times_{\max} / K^p \prod_{\mathfrak{p}\in\Sigma_p} K^{\max}_\mathfrak{p}$$

compatible with prime-to-p Hecke correspondences.

(2) *For each $\mathfrak{p} \in \Sigma_p$, let $\Pi_\mathfrak{p}$ be a uniformizer of the quaternion division algebra $B_{\mathrm{S}_{\max}} \otimes_F F_\mathfrak{p}$. Let $\underline{\Pi}_p$ be the element of $\hat{B}^\times_{\mathrm{S}_{\max}}$ whose $\mathfrak{p}$-component is $\Pi_\mathfrak{p}$ for each $\mathfrak{p} \in \Sigma_p$ and other components are* 1. *Then under the bijection in* (1), *the action of the arithmetic Frobenius element $\sigma_p \in \mathrm{Gal}(\mathbb{F}_p^{\mathrm{ac}}/\mathbb{F}_p)$ on $\mathbf{Sh}(G, K^p)^{\mathrm{sp}}(\mathbb{F}_p^{\mathrm{ac}})$ is induced by the right multiplication by $\underline{\Pi}_p^{-1}$ on $\hat{B}^\times_{\max}$.*

Proof. Statement (1) follows from Proposition 3.8.

To prove (2), we take a superspecial point $x = (A, \iota, \bar{\lambda}, \bar{\alpha}_{K^p}) \in \mathbf{Sh}(G, K^p)^{\mathrm{sp}}(\mathbb{F}_p^{\mathrm{ac}})$ as in Section 2E. Then A is of the form $A = C \otimes_{\mathbb{Z}} \mathcal{I}$, where C is a supersingular elliptic curve and $\mathcal{I}$ is a (left) fractional ideal of $\mathcal{O}_B$. For each $\mathfrak{p} \in \Sigma_p$, we have an equality of p-divisible groups $A[\mathfrak{p}^\infty] = C[p^\infty] \otimes_{\mathbb{Z}_p} \mathcal{I}_\mathfrak{p}$, and hence an equality

$$\mathcal{D}(A[\mathfrak{p}^\infty]) = \mathcal{D}(A[p^\infty]) \otimes_{\mathbb{Z}_p} \mathcal{I}_\mathfrak{p}$$

for the corresponding covariant Dieudonné modules. Let B_p be the unique quaternion division algebra over $\mathbb{Q}_p$. Then we have $\mathrm{End}(C[p^\infty]) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = B_p$ and

$$B_p \otimes_{\mathbb{Q}_p} F_\mathfrak{p} = B_{\max} \otimes_F F_\mathfrak{p} = \mathrm{End}_{\mathcal{O}_B}(A[\mathfrak{p}^\infty]) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Let $\Pi \in B_p$ denote a uniformizer of B_p, and we view it also as a uniformizer of $B_{\max} \otimes_F F_\mathfrak{p}$. Via p-Frobenius isogeny $F_C : C \to C^{(p)}$, $\mathcal{D}(C^{(p)}[p^\infty])$ is identified with lattice $\Pi^{-1}\mathcal{D}(C[p^\infty])$ in $\mathcal{D}(C[p^\infty])[1/p]$. Since $F_A : A \to A^{(p)}$ is induced from F_C by tensoring with $\mathcal{I}$, we see that F_A allows us to identify $\mathcal{D}(A^{(p)}[\mathfrak{p}^\infty])$ with the lattice $\Pi^{-1}\mathcal{D}(A[\mathfrak{p}^\infty])$ inside $\mathcal{D}(A[\mathfrak{p}^\infty])[1/p]$. Since $\sigma_p(x)$ is given by $A^{(p)}$ together with the induced polarization and level structure, the description for σ_p on $\mathbf{Sh}(G, K^p)^{\mathrm{sp}}(\bar{\mathbb{F}}_p)$ follows. □

Note that the action of $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ on $\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)(\bar{\mathbb{F}}_p)$ defined in Theorem 3.16(2) is independent of $\underline{\mathfrak{a}} \in \mathfrak{B}_\varnothing$. In other words, we have a canonical $\mathbb{F}_p$-scheme structure on $\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$, which we denote by $\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)$.

Corollary 3.17. *Assume that $g_\mathfrak{p}$ is odd for every $\mathfrak{p} \in \Sigma_p$. For every $\underline{\mathfrak{a}} \in \mathfrak{B}_\varnothing$, the morphism $\pi_{\underline{\mathfrak{a}}} : W_{\varnothing,\varnothing}(\underline{\mathfrak{a}})_{\mathbb{F}_p^{\mathrm{ac}}} \to \mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$ is equivariant under* $\mathrm{Gal}(\mathbb{F}_p^{\mathrm{ac}}/k_0)$, *hence it descends to a morphism of k_0-schemes*:

$$\pi_{\underline{\mathfrak{a}}} : W_{\varnothing,\varnothing}(\underline{\mathfrak{a}}) \to \mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)_{k_0}.$$

Proof. This follows from the definition of underlying k_0-structure on $\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}$ and the fact that the inclusion $\mathbf{Sh}(G, K^p)^{\mathrm{sp}}_{\mathbb{F}_p^{\mathrm{ac}}} \hookrightarrow W_{\varnothing,\varnothing}(\underline{\mathfrak{a}})_{\mathbb{F}_p^{\mathrm{ac}}}$ is equivariant under $\mathrm{Gal}(\mathbb{F}_p^{\mathrm{ac}}/k_0)$. □

4. Arithmetic level raising

In this section, we state and prove the arithmetic level raising result. We suppose that $g = [F : \mathbb{Q}]$ is odd. Fix an irreducible cuspidal automorphic representation Π of $\mathrm{GL}_2(\mathbb{A}_F)$ of parallel weight 2 defined over a number field $\mathbb{E}$.

4A. ***Statement of arithmetic level raising.*** Let B be a totally indefinite quaternion algebra over F, and put $G := \mathrm{Res}_{F/\mathbb{Q}} B^\times$. Let K be a neat open compact subgroup of $G(\mathbb{A}^\infty)$ (Definition 2.6) such that $(\Pi^\infty)^K \neq 0$. We have the Shimura variety $\mathrm{Sh}(G, K)$ defined over $\mathbb{Q}$ whose $\mathbb{C}$-points are given by

$$\mathrm{Sh}(G, K)(\mathbb{C}) = G(\mathbb{Q}) \backslash (\mathfrak{H}^\pm)^{\Sigma_\infty} \times G(\mathbb{A}^\infty)/K.$$

Let $\mathtt{R}$ be a finite set of places of F away from which K is hyperspecial maximal.[4] Let $\mathbb{T}^{\mathtt{R}}$ be the Hecke monoid away from $\mathtt{R}$ [Liu 2019, Notation 3.1] (that is, the commutative monoid generated by $\mathrm{T}_{\mathfrak{q}}$, $\mathrm{S}_{\mathfrak{q}}$, $\mathrm{S}_{\mathfrak{q}}^{-1}$ with the relation $\mathrm{S}_{\mathfrak{q}}\mathrm{S}_{\mathfrak{q}}^{-1} = 1$ for all primes $\mathfrak{q} \notin \mathtt{R}$). Then Π induces a homomorphism

$$\phi_{\Pi}^{\mathtt{R}} : \mathbb{Z}[\mathbb{T}^{\mathtt{R}}] \to \mathcal{O}_{\mathbb{E}}$$

by its Hecke eigenvalues. For every prime λ of $\mathbb{E}$, we have an attached Galois representation

$$\rho_{\Pi,\lambda} : \mathrm{G}_F = \mathrm{Gal}(F^{\mathrm{ac}}/F) \to \mathrm{GL}_2(\mathcal{O}_{\mathbb{E}_\lambda}) \tag{4-1}$$

which is unramified outside $\mathtt{R} \cup \mathtt{R}_\lambda$, where $\mathtt{R}_\lambda$ denotes the subset of all places of F with the same residue characteristic as λ. The Galois representation $\rho_{\Pi,\lambda}$ is normalized so that if $\sigma_{\mathfrak{q}}$ denotes an *arithmetic* Frobenius element at $\mathfrak{q}$ for a place $\mathfrak{q} \notin \mathtt{R} \cup \mathtt{R}_\lambda$, then the characteristic polynomial of $\rho_{\Pi,\lambda}(\sigma_{\mathfrak{q}})$ is given by

$$X^2 - \phi_{\Pi}^{\mathtt{R}}(\mathrm{T}_{\mathfrak{q}})X + \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{q})\phi_{\Pi}^{\mathtt{R}}(\mathrm{S}_{\mathfrak{q}}).$$

Let $\mathfrak{m}_{\Pi,\lambda}^{\mathtt{R}}$ be the kernel of the composite map $\mathbb{Z}[\mathbb{T}^{\mathtt{R}}] \xrightarrow{\phi_\Pi} \mathcal{O}_{\mathbb{E}} \to \mathcal{O}_{\mathbb{E}}/\lambda$.

Assumption 4.1. Let ℓ be the underlying rational prime of λ. We propose the following assumptions on λ:

(1) ℓ is coprime to 5, $\mathtt{R}$, disc F, and the cardinality of $F^\times \backslash \mathbb{A}_F^{\infty,\times}/(\mathbb{A}_F^{\infty,\times} \cap K)$.

(2) $\ell \geq g + 2$.

(3) The image of $\bar{\rho}_{\Pi,\lambda} := \rho_{\Pi,\lambda} \mod \lambda$ contains a subgroup conjugate to $\mathrm{SL}_2(\mathbb{F}_\ell)$.

(4) $\bar{\rho}_{\Pi,\lambda}$ satisfies the condition ($\mathbf{LI}_{\mathrm{Ind}\,\bar{\rho}_{\Pi,\lambda}}$) in [Dimitrov 2005, Proposition 0.1].

(5) $\mathrm{H}^g(\mathrm{Sh}(G, K)_{\mathbb{Q}^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}}/\lambda)/\mathfrak{m}_{\Pi,\lambda}^{\mathtt{R}}$ has dimension $2^g \dim(\Pi_B^\infty)^K$ over $\mathcal{O}_{\mathbb{E}}/\lambda$, where Π_B is the automorphic representation of $G(\mathbb{A})$ whose Jacquet–Langlands transfer to $\mathrm{GL}_2(\mathbb{A}_F)$ is Π.

Remark 4.2. We have the following remarks concerning Assumption 4.1:

(1) Assumption 4.1(3) is equivalent to saying that $\bar{\rho}_{\Pi,\lambda}$ is absolutely irreducible and that ℓ divides the image of $\bar{\rho}_{\Pi,\lambda}$.

(2) Assumption 4.1(3) (and the part $\ell \neq 5$ in (1)) is used to guarantee Ihara's lemma for Shimura curves over totally real fields [Manning and Shotton 2019].

(3) If Π is not dihedral (that is, not a theta series) and not isomorphic to a twist by a character of any of its internal conjugates, then Assumption 4.1(3) and (4) hold for all but finitely many λ by [Dimitrov 2005, Proposition 0.1]. In particular, for such a Π, the entire Assumption 4.1 holds for all but finitely many λ.

(4) In general, the dimension of $\mathrm{H}^g(\mathrm{Sh}(G, K)_{\mathbb{Q}^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}}/\lambda)/\mathfrak{m}_{\Pi,\lambda}^{\mathtt{R}}$ is at least $2^g \dim_E(\Pi_B^\infty)^K$ over $\mathcal{O}_{\mathbb{E}}/\lambda$.

[4] The meaning of $\mathtt{R}$ changes from here; in particular, it contains the ramification set of B, which it previously stood for.

Let p be a rational prime inert in F, coprime to $\mathtt{R}\cup\{2,\ell\}$. Denote by $\mathfrak{p}$ the unique prime of F above p. To ease notation, we put

$$\phi := \phi_{\Pi}^{\mathtt{R}\cup\{\mathfrak{p}\}} \colon \mathbb{Z}[\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}] \to \mathcal{O}_{\mathbb{E}}, \quad \mathfrak{m} := \mathfrak{m}_{\Pi,\lambda}^{\mathtt{R}\cup\{\mathfrak{p}\}} \subseteq \mathbb{Z}[\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}].$$

For a $\mathbb{Z}[\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}]$-module M, we denote by $M_{\mathfrak{m}}$ its localization at $\mathfrak{m}$. Write $K = K_pK^p$ where K_p is a hyperspecial maximal subgroup of $G(\mathbb{Q}_p)$ as $p \notin \mathtt{R}$. We have the integral model $\mathbf{Sh}(G, K^p)$ over $\mathbb{Z}_p$ defined in Section 2E for the Shimura variety $\mathrm{Sh}(G, K^p) = \mathrm{Sh}(G, K)$. Put $\mathfrak{B} := \mathfrak{B}(\varnothing, (g-1)/2)$, the set of periodic semimeanders attached to $\mathtt{S} = \varnothing$ with g-nodes and $(g-1)/2$-arcs. We note that k_0 defined in Section 3A is $\mathbb{F}_{p^{2g}}$ in the current case. Then Theorem 3.13 asserts that

$$\mathbf{Sh}(G, K^p)^{\mathrm{ss}}_{\mathbb{F}_p} \otimes \mathbb{F}_{p^{2g}} = \bigcup_{\mathfrak{a}\in\mathfrak{B}} W_{\varnothing,\varnothing}(\mathfrak{a}),$$

where each $W_{\varnothing,\varnothing}(\mathfrak{a})$ is equipped with a $(g-1)/2$-th iterated $\mathbb{P}^1$-fibration

$$\pi_{\mathfrak{a}} \colon W_{\varnothing,\varnothing}(\mathfrak{a}) \to \mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)_{\mathbb{F}_{p^{2g}}}.$$

Let

$$\mathbf{Sh}(G, K^p)^{\mathrm{sp}}_{\mathbb{F}_p} \subseteq \mathbf{Sh}(G, K^p)_{\mathbb{F}_p}$$

be the superspecial locus as in Definition 3.15. By Theorem 3.16, each $W_{\varnothing,\varnothing}(\mathfrak{a})$ for $\mathfrak{a} \in \mathfrak{B}$ contains $\mathbf{Sh}(G, K^p)^{\mathrm{sp}}_{\mathbb{F}_{p^{2g}}}$, and the morphism $\pi_{\mathfrak{a}}$ induces an isomorphism

$$\mathbf{Sh}(G, K^p)^{\mathrm{sp}}_{\mathbb{F}_{p^{2g}}} \xrightarrow{\sim} \mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)_{\mathbb{F}_{p^{2g}}}$$

which is equivariant under prime-to-p Hecke correspondences, and independent of $\mathfrak{a}$.

Consider the set $\mathfrak{B} \times \mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)(\mathbb{F}_p^{\mathrm{ac}})$, equipped with the diagonal action by $\mathrm{G}_{\mathbb{F}_p}$. The Hecke monoid $\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}$ acts through the second factor. We have a Chow cycle class map

$$\Gamma(\mathfrak{B} \times \mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)(\mathbb{F}_p^{\mathrm{ac}}), \mathbb{Z}) \to \mathrm{CH}^{(g+1)/2}(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}) \tag{4-2}$$

sending a function f on $\mathfrak{B} \times \mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)(\mathbb{F}_p^{\mathrm{ac}})$ to the Chow class of $\sum_{\mathfrak{a},s} f(\mathfrak{a}, s)\pi_{\mathfrak{a}}^{-1}(s)$.

Lemma 4.3. *The map* (4-2) *is equivariant under both* $\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}$ *and* $\mathrm{G}_{\mathbb{F}_p}$.

Proof. The equivariance of $\pi_{\mathfrak{a}}$ under prime-to-p Hecke correspondences follows from Theorem 3.16. The equivariance under $\mathrm{G}_{\mathbb{F}_p}$ follows from the definition of $\mathrm{G}_{\mathbb{F}_p}$-action on $\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)(\mathbb{F}_p^{\mathrm{ac}})$. □

Lemma 4.4. *Under the notation above*, *the following statements hold*:

(1) *There exists a canonical isomorphism*

$$\mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}_\lambda})_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{H}^g(\mathrm{Sh}(G, K)_{\mathbb{Q}^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}_\lambda})_{\mathfrak{m}}$$

compatible with Galois actions. In particular, *we have a canonical isomorphism*

$$\mathrm{H}^1(\mathbb{F}_{p^h}, \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}}/\lambda((g+1)/2))_{\mathfrak{m}}) \cong \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_{p^h}, \mathrm{H}^g(\mathrm{Sh}(G, K)_{\mathbb{Q}^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}}/\lambda((g+1)/2))_{\mathfrak{m}})$$

for every integer $h \geq 1$.

(2) *Suppose that ℓ satisfies Assumption 4.1. We have* $\mathrm{H}^i(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}_\lambda})_{\mathfrak{m}} = 0$ *unless* $i = g$.

(3) *Suppose that ℓ satisfies Assumption 4.1. We have that* $\mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}_\lambda})_{\mathfrak{m}}$ *is a finite free* $\mathcal{O}_{\mathbb{E}_\lambda}$*-module.*

Proof. By [Lan and Stroh 2018, Corollary 4.6], no matter whether the Shimura variety $\mathbf{Sh}(G, K^p)$ is proper over $\mathbb{Z}_{(p)}$, the canonical maps

$$\mathrm{H}^i(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}_\lambda}) \xrightarrow{\sim} \mathrm{H}^i(\mathbf{Sh}(G, K^p)_{\mathbb{Q}_p^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}_\lambda}) \xleftarrow{\sim} \mathrm{H}^i(\mathrm{Sh}(G, K^p)_{\mathbb{Q}^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}_\lambda})$$

for all $i \geq 0$ are isomorphisms compatible with Hecke and Galois actions. One gets thus Statement (1) by localizing the Hecke action at $\mathfrak{m}$. Statements (2) and (3) follow from Assumption 4.1 and [Dimitrov 2005, Theorem 0.3]. We remark that although Dimitrov's theorem is stated for Hilbert modular varieties, the same argument there applies to our situation without change. □

To ease notation, put $\mathrm{G}' := \mathrm{Gal}(\mathbb{F}_p^{\mathrm{ac}}/\mathbb{F}_{p^{2g}})$. Lemma 4.3 induces the following map

$$\Gamma(\mathfrak{B} \times \mathbf{Sh}(G_{\mathrm{S}_{\max}}, K^p)(\mathbb{F}_p^{\mathrm{ac}}), \mathbb{Z})^{\mathrm{G}'} \to \mathrm{CH}^{(g+1)/2}(\mathbf{Sh}(G, K^p)_{\mathbb{F}_{p^{2g}}}) \tag{4-3}$$

which is equivariant under both $\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}$ and $\mathrm{Gal}(\mathbb{F}_{p^{2g}}/\mathbb{F}_p)$. On the other hand, one has a cycle class map

$$\mathrm{CH}^{(g+1)/2}(\mathbf{Sh}(G, K^p)_{\mathbb{F}_{p^{2g}}}) \to \mathrm{H}^{g+1}(\mathbf{Sh}(G, K^p)_{\mathbb{F}_{p^{2g}}}, \mathcal{O}_{\mathbb{E}_\lambda}((g+1)/2)).$$

However, by the Hochschild–Serre spectral sequence and Lemma 4.4(2), we have a canonical isomorphism

$$\mathrm{H}^{g+1}(\mathbf{Sh}(G, K^p)_{\mathbb{F}_{p^{2g}}}, \mathcal{O}_{\mathbb{E}_\lambda}((g+1)/2))_{\mathfrak{m}} \cong \mathrm{H}^1(\mathbb{F}_{p^{2g}}, \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}_\lambda}((g+1)/2))_{\mathfrak{m}}).$$

Therefore, composing with (the localization of) (4-3) and modulo λ, we obtain a morphism

$$\Phi_{\mathfrak{m}} : \Gamma(\mathfrak{B} \times \mathbf{Sh}(G_{\mathrm{S}_{\max}}, K^p)(\mathbb{F}_p^{\mathrm{ac}}), \mathcal{O}_{\mathbb{E}}/\lambda)_{\mathfrak{m}}^{\mathrm{G}'} \to \mathrm{H}^1(\mathbb{F}_{p^{2g}}, \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}}/\lambda((g+1)/2))_{\mathfrak{m}}), \tag{4-4}$$

called the *unramified level raising map at* $\mathfrak{m}$. It is equivariant under the action of $\mathrm{Gal}(\mathbb{F}_{p^{2g}}/\mathbb{F}_p)$.

Definition 4.5. We say that a rational prime p is a λ*-level raising prime* (with respect to Π, B, K, $\mathtt{R}$) if

(L1) p is inert in F, and coprime to $\mathtt{R} \cup \{2, \ell\}$;

(L2) $\ell \nmid \prod_{i=1}^{g}(p^{2gi} - 1)$;

(L3) $\phi_{\Pi}^{\mathtt{R}}(\mathrm{T}_{\mathfrak{p}})^2 \equiv (p^g + 1)^2 \mod \lambda$ and $\phi_{\Pi}^{\mathtt{R}}(\mathrm{S}_{\mathfrak{p}}) \equiv 1 \mod \lambda$.

Remark 4.6. We have the following remarks concerning level raising primes:

(1) By a similar argument of [Liu 2019, Lemma 4.11], one can show there are infinitely many λ-level raising primes with positive density, as long as there exist rational primes inert in F and λ satisfies Assumption 4.1.

(2) By the Eichler–Shimura congruence relation, Definition 4.5(L3) is equivalent to saying that $\bar{\rho}_{\Pi,\lambda}(\sigma_{\mathfrak{p}})$ is conjugate to $\pm\left(\begin{smallmatrix}1 & 0\\ 0 & p^g\end{smallmatrix}\right)$.

(3) By the Eichler–Shimura congruence relation and the Chebotarev's density theorem, we know that the canonical map
$$\mathrm{H}^g(\mathrm{Sh}(G,K)_{\mathbb{Q}^{\mathrm{ac}}},\mathcal{O}_{\mathbb{E}}/\lambda)/\mathfrak{m}\to\mathrm{H}^g(\mathrm{Sh}(G,K)_{\mathbb{Q}^{\mathrm{ac}}},\mathcal{O}_{\mathbb{E}}/\lambda)/\mathfrak{m}^{\mathtt{R}}_{\Pi,\lambda}$$
is an isomorphism of $\mathcal{O}_{\mathbb{E}}/\lambda[\mathrm{G}_{\mathbb{Q}}]$-modules.

Theorem 4.7 (arithmetic level raising). *Let λ be a prime of $\mathcal{O}_{\mathbb{E}}$ satisfying Assumption 4.1, and p a λ-level raising prime. Then G' acts trivially on $\Gamma(\mathfrak{B}\times\mathbf{Sh}(G_{\mathtt{S}_{\max}},K^p)(\mathbb{F}_p^{\mathrm{ac}}),\mathcal{O}_{\mathbb{E}}/\lambda)_{\mathfrak{m}}$ and the induced map*
$$\Gamma(\mathfrak{B}\times\mathbf{Sh}(G_{\mathtt{S}_{\max}},K^p)(\mathbb{F}_p^{\mathrm{ac}}),\mathcal{O}_{\mathbb{E}}/\lambda)/\mathfrak{m}\to\mathrm{H}^1(\mathbb{F}_{p^{2g}},\mathrm{H}^g(\mathbf{Sh}(G,K^p)_{\mathbb{F}_p^{\mathrm{ac}}},\mathcal{O}_{\mathbb{E}}/\lambda((g+1)/2))/\mathfrak{m})\tag{4-5}$$
is surjective.

4B. ***Proof of arithmetic level raising.*** This section is devoted to the proof of Theorem 4.7. We assume that we are not in the case where $F=\mathbb{Q}$ and B is the matrix algebra, since this is already known by Ribet.

For $\mathfrak{a}\in\mathfrak{B}$, denote $\tau(\mathfrak{a})\in\Sigma_\infty$ the end point of the unique semiline in $\mathfrak{a}$. By the construction in Section 3G, for each $\mathfrak{a}\in\mathfrak{B}$, the stratum $W_{\varnothing,\varnothing}(\mathfrak{a})$ fits into the following commutative diagram
$$\begin{tikzcd}
W_{\varnothing,\varnothing}(\mathfrak{a}) \arrow[r, hook] \arrow[d] & Z_{\varnothing,\varnothing}(\mathfrak{a}) \arrow[r, hook] \arrow[d, "\pi_{\mathfrak{a}}"] & \mathbf{Sh}(G,K^p)_{\mathbb{F}_{p^{2g}}} \\
\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing'_{\mathfrak{a}}},K^p)_{\mathbb{F}_{p^{2g}},\tau(\mathfrak{a})} \arrow[r, hook] \arrow[d, "\cong"] & \mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing'_{\mathfrak{a}}},K^p)_{\mathbb{F}_{p^{2g}}} & \\
\mathbf{Sh}(G_{\mathtt{S}_{\max}},K^p)_{\mathbb{F}_{p^{2g}}}, & &
\end{tikzcd}\tag{4-6}$$
where the square is Cartesian. Here, $\varnothing_{\mathfrak{a}}$ is the set $\mathtt{S}_{\mathfrak{a}}$ defined by (3-3) with $\mathtt{S}=\varnothing$ and $\varnothing'_{\mathfrak{a}}$ is the subset defined by (3-8) with $\mathtt{T}=\varnothing$, and we used slightly different notations to avoid confusion. Note that $\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing_{\mathfrak{a}}},K^p)$ is a *proper* Shimura curve over $\mathcal{O}_{F,\mathfrak{p}}$ (with F regarded as a subfield of $\mathbb{Q}^{\mathrm{ac}}$ determined by $\mathfrak{a}$), and $\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing_{\mathfrak{a}}},K^p)_{\mathbb{F}_{p^{2g}},\tau(\mathfrak{a})}\cong\mathbf{Sh}(G_{\mathtt{S}_{\max}},K^p)_{\mathbb{F}_{p^{2g}}}$ is exactly its supersingular locus in the sense of [Carayol 1986, Section 6.7]. Similarly to (4-3), we have a Chow class map
$$\Gamma(\mathbf{Sh}(G_{\mathtt{S}_{\max}},K^p)(\mathbb{F}_p^{\mathrm{ac}}),\mathbb{Z})\to\mathrm{CH}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing'_{\mathfrak{a}}},K^p)_{\mathbb{F}_p^{\mathrm{ac}}}),$$
which induces an unramified level raising map for the Shimura curve $\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing'_{\mathfrak{a}}},K^p)$:
$$\Phi_{\mathfrak{m}}(\mathfrak{a})\colon\Gamma(\mathbf{Sh}(G_{\mathtt{S}_{\max}},K^p)(\mathbb{F}_p^{\mathrm{ac}}),\mathcal{O}_{\mathbb{E}}/\lambda)^{\mathrm{G}'}_{\mathfrak{m}}\to\mathrm{H}^1(\mathbb{F}_{p^{2g}},\mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing'_{\mathfrak{a}}},K^p)_{\mathbb{F}_p^{\mathrm{ac}}},\mathcal{O}_{\mathbb{E}}/\lambda(1))_{\mathfrak{m}}).\tag{4-7}$$
The following is an analogue of Theorem 4.7 for Shimura curves.

Proposition 4.8. *Under the hypothesis of Theorem 4.7, the map $\Phi_{\mathfrak{m}}(\mathfrak{a})$ is surjective.*

To prove this proposition, we need some preparation. We fix an isomorphism $G_{\varnothing_{\mathfrak{a}}}(\mathbb{Q}_p)\cong\mathrm{GL}_2(F_{\mathfrak{p}})$ so that K_p is identified with $\mathrm{GL}_2(\mathcal{O}_{F_{\mathfrak{p}}})$. Let $\mathrm{Iw}_p\subseteq K_p$ be the standard upper triangular Iwahori subgroup. Let $\mathrm{Sh}(G_{\varnothing_{\mathfrak{a}}},K^p\,\mathrm{Iw}_p)$ be the Shimura curve attached to $G_{\varnothing_{\mathfrak{a}}}$ of level $K^p\,\mathrm{Iw}_p$. By [Carayol

1986], $\mathrm{Sh}(G_{\varnothing_\mathfrak{a},\varnothing'_\mathfrak{a}}, K^p\,\mathrm{Iw}_p)$ admits an integral model $\mathbf{Sh}(G_{\varnothing_\mathfrak{a},\varnothing'_\mathfrak{a}}, K^p\,\mathrm{Iw}_p)$ over $\mathcal{O}_{F,\mathfrak{p}}$ with semistable reduction. The special fiber $\mathbf{Sh}(G_{\varnothing_\mathfrak{a},\varnothing'_\mathfrak{a}}, K^p\,\mathrm{Iw}_p)_{\mathbb{F}_{p^g}}$ consists of two copies of $\mathbf{Sh}(G_{\varnothing_\mathfrak{a},\varnothing'_\mathfrak{a}}, K^p\,\mathrm{Iw}_p)_{\mathbb{F}_{p^g}}$ cutting transversally at supersingular points. There are two natural degeneracy maps

$$\pi_1, \pi_2\colon\ \mathbf{Sh}(G_{\varnothing_\mathfrak{a},\varnothing'_\mathfrak{a}}, K^p\,\mathrm{Iw}_p) \to \mathbf{Sh}(G_{\varnothing_\mathfrak{a},\varnothing'_\mathfrak{a}}, K^p)$$

whose restrictions to generic fibers are described as in [Tian and Xiao 2019, (2.14.1)]. We note the following generalization of Ihara's lemma to Shimura curves over totally real fields.

Lemma 4.9. *Under the hypothesis of Theorem 4.7, the canonical map*

$$\pi_1^* + \pi_2^*\colon \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_\mathfrak{a},\varnothing'_\mathfrak{a}}, K^p)_{\mathbb{Q}^{\mathrm{ac}}}, \mathcal{O}_\mathbb{E}/\lambda)_\mathfrak{m}^{\oplus 2} \to \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_\mathfrak{a},\varnothing'_\mathfrak{a}}, K^p\,\mathrm{Iw}_p)_{\mathbb{Q}^{\mathrm{ac}}}, \mathcal{O}_\mathbb{E}/\lambda)_\mathfrak{m}$$

is injective.

Proof. This follows from [Manning and Shotton 2019, Theorem 6.5], under Assumption 4.1(1) and (3). □

Proof of Proposition 4.8. To simplify notation, let us put $X := \mathbf{Sh}(G_{\varnothing_\mathfrak{a},\varnothing_\mathfrak{a}}, K^p)$ viewed as a proper smooth scheme over $\mathcal{O}_{F,\mathfrak{p}}$, denote the supersingular locus as

$$X^{\mathrm{ss}}_{\mathbb{F}_{p^{2g}}} := \mathbf{Sh}(G_{\varnothing_\mathfrak{a},\varnothing'_\mathfrak{a}}, K^p)_{\mathbb{F}_{p^{2g}},\tau_\mathfrak{a}} \cong \mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)_{\mathbb{F}_{p^{2g}}},$$

and put $X_0(p) := \mathbf{Sh}(G_{\varnothing_\mathfrak{a},\varnothing_\mathfrak{a}}, K^p\,\mathrm{Iw}_p)$. We put also $k_\lambda := \mathcal{O}_\mathbb{E}/\lambda$. Consider the canonical short exact sequence

$$\mathrm{H}^0(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda) \to \mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda) \to \mathrm{H}^1_c(X^{\mathrm{ord}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda) \to \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda) \to 0$$

equivariant under the action of $\mathrm{G}(\mathbb{F}_p^{\mathrm{ac}}/\mathbb{F}_{p^g}) \times \mathbb{Z}[\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}]$, where $X^{\mathrm{ord}}_{\mathbb{F}_p^{\mathrm{ac}}} := X_{\mathbb{F}_p^{\mathrm{ac}}} - X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}$ is the ordinary locus. The first term vanishes after localizing at $\mathfrak{m}$ by Assumption 4.1(3). Taking Galois cohomology $\mathrm{H}^i(\mathbb{F}_{p^{2g}}, -)$, one deduces a boundary map

$$\Phi^*_\mathfrak{m}(\mathfrak{a})\colon \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\mathrm{G}'}_\mathfrak{m} \to \mathrm{H}^1(\mathbb{F}_{p^{2g}}, \mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_\mathfrak{m}).$$

By the Poincaré duality and the duality of Galois cohomology over finite fields, it is easy to see that $\Phi^*_\mathfrak{m}(\mathfrak{a})$ is identified with the dual map of $\Phi_\mathfrak{m}(\mathfrak{a})$. Therefore, to finish the proof of Proposition 4.8, it suffices to show that $\Phi^*_\mathfrak{m}(\mathfrak{a})$ is injective.

Recall that $X_0(p)_{\mathbb{F}_{p^g}}$ consists of two copies of $X_{\mathbb{F}_{p^g}}$. Let $i_1\colon X_{\mathbb{F}_{p^g}} \to X_0(p)_{\mathbb{F}_{p^g}}$ be the copy such that $\pi_1 \circ i_1$ is the identity, and $i_2\colon X_{\mathbb{F}_{p^g}} \to X_0(p)_{\mathbb{F}_{p^g}}$ be the one such that $\pi_2 \circ i_2$ is the identity. Then $\pi_2 \circ i_1$ is the Frobenius endomorphism of $X_{\mathbb{F}_{p^g}}$ relative to $\mathbb{F}_{p^g}$ composed with the Hecke action $\mathrm{S}_\mathfrak{p}^{(g-1)/2}$; and $\pi_1 \circ i_2$ is the Frobenius endomorphism of $X_{\mathbb{F}_{p^g}}$ relative to $\mathbb{F}_{p^g}$ composed with the Hecke action $\mathrm{S}_\mathfrak{p}^{(g+1)/2}$. Consider the normalization map

$$\delta\colon \widetilde{X}_0(p)_{\mathbb{F}_{p^g}} := X_{\mathbb{F}_{p^g}} \coprod X_{\mathbb{F}_{p^g}} \xrightarrow{i_1 \coprod i_2} X_0(p)_{\mathbb{F}_{p^g}}.$$

Then one has an exact sequence of étale sheaves

$$0 \to k_\lambda \to \delta_* k_\lambda \to i^{\mathrm{ss}}_* k_\lambda \to 0$$

on $X_0(p)_{\mathbb{F}_{p^g}}$, where $i^{\mathrm{ss}}\colon X^{\mathrm{ss}}_{\mathbb{F}_{p^g}} \to X_0(p)_{\mathbb{F}_{p^g}}$ denotes the closed immersion of the singular locus of $X_0(p)_{\mathbb{F}_{p^g}}$, and the second map $\delta_*k_\lambda \to i^{\mathrm{ss}}_*k_\lambda$ is given as follows: If $x \in X^{\mathrm{ss}}_{\mathbb{F}_{p^g}}(\mathbb{F}_p^{\mathrm{ac}})$ is a supersingular geometric point with preimage $\delta^{-1}(x) = (x_1, x_2)$ with $x_j \in i_j(X(\mathbb{F}_p^{\mathrm{ac}}))$ for $j = 1, 2$, then $(\delta_*k_\lambda)_x = k_{\lambda,x_1} \oplus k_{\lambda,x_2} \to k_{\lambda,x}$ is given by $(a, b) \mapsto a - b$. By the functoriality of cohomology, we get

$$0 = \mathrm{H}^0(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}} \to \mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}} \to \mathrm{H}^1(X_0(p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}} \xrightarrow{(i_1^*, i_2^*)} \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}_{\mathfrak{m}} \to 0. \tag{4-8}$$

Consider the map

$$\pi_1^* + \pi_2^*\colon \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}_{\mathfrak{m}} \to \mathrm{H}^1(X_0(p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}} \tag{4-9}$$

induced by the two degeneracy maps $\pi_1, \pi_2\colon X_0(p) \to X$. If $\mathrm{Fr}_{\mathfrak{p}}$ denotes the action on $\mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)$ induced by the Frobenius endomorphism of $X_{\mathbb{F}_{p^g}}$ relative to $\mathbb{F}_{p^g}$, then $\mathrm{Fr}_{\mathfrak{p}} = \sigma_{\mathfrak{p}}^{-1}$ and the composite map

$$\theta\colon \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}_{\mathfrak{m}} \xrightarrow{\pi_1^*+\pi_2^*} \mathrm{H}^1(X_0(p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}} \xrightarrow{(i_1^*, i_2^*)} \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}_{\mathfrak{m}}$$

is given by the matrix

$$\begin{pmatrix} 1 & \mathrm{Fr}_{\mathfrak{p}}\,\mathrm{S}_{\mathfrak{p}}^{(g-1)/2} \\ \mathrm{Fr}_{\mathfrak{p}}\,\mathrm{S}_{\mathfrak{p}}^{(g+1)/2} & 1 \end{pmatrix}.$$

By Definition 4.5(L3), the Hecke operator $\mathrm{S}_{\mathfrak{p}}$ acts trivially on $\mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}$ since the trivial action is the only lifting of the trivial action modulo $\mathfrak{m}$ by Assumption 4.1(1). We see that $\ker\theta$ is identified with the image of the injective morphism

$$\mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}^{\mathrm{Fr}_{\mathfrak{p}}^2=1} \xrightarrow{(-\mathrm{Fr}_{\mathfrak{p}}, \mathrm{Id})} \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}_{\mathfrak{m}}.$$

However, by Ihara's Lemma 4.9 and the proper base change, the map $\pi_1^* + \pi_2^*$ in (4-9) is injective. Thus, it induces an injection

$$\Phi^*\colon \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}^{\mathrm{Fr}_{\mathfrak{p}}^2=1} \cong \ker\theta \to \ker(i_1^*, i_2^*) \cong \mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}.$$

To finish the proof of Proposition 4.8, it suffices to show the following claims:

(1) The action of $\mathrm{Fr}_{\mathfrak{p}}^2$ on $\mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}$ is trivial so that the natural projection

$$\mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}} \to \mathrm{H}^1(\mathbb{F}_{p^{2g}}, \mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}) \cong \mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}/(\mathrm{Fr}_{\mathfrak{p}}^2 - 1)$$

is an isomorphism.

(2) The morphism Φ^* is identified with $\Phi^*_{\mathfrak{m}}(\mathfrak{a})$.

Claim (1) follows from Assumption 4.1(1), Definition 4.5(L3) and the observation that $\mathrm{Fr}_{\mathfrak{p}}^2$ acts through the Hecke translation by $(1, \dots, 1, p, 1, \dots) \in \mathbb{A}_F^{\infty,\times}$ where p is placed at the prime $\mathfrak{p}$.

To prove Claim (2), consider the following commutative diagram:

$$\begin{tikzcd}
 & & \mathrm{H}^1_c(X^{\mathrm{ord}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}} \arrow[r] \arrow[d, "\pi_2^*-\pi_1^*\,\mathrm{Fr}_{\mathfrak{p}}"] & \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda) \arrow[r] \arrow[d, "\pi_2^*-\pi_1^*\,\mathrm{Fr}_{\mathfrak{p}}"] & 0 \\
0 \arrow[r] & \mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}} \arrow[r] \arrow[d, "\Delta"] & \mathrm{H}^1_c(X^{\mathrm{ord}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}_{\mathfrak{m}} \arrow[r] \arrow[d, equal] & \mathrm{H}^1(X_0(p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}} \arrow[r] \arrow[d, "(i_1^*, i_2^*)"] & 0 \\
0 \arrow[r] & \mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}_{\mathfrak{m}} \arrow[r] & \mathrm{H}^1_c(X^{\mathrm{ord}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}_{\mathfrak{m}} \arrow[r] & \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}_{\mathfrak{m}} \arrow[r] & 0
\end{tikzcd}$$

where Δ is the diagonal map, and horizontal rows are exact. Then the coboundary isomorphism $\ker(i_1^*, i_2^*) \cong \mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}$ given by (4-8) coincides with

$$\ker(i_1^*, i_2^*) \xrightarrow{\sim} \operatorname{coker}\Delta \xleftarrow{\sim} \mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}},$$

where the first isomorphism is deduced from the commutative diagram above by the snake lemma, and the second is induced by the injection $\mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}} \hookrightarrow \mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}_{\mathfrak{m}}$ to the second component.

Now take $x \in \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}^{\mathrm{Fr}_{\mathfrak{p}}^2=1} \cong \ker\theta$, and let $\tilde{x} \in \mathrm{H}^1_c(X^{\mathrm{ord}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}$ be a lift of x that is fixed by $\mathrm{S}_{\mathfrak{p}}$. This is possible as the action of $\mathrm{S}_{\mathfrak{p}}$ on $\mathrm{H}^1_c(X^{\mathrm{ord}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)$ is semisimple. Then $\pi_2^*(\tilde{x}) - \pi_1^*\,\mathrm{Fr}_{\mathfrak{p}}(\tilde{x}) \in \mathrm{H}^1_c(X^{\mathrm{ord}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}$ is an element lifting $\pi_2^*(x) - \pi_1^*\,\mathrm{Fr}_{\mathfrak{p}}(x) \in \ker(i_1^*, i_2^*)$, and $\pi_2^*(\tilde{x}) - \pi_1^*\,\mathrm{Fr}_{\mathfrak{p}}(\tilde{x})$ lies actually in the image of $\mathrm{H}^0(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)^{\oplus 2}_{\mathfrak{m}}$. Note that

$$\pi_2^*(\tilde{x}) - \pi_1^*\,\mathrm{Fr}_{\mathfrak{p}}(\tilde{x}) = (\mathrm{S}_{\mathfrak{p}}^{-1}\,\mathrm{Fr}_{\mathfrak{p}}(\tilde{x}), \tilde{x}) - (\mathrm{Fr}_{\mathfrak{p}}(\tilde{x}), \mathrm{Fr}_{\mathfrak{p}}^2(\tilde{x})) = (0, (1-\mathrm{Fr}_{\mathfrak{p}}^2)(\tilde{x})).$$

Since $\Phi^*(x)$ is by definition the image of $\pi_2^*(\tilde{x}) - \pi_1^*\,\mathrm{Fr}_{\mathfrak{p}}(\tilde{x})$ in $\operatorname{coker}\Delta \cong \mathrm{H}^1(X^{\mathrm{ss}}_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}$, we get $\Phi^*(x) = (1-\mathrm{Fr}_{\mathfrak{p}}^2)(\tilde{x})$. However, this is nothing but the image of $x \in \mathrm{H}^1(X_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}}^{\mathrm{G}'}$ via the coboundary map $\Phi^*_{\mathfrak{m}}(\mathfrak{a})$. This finishes the proof of claim, hence also the proof of Proposition 4.8. □

Recall that we have, for each $\mathfrak{a} \in \mathfrak{B}$, an algebraic correspondence

$$\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}}, \varnothing'_{\mathfrak{a}}}, K^p)_{\mathbb{F}_{p^{2g}}} \xleftarrow{\pi_{\mathfrak{a}}} Z_{\varnothing,\varnothing}(\mathfrak{a}) \xrightarrow{i_{\mathfrak{a}}} \mathbf{Sh}(G, K^p)_{\mathbb{F}_{p^{2g}}}.$$

Let Λ be $\mathcal{O}_{\mathbb{E}_\lambda}$, $\mathcal{O}_{\mathbb{E}}/\lambda$ or $\mathbb{Q}_\ell^{\mathrm{ac}}$. We define $\mathrm{Gys}_{\mathfrak{a}}(\Lambda)$ to be the composite map

$$\mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}}, \varnothing'_{\mathfrak{a}}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda)_{\mathfrak{m}} \xrightarrow{\pi_{\mathfrak{a}}^*} \mathrm{H}^1(W_{\varnothing,\varnothing}(\mathfrak{a})_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda)_{\mathfrak{m}} \xrightarrow{\text{Gysin}} \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda((g-1)/2))_{\mathfrak{m}},$$

where the first map is an isomorphism since $\pi_{\mathfrak{a}}$ is a $(g-1)/2$-th iterated $\mathbb{P}^1$-fibrations, and the second map is the Gysin map induced by the closed immersion $i_{\mathfrak{a}}$. Taking sum, we get a map

$$\mathrm{Gys}(\Lambda) := \sum_{\mathfrak{a}} \mathrm{Gys}_{\mathfrak{a}}(\Lambda) \colon \bigoplus_{\mathfrak{a}\in\mathfrak{B}} \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}}, \varnothing'_{\mathfrak{a}}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda)_{\mathfrak{m}} \to \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda((g-1)/2))_{\mathfrak{m}}.$$

Proposition 4.10. *Under the assumption of Theorem 4.7, we have that*

(1) *the map* $\mathrm{Gys}(\Lambda)$ *is injective for* $\Lambda = \mathcal{O}_{\mathbb{E}_\lambda}, \mathcal{O}_{\mathbb{E}}/\lambda, \mathbb{Q}_\ell^{\mathrm{ac}}$;

(2) *the induced map*

$$\mathrm{Gys}(\mathcal{O}_{\mathbb{E}}/\lambda)/\mathfrak{m}\colon \bigoplus_{\mathfrak{a}\in\mathfrak{B}} \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing'_{\mathfrak{a}}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}}/\lambda)/\mathfrak{m} \to \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}}/\lambda((g-1)/2))/\mathfrak{m}$$

is injective.

Before giving the proof of the proposition, we introduce some notation. Let $R_{\mathfrak{m}}$ be the set of all automorphic representations that contribute to $\mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda((g-1)/2))_{\mathfrak{m}}$. Then it is the same as the set of all automorphic representations that contribute to $\mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing_{\mathfrak{a}}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda)_{\mathfrak{m}}$ for every $\mathfrak{a}$ by the Jacquet–Langlands correspondence. It is finite and contains Π. We may enlarge $\mathbb{E}$ such that every automorphic representation $\Pi' \in R_{\mathfrak{m}}$ is defined over $\mathbb{E}$. Fix an embedding $\mathbb{E}_\lambda \hookrightarrow \mathbb{Q}_\ell^{\mathrm{ac}}$. Let $\alpha_{\Pi'}, \beta_{\Pi'} \in \mathbb{Z}_\ell^{\mathrm{ac}}$ be the eigenvalues of $\rho_{\Pi',\lambda}(\sigma_{\mathfrak{p}})$, where $\mathbb{Z}_\ell^{\mathrm{ac}}$ denotes the ring of integers of $\mathbb{Q}_\ell^{\mathrm{ac}}$. By Remark 4.6(2), we may assume that $\alpha_{\Pi'}^2$ and $\beta_{\Pi'}^2$ are respectively congruent to 1 and p^{2g} (modulo the maximal ideal of $\mathbb{Z}_\ell^{\mathrm{ac}}$); in particular, $\alpha_{\Pi'}/\beta_{\Pi'}$ is not congruent to any i-th root of unity for $1 \le i \le 2g$ by Definition 4.5(L2).

Proof of Proposition 4.10. Following [Tian and Xiao 2019], we consider the composite map

$$\mathrm{Res}_{\mathfrak{a}}(\Lambda)\colon \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda)_{\mathfrak{m}} \xrightarrow{i_{\mathfrak{a}}^*} \mathrm{H}^g(W_{\varnothing,\varnothing}(\mathfrak{a})_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda)_{\mathfrak{m}} \xrightarrow{\pi_{\mathfrak{a}!}} \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing'_{\mathfrak{a}}}, K^p), \Lambda)_{\mathfrak{m}}$$

for each $\mathfrak{a} \in \mathfrak{B}$, and put

$$\mathrm{Res}(\Lambda) := \bigoplus_{\mathfrak{a}\in\mathfrak{B}} \mathrm{Res}_{\mathfrak{a}}(\Lambda)\colon \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda)_{\mathfrak{m}} \to \bigoplus_{\mathfrak{a}\in\mathfrak{B}} \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing'_{\mathfrak{a}}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda)_{\mathfrak{m}}.$$

To prove that $\mathrm{Gys}(\Lambda)$ is injective, it suffices to show that the composite map $\mathrm{Res}(\Lambda) \circ \mathrm{Gys}(\Lambda)$, which is an endomorphism of $\bigoplus_{\mathfrak{a}\in\mathfrak{B}} \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing'_{\mathfrak{a}}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda)_{\mathfrak{m}}$, is injective.

It follows from Lemma 4.4 that

$$\mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \Lambda)_{\mathfrak{m}} = \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathcal{O}_{\mathbb{E}_\lambda})_{\mathfrak{m}} \otimes_{\mathcal{O}_{\mathbb{E}_\lambda}} \Lambda, \tag{4-10}$$

and it is a finite free Λ-module. Note that we have

$$\mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathbb{Q}_\ell^{\mathrm{ac}})_{\mathfrak{m}} = \bigoplus_{\Pi'\in R_{\mathfrak{m}}} \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathbb{Q}_\ell^{\mathrm{ac}})[\Pi'^{\infty}]$$

as modules over $\mathbb{Z}[\mathbb{T}^{\mathtt{R}\cup\{\mathfrak{p}\}}]$. Then it was shown in the proof of [Tian and Xiao 2019, Theorem 4.4(2)] that on each Π'^{∞}-isotypic component, $\det(\mathrm{Res}(\Lambda) \circ \mathrm{Gys}(\Lambda))$ is equal to a power of

$$\pm p^{(g-1)/2\cdot\binom{g}{(g-1)/2}}[(\alpha_{\Pi'} - \beta_{\Pi'})^2/(\alpha_{\Pi'}\beta_{\Pi'})]^{t_{g,(g-1)/2}}$$

for $\Lambda = \mathbb{Q}_\ell^{\mathrm{ac}}$, where $t_{g,(g-1)/2} = \sum_{i=0}^{(g-1)/2-1} \binom{g}{i}$. By (4-10), it is clear that the same formula also holds for $\Lambda = \mathcal{O}_{\mathbb{E}_\lambda}$. Therefore, we see that $\det(\mathrm{Res}(\mathcal{O}_{\mathbb{E}_\lambda}) \circ \mathrm{Gys}(\mathcal{O}_{\mathbb{E}_\lambda}))$ is nonvanishing modulo λ by Definition 4.5(L2). It follows that $\mathrm{Res}(\Lambda) \circ \mathrm{Gys}(\Lambda)$ is an isomorphism for all choices of Λ, hence $\mathrm{Gys}(\Lambda)$ is injective and (1) follows.

The above argument also implies (2). □

We can now finish the proof of Theorem 4.7. The assertion that G' acts trivially on $\Gamma(\mathfrak{B} \times \mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)(\mathbb{F}_p^{\mathrm{ac}}), \mathcal{O}_{\mathbb{E}}/\lambda)_{\mathfrak{m}}$ follows from Theorem 3.13(2) and Definition 4.5(L3). We focus now on the surjectivity of $\Phi_{\mathfrak{m}}$ (4-4).

We write $k_\lambda = \mathcal{O}_{\mathbb{E}}/\lambda$ for simplicity as before. Under the canonical isomorphism

$$\Gamma(\mathfrak{B} \times \mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)(\mathbb{F}_p^{\mathrm{ac}}), k_\lambda)_{\mathfrak{m}} \cong \bigoplus_{\mathfrak{a} \in \mathfrak{B}} \Gamma(\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)_{\mathfrak{m}},$$

the map (4-5) is identified with the composite map

$$\begin{tikzcd}
\bigoplus_{\mathfrak{a} \in \mathfrak{B}} \Gamma(\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda)/\mathfrak{m} \arrow[r, "\oplus_{\mathfrak{a}} \Phi_{\mathfrak{m}}(\mathfrak{a})/\mathfrak{m}"] \arrow[dr, "\Phi_{\mathfrak{m}}/\mathfrak{m}"'] & \bigoplus_{\mathfrak{a} \in \mathfrak{B}} \mathrm{H}^1(\mathbb{F}_{p^{2g}}, \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}}, \varnothing'_{\mathfrak{a}}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda(1)/\mathfrak{m}) \arrow[d, "\mathrm{Gys}"] \\
& \mathrm{H}^1(\mathbb{F}_{p^{2g}}, \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda((g+1)/2))/\mathfrak{m}),
\end{tikzcd}$$

where the vertical map Gys is simply $\mathrm{H}^1(\mathbb{F}_{p^{2g}}, (\mathrm{Gys}(k_\lambda)/\mathfrak{m})(1))$. Here, we use the fact that the canonical maps

$$\mathrm{H}^1(\mathbb{F}_{p^{2g}}, \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}}, \varnothing'_{\mathfrak{a}}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda(1))/\mathfrak{m} \to \mathrm{H}^1(\mathbb{F}_{p^{2g}}, \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}}, \varnothing'_{\mathfrak{a}}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda(1)/\mathfrak{m})$$
$$\mathrm{H}^1(\mathbb{F}_{p^{2g}}, \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda((g+1)/2)))/\mathfrak{m} \to \mathrm{H}^1(\mathbb{F}_{p^{2g}}, \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda((g+1)/2))/\mathfrak{m})$$

are both isomorphisms since $\mathrm{H}^2(\mathbb{F}_{p^{2g}}, -)$ vanishes. By Proposition 4.8, the map $\oplus_{\mathfrak{a}} \Phi_{\mathfrak{m}}(\mathfrak{a})/\mathfrak{m}$ is surjective. To prove that $\Phi_{\mathfrak{m}}/\mathfrak{m}$ is surjective, it suffices to show that so is Gys.

First, we have a description of $\mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}}, \varnothing'_{\mathfrak{a}}}, K^p), k_\lambda(1))/\mathfrak{m}$ in terms of $\bar{\rho}_{\Pi,\lambda}$, which is the residue representation of (4-1) as we recall. Since $\bar{\rho}_{\Pi,\lambda}$ is absolutely irreducible by Remark 4.2(1), the $k_\lambda[\mathrm{G}_F]$-module $\mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}}, \varnothing_{\mathfrak{a}}}, K^p)_{\mathbb{Q}^{\mathrm{ac}}}, k_\lambda(1))/\mathfrak{m}$ is isomorphic to r copies of $\bar{\rho}^{\vee}_{\Pi,\lambda}(1) \cong \bar{\rho}_{\Pi,\lambda}$ with $r \geq \dim(\Pi_B^\infty)^K$ by [Boston et al. 1991] and the theory of old forms. By Remark 4.6(2), one has an isomorphism of $k_\lambda[\mathrm{G}']$-modules

$$\bar{\rho}_{\Pi,\lambda} \cong k_\lambda \oplus k_\lambda(1).$$

In particular, $\mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}}, \varnothing_{\mathfrak{a}}}, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda(1))/\mathfrak{m}$ is the direct sum of the eigenspaces of $\sigma_{\mathfrak{p}}^2$ with eigenvalues 1 and p^{2g} both with multiplicity r.

By [Brylinski and Labesse 1984], Remarks 4.2(4) and 4.6(3) and the similar argument as above, the (generalized) eigenvalues of $\sigma_{\mathfrak{p}}^2$ on $\mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, \mathbb{Q}_\ell^{\mathrm{ac}}((g+1)/2))/\mathfrak{m}$ are $p^{g(g+1)}\alpha_\Pi^{-2i}\beta_\Pi^{-2(g-i)}$ with multiplicity $\binom{g}{i}\dim(\Pi_B^\infty)^K$. Note that $p^{g(g+1)}\alpha_\Pi^{-2i}\beta_\Pi^{-2(g-i)}$ has image $p^{g(1+2i-g)}$ in $\mathbb{F}_\ell^{\mathrm{ac}}$, which are distinct for different i under Definition 4.5(L2). For every $\mu \in k_\lambda$, let

$$(\mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda((g+1)/2))/\mathfrak{m})^{\sigma_{\mathfrak{p}}^2 \approx \mu} \subseteq \mathrm{H}^g(\mathbf{Sh}(G, K^p)_{\mathbb{F}_p^{\mathrm{ac}}}, k_\lambda((g+1)/2))/\mathfrak{m}$$

denote the generalized eigenspace of $\sigma_{\mathfrak{p}}^2$ with eigenvalue μ, that is, the maximal subspace annihilated by $(\sigma_{\mathfrak{p}}^2-\mu)^{\ell^N}$ for $N=1,2,\dots$. Then by the base change property (4-10), one has a canonical decomposition

$$\mathrm{H}^g(\mathbf{Sh}(G,K^p)_{\mathbb{F}_p^{\mathrm{ac}}},k_\lambda((g+1)/2))/\mathfrak{m}=\bigoplus_{i=0}^{g}(\mathrm{H}^g(\mathbf{Sh}(G,K^p)_{\mathbb{F}_p^{\mathrm{ac}}},k_\lambda((g+1)/2))/\mathfrak{m})^{\sigma_{\mathfrak{p}}^2\approx p^{g(1+2i-g)}},$$

where the i-th direct summand has dimension $\binom{g}{i}\dim(\Pi_B^\infty)^K$ over k_λ. The direct summand with $\sigma_{\mathfrak{p}}^2\approx 1$ corresponds to the term with $i=(g-1)/2$, and it has dimension $\binom{g}{(g-1)/2}\dim(\Pi_B^\infty)^K$. Note that

$$\mathrm{H}^1(\mathbb{F}_{p^{2g}},(\mathrm{H}^g(\mathbf{Sh}(G,K^p)_{\mathbb{F}_p^{\mathrm{ac}}},k_\lambda((g+1)/2))/\mathfrak{m})^{\sigma_{\mathfrak{p}}^2\approx p^{g(1+2i-g)}})=0$$

for $i\neq(g-1)/2$. It follows that the natural map

$$(\mathrm{H}^g(\mathbf{Sh}(G,K^p)_{\mathbb{F}_p^{\mathrm{ac}}},k_\lambda((g+1)/2))/\mathfrak{m})^{\sigma_{\mathfrak{p}}^2\approx 1}\to\mathrm{H}^1(\mathbb{F}_{p^{2g}},\mathrm{H}^g(\mathbf{Sh}(G,K^p)_{\mathbb{F}_p^{\mathrm{ac}}},k_\lambda((g+1)/2))/\mathfrak{m})\tag{4-11}$$

is surjective. One gets a commutative diagram:

$$\begin{tikzcd}
\bigoplus_{\mathfrak{a}\in\mathfrak{B}}(\mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing'_{\mathfrak{a}}},K^p)_{\mathbb{F}_p^{\mathrm{ac}}},k_\lambda(1))/\mathfrak{m})^{\sigma_{\mathfrak{p}}^2=1} \arrow[r, "\cong"] \arrow[d, "(\mathrm{Gys}(k_\lambda)/\mathfrak{m})(1)", "\cong"'] & \bigoplus_{\mathfrak{a}\in\mathfrak{B}}\mathrm{H}^1(\mathbb{F}_{p^{2g}},\mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing'_{\mathfrak{a}}},K^p)_{\mathbb{F}_p^{\mathrm{ac}}},k_\lambda(1))/\mathfrak{m}) \arrow[d, "\mathrm{Gys}"] \\
(\mathrm{H}^g(\mathbf{Sh}(G,K^p)_{\mathbb{F}_p^{\mathrm{ac}}},k_\lambda((g+1)/2))/\mathfrak{m})^{\sigma_{\mathfrak{p}}^2\approx 1} \arrow[r, "(4\text{-}11)"] & \mathrm{H}^1(\mathbb{F}_{p^{2g}},\mathrm{H}^g(\mathbf{Sh}(G,K^p)_{\mathbb{F}_p^{\mathrm{ac}}},k_\lambda((g+1)/2))/\mathfrak{m})
\end{tikzcd}$$

Here, $(\mathrm{Gys}(k_\lambda)/\mathfrak{m})(1)$ is injective by Proposition 4.10(2), and we deduce that it is an isomorphism for dimension reasons. It follows immediately that Gys is surjective. This finishes the proof of Theorem 4.7.

5. Selmer groups of triple product motives

In this section, we study Selmer groups of certain triple product motives of elliptic curves in the context of the Bloch–Kato conjecture, which can be viewed as an application of the level raising result established in the previous section.

From now on, we fix a cubic totally real number field F, and let $\tilde{F}$ be the normal closure of F in $\mathbb{C}$.

5A. ***Main theorem.*** Let E be an elliptic curve over F. We have the $\mathbb{Q}$-motive $\otimes\operatorname{Ind}_{\mathbb{Q}}^F\mathsf{h}^1(E)$ (with coefficient $\mathbb{Q}$) of rank 8, which is the multiplicative induction of the F-motive $\mathsf{h}^1(E)$ to $\mathbb{Q}$. The *cubic-triple product motive* of E is defined to be

$$\mathsf{M}(E):=(\otimes\operatorname{Ind}_{\mathbb{Q}}^F\mathsf{h}^1(E))(2).$$

It is canonically polarized. For every prime p, the p-adic realization of $\mathsf{M}(E)$, denoted by $\mathsf{M}(E)_p$, is a Galois representation of $\mathbb{Q}$ of dimension 8 with $\mathbb{Q}_p$-coefficients. In fact, up to a twist, it is the multiplicative induction from F to $\mathbb{Q}$ of the rational p-adic Tate module of E.

Now we assume that E is modular. Then it gives rise to an irreducible cuspidal automorphic representation Π_E of $(\operatorname{Res}_{F/\mathbb{Q}}\mathrm{GL}_{2,F})(\mathbb{A})$ with trivial central character. In particular, the set $\Sigma(\Pi_E,\tau)$ defined in Section 1C contains ∞. We have $L(s,\mathsf{M}(E))=L\bigl(s+\frac{1}{2},\Pi_E,\tau\bigr)$ (again see Section 1C).

Put $\Delta^\flat := \Sigma(\Pi_E, \tau) - \{\infty\}$. Let Δ (resp. Δ', Δ'') be the set of primes of F above $\Delta^\flat$ that is of degree either 1 or 3 (resp. unramified of degree 2, ramified of degree 2). We write the conductor of E as $\mathfrak{c}\mathfrak{c}'\mathfrak{c}''\mathfrak{c}^+$ such that $\mathfrak{c}$ (resp. $\mathfrak{c}'$, $\mathfrak{c}''$, $\mathfrak{c}^+$) has factors in Δ (resp. Δ', Δ'', elsewhere).

Assumption 5.1. We consider the following assumptions:

(E0) The cardinality of $\Sigma(\Pi_E, \tau)$ is odd and at least 3.

(E1) For every finite place w of F over some prime in $\Sigma(\Pi_E, \tau)$, the elliptic curve E has either good or multiplicative reduction at w.

(E2) For distinct embeddings $\tau_1, \tau_2 \colon F \hookrightarrow \tilde{F}$, the $\tilde{F}$-elliptic curve $E \otimes_{F,\tau_1} \tilde{F}$ is not isogenous to any (possibly trivial) quadratic twist of $E \otimes_{F,\tau_2} \tilde{F}$.

Remark 5.2. Assumption 5.1(E0) implies that Δ is not empty. Assumption 5.1(E1) implies that E has multiplicative reduction at $w \in \Delta$. Together, they imply that the geometric fiber $E \otimes_F F^{\mathrm{ac}}$ does not admit complex multiplication.

We now assume that E is modular and satisfies Assumption 5.1. Then Assumption 5.1(E1) implies that $\mathfrak{c}\mathfrak{c}'$ is square-free, and $\mathfrak{c}'' = \mathcal{O}_F$ by [Liu 2019, Lemma 4.8]. We take an ideal $\mathfrak{r}$ of $\mathcal{O}_F$ contained in $N\mathfrak{c}^+$ for some integer $N \geq 4$ and coprime to $\Delta^\flat$.

Assumption 5.1(E0) implies that Δ is a nonempty finite set of even cardinality. Let B be a quaternion algebra over F, unique up to isomorphism, with ramification set Δ, and $\mathcal{O} \subseteq B$ be an $\mathcal{O}_F$-maximal order. Let $\mathfrak{r}_0$ and $\mathfrak{r}_1$ be two ideals of $\mathcal{O}_F$ such that $\mathfrak{r}_0$, $\mathfrak{r}_1$ and Δ are mutually coprime. We recall the definition of the Hilbert modular stack $\mathcal{X}(\Delta)_{\mathfrak{r}_0,\mathfrak{r}_1}$ over $\operatorname{Spec}(\mathbb{Z}[\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{r}_0\mathfrak{r}_1)^{-1}(\operatorname{disc} F)^{-1}])$ defined in [Liu 2019, Definition B.3]. For every $\mathbb{Z}[\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{r}_0\mathfrak{r}_1)^{-1}(\operatorname{disc} F)^{-1}]$-scheme T, $\mathcal{X}(\Delta)_{\mathfrak{r}_0,\mathfrak{r}_1}(T)$ is the groupoid of quadruples $(A, \iota_A, C_A, \alpha_A)$ where

- A is a projective abelian scheme over T;
- $\iota_A \colon \mathcal{O} \to \operatorname{End}(A)$ is an injective homomorphism satisfying

$$\operatorname{Tr}(\iota_A(b) \,|\, \operatorname{Lie}(A)) = \operatorname{Tr}_{F/\mathbb{Q}} \operatorname{Tr}^\circ_{B/F}(b)$$

  for all $b \in \mathcal{O}$;
- C_A is an $\mathcal{O}$-stable finite flat subgroup of $A[\mathfrak{r}_0]$ which is étale locally isomorphic to $(\mathcal{O}_F/\mathfrak{r}_0)^2$ as $\mathcal{O}/\mathfrak{r}_0\mathcal{O} \cong \mathrm{M}_2(\mathcal{O}_F/\mathfrak{r}_0)$-modules;
- $\alpha_A \colon (\mathcal{O}_F/\mathfrak{r}_1)^2_T \to A$ is an $\mathcal{O}$-equivariant injective homomorphism of group schemes over T.

If $\mathfrak{r}_1 = \mathcal{O}_F$, α_A is trivial and we usually omit it from the notation. If $\mathfrak{r}_1$ is contained in $N\mathcal{O}_F$ for some integer $N \geq 4$, then $\mathcal{X}(\Delta)_{\mathfrak{r}_0,\mathfrak{r}_1}$ is a scheme.

We put $\mathcal{X}_{\mathfrak{r}} := \mathcal{X}(\Delta)_{\mathfrak{c}',\mathfrak{r}}$. Let $\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)$ be the set of all ideals of O_F containing $\mathfrak{r}(\mathfrak{c}^+)^{-1}$ as in [Liu 2019, Notation A.5]. For every $\mathfrak{d} \in \mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)$, we have the following composite map

$$\tilde{\delta}^{\mathfrak{d}} \colon \mathcal{X}_{\mathfrak{r}} = \mathcal{X}(\Delta)_{\mathfrak{c}',\mathfrak{r}} \to \mathcal{X}(\Delta)_{\mathfrak{c}'\mathfrak{r},\mathcal{O}_F} \xrightarrow{\delta^{\mathfrak{d}}} \mathcal{X}(\Delta)_{\mathfrak{c}'\mathfrak{c}^+,\mathcal{O}_F} \tag{5-1}$$

which is a finite étale morphism of Deligne–Mumford stacks, where $\delta^{\mathfrak{d}}$ is the degeneracy map defined as follows. If (A, ι_A, C_A) is an object of $\mathcal{X}(\Delta)_{\mathfrak{c}'\mathfrak{r},\mathcal{O}_F}(T)$ for some $\mathrm{Spec}(\mathbb{Z}[\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{c}'\mathfrak{r})^{-1}\,\mathrm{disc}(F)^{-1}])$-scheme T, then its image by $\delta^{\mathfrak{d}}$ is given by the object $(A', \iota_{A'}, C_{A'})$, where

- A' is the quotient A by the finite flat subgroup $C_A[\mathfrak{d}]$,
- $\iota_{A'}$ is the induced $\mathcal{O}$-action on A' from A,
- $C_{A'}$ is the unique subgroup scheme of $C_A/C_A[\mathfrak{d}]$ étale locally isomorphic to $(\mathcal{O}_F/\mathfrak{c}'\mathfrak{c}^+)^2$.

See [Liu 2019, Section B.1] for more details.

Remark 5.3. The requirement that $|\Sigma(\Pi_E, \tau)| \geq 3$, that is, $\Delta \neq \varnothing$ is not essential. The reason we require this is *not* to make the relevant Shimura variety $\mathcal{X}_{\mathfrak{r}}$ proper. In fact, it is used to obtain a refinement (Proposition 5.13) of Theorem 4.7 so that the map (4-5) is also *injective* in order to deduce Lemma 5.18 which is needed for the *first explicit reciprocity law* back in [Liu 2019], through a trick using Jacquet–Langlands correspondence. However, it is not clear to us what are optimal conditions for the map (4-5) to be injective.

From now on, we fix an element $\mathfrak{w} \in \Delta$. Let $\mathcal{B}$ be the totally definite quaternion algebra over F, ramified exactly at $\Delta \setminus \{\mathfrak{w}\}$. Put

$$\mathcal{Y}_{\mathfrak{r}} := \mathcal{B}^\times \backslash \widehat{\mathcal{B}}^\times / K_{0,1}(\mathfrak{w}\mathfrak{c}', \mathfrak{r})$$

where $K_{0,1}(\mathfrak{w}\mathfrak{c}', \mathfrak{r}) \subseteq \widehat{\mathcal{B}}^\times$ is an open compact subgroup defined similarly as in Example 2.12.

For every ideal $\mathfrak{s}$ contained in $\mathfrak{c}^+$, we let $\mathtt{R}(\mathfrak{s})$ be the union of primes dividing $\mathfrak{s}$ and primes above $\Delta^\flat$. In particular, we have the homomorphism

$$\phi^{\mathfrak{s}} := \phi^{\mathtt{R}(\mathfrak{s})}_{\Pi_E} \colon \mathbb{Z}[\mathbb{T}^{\mathtt{R}(\mathfrak{s})}] \to \mathbb{Z}$$

such that $\phi^{\mathfrak{s}}(\mathrm{T}_{\mathfrak{q}}) = a_{\mathfrak{q}}(E)$ and $\phi^{\mathfrak{s}}(\mathrm{S}_{\mathfrak{q}}) = 1$ for every prime $\mathfrak{q} \notin \mathtt{R}(\mathfrak{s})$. Here we recall that $\mathbb{T}^{\mathtt{R}}$ is the Hecke monoid away from $\mathtt{R}$ [Liu 2019, Notation 3.1].

Let p be a rational prime.[5] Let $\mathfrak{m}^{\mathfrak{s}}_p$ be the kernel of the composite map $\mathbb{Z}[\mathbb{T}^{\mathtt{R}(\mathfrak{s})}] \xrightarrow{\phi^{\mathfrak{s}}} \mathbb{Z} \to \mathbb{F}_p$. We also have an induced Galois representation

$$\rho_{\Pi_E,p} \colon \mathrm{G}_F \to \mathrm{GL}(T_p(E)) \cong \mathrm{GL}_2(\mathbb{Z}_p),$$

where $T_p(E)$ is the p-adic Tate module of E. Put $\bar{\rho}_{\Pi_E,p} := \rho_{\Pi_E,p} \mod p$.

Definition 5.4 (perfect pair). We say that:

(1) p is *generic* if $(\mathrm{Ind}^{\mathbb{Q}}_F\, \bar{\rho}_{\Pi_E,p})|_{\mathrm{G}_{\tilde{F}}}$ has the largest possible image, which is isomorphic to $\mathrm{G}(\mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p) \times \mathrm{SL}_2(\mathbb{F}_p))$.

(2) The pair $(p, \mathfrak{r})$ is $\mathfrak{s}$-*clean*, for an ideal $\mathfrak{s}$ of $\mathcal{O}_F$ contained in $\mathfrak{r}$, if:

(a) The space $\Gamma(\mathcal{Y}_{\mathfrak{r}}, \mathbb{Z}_p)/\mathfrak{m}^{\mathfrak{s}}_p$ has dimension $|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$ over $\mathbb{F}_p$.

[5] The readers may notice that we switch the roles of p and ℓ (or λ) in Section 5 from Section 4. This is due to a different convention in the study of Selmer groups.

(b) $\mathrm{H}^3(\mathcal{X}(\Delta)_{\mathfrak{c}'\mathfrak{c}^+,\mathcal{O}_F} \otimes \mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p)/\mathfrak{m}_p^{\mathfrak{s}}$ has dimension 8 over $\mathbb{F}_p$, and the canonical map

$$\bigoplus_{\mathfrak{d}\in\mathfrak{D}(\mathfrak{r},\mathfrak{c}^+)} \tilde{\delta}^{\mathfrak{d}}_*\colon \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p)/\mathfrak{m}_p^{\mathfrak{s}} \to \bigoplus_{\mathfrak{d}\in\mathfrak{D}(\mathfrak{r},\mathfrak{c}^+)} \mathrm{H}^3(\mathcal{X}(\Delta)_{\mathfrak{c}'\mathfrak{c}^+,\mathcal{O}_F} \otimes \mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p)/\mathfrak{m}_p^{\mathfrak{s}}$$

is an isomorphism.

(3) The pair $(p, \mathfrak{r})$ is *perfect* if:

(a) $p \geq 11$ and $p \neq 13, 19$.

(b) p is coprime to $\Delta^\flat$ and $\mathfrak{r}\cdot|(\mathbb{Z}/\mathfrak{r}\cap\mathbb{Z})^\times|\cdot\mu(\mathfrak{r}, \mathfrak{c}^+)\cdot|\mathrm{Cl}(F)_\mathfrak{r}|\cdot\mathrm{disc}\, F$, where disc F is the discriminant of F, $\mathrm{Cl}(F)_\mathfrak{r}$ is the ray class group of F with respect to $\mathfrak{r}$, and

$$\mu(\mathfrak{r}, \mathfrak{c}^+) = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{r}(\mathfrak{c}^+)^{-1}) \prod_{\mathfrak{q}} \left(1 + \frac{1}{\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{q})}\right)$$

with $\mathfrak{q}$ running through the prime ideals of $\mathcal{O}_F$ dividing $\mathfrak{r}$ but not $\mathfrak{c}^+$.

(c) p is generic.

(d) It is $\mathfrak{r}$-clean.

(e) $\bar{\rho}_{\Pi_E,p}$ is ramified at $\mathfrak{w}$.

Remark 5.5. Note that the condition that p is generic implies that the condition $(\mathbf{LI}_{\mathrm{Ind}\bar{\rho}_{\Pi_E,p}})$ in [Dimitrov 2005, Proposition 0.1] is satisfied. Consequently, $\mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p)_{\mathfrak{m}_p^{\mathfrak{s}}}$ is finite free over $\mathbb{Z}_p$ for any ideal $\mathfrak{s}$ of $\mathcal{O}_F$ containing $\mathfrak{r}$ by [loc. cit., Theorem 0.3].

Let $B^\flat$ be a quaternion algebra over $\mathbb{Q}$, unique up to isomorphisms, with ramification set $\Delta^\flat$ so that $B \cong B^\flat \otimes_\mathbb{Q} F$. We have similarly a moduli scheme $\mathcal{X}^\flat_\mathfrak{r} := \mathcal{X}(\Delta^\flat)_{\mathbb{Z},\mathfrak{r}\cap\mathbb{Z}}$ attached to $B^\flat$. Then we obtain a canonical morphism

$$\theta\colon \mathcal{X}^\flat_\mathfrak{r} \to \mathcal{X}_\mathfrak{r}$$

over $\mathbb{Z}[(\mathfrak{r}\,\mathrm{disc}\, F)^{-1}]$ similar to [Liu 2019, (4.1.1)]. It is a finite morphism. Denote by $\Theta_{p,\mathfrak{r}}$ the image of $\theta_*[\mathcal{X}^\flat_\mathfrak{r} \otimes \mathbb{Q}] \in \mathrm{CH}^2(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q})$ under the Abel–Jacobi map

$$\mathrm{AJ}_p\colon \mathrm{CH}^2(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}) \to \mathrm{H}^1(\mathbb{Q}, \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \mathbb{Q}_p(2))/\ker \phi^\mathfrak{r}).$$

By [loc. cit., Lemma 4.6], we have $\mathrm{H}^1(\mathbb{Q}_v, \mathsf{M}(E)_p) = 0$ for all primes $v \nmid p$. Thus, we recall the following definition.

Definition 5.6 [Bloch and Kato 1990; Liu 2019, Definition 4.7]. The *Bloch–Kato Selmer group* for the representation $\mathsf{M}(E)_p$ is the subspace $\mathrm{H}^1_f(\mathbb{Q}, \mathsf{M}(E)_p)$ consisting of classes $s \in \mathrm{H}^1(\mathbb{Q}, \mathsf{M}(E)_p)$ such that

$$\mathrm{loc}_p(s) \in \mathrm{H}^1_f(\mathbb{Q}_p, \mathsf{M}(E)_p) := \ker[\mathrm{H}^1(\mathbb{Q}_p, \mathsf{M}(E)_p) \to \mathrm{H}^1(\mathbb{Q}_p, \mathsf{M}(E)_p \otimes_{\mathbb{Q}_p} \mathrm{B}_{\mathrm{cris}})].$$

Theorem 5.7. *Let E be a modular elliptic curve over F satisfying Assumption 5.1. For a rational prime p, if there exists a perfect pair $(p, \mathfrak{r})$ (Definition 5.4) such that $\Theta_{p,\mathfrak{r}} \neq 0$, then*

$$\dim_{\mathbb{Q}_p} \mathrm{H}^1_f(\mathbb{Q}, \mathsf{M}(E)_p) = 1.$$

Remark 5.8. By an argument similar to [Liu 2019, Lemma 4.10], given an ideal $\mathfrak{r}$ of $\mathcal{O}_F$ contained in $N\mathfrak{c}^+$ for some integer $N \geq 4$ and coprime to $\Delta^\flat$, there exists a finite set $\mathcal{P}_{E,\mathfrak{r}}$ of rational primes such that $(p, \mathfrak{r})$ is a perfect pair for every $p \notin \mathcal{P}_{E,\mathfrak{r}}$. An upper bound for $\mathcal{P}_{E,\mathfrak{r}}$ can be computed effectively.

Remark 5.9. Assuming the (conjectural) triple product version of the Gross–Zagier formula and the Beilinson–Bloch conjecture on the injectivity of the Abel–Jacobi map, the following two statements should be equivalent:

- $L'(0, \mathsf{M}(E)) \neq 0$ (note that $L(0, \mathsf{M}(E)) = 0$ by Assumption 5.1(E0)).
- There exists some $\mathfrak{r}_0$ such that for every other $\mathfrak{r}$ contained in $\mathfrak{r}_0$, we have $\Theta_{p,\mathfrak{r}} \neq 0$ as long as $(p, \mathfrak{r})$ is a perfect pair.

Here, we need to use (the proof of) [Liu 2019, Proposition 4.9]. Then Theorem 5.7 implies that if $L'(0, \mathsf{M}(E)) \neq 0$, that is, $\operatorname{ord}_{s=0} L(s, \mathsf{M}(E)) = 1$, then $\dim_{\mathbb{Q}_p} \mathrm{H}^1_f(\mathbb{Q}, \mathsf{M}(E)_p) = 1$ for all but finitely many p.

5B. *A refinement of arithmetic level raising.* From now on, we fix a perfect pair $(p, \mathfrak{r})$ (Definition 5.4), and put $\mathfrak{m}^\mathfrak{s} := \mathfrak{m}^\mathfrak{s}_p$ for short.

Definition 5.10. Let $\nu \geq 1$ be an integer. We say that a prime ℓ is $(p^\nu, \mathfrak{r})$-*admissible* if:

(A1) ℓ is inert in F (with $\mathfrak{l} = \ell\mathcal{O}_F$), unramified in $\tilde{F}$, and coprime to $\mathtt{R}(\mathfrak{r}) \cup \{2, p\}$.

(A2) $(p, \mathfrak{r})$ is $\mathfrak{r}\mathfrak{l}$-clean.

(A3) $p \nmid (\ell^{18} - 1)(\ell^6 + 1)$.

(A4) $\phi^\mathfrak{r}(\mathrm{T}_\mathfrak{l}) \equiv \ell^3 + 1 \mod p^\nu$.

Notation 5.11. For now on, we fix an integer $\nu \geq 1$ and put $\Lambda := \mathbb{Z}/p^\nu$. Let $\rho\colon \mathrm{G}_F \to \mathrm{GL}(\mathrm{N}_\rho)$ be the reduction of $\rho_{\Pi_E,p}$ modulo p^ν, where $\mathrm{N}_\rho = T_p(E) \otimes \Lambda$. We have the multiplicatively induced representation $\rho^\sharp\colon \mathrm{G}_\mathbb{Q} \to \mathrm{GL}(\mathrm{N}^\sharp_\rho)$ with $\mathrm{N}^\sharp_\rho = \mathrm{N}_\rho^{\otimes 3}$.

Lemma 5.12. *Let ℓ be a $(p^\nu, \mathfrak{r})$-admissible prime. Then the cohomology groups*

$$\mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \mathrm{H}^3(\mathcal{X}(\Delta)_{\mathfrak{c}'\mathfrak{c}^+,\mathcal{O}_F} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}), \quad \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}})$$

are free Λ-modules of ranks 1 *and* $|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$, *respectively.*

Proof. By Definition 5.10(A2), Nakayama's lemma and [Brylinski and Labesse 1984], we have isomorphisms of $\Lambda[\mathrm{G}_{\mathbb{Q}_\ell}]$-modules

$$\mathrm{H}^3(\mathcal{X}(\Delta)_{\mathfrak{c}'\mathfrak{c}^+,\mathcal{O}_F} \otimes \mathbb{Q}^{\mathrm{ac}}_\ell, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}} \cong \mathrm{N}^\sharp_\rho(-1), \quad \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}_\ell, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}} \cong \mathrm{N}^\sharp_\rho(-1)^{\oplus|\mathfrak{D}(\mathfrak{r},\mathfrak{c}^+)|}.$$

If $\sigma_\mathfrak{l} \in \mathrm{G}_F$ denotes an arithmetic Frobenius element at $\mathfrak{l}$, then $\rho(\sigma_\mathfrak{l})$ is conjugate to $\left(\begin{smallmatrix}1 & 0\\ 0 & \ell^3\end{smallmatrix}\right)$ by Definition 5.10(A4). Hence, the $\Lambda[\mathrm{G}_{\mathbb{Q}_\ell}]$-module $\mathrm{N}^\sharp_\rho(-1)$ is unramified and isomorphic to $\Lambda(-1) \oplus \Lambda \oplus \mathrm{R} \oplus \Lambda(1) \oplus \mathrm{R}(1) \oplus \Lambda(2)$, where $\mathrm{R} \cong \Lambda^{\oplus 2}$ is the rank 2 unramified representation of $\mathrm{G}_{\mathbb{Q}_\ell}$ with the action of the arithmetic Frobenius σ_ℓ given by $\left(\begin{smallmatrix}0 & -1\\ 1 & -1\end{smallmatrix}\right)$. By Definition 5.10(A3), it follows that $\mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \mathrm{N}^\sharp_\rho(-1)) \cong \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \Lambda)$, which is free of rank 1 over Λ. □

Let ℓ be a $(p^\nu, \mathfrak{r})$-admissible prime. Then $\mathcal{X}_{\mathfrak{r}} \otimes \mathbb{Z}_{(\ell)}$ is canonically isomorphic to $\mathbf{Sh}(G, K_{0,1}(\mathfrak{c}', \mathfrak{r})^{\ell})$ with $G = \mathrm{Res}_{F/\mathbb{Q}} B^\times$ considered in Section 2E (See Remark 2.5 on the issue of polarizations and Example 2.12 for the open compact subgroup $K_{0,1}(\mathfrak{c}', \mathfrak{r})$), and $\mathcal{X}^{\flat}_{\mathfrak{r}} \otimes \mathbb{Z}_{(\ell)}$ is canonically isomorphic to $\mathbf{Sh}(G^\flat, K_{0,1}(\mathbb{Z}, \mathfrak{r}\cap\mathbb{Z})^{\ell})$ with $G^\flat = (B^\flat)^\times$. Put $X_{\mathfrak{r}} := \mathcal{X}_{\mathfrak{r}} \otimes \mathbb{F}_\ell$. As before, we denote by $X^{\mathrm{sp}}_{\mathfrak{r}}$ the superspecial locus of $X_{\mathfrak{r}}$. By Theorem 3.16, we may identify $X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_\ell)$ with $\mathbf{Sh}(G_{\mathtt{S}_{\max}}, K_{0,1}(\mathfrak{c}', \mathfrak{r})^{\ell})(\mathbb{F}^{\mathrm{ac}}_\ell)$.

The following proposition is a refinement of Theorem 4.7 in our situation.

Proposition 5.13. *Let ℓ be a $(p^\nu, \mathfrak{r})$-admissible prime. Then the level raising map*

$$\Gamma(\mathfrak{B} \times X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_\ell), \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \to \mathrm{H}^1(\mathbb{F}_{\ell^6}, \mathrm{H}^3(X_{\mathfrak{r}} \otimes \mathbb{F}^{\mathrm{ac}}_\ell, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}) \tag{5-2}$$

defined similarly as (4-5) *is an isomorphism.*

Proof. In the proof of Lemma 5.12, we have seen that, as a $\Lambda[\mathrm{G}_{\mathbb{F}_\ell}]$-module, $\mathrm{H}^3(X_{\mathfrak{r}} \otimes \mathbb{F}^{\mathrm{ac}}_\ell, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}$ is isomorphic to $|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$-copies of

$$\mathrm{N}^\sharp_\rho(-1) \cong \Lambda(-1) \oplus \Lambda \oplus \mathrm{R} \oplus \Lambda(1) \oplus \mathrm{R}(1) \oplus \Lambda(2).$$

We get thus an isomorphism of $\Lambda[\mathrm{Gal}(\mathbb{F}_{\ell^6}/\mathbb{F}_\ell)]$-modules

$$\mathrm{H}^1(\mathbb{F}_{\ell^6}, \mathrm{H}^3(X_{\mathfrak{r}} \otimes \mathbb{F}^{\mathrm{ac}}_\ell, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}) \cong \mathrm{H}^1(\mathbb{F}_{\ell^6}, \Lambda \oplus \mathrm{R})^{\oplus|\mathfrak{D}(\mathfrak{r},\mathfrak{c}^+)|} \cong (\Lambda \oplus \mathrm{R})^{\oplus|\mathfrak{D}(\mathfrak{r},\mathfrak{c}^+)|}, \tag{5-3}$$

which is free of rank $3|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$ over Λ. By Theorem 4.7 and Nakayama's lemma, the map (5-2) is surjective. Thus it suffices to show that $\Gamma(X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_\ell), \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}}$ is a free Λ-module of rank $|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$. By Nakayama's lemma, it suffices to show that $\Gamma(X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_\ell), \mathbb{F}_p)/\mathfrak{m}^{\mathfrak{r}\mathfrak{l}}$ has dimension $|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$ over $\mathbb{F}_p$.

Recall that so far, we have three quaternion algebras over F in the story: $\mathcal{B}$ ramified at $\Sigma_\infty \cup \Delta \setminus \{\mathfrak{w}\}$, B ramified at Δ, and $B_{\mathtt{S}_{\max}}$ ramified at $\Sigma_\infty \cup \{\mathfrak{l}\} \cup \Delta$. Now we let B' be the fourth quaternion algebra over F ramified at $\Sigma \cup \{\mathfrak{l}\} \cup \Delta \setminus \{\mathfrak{w}\}$ where Σ is a fixed subset of Σ_∞ of cardinality 2. Let C be the corresponding proper Shimura curve over F (with the embedding into $\mathbb{Q}^{\mathrm{ac}}$ given by the unique element in $\Sigma_\infty \setminus \Sigma$) of the similarly defined level $K_{0,1}(\mathfrak{w}\mathfrak{c}', \mathfrak{r})$. As in Step 4 of the proof of [Liu 2019, Proposition 3.32], C has a natural strictly semistable model at $\mathfrak{l}$. The corresponding weight spectral sequence provides us with a canonical isomorphism

$$\Gamma(\mathcal{Y}_{\mathfrak{r}}, \mathbb{Z}_p)/\mathfrak{m}^{\mathfrak{r}\mathfrak{l}} \simeq \mathrm{H}^1_{\mathrm{sing}}(\mathbb{Q}_{\ell^6}, \mathrm{H}^1(C \otimes \mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p)/\mathfrak{m}^{\mathfrak{r}\mathfrak{l}})$$

as in the proof of [Liu 2019, Proposition 3.32]. By Definition 5.10(A2), $\mathrm{H}^1_{\mathrm{sing}}(\mathbb{Q}_{\ell^6}, \mathrm{H}^1(C \otimes \mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p)/\mathfrak{m}^{\mathfrak{r}\mathfrak{l}})$ has dimension $|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$. By [Boston et al. 1991], we conclude that $\mathrm{H}^1(C \otimes \mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p)/\mathfrak{m}^{\mathfrak{r}\mathfrak{l}}$ is isomorphic to $\bar{\rho}^{\oplus|\mathfrak{D}(\mathfrak{r},\mathfrak{c}^+)|}_{\Pi_E, p}$ as an $\mathbb{F}_p[\mathrm{G}_F]$-module. In particular, $\mathrm{H}^1(C \otimes \mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p)/\mathfrak{m}^{\mathfrak{r}\mathfrak{l}}$ has dimension $2|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$.

Now consider the semistable reduction of C at $\mathfrak{w}$. Let C_0 be the proper Shimura curve over F associated to B' of the level $K_{0,1}(\mathfrak{c}', \mathfrak{r})$. Then $\mathrm{H}^1(C_0 \otimes \mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p)/\mathfrak{m}^{\mathfrak{r}\mathfrak{l}} = 0$ by Definition 5.4(3e). Therefore, we have a canonical isomorphism

$$\mathrm{H}^1(\mathrm{I}_{\mathfrak{w}}, \mathrm{H}^1(C \otimes \mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p)/\mathfrak{m}^{\mathfrak{r}\mathfrak{l}}) \simeq \Gamma(X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_\ell), \mathbb{F}_p)/\mathfrak{m}^{\mathfrak{r}\mathfrak{l}}$$

from the weight spectral sequence, as the supersingular set of C at $\mathfrak{w}$ is also $X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_{\ell})$. Therefore, $\Gamma(X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_{\ell}), \mathbb{F}_p)/\mathfrak{m}^{\mathfrak{r}\mathfrak{l}}$ has dimension $|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^{+})|$. The proposition follows. □

5C. *Second explicit reciprocity law.* Let ℓ be a $(p^{\nu}, \mathfrak{r})$-admissible prime, and $\mathfrak{l} = \ell O_F$. Recall that Σ_{∞} denotes the set of archimedean places of F. For every ideal $\mathfrak{s}$ of O_F coprime to $\Delta \cup \{\mathfrak{l}\}$, let $\mathcal{S}_{\ell,\mathfrak{s}} := \mathcal{S}(\Sigma_{\infty} \cup \Delta \cup \{\mathfrak{l}\})_{\mathfrak{s}}$ be the set of isomorphism classes of oriented O_F-Eichler orders of discriminant $\Sigma_{\infty} \cup \Delta \cup \{\mathfrak{l}\}$ and level $\mathfrak{s}$ (see [Liu 2019, Definition A.1]). It has an action by $\mathrm{G}_{\mathbb{F}_{\ell}}$ such that the arithmetic Frobenius σ_{ℓ} acts by switching the orientation at $\mathfrak{l}$.

Lemma 5.14. *There is a canonical isomorphism* $X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_{\ell})/\operatorname{Cl}(F)_{\mathfrak{r}} \cong \mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}$. *Moreover, the induced action of* $\mathrm{G}_{\mathbb{F}_{\ell}}$ *on* $\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}$ *factors through* $\operatorname{Gal}(\mathbb{F}_{\ell^2}/\mathbb{F}_{\ell})$ *and is given by the map* op_{ℓ} *switching the orientation at* $\mathfrak{l}$.

Proof. It is a special case of [loc. cit., Proposition A.13(1)]. □

Denote by $\psi\colon X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_{\ell}) \to \mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}$ the canonical projection from the above lemma.

Lemma 5.15. *The canonical map*

$$\psi^{*}\colon \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \to \Gamma(X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_{\ell}), \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}}$$

is an isomorphism.

Proof. It follows similarly to [loc. cit., Lemma 3.24]. □

Proposition 5.16. *Under the notation above, the following statements hold*:

(1) *The action of* op_{ℓ} *on* $\Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}}$ *is trivial.*

(2) *There exists a unique isomorphism* Φ *such that the following diagram is commutative, where the lower left vertical arrow is the diagonal map*:

$$\begin{tikzcd}
\Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \arrow[r, "\Phi"] \arrow[d, "\psi^{*}"] & \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_{\ell}, \mathrm{H}^3(\mathcal{X}_{\mathfrak{r}} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2)/\ker\phi^{\mathfrak{r}\mathfrak{l}}) \arrow[d, "\cong"] \\
\Gamma(X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_{\ell}), \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \arrow[d] & \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_{\ell^6}, \mathrm{H}^3(\mathcal{X}_{\mathfrak{r}} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2)/\ker\phi^{\mathfrak{r}\mathfrak{l}}))^{\operatorname{Gal}(\mathbb{Q}_{\ell^6}/\mathbb{Q}_{\ell})} \arrow[d, hook] \\
\Gamma(\mathfrak{B} \times X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_{\ell}), \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \arrow[r, "(5\text{-}2)"] & \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_{\ell^6}, \mathrm{H}^3(\mathcal{X}_{\mathfrak{r}} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2)/\ker\phi^{\mathfrak{r}\mathfrak{l}}))
\end{tikzcd}$$

Proof. Consider the action of $\operatorname{Gal}(\mathbb{Q}_{\ell^6}/\mathbb{Q}_{\ell})$ on both sides of the isomorphism

$$\Gamma(\mathfrak{B} \times \mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \xrightarrow{\psi^{*}} \Gamma(\mathfrak{B} \times X^{\mathrm{sp}}_{\mathfrak{r}}(\mathbb{F}^{\mathrm{ac}}_{\ell}), \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \to \mathrm{H}^1(\mathbb{F}_{\ell^6}, \mathrm{H}^3(X_{\mathfrak{r}} \otimes \mathbb{F}^{\mathrm{ac}}_{\ell}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}).$$

By (5-3), we obtain an isomorphism

$$(\Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}})^{\mathrm{op}_{\ell}=1} \cong \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_{\ell}, \mathrm{H}^3(\mathcal{X}_{\mathfrak{r}} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2)/\ker\phi^{\mathfrak{r}\mathfrak{l}}).$$

By Lemma 5.12, $\mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2)/\ker\phi^{\mathfrak{r}\mathfrak{l}})$ is a free Λ-module of rank $|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$. Therefore, the inclusion

$$(\Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}})^{\mathrm{op}_\ell=1} \subseteq \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}}$$

is an isomorphism as both sides are free Λ-module of rank $|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$. Thus both (1) and (2) follow. □

Denote by $\Theta^\nu_{p,\mathfrak{r}}$ the image of $\theta_*[\mathcal{X}^\flat_\mathfrak{r} \otimes \mathbb{Q}] \in \mathrm{CH}^2(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q})$ under the Abel–Jacobi map

$$\mathrm{AJ}_p\colon\ \mathrm{CH}^2(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}) \to \mathrm{H}^1(\mathbb{Q}, \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}).$$

For any ideal $\mathfrak{s} \subseteq \mathcal{O}_F$, let $\mathcal{S}^\flat_{\ell,\mathfrak{s}} = \mathcal{S}(\{\infty\} \cup \Delta^\flat \cup \{\ell\})_{\mathfrak{s}\cap\mathbb{Z}}$ denote the set of isomorphism classes of oriented $\mathbb{Z}$-Eichler orders of discriminant $\{\infty\} \cup \Delta^\flat \cup \{\ell\}$ and level $\mathfrak{s} \cap \mathbb{Z}$ [Liu 2019, Definition A.1]. We have a natural map given by extension of scalars

$$\vartheta\colon \mathcal{S}^\flat_{\ell,\mathfrak{r}} \to \mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}. \tag{5-4}$$

We have a bilinear pairing $(\,\cdot\,,\cdot\,)\colon \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \mathbb{Z}) \times \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \mathbb{Z}) \to \mathbb{Z}$ defined by the formula $(f_1, f_2) = \sum_{h\in\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}} f_1(h) f_2(h)$. It induces a perfect pairing

$$(\,\cdot\,,\cdot\,)\colon \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \times \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)[\ker\phi^{\mathfrak{r}\mathfrak{l}}] \to \Lambda.$$

Theorem 5.17 (second explicit reciprocity law). *Let ℓ be an $(p^\nu, \mathfrak{r})$-admissible prime. Then* $\mathrm{loc}_\ell(\Theta^\nu_{p,\mathfrak{r}})$ *lies in* $\mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}})$, *and we have*

$$(\Phi^{-1}\,\mathrm{loc}_\ell\,\Theta^\nu_{p,\mathfrak{r}}, f) = \frac{|(\mathbb{Z}/\mathfrak{r}\cap\mathbb{Z})^\times|}{(\ell-1)^2|\mathrm{Cl}(F)_\mathfrak{r}|} \cdot \sum_{x\in\mathcal{S}^\flat_{\ell,\mathfrak{r}}} f(\vartheta(x))$$

for every $f \in \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)[\ker\phi^{\mathfrak{r}\mathfrak{l}}]$. *Here*, Φ *is the isomorphism in Proposition 5.16.*

We note that $(\ell-1)^2|\mathrm{Cl}(F)_\mathfrak{r}|$ is invertible in Λ.

Proof. The fact that $\Theta^\nu_{p,\mathfrak{r}}$ is unramified follows from the fact that both $\mathfrak{X}_\mathfrak{r}$ and $\mathfrak{X}^\flat_\mathfrak{r}$ have good reduction at ℓ. Recall that $X_\mathfrak{r} = \mathcal{X}_\mathfrak{r} \otimes \mathbb{F}_\ell$. Similarly, we put $X^\flat_\mathfrak{r} := \mathcal{X}^\flat_\mathfrak{r} \otimes \mathbb{F}_\ell$. Then we have the morphism $\theta\colon X^\flat_\mathfrak{r} \to X_\mathfrak{r}$ over $\mathbb{F}_\ell$. Let $\overline{\Theta}$ be the image of $\theta_*[X^\flat_\mathfrak{r}] \in \mathrm{CH}^2(X_\mathfrak{r})$ in the Galois cohomology $\mathrm{H}^1(\mathbb{F}_\ell, \mathrm{H}^3(X_\mathfrak{r} \otimes \mathbb{F}^{\mathrm{ac}}_\ell, \Lambda(2)/\ker\phi^{\mathfrak{r}\mathfrak{l}})$ defined similarly as for $\Theta^\nu_{p,\mathfrak{r}}$. Then under the canonical identification

$$\mathrm{H}^1(\mathbb{F}_\ell, \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{F}^{\mathrm{ac}}_\ell, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}) \cong \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}),$$

$\overline{\Theta}$ coincides with $\mathrm{loc}_\ell\,\Theta^\nu_{p,\mathfrak{r}}$.

From Proposition 5.13, we have an isomorphism

$$\Gamma(\mathfrak{B} \times X^{\mathrm{sp}}_\mathfrak{r}(\mathbb{F}^{\mathrm{ac}}_\ell), \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} = \bigoplus_{\mathfrak{a}\in\mathfrak{B}} \Gamma(X^{\mathrm{sp}}_\mathfrak{r}(\mathbb{F}^{\mathrm{ac}}_\ell), \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \xrightarrow{\cong} \mathrm{H}^1(\mathbb{F}_{\ell^6}, \mathrm{H}^3(X_\mathfrak{r} \otimes \mathbb{F}^{\mathrm{ac}}_\ell, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}).$$

For each $\mathfrak{a} \in \mathfrak{B}$, we denote by

$$\Psi_\mathfrak{a}\colon \mathrm{H}^1(\mathbb{F}_{\ell^6}, \mathrm{H}^3(X_\mathfrak{r} \otimes \mathbb{F}^{\mathrm{ac}}_\ell, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}) \to \Gamma(X^{\mathrm{sp}}_\mathfrak{r}(\mathbb{F}^{\mathrm{ac}}_\ell), \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}}$$

the map obtained by taking the inverse of the previous isomorphism followed by the canonical projection to the direct summand indexed by $\mathfrak{a}$. By a similar proof to [Liu 2019, Proposition 4.3], we have the following commutative diagram:

$$\begin{tikzcd}
X_{\mathfrak{r}}^{\flat,\mathrm{sp}}(\mathbb{F}_\ell^{\mathrm{ac}}) \arrow[r, "\theta"] \arrow[d, "\psi^\flat"'] & X_{\mathfrak{r}}^{\mathrm{sp}}(\mathbb{F}_\ell^{\mathrm{ac}}) \arrow[d, "\psi"] \\
\mathcal{S}_{\ell,\mathfrak{r}}^{\flat} \arrow[r, "\vartheta"] & \mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}
\end{tikzcd}$$

where $\psi^\flat$ is obtained similarly as ψ, but for $X_{\mathfrak{r}}^{\flat}$. Therefore, the theorem will follow if we can show that for every $f \in \Gamma(X_{\mathfrak{r}}^{\mathrm{sp}}(\mathbb{F}_\ell^{\mathrm{ac}}), \Lambda)[\ker\phi^{\mathfrak{rl}}]$, we have

$$(\Psi_{\mathfrak{a}}\overline{\Theta}, f) = \frac{1}{(\ell-1)^2} \sum_{x \in X_{\mathfrak{r}}^{\flat,\mathrm{sp}}(\mathbb{F}_\ell^{\mathrm{ac}})} f(\theta(x)) \tag{5-5}$$

since ψ is of degree $|\mathrm{Cl}(F)_{\mathfrak{r}}|$ by Lemma 5.14 and similarly $\psi^\flat$ is of degree $|(\mathbb{Z}/\mathfrak{r}\cap\mathbb{Z})^\times|$.

For every $\mathfrak{a} \in \mathfrak{B}$, we have the following commutative diagram as (4-6):

$$\begin{tikzcd}
 & W_{\varnothing,\varnothing}(\mathfrak{a}) \arrow[r, hook] \arrow[d] & Z_{\varnothing,\varnothing}(\mathfrak{a}) \arrow[r, hook, "i_{\mathfrak{a}}"] \arrow[d, "\pi_{\mathfrak{a}}"] & \mathbf{Sh}(G)_{\mathbb{F}_{\ell^6}} \cong X_{\mathfrak{r}} \otimes \mathbb{F}_{\ell^6} \\
X_{\mathfrak{r}}^{\mathrm{sp}} \otimes \mathbb{F}_{\ell^6} \arrow[r, "\cong"] & \mathbf{Sh}(G_{\mathtt{S}_{\max}})_{\mathbb{F}_{\ell^6}} \arrow[r, hook, "j_{\mathfrak{a}}"] & \mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing_{\mathfrak{a}}})_{\mathbb{F}_{\ell^6}} &
\end{tikzcd}$$

where the square is Cartesian. Here, we omit the away-from-ℓ level structure $K_{0,1}(\mathfrak{c}',\mathfrak{r})^\ell$ in the notation. However, in this case, $Z_{\varnothing,\varnothing}(\mathfrak{a})$ coincides with the Goren–Oort divisor $\mathbf{Sh}(G)_{\mathbb{F}_{\ell^6},\tau(\mathfrak{a})}$ for some $\tau(\mathfrak{a}) \in \Sigma_\infty$ determined by $\mathfrak{a}$. Thus it is easy to see that the (scheme-theoretical) intersection $\Gamma_\theta \cap \mathrm{pr}_2^* Z_{\varnothing,\varnothing}(\mathfrak{a})$ is contained in $X_{\mathfrak{r}}^{\flat,\mathrm{sp}} \times X_{\mathfrak{r}}^{\mathrm{sp}}$, where $\Gamma_\theta \subseteq X_{\mathfrak{r}}^{\flat} \times X_{\mathfrak{r}}$ is the graph of θ and $\mathrm{pr}_2 \colon X_{\mathfrak{r}}^{\flat} \times X_{\mathfrak{r}} \to X_{\mathfrak{r}}$ is the canonical projection. More precisely, it is the graph of the restricted morphism $\theta \colon X_{\mathfrak{r}}^{\flat,\mathrm{sp}} \to X_{\mathfrak{r}}^{\mathrm{sp}}$. Therefore, we have

$$\pi_{\mathfrak{a}*} i_{\mathfrak{a}}^* \theta_* [X_{\mathfrak{r}}^{\flat}] = \theta_{\mathfrak{a}*}[X_{\mathfrak{r}}^{\flat,\mathrm{sp}} \otimes \mathbb{F}_{\ell^6}] \tag{5-6}$$

in $\mathrm{CH}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing_{\mathfrak{a}}})_{\mathbb{F}_{\ell^6}})$, where $\theta_{\mathfrak{a}}$ is the composite morphism

$$X_{\mathfrak{r}}^{\flat,\mathrm{sp}} \otimes \mathbb{F}_{\ell^6} \xrightarrow{\theta} X_{\mathfrak{r}}^{\mathrm{sp}} \otimes \mathbb{F}_{\ell^6} \cong \mathbf{Sh}(G_{\mathtt{S}_{\max}})_{\mathbb{F}_{\ell^6}} \xrightarrow{j_{\mathfrak{a}}} \mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing_{\mathfrak{a}}})_{\mathbb{F}_{\ell^6}}.$$

Recall that we have two morphisms

$$\begin{aligned}
\mathrm{Gys}_{\mathfrak{a}} = i_{\mathfrak{a}!} \circ \pi_{\mathfrak{a}}^* &\colon \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing_{\mathfrak{a}}})_{\mathbb{F}_\ell^{\mathrm{ac}}}, \Lambda(1))/\ker\phi^{\mathfrak{rl}} \to \mathrm{H}^3(X_{\mathfrak{r}} \otimes \mathbb{F}_\ell^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{rl}}, \\
\mathrm{Res}_{\mathfrak{a}} = \pi_{\mathfrak{a}!} \circ i_{\mathfrak{a}}^* &\colon \mathrm{H}^3(X_{\mathfrak{r}} \otimes \mathbb{F}_\ell^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{rl}} \to \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}},\varnothing_{\mathfrak{a}}})_{\mathbb{F}_\ell^{\mathrm{ac}}}, \Lambda(1))/\ker\phi^{\mathfrak{rl}}.
\end{aligned}$$

We write $\mathfrak{B} = \{\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3\}$ with $\mathfrak{a}_{i-1} = \sigma(\mathfrak{a}_i)$ for all i viewed as elements in $\mathbb{Z}/3\mathbb{Z}$, where $\sigma(\mathfrak{a}_i)$ means the translate of $\mathfrak{a}_i$ by the Frobenius as defined just above Definition 3.15. By [Tian and Xiao 2019, Theorem 4.3] and the proof of [loc. cit., Theorem 4.4], the intersection matrix $(\mathrm{Res}_{\mathfrak{a}_i} \circ \mathrm{Gys}_{\mathfrak{a}_j})_{1 \le i,j \le 3}$ is given by

$$\begin{pmatrix} -2\ell & \ell\eta_1^{-1} & \ell\eta_3 \\ \ell\eta_1 & -2\ell & \ell\eta_2^{-1} \\ \ell\eta_3^{-1} & \ell\eta_2 & -2\ell \end{pmatrix},$$

where

$$\eta_i \colon \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}_i},\varnothing_{\mathfrak{a}_i}})_{\mathbb{F}_\ell^{\mathrm{ac}}}, \Lambda(1))/\ker\phi^{\mathfrak{rl}} \to \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}_{i+1}},\varnothing_{\mathfrak{a}_{i+1}}})_{\mathbb{F}_\ell^{\mathrm{ac}}}, \Lambda(1))/\ker\phi^{\mathfrak{rl}}$$

is a certain normalized link morphism introduced in [loc. cit., Section 2.25] which commutes with the Galois action and such that the product $\eta_{i+2}\eta_{i+1}\eta_i$ for $i \in \mathbb{Z}/3\mathbb{Z}$ is the endomorphism on $\mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}_i},\varnothing_{\mathfrak{a}_i}})_{\mathbb{F}_\ell^{\mathrm{ac}}}, \Lambda(1))/\ker\phi^{\mathfrak{rl}}$ given as follows. Let $\sigma_\ell \in \mathrm{G}_{\mathbb{F}_\ell}$ denotes an arithmetic Frobenius element. By [Brylinski and Labesse 1984] and Definition 5.10(A4), one has a decomposition of $\Lambda[\mathrm{G}_{\mathbb{F}_{\ell^3}}]$-modules

$$\mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}_i},\varnothing_{\mathfrak{a}_i}})_{\mathbb{F}_\ell^{\mathrm{ac}}}, \Lambda(1))/\ker\phi^{\mathfrak{rl}} = \mathrm{M}_i^1 \oplus \mathrm{M}_i^{\ell^3},$$

where each M_i^λ for $\lambda = 1, \ell^3$ is a finite free Λ-module on which the action of $\sigma_\ell^3 - \lambda$ is nilpotent. Then the action of $\eta_{i+2}\eta_{i+1}\eta_i$ on M_i^1 (respectively on $\mathrm{M}_i^{\ell^3}$) is the multiplication by ℓ^{-3} (respectively ℓ^3). Since the roles of $\mathfrak{a}_i$ are symmetric, $\mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}_i},\varnothing_{\mathfrak{a}_i}})_{\mathbb{F}_\ell^{\mathrm{ac}}}, \Lambda(1))/\ker\phi^{\mathfrak{rl}}$ for $i = 1, 2, 3$ must be isomorphic. Thus, we can identify M_i^λ with $\lambda = 1, \ell^3$ for different i and write it commonly as M^λ in such a way that the morphisms η_i are identified with the same endomorphism η on $\mathrm{M}^1 \oplus \mathrm{M}^{\ell^3}$, where η acts by ℓ^{-1} on M^1 and by ℓ on M^{ℓ^3}, respectively. With these identification, the intersection matrix writes as

$$(\mathrm{Res}_{\mathfrak{a}_i} \circ \mathrm{Gys}_{\mathfrak{a}_j})_{1 \le i,j \le 3} = \ell \begin{pmatrix} -2 & \eta^{-1} & \eta \\ \eta & -2 & \eta^{-1} \\ \eta^{-1} & \eta & -2 \end{pmatrix}. \tag{5-7}$$

Note also the isomorphism $\mathrm{H}^1(\mathbb{F}_{\ell^6}, \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}_i},\varnothing_{\mathfrak{a}_i}})_{\mathbb{F}_\ell^{\mathrm{ac}}}, \Lambda(1))/\ker\phi^{\mathfrak{rl}}) \cong \mathrm{H}^1(\mathbb{F}_{\ell^6}, \mathrm{M}^1)$ on which η acts by the scalar ℓ^{-1}.

By the proof of Theorem 4.7 in Section 4B, we have a commutative diagram

$$\begin{tikzcd}
\mathrm{H}^1(\mathbb{F}_{\ell^6}, \mathrm{H}^3(X_{\mathfrak{t}} \otimes \mathbb{F}_\ell^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{rl}}) \arrow[d, "\Psi_{\mathfrak{a}_i}"'] & \mathrm{H}^1(\mathbb{F}_{\ell^6}, \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}_i},\varnothing_{\mathfrak{a}_i}})_{\mathbb{F}_\ell^{\mathrm{ac}}}, \Lambda(1))/\ker\phi^{\mathfrak{rl}})) \arrow[l, "\mathrm{Gys}_{\mathfrak{a}_i}"'] \\
\Gamma(X_{\mathfrak{t}}^{\mathrm{sp}}(\mathbb{F}_\ell^{\mathrm{ac}}), \Lambda)/\ker\phi^{\mathfrak{rl}} & \Gamma(\mathbf{Sh}(G_{\mathtt{S}_{\max}})(\mathbb{F}_\ell^{\mathrm{ac}}), \Lambda)/\ker\phi^{\mathfrak{rl}} \arrow[l, "\cong"'] \arrow[u, "\Phi_{\mathfrak{a}_i}"']
\end{tikzcd}$$

where the bottom isomorphism is the one induced by the identification $X_{\mathfrak{t}}^{\mathrm{sp}} \otimes \mathbb{F}_{\ell^6} \cong \mathbf{Sh}(G_{\mathtt{S}_{\max}})_{\mathbb{F}_{\ell^6}}$, and $\Phi_{\mathfrak{a}_i}$ is the map induced from (4-7). We claim that $\Phi_{\mathfrak{a}_i}$ is an isomorphism. Indeed, by Proposition 4.8 and

Nakayama's lemma, $\Phi_{\mathfrak{a}_i}$ is surjective. On the other hand, we have a commutative diagram

$$\begin{tikzcd}
\bigoplus_{i=1}^{3} \Gamma(\mathbf{Sh}(G_{\mathrm{S}_{\max}})(\mathbb{F}_\ell^{\mathrm{ac}}), \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \arrow[r, "\oplus_i \Phi_{\mathfrak{a}_i}"] \arrow[dr, "(5\text{-}2)"'] & \bigoplus_{i=1}^{3} \mathrm{H}^1(\mathbb{F}_{\ell^6}, \mathrm{H}^1(\mathbf{Sh}(G_{\varnothing_{\mathfrak{a}_i},\varnothing_{\mathfrak{a}_i}})_{\mathbb{F}_\ell^{\mathrm{ac}}}, \Lambda(1))/\ker\phi^{\mathfrak{r}\mathfrak{l}})) \arrow[d, "\sum_i \mathrm{Gys}_{\mathfrak{a}_i}"] \\
 & \mathrm{H}^1(\mathbb{F}_{\ell^6}, \mathrm{H}^3(X_{\mathfrak{r}} \otimes \mathbb{F}_\ell^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}})
\end{tikzcd}$$

where the composite map is an isomorphism by Proposition 5.13. It follows that each $\Phi_{\mathfrak{a}_i}$ is injective, hence an isomorphism.

Now, we have $\overline{\Theta} = \sum_{i=1}^{3} \mathrm{Gys}_{\mathfrak{a}_i} \circ \Phi_{\mathfrak{a}_i} \circ \Psi_{\mathfrak{a}_i}(\overline{\Theta})$ and

$$\Phi_{\mathfrak{a}_1}^{-1} \circ \mathrm{Res}_{\mathfrak{a}_1} \overline{\Theta} = \ell(-2\Psi_{\mathfrak{a}_1}(\overline{\Theta}) + \ell\Psi_{\mathfrak{a}_2}(\overline{\Theta}) + \ell^{-1}\Psi_{\mathfrak{a}_3}(\overline{\Theta})) = (\ell-1)^2\Psi_{\mathfrak{a}_1}(\overline{\Theta})$$

by (5-7). Here, the last equality uses $\Psi_{\mathfrak{a}_1}(\overline{\Theta}) = \Psi_{\mathfrak{a}_2}(\overline{\Theta}) = \Psi_{\mathfrak{a}_3}(\overline{\Theta})$ by symmetry. On the other hand, by (5-6), we have

$$\Phi_{\mathfrak{a}}^{-1} \circ \mathrm{Res}_{\mathfrak{a}} \overline{\Theta} = \theta_* \underline{1}^{\flat}$$

for all $\mathfrak{a} \in \mathfrak{B}$, where $\underline{1}^{\flat}$ is the characteristic function on $X_{\mathfrak{r}}^{\flat,\mathrm{sp}}(\mathbb{F}_\ell^{\mathrm{ac}})$. Thus (5-5) follows immediately, and the theorem is proved. □

The following lemma will be needed in the next section.

Lemma 5.18. *When $\mathfrak{s} = \mathfrak{r}\mathfrak{l}$, the map*

$$\bigoplus_{\mathfrak{d}\in\mathfrak{D}(\mathfrak{r},\mathfrak{c}^+)} \delta_*^{\mathfrak{d}} \colon \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{s}} \to \bigoplus_{\mathfrak{d}\in\mathfrak{D}(\mathfrak{r},\mathfrak{c}^+)} \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{c}^+}, \Lambda)/\ker\phi^{\mathfrak{s}}$$

is an isomorphism of free Λ-modules of rank $|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$.

Proof. The idea of proof is similar to [Liu 2019, Lemma 3.33]. Recall that we have morphisms $\tilde{\delta}^{\mathfrak{d}}$ in (5-1) for each $\mathfrak{d} \in \mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)$. As usual, we put $\tilde{\delta} := \tilde{\delta}^{\mathcal{O}_F}$. Form the following pullback square

$$\begin{tikzcd}
\mathcal{X}_{\mathfrak{r}}^{\mathfrak{d}} \arrow[r, "\varepsilon"] \arrow[d, "\varepsilon^{\mathfrak{d}}"'] & \mathcal{X}_{\mathfrak{r}} \arrow[d, "\tilde{\delta}^{\mathfrak{d}}"] \\
\mathcal{X}_{\mathfrak{r}} \arrow[r, "\tilde{\delta}"] & \mathcal{X}(\Delta)_{\mathfrak{c}'\mathfrak{c}^+,\mathcal{O}_F}
\end{tikzcd}$$

of schemes over $\mathbb{Z}_{(\ell)}$, where all morphisms are finite étale. The scheme $\mathcal{X}_{\mathfrak{r}}^{\mathfrak{d}}$ has a natural action by $\mathbb{T}^{\mathrm{R}(\mathfrak{r}\mathfrak{l})}$ under which the above diagram is equivariant. By an argument similar to [loc. cit., Lemma 3.33], we obtain a commutative diagram

$$\begin{tikzcd}
\Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \arrow[r, "\Phi"] \arrow[d, "|(\mathcal{O}_F/\mathfrak{r})^\times|\cdot\delta^*\circ\delta_*^{\mathfrak{d}}"'] & \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \mathrm{H}^3(\mathcal{X}_{\mathfrak{r}} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}) \arrow[d, "\varepsilon_*^{\mathfrak{d}}\circ\varepsilon^*"] \\
\Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \arrow[r, "\Phi"] & \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \mathrm{H}^3(\mathcal{X}_{\mathfrak{r}} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}})
\end{tikzcd} \tag{5-8}$$

where Φ is the isomorphism in Proposition 5.16. By proper base change, the endomorphism $\varepsilon^{\mathfrak{d}}_* \circ \varepsilon^*$ of $\mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))$ coincides with the composite map

$$\mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2)) \xrightarrow{\tilde{\delta}^{\mathfrak{d}}_*} \mathrm{H}^3(\mathcal{X}(\Delta)_{\mathfrak{c}'\mathfrak{c}^+, \mathcal{O}_F} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2)) \xrightarrow{\tilde{\delta}^*} \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2)).$$

Definition 5.10(A2) and Proposition 5.16(1) imply that the image of

$$\varepsilon^{\mathfrak{d}}_* \circ \varepsilon^* \colon \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}}) \to \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \mathrm{H}^3(\mathcal{X}_\mathfrak{r} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}})$$

is a free Λ-module of rank 1. Here, we use the fact that $\tilde{\delta}^*$ is injective, as $p \nmid \mu(\mathfrak{r}, \mathfrak{c}^+)$ in Definition 5.4(3b).

By the commutative diagram (5-8), we know that the image of

$$\delta^* \circ \delta^{\mathfrak{d}}_* \colon \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \to \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}}$$

is a free Λ-module of rank 1. Since $\delta^{\mathfrak{d}}_*$ is surjective and δ^* is injective, $\Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{c}^+}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}}$ is a free Λ-module of rank 1. Similarly, we may deduce that the map

$$\bigoplus_{\mathfrak{d}\in\mathfrak{D}(\mathfrak{r},\mathfrak{c}^+)} \delta^{\mathfrak{d}}_* \colon \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \to \bigoplus_{\mathfrak{d}\in\mathfrak{D}(\mathfrak{r},\mathfrak{c}^+)} \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{c}^+}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}} \tag{5-9}$$

is injective. However, since the source of (5-9) a free Λ-module of rank $|\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^+)|$ by Proposition 5.16, the map (5-9) has to be an isomorphism. The lemma follows. □

Remark 5.19. Note that since the images of $\ker\phi^{\mathfrak{r}\mathfrak{l}}$ in both $\mathrm{End}_\Lambda(\Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda))$ and $\mathrm{End}_\Lambda(\Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{c}^+}, \Lambda))$ are finite sets, it follows by Chebotarev's density theorem that for all but finitely many primes $\mathfrak{l}'$ of F, the conclusion of Lemma 5.18 also holds for $\mathfrak{s} = \mathfrak{r}\mathfrak{l}\mathfrak{l}'$.

5D. ***First explicit reciprocity law.*** We keep the notation in Section 5C. Let $\underline{\ell} = (\ell, \ell')$ be a pair of distinct $(p^\nu, \mathfrak{r})$-admissible primes (Definition 5.10) such that Lemma 5.18 holds for $\mathfrak{s} = \mathfrak{r}\mathfrak{l}\mathfrak{l}'$, where $\mathfrak{l}' := \ell'\mathcal{O}_F$ (see Remark 5.19).

Put $\mathcal{X}_{\mathfrak{r},\underline{\ell}} := \mathcal{X}(\Delta \cup \{\mathfrak{l}, \mathfrak{l}'\})_{\mathfrak{c}',\mathfrak{r}}$ and $\mathcal{X}^\flat_{\mathfrak{r},\underline{\ell}} := \mathcal{X}(\Delta^\flat \cup \{\ell, \ell'\})_{\mathbb{Z},\mathfrak{r}\cap\mathbb{Z}}$ (in the notation of [Liu 2019, Definition B.1]), as schemes over $\mathbb{Z}_{(\ell')}$. Then we obtain a canonical morphism

$$\theta_{\underline{\ell}} \colon \mathcal{X}^\flat_{\mathfrak{r},\underline{\ell}} \to \mathcal{X}_{\mathfrak{r},\underline{\ell}}. \tag{5-10}$$

Denote by $\Theta^\nu_{p,\mathfrak{r},\underline{\ell}}$ the image of $\theta_{\underline{\ell}*}[\mathcal{X}^\flat_{\mathfrak{r},\underline{\ell}} \otimes \mathbb{Q}] \in \mathrm{CH}^2(\mathcal{X}_{\mathfrak{r},\underline{\ell}} \otimes \mathbb{Q})$ under the Abel–Jacobi map

$$\mathrm{AJ}_p \colon \mathrm{CH}^2(\mathcal{X}_{\mathfrak{r},\underline{\ell}} \otimes \mathbb{Q}) \to \mathrm{H}^1(\mathbb{Q}, \mathrm{H}^3(\mathcal{X}_{\mathfrak{r},\underline{\ell}} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}\mathfrak{l}'}).$$

Theorem 5.20 (first explicit reciprocity law). *Let* $\underline{\ell} = (\ell, \ell')$ *be as above*:

(1) *There is a canonical decomposition of the* $\Lambda[\mathrm{G}_\mathbb{Q}]$*-module*

$$\mathrm{H}^3(\mathcal{X}_{\mathfrak{r},\underline{\ell}} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}\mathfrak{l}'} = \bigoplus_{\mathfrak{d}\in\mathfrak{D}(\mathfrak{r},\mathfrak{c}^+)} \mathrm{M}_\mathfrak{d}$$

where $\mathrm{M}_\mathfrak{d}$ *is isomorphic to* $\mathrm{N}^\sharp_\rho(-1)$ *(Notation 5.11) as a* $\Lambda[\mathrm{G}_\mathbb{Q}]$*-module.*

(2) *There is a canonical isomorphism*

$$\mathrm{H}^1_{\mathrm{sing}}(\mathbb{Q}_{\ell'}, \mathrm{H}^3(\mathcal{X}_{\mathfrak{r},\underline{\ell}} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}\mathfrak{l}'}) \cong \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)/\ker\phi^{\mathfrak{r}\mathfrak{l}},$$

under which we have

$$(\partial\,\mathrm{loc}_{\ell'}\,\Theta^{\nu}_{p,\mathfrak{r},\underline{\ell}}, f) = (\ell'+1)\cdot\frac{|(\mathbb{Z}/\mathfrak{r}\cap\mathbb{Z})^{\times}|}{|\mathrm{Cl}(F)_{\mathfrak{r}}|}\cdot\sum_{x\in\mathcal{S}^{\flat}_{\ell,\mathfrak{r}}} f(\vartheta(x))$$

for every $f \in \Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{r}}, \Lambda)[\ker\phi^{\mathfrak{r}\mathfrak{l}}]$.

Proof. We will use results from [Liu 2019, Sections 3 and 4]. Put $\nabla^{\flat} := \Delta^{\flat}\cup\{\infty, \ell\}$ as in the setup of [loc. cit., Section 4.1]. By Lemma 5.18, $(\rho, \mathfrak{c}'\mathfrak{c}^{+}, \mathfrak{c}', \mathfrak{r})$ is a perfect quadruple in the sense of [loc. cit., Definition 3.2], satisfying [loc. cit., Assumption 4.1]. Moreover, ℓ' is a cubic-level raising prime for $(\rho, \mathfrak{c}'\mathfrak{c}^{+}, \mathfrak{c}', \mathfrak{r})$ in the sense of [loc. cit., Definition 3.3].

Note that the morphism (5-10) is nothing but $\theta\colon \mathcal{X}(\ell')^{\flat}_{\mathfrak{r}} \to \mathcal{X}(\ell')_{\mathfrak{c}',\mathfrak{r}}$ in [loc. cit., (4.1.1)]; and the map (5-4) is nothing but $\vartheta\colon \mathcal{S}^{\flat}_{\mathfrak{r}} \to \mathcal{S}_{\mathfrak{c}'\mathfrak{r}}$ in [loc. cit., (4.1.2)]. Therefore, (1) follows from [loc. cit., Theorem 3.5(2)]; and (2) follows from [loc. cit., Theorems 3.5(3) and 4.5]. □

5E. *Proof of main theorem.* Recall that we have the multiplicatively induced representation $\mathrm{N}^{\sharp}_{\rho}$ and the $\mathbb{Z}/p^{\nu}[\mathrm{G}_{\mathbb{Q}}]$-module M_0 as in Theorem 5.20. We have a $\mathrm{G}_{\mathbb{Q}}$-equivariant pairing

$$\mathrm{N}^{\sharp}_{\rho}(-1)\times\mathrm{M}_0 \to \mathbb{Z}/p^{\nu}(1)$$

which induces, for every prime power v, a local Tate pairing

$$\langle\cdot,\cdot\rangle_v\colon \mathrm{H}^1(\mathbb{Q}_v, \mathrm{N}^{\sharp}_{\rho}(-1))\times\mathrm{H}^1(\mathbb{Q}_v, \mathrm{M}_0) \to \mathrm{H}^2(\mathbb{Q}_v, \mathbb{Z}/p^{\nu}(1)) \simeq \mathbb{Z}/p^{\nu}.$$

For $s\in\mathrm{H}^1(\mathbb{Q}, \mathrm{N}^{\sharp}_{\rho}(-1))$ and $r\in\mathrm{H}^1(\mathbb{Q}, \mathrm{M}_0)$, we will write $\langle s, r\rangle_v$ rather than $\langle\mathrm{loc}_v(s), \mathrm{loc}_v(r)\rangle_v$.

Proof of Theorem 5.7. We assume that $\Theta_{p,\mathfrak{r}}$ is nonzero. Regard $\Theta_{p,\mathfrak{r}}$ as an element in $\mathrm{H}^1_f(\mathbb{Q}, \mathrm{H}^3(\mathcal{X}_{\mathfrak{r}}\otimes\mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p(2))/\ker\phi^{\mathfrak{r}})$, which is not torsion. By [Brylinski and Labesse 1984] and the assumption that $(p, \mathfrak{r})$ is $\mathfrak{r}$-clean (Definition 5.4), we know that $\mathrm{N}_p := \mathrm{H}^3(\mathcal{X}(\Delta)_{\mathfrak{c}'\mathfrak{c}^{+},O_F}\otimes\mathbb{Q}^{\mathrm{ac}}, \mathbb{Z}_p(2))/\ker\phi^{\mathfrak{r}}$ is a $\mathrm{G}_{\mathbb{Q}}$-stable lattice in $\mathsf{M}(E)_p$; and there exists some $\mathfrak{d}\in\mathfrak{D}(\mathfrak{r}, \mathfrak{c}^{+})$ such that $\delta^{\mathfrak{d}}_{*}\Theta_{p,\mathfrak{r}}\in\mathrm{H}^1_f(\mathbb{Q}, \mathrm{N}_p)$ is not torsion. Here, $\mathrm{H}^1_f(\mathbb{Q}, \mathrm{N}_p)$ is by definition of the preimage of $\mathrm{H}^1_f(\mathbb{Q}, \mathsf{M}(E)_p)$ under the natural map $\mathrm{H}^1(\mathbb{Q}, \mathrm{N}_p)\to\mathrm{H}^1(\mathbb{Q}, \mathsf{M}(E)_p)$. We fix such an element $\mathfrak{d}$. Let $\nu_0\geq 0$ be the largest integer such that $\delta^{\mathfrak{d}}_{*}\Theta_{p,\mathfrak{r}}\in p^{\nu_0}\mathrm{H}^1_f(\mathbb{Q}, \mathrm{N}_p)$.

We prove by contradiction, hence assume $\dim_{\mathbb{Q}_p}\mathrm{H}^1_f(\mathbb{Q}, \mathsf{M}(E)_p)\geq 2$. In what follows, we fix a sufficiently large integer ν as before, and will give a lower bound on ν for which a contradiction emerges at the end of proof.

By [Liu 2016, Lemma 5.9], we may find a free $\mathbb{Z}/p^{\nu}$-submodule S of $\mathrm{H}^1_f(\mathbb{Q}, \mathrm{N}^{\sharp}_{\rho}(-1))$ of rank 2 with a basis $\{s, s'\}$ such that $p^{\nu_0}s = \delta^{\mathfrak{d}}_{*}\Theta^{\nu}_{p,\mathfrak{r}}$. By the same discussion in [Liu 2019, Section 4.3 (after Lemma 4.12)], we have tower of fields $\mathbb{L}_{\mathrm{S}}/\mathbb{L}/\mathbb{Q}$ contained in $\mathbb{Q}^{\mathrm{ac}}$. Let $\Box$ be the (finite) set of rational primes that are either ramified in $\mathbb{L}_{\mathrm{S}}$ or not coprime to Δ or $\mathfrak{r}\,\mathrm{disc}\,F$. Put $\nu_{\Box} := \max\{\nu_v \mid v\in\Box\}$ where ν_v is in [loc. cit., Lemma 4.12(2)]. We choose a prime $\ell_0 \notin \Box$ such that ℓ_0 is $(p^\nu, \mathfrak{r})$-admissible (Definition 5.10), which is possible by [loc. cit., Lemma 4.11]. Let $\gamma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ be the image of Frob_{w_0} under $\rho^\sharp(-1)$ (the image of $\rho^\sharp(-1)$ has been identified with $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$), where w_0 is some prime of $\mathbb{L}$ above ℓ_0. Then γ has order coprime to p; and $(\mathrm{N}_\rho^\sharp(-1))^{\langle\gamma\rangle}$ is a free $\mathbb{Z}/p^\nu$-module of rank 1.

By [loc. cit., Lemma 4.16] and (the argument for) [loc. cit., Lemma 4.11], we may choose two $(\Box, \gamma)$-admissible places (in the sense of [loc. cit., Definition 4.15]) w, w' of $\mathbb{L}$ such that

(1) $\Psi_w(s') = 0$, $\Psi_w(s) = t$, $\Psi_{w'}(s') = t'$ with $t, t' \in (\mathrm{N}_\rho^\sharp(-1))^{\langle\gamma\rangle}$ that are not divisible by p;

(2) the underlying prime ℓ of w and the underlying prime ℓ' of w' are distinct $(p^\nu, \mathfrak{r})$-admissible primes, such that Lemma 5.18 holds for $\mathfrak{s} = \mathfrak{r}\mathfrak{l}\mathfrak{l}'$ (see Remark 5.19).

Put $\underline{\ell} := (\ell, \ell')$. Then there are elements $\Theta^\nu_{p,\mathfrak{r},\underline{\ell}} \in \mathrm{H}^1(\mathbb{Q}, \mathrm{H}^3(\mathcal{X}_{\mathfrak{r},\underline{\ell}} \otimes \mathbb{Q}^{\mathrm{ac}}, \Lambda(2))/\ker\phi^{\mathfrak{r}\mathfrak{l}\mathfrak{l}'})$ from Section 5D, and $\delta^{\mathfrak{d}}_*\Theta^\nu_{p,\mathfrak{r},\underline{\ell}} \in \mathrm{H}^1(\mathbb{Q}, \mathrm{M}_0)$. We have

(3) $\mathrm{loc}_v\, \Theta^\nu_{p,\mathfrak{r},\underline{\ell}} \in \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_v, \mathrm{M}_0)$ for a prime $v \notin \Box \cup \{p, \ell, \ell'\}$, by [Liu 2016, Lemma 3.4];

(4) $\mathrm{loc}_p\, \Theta^\nu_{p,\mathfrak{r},\underline{\ell}} \in \mathrm{H}^1_f(\mathbb{Q}_p, \mathrm{M}_0)$, by [Nekovář 2000, Theorem 3.1(ii)].

By [Liu 2019, Lemma 4.6] and [Liu 2016, Lemma 3.4], we have $\mathrm{loc}_v(s') \in \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_v, \mathrm{N}_\rho^\sharp(-1))$ for every prime $v \notin \Box \cup \{p, \ell, \ell'\}$. By [Liu 2016, Definition 4.6, Remark 4.7], we have $\mathrm{loc}_p(s') \in \mathrm{H}^1_f(\mathbb{Q}_v, \mathrm{N}_\rho^\sharp(-1))$. Then by [Liu 2019, Lemma 4.12(2,3,5)] and (3), (4) above, we have

$$p^{\nu-\nu_\Box} \mid \sum_{v \notin \{\ell,\ell'\}} \langle s', \Theta^\nu_{p,\mathfrak{r},\underline{\ell}}\rangle_v. \tag{5-11}$$

Since $\Psi_w(s') = 0$ by (1), we also have

$$\langle s', \Theta^\nu_{p,\mathfrak{r},\underline{\ell}}\rangle_\ell = 0. \tag{5-12}$$

Let ϕ_0 be a generator of $\Gamma(\mathcal{S}_{\ell,\mathfrak{c}'\mathfrak{c}^+}, \mathbb{Z}/p^\nu)[\ker\phi^{\mathfrak{r}\mathfrak{l}\mathfrak{l}'}]$ which is a free $\mathbb{Z}/p^\nu$-module of rank 1. Then by the choice of s, w in (1), and Theorem 5.17, we have

$$\sum_{\mathcal{S}^\flat_{\ell,\mathfrak{r}}} \phi_0(\delta^{\mathfrak{d}}(\vartheta(x))) \in p^{\nu_0}\mathbb{Z}/p^\nu - p^{\nu_0+1}\mathbb{Z}/p^\nu.$$

By the choice of w' in (1) and Theorem 5.20, we have

$$\langle s', \Theta^\nu_{p,\mathfrak{r},\underline{\ell}}\rangle_{\ell'} \in p^{\nu_0}\mathbb{Z}/p^\nu - p^{\nu_0+1}\mathbb{Z}/p^\nu. \tag{5-13}$$

Here, we have used the fact that p is coprime to $|(\mathbb{Z}/\mathfrak{r}\cap\mathbb{Z})^\times|$, $|\mathrm{Cl}(F)_\mathfrak{r}|$, $(\ell-1)$, and $\ell'+1$.

Take $\nu \in \mathbb{Z}$ such that $\nu > \nu_0 + \nu_\Box$. Then the combination of (5-11), (5-12) and (5-13) contradicts with the following well-known fact:

$$\sum_v \langle s', \Theta^\nu_{p,\mathfrak{r},\underline{\ell}}\rangle_v = 0$$

due to the global class field theory and the fact that p is odd, where the sum is taken over all primes v. Theorem 5.7 is proved. □

Acknowledgements

The authors would like to thank Liang Xiao for his collaboration in some previous work with Tian, which plays an important role in the current one. They thank Mladen Dimitrov for helpful discussion concerning his work of cohomology of Hilbert modular varieties. They also thank the anonymous referee for careful reading and numerous suggestions for improving the article. Liu would like to thank the hospitality of Universität Bonn during his visit to Tian where part of the work was done. Liu is partially supported by NSF grant DMS–1702019 and a Sloan Research Fellowship.

References

[Bachmat and Goren 1999] E. Bachmat and E. Z. Goren, "On the non-ordinary locus in Hilbert–Blumenthal surfaces", *Math. Ann.* **313**:3 (1999), 475–506. MR Zbl

[Bloch and Kato 1990] S. Bloch and K. Kato, "L-functions and Tamagawa numbers of motives", pp. 333–400 in *The Grothendieck Festschrift, I*, edited by P. Cartier et al., Progr. Math. **86**, Birkhäuser, Boston, 1990. MR Zbl

[Boston et al. 1991] N. Boston, H. W. Lenstra, Jr., and K. A. Ribet, "Quotients of group rings arising from two-dimensional representations", *C. R. Acad. Sci. Paris Sér. I Math.* **312**:4 (1991), 323–328. MR Zbl

[Brylinski and Labesse 1984] J.-L. Brylinski and J.-P. Labesse, "Cohomologie d'intersection et fonctions L de certaines variétés de Shimura", *Ann. Sci. École Norm. Sup.* (4) **17**:3 (1984), 361–412. MR Zbl

[Carayol 1986] H. Carayol, "Sur la mauvaise réduction des courbes de Shimura", *Compos. Math.* **59**:2 (1986), 151–230. MR Zbl

[Deligne 1979] P. Deligne, "Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques", pp. 247–289 in *Automorphic forms, representations and L-functions, II* (Corvallis, OR, 1977), edited by A. Borel and W. Casselman, Proc. Sympos. Pure Math. **33**, Amer. Math. Soc., Providence, RI, 1979. MR Zbl

[Dimitrov 2005] M. Dimitrov, "Galois representations modulo p and cohomology of Hilbert modular varieties", *Ann. Sci. École Norm. Sup.* (4) **38**:4 (2005), 505–551. MR Zbl

[Garrett 1987] P. B. Garrett, "Decomposition of Eisenstein series: Rankin triple products", *Ann. of Math.* (2) **125**:2 (1987), 209–235. MR Zbl

[Kolyvagin 1990] V. A. Kolyvagin, "Euler systems", pp. 435–483 in *The Grothendieck Festschrift, II*, edited by P. Cartier et al., Progr. Math. **87**, Birkhäuser, Boston, 1990. MR Zbl

[Lan 2013] K.-W. Lan, *Arithmetic compactifications of PEL-type Shimura varieties*, Lond. Math. Soc. Monogr. Series **36**, Princeton Univ. Press, 2013. MR Zbl

[Lan and Stroh 2018] K.-W. Lan and B. Stroh, "Nearby cycles of automorphic étale sheaves", *Compos. Math.* **154**:1 (2018), 80–119. MR Zbl

[Liu 2016] Y. Liu, "Hirzebruch–Zagier cycles and twisted triple product Selmer groups", *Invent. Math.* **205**:3 (2016), 693–780. MR Zbl

[Liu 2019] Y. Liu, "Bounding cubic-triple product Selmer groups of elliptic curves", *J. Eur. Math. Soc.* **21**:5 (2019), 1411–1508. MR Zbl

[Manning and Shotton 2019] J. Manning and J. Shotton, "Ihara's lemma for Shimura curves over totally real fields via patching", preprint, 2019. arXiv

[Nekovář 2000] J. Nekovář, "p-adic Abel–Jacobi maps and p-adic heights", pp. 367–379 in *The arithmetic and geometry of algebraic cycles* (Banff, AB, 1998), edited by B. B. Gordon et al., CRM Proc. Lecture Notes **24**, Amer. Math. Soc., Providence, RI, 2000. MR Zbl

[Piatetski-Shapiro and Rallis 1987] I. Piatetski-Shapiro and S. Rallis, "Rankin triple L functions", *Compos. Math.* **64**:1 (1987), 31–115. MR Zbl

[Ribet 1990] K. A. Ribet, “On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms”, *Invent. Math.* **100**:2 (1990), 431–476. MR Zbl

[Serre 1996] J.-P. Serre, “Two letters on quaternions and modular forms (mod p)”, *Israel J. Math.* **95** (1996), 281–299. MR Zbl

[SGA 1 2003] A. Grothendieck, *Revêtements étales et groupe fondamental* (Séminaire de Géométrie Algébrique du Bois Marie 1960–1961), Doc. Math. (Paris) **3**, Soc. Math. France, Paris, 2003. Updated and annotated reprint of the 1971 original. MR Zbl

[Tian and Xiao 2016] Y. Tian and L. Xiao, “On Goren–Oort stratification for quaternionic Shimura varieties”, *Compos. Math.* **152**:10 (2016), 2134–2220. MR Zbl

[Tian and Xiao 2019] Y. Tian and L. Xiao, “Tate cycles on some quaternionic Shimura varieties mod p”, *Duke Math. J.* **168**:9 (2019), 1551–1639. MR Zbl

[Yu 2003] C.-F. Yu, “On the supersingular locus in Hilbert–Blumenthal 4-folds”, *J. Algebraic Geom.* **12**:4 (2003), 653–698. MR Zbl

[Zink 1982] T. Zink, “Über die schlechte Reduktion einiger Shimuramannigfaltigkeiten”, *Compos. Math.* **45**:1 (1982), 15–107. MR Zbl

Communicated by Christopher Skinner
Received 2018-10-22 Revised 2019-09-30 Accepted 2020-03-26

yifeng.liu@yale.edu *Department of Mathematics, Yale University, New Haven, CT, United States*

tian@math.unistra.fr *UFR de mathématique et de l'informatique, IRMA, University of Strasbourg, France*

ALGEBRA AND NUMBER THEORY 14:8 (2020)
https://doi.org/10.2140/ant.2020.14.2121

Burch ideals and Burch rings

Hailong Dao, Toshinori Kobayashi and Ryo Takahashi

Dedicated to Lindsay Burch

We introduce the notion of Burch ideals and Burch rings. They are easy to define, and can be viewed as generalization of many well-known concepts, for example integrally closed ideals of finite colength and Cohen–Macaulay rings of minimal multiplicity. We give several characterizations of these objects. We show that they satisfy many interesting and desirable properties: ideal-theoretic, homological, categorical. We relate them to other classes of ideals and rings in the literature.

1. Introduction

This article introduces and studies a class of ideals and their affiliated rings which we call Burch ideals and Burch rings. While their definitions are quite simple, our investigation shows that they enjoy remarkable ideal-theoretic and homological properties. These properties allow us to link them to many classes of ideals and rings in the literature, and consequently strengthen numerous old results as well as establish new ones.

Let us make a brief remark on our motivation and historical context. The project originated from our effort to understand a beautiful result by Burch on homological properties of ideals [1968b, Theorem 5(ii) and Corollary 1(ii)].

Theorem 1.1 (Burch). *Let $(R, \mathfrak{m})$ be a local ring. Let I be an ideal of R with $\mathfrak{m}I \neq \mathfrak{m}(I : \mathfrak{m})$.*

(1) *Let M be a finitely generated R-module. If $\operatorname{Tor}_n^R(R/I, M) = \operatorname{Tor}_{n+1}^R(R/I, M) = 0$ for some positive integer n, then M has projective dimension at most n.*

(2) *If I has finite projective dimension, then R is regular.*

MSC2010: primary 13C13; secondary 13D09, 13H10.

Keywords: Burch ideal, Burch ring, direct summand, fiber product, Gorenstein ring, hypersurface, singular locus, singularity category, syzygy, thick subcategory, (weakly) m-full ideal.

Lindsay Burch[1] was a PhD student of David Rees, and she wrote several (short) papers that have had a sizable impact on two active corners of commutative algebra: homological theory and integral closure of ideals. Perhaps most researchers in the field know of her work via the frequently used Hilbert–Burch theorem [Burch 1968b], her construction of ideals with only three-generators while possessing arbitrarily complicated homological behavior [Burch 1968a], and the Burch inequality on analytic spreads [Burch 1972]. The ideas of Burch's particular result above, while less well-known, have resurfaced in the work of several authors which also motivated our work; see [Corso et al. 2018; 2006; Kostrikin and Shafarevich 1957; Kustin and Vraciu 2018; Striuli and Vraciu 2011]. However, it has appeared to us that what was known previously is just the tip of an iceberg, and led us to formally make the following definitions.

Let $(R, \mathfrak{m})$ be a local ring. We define an ideal I of R to be a *Burch ideal* if $\mathfrak{m}I \neq \mathfrak{m}(I : \mathfrak{m})$. We also define *Burch rings of depth zero* to be those local rings whose completions are quotients of regular local rings by Burch ideals. Then we further define *Burch rings* of positive depth as local rings which "deform" to Burch rings of depth zero; see Section 2 for the precise definitions.

It is not hard to see that the class of Burch ideals contains other well-studied classes: integrally closed ideals of codepth zero (under mild conditions), $\mathfrak{m}$-full ideals, weakly $\mathfrak{m}$-full ideals, etc.

One of our main results characterizes Burch ideals and Burch rings of depth zero:

Theorem 1.2 (Theorem 4.1). *Let $(R, \mathfrak{m}, k)$ be a local ring and $I \neq \mathfrak{m}$ an ideal of R. Then I is Burch if and only if the second syzygy $\Omega^2_{R/I}k$ of k over R/I contains k as a direct summand.*

From this, we can quickly deduce a characterization of Gorenstein Burch ideals, which extends results on integrally closed or $\mathfrak{m}$-full ideals in [Goto 1987; Goto and Hayasaka 2002]. In fact, our proofs allow us to completely characterized modules over Burch rings of depth zero whose some higher syzygies contain the residue field as a direct summand, as follows:

Theorem 1.3 (Theorem 4.5). *Let $(R, \mathfrak{m}, k)$ be a Burch ring of depth zero. Let M be a finitely generated R-module. The following are equivalent*:

(1) *The ideal $\mathrm{I}(M)$ generated by all entries of the matrices ∂_i, $i > 0$ in a minimal free resolution (F, ∂) of M is equal to $\mathfrak{m}$.*

(2) *The R-module k is a direct summand of $\Omega^r_R M$ for some $r \geq 2$.*

Our work reveals some interesting connections between Burch ideals/rings and concepts studied by other authors in quite different contexts. For instance, we show that in codimension two, artinian almost Gorenstein rings as introduced by Huneke and Vraciu [2006] (also studied in [Striuli and Vraciu 2011])

[1] We are grateful to Rodney Sharp and Edmund Robertson for providing us with the following brief biography of Burch. Lindsay Burch was born in 1939. She did her first degree at Girton College, Cambridge from 1958 to 1961. She then went to Exeter University to study for a Ph.D. advised by David Rees. She was appointed to Queen's College, Dundee in 1964 before the award of her Ph.D., which she received in 1967 for her thesis "Homological algebra in local rings". At the time she was appointed to Queen's College it was a college of the University of St. Andrews but later, in 1967, it became a separate university, the University of Dundee. Burch continued to work in the Mathematics Department of the University of Dundee until at least 1978. She then took up computing and moved to a computing position at Keele University near Stafford in the north of England. She remained there until she retired and she still lives near Keele University.

are Burch; see Proposition 6.10. Over a regular local ring, the “Burchness” of an ideal I imposes a strong condition on the matrix at the end of a minimal free resolution of I, a condition that also appeared in the work of Corso, Goto, Huneke, Polini and Ulrich [Corso et al. 2018] on iterated socles. That connection led us to obtain a refinement of their result in Theorem 6.2.

We also study Burch rings of higher depth, especially their homological and categorical aspects. We completely classify Burch rings which are fiber products in Proposition 6.15. The Cohen–Macaulay rings of minimal multiplicity are Burch. Non-Gorenstein Burch rings turn out to be *G-regular* in Theorem 7.7, in the sense that all the totally reflexive modules are free. Moreover, we show an explicit result on vanishing behavior of Tor for any pair of modules.

Theorem 1.4 (Corollary 7.13). *Let R be a Burch ring of depth t. Let M, N be finitely generated R-modules. Assume that there exists an integer $l \geq \max\{3, t+1\}$ such that $\operatorname{Tor}_i^R(M, N) = 0$ for all $l+t \leq i \leq l+2t+1$. Then either M or N has finite projective dimension.*

To state our last main result in this introduction, recall that the *singularity category* $\mathrm{D}_{\mathrm{sg}}(R)$ is by definition the triangulated category given as the Verdier quotient of the bounded derived category of finitely generated R-modules by perfect complexes. Under some assumptions, one can classify all the thick subcategories of $\mathrm{D}_{\mathrm{sg}}(R)$ for a Burch ring R.

Theorem 1.5 (Theorem 7.10). *Let R be a singular Cohen–Macaulay Burch ring. Suppose that on the punctured spectrum R is either locally a hypersurface or locally has minimal multiplicity. Then there is a one-to-one correspondence between the thick subcategories of $\mathrm{D}_{\mathrm{sg}}(R)$ and the specialization-closed subsets of $\operatorname{Sing} R$.*

Next we describe the structure of the paper as well as other notable results. In Section 2 we state our convention, basic definitions and preliminary results. Section 3 is devoted to giving a sufficient condition for a module to have a second syzygy having a cyclic direct summand (Proposition 3.4). This is a generalization of [Kustin and Vraciu 2018, Lemma 4.1], and has an application to provide an exact pair of zero divisors (Corollary 3.6). These materials are used in Section 4 and are perhaps of independent interest.

In Section 5, we focus on the study of Burch rings of positive depth. We verify that the class of Gorenstein Burch rings coincides with that of hypersurfaces (Proposition 5.1). Cohen–Macaulay local rings of minimal multiplicity with infinite residue field are Burch (Proposition 5.2). Quotients of polynomial rings by perfect ideals with linear resolution are Burch (Proposition 5.6). We also consider the subtle question of whether the Burch property is preserved by cutting down by *any* regular sequence consisting of minimal generators of $\mathfrak{m}$. Remarkably, this holds for Cohen–Macaulay local rings of dimension one with minimal multiplicity (Proposition 5.5). However, the answer turns out to be negative in general (Example 5.8).

In Section 6 we focus more deeply on Burch ideals in a regular local ring. We give a complete characterization in dimension two and link Burch rings and Burch ideals to various other concepts. Moreover, we give a characterization of the Burch local rings $(R, \mathfrak{m}, k)$ with $\mathfrak{m}^3 = 0$ in terms of a Betti number of k, the embedding dimension and type of R (Theorem 6.12). We also characterize the Burch monomial ideals of regular local rings (Proposition 6.4).

In Section 7, we explore the homological and categorical aspects of Burch rings. We find out the significant property of Burch rings that every module of infinite projective dimension contains a high syzygy of the residue field in its resolving closure (Proposition 7.6). We apply this and make an analogous argument as in [Nasseh and Takahashi 2020] to classify various subcategories.

2. Convention, definitions and basic properties of Burch ideals and rings

Throughout this paper, we assume that all rings are commutative and noetherian, that all modules are finitely generated and that all subcategories are full and strict. For a local ring $(R, \mathfrak{m}, k)$, we denote by $\operatorname{edim} R$ the embedding dimension of R, by $r(R)$ the (Cohen–Macaulay) type of R, and by K^R the Koszul complex of R, i.e., the Koszul complex of a minimal system of generators of $\mathfrak{m}$. We set $\mathrm{K}^R = 0$ when R is a field. For an R-module M, we denote by $\ell_R(M)$ the length of M, by $\mu_R(M)$ the minimal number of generators of M, and by $\beta_i^R(M)$ the i-th Betti number of M. The i-th syzygy of M in the minimal free resolution of M is denoted by $\Omega^i_R M$. We omit subscripts and superscripts if there is no fear of confusion.

The remainder of this section deals with the formal notion of Burch ideals and Burch rings and their basic properties.

Definition 2.1. Let $(R, \mathfrak{m})$ be a local ring. We define a *Burch ideal* as an ideal I with $\mathfrak{m}I \neq \mathfrak{m}(I :_R \mathfrak{m})$. Note by definition that any Burch ideal I of R satisfies $\operatorname{depth} R/I = 0$.

Here are some quick examples of Burch ideals. Many more examples will follow from our results later.

Example 2.2. (1) Let (R, xR) be a discrete valuation ring. Then (x^n) is a Burch ideal of R for all $n \geq 1$, since $x(x^n) = (x^{n+1}) \neq (x^n) = x(x^{n-1}) = x((x^n) : (x))$.

(2) Let I be an ideal of a local ring $(R, \mathfrak{m})$. Put $J = \mathfrak{m}I$ and suppose $J \neq 0$. Then $\mathfrak{m}(J : \mathfrak{m}) = J \neq \mathfrak{m}J$, so J is a Burch ideal of R.

(3) By the previous item, if $(R, \mathfrak{m})$ has positive depth then $I = \mathfrak{m}^t$ is Burch for any $t \geq 1$. More generally, if $\mathfrak{m}^{t+1} \subseteq I \subseteq \mathfrak{m}^t$, then I is Burch if and only if $I : \mathfrak{m} \neq \mathfrak{m}^t$ and $I\mathfrak{m} \neq \mathfrak{m}^{t+1}$. Using this one can show that the set of Burch ideals is Zariski-open in $\mathrm{Grass}_k(r, \mathfrak{m}^t/\mathfrak{m}^{t+1})$, for each $r = \dim_k I/\mathfrak{m}^{t+1}$.

(4) Let $(R, \mathfrak{m})$ be a local ring of positive depth. Let I be an integrally closed ideal of R. Then $\mathfrak{m}I : \mathfrak{m} = I$ by the determinantal trick, so it is Burch. See Proposition 2.3 below.

The following proposition gives some basic characterizations of Burch ideals.

Proposition 2.3. *Let $(R, \mathfrak{m})$ be a local ring and I an ideal of R. The following are equivalent*:

(1) *I is a Burch ideal.*

(2) $(I : \mathfrak{m}) \neq (\mathfrak{m}I : \mathfrak{m})$.

(3) $\operatorname{Soc}(R/I) \cdot \mathfrak{m}/I\mathfrak{m} \neq 0$.

(4) $\operatorname{depth} R/I = 0$ *and* $r(R/\mathfrak{m}I) \neq r(R/I) + \mu(I)$.

(5) *$I\widehat{R}$ is a Burch ideal of $\widehat{R}$, where $\widehat{R}$ is the completion of R.*

Proof. (1) $\Leftrightarrow$ (2): If $(I : \mathfrak{m}) = (\mathfrak{m}I : \mathfrak{m})$, then $\mathfrak{m}(I : \mathfrak{m}) = \mathfrak{m}(\mathfrak{m}I : \mathfrak{m}) = \mathfrak{m}I$. Conversely, if $\mathfrak{m}I = \mathfrak{m}(I : \mathfrak{m})$, then $(\mathfrak{m}I : \mathfrak{m}) = (\mathfrak{m}(I : \mathfrak{m}) : \mathfrak{m}) = (I : \mathfrak{m})$.

(1) $\Leftrightarrow$ (3): As $\operatorname{Soc} R/I = (I : \mathfrak{m})/I$, we have $\operatorname{Soc} R/I \cdot \mathfrak{m}/I\mathfrak{m} = 0$ if and only if $\mathfrak{m}(I : \mathfrak{m}) = \mathfrak{m}I$.

(2) $\Leftrightarrow$ (4): There are inclusions $\mathfrak{m}I \subseteq I \subseteq (\mathfrak{m}I : \mathfrak{m}) \subseteq (I : \mathfrak{m})$, which especially says that $(\mathfrak{m}I : \mathfrak{m}) \neq (I : \mathfrak{m})$ implies $\operatorname{depth} R/I = 0$. We have $\ell((I : \mathfrak{m})/\mathfrak{m}I) = \ell((I : \mathfrak{m})/I) + \ell(I/\mathfrak{m}I) = r(R/I) + \mu(I)$ if $\operatorname{depth} R/I = 0$, and $\ell((\mathfrak{m}I : \mathfrak{m})/\mathfrak{m}I) = r(R/\mathfrak{m}I)$. Thus, under the assumption $\operatorname{depth} R/I = 0$, the equalities $(I : \mathfrak{m}) = (\mathfrak{m}I : \mathfrak{m})$ and $r(R/\mathfrak{m}I) = r(R/I) + \mu(I)$ are equivalent.

(1) $\Leftrightarrow$ (5): It is clear that $\mathfrak{m}I = \mathfrak{m}(I :_R \mathfrak{m})$ if and only if $\widehat{\mathfrak{m}}I = \widehat{\mathfrak{m}}(I :_{\widehat{R}} \widehat{\mathfrak{m}})$. □

Recall that an ideal I of a local ring $(R, \mathfrak{m})$ is $\mathfrak{m}$-*full* (resp. *weakly* $\mathfrak{m}$-*full*) if $(\mathfrak{m}I : x) = I$ for some $x \in \mathfrak{m}$ (resp. $(\mathfrak{m}I : \mathfrak{m}) = I$). Clearly, every $\mathfrak{m}$-full ideal is weakly $\mathfrak{m}$-full. The notion of $\mathfrak{m}$-full ideals has been studied by many authors so far; see [Conca et al. 2010; Goto 1987; Goto and Hayasaka 2002; Watanabe 1987; 1991] for instance. Notably, it is fundamental to figure out the connections between $\mathfrak{m}$-full ideals and another class of ideals. For example, $\mathfrak{m}$-primary integrally closed ideals are $\mathfrak{m}$-full or equal to the nilradical of R under the assumption that the residue field k is infinite; see [Goto 1987, Theorem 2.4]. There are many related classes of ideals, such as ideals satisfying the Rees property, contracted ideals and basically full ideals. See [Hong et al. 2009; Rush 2013] for the hierarchy of these classes. The notion of weakly $\mathfrak{m}$-full ideals is introduced in [Celikbas et al. 2018, Definition 3.7]. The class of weakly $\mathfrak{m}$-full ideals coincide with that of basically full ideals if they are $\mathfrak{m}$-primary; see [Heinzer et al. 2002, Theorem 2.12]. The following corollary is immediate from the implication (2) $\Rightarrow$ (1) in the above proposition.

Corollary 2.4. *Let* $(R, \mathfrak{m})$ *be a local ring. Let I be an ideal of R such that* $\operatorname{depth} R/I = 0$. *If I is weakly* $\mathfrak{m}$-*full*, *then it is Burch.*

Burch ideals have minimal free resolutions of extremal growth.

Remark 2.5. Let $(R, \mathfrak{m}, k)$ be a local ring. Let I be a Burch ideal of R. Then the equalities $\operatorname{cx}_R I = \operatorname{cx}_R k$ and $\operatorname{curv}_R I = \operatorname{curv}_R k$ hold. For the definitions of the *complexity* $\operatorname{cx}_R M$ and the *curvature* $\operatorname{curv}_R M$ of a module M over a local ring R, see [Avramov 1998, 4.2].

Proof. We may apply [Avramov 1996, Theorem 4] by letting $M = I : \mathfrak{m}$ and $L = I$ because they satisfy $L \supseteq \mathfrak{m}M \neq \mathfrak{m}L$. □

Let $f : (S, \mathfrak{n}, k) \to (R, \mathfrak{m}, k)$ be a surjective homomorphism of local rings, and set $I = \operatorname{Ker} f$. Choi [1992] defined the invariant

$$c_R(S, f) = \dim_k(\mathfrak{n}(I :_S \mathfrak{n})/\mathfrak{n}I).$$

Clearly, an ideal I of a local ring $(S, \mathfrak{n})$ is Burch if and only if Choi's invariant $c_{S/I}(S, \pi)$ is positive, where π is the canonical surjection $S \to S/I$. We give a description of Choi's invariant for a regular local ring.

Proposition 2.6. *Let $(R, \mathfrak{m}, k)$ be a local ring, $(S, \mathfrak{n}, k)$ a regular local ring, and $f : S \to R$ a surjective homomorphism with kernel I. Then*

$$c_R(S, f) = \begin{cases} \dim_k \operatorname{Soc} R + \dim_k \mathrm{H}_1(\mathrm{K}^R) - \operatorname{edim} R - \dim_k \mathrm{H}_1(\mathrm{K}^{R'}) + \operatorname{edim} R' & \text{if } I \neq \mathfrak{n}, \\ \dim_k \mathfrak{n}/\mathfrak{n}^2 & \text{if } I = \mathfrak{n}, \end{cases}$$

where $R' = R/\operatorname{Soc} R$.

Proof. Put $J = (I :_S \mathfrak{n})$. We may assume $I \neq \mathfrak{n}$, and hence $J \neq S$. Then there are equalities

$$\begin{aligned} c_R(S, f) &= \dim_k \mathfrak{n}J/\mathfrak{n}I = \ell(J/I) + (\ell(I/\mathfrak{n}I) - \ell(\mathfrak{n}/\mathfrak{n}^2)) - (\ell(J/\mathfrak{n}J) - \ell(\mathfrak{n}/\mathfrak{n}^2)) \\ &= \dim_k \operatorname{Soc} R + (\dim_k \mathrm{H}_1(\mathrm{K}^R) - \operatorname{edim} R) - (\dim_k \mathrm{H}_1(\mathrm{K}^{R'}) - \operatorname{edim} R'). \end{aligned}$$

Now the proof of the proposition is completed. □

The above result especially says that in the case where $I \neq \mathfrak{n}$ the number $c_R(S, f)$ is determined by the target R of the surjection f. Thus the following result is immediately obtained.

Corollary 2.7 (cf. [Choi 1992, Theorem 2.4]). *Let R be a local ring that is not a field. Let $(S_1, \mathfrak{n}_1)$ and $(S_2, \mathfrak{n}_2)$ be regular local rings, and $f_i : S_i \to R$ surjective homomorphisms for $i = 1, 2$. Then the equality $c_R(S_1, f_1) = c_R(S_2, f_2)$ holds. In particular,* Ker f_1 *is Burch if and only if so is* Ker f_2.

We are now ready to define Burch rings.

Definition 2.8. Let $(R, \mathfrak{m})$ be a local ring of depth t. Denote by $\widehat{R}$ the $\mathfrak{m}$-adic completion of R. We say that R is *Burch* if there exist a maximal $\widehat{R}$-regular sequence $\boldsymbol{x} = x_1, \dots, x_t$ in $\widehat{R}$, a regular local ring S and a Burch ideal I of S such that $\widehat{R}/(\boldsymbol{x}) \cong S/I$.

Remark 2.9. If I is a Burch ideal of a local ring $(R, \mathfrak{m})$, then R/I is a Burch ring of depth zero. Indeed, $I\widehat{R}$ is a Burch ideal of $\widehat{R}$ by Proposition 2.3. Take a Cohen presentation $\widehat{R} \cong S/J$, where $(S, \mathfrak{n})$ is a regular local ring. Let I' be the ideal of S such that $I' \supseteq J$ and $I'/J = I\widehat{R}$. Then one can easily verify that $\mathfrak{n}I' \neq \mathfrak{n}(I' :_S \mathfrak{n})$, that is, I' is a Burch ideal of S. Note that the completion of the local ring R/I is isomorphic to S/I'. Hence R/I is a Burch ring of depth zero.

Let R be a local ring. The *codimension* and *codepth* of R are defined by

$$\operatorname{codim} R = \operatorname{edim} R - \dim R, \qquad \operatorname{codepth} R = \operatorname{edim} R - \operatorname{depth} R.$$

Then R is said to be a *hypersurface* if codepth $R \leq 1$. This is equivalent to saying that the completion $\widehat{R}$ of R is isomorphic to $S/(f)$ for some regular local ring S and some element $f \in S$.

Example 2.10. If R is a hypersurface, then it is a Burch ring. Indeed, take a regular sequence $\boldsymbol{x}$ in $\widehat{R}$ such that $\widehat{R}/(\boldsymbol{x})$ is an artinian local ring with edim $\widehat{R}/(\boldsymbol{x}) \leq 1$. Then $\widehat{R}/(\boldsymbol{x})$ is isomorphic to the quotient ring of a discrete valuation ring S by a nonzero ideal I. By Example 2.2(1), the ideal I of S is Burch.

We define the invariant c_R of a local ring $(R, \mathfrak{m}, k)$ by

$$c_R = \dim_k \operatorname{Soc} R + \dim_k \mathrm{H}_1(\mathrm{K}^R) - \operatorname{edim} R - \dim_k \mathrm{H}_1(\mathrm{K}^{R'}) + \operatorname{edim} R'.$$

Here, we set $R' = R/\operatorname{Soc} R$, and adopt the convention that $\dim_k \mathrm{H}_1(\mathrm{K}^{R'}) = 0 = \operatorname{edim} R'$ in the case where $R' = 0$ (i.e., R is a field). Then we can characterize the Burch rings of depth zero:

Lemma 2.11. *Let $(R, \mathfrak{m}, k)$ be a local ring. Then $c_R = c_{\widehat{R}}$, and the following are equivalent*:

(1) *R is a Burch ring and* $\operatorname{depth} R = 0$.

(2) *$\widehat{R}$ is a Burch ring and* $\operatorname{depth} R = 0$.

(3) $c_R \neq 0$.

(4) $c_R > 0$.

Moreover, *if R is not a field but a Burch ring of depth zero and isomorphic to S/I for some regular local ring $(S, \mathfrak{n})$ and some ideal I of S*, *then I is a Burch ideal of S.*

Proof. The numbers $\dim_k \operatorname{Soc} R$, $\dim_k \mathrm{H}_1(\mathrm{K}^R)$, $\operatorname{edim} R$, $\dim_k \mathrm{H}_1(\mathrm{K}^{R'})$, $\operatorname{edim} R'$ are preserved by the completion of R. In particular, one has $c_R = c_{\widehat{R}}$. Furthermore, take a Cohen presentation $\widehat{R} \cong S/I$ with a complete regular local ring S. Letting $\pi : S \to S/I$ be the natural surjection, we have $c_{\widehat{R}} = c_R(S, \pi)$. This especially shows that c_R is nonnegative. Now we show the equivalence of (1)–(4). It is obvious that (1) and (3) are equivalent to (2) and (4), respectively. The equivalence of (2) and (3) follows from Proposition 2.6. Finally, we show the last assertion. Suppose that R is Burch of depth zero and that $R \cong S/I$, where S is a regular local ring and I is an ideal of S. Then $\widehat{R} \cong T/J$ for some regular local ring T and a Burch ideal J of T. There are surjections from the regular local rings $\widehat{S}$ (the completion of S) and T to the local ring $\widehat{S}/I\widehat{S} \cong \widehat{R} \cong T/J$, and the kernel of the latter is the Burch ideal J. Since $\widehat{R}$ is not a field, Corollary 2.7 implies that $I\widehat{S}$ is a Burch ideal of $\widehat{S}$, and I is a Burch ideal of S by Proposition 2.3. □

We end this section by proving an useful characterization of Burch ideals when $\operatorname{depth} R > 1$. The only if direction is known for $\mathfrak{m}$-full ideals; see [Watanabe 1991, Corollary 7].

Lemma 2.12. *Let $(R, \mathfrak{m})$ be a local ring of depth > 1. An ideal I of R is Burch if and only if there exists a non-zerodivisor $a \in \mathfrak{m}$ such that $R/\mathfrak{m}$ is a direct summand of the R-module I/aI.*

Proof. Assume that I is Burch. Then there exist $a \in \mathfrak{m}$ and $b \in (I :_R \mathfrak{m})$ such that $ab \in I \setminus \mathfrak{m}I$. We have $a \notin \mathfrak{m}^2$, since otherwise $ab \in \mathfrak{m}^2(I :_R \mathfrak{m}) = \mathfrak{m}I$. As $b\mathfrak{m} \subseteq I$, it holds that $ab\mathfrak{m} \subseteq aI$. We can define an R-homomorphism $f : R/\mathfrak{m} \to I/aI$ by $f(\bar{1}) = \overline{ab}$. As $ab \notin \mathfrak{m}I$, the element $\overline{ab}$ is a part of a minimal system of generators of I/aI, and hence f is a split monomorphism.

Conversely, assume that there is a split monomorphism $f : R/\mathfrak{m} \to I/aI$, where $a \in R$ is a non-zerodivisor. Let $c \in I$ be the preimage of $f(\bar{1}) \in I/aI$. Then $c\mathfrak{m} \subseteq aI \subseteq (a)$. The assumption $\operatorname{depth} R > 1$ implies $\operatorname{depth} R/(a) > 0$. Hence c has to be in (a), that is, there exists $b \in R$ with $c = ab$. Observe $ab\mathfrak{m} = c\mathfrak{m} \subseteq aI$. Then a being non-zerodivisor yields $b\mathfrak{m} \in I$. In other words, $b \in (I :_R \mathfrak{m})$. The image of $ab = c$ is a part of a minimal system of generators of I/aI, and we have $ab \notin \mathfrak{m}I$. Thus $\mathfrak{m}(I :_R \mathfrak{m}) \neq \mathfrak{m}I$, which means that I is a Burch ideal. □

Remark 2.13. It is worth noting that Lemma 2.12 can be used to give a quick proof of Theorem 1.1 when depth $R > 1$ and $n > 1$. Namely, if $\operatorname{Tor}_n^R(R/I, M) = \operatorname{Tor}_{n+1}^R(R/I, M) = 0$ then it follows that $\operatorname{Tor}_n^R(I/aI, M) = 0$, which implies that $\operatorname{Tor}_n^R(k, M) = 0$.

3. Cyclic direct summands of second syzygies

The main purpose of this section is to study sufficient conditions for an R-module to have a cyclic direct summand in its second syzygy. They will be used in the proofs of Section 4 and are perhaps of independent interest. In fact, some of our proofs were motivated by [Kustin and Vraciu 2018; Striuli and Vraciu 2011] which focused on different but related problems.

We start by some simple criteria for a homomorphism $f : R \to M$ to be a split monomorphism.

Lemma 3.1. *Let $(R, \mathfrak{m})$ be a local ring of depth zero. Let $f : R \to M$ be a homomorphism of R-modules. Assume one of the following conditions holds*:

(a) *R is Gorenstein.* (b) *M is free.* (c) *M is a syzygy* (*i.e.*, *a submodule of a free module*).

Then the following are equivalent:

(1) *f is a split monomorphism.* (2) *f is a monomorphism.* (3) $f(\operatorname{Soc} R) \neq 0$.

Proof. The implications (1) ⇒ (2) ⇒ (3) are clear. To show (3) ⇒ (1), put $C = \operatorname{Coker} f$.

(a) As R is Gorenstein, we have $\operatorname{Soc} R \cong R/\mathfrak{m}$. The equality $f(\operatorname{Soc} R) \neq 0$ implies $\operatorname{Ker} f \cap \operatorname{Soc} R = 0$. Hence $\operatorname{Ker} f = 0$, and f is injective. As $\operatorname{Ext}_R^1(C, R) = 0$, the map f is split injective.

(b) If f is not split injective, then $\operatorname{Im} f$ is contained in $\mathfrak{m}M$ by the assumption that M is free. This yields that the inclusions $\operatorname{Ker} f \supseteq \operatorname{Ann}(\mathfrak{m}M) \supseteq \operatorname{Soc} R$ hold.

(c) Let $g : M \to F$ be a monomorphism with F free. The composition $gf : R \to F$ satisfies $gf(\operatorname{Soc} R) \neq 0$. By the previous argument, gf is split injective. There is a retraction $r : F \to R$ with $rgf = \mathrm{id}_R$. We see that $rg : M \to R$ is a retraction of f. Therefore f is split injective. □

Next we consider R-homomorphisms from a cyclic R-module to an R-module.

Lemma 3.2. *Let R be a ring, I an ideal of R and M an R-module. Consider an R-homomorphism $f : R/I \to M$. Then f is split injective if and only if the composition map $pf : R/I \to M/IM$ is split injective*, *where $p : M \to M/IM$ is the natural surjection.*

Proof. Suppose f is split injective. Then there is an R-homomorphism $g : M \to R/I$ such that $gf = \mathrm{id}_{R/I}$. On the other hand, g factor through $p : M \to M/IM$, that is $g = g'p$ for some $g' : M/IM \to R/I$. So we see that g' is a retraction of pf. Next, suppose pf is split injective. Then there is an R-homomorphism $h : R/I \to M/IM$ such that $hpf = \mathrm{id}_{R/I}$. Thus $hp : M \to R/I$ is a retraction of f. □

For a matrix A over R we denote by $\mathrm{I}_i(A)$ the ideal of R generated by the i-minors of A. For a linear map ϕ of free R-modules, we define $\mathrm{I}_i(\phi)$ as the ideal $\mathrm{I}_i(A)$, where A is a presentation matrix of ϕ. The following lemma is well-known; we state it for the convenience of the reader.

Lemma 3.3. *Let $R^n \xrightarrow{d} R^m \to M \to 0$ be exact. If $\mathrm{I}_1(d) \subseteq I$, then M/IM is R/I-free.*

Proof. The tensored sequence $(R/I)^n \xrightarrow{d\otimes R/I} (R/I)^m \to M/IM \to 0$ is exact. Since $\mathrm{I}_1(d)$ is contained in I, we see that $d \otimes R/I = 0$, and hence $M \cong (R/I)^m$. □

We generalize [Kustin and Vraciu 2018, Lemma 4.1] as follows.

Proposition 3.4. *Let $(S, \mathfrak{n}, k)$ be a local ring and $I \subseteq J$ ideals of S. Set $R = S/I$. Let*

$$\cdots \to R^q \xrightarrow{\bar{C}} R^p \xrightarrow{\bar{B}} R^n \xrightarrow{\bar{A}} R^m \to M \to 0$$

be a minimal R-free resolution of an R-module M, where $A, B, C, \dots$ are matrices over S. Assume that J satisfies either of the following conditions:

(a) $J \supseteq \mathrm{I}_1(A) + \mathrm{I}_1(C)$. (b) $J \supseteq \mathrm{I}_1(A)$ *and S/J is Gorenstein.*

If $(I :_S J) \not\subseteq (IJ :_S (J :_S \mathfrak{n})\,\mathrm{I}_1(A))$, then S/J is a direct summand of $\Omega^2_R M$.

Proof. For each integer i, let J_i be the ideal of S generated by the entries of the i-th column of A. Then $\mathrm{I}_1(A) = J_1 + \cdots + J_n$, and $(I :_S J) \not\subseteq (IJ :_S (J :_S \mathfrak{n})\,\mathrm{I}_1(A)) = (IJ :_S (J :_S \mathfrak{n})J_1) \cap \cdots \cap (IJ :_S (J :_S \mathfrak{n})J_n)$. Hence $(I :_S J) \not\subseteq (IJ :_S (J :_S \mathfrak{n})J_s)$ for some s. Choose an element $u \in (I :_S J) \setminus (IJ :_S (J :_S \mathfrak{n})J_s)$ and let $v \in R^n$ be the image of $u \cdot e_s$, where e_s is the s-th unit vector of S^n. Since $Ju \subseteq I$ and $\mathrm{I}_1(A) \subseteq J$, v is in $\operatorname{Ker} \bar{A} = \Omega^2_R M =: X$. We can define an R-homomorphism $f : S/J \to X$ by $f(\bar{1}) = v$.

Now we want to show f is split injective. By Lemma 3.2, it is enough to verify so is the induced map $f' = pf : S/J \to X/\bar{J}X$. By Lemmas 3.1 and 3.3, it suffices to check $f'(\operatorname{Soc} S/J) \neq 0$.

Since $u \notin ((IJ) :_S (J :_S \mathfrak{n})J_s)$, we can choose an element $a \in (J :_S \mathfrak{n})$ such that $auJ_s \not\subseteq IJ$. Remark that $a \notin J$, otherwise one has $au \in I$, which forces auJ_S to be contained in IJ. Let $\bar{a}$ be the image of a in S/J. We have that $0 \neq \bar{a} \in \operatorname{Soc} S/J$. If $f'(\bar{a}) = 0$, then $av \in \bar{J}X$. Then there exist elements $x \in JR^p$ and $y \in IR^n$ such that $aue_s = Bx + y$. Observe that $auAe_s = ABx + Ay \in IJR^m$. So we obtain the inclusion $auJ_s \subseteq IJ$, which is contradiction. Thus $f'(\bar{a}) \neq 0$ and we conclude that f is split injective. □

As a corollary, we have the following restatement of [Kustin and Vraciu 2018, Lemma 4.1].

Corollary 3.5. *Let $(S, \mathfrak{n}, k)$ be a local ring and I an ideal of S. Set $R = S/I$ and consider a minimal R-free presentation $R^n \xrightarrow{\bar{A}} R^m \to M \to 0$ of an R-module M, where A is an $m \times n$ matrix over S and $\bar{A}$ is the corresponding matrix over R. If $(I :_S \mathfrak{n}) \not\subseteq (\mathfrak{n}I :_S \mathrm{I}_1(A))$, then k is a direct summand of $\Omega^2_R M$.*

Recall that a module M over a ring R is called *totally reflexive* if the natural map $M \to M^{**}$ is an isomorphism and $\operatorname{Ext}^i_R(M, R) = \operatorname{Ext}^i_R(M^*, R) = 0$ for all $i > 0$, where $(-)^* = \operatorname{Hom}_R(-, R)$. Over a Cohen–Macaulay local ring, a totally reflexive module is a maximal Cohen–Macaulay module, and the converse holds as well over a Gorenstein local ring.

Also, recall that a pair (x, y) of elements of a ring R is called an *exact pair of zerodivisors* if the equalities $(0 :_R x) = yR$ and $(0 :_R y) = xR$ hold [Bonacho Dos Anjos Henriques and Şega 2011]. This is equivalent to saying that the sequence $\cdots \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R \xrightarrow{y} \cdots$ is exact. It is easy to see that for each exact pair of zerodivisors (x, y) the R-modules R/xR and R/yR are totally reflexive.

The following result is another application of Proposition 3.4.

Corollary 3.6. *Let $(S, \mathfrak{n}, k)$ be a local ring and $I \subseteq J$ be $\mathfrak{n}$-primary ideals of S. Assume that S/I, S/J are Gorenstein and that $(I :_S J) \nsubseteq (IJ) :_S ((J :_S \mathfrak{n})J)$. Then there exist elements $a, b \in S$ such that $J = I + (a)$, $(I :_S J) = I + (b)$, and $(\bar{a}, \bar{b})$ is an exact pair of zerodivisors of S/I.*

Proof. Put $R = S/I$. Consider a minimal R-free resolution $\cdots \to R^n \xrightarrow{\bar{A}} R \to S/J \to 0$ of the R-module S/J. Clearly, the equality $\mathrm{I}_1(A) + I = J$ holds. We can derive from Proposition 3.4 that the R-module $\Omega^2_R(S/J)$ has a direct summand isomorphic to S/J. Since R is Gorenstein and the R-module S/J is indecomposable, $\Omega^2_R(S/J)$ is also indecomposable. This implies that $\Omega^2_R(S/J) \cong S/J$, that is, the sequence $0 \to S/J \to R^n \to R \to S/J \to 0$ is exact. We have $\ell(R^n) + \ell(S/J) = \ell(R) + \ell(S/J)$, which yields $n = 1$. Thus the ideal J/I of R is principal, and we find $a \in R$ with $J/I = aR$. As $(0 :_R a) = \Omega^1_R(J/I) \cong S/J$, the ideal $(0 :_R a)$ of R is also principal. Taking a generator b of $(0 :_R a)$, we get an exact pair of zerodivisors (a, b) of R. □

4. Proof of Theorem 4.1 and some applications

This section concerns a surprising characterization of Burch rings of depth zero, and some applications.

Theorem 4.1. *Let $(R, \mathfrak{m}, k)$ be a local ring that is not a field. Then R is a Burch ring of depth zero if and only if k is isomorphic to a direct summand of its second syzygy $\Omega^2_R k$.*

We shall delay the proof until the end of this section. First, note that we can interpret Corollary 3.5 in terms of Burch rings as follows. Here we use the notation $\mathrm{I}_1(M)$ for an R-module M to be the ideal $\mathrm{I}_1(A)$ where A is a matrix in a minimal free presentation $F \xrightarrow{A} G \to M \to 0$ of M. Remark that $\mathrm{I}_1(M)$ is independent of the choice of A (see [Bruns and Herzog 1998, p. 21] for instance).

Proposition 4.2. *Let $(R, \mathfrak{m}, k)$ be a Burch ring of depth zero that is not a field. Let M be an R-module with $\mathrm{I}_1(M) = \mathfrak{m}$. Then k is a direct summand of $\Omega^2_R M$. In particular, k is a direct summand of $\Omega^2_R k$.*

Proof. By [Leuschke and Wiegand 2012, Corollary 1.15], the module $\Omega^2_R M$ contains k as a direct summand if and only if so does $\Omega^2_R M \otimes_R \widehat{R} \cong \Omega^2_{\widehat{R}}(M \otimes_R \widehat{R})$. Hence we may assume that R is complete, and then there is a regular local ring $(S, \mathfrak{n})$ and a Burch ideal $I \subset \mathfrak{n}^2$ such that $R \cong S/I$. Consider a minimal R-free presentation $R^n \xrightarrow{\bar{A}} R^m \to M \to 0$ of an R-module M, where A is a matrix over S and $\bar{A}$ is A modulo I. Then we see that $\mathrm{I}_1(\bar{A}) = \mathrm{I}_1(M) = \mathfrak{m}$, which implies that $\mathrm{I}_1(A) = \mathfrak{n}$. Hence $(I :_S \mathfrak{n}) \nsubseteq (\mathfrak{n}I :_S \mathrm{I}_1(A))$, and thus k is a direct summand of $\Omega^2_R M$ by Corollary 3.5. □

In the situation of the above proposition, M has extremal behavior in the sense of [Avramov 1996], that is, it has maximal projective/injective dimension, complexity and curvature.

Here is an immediate consequence of the above proposition.

Corollary 4.3. *Let $(R, \mathfrak{m}, k)$ be an artinian Burch ring. Then there exists an element $x \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that k is a direct summand of the ideal $(0 :_R x)$ of R.*

Proof. Let $x_1, \dots, x_n$ be a minimal system of generators of $\mathfrak{m}$. There is an exact sequence

$$0 \to \bigoplus_{i=1}^{n} (0 : x_i) \to R^n \xrightarrow{\partial} R^n \to \bigoplus_{i=1}^{n} R/(x_i) \to 0 \quad \text{with} \quad \partial = \begin{pmatrix} x_1 & & & \\ & x_2 & & \\ & & \ddots & \\ & & & x_n \end{pmatrix}.$$

This shows $\mathrm{I}_1(\partial) = \mathfrak{m}$ and $\Omega^2\big(\bigoplus_{i=1}^n R/(x_i)\big) = \bigoplus_{i=1}^n (0 : x_i)$. Proposition 4.2 implies that k is a direct summand of $\bigoplus_{i=1}^n (0 : x_i)$. Since R is artinian, it is henselian. The Krull–Schmidt theorem shows that k is a direct summand of $(0 : x_i)$ for some i. □

The following theorem classifies $\mathfrak{m}$-primary Gorenstein Burch ideals.

Theorem 4.4. *Let $(R, \mathfrak{m})$ be a local ring and I an $\mathfrak{m}$-primary ideal. The following are equivalent*:

(1) *I is a Burch ideal of R and R/I is Gorenstein.*

(2) *I is weakly $\mathfrak{m}$-full and R/I is Gorenstein.*

(3) *I is $\mathfrak{m}$-full and R/I is Gorenstein.*

(4) *$I = (x_1^r, x_2, \dots, x_n)$ with $x_1, \dots, x_n$ a minimal system of generators of $\mathfrak{m}$ and $n, r > 0$.*

Proof. It follows from [Goto and Hayasaka 2002, Proposition 2.4] that (3) is equivalent to (4), while it is obvious that (3) implies (2) and (2) implies (1). Assume (1) to deduce (4). Remark 2.9 shows that R/I is a Burch ring. Proposition 4.2 implies that k is a direct summand of $\Omega^2_{R/I} k$. As $\Omega^2_{R/I} k$ is indecomposable (see [Yoshino 1990, Lemma 8.17] for instance), we get $k \cong \Omega^2_{R/I} k$, whence R/I is a hypersurface. Thus $\mathfrak{m}/I$ is cyclic. Choose an element $x_1 \in \mathfrak{m}$ such that $\overline{x_1}$ is a minimal generator of $\mathfrak{m}/I$. Then x_1 is a minimal generator of $\mathfrak{m}$, and $\mathfrak{m} = I + (x_1)$. There is a unique integer $r > 0$ with $x_1^r \in I$ and $x_1^{r-1} \notin I$. Choose $x_2, \dots, x_n \in I$ so that $\overline{x_2}, \dots, \overline{x_n}$ is a minimal system of generators of $I(R/(x_1)) = \mathfrak{m}/(x_1)$. We see that $x_1, x_2, \dots, x_n$ is a minimal system of generators of $\mathfrak{m}$. Clearly, I contains $J := (x_2, \dots, x_n)$. Note that every $\mathfrak{m}/J$-primary ideal is a power of $\mathfrak{m}/J = ((x_1) + J)/J$. As $x_1^r \in I$ and $x_1^{r-1} \notin I$, we get $I/J = ((x_1^r) + J)/J$. This shows $I = (x_1^r, x_2, \dots, x_n)$. □

We now characterize the modules over a Burch ring having the residue field as a direct summand of some high syzygy.

Theorem 4.5. *Let $(R, \mathfrak{m}, k)$ be a Burch local ring of depth zero which is not a field. Let M be an R-module. Take a minimal free resolution (F, ∂) of M. The following are equivalent*:

(1) $\sum_{i>0} \mathrm{I}_1(\partial_i) = \mathfrak{m}$. (2) *$k$ is a direct summand of $\Omega^r_R M$ for some $r \geq 2$.*

In particular, if $\sum_{i>0} \mathrm{I}_1(\partial_i) = \mathfrak{m}$, then there exists an integer $i \geq 3$ such that $\mathrm{I}_1(\partial_i) = \mathfrak{m}$.

Proof. (2) ⇒ (1): The minimal presentation matrix A of $\Omega^r_R M$ is equivalent to $\left(\begin{smallmatrix} B & 0 \\ 0 & C \end{smallmatrix}\right)$, where B and C are the minimal presentation matrices of k and N, respectively. Hence $\mathrm{I}_1(\partial_{r+1}) = \mathrm{I}_1(A) = \mathrm{I}_1(B) + \mathrm{I}_1(C) = \mathfrak{m} + \mathrm{I}_1(C) = \mathfrak{m}$, which shows $\sum_{i>0} \mathrm{I}_1(\partial_i) = \mathfrak{m}$.

(1) ⇒ (2): We may assume that R is complete, and hence there is a regular local ring $(S, \mathfrak{n})$ and a Burch ideal $I \subseteq S$ with $R \cong S/I$. For each $i > 0$ we identify ∂_i with a matrix over R, and let d_i be a matrix over S lifting ∂_i. Then $\mathfrak{n} = \sum_{i>0} \mathrm{I}_1(d_i) + I$. The noetherian property shows $\mathfrak{n} = \mathrm{I}_1(d_1) + \cdots + \mathrm{I}_1(d_n) + I$ for some $n > 0$. Hence $(\mathfrak{n}I : \mathfrak{n}) = (\mathfrak{n}I : \mathrm{I}_1(d_1) + \cdots + \mathrm{I}_1(d_n) + I) = (\mathfrak{n}I : \mathrm{I}_1(d_1)) \cap \cdots \cap (\mathfrak{n}I : \mathrm{I}_1(d_n)) \cap (\mathfrak{n}I : I)$. Since I is Burch, we have $(I : \mathfrak{n}) \nsubseteq (\mathfrak{n}I : \mathfrak{n})$ by Proposition 2.3. In particular I is nonzero, and we see that $(I : \mathfrak{n}) \subseteq \mathfrak{n} = (\mathfrak{n}I : I)$. We obtain $(I : \mathfrak{n}) \nsubseteq (\mathfrak{n}I : \mathrm{I}_1(d_t))$ for some $1 \le t \le n$. It follows from Corollary 3.5 that k is a direct summand of the cokernel of ∂_t, which is $\Omega_R^{t+1} M$. □

Let k be a field. A local ring R is said to be a *fiber product* (over k) provided that it is of the form

$$R \cong S \times_k T = \{(s, t) \in S \times T \mid \pi_S(s) = \pi_T(t)\},$$

where $(S, \mathfrak{m}_S)$ and $(T, \mathfrak{m}_T)$ are local rings with common residue field k, and $\pi_S : S \twoheadrightarrow k$ and $\pi_T : T \twoheadrightarrow k$ are the natural surjections. The set $S \times_k T$ is a local ring with maximal ideal $\mathfrak{m}_{S \times_k T} = \mathfrak{m}_S \oplus \mathfrak{m}_T$ and residue field k. Conversely, a local ring R with decomposable maximal ideal $\mathfrak{m}_R = I \oplus J$ is a fiber product since $R \cong (R/I) \times_k (R/J)$. These observations are due to Ogoma [1984, Lemma 3.1].

We can now complete the proof of Theorem 4.1.

Proof of Theorem 4.1. The "only if" part is a direct consequence of Proposition 4.2.

We consider the "if" part. Again we may assume that R is complete. Take a Cohen presentation $R \cong S/I$, where $(S, \mathfrak{n})$ is a regular local ring and I is an ideal of S contained in $\mathfrak{n}^2$. If $(I :_S \mathfrak{n}) \nsubseteq \mathfrak{n}^2$, then there is an element $x \in (\mathfrak{m} \cap \operatorname{Soc} R) \setminus \mathfrak{m}^2$. One has a decomposition $\mathfrak{m} = J \oplus (x)$, which means that R is of the form $S \times_k T$ with $\operatorname{edim} T = 1$. Then R is Burch by Example 2.10 and Lemma 6.14. Thus we may assume that $(I :_S \mathfrak{n}) \subseteq \mathfrak{n}^2$. Suppose that I is not Burch, so that $\mathfrak{n}(I :_S \mathfrak{n}) = \mathfrak{n}I$. We aim to show that $\operatorname{Soc} \Omega_R^2 k \subseteq \mathfrak{m}\Omega_R^2 k$. Take minimal generators $x_1, \dots, x_e$ of $\mathfrak{n}$. There is a commutative diagram

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & \Omega_S^2 k \arrow[r] \arrow[d] & \Omega_R^2 k \arrow[d] & \\
0 \arrow[r] & I^e \arrow[r] \arrow[d] & S^e \arrow[r] \arrow[d] & R^e \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & I \arrow[r] \arrow[d] & \mathfrak{n} \arrow[r] \arrow[d] & \mathfrak{m} \arrow[r] \arrow[d] & 0 \\
 & I/\mathfrak{n}I \arrow[d] & 0 & 0 & \\
 & 0 & & &
\end{tikzcd}$$

of S-modules with exact rows and columns. Applying the snake lemma, we get an exact sequence

$$\Omega_S^2 k \to \Omega_R^2 k \xrightarrow{\delta} I/\mathfrak{n}I \to 0, \tag{4.5.1}$$

where δ sends each element $a \in \Omega_R^2 k$ whose preimage in S^e is ${}^{\mathrm{t}}(a_1, \dots, a_e)$ to the image of $\sum_i x_i a_i$ in $I/\mathfrak{n}I$. Now consider element $a \in \operatorname{Soc} \Omega_R^2 k$. This means that the preimage ${}^{\mathrm{t}}(a_1, \dots, a_e) \in S^e$ of a satisfies $a_i \in (I :_S \mathfrak{n})$ for all i. Therefore, the element $\sum_i x_i a_i \in S$ is contained in $\mathfrak{n}(I :_S \mathfrak{n}) = \mathfrak{n}I$. This yields that $\delta(a) = 0$. By the exact sequence (4.5.1), we can take the preimage $(a_1, \dots, a_e) \in S^e$ of a to be contained in $\Omega_S^2 k$. We already have ${}^{\mathrm{t}}(a_1, \dots, a_e) \in (I :_S \mathfrak{n})S^e \subseteq \mathfrak{n}^2 S^e$. It follows that ${}^{\mathrm{t}}(a_1, \dots, a_e) \in \Omega_S^2 k \cap \mathfrak{n}^2 S^e \subseteq \mathfrak{n}\Omega_S^2 k$, see [Herzog et al. 1983, Theorems 3.7 and 4.1] for the second containment. Consequently, the element a is contained in $\mathfrak{m}\Omega_R^2 k$. This allows us to conclude that if $\operatorname{Soc} \Omega_R^2 k \not\subseteq \mathfrak{m}\Omega_R^2 k$ then I is a Burch ideal, and hence R is a Burch ring. □

In view of Theorem 4.1, one may wonder if an artinian local ring R is Burch if the residue field k is a direct summand of $\Omega^n k$ for some $n \geq 3$. This is not true in general:

Example 4.6. Let k be a field, and consider the ring $R = k[\![x, y]\!]/I$, where $I = (x^4, x^2y^2, y^4)$. The minimal free resolution of k is

$$0 \leftarrow k \leftarrow R \xleftarrow{(x\ y)} R^2 \xleftarrow{\begin{pmatrix} -y & xy^2 & x^3 & 0 \\ x & 0 & 0 & y^3 \end{pmatrix}} R^4 \xleftarrow{\begin{pmatrix} xy^2 & 0 & x^3 & 0 & 0 & y^3 & 0 & 0 \\ y & x & 0 & 0 & 0 & 0 & y^2 & 0 \\ 0 & 0 & y & x & 0 & 0 & 0 & y^2 \\ 0 & 0 & 0 & 0 & y & -x & 0 & 0 \end{pmatrix}} R^8 \leftarrow \cdots .$$

We have $\operatorname{Soc} \Omega^3 k = \operatorname{Soc} R^4 = (x^3y, xy^3)R^4$. The column vector

$$z := {}^{\mathrm{t}}(x^3y, 0, 0, 0) = y \cdot {}^{\mathrm{t}}(x^3, 0, y, 0) - {}^{\mathrm{t}}(0, 0, y^2, 0)$$

is in $\operatorname{Soc} \Omega^3 k \setminus \mathfrak{m}\Omega^3 k$. The assignment $1 \mapsto z$ makes a split monomorphism $k \to \Omega^3 k$, and k is a direct summand of $\Omega^3 k$. However, R is not Burch as one can easily check the equality $\mathfrak{m}(I : \mathfrak{m}) = \mathfrak{m}I$.

5. Burch rings of positive depth

In this section, we study Burch rings of positive depth. First of all, let us investigate what Gorenstein Burch rings are.

Proposition 5.1. *A local ring is Burch and Gorenstein if and only if it is a hypersurface.*

Proof. Let R be a local ring of dimension d. If R is hypersurface, then R is clearly Gorenstein, and it is also Burch by Example 2.10. Conversely, suppose that R is Burch and Gorenstein. Then there exists a system of parameters $\boldsymbol{x} = x_1, \dots, x_d$ such that $\widehat{R}/(\boldsymbol{x})$ is an artinian Gorenstein Burch local ring. By definition, there exist a regular local ring $(S, \mathfrak{n})$ and a Burch ideal I of S such that $\widehat{R}/(\boldsymbol{x}) \cong S/I$. By Theorem 4.4, there are a minimal system of generators $y_1, \dots, y_n$ of $\mathfrak{n}$ with $n > 0$ and an integer $r > 0$ such that $I = (y_1^r, y_2, \dots, y_n)$. In particular, $S/I \cong \widehat{R}/(\boldsymbol{x})$ is a hypersurface, and so is R. □

A Cohen–Macaulay local ring R is said to have *minimal multiplicity* if $e(R) = \operatorname{codim} R + 1$.

Proposition 5.2. *Let $(R, \mathfrak{m}, k)$ be a Cohen–Macaulay local ring with minimal multiplicity, and assume that k is infinite. Then R is Burch.*

Proof. We can find a general system of parameters $\underline{x}$ such that $A = R/(\underline{x})$ is artinian and still has minimal multiplicity. This simply means that $\mathfrak{m}_A^2 = 0$, so the first syzygy of k is a k-vector space. Thus A is Burch by Theorem 4.1 and so is R. □

Remark 5.3. A Cohen–Macaulay local ring with minimal multiplicity is a typical example of a Golod local ring. In view of Proposition 5.2, the reader may wonder if a Golod local ring is Burch. This is not true in general; the ring R given in Example 4.6 is not Burch but Golod by [Avramov 2012, 1.4.3 and 2.1]. Neither can we say that Burch ideals are Golod. Indeed, let $R = k[x, y, z, w]/\mathfrak{m}J$, where $\mathfrak{m} = (x, y, z, w)$ and $J = (x^2, y^2, z^2, w^2)$ in $k[x, y, z, w]$. This is the example of non-Golod ring R given in [De Stefani 2016, Example 2.1]. However, it is Burch by Example 2.2(2).

We establish a lemma to prove our next result on Burch rings.

Lemma 5.4. *Let $(R, \mathfrak{m}, k)$ be a 1-dimensional Cohen–Macaulay local ring with minimal multiplicity. Then there exists an isomorphism $\mathfrak{m}^* \cong \mathfrak{m}$, where $(-)^* = \operatorname{Hom}_R(-, R)$.*

Proof. If R is a discrete valuation ring, then $\mathfrak{m} \cong R$, and hence $\mathfrak{m}^* \cong \mathfrak{m}$. So we assume that R is not a discrete valuation ring. Since R has minimal multiplicity, by [Lipman 1971, Lemma 1.11], there is an R-regular element $x \in \mathfrak{m}$ such that $\mathfrak{m}^2 = x\mathfrak{m}$. Let Q be the total quotient ring of R. We have

$$\mathfrak{m}^* = \operatorname{Hom}_R(\mathfrak{m}, R) \cong \operatorname{Hom}_R(\mathfrak{m}, xR) \cong (xR :_Q \mathfrak{m}) \supseteq \mathfrak{m},$$

where the second isomorphism follows from [Kobayashi and Takahashi 2019, Proposition 2.4(1)] for instance. For each element $\frac{a}{s} \in (xR :_Q \mathfrak{m})$, we have $ax \in a\mathfrak{m} \subseteq sxR$, which implies $a \in sR$ as x is R-regular, and hence $\frac{a}{s} \in R$. Therefore $(xR :_Q \mathfrak{m})$ is an ideal of R containing $\mathfrak{m}$. Since R is not a discrete valuation ring, it is a proper ideal. We get $(xR :_Q \mathfrak{m}) = \mathfrak{m}$, and consequently $\mathfrak{m}^* \cong \mathfrak{m}$. □

Cohen–Macaulay rings of dimension 1 with minimal multiplicity have a remarkable property.

Proposition 5.5. *Let $(R, \mathfrak{m}, k)$ be a 1-dimensional Cohen–Macaulay local ring with minimal multiplicity. Then the quotient artinian ring $R/(x)$ is a Burch ring for any parameter $x \in \mathfrak{m} \setminus \mathfrak{m}^2$.*

Proof. If R is regular, then it is a discrete valuation ring, and x is a uniformizer. Hence $R/(x)$ is a field, and it is Burch. Thus we assume that R is singular. Applying $(-)^* = \operatorname{Hom}_R(-, R)$ to the natural exact sequence $0 \to \mathfrak{m} \to R \to k \to 0$, we get an exact sequence $0 \to R \to \mathfrak{m}^* \to k^{\oplus r} \to 0$, where r is the type of R. Making the pullback diagram of the map $\mathfrak{m}^* \to k^{\oplus r}$ and the natural surjection $R^{\oplus r} \to k^{\oplus r}$, we obtain an exact sequence $0 \to \mathfrak{m}^{\oplus r} \to R^{\oplus(r+1)} \to \mathfrak{m}^* \to 0$. As R is singular, $\mathfrak{m}^{\oplus r}$ does not have a nonzero free summand by [Dutta 1989, Corollary 1.3]. We get an isomorphism $\mathfrak{m}^{\oplus r} \cong \Omega(\mathfrak{m}^*)$. Combining this with Lemma 5.4 yields $\mathfrak{m}^{\oplus r} \cong \Omega\mathfrak{m} \cong \Omega^2 k$. Since x is an R-regular element in $\mathfrak{m} \setminus \mathfrak{m}^2$, there is a split exact sequence $0 \to k \to \mathfrak{m}/x\mathfrak{m} \to \mathfrak{m}/(x) \to 0$, which induces $\mathfrak{m}/x\mathfrak{m} \cong k \oplus \mathfrak{m}/(x)$. We obtain isomorphisms of $R/(x)$-modules

$$\begin{aligned} k^{\oplus r} \oplus (\mathfrak{m}/(x))^{\oplus r} &\cong (\mathfrak{m}/x\mathfrak{m})^{\oplus r} \cong \Omega^2 k/x\Omega^2 k \cong \Omega_{R/(x)}(\mathfrak{m}/x\mathfrak{m}) \\ &\cong \Omega_{R/(x)}k \oplus \Omega_{R/(x)}(\mathfrak{m}/(x)) \cong \Omega_{R/(x)}k \oplus \Omega^2_{R/(x)}k, \end{aligned}$$

where the third isomorphism holds since there is an exact sequence $0 \to \Omega^2 k \to R^{\oplus n} \to \mathfrak{m} \to 0$ with $n = \operatorname{edim} R$, which induces an exact sequence $0 \to \Omega^2 k/x\Omega^2 k \to (R/(x))^{\oplus n} \to \mathfrak{m}/x\mathfrak{m} \to 0$. As $R/(x)$ is an artinian local ring, it is henselian. The Krull–Schmidt theorem implies that k is a direct summand of either $\Omega_{R/(x)}k$ or $\Omega^2_{R/(x)}k$. In the former case, applying $\Omega_{R/(x)}(-)$ shows that k is a direct summand of $\Omega^2_{R/(x)}k$. Theorem 4.1 concludes that $R/(x)$ is a Burch ring. □

Proposition 5.6. *Let $S = k[x_1, \dots, x_n]$ be a polynomial ring over an infinite field and $I \subset S$ is a homogenous ideal such that S/I is Cohen–Macaulay and I has a linear resolution. Then $R = (S/I)_\mathfrak{m}$ is Burch where $\mathfrak{m} = (x_1, \dots, x_n)$.*

Proof. Let $A = S/I$ and $(l_1, \dots, l_d)$ be a general linear system of parameters on A. We write $A/(l_1, \dots, l_d)A$ as T/J where T is a polynomial ring in $n-d$ variables over k and J is a zero-dimensional ideal. Then J still has linear resolution. Assume I (and J) are generated in degree t, then the regularity of J is t, but since J is zero-dimensional, the socle degree of J is $t-1$. Thus $J = \mathfrak{n}^t$ where $\mathfrak{n}$ is the irrelevant ideal of T, and so R is Burch by definition and Example 2.2. □

Example 5.7. There are many examples satisfying the conditions of Proposition 5.6. For example, let $m \geq n$ and let $I = I_n \subset k[x_{ij}] = S$ be the ideal generated by maximal minors in a m by n matrix of indeterminates. Then it is well-known that S/I is Cohen–Macaulay with $\dim S/I = (m+1)(n-1)$ and the a-invariant of S/I is $-m(n-1)$; see [Bruns and Herzog 1998]. It follows that the regularity of I is n, so it has linear resolution.

Another source of examples are Stanley–Reisner rings of "facet constructible" or "stacked" simplicial complexes; see [Dao and Schweig 2019, Theorems 4.1 and 4.4].

We will show in Corollary 7.9 that if x is a regular element of a local ring $(R, \mathfrak{m})$ such that $R/(x)$ is Burch, then $x \notin \mathfrak{m}^2$. It is natural to ask whether the quotient ring R/Q of a Burch ring R is again Burch for any ideal Q generated by regular sequence consisting of elements in $\mathfrak{m} \setminus \mathfrak{m}^2$. This is true if R is either a hypersurface or a Cohen–Macaulay local ring of dimension one with minimal multiplicity, as we saw in Propositions 5.1 and 5.5. The example below says that the question is not always affirmative.

Example 5.8. Let k be a field, and let $R = k[\![x, y, z]\!]/\mathrm{I}_2\begin{pmatrix} x^2 & y & z^2 \\ y & z^2 & x^2 \end{pmatrix}$. The Hilbert–Burch theorem implies that R is a Cohen–Macaulay local ring of dimension 1. The ring R is a Burch ring since so is the artinian quotient ring $R/(x) = k[\![y, z]\!]/(y^2, yz^2, z^4)$. However, the artinian ring $R/(y) = k[\![x, z]\!]/(x^4, x^2z^2, z^4)$ is not Burch. By Theorem 4.1, the R-module k is a direct summand of $\Omega^2_{R/(x)}k$, but not a direct summand of $\Omega^2_{R/(y)}k$. Incidentally, the module k is a direct summand of $\Omega^3_{R/(y)}k$ by Example 4.6.

To show our next result on Burch rings, we prepare a lemma on cancellation of free summands.

Lemma 5.9. *Let R be a local ring. Let M, N be R-modules having no nonzero free summand. If $M \oplus R^{\oplus a} \cong N \oplus R^{\oplus b}$ for some $a, b \geq 0$, then $M \cong N$ and $a = b$.*

Proof. We may assume $a \geq b$. Taking the completions, we get isomorphisms $\widehat{M} \oplus \widehat{R}^{\oplus a} \cong \widehat{N} \oplus \widehat{R}^{\oplus b}$. Write $\widehat{M} = X \oplus \widehat{R}^{\oplus c}$ and $\widehat{N} = Y \oplus \widehat{R}^{\oplus d}$ with $c, d \geq 0$ integers and X, Y having no nonzero free summand. Then $X \oplus \widehat{R}^{\oplus(c+a)} \cong Y \oplus \widehat{R}^{\oplus(d+b)}$. As $\widehat{R}$ is henselian, we can apply the Krull–Schmidt theorem to deduce $X \cong Y$ and $c+a = d+b$. Hence $d = c+(a-b)$, and we get $\widehat{N} = Y \oplus \widehat{R}^{\oplus d} \cong X \oplus \widehat{R}^{\oplus(c+(a-b))} = \widehat{M} \oplus \widehat{R}^{\oplus(a-b)} \cong \widehat{L}$, where $L := M \oplus R^{\oplus(a-b)}$. It follows from [Leuschke and Wiegand 2012, Corollary 1.15] that N is isomorphic to L. Since N has no nonzero free summand, we must have $a = b$, and therefore $M = L \cong N$. □

The following result is a higher-dimensional version of the "only if" part of Theorem 4.1.

Proposition 5.10. *Let $(R, \mathfrak{m}, k)$ be a singular Burch ring of depth t. Then $\Omega^t k$ is a direct summand of $\Omega^{t+2}k$.*

Proof. We prove the proposition by induction on t. The case $t = 0$ follows from Lemma 2.11, so let $t \geq 1$. There is an R-sequence $\boldsymbol{x} = x_1, \ldots, x_t$ such that $R/(\boldsymbol{x})$ is a Burch ring of depth zero. Hence $R/(x_1)$ is a Burch ring of dimension $d-1$. The induction hypothesis implies that $\Omega^{t-1}_{R/(x_1)}k$ is a direct summand of $\Omega^{t+1}_{R/(x_1)}k$. Taking the syzygy over R, we see that $\Omega_R \Omega^{t-1}_{R/(x_1)}k$ is a direct summand of $\Omega_R \Omega^{t+1}_{R/(x_1)}k$. For each $n \geq 0$ there is an exact sequence $0 \to \Omega^n_{R/(x_1)}k \to P_{n-1} \to \cdots \to P_1 \to P_0 \to k \to 0$ with each P_i being a direct sum of copies of $R/(x_1)$, which gives rise to an exact sequence

$$0 \to \Omega_R \Omega^n_{R/(x_1)}k \to \Omega_R P_{n-1} \oplus R^{\oplus e_{n-1}} \to \cdots \to \Omega_R P_1 \oplus R^{\oplus e_1} \to \Omega_R P_0 \oplus R^{\oplus e_0} \to \Omega_R k \to 0$$

with $e_i \geq 0$ for $0 \leq i \leq n-1$. Note that each $\Omega_R P_i$ is a free R-module. The above sequence shows that $\Omega^{n+1}_R k = \Omega^n_R(\Omega_R k)$ is isomorphic to $\Omega_R \Omega^n_{R/(x_1)}k$ up to free R-summands. We obtain an R-isomorphism $\Omega^{n+1}_R k \oplus R^{\oplus e} \cong \Omega_R \Omega^n_{R/(x_1)}k$ with $e \geq 0$. Thus, for some $a, b \geq 0$ we have that $\Omega^t_R k \oplus R^{\oplus a}$ is a direct summand of $\Omega^{t+2}_R k \oplus R^{\oplus b}$. Since R is singular, it follows from [Dutta 1989, Corollary 1.3] that $\Omega^i_R k$ has no nonzero free summand for all $i \geq 0$. Applying Lemma 5.9, we observe that $\Omega^t_R k$ is a direct summand of $\Omega^{t+2}_R k$. □

We pose a question asking whether or not the converse of Proposition 5.10 holds true.

Question 5.11. Does there exist a non-Burch local ring $(R, \mathfrak{m}, k)$ of depth t such that $\Omega^t k$ is a direct summand of $\Omega^{t+2}k$?

6. Some classes of Burch ideals and rings

In this section, we study Burch ideals in a regular local ring and give a complete characterization in dimension two. We also give a simple characterization of monomial Burch ideals. We compare Burch rings to other classes of rings: radical cube zero, almost Gorenstein, nearly Gorenstein, and fiber products.

Over a two-dimensional regular local ring $(R, \mathfrak{m})$, the Burch ideals I are characterized in terms of the minimal numbers of generators of I and $\mathfrak{m}I$.

Lemma 6.1. *Let $(R, \mathfrak{m})$ be a regular local ring of dimension two, and let I be an $\mathfrak{m}$-primary ideal of R. Then I is a Burch ideal of R if and only if $\mu(\mathfrak{m}I) < 2\mu(I)$.*

Proof. It follows from the Hilbert–Burch theorem that $\mu(I) = r(R/I) + 1$ and $\mu(\mathfrak{m}I) = r(R/\mathfrak{m}I) + 1$. The assertion follows from the equivalence (1) ⇔ (2) in Proposition 2.3. □

Now we can show the following theorem, which particularly gives a characterization of the Burch ideals of two-dimensional regular local rings in terms of minimal free resolutions. Compare this theorem with the result of Corso, Huneke and Vasconcelos [Corso et al. 1998, Lemma 3.6].

Theorem 6.2. *Let $(R, \mathfrak{m})$ be a regular local ring of dimension d. Let I be an $\mathfrak{m}$-primary ideal of R. Take a minimal free resolution $0 \to F_d \xrightarrow{\varphi_d} F_{d-1} \to \cdots \to F_1 \xrightarrow{\varphi_1} F_0 \to R/I \to 0$ of the R-module R/I. Consider the following conditions*:

1. *The ideal I is Burch.*
2. *There exist a regular system of parameters $x_1, \dots, x_d$ and an integer $r > 0$ such that $\mathrm{I}_1(\varphi_d) = (x_1^r, x_2, \dots, x_d)$.*
3. *One has $(I : \mathfrak{m})^2 \neq I(I : \mathfrak{m})$.*

Then the implication (1) ⇒ (2) *holds. If R contains a field, then the implication* (3) ⇒ (2) *holds. If $d = 2$, then the implication* (2) ⇒ (1) *holds as well.*

Proof. We first show that (1) implies (2). We may assume $d \geq 2$, so that R has depth greater than 1. By Lemma 2.12 and its proof, there is a non-zerodivisor $x_1 \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that I/x_1I contains the residue field $R/\mathfrak{m}$ as a direct summand. Tensoring $R/(x)$ with the complex $F = (0 \to F_d \to \cdots \to F_0 \to 0)$, we get a minimal free resolution

$$(0 \to F_d/x_1F_d \xrightarrow{\varphi_d \otimes S/(x_1)} F_{d-1}/F_{d-1} \to \cdots \to F_2/x_1F_2 \to F_1/x_1F_1 \to 0)$$

of I/x_1I over $R/(x_1)$. As $R/\mathfrak{m}$ is a direct summand of I/x_1I, a minimal $R/(x_1)$-free resolution G of $R/\mathfrak{m}$ is a direct summand of the above complex. Since G is isomorphic to the Koszul complex $\mathrm{K}^{R/(x_1)}$ of $R/(x_1)$, the ideal $\mathrm{I}_1(\varphi_d \otimes R/(x_1))$ of $R/(x_1)$ contains the maximal ideal $\mathfrak{m}/(x_1)$. Therefore $\mathrm{I}_1(\varphi_d)$ contains elements $x_2, \dots, x_d$ such that $x_1, x_2, \dots, x_d$ form a regular system of parameters of R. Since the radical of $\mathrm{I}_1(\varphi_d)$ contains I, it is an $\mathfrak{m}$-primary ideal. It follows that there is an integer $r > 0$ such that $x_1^r \in \mathrm{I}_1(\varphi_d)$ but $x_1^{r-1} \notin \mathrm{I}_1(\varphi_d)$. We obtain $\mathrm{I}_1(\varphi_d) = (x_1^r, x_2, \dots, x_d)$, and (2) follows.

Next, under the assumption that R contains a field, we prove that (3) implies (2). We use an analogue of the proof of [Corso et al. 2018, Theorem 2.4]. After completion, we may assume that R is a formal power series ring over a field k. Suppose that (2) does not hold. Then $d \geq 2$ and we can take an ideal L containing $\mathrm{I}_1(\varphi_d)$ such that there is a regular system of parameters $x_1, \dots, x_d$ with $L = (x_1^2, x_1x_2, x_2^2, x_3, \dots, x_d)$. By [Corso et al. 2018, Proposition 2.1], an isomorphism $(I : L)/I \cong \omega_{R/L} \otimes_R F_d$ and its retraction $(I : \mathfrak{m})/I \cong \omega_{R/\mathfrak{m}} \otimes_R F_d$ are given. Note that the canonical module $\omega_{R/L}$ of R/L is isomorphic to $(0 :_{\mathrm{E}_R(k)} L)$. The module $\mathrm{E}_R(k)$ is identified with $k[x_1, x_1^{-1}, \dots, x_d, x_d^{-1}]/N$, where N is the subspace spanned by the monomials not in $k[x_1^{-1}, \dots, x_d^{-1}]$. Under this identification, $\omega_{R/L} = (0 : L)$ is generated by the monomials x_1^{-1} and x_2^{-1}. Set $M = \{x_1^{-1}, x_2^{-1}\}$. Then $x_1M = \{1\} = x_2M$ generates $\omega_{R/\mathfrak{m}}$. Also, either $x_1w = 0$ or $x_2w = 0$ holds for all $w \in M$. We may apply [Corso et al. 2018, Proposition 2.3] as in the proof of [Corso et al. 2018, Theorem 2.4] to get $(I:\mathfrak{m})^2 = I(I:\mathfrak{m})$, contrary to (3). We have shown that (3) implies (2).

Finally, assuming $d = 2$, we prove (2) implies (1). As the entries of φ_2 are contained in $\mathfrak{m}$, we have an exact sequence $0 \to F_2 \xrightarrow{\varphi_2} \mathfrak{m}F_1 \to \mathfrak{m}I \to 0$. This induces an exact sequence

$$F_2/\mathfrak{m}F_2 \xrightarrow{\varphi_2 \otimes_R R/\mathfrak{m}} \mathfrak{m}F_1/\mathfrak{m}^2F_1 \to \mathfrak{m}I/\mathfrak{m}^2 I \to 0.$$

Suppose that (2) holds. Then $\varphi_2 \otimes_R R/\mathfrak{m} \neq 0$, and $\dim_{R/\mathfrak{m}}(\mathfrak{m}I/\mathfrak{m}^2I) < \dim_{R/\mathfrak{m}}(\mathfrak{m}F_1/\mathfrak{m}^2F_1)$. Note that $\dim_{R/\mathfrak{m}}(\mathfrak{m}I/\mathfrak{m}^2I) = \mu(\mathfrak{m}I)$ and $\dim_{R/\mathfrak{m}}(\mathfrak{m}F_1/\mathfrak{m}^2F_1) = 2\mu(I)$. Lemma 6.1 shows that I is a Burch ideal, that is, (1) holds. □

Example 6.3. (1) Let $I = (x^4, y^4, z^4, x^2y, y^2z, z^2x)$ be an ideal of $(R, \mathfrak{m}) = k[\![x, y, z]\!]$. Then one can check that $(I:\mathfrak{m}) = (x^4, x^3z, x^2y, xy^3, xyz, xz^2, y^4, y^2z, yz^3, z^4)$, and so $(I:\mathfrak{m})^2 \neq I(I:\mathfrak{m})$. However, I is not Burch. This gives a counterexample of the implication (3) ⇒ (1) in Theorem 6.2.

(2) Let $I = (x^4, y^4, x^3y, xy^3)$ be an ideal of $(R, \mathfrak{m}) = k[\![x, y]\!]$. Then $(I:\mathfrak{m}) = (x^3, x^2y^2, y^3)$. We see that $(I:\mathfrak{m})^2 = I(I:\mathfrak{m})$ and I is Burch. This shows that the implication (1) ⇒ (3) in Theorem 6.2 is not affirmative, even when R has dimension two.

We provide some characterizations of Burchness for monomial ideals of regular local rings.

Proposition 6.4. *Let $(R, \mathfrak{m})$ be a regular local ring of dimension d. Let $x_1, \dots, x_d$ be a regular system of parameters of R, and let I be a monomial ideal (in the x_is) of R. Then I is Burch if and only if there exist a monomial $m \in I \setminus \mathfrak{m}I$ and an integer $1 \le i \le d$ such that $x_i \mid m$ and $m(x_j/x_i) \in I$ for all $1 \le j \le d$.*

Proof. Since I is a Burch ideal, we have $\mathfrak{m}I \neq \mathfrak{m}(I:\mathfrak{m})$. Therefore, there is a monomial $m' \in (I:\mathfrak{m})$ and an integer i such that $x_im' \notin \mathfrak{m}I$. It also holds that $x_jm' \in I$ for all $j = 1, \dots, d$. So the element $m := x_im'$ satisfies $m(x_j/x_i) \in I$ for all $j = 1, \dots, d$. □

Corollary 6.5. *Let $(R, \mathfrak{m})$ be a regular local ring of dimension 2 with a regular system of parameters x, y. Let $I = (x^{a_1}y^{b_1}, x^{a_2}y^{b_2}, \dots, x^{a_n}y^{b_n})$ be a monomial ideal with $a_1 > a_2 > \cdots > a_n$ and $b_1 < b_2 < \cdots < b_n$. Then I is a Burch ideal of R if and only if $a_i = a_{i+1} + 1$ or $b_i = b_{i+1} - 1$ for some $i = 1, \dots, n$.*

Proof. By Proposition 6.4, the ideal I is Burch if and only if $x^{a_i}y^{b_i}(y/x) \in I$ or $x^{a_i}y^{b_i}(x/y) \in I$ for some $i = 1, \dots, n$. Equivalently, either $x^{a_i-1}y^{b_i+1} \in I$ or $x^{a_i+1}y^{b_i-1} \in I$ holds for some $i = 1, \dots, n$. Since $a_{i+1} \le a_i - 1 < a_i < a_i + 1 \le a_{i-1}$ and $b_{i-1} \le b_i - 1 < b_i < b_i + 1 \le b_{i+1}$, the condition is equivalent to saying that $b_i + 1 = b_{i+1}$ or $a_i + 1 = a_{i-1}$ for some $i = 1, \dots, n$. □

Next, we discuss the relationship between Burch rings and several classes of rings studied previously in the literature.

Recall that the *trace ideal* $\operatorname{tr} M$ of an R-module M is defined by $\operatorname{tr} M = \sum_{f \in \operatorname{Hom}_R(M,R)} \operatorname{Im} f$. The following notions are introduced in [Herzog et al. 2019; Striuli and Vraciu 2011].

Definition 6.6 (Herzog–Hibi–Stamate). Let $(R, \mathfrak{m})$ be a Cohen–Macaulay local ring with canonical module ω. Then R is called *nearly Gorenstein* if $\operatorname{tr} \omega$ contains $\mathfrak{m}$.

Definition 6.7 (Striuli–Vraciu). Let $(R, \mathfrak{m})$ be an artinian local ring. Then R is called *almost Gorenstein*[2] if $(0 : (0 : I)) \subseteq (I : \mathfrak{m})$ for all ideals I of R.

It follows from [Huneke and Vraciu 2006, Proposition 1.1] that artinian nearly Gorenstein local rings are almost Gorenstein.

We want to consider the relationship of Burchness with near Gorensteinness and almost Gorensteinness. For this, we establish two lemmas.

Lemma 6.8. *Let $(R, \mathfrak{m}, k)$ be a non-Gorenstein artinian almost Gorenstein local ring. Let $R^n \xrightarrow{A} R^m \to E \to 0$ be a minimal R-free presentation of the R-module $E = \mathrm{E}_R(k)$. One then has $\mathrm{I}_1(A) = \mathfrak{m}$.*

Proof. Choose an artinian Gorenstein local ring $(S, \mathfrak{n})$ and an ideal I of S such that $R \cong S/I$. We identify E with $(0 :_S I)$ via the isomorphisms $E \cong \mathrm{Hom}_S(R, S) \cong (0 :_S I)$. Let $x_1, \dots, x_m$ be a minimal system of generators of E. By [Striuli and Vraciu 2011, Lemma 1.2] we have

$$\mathfrak{n} = ((x_1) :_S (x_2, \dots, x_m)) + ((x_2, \dots, x_m) :_S x_1).$$

We find a matrix B over S with m rows such that $\mathrm{I}_1(B) = \mathfrak{n}$ and $(x_1 \cdots x_m)B = 0$. We find a matrix C over R such that the matrix $\bar{B}$ over R corresponding to B is equal to AC. We have $\mathfrak{m} = \mathrm{I}_1(\bar{B}) = \mathrm{I}_1(A \cdot C) \subseteq \mathrm{I}_1(A) \subseteq \mathfrak{m}$, which implies $\mathrm{I}_1(A) = \mathfrak{m}$. □

Lemma 6.9. *Let $(R, \mathfrak{m})$ be a regular local ring of dimension d, and let $I \subseteq \mathfrak{m}^2$ be an ideal of R. Take a minimal free resolution $0 \to F_d \xrightarrow{\varphi_d} F_{d-1} \to \cdots \to F_1 \xrightarrow{\varphi_1} F_0 \to R/I \to 0$ of the R-module R/I. If R/I is artinian, non-Gorenstein and almost Gorenstein, then $\mathrm{I}_1(\varphi_d) = \mathfrak{m}$.*

Proof. Set $A = R/I$ and $E = \mathrm{E}_A(k)$. Then the sequence $(F_{d-1}/IF_{d-1})^* \xrightarrow{(\varphi_d \otimes A)^*} (F_d/IF_d)^* \to E \to 0$ gives a minimal A-free presentation of E, where $(-)^* = \mathrm{Hom}_A(-, A)$. Note that $\mathrm{rank}_A(F_d/IF_d)^* = r(A) = \mu(E)$. Lemma 6.8 implies $\mathrm{I}_1((\varphi_d \otimes A)^*) = \mathfrak{m}$, which shows $\mathrm{I}_1(\varphi_d) + I = \mathfrak{m}$. The desired result follows from Nakayama's lemma. □

We can show an artinian almost Gorenstein local ring of embedding dimension two is Burch.

Proposition 6.10. *Let $(R, \mathfrak{m})$ be a regular local ring of dimension 2 and I an ideal of R. Assume that R/I is a non-Gorenstein artinian almost Gorenstein ring. Then I is a Burch ideal of R.*

Proof. Take a minimal free resolution $0 \to F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \to R/I \to 0$ of the R-module R/I. It follows from Lemma 6.9 that $I_1(\varphi_2) = \mathfrak{m}$. Since R has dimension two, we can use the implication (2) ⇒ (1) in Theorem 6.2 to have that I is Burch. □

Remark 6.11. One may hope a non-Gorenstein nearly Gorenstein local ring is Burch, but this is not necessarily true. Indeed, let $(R, \mathfrak{m})$ be a 1-dimensional nearly Gorenstein local ring (e.g., $R = k[\![t^3, t^4, t^5]\!] \subseteq k[\![t]\!]$ with k a field). Take a regular element $x \in \mathfrak{m}^2$, and set $A = R/(x)$. Then A is nearly Gorenstein by [Herzog et al. 2019, Proposition 2.3(b)], but A is not a Burch ring by Corollary 7.9.

[2] There is another notion of an almost Gorenstein ring; see [Goto et al. 2015].

Next, we deal with local rings the cube of whose maximal ideal is zero. The following gives a characterization of Burchness for such rings.

Theorem 6.12. *Let $(R, \mathfrak{m}, k)$ be a local ring with $\mathfrak{m}^3 = 0$. Then R is a Burch ring if and only if there is an inequality $\beta_2(k) > (\operatorname{edim} R)^2 - r(R)$.*

Proof. Put $e = \operatorname{edim} R$ and $r = r(R)$. By Theorem 4.1, the ring R is Burch if and only if k is a direct summand of $\Omega^2 k$, if and only if $\operatorname{Soc} \Omega^2 k \not\subseteq \mathfrak{m}\Omega^2 k$. There is a short exact sequence $0 \to \Omega^2 k \to R^e \to \mathfrak{m} \to 0$, which gives an inclusion $\Omega^2 k \subseteq \mathfrak{m}R^e$ and an equality $\operatorname{Soc} \Omega^2 k = \operatorname{Soc} R^e$. Since $\mathfrak{m}^3 = 0$, we have an inclusion $\mathfrak{m}\Omega^2 k \subseteq \operatorname{Soc} \Omega^2 k$. Thus R is Burch if and only if $\ell(\operatorname{Soc} \Omega^2 k) > \ell(\mathfrak{m}\Omega^2 k)$. There are equalities

$$\begin{aligned}\beta_2(k) &= \ell(\Omega^2 k) - \ell(\mathfrak{m}\Omega^2 k) = \ell(R^e) - \ell(\mathfrak{m}) - \ell(\mathfrak{m}\Omega^2 k) = (e-1)\ell(\mathfrak{m}) + e - \ell(\mathfrak{m}\Omega^2 k)\\ &= (e-1)(e + \ell(\mathfrak{m}^2)) + e - \ell(\mathfrak{m}\Omega^2 k) = e^2 + (e-1)\ell(\mathfrak{m}^2) - \ell(\mathfrak{m}\Omega^2 k).\end{aligned}$$

On the other hand, there is an inclusion $\Omega^2 k \subseteq \mathfrak{m}^e$, which induces an inclusion $\mathfrak{m}\Omega^2 k \subseteq (\mathfrak{m}^2)^e$. Thus one has $\ell(\mathfrak{m}\Omega^2 k) \le e\ell(\mathfrak{m}^2) \le er = \ell(\operatorname{Soc} \Omega^2 k)$. If $\ell(\mathfrak{m}^2) < \ell(\operatorname{Soc} R) = r$, then we see that $\ell(\operatorname{Soc} \Omega^2 k) > \ell(\mathfrak{m}\Omega^2 k)$. The above equalities show that $\beta_2(k) \ge e^2 - \ell(\mathfrak{m}^2) > e^2 - r$. Therefore, we may assume $\ell(\mathfrak{m}^2) = r$. We obtain $\beta_2(k) = e^2 - r + er - \ell(\mathfrak{m}\Omega^2 k)$. It follows that $\beta_2 > e^2 - r$ if and only if $er - \ell(\mathfrak{m}\Omega^2 k) > 0$. The latter condition is equivalent to $\ell(\operatorname{Soc} \Omega^2 k) > \ell(\mathfrak{m}\Omega^2 k)$. □

Let R be a local ring with maximal ideal $\mathfrak{m}$. An element $x \in \mathfrak{m}$ is called a *Conca generator* of $\mathfrak{m}$ if $x^2 = 0$ and $\mathfrak{m}^2 = x\mathfrak{m}$. This notion has been introduced in [Avramov et al. 2008]. Note that the condition $\mathfrak{m}^3 = 0$ is necessary for R to possess a Conca generator.

Corollary 6.13. *Let $(R, \mathfrak{m}, k)$ be a local ring with $\mathfrak{m}^3 = 0$ and $\operatorname{Soc} R \subseteq \mathfrak{m}^2$. If R is a Burch ring, then R has no Conca generator.*

Proof. If R has a Conca generator, then the Poincaré series $P_k(t) = \sum \beta_i t^i$ is of the form $1/(1-et+rt^2)$ by [Avramov et al. 2008, Theorem 1.1]. In particular, $\beta_2(k) = e^2 - r$. Thus R is not Burch by Theorem 6.12. □

Next, we consider the Burchness of a fiber product. Let S, T be local rings having common residue field k. We say that the fiber product $S \times_k T$ is *nontrivial* if $S \ne k \ne T$. It holds that depth $S \times_k T = \min\{\operatorname{depth} S, \operatorname{depth} T, 1\}$; see [Lescot 1981, Remarque 3.3]. We compute some invariants.

Lemma 6.14. *Let $R = S \times_k T$ be a nontrivial fiber product, where $(S, \mathfrak{m}_S, k)$ and $(T, \mathfrak{m}_T, k)$ are local rings. Then the following equalities hold.*

(1) $\operatorname{edim} R = \operatorname{edim} S + \operatorname{edim} T$.

(2) $\dim_k \operatorname{Soc} R = \dim_k \operatorname{Soc} S + \dim_k \operatorname{Soc} T$.

(3) $\dim_k \mathrm{H}_1(\mathrm{K}^R) = \dim_k \mathrm{H}_1(\mathrm{K}^S) + \dim_k \mathrm{H}_1(\mathrm{K}^T) + \operatorname{edim} S \cdot \operatorname{edim} T$.

(4) $c_R = c_S + c_T + \operatorname{edim} S \cdot \operatorname{edim} T - \operatorname{edim}(S/\operatorname{Soc} S) \cdot \operatorname{edim}(T/\operatorname{Soc} T)$.

Proof. (1), (2) These equalities can be checked directly.

(3) One has $\beta_2^R(k) = \beta_2^S(k) + \beta_2^T(k) + 2 \operatorname{edim} S \cdot \operatorname{edim} T$ and $\dim_k \mathrm{H}_1(\mathrm{K}^R) = \beta_2^R(k) - \binom{\operatorname{edim} R}{2}$; see [Kostrikin and Shafarevich 1957; Bruns and Herzog 1998, Theorem 2.3.2] for example. Thus there are equalities

$$\begin{aligned}\dim_k \mathrm{H}_1(\mathrm{K}^R) &= \beta_2^R(k) - \tbinom{\operatorname{edim} R}{2} = \beta_2^S(k) + \beta_2^T(k) + 2 \operatorname{edim} S \cdot \operatorname{edim} T - \tbinom{\operatorname{edim} R}{2} \\ &= \dim_k \mathrm{H}_1(\mathrm{K}^S) - \tbinom{\operatorname{edim} S}{2} + \dim_k \mathrm{H}_1(\mathrm{K}^T) - \tbinom{\operatorname{edim} T}{2} + 2 \operatorname{edim} S \cdot \operatorname{edim} T - \tbinom{\operatorname{edim} R}{2} \\ &= \dim_k \mathrm{H}_1(\mathrm{K}^{R_1}) + \dim_k \mathrm{H}_1(\mathrm{K}^{R_2}) + \operatorname{edim} S \cdot \operatorname{edim} T.\end{aligned}$$

(4) Put $R' = R/\operatorname{Soc} R$, $S' = S/\operatorname{Soc} S$ and $T' = T/\operatorname{Soc} T$. Then $R' \cong S' \times T'$ unless $S = k$ or $T = k$. Using (1), (2) and (3), we can calculate c_R as follows:

$$\begin{aligned} c_R &= \dim_k \operatorname{Soc} R + \dim \mathrm{H}_1(\mathrm{K}^R) - \operatorname{edim} R - \dim \mathrm{H}_1(\mathrm{K}^{R'}) + \operatorname{edim} R' \\ &= \dim_k \operatorname{Soc} S + \dim_k \operatorname{Soc} T + \dim_k \mathrm{H}_1(\mathrm{K}^S) + \dim_k \mathrm{H}_1(\mathrm{K}^{R_2}) + \operatorname{edim} S \cdot \operatorname{edim} T \\ &\quad - \operatorname{edim} S - \operatorname{edim} T - \dim_k \mathrm{H}_1(\mathrm{K}^{S'}) - \dim_k \mathrm{H}_1(\mathrm{K}^{T'}) - \operatorname{edim} S' \cdot \operatorname{edim} T' + \operatorname{edim} S' + \operatorname{edim} T' \\ &= c_S + c_T + \operatorname{edim} S \cdot \operatorname{edim} T - \operatorname{edim} S' \cdot \operatorname{edim} T'. \end{aligned}$$ □

Using the above lemma, we can characterize the Burch fiber products.

Proposition 6.15. *Let $R = S \times_k T$ be a nontrivial fiber product, where $(S, \mathfrak{m}_S, k)$ and $(T, \mathfrak{m}_T, k)$ are local rings. Then R is a Burch ring if and only if*

(a) depth $R > 0$, *or* (b) depth $R = 0$ *and either S or T is a Burch ring of depth zero.*

Proof. First we deal with the case where depth $R = 0$. Lemma 2.11 shows that R is Burch if and only if $c_R > 0$. Note that the integers c_S, c_T and $N := \operatorname{edim} S \cdot \operatorname{edim} T - \operatorname{edim}(S/\operatorname{Soc} S) \cdot \operatorname{edim}(T/\operatorname{Soc} T)$ are always nonnegative. By Lemmas 6.14(4), the positivity of c_S or c_T implies that R is Burch. Conversely, assume that R is Burch. Then by Lemma 6.14(4) again, one of the three integers c_S, c_T, N is positive. If c_S or c_T is positive, then S or T is Burch. When $N > 0$, either $\operatorname{edim} S > \operatorname{edim} S/\operatorname{Soc} S$ or $\operatorname{edim} T > \operatorname{edim} T/\operatorname{Soc} T$ holds. Without loss of generality, we may assume that $\operatorname{edim} S > \operatorname{edim} S/\operatorname{Soc} S$. This inequality means that there is an element $x \in (\mathfrak{m}_S \cap \operatorname{Soc} S) \setminus \mathfrak{m}_S^2$. Then $\mathfrak{m}_S = I \oplus (x)$ for some ideal I. We see that $S \cong S/(x) \times_k S/I$ and $\operatorname{edim} S/I \leq 1$. Example 2.10 implies that S/I is Burch, and so is S.

Next, we consider the case where depth $R > 0$. In this case, we have depth $S > 0$, depth $T > 0$ and depth $R = 1$. Take regular elements $x \in \mathfrak{m}_S \setminus \mathfrak{m}_S^2$ and $y \in \mathfrak{m}_T \setminus \mathfrak{m}_T^2$. The element $x - y \in \mathfrak{m}_R = \mathfrak{m}_S \oplus \mathfrak{m}_T$ is also a regular element of R. The equalities $x\mathfrak{m}_R = x\mathfrak{m}_S = (x - y)\mathfrak{m}_S$ show that the image $\bar{x} \in R/(x - y)$ of x is in $\operatorname{Soc} R/(x - y)$. We have $\mathfrak{m}_R/(x - y) = (\bar{x}) \oplus I$ for some ideal I of $R/(x - y)$. Hence $R/(x - y)$ is isomorphic to the fiber product $U \times_k V$ of local rings over their common residue field k such that $\operatorname{edim} V \leq 1$. As V is Burch by Example 2.10, it follows that so is $R/(x - y)$, and hence so is R. □

Example 6.16. Let $R = k[x, y]/(x^a, xy, y^b)$ with k a field and $a, b \geq 1$. Then R is a Burch ring. In fact, R is isomorphic to the fiber product of $k[x]/(x^a)$ and $k[y]/(y^b)$ over k. By Example 2.10, the rings $k[x]/(x^a)$ and $k[y]/(y^b)$ are Burch, and so is R by Proposition 6.15.

7. Homological and categorical properties of Burch rings

In this section, we explore some homological and categorical aspects of Burch rings. They come in several flavors. We prove a classification theorem of subcategories over Burch rings. We also prove that non-Gorenstein Burch rings are G-regular in the sense of [Takahashi 2008], and that nontrivial consecutive vanishings of Tor over Burch rings cannot happen. We begin with recalling the definition of resolving subcategories.

Definition 7.1. Let R be a ring. A subcategory $\mathcal{X}$ of $\operatorname{mod} R$ is *resolving* if the following hold.

(1) The projective R-modules belong to $\mathcal{X}$.

(2) Let M be an R-module and N a direct summand of M. If M is in $\mathcal{X}$, then so is N.

(3) For an exact sequence $0 \to L \to M \to N \to 0$, if L and N are in $\mathcal{X}$, then so is M.

(4) For an exact sequence $0 \to L \to M \to N \to 0$, if M and N are in $\mathcal{X}$, then so is L.

Note that (1) can be replaced by the condition that $\mathcal{X}$ contains R. Also, (4) can be replaced by the condition that if M is an R-module in $\mathcal{X}$, then so is ΩM. For an R-module C, we denote by $\operatorname{res}_R C$ the *resolving closure* of C, the smallest resolving subcategory of $\operatorname{mod} R$ containing C.

We establish a couple of lemmas to prove Proposition 7.6. The first lemma is used as a base result of this section, which is essentially shown in [Takahashi 2009, Proposition 4.2]. For an R-module M we denote by $\operatorname{NF}(M)$ the *nonfree locus* of M, that is, the set of prime ideals $\mathfrak{p}$ of R such that $M_{\mathfrak{p}}$ is nonfree as an $R_{\mathfrak{p}}$-module.

Lemma 7.2. *Let $(R, \mathfrak{m})$ be a local ring, M a nonfree R-module, and x an element in $\mathfrak{m}$.*

(1) *There exists a short exact sequence $0 \to \Omega M \to M(x) \to M \to 0$ such that $x \in \mathrm{I}_1(M(x)) \subseteq \mathfrak{m}$ and $\operatorname{pd}_R M(x) \geq \operatorname{pd}_R M$. In particular, $M(x)$ belongs to $\operatorname{res}_R M$.*

(2) *For each $\mathfrak{p} \in \mathrm{V}(x) \cap \operatorname{NF}(M)$ one has $\mathrm{V}(\mathfrak{p}) \subseteq \operatorname{NF}(M(x)) \subseteq \operatorname{NF}(M)$ and $\mathrm{D}(x) \cap \operatorname{NF}(M(x)) = \varnothing$.*

Proof. (1) Let $\cdots \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\pi} M \to 0$ be a minimal free resolution of M. Taking the mapping cone of the multiplication map of the complex F by x, we get an exact sequence

$$\cdots \to F_3 \oplus F_2 \xrightarrow{\left(\begin{smallmatrix} d_3 & x \\ 0 & -d_2 \end{smallmatrix}\right)} F_2 \oplus F_1 \xrightarrow{\left(\begin{smallmatrix} d_2 & x \\ 0 & -d_1 \end{smallmatrix}\right)} F_1 \oplus F_0 \xrightarrow{\left(\begin{smallmatrix} d_1 & x \\ 0 & -\pi \end{smallmatrix}\right)} F_0 \oplus M \xrightarrow{(\pi\ x)} M \to 0.$$

Set $M(x) = \operatorname{Im}\left(\begin{smallmatrix} d_1 & x \\ 0 & -\pi \end{smallmatrix}\right) = \operatorname{Coker}\left(\begin{smallmatrix} d_2 & x \\ 0 & -d_1 \end{smallmatrix}\right)$. The free resolution of $M(x)$ given by truncating the above sequence is minimal. We see that $x \in \mathrm{I}_1(M(x)) \subseteq \mathfrak{m}$ as M is nonfree, and that $\operatorname{pd}_R M(x) \geq \operatorname{pd}_R M$. The following pullback diagram gives an exact sequence as in the assertion.

$$\begin{tikzcd}
0 \arrow[r] & \Omega M \arrow[r, "f"] & F_0 \arrow[r, "\pi"] & M \arrow[r] & 0 \\
0 \arrow[r] & \Omega M \arrow[r] \arrow[u, equal] & M(x) \arrow[r] \arrow[u] & M \arrow[r] \arrow[u, "x"'] & 0
\end{tikzcd}$$

(2) The module $M(x)$ fits into the pushout diagram

$$\begin{tikzcd}
0 \arrow[r] & \Omega M \arrow[r, "f"] \arrow[d, "x"] & F_0 \arrow[r, "\pi"] \arrow[d] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \Omega M \arrow[r] & M(x) \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

Using the same argument as in the proof of [Takahashi 2009, Proposition 4.2], we observe that $\mathrm{V}(\mathfrak{p}) \subseteq \mathrm{NF}(M(x)) \subseteq \mathrm{NF}(M)$ and $\mathrm{D}(x) \cap \mathrm{NF}(M(x)) = \varnothing$ hold. □

Lemma 7.3. *Let* $(R, \mathfrak{m})$ *be a local ring and* M *an* R*-module. Let* $W \subseteq \mathrm{NF}(M)$ *be a closed subset of* $\operatorname{Spec} R$*. Then there exists an* R*-module* X *such that* $\mathrm{pd}_R X \geq \mathrm{pd}_R M$ *and* $\mathrm{NF}(X) = W$*.*

Proof. The assertion follows from the proof of [Takahashi 2009, Theorem 4.3] by replacing [Takahashi 2009, Lemma 4.2] used there with our Lemma 7.2. □

Lemma 7.4. *Let* $(R, \mathfrak{m})$ *be a local ring and* M *a nonfree* R*-module. Then there is an exact sequence* $0 \to (\Omega M)^n \to N \to M^n \to 0$ *with* $n \geq 1$, $\mathrm{I}_1(N) = \mathfrak{m}$ *and* $\mathrm{pd}_R N \geq \mathrm{pd}_R M$*. In particular,* $N \in \mathrm{res}_R M$*.*

Proof. Let $x_1, \dots, x_n$ be a minimal system of generators of $\mathfrak{m}$. According to Lemma 7.2, for each i there exists an exact sequence $0 \to \Omega M \to M(x_i) \to M \to 0$ such that $x_i \in \mathrm{I}_1(M(x_i)) \subseteq \mathfrak{m}$ and $\mathrm{pd}_R M(x_i) \geq \mathrm{pd}_R M$. Putting $N = \bigoplus_{i=1}^n M(x_i)$, we obtain an exact sequence $0 \to (\Omega M)^n \to N \to M^n \to 0$ with $\mathrm{I}_1(N) = \sum_{i=1}^n \mathrm{I}_1(M(x_i)) = \mathfrak{m}$ and $\mathrm{pd}_R N \geq \mathrm{pd}_R M$. □

Lemma 7.5. *Let* R *be a local ring. Let* M *be an* R*-module that is locally free on the punctured spectrum of* R*.*

(1) *For every* $X \in \mathrm{res}_{\widehat{R}} \widehat{M}$ *there exists* $Y \in \mathrm{res}_R M$ *such that* X *is a direct summand of* $\widehat{Y}$*.*

(2) *Let* N *be an* R*-module. If* $\widehat{N} \in \mathrm{res}_{\widehat{R}} \widehat{M}$*, then* $N \in \mathrm{res}_R M$*.*

Proof. (1) Let $\mathcal{C}$ be the subcategory of $\operatorname{mod} \widehat{R}$ consisting of direct summands of the completions of modules in $\mathrm{res}_R M$. We claim that $\mathcal{C}$ is a resolving subcategory of $\operatorname{mod} \widehat{R}$ containing $\widehat{M}$. Indeed, since R, M are in $\mathrm{res}_R M$, the completions $\widehat{R}, \widehat{M}$ are in $\mathcal{C}$. For each $E \in \mathcal{C}$, there exists $D \in \mathrm{res}_R M$ such that E is a direct summand of $\widehat{D}$. The module $\Omega_{\widehat{R}} E$ is a direct summand of $\Omega_{\widehat{R}} \widehat{D} = \widehat{\Omega_R D}$. As $\Omega_R D \in \mathrm{res}_R M$, we have $\Omega_R E \in \mathcal{C}$. Let $0 \to A \to B \to C \to 0$ be an exact sequence of $\widehat{R}$-modules with $A, C \in \mathcal{C}$. Then A, C are direct summands of $\widehat{V}, \widehat{W}$ for some $V, W \in \mathrm{res}_R M$, respectively. Writing $A \oplus A' = \widehat{V}$ and $C \oplus C' = \widehat{W}$, we get an exact sequence $\sigma : 0 \to \widehat{V} \to B' \to \widehat{W} \to 0$, where $B' = A' \oplus B \oplus C'$. The exact sequence σ corresponds to an element of $\mathrm{Ext}^1_{\widehat{R}}(\widehat{W}, \widehat{V}) = \widehat{\mathrm{Ext}^1_R(W, V)}$. Since M is locally free on the punctured spectrum of R, so are V and W. Hence $\mathrm{Ext}^1_R(W, V)$ has finite length as an R-module, and is complete. This implies that there exists an exact sequence $\tau : 0 \to V \to U \to W \to 0$ of R-modules such that $\widehat{\tau} \cong \sigma$. Therefore U is in $\mathrm{res}_R M$ and B' is isomorphic to $\widehat{U}$. Thus B belongs to $\mathcal{C}$, and the claim follows. The claim shows that $\mathcal{C}$ contains $\mathrm{res}_{\widehat{R}} \widehat{M}$. Hence X is in $\mathcal{C}$, which shows the assertion.

(2) By (1) there is an R-module $Y \in \operatorname{res}_R M$ such that $\widehat{N}$ is a direct summand of $\widehat{Y}$. Thanks to [Leuschke and Wiegand 2012, Corollary 1.15(i)], the module N is a direct summand of Y. Hence N belongs to $\operatorname{res}_R M$. □

Now we can show the proposition below, which yields a significant property of Burch rings. This is also used in the proofs of Theorems 7.7 and 7.10.

Proposition 7.6. *Let R be a Burch local ring of depth t with residue field k. Let M be an R-module of infinite projective dimension. Then $\Omega^t k$ belongs to* $\operatorname{res}_R M$.

Proof. We begin with proving the proposition when R is complete and $t = 0$. As M has infinite projective dimension, Lemma 7.4 gives rise to an R-module $N \in \operatorname{res}_R M$ with $\mathrm{I}_1(N) = \mathfrak{m}$. Proposition 4.2 implies that k is a direct summand of $\Omega_R^2 N$. As $\Omega_R^2 N$ is in $\operatorname{res}_R M$, so is k.

Now, let us consider the case where R is complete and $t > 0$. By definition, there is a maximal regular sequence $\boldsymbol{x}$ of R such that $R/(\boldsymbol{x})$ is a Burch ring of depth 0. Note that $\Omega^t M \in \operatorname{res}_R M$. For all $i > 0$ we have $\operatorname{Tor}_i^R(\Omega^t M, R/(\boldsymbol{x})) = \operatorname{Tor}_{i+t}^R(M, R/(\boldsymbol{x})) = 0$, which says that $\boldsymbol{x}$ is a regular sequence on $\Omega^t M$. The $R/(\boldsymbol{x})$-module $\Omega^t M/\boldsymbol{x}\Omega^t M$ has infinite projective dimension by [Bruns and Herzog 1998, Lemma 1.3.5]. The case $t = 0$ implies that k belongs to $\operatorname{res}_{R/(\boldsymbol{x})} \Omega^t M/\boldsymbol{x}\Omega^t M$. It follows from [Takahashi 2010, Lemma 5.8] that $\Omega_R^t k \in \operatorname{res}_R \Omega^t M \subseteq \operatorname{res}_R M$.

Finally, we consider the case where R is not complete. Lemma 7.3 gives an R-module $X \in \operatorname{res}_R M$ with $\operatorname{pd}_R X = \infty$ and $\operatorname{NF}(X) = \{\mathfrak{m}\}$. As $\widehat{R}$ is Burch and $\operatorname{pd}_{\widehat{R}} \widehat{X} = \operatorname{pd}_R X = \infty$, the above argument yields $\Omega_{\widehat{R}}^t k \in \operatorname{res}_{\widehat{R}} \widehat{X}$. Using Lemma 7.5, we see $\Omega^t k \in \operatorname{res}_R X$, and $\Omega^t k \in \operatorname{res}_R M$. □

Non-Gorenstein Burch rings admit only trivial totally reflexive modules. Recall that a local ring R is called *G-regular* if every totally reflexive R-module is free.

Theorem 7.7. *Let R be a non-Gorenstein Burch local ring. Then R is G-regular.*

Proof. By taking the completion and using [Takahashi 2008, Corollary 4.7], we may assume that R is complete. Let $\mathcal{G}$ be the category of totally reflexive R-modules. Then $\mathcal{G}$ is a resolving subcategory of $\operatorname{mod} R$ by [Christensen 2000, (1.1.10) and (1.1.11)]. If R is not G-regular, that is, there is a nonfree R-module M in $\mathcal{G}$, then Proposition 7.6 shows that $\mathcal{G}$ contains the R-module $\Omega^d k$, where $d = \dim R$. In other words, $\Omega^d k$ is totally reflexive. This especially says that the R-module k has finite G-dimension, and R is Gorenstein; see [Christensen 2000, (1.4.9)]. This contradiction shows that R is G-regular. □

Remark 7.8. The converse of Theorem 7.7 does not necessarily hold. In fact, the nontrivial fiber product $R = S \times_k T$ of non-Burch local rings S, T is non-Burch. However, thanks to [Nasseh and Takahashi 2020, Lemma 4.4], the same argument of the proof of Theorem 7.7 works, and hence R is G-regular.

As a corollary of Theorem 7.7, "embedded deformations" of Burch rings are never Burch.

Corollary 7.9. *Let $(R, \mathfrak{m})$ be a singular local ring. Let $x \in \mathfrak{m}^2$ be an R-regular element. Then the local ring $R/(x)$ is not Burch.*

Proof. The proof of [Takahashi 2008, Proposition 4.6] gives rise to an endomorphism $\delta : R^n \to R^n$ such that $\delta^2 = x \cdot \mathrm{id}_{R^n}$ and $\operatorname{Im} \delta \subseteq \mathfrak{m} R^n$. It is easy to see that δ is injective, and we have an exact sequence $0 \to R^n \xrightarrow{\delta} R^n \to C \to 0$ with $xC = 0$. This induces an exact sequence $\cdots \xrightarrow{\bar{\delta}} (R/(x))^n \xrightarrow{\bar{\delta}} (R/(x))^n \xrightarrow{\bar{\delta}} (R/(x))^n \xrightarrow{\bar{\delta}} \cdots$ of $R/(x)$-modules whose $R/(x)$-dual is exact as well. Since $\operatorname{Im} \bar{\delta} = C$, the $R/(x)$-module C is totally reflexive. As $\operatorname{Im} \delta \subseteq \mathfrak{m}R^n$, we see that C is not $R/(x)$-free. Hence $R/(x)$ is not G-regular.

Suppose that $R/(x)$ is Burch. Then Theorem 7.7 implies that $R/(x)$ is Gorenstein. By Proposition 5.1, the ring $R/(x)$ is a hypersurface. We have

$$1 \geq \operatorname{codepth} R/(x) = \operatorname{edim} R/(x) - \operatorname{depth} R/(x) = \operatorname{edim} R - (\dim R - 1) = \operatorname{codim} R + 1,$$

where the second equality follows from the assumption that x is not in $\mathfrak{m}^2$. We get $\operatorname{codim} R = 0$, which means that R is regular, contrary to our assumption. □

Let $(R, \mathfrak{m})$ be a local ring. We denote by $\operatorname{Spec}^0 R$ the punctured spectrum of R. For a property $\mathbb{P}$, we say that $\operatorname{Spec}^0 R$ *satisfies* $\mathbb{P}$ if $R_\mathfrak{p}$ satisfies $\mathbb{P}$ for all $\mathfrak{p} \in \operatorname{Spec}^0 R$. We denote by $\mathrm{CM}(R)$ the subcategory of $\operatorname{mod} R$ consisting of maximal Cohen–Macaulay modules. Also, $\mathrm{D^b}(R)$ stands for the bounded derived category of $\operatorname{mod} R$, and $\mathrm{D_{sg}}(R)$ the *singularity category* of R, that is, the Verdier quotient of $\mathrm{D^b}(R)$ by perfect complexes. Note that $\mathrm{D^b}(R)$ and $\mathrm{D_{sg}}(R)$ have the structure of a triangulated category. A *thick* subcategory of a triangulated category is by definition a triangulated subcategory closed under direct summands. The following theorem gives rise to classifications of several kinds of subcategories over Burch rings; recall that a Cohen–Macaulay local ring R is said to have *finite Cohen–Macaulay representation type* if there exist only finitely many isomorphism classes of indecomposable maximal Cohen–Macaulay R-modules. For the unexplained notations and terminologies appearing in the theorem, we refer to [Nasseh and Takahashi 2020, §2].

Theorem 7.10. *Let $(R, \mathfrak{m})$ be a singular Cohen–Macaulay Burch local ring.*

(1) *Suppose that $\operatorname{Spec}^0 R$ is either a hypersurface or has minimal multiplicity. Then there is a commutative diagram of mutually inverse bijections*:

$$\begin{tikzcd}
\left\{\begin{matrix}\textit{resolving subcategories of}\\ \operatorname{mod} R \textit{ contained in } \mathrm{CM}(R)\end{matrix}\right\} \arrow[r, shift left, "\mathrm{NF}"] \arrow[d, equal] & \left\{\begin{matrix}\textit{specialization-closed}\\ \textit{subsets of } \operatorname{Sing} R\end{matrix}\right\} \arrow[l, shift left, "\mathrm{NF}_{\mathrm{CM}}^{-1}"] \arrow[d, shift left, "\mathrm{IPD}^{-1}"] \\
\left\{\begin{matrix}\textit{thick subcategories of}\\ \mathrm{CM}(R) \textit{ containing } R\end{matrix}\right\} \arrow[r, shift left, "\mathrm{thick}_{\operatorname{mod} R}"] \arrow[d, shift left, "\mathrm{thick}_{\mathrm{D_{sg}}(R)}"] & \left\{\begin{matrix}\textit{thick subcategories of}\\ \operatorname{mod} R \textit{ containing } R\end{matrix}\right\} \arrow[l, shift left, "\mathrm{rest}_{\mathrm{CM}(R)}"] \arrow[u, shift left, "\mathrm{IPD}"] \arrow[d, shift left, "\mathrm{thick}_{\mathrm{D^b}(R)}"] \\
\left\{\begin{matrix}\textit{thick subcategories of}\\ \mathrm{D_{sg}}(R)\end{matrix}\right\} \arrow[r, shift left, "\pi^{-1}"] \arrow[u, shift left, "\mathrm{rest}_{\mathrm{CM}(R)}"] & \left\{\begin{matrix}\textit{thick subcategories of}\\ \mathrm{D^b}(R) \textit{ containing } R\end{matrix}\right\} \arrow[l, shift left, "\pi"] \arrow[u, shift left, "\mathrm{rest}_{\operatorname{mod} R}"]
\end{tikzcd}$$

(2) *Assume that R is excellent and admits a canonical module ω. Suppose that* $\operatorname{Spec}^0 R$ *has finite Cohen–Macaulay representation type. Then there is a commutative diagram of mutually inverse bijections*:

$$\begin{tikzcd}
\begin{Bmatrix}\textit{resolving subcategories}\\ \textit{of } \operatorname{mod} R \textit{ contained in}\\ \operatorname{CM}(R) \textit{ and containing } \omega\end{Bmatrix} \arrow[r, shift left, "\mathrm{NF}"] \arrow[d, equal] & \begin{Bmatrix}\textit{specialization-closed}\\ \textit{subsets of } \operatorname{Sing} R\\ \textit{containing } \operatorname{NG} R\end{Bmatrix} \arrow[l, shift left, "\mathrm{NF}_{\mathrm{CM}}^{-1}"] \arrow[d, shift left, "\mathrm{IPD}^{-1}"] \\
\begin{Bmatrix}\textit{thick subcategories of}\\ \operatorname{CM}(R) \textit{ containing}\\ R \textit{ and } \omega\end{Bmatrix} \arrow[r, shift left, "\mathrm{thick}_{\operatorname{mod} R}"] \arrow[d, shift left, "\mathrm{thick}_{\mathrm{D_{sg}}(R)}"] & \begin{Bmatrix}\textit{thick subcategories of}\\ \operatorname{mod} R \textit{ containing}\\ R \textit{ and } \omega\end{Bmatrix} \arrow[l, shift left, "\mathrm{rest}_{\operatorname{CM}(R)}"] \arrow[u, shift left, "\mathrm{IPD}"] \arrow[d, shift left, "\mathrm{thick}_{\mathrm{D^b}(R)}"] \\
\begin{Bmatrix}\textit{thick subcategories of}\\ \mathrm{D_{sg}}(R) \textit{ containing } \omega\end{Bmatrix} \arrow[r, shift left, "\pi^{-1}"] \arrow[u, shift left, "\mathrm{rest}_{\operatorname{CM}(R)}"] & \begin{Bmatrix}\textit{thick subcategories of}\\ \mathrm{D^b}(R) \textit{ containing}\\ R \textit{ and } \omega\end{Bmatrix} \arrow[l, shift left, "\pi"] \arrow[u, shift left, "\mathrm{rest}_{\operatorname{mod} R}"]
\end{tikzcd}$$

Proof. The proof of [Nasseh and Takahashi 2020, Theorem 4.5] uses [Nasseh and Takahashi 2020, Lemma 4.4]. Replace this lemma with our Proposition 7.6. Then the same argument works, and the theorem follows. □

Example 7.11. We have the following list of examples of non-Gorenstein Cohen–Macaulay local rings not having isolated singularities, where ∘ and × mean "Yes" and "No" respectively.

Example no. of [Takahashi 2013]	R	$\dim R$	Burch	$\operatorname{Spec}^0 R$		
				hypersurface	min. mult.	finite CM rep. type
7.1	$\dfrac{k[\![x,y,z]\!]}{(x^2,xz,yz)}$	1	∘	∘	∘	∘
7.2	$\dfrac{k[\![x,y,z]\!]}{(x^2,xy,y^2)}$	1	∘	×	∘	×
7.3	$\dfrac{k[\![x,y,z]\!]}{(xy,z^2,zw,w^3)}$	1	×	×	∘	×
7.4	$\dfrac{k[\![x,y,z]\!]}{(x^2-yz,xy,y^2)}$	1	∘	∘	×	∘
7.5	$\dfrac{k[\![x,y,z,w]\!]}{(xy,xz,yz)}$	2	∘	×	∘	∘

The assertions are shown in [Takahashi 2013, Examples 7.1–7.5], except those on the Burch property. As to the first, second, fourth and fifth rings R are Burch since the quotient of a system of parameters is isomorphic to $k[x, y]/(x^2, xy, y^2)$, which is an artinian Burch ring by Example 6.16. As for the third ring R, note that (x, y) is an exact pair of zerodivisors. Hence it is not G-regular, and not Burch by Theorem 7.7.

Now we discuss the vanishing of Tor modules over Burch rings. The following result is a simple consequence of Lemmas 2.11 and 7.4.

Proposition 7.12. *Let $(R, \mathfrak{m}, k)$ be a Burch ring of depth zero, and M, N be R-modules. If $\operatorname{Tor}_l^R(M, N) = \operatorname{Tor}_{l+1}^R(M, N) = 0$ for some $l \geq 3$, then either M or N is a free R-module.*

Proof. We may assume that R is complete. Assume that M is nonfree. Since depth $R = 0$, the R-module M has infinite projective dimension. By Lemma 7.4, there is a short exact sequence $0 \to (\Omega M)^n \to X \to M^n \to 0$, where X satisfies $\mathrm{I}_1(X) = \mathfrak{m}$. It induces an exact sequence $0 \to (\Omega^3 M)^n \to \Omega^2 X \oplus F \to (\Omega^2 M)^n \to 0$ with F free. We also have $\operatorname{Tor}_{l-2}(\Omega^2 M, N) = \operatorname{Tor}_{l-2}(\Omega^3 M, N) = 0$, which implies that $\operatorname{Tor}_{l-2}(\Omega^2 X, N) = 0$. Proposition 4.2 implies that k is a direct summand of $\Omega^2 X$, as R is Burch. We see that $\operatorname{Tor}_{l-2}(k, N)$ vanishes. This shows that N has finite projective dimension, and so it is R-free. □

We can prove the following by applying a similar argument as in the proof of [Nasseh and Takahashi 2020, Corollary 6.5], where we use Proposition 7.12 instead of [Nasseh and Takahashi 2020, Corollary 6.2].

Corollary 7.13. *Let $(R, \mathfrak{m}, k)$ be a Burch ring of depth t. Let M, N be R-modules. Assume that there exists an integer $l \geq \max\{3, t+1\}$ such that $\operatorname{Tor}_i^R(M, N) = 0$ for all $l + t \leq i \leq l + 2t + 1$. Then either M or N has finite projective dimension.*

Remark 7.14. Using an analogous argument as in the proof of [Nasseh and Takahashi 2020, Corollary 6.6], one can also prove a variant of Corollary 7.13 regarding Ext modules.

We state a remark on the ascent of Burchness along a flat local homomorphism.

Remark 7.15. Let $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a flat local homomorphism of local rings. Even if the rings R and $S/\mathfrak{m}S$ are Burch, S is not necessarily Burch. In fact, consider the natural injection

$$\phi : R = k[x, y]/(x^2, xy, y^2) \hookrightarrow k[x, y, t]/(x^2, xy, y^2, t^2) = S.$$

Then ϕ is a flat local homomorphism. The artinian local rings R and $S/\mathfrak{m}S = k[t]/(t^2)$ are Burch by Examples 6.16 and 2.2(1). The ring S is not G-regular since (t, t) is an exact pair of zerodivisors of S. Theorem 7.7 implies that S is not Burch.

In the case when the closed fiber is regular, the ascent of Burchness along a flat local homomorphism holds.

Remark 7.16. Let $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a flat local homomorphism of local rings. If R is Burch and $S/\mathfrak{m}$ is regular, then S is Burch.

Proof. To prove this, we may take the completions, and assume that R (resp. S) is complete with respect to $\mathfrak{m}$-adic (resp. n-adic) topology. Then we get a regular sequence $\boldsymbol{x}$ of R such that $R/(\boldsymbol{x})$ is a Burch ring of depth zero. By the flatness of S over R, $\boldsymbol{x}$ is also regular on S, and so it is enough to show that $S/(\boldsymbol{x})$ is Burch. Thus we can replace the flat local homomorphism $R \to S$ by $R/(\boldsymbol{x}) \to S/(\boldsymbol{x})$, and assume that R is of depth zero. Let $\boldsymbol{y}$ be a sequence of elements in S which forms a regular system of parameters of $S/\mathfrak{m}S$. Then $\boldsymbol{y}$ is regular on S and $S/(\boldsymbol{y})$ is flat over R (see [Bruns and Herzog 1998, Lemma 1.2.17] for instance). Therefore replacing $R \to S$ by the composition $R \to S \to S/(\boldsymbol{y})$, we may assume that $\mathfrak{m} = \mathfrak{n}$. Thanks to Theorem 4.1, it follows that $R/\mathfrak{m}$ is a direct summand of $\Omega^2_R R/\mathfrak{m}$. Tensoring with S over R, we obtain that $S/\mathfrak{m}S$ (which is equal to $S/\mathfrak{n}$) is a direct summand of $(\Omega^2_R R/\mathfrak{m}) \otimes_R S$. By the flatness of S over R again, $(\Omega^2_R R/\mathfrak{m}) \otimes_R S$ is isomorphic to $\Omega^2_S S/\mathfrak{n}$. Hence $S/\mathfrak{n}$ is isomorphic to a direct summand of $\Omega^2_S S/\mathfrak{n}$, and Theorem 4.1 yields that S is Burch. □

A localization of a Burch ring at a prime ideal may not be Burch. Indeed, we have an example below.

Example 7.17. Let $R = k[\![x, y, z, w]\!]/(x^2, y^2, xw, yw, zw)$ and $\mathfrak{p}$ be the minimal prime ideal (x, y, w) of R. Then R is a local ring of depth zero and isomorphic to the fiber product of $k[\![x, y, z]\!]/(x^2, y^2)$ and $k[\![w]\!]$ over k. Therefore R is Burch by Proposition 6.15. On the other hand, the localization $R_\mathfrak{p}$ of R at $\mathfrak{p}$ is isomorphic to $k((z))[\![x, y]\!]/(x^2, y^2)$, which is a complete intersection of codimension two. Thus $R_\mathfrak{p}$ is not Burch by Proposition 5.1.

Acknowledgments

Most of this work was done during Kobayashi's visit to the University of Kansas in 2018–2019. He is grateful to the Department of Mathematics for their hospitality. We thank Professors Rodney Sharp and Edmund Robertson for providing useful biographical data on Professor Burch. We also thank Professors Craig Huneke and Shinya Kumashiro for helpful comments. Dao was partly supported by Simons Collaboration Grant FND0077558. Kobayashi was partly supported by JSPS Grant-in-Aid for JSPS Fellows 18J20660. Takahashi was partly supported by JSPS Grant-in-Aid for Scientific Research 16K05098, 19K03443 and JSPS Fund for the Promotion of Joint International Research 16KK0099. Finally, the authors thank the referees for reading the paper carefully and giving useful comments and helpful suggestions.

References

[Avramov 1996] L. L. Avramov, "Modules with extremal resolutions", *Math. Res. Lett.* **3**:3 (1996), 319–328. MR Zbl

[Avramov 1998] L. L. Avramov, "Infinite free resolutions", pp. 1–118 in *Six lectures on commutative algebra* (Bellaterra, Spain, 1996), edited by J. M. Giral et al., Progr. Math. **166**, Birkhäuser, 1998. MR Zbl

[Avramov 2012] L. L. Avramov, "A cohomological study of local rings of embedding codepth 3", *J. Pure Appl. Algebra* **216**:11 (2012), 2489–2506. MR Zbl

[Avramov et al. 2008] L. L. Avramov, S. B. Iyengar, and L. M. Şega, "Free resolutions over short local rings", *J. Lond. Math. Soc.* (2) **78**:2 (2008), 459–476. MR Zbl

[Bonacho Dos Anjos Henriques and Şega 2011] I. Bonacho Dos Anjos Henriques and L. M. Şega, "Free resolutions over short Gorenstein local rings", *Math. Z.* **267**:3-4 (2011), 645–663. MR Zbl

[Bruns and Herzog 1998] W. Bruns and J. Herzog, *Cohen–Macaulay rings*, 2nd ed., Cambridge Stud. Adv. Math. **39**, Cambridge Univ. Press, 1998. Zbl

[Burch 1968a] L. Burch, "A note on the homology of ideals generated by three elements in local rings", *Proc. Cambridge Philos. Soc.* **64** (1968), 949–952. MR Zbl

[Burch 1968b] L. Burch, "On ideals of finite homological dimension in local rings", *Proc. Cambridge Philos. Soc.* **64** (1968), 941–948. MR Zbl

[Burch 1972] L. Burch, "Codimension and analytic spread", *Proc. Cambridge Philos. Soc.* **72** (1972), 369–373. MR Zbl

[Celikbas et al. 2018] O. Celikbas, K.-i. Iima, A. Sadeghi, and R. Takahashi, "On the ideal case of a conjecture of Auslander and Reiten", *Bull. Sci. Math.* **142** (2018), 94–107. MR Zbl

[Choi 1992] S. Choi, "Exponential growth of Betti numbers", *J. Algebra* **152**:1 (1992), 20–29. MR Zbl

[Christensen 2000] L. W. Christensen, *Gorenstein dimensions*, Lecture Notes in Math. **1747**, Springer, 2000. MR Zbl

[Conca et al. 2010] A. Conca, E. De Negri, and M. E. Rossi, "Integrally closed and componentwise linear ideals", *Math. Z.* **265**:3 (2010), 715–734. MR Zbl

[Corso et al. 1998] A. Corso, C. Huneke, and W. V. Vasconcelos, "On the integral closure of ideals", *Manuscripta Math.* **95**:3 (1998), 331–347. MR Zbl

[Corso et al. 2006] A. Corso, C. Huneke, D. Katz, and W. V. Vasconcelos, "Integral closure of ideals and annihilators of homology", pp. 33–48 in *Commutative algebra*, edited by A. Corso et al., Lect. Notes Pure Appl. Math. **244**, Chapman & Hall, Boca Raton, FL, 2006. MR Zbl

[Corso et al. 2018] A. Corso, S. Goto, C. Huneke, C. Polini, and B. Ulrich, "Iterated socles and integral dependence in regular rings", *Trans. Amer. Math. Soc.* **370**:1 (2018), 53–72. MR Zbl

[Dao and Schweig 2019] H. Dao and J. Schweig, "The type defect of a simplicial complex", *J. Combin. Theory Ser. A* **163** (2019), 195–210. MR Zbl

[De Stefani 2016] A. De Stefani, "Products of ideals may not be Golod", *J. Pure Appl. Algebra* **220**:6 (2016), 2289–2306. MR Zbl

[Dutta 1989] S. P. Dutta, "Syzygies and homological conjectures", pp. 139–156 in *Commutative algebra* (Berkeley, 1987), edited by M. Hochster et al., Math. Sci. Res. Inst. Publ. **15**, Springer, 1989. MR Zbl

[Goto 1987] S. Goto, "Integral closedness of complete-intersection ideals", *J. Algebra* **108**:1 (1987), 151–160. MR Zbl

[Goto and Hayasaka 2002] S. Goto and F. Hayasaka, "Finite homological dimension and primes associated to integrally closed ideals", *Proc. Amer. Math. Soc.* **130**:11 (2002), 3159–3164. MR Zbl

[Goto et al. 2015] S. Goto, R. Takahashi, and N. Taniguchi, "Almost Gorenstein rings: towards a theory of higher dimension", *J. Pure Appl. Algebra* **219**:7 (2015), 2666–2712. MR Zbl

[Heinzer et al. 2002] W. J. Heinzer, L. J. Ratliff, Jr., and D. E. Rush, "Basically full ideals in local rings", *J. Algebra* **250**:1 (2002), 371–396. MR Zbl

[Herzog et al. 1983] J. Herzog, A. Simis, and W. V. Vasconcelos, "Approximation complexes of blowing-up rings, II", *J. Algebra* **82**:1 (1983), 53–83. MR Zbl

[Herzog et al. 2019] J. Herzog, T. Hibi, and D. I. Stamate, "The trace of the canonical module", *Israel J. Math.* **233**:1 (2019), 133–165. MR Zbl

[Hong et al. 2009] J. Hong, H. Lee, S. Noh, and D. E. Rush, "Full ideals", *Comm. Algebra* **37**:8 (2009), 2627–2639. MR Zbl

[Huneke and Vraciu 2006] C. Huneke and A. Vraciu, "Rings that are almost Gorenstein", *Pacific J. Math.* **225**:1 (2006), 85–102. MR Zbl

[Kobayashi and Takahashi 2019] T. Kobayashi and R. Takahashi, "Rings whose ideals are isomorphic to trace ideals", *Math. Nachr.* **292**:10 (2019), 2252–2261. MR Zbl

[Kostrikin and Shafarevich 1957] A. I. Kostrikin and I. R. Shafarevich, "Groups of homologies of nilpotent algebras", *Dokl. Akad. Nauk SSSR* (*N.S.*) **115**:6 (1957), 1066–1069. In Russian. MR

[Kustin and Vraciu 2018] A. R. Kustin and A. Vraciu, "Totally reflexive modules over rings that are close to Gorenstein", *J. Algebra* (online publication September 2018).

[Lescot 1981] J. Lescot, “La série de Bass d’un produit fibré d’anneaux locaux”, *C. R. Acad. Sci. Paris Sér. I Math.* **293**:12 (1981), 569–571. MR Zbl

[Leuschke and Wiegand 2012] G. J. Leuschke and R. Wiegand, *Cohen–Macaulay representations*, Math. Surv. Monogr. **181**, Amer. Math. Soc., Providence, RI, 2012. MR Zbl

[Lipman 1971] J. Lipman, “Stable ideals and Arf rings”, *Amer. J. Math.* **93**:3 (1971), 649–685. MR Zbl

[Nasseh and Takahashi 2020] S. Nasseh and R. Takahashi, “Local rings with quasi-decomposable maximal ideal”, *Math. Proc. Cambridge Philos. Soc.* **168**:2 (2020), 305–322. MR Zbl

[Ogoma 1984] T. Ogoma, “Existence of dualizing complexes”, *J. Math. Kyoto Univ.* **24**:1 (1984), 27–48. MR Zbl

[Rush 2013] D. E. Rush, “Contracted, $\mathfrak{m}$-full and related classes of ideals in local rings”, *Glasg. Math. J.* **55**:3 (2013), 669–675. MR Zbl

[Striuli and Vraciu 2011] J. Striuli and A. Vraciu, “Some homological properties of almost Gorenstein rings”, pp. 201–215 in *Commutative algebra and its connections to geometry*, edited by A. Corso and C. Polini, Contemp. Math. **555**, Amer. Math. Soc., Providence, RI, 2011. MR Zbl

[Takahashi 2008] R. Takahashi, “On G-regular local rings”, *Comm. Algebra* **36**:12 (2008), 4472–4491. MR Zbl

[Takahashi 2009] R. Takahashi, “Modules in resolving subcategories which are free on the punctured spectrum”, *Pacific J. Math.* **241**:2 (2009), 347–367. MR Zbl

[Takahashi 2010] R. Takahashi, “Classifying thick subcategories of the stable category of Cohen–Macaulay modules”, *Adv. Math.* **225**:4 (2010), 2076–2116. MR Zbl

[Takahashi 2013] R. Takahashi, “Classifying resolving subcategories over a Cohen–Macaulay local ring”, *Math. Z.* **273**:1-2 (2013), 569–587. MR Zbl

[Watanabe 1987] J. Watanabe, “$\mathfrak{m}$-full ideals”, *Nagoya Math. J.* **106** (1987), 101–111. MR Zbl

[Watanabe 1991] J. Watanabe, “The syzygies of $\mathfrak{m}$-full ideals”, *Math. Proc. Cambridge Philos. Soc.* **109**:1 (1991), 7–13. MR Zbl

[Yoshino 1990] Y. Yoshino, *Cohen–Macaulay modules over Cohen–Macaulay rings*, Lond. Math. Soc. Lect. Note Ser. **146**, Cambridge Univ. Press, 1990. MR Zbl

Communicated by Keiichi Watanabe
Received 2019-06-12 Revised 2019-11-23 Accepted 2020-03-05

hdao@ku.edu *Department of Mathematics, University of Kansas, Lawrence, KS, United States*

m16021z@math.nagoya-u.ac.jp *Graduate School of Mathematics, Nagoya University, Nagoya, Japan*

takahashi@math.nagoya-u.ac.jp *Graduate School of Mathematics, Nagoya University, Nagoya, Japan*
Department of Mathematics, University of Kansas, Lawrence, KS, United States

ALGEBRA AND NUMBER THEORY 14:8 (2020)
https://doi.org/10.2140/ant.2020.14.2151

Sous-groupe de Brauer invariant et obstruction de descente itérée

Yang Cao

Pour une variété quasi-projective, lisse, géométriquement intègre sur un corps de nombres k, on montre que l'obstruction de descente itérée est équivalente à l'obstruction de descente. Ceci généralise un résultat de Skorobogatov, et ceci répond à une question ouverte de Poonen. Les outils principaux sont la notion de sous-groupe de Brauer invariant et la notion d'obstruction de Brauer–Manin étale invariante pour une k-variété munie d'une action d'un groupe linéaire connexe.

For a quasi-projective smooth geometrically integral variety over a number field k, we prove that the iterated descent obstruction is equivalent to the descent obstruction. This generalizes a result of Skorobogatov, and this answers an open question of Poonen. Our main tools are the notion of invariant Brauer subgroup and the notion of invariant étale Brauer–Manin obstruction for a k-variety equipped with an action of a connected linear algebraic group.

1. Introduction

Soit k un corps de nombres. Soit $\mathbf{A}_k$ l'anneau des adèles de k. Pour une k-variété lisse X, on note $X(\mathbf{A}_k)$ l'ensemble des points adéliques de X. On a le plongement diagonal

$$X(k) \subset X(\mathbf{A}_k).$$

C'est une question importante de caractériser l'adhérence des points rationnels dans les points adéliques (principe de Hasse, approximation faible, approximation forte). Manin [1971] a montré que cette adhérence est contenue dans un fermé déterminé par le groupe de Brauer de la variété X. Depuis lors, divers auteurs

MSC2010 : primary 11G35; secondary 14G05, 20G35.
Mots-clefs : Hasse principle, Brauer–Manin obstruction, algebraic group.

(Manin, Colliot-Thélène, Sansuc, Skorobogatov, Harari, Demarche) ont décrit d'autres fermés de $X(\boldsymbol{A}_k)$ contenant les points rationnels, et se sont attachés à comprendre les inclusions entre ces divers fermés. On a utilisé pour cela les torseurs sous des groupes linéaires (finis ou non) sur X, et on a utilisé des combinaisons de ces deux approches pour déterminer des fermés minimaux de $X(\boldsymbol{A}_k)$ contenant $X(k)$. Harari et Skorobogatov [2002, Definition 4.2] ont décrit une inclusion (cf. (1-2) pour la définition)

$$X(k) \subset X(\boldsymbol{A}_k)^{\text{descent}}.$$

Ensuite Poonen [2017, §8.5.2] a itéré cette inclusion en (cf. (1-3) pour la définition)

$$X(k) \subset X(\boldsymbol{A}_k)^{\text{descent, descent}} \subset X(\boldsymbol{A}_k)^{\text{descent}},$$

et demandé [Poonen 2017, §8.5.4] si la deuxième inclusion raffine la première. Le théorème principal du présent article (théorème 1.1) permet de répondre à cette question de Poonen : $X(\boldsymbol{A}_k)^{\text{descent, descent}} = X(\boldsymbol{A}_k)^{\text{descent}}$ (théorème 1.2 ci-dessous). Ce théorème 1.2 apporte un point final à l'utilisation combinée du groupe de Brauer et de la descente sous des groupes linéaires dans la détermination de l'adhérence de $X(k)$ dans $X(\boldsymbol{A}_k)$.

Donnons maintenant des énoncés précis.

On note Ω_k l'ensemble des places du corps de nombres k. Pour chaque $v \in \Omega_k$, on note k_v le complété de k en v et $\mathcal{O}_v \subset k_v$ l'anneau des entiers ($\mathcal{O}_v = k_v$ pour v archimédienne).

Pour B un sous-groupe de $\mathrm{Br}(X)$, on définit

$$X(\boldsymbol{A}_k)^B = \left\{ (x_v)_{v\in\Omega_k} \in X(\boldsymbol{A}_k) : \sum_{v\in\Omega_k} \mathrm{inv}_v(\xi(x_v)) = 0 \in \mathbb{Q}/\mathbb{Z},\ \forall \xi \in B \right\}.$$

Comme l'a remarqué Manin [1971], la théorie du corps de classes donne $X(k) \subseteq X(\boldsymbol{A}_k)^B$.

Soient F un k-groupe algébrique et $f : Y \to X$ un F-torseur. Pour tout 1-cocycle $\sigma \in Z^1(k, F)$, on note F_σ, respectivement $f_\sigma : Y_\sigma \to X$ le tordu du k-groupe F, respectivement du torseur f, par le 1-cocycle σ. Alors f_σ est un F_σ-torseur. La classe d'isomorphisme du k-groupe F_σ, respectivement du torseur f_σ, ne dépend que de la classe de σ dans $H^1(k, F)$. Par abus de notation, étant donnée une classe $[\sigma] \in H^1(k, F)$, on note $F_\sigma = F_{[\sigma]}$ et $f_\sigma = f_{[\sigma]}$.

Pour une k-variété lisse X, Skorobogatov [1999] et Poonen [2010, §3.3] définissent l'ensemble suivant :

$$X(\boldsymbol{A}_k)^{\text{ét,Br}} := \bigcap_{\substack{f:Y \xrightarrow{F} X \\ F \text{ fini}}} \bigcup_{\sigma\in H^1(k,F)} f_\sigma(Y_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}(Y_\sigma)}), \tag{1-1}$$

où F parcourt les k-groupes finis. Ils obtiennent une inclusion $X(k) \subset X(\boldsymbol{A}_k)^{\text{ét, Br}}$. Ceci définit une obstruction au principe de Hasse pour X, appelée *obstruction de Brauer–Manin étale*, étudiée dans le cas projectif par Skorobogatov, Harari et Demarche, puis dans le cas quasi-projectif [Cao et al. 2019a].

Le résultat principal de cet article est :

Théorème 1.1. *Soient G un k-groupe linéaire quelconque, Z une k-variété lisse et $p : X \to Z$ un G-torseur. Alors :*

$$Z(\mathbf{A}_k)^{\text{ét, Br}} = \bigcup_{\sigma \in H^1(k,G)} p_\sigma(X_\sigma(\mathbf{A}_k)^{\text{ét, Br}}).$$

Pour G fini et Z projective, ce théorème avait déjà été établi par Skorobogatov [2009, Theorem 1.1]. Pour G fini et Z quasi-projective, il avait été ensuite établi par Demarche, Xu et l'auteur [Cao et al. 2019a, Proposition 6.6]. Si Z est projective, $\pi_1(Z_{\bar{k}})$ est fini et G est une extension d'un k-groupe fini par un tore, Balestrieri [2018, Theorem 1.9] a établi une variante simple, où elle considère l'obstruction de Brauer–Manin algébrique étale.

Par ailleurs, dans [Poonen 2010, §3.2 ; 2017, §8], on définit deux ensembles

$$X(\mathbf{A}_k)^{\text{descent}} := \bigcap_{\substack{f:Y \xrightarrow{F} X \\ F \text{ linéaire}}} \bigcup_{\sigma \in H^1(k,F)} f_\sigma(Y_\sigma(\mathbf{A}_k)), \tag{1-2}$$

$$X(\mathbf{A}_k)^{\text{descent, descent}} := \bigcap_{\substack{f:Y \xrightarrow{F} X \\ F \text{ linéaire}}} \bigcup_{\sigma \in H^1(k,F)} f_\sigma(Y_\sigma(\mathbf{A}_k)^{\text{descent}}). \tag{1-3}$$

On a $X(k) \subset X(\mathbf{A}_k)^{\text{descent}}$ et $X(k) \subset X(\mathbf{A}_k)^{\text{descent, descent}}$. Ceci définit deux nouvelles obstructions au principe de Hasse pour X, appelées *obstruction de descente* et *obstruction de descente itérée*. D'après la série de travaux [Demarche 2009b ; Skorobogatov 2009 ; Cao et al. 2019a], on a $X(\mathbf{A}_k)^{\text{ét, Br}} = X(\mathbf{A}_k)^{\text{descent}}$ lorsque X est quasi-projective [Cao et al. 2019a, Theorem 1.5]. Du théorème 1.1 on déduit facilement le :

Théorème 1.2. *Pour toute variété quasi-projective lisse géométriquement intègre X, on a*

$$X(\mathbf{A}_k)^{\text{descent, descent}} = X(\mathbf{A}_k)^{\text{descent}}.$$

L'idée clé de la démonstration du théorème 1.1 est la notion de sous-groupe de Brauer invariant [Cao 2018, définition 3.1], que nous rappelons ici :

Définition 1.3. Soit G un groupe algébrique connexe.

(1) Soit (X, ρ) une G-variété lisse connexe. *Le sous-groupe de Brauer G-invariant* de X est le sous-groupe

$$\mathrm{Br}_G(X) := \{b \in \mathrm{Br}(X) \ : \ (\rho^*(b) - p_2^*(b)) \in p_1^*\mathrm{Br}(G)\}$$

de $\mathrm{Br}(X)$, où $G \times X \xrightarrow{p_1} G$, $G \times X \xrightarrow{p_2} X$ sont les projections et $G \times X \xrightarrow{\rho} X$ est l'action de G.

(2) Soit X une G-variété lisse quelconque. *Le sous-groupe de Brauer G-invariant* de X est le sous-groupe $\mathrm{Br}_G(X) \subset \mathrm{Br}(X)$ des éléments α vérifiant $\alpha|_{X'} \in \mathrm{Br}_G(X')$ pour toute composante connexe X' de X.

(3) Soient F un k-groupe fini et X une G-variété lisse quelconque. Un F-torseur $Y \xrightarrow{f} X$ est *G-compatible* s'il existe une action de G sur Y telle que f soit un G-morphisme.

D'après la proposition 3.3, l'action de G sur Y vérifiant les conditions ci-dessus est unique et le F_σ-torseur f_σ est aussi G-compatible pour tout $\sigma \in H^1(k, F)$. On définit la variante de $X(\boldsymbol{A}_k)^{\text{ét, Br}}$ suivante :

$$X(\boldsymbol{A}_k)^{G\text{-ét, Br}_G} := \bigcap_{\substack{f:Y\xrightarrow{F}X\ G\text{-compatible}\\ F \text{ fini}}} \bigcup_{\sigma\in H^1(k,F)} f_\sigma(Y_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_G(Y_\sigma)}). \tag{1-4}$$

Alors $X(k) \subset X(\boldsymbol{A}_k)^{\text{ét, Br}} \subset X(\boldsymbol{A}_k)^{G\text{-ét, Br}_G}$. Ceci définit une obstruction au principe de Hasse pour X, appelée *obstruction de Brauer–Manin étale invariante*.

Le théorème suivant joue un rôle clé dans la démonstration du théorème 1.1.

Théorème 1.4. *Soient G un groupe linéaire connexe et X une G-variété lisse. Alors*

$$X(\boldsymbol{A}_k)^{G\text{-ét, Br}_G} = X(\boldsymbol{A}_k)^{\text{ét, Br}}.$$

Dans le cas où X est un G-espace homogène à stabilisateur géométrique connexe, tout torseur G-compatible sous un k-groupe fini est constant, d'après le corollaire 3.5(4). Donc on peut obtenir facilement le résultat suivant.

Corollaire 1.5. *Soient G un groupe linéaire connexe et X un G-espace homogène à stabilisateur géométrique connexe. Alors*

$$X(\boldsymbol{A}_k)^{\text{ét, Br}} = X(\boldsymbol{A}_k)^{G\text{-ét, Br}_G} = X(\boldsymbol{A}_k)^{\mathrm{Br}_G(X)}.$$

Ce résultat particulier peut s'établir aussi via l'approximation forte sur X par rapport à $\mathrm{Br}_G(X)$ (voir [Borovoi et Demarche 2013, Theorem 1.4]).

Donnons maintenant la structure de l'article.

Au paragraphe 2, sur un corps k quelconque, s'inspirant de la notion de torseur universel de Colliot-Thélène et Sansuc, on introduit la notion de torseur universel de n-torsion (définition 2.1). Ensuite, on utilise cette notion à établir une formule de Künneth spéciale pour la cohomologie étale de degré 2.

Au paragraphe 3, sur un corps k de caractéristique zéro, on considère la donnée d'un k-groupe algébrique G, d'une G-variété X lisse, d'un k-groupe fini F, d'un torseur $Y \to X$ sous F, on donne des conditions équivalentes pour le relèvement, de façon compatible, de l'action de G sur X en une action sur Y. Ce relèvement n'est pas toujours possible. On étudie les homomorphismes surjectifs de groupes algébriques connexes $H \to G$ avec une action compatible de H sur Y, et on montre qu'il existe un objet minimal H_Y. Étant donné un élément $\alpha \in \mathrm{Br}(X)$, en utilisant la formule de Künneth ci-dessus, on montre ensuite qu'il existe un torseur $Y \to X$ sous un k-groupe fini commutatif F tel que l'image réciproque de α dans $\mathrm{Br}(Y)$ soit invariante sous H_Y.

Au paragraphe 4, on rappelle des notions et des résultats établis dans [Cao 2018, §3], en particulier, la notion de sous-groupe de Brauer invariant et aussi ses propriétés élémentaires. Ces résultats seront utilisés dans les paragraphes 5 et 6.

Au paragraphe 5, le corps de base k est un corps de nombres. Dans [Cao 2018], étant donné un torseur $Y \to X$ sous un groupe linéaire connexe G, j'ai développé la méthode de descente des points adéliques orthogonaux aux sous-groupes de Brauer invariants. Au paragraphe 5, on donne deux nouvelles variantes de cette descente. La première (proposition 5.1) traite du cas où G est un k-groupe fini commutatif. La seconde (proposition 5.5) implique l'obstruction de Brauer–Manin étale invariante.

Les paragraphes 3, 4 et 5 sont utilisés de façon essentielle au paragraphe 6 où l'on établit le théorème 1.4.

Au paragraphe 7, en combinant le théorème 1.4 et la proposition 5.5, on établit les théorèmes 1.1 et 1.2.

Conventions et notations. Soit k un corps quelconque de caractéristique $\mathrm{char}(k)$. On note $\bar{k}$ une clôture algébrique, k_s une clôture séparable et $\Gamma_k := \mathrm{Gal}(k_s/k)$. Si $\mathrm{char}(k) = 0$, on a $k_s = \bar{k}$ et $\Gamma_k := \mathrm{Gal}(\bar{k}/k)$.

Tous les groupes de cohomologie sont des groupes de cohomologie étale.

Une k-variété X est un k-schéma séparé de type fini. Pour X une telle variété, on note $k[X]$ son anneau des fonctions globales, $k[X]^\times$ son groupe des fonctions inversibles, $\mathrm{Pic}(X) := H^1_{\text{ét}}(X, \mathbb{G}_m)$ son groupe de Picard et $\mathrm{Br}(X) := H^2_{\text{ét}}(X, \mathbb{G}_m)$ son groupe de Brauer. Notons

$$\mathrm{Br}_1(X) := \mathrm{Ker}[\mathrm{Br}(X) \to \mathrm{Br}(X_{\bar{k}})] \quad \text{et} \quad \mathrm{Br}_a(X) := \mathrm{Br}_1(X)/\mathrm{Im}\mathrm{Br}(k).$$

Le groupe $\mathrm{Br}_1(X)$ est le sous-groupe "algébrique" du groupe de Brauer de X. Si X est intègre, on note $k(X)$ son corps des fonctions rationnelles et $\pi_1(X, \bar{x})$ (ou $\pi_1(X)$) son groupe fondamental étale, où $\bar{x}$ est un point géométrique de X. Soit $\pi_1(X_{k_s})^{\mathrm{ab}}$ le quotient maximal abélien de $\pi_1(X_{k_s})$. Alors $\pi_1(X_{k_s})^{\mathrm{ab}}$ est un Γ_k-module.

Un k-groupe algébrique G est une k-variété qui est un k-schéma en groupes. On note e_G l'unité de G et $G^* := \mathrm{Hom}_{k_s\text{-groupe}}(G_{k_s}, \mathbb{G}_m)$ le groupe des caractères de G_{k_s}. C'est un module galoisien de type fini. De plus, si G est connexe sur $\mathbb{C}$, le groupe $\pi_1(G)$ est commutatif (cf. [Brion et Szamuely 2013, Proposition 1.1(2)]).

Un k-groupe fini F est un k-groupe algébrique qui est fini sur k. Dans ce cas, F est déterminé par le Γ_k-groupe $F(k_s)$. Pour toute k-variété lisse connexe X, on a un isomorphisme canonique [SGA 1 1971, §XI.5] :

$$H^1(\pi_1(X), F(k_s)) \xrightarrow{\sim} H^1(X, F) \quad \text{et donc} \quad H^1(X_{k_s}, F) \cong \mathrm{Hom}_{\mathrm{cont}}(\pi_1(X_{k_s}), F(k_s))/\sim \tag{1-5}$$

où l'action de $\pi_1(X)$ sur $F(k_s)$ est induite par celle de Γ_k et $\sim$ est induite par la conjugaison.

Soit G un k-groupe algébrique. Une *G-variété* (X, ρ) (ou X) est une k-variété X munie d'une action à gauche $G \times_k X \xrightarrow{\rho} X$. Un k-morphisme de G-variétés est appelé *G-morphisme* s'il est compatible avec l'action de G.

Comme déjà indiqué ci-dessus, pour tout k-groupe algébrique F, tout F-torseur $f : Y \to X$ et tout $\sigma \in H^1(k, F)$, on note F_σ (resp. $f_\sigma : Y_\sigma \to X$) le tordu de F (resp. de f). Ainsi f_σ est un F_σ-torseur.

2. Torseur universel de *n*-torsion et formule de Künneth de degré 2

Dans toute cette section, k est un corps quelconque. Sauf mention explicite du contraire, une variété est une k-variété. Fixons un entier $n \geq 2$ avec $\mathrm{char}(k) \nmid n$ et notons $- \otimes - := - \otimes_{\mathbb{Z}/n} -$.

Cette section contient deux parties. On introduit d'abord la version de n-torsion de la notion de torseur universel (Colliot-Thélène et Sansuc) dans la définition 2.1, et aussi la notion de type prolongé d'un torseur (Harari et Skorobogatov) dans la proposition 2.2. En utilisant ces notions, on considère ensuite le cup-produit de la cohomologie étale de degré 2 sur un produit de deux variétés quelconques et on établit une formule de Künneth pour ce produit (proposition 2.6). Cette formule généralise un résultat de Skorobogatov et Zarhin, qui traite du cas où les deux variétés sont propres.

Soient $\mathrm{Sh}(k)$ la catégorie des faisceaux étales sur le petit site de $\mathrm{Spec}\, k$ et $D^+(k)$ la catégorie dérivée bornée à gauche de $\mathrm{Sh}(k)$ et $D^b(k)$ la catégorie dérivée bornée de $\mathrm{Sh}(k)$ (une sous-catégorie pleine de $D^+(k)$). Pour tout $i \in \mathbb{Z}$, on a les sous-catégories canoniques $D^{\geq i}(k)$ et $D^{\leq i}(k)$ de $D^+(k)$ et deux foncteurs canoniques $\tau_{\leq i}$, $\tau_{\geq i}$ [Kashiwara et Schapira 2006, Definition 12.3.1, Proposition 13.1.5]. Donc $\mathrm{Sh}(k) = D^{\geq 0}(k) \cap D^{\leq 0}(k)$ est une sous-catégorie pleine canonique de $D^+(k)$. Par abus de notation, pour un objet M de $\mathrm{Sh}(k)$, on note M l'objet de $D^+(k)$ représenté par le complexe qui consiste en M en degré 0.

Soient X une variété géométriquement intègre et $p : X \to \mathrm{Spec}\, k$ le morphisme de structure. Soit S_X un groupe de type multiplicatif tel que $S_X^* \cong H^1(X_{k_s}, \mu_n)$ comme Γ_k-modules. On rappelle que $H^1(X_{k_s}, \mu_n)$ est fini.

Dans $D^+(k)$, il existe deux morphismes canoniques $\mathbb{G}_m \to Rp_*\mathbb{G}_m$ et $\mu_n \to Rp_*\mu_n$. Soient Δ le cône de $\mathbb{G}_m[1] \to Rp_*\mathbb{G}_m[1]$ et Δ_n le cône de $\mu_n[1] \to Rp_*\mu_n[1]$. La suite exacte de Kummer donne un diagramme commutatif de triangles distingués :

$$\begin{tikzcd}
\Delta_n[-2] \arrow[r] \arrow[d, "\psi"] & \mu_n \arrow[r] \arrow[d] & Rp_*\mu_n \arrow[r, "+1"] \arrow[d] & {} \\
\Delta[-2] \arrow[r] \arrow[d, "n\cdot"] & \mathbb{G}_m \arrow[r] \arrow[d, "n\cdot"] & Rp_*\mathbb{G}_m \arrow[r, "+1"] \arrow[d, "n\cdot"] & {} \\
\Delta[-2] \arrow[r] \arrow[d, "+1"] & \mathbb{G}_m \arrow[r] \arrow[d, "+1"] & Rp_*\mathbb{G}_m \arrow[r, "+1"] \arrow[d, "+1"] & {} \\
{} & {} & {} &
\end{tikzcd}$$

Les faisceaux de cohomologie des complexes Δ_n et Δ se calculent comme suit :

$$\Delta_n \in D^{\geq 0}(k), \quad \mathcal{H}^0(\Delta_n) \cong H^1(X_{k_s}, \mu_n) \cong S_X^*,$$
$$\Delta \in D^{\geq -1}(k), \quad \mathcal{H}^{-1}(\Delta) = k_s[X]^\times / k_s^\times \quad \text{et} \quad \mathcal{H}^0(\Delta) = \mathrm{Pic}(X_{k_s}).$$

Le morphisme $\psi : \Delta_n \to \Delta$ induit un morphisme $\psi_{\leq 0} := \tau_{\leq 0}\psi : S_X^* \to \tau_{\leq 0}\Delta$.

Harari et Skorobogatov montrent que, pour tout groupe de type multiplicatif S, on a une suite exacte naturelle [2013, Proposition 1.1, où $\tau_{\leq 0}\Delta$ est noté $KD'(X)$] :

$$H^1(k, S) \to H^1(X, S) \xrightarrow{\chi} \mathrm{Hom}_{D^+(k)}(S^*, \tau_{\leq 0}\Delta) \to H^2(k, S). \tag{2-1}$$

Définition 2.1. Un *torseur universel de n-torsion* pour X est un S_X-torseur $\mathcal{T}_X$ sur X tel que $\chi([\mathcal{T}_X]) = \psi_{\leq 0} : S_X^* \to \tau_{\leq 0}\Delta$.

D'après [Harari et Skorobogatov 2013, Proposition 1.3], si $X(k) \neq \varnothing$, pour chaque $x \in X(k)$, il existe alors un unique torseur universel de n-torsion $\mathcal{T}_X$ pour X tel que $x^*[\mathcal{T}_X] = 0 \in H^1(k, S_X)$.

Dans le cas où k est un corps de nombres, il existe un torseur universel de n-torsion pour X lorsque $X(\boldsymbol{A}_k)^{\mathrm{Br}_1(X)} \neq \varnothing$ [Harari et Skorobogatov 2013, Corollary 3.6].

Proposition 2.2. *Soit $\mathcal{T}_X$ un torseur universel de n-torsion pour X. Soit S un groupe de type multiplicatif tel que $n \cdot S = 0$. Alors, pour tout S-torseur Y sur X, il existe un unique homomorphisme $\phi : S_X \to S$ tel que*

$$\phi_*([\mathcal{T}_X]) - [Y] \in \mathrm{Im}(H^1(k, S) \to H^1(X, S)).$$

Démonstration. Le triangle $\Delta_n \to \Delta \xrightarrow{n\cdot} \Delta \xrightarrow{+1}$ induit une suite exacte

$$\mathrm{Hom}_{D^+(k)}(S^*, \Delta[-1]) \to \mathrm{Hom}_{D^+(k)}(S^*, \Delta_n) \to \mathrm{Hom}_{D^+(k)}(S^*, \Delta) \xrightarrow{n\cdot} \mathrm{Hom}_{D^+(k)}(S^*, \Delta).$$

Puisque $S^* \in D^{\leq 0}(k)$ et $n \cdot S^* = 0$, on a

$$\mathrm{Hom}_{D^+(k)}(S^*, \Delta[-1]) = \mathrm{Hom}_k(S^*, \mathcal{H}^{-1}(\Delta)) = \mathrm{Hom}_k(S^*, \bar{k}[X]^\times/\bar{k}^\times) = 0$$

et donc $\mathrm{Hom}_k(S^*, S_X^*)$ est isomorphe à

$$\mathrm{Hom}_{D^+(k)}(S^*, S_X^*) \xrightarrow{\sim} \mathrm{Hom}_{D^+(k)}(S^*, \Delta_n) \xrightarrow{\sim} \mathrm{Hom}_{D^+(k)}(S^*, \Delta) \xleftarrow{\sim} \mathrm{Hom}_{D^+(k)}(S^*, \tau_{\leq 0}\Delta).$$

Alors $\chi([Y]) \in \mathrm{Hom}_{D^+(k)}(S^*, \tau_{\leq 0}\Delta)$ donne un homomorphisme $\phi^* \in \mathrm{Hom}_k(S^*, S_X^*)$, et donc $\chi([Y]) = \psi_{\leq 0} \circ \phi^*$. Soit $\phi : S_X \to S$ l'homomorphisme correspondant. La suite exacte (2-1) implique l'énoncé. □

L'homomorphisme ϕ dans la proposition 2.2 est appelé *le n-type de* $[Y]$.

Soit $\mathcal{T}_X$ le torseur universel de n-torsion pour X_{k_s}, on obtient un isomorphisme de Γ_k-modules :

$$\tau_{X,S} : \mathrm{Hom}_{k_s}(S_X, S) \cong \mathrm{Hom}_{k_s}(S^*, S_X^*) \to H^1(X_{k_s}, S) : \phi \mapsto \phi_*([\mathcal{T}_X]). \tag{2-2}$$

En particulier, on a deux Γ_k-isomorphismes naturels

$$\tau_X := \tau_{X,\mu_n} : S_X^* \xrightarrow{\sim} H^1(X_{k_s}, \mu_n) : \phi \mapsto \phi_*(\mathcal{T}_X) \tag{2-3}$$

et

$$\tau_X(-1) := \tau_{X,\mathbb{Z}/n} : \mathrm{Hom}_{k_s}(S_X, \mathbb{Z}/n) \xrightarrow{\sim} H^1(X_{k_s}, \mathbb{Z}/n) : \phi \mapsto \phi_*(\mathcal{T}_X). \tag{2-4}$$

En fait, par définition, τ_X est exactement l'homomorphisme $S_X^* \to \mathcal{H}^0(\Delta_n)$ induit par $\psi_{\leq 0}$.

Rappelons que, pour tous $F_1, F_2 \in D^b(k)$, le produit tensoriel $F_1 \otimes^L F_2$ est bien défini et *le cup-produit* est le homomorphisme canonique

$$\cup_j : \textstyle\bigoplus_{r+s=j} \mathcal{H}^r(F_1) \otimes \mathcal{H}^s(F_2) \to \mathcal{H}^j(F_1 \otimes^L F_2)$$

induit par la suite spectrale de Godement (cf. [Milne 1980, Lemma VI.8.6] ou [Fu 2011, Proposition 6.4.12]). De plus, $Rp_*\mu_n \in D^b(k)$ [Fu 2011, Corollary 7.5.6].

Corollaire 2.3. *Supposons que k est séparablement clos. Soit $p : X \to \operatorname{Spec} k$ une variété intègre. Alors*

(1) *le cup-produit* $\cup : H^1(X, \mu_n) \otimes \operatorname{Hom}(\mu_n, S) \to H^1(X, S) : (\alpha, \varphi) \mapsto \varphi_*(\alpha)$ *est un isomorphisme* ;

(2) *pour tout complexe de $\mathbb{Z}/n$-modules* (vus comme k-faisceaux) *de type fini F avec $F \in D^{\geq 0}(k) \cap D^b(k)$, on a $Rp_*\mu_n \otimes^L F \in D^{\geq 0}(k)$ et le cup-produit*

$$\cup_j(F) : \bigoplus_{r+s=j} R^r p_*\mu_n \otimes \mathcal{H}^s(F) \cong \bigoplus_{r+s=j} \mathcal{H}^r(Rp_*\mu_n) \otimes \mathcal{H}^s(F) \to \mathcal{H}^j(Rp_*\mu_n \otimes^L F)$$

est un isomorphisme pour $j = 0$ et $j = 1$;

(3) *dans* (2), *si $\mathcal{H}^0(F)$ est plat, alors $\cup_2(F)$ est un isomorphisme.*

Démonstration. Puisque $X(k) \neq \varnothing$, il existe un torseur universel de n-torsion $\mathcal{T}_X \to X$. D'après (2-2), on a le diagramme

$$\begin{tikzcd} \operatorname{Hom}(S_X, \mu_n) \otimes \operatorname{Hom}(\mu_n, S) \arrow[r, "- \circ -", "\cong"'] \arrow[d, "\cong"', "\tau_X \otimes id"] & \operatorname{Hom}(S_X, S) \arrow[d, "\cong"', "\tau_{X,S}"] \\ H^1(X, \mu_n) \otimes \operatorname{Hom}(\mu_n, S) \arrow[r, "\cup"] & H^1(X, S) \end{tikzcd}$$

où $- \circ - : (\psi, \phi) \mapsto \phi \circ \psi$. Ce diagramme est commutatif car

$$\tau_{X,S}(\varphi \circ \phi) = (\varphi \circ \phi)_*[\mathcal{T}_X] = \varphi_*(\phi_*[\mathcal{T}_X]) \overset{(2\text{-}3)}{=} \tau_X[\phi] \cup \varphi$$

pour tout $\phi \in \operatorname{Hom}(S_X, \mu_n)$ et tout $\varphi \in \operatorname{Hom}(\mu_n, S)$. Donc on a (1).

Pour tout complexe F dans (2), puisque la dimension cohomologique de Rp_* est finie [SGA 4_3 1973, XIV] (cf. [Fu 2011, Corollary 7.5.6]), on a :

(i) D'après [SGA 4_3 1973, XVII. Theorem 5.2.11], pour tout $j < 0$, on a $\mathcal{H}^j(Rp_*\mu_n \otimes^L F) = 0$ et donc $Rp_*\mu_n \otimes^L F \in D^{\geq 0}(k)$. Ceci implique le premier énoncé de (2).

(ii) Si $F \cong \mathcal{H}^0(F)$ avec $\mathcal{H}^0(F)$ plat, on a $\mathcal{H}^j(Rp_*\mu_n \otimes^L F) = \mathcal{H}^j(Rp_*\mu_n) \otimes F$ et donc $\cup_j(F)$ est un isomorphisme pour tout j.

(iii) Si $F \cong \mathcal{H}^0(F)$, on a $Rp_*\mu_n \otimes^L F \cong Rp_*(\mu_n \otimes p^*F)$ [SGA 4_3 1973, XVII. (5.2.11.1)] (cf. [Fu 2011, Corollary 6.5.6]). Puisque X est intègre, $\cup_0(F) : \mu_n \otimes F \to R^0 p_*(\mu_n \otimes p^*F)$ est un isomorphisme, et d'après l'énoncé (1) et [Milne 1980, Proposition V.1.20], le cup-produit

$$\cup_1(F) : R^1 p_*\mu_n \otimes F \cong H^1(X, \mu_n) \otimes \operatorname{Hom}(\mu_n, \mu_n \otimes F) \overset{\cup}{\to} H^1(X, \mu_n \otimes F) \cong \mathcal{H}^1(Rp_*(\mu_n \otimes p^*F))$$

est un isomorphisme. Ceci vaut seulement pour le cup-produit de degré 1.

Pour tout complexe F dans (2), notons $F_+ := (\tau_{\geq 1}F)[1]$ un objet dans $D^{\geq 0}(k) \cap D^b(k)$. Alors F_+ vérifie toutes les hypothèses dans (2).

Le triangle $\mathcal{H}^0(F) \to F \to F_+[-1] \xrightarrow{+1}$ donne un diagramme commutatif de suites exactes :

$$\begin{tikzcd}
0 \arrow[r] & R^j(\mathcal{H}^0(F)) \arrow[r] \arrow[d, "\cup_j(\mathcal{H}^0(F))"] & \bigoplus_{r+s=j} R^r(\mathcal{H}^s(F)) \arrow[r] \arrow[d, "\cup_j(F)"] & \bigoplus_{r+s=j-1} R^r(\mathcal{H}^s(F_+)) \arrow[r] \arrow[d, "\cup_{j-1}(F_+)"] & 0 \arrow[d] \\
H^{j-2}_{\mu_n}(F_+) \arrow[r, "\theta_{j-1}"] & H^j_{\mu_n}(\mathcal{H}^0(F)) \arrow[r] & H^j_{\mu_n}(F) \arrow[r] & H^{j-1}_{\mu_n}(F_+) \arrow[r, "\theta_j"] & H^{j+1}_{\mu_n}(\mathcal{H}^0(F))
\end{tikzcd} \tag{2-5}$$

où $H^j_{\mu_n}(-) := \mathcal{H}^j(Rp_*\mu_n \otimes^L -)$, $R^r(-) := R^r p_*\mu_n \otimes -$ et la première ligne est exacte car elle est scindée.

Montrons l'énoncé (2). D'après (i), on a : $H^{-2}_{\mu_n}(F_+) = H^{-1}_{\mu_n}(F_+) = 0$. D'après (iii), $\cup_0(\mathcal{H}^0(F))$ est un isomorphisme. Le lemme des cinq implique : $\cup_0(F)$ est un isomorphisme. Ceci donne l'énoncé(2) pour $j = 0$. Donc $\cup_0(F_+)$ est un isomorphisme. D'après (iii), $\cup_1(\mathcal{H}^0(F))$ est un isomorphisme. Le lemme des cinq implique : $\cup_1(F)$ est un isomorphisme.

Montrons l'énoncé (3). Par hypothèse, $\mathcal{H}^0(F)$ est plat, et d'après (ii), $\cup_2(\mathcal{H}^0(F))$ est un isomorphisme. D'après (2), $\cup_1(F_+)$ et $\cup_0(F_+)$ sont des isomorphismes. Donc $\theta_1 = 0$ et le lemme des cinq implique : $\cup_2(F)$ est un isomorphisme. □

Si X est lisse, d'après (1-5), l'isomorphisme (2-4) donne un Γ_k-isomorphisme naturel

$$\tau_X(-1) : \mathrm{Hom}(S_X, \mathbb{Z}/n) \xrightarrow{\sim} H^1(X_{k_s}, \mathbb{Z}/n) \cong \mathrm{Hom}_{\mathrm{cont}}\big(\pi_1(X_{k_s})^{\mathrm{ab}}, \mathbb{Z}/n\big) : \psi \mapsto \psi(k_s) \circ \tau_{\pi_1}, \tag{2-6}$$

où $\tau_{\pi_1} : \pi_1(X_{k_s})^{\mathrm{ab}} \to S_X(k_s)$ est l'homomorphisme induit par $\mathcal{T}_X$. Ainsi τ_{π_1} induit un isomorphisme de Γ_k-modules $\pi_1(X_{k_s})^{\mathrm{ab}}/n \xrightarrow{\sim} S_X(k_s)$ et $\mathcal{T}_X$ est géométriquement intègre.

Corollaire 2.4. *Soit X une variété lisse géométriquement intègre. Soient M un $\mathbb{Z}/n$-module et*

$$\pi_1(X_{k_s})^{\mathrm{ab}} \xrightarrow{\theta} M$$

un homomorphisme surjectif de noyau Γ_k-invariant. Supposons qu'il existe un torseur universel de n-torsion pour X. Alors il existe un k-groupe fini commutatif S et un S-torseur $\mathcal{T} \to X$ tels que $\mathcal{T}$ soit lisse géométriquement intègre, $S(k_s) = M$ et que, dans $H^1(X_{k_s}, S) \cong \mathrm{Hom}_{\mathrm{cont}}\big(\pi_1(X_{k_s})^{\mathrm{ab}}, M\big)$, on ait $[\mathcal{T}_{k_s}] = \theta$.

Démonstration. Soit $\mathcal{T}_X$ un torseur universel de n-torsion pour X (un torseur sous le k-groupe S_X). Puisque $\mathrm{Ker}(\theta)$ est Γ_k-invariant, il existe une unique Γ_k-structure sur M telle que θ soit un Γ_k-morphisme. Ceci induit un k-groupe commutatif S et un homomorphisme surjectif $\theta' : S_X \to S$ tels que $S(k_s) = M$ et que $\theta'(k_s) \circ \tau_{\pi_1} = \theta$. Alors $\mathcal{T} := \theta'_*\mathcal{T}_X := \mathcal{T}_X \times^{S_X} S$ donne l'énoncé. □

Soient U, V deux variétés géométriquement intègres sur k. On considère le diagramme commutatif

$$\begin{tikzcd}
U \times_k V \arrow[r, "p_2"] \arrow[d, "p_1"] & V \arrow[d, "q_2"] \\
U \arrow[r, "q_1"] & \operatorname{Spec} k
\end{tikzcd} \tag{2-7}$$

Soient M, N deux $\mathbb{Z}/n$-faisceaux finis plats sur le grand site de k. Le cup-produit donne un quasi-isomorphisme [SGA 4½ 1977, Th. finitude, corolaire 1.11] (cf. [Fu 2011, Corollary 9.3.5]) :

$$\cup:\ Rq_{1,*}M\otimes^L Rq_{2,*}N\cong R(q_1\circ p_1)_*(M\otimes^L N). \tag{2-8}$$

Ceci induit le cup-produit [Fu 2011, Proposition 6.4.12] :

$$\cup_j:\bigoplus\nolimits_{r+s=j}R^rq_{1,*}M\otimes_{\mathbb{Z}/n}R^sq_{2,*}N\to\mathcal{H}^j(Rq_{1,*}M\otimes^L Rq_{2,*}N)\xrightarrow{\sim}R^j(q_1\circ p_1)_*(M\otimes^L N).$$

Lemme 2.5. *Le cup-produit $\cup_j$ est un isomorphisme pour $j=0,1,2$.*

Démonstration. On peut supposer que k est séparablement clos. Les $\mathbb{Z}/n$-modules finis M, N sont plats et donc ils sont des facteurs directs de $(\mathbb{Z}/n)^{\oplus i}$ pour i assez grand. Puisque tous les foncteurs ci-dessus commutent avec les sommes directs finies, on peut supposer que $M=N=\mu_n$. L'énoncé découle du corollaire 2.3(3) et de (2-8). □

Le résultat ci-dessous généralise [Skorobogatov et Zarhin 2014, Theorem 2.6].

Proposition 2.6. *Supposons que k est séparablement clos. Soient U, V deux variétés géométriquement intègres et F un $\mathbb{Z}/n$-module fini plat. On considère le diagramme* (2-7). *Alors on a des isomorphismes naturels*

$$(p_1^*,p_2^*):\ H^1(U,F)\oplus H^1(V,F)\xrightarrow{\sim}H^1(U\times V,F)$$

et

$$(p_1^*,\cup,p_2^*):H^2(U,F)\oplus[H^1(U,\mathbb{Z}/n)\otimes_{\mathbb{Z}}H^1(V,F)]\oplus H^2(V,F)\xrightarrow{\sim}H^2(U\times V,F),$$

où $\cup:H^1(U,\mathbb{Z}/n)\otimes_{\mathbb{Z}}H^1(V,F)\to H^2(U\times V,F)$ est le cup-produit.

C'est clair que si U, V sont définis sur un sous-corps $k_0\subset k$ avec k/k_0 galoisienne et F un $\mathrm{Gal}(k/k_0)$-module, alors les deux isomorphismes ci-dessus sont des isomorphismes de $\mathrm{Gal}(k/k_0)$-modules.

Si $\mathrm{char}(k)=0$, cette proposition découle de [Skorobogatov et Zarhin 2014, Proposition 2.2] et de [Milne 1980, Theorem III.3.12] (on peut vérifier que l'homomorphisme dans [Skorobogatov et Zarhin 2014, Proposition 2.2] est compatible avec le cup-produit).

Démonstration. On applique le lemme 2.5 au cas $U\times k$ et au cas $k\times V$, et on obtient deux diagrammes commutatifs :

$$\begin{tikzcd}
H^i(U,\mathbb{Z}/n)\otimes H^0(k,F) \arrow[r, "\cup_U", "\cong"'] \arrow[d, "id\times q_2^*"', "\cong"] & H^i(U,F) \arrow[d, "p_1^*"] \\
H^i(U,\mathbb{Z}/n)\otimes H^0(V,F) \arrow[r, "\cup_i"] & H^i(U\times V,F)
\end{tikzcd}
\qquad
\begin{tikzcd}
H^0(k,\mathbb{Z}/n)\otimes H^i(V,F) \arrow[r, "\cup_V", "\cong"'] \arrow[d, "q_1^*\times id"', "\cong"] & H^i(V,F) \arrow[d, "p_2^*"] \\
H^0(U,\mathbb{Z}/n)\otimes H^i(V,F) \arrow[r, "\cup_i"] & H^i(U\times V,F)
\end{tikzcd}$$

pour $i=1$ et 2, où $\cup_U$ (resp. $\cup_V$) est le cup-produit sur U (resp. V). Donc

$$p_1^*(H^i(U,F))=\cup_i\big(H^i(U,\mathbb{Z}/n)\otimes H^0(V,F)\big)\quad\text{et}\quad p_2^*(H^i(V,F))=\cup_i\big(H^0(U,\mathbb{Z}/n)\otimes H^i(V,F)\big).$$

L'énoncé découle du lemme 2.5. □

Soient $\mathcal{T}_U$ (resp. $\mathcal{T}_V$) un torseur universel de n-torsion pour U (resp. pour V) et S_U (resp. S_V) le groupe correspondant (cf. définition 2.1). Skorobogatov et Zarhin [2014, §5] introduisent un homomorphisme :

$$\varepsilon : \mathrm{Hom}_k(S_U, S_V^*) \to H^2(U \times V, \mu_n) : \phi \mapsto \phi_*[\mathcal{T}_U] \cup [\mathcal{T}_V], \tag{2-9}$$

où $\cup$ est le cup-produit $H^1(U, S_V^*) \times H^1(V, S_V) \to H^2(U \times V, \mu_n)$. Les isomorphismes τ_V dans (2-3) et $\tau_U(-1)$ dans (2-4) donnent un diagramme :

$$\begin{tikzcd}
(\mathrm{Hom}_{k_s}(S_U, \mathbb{Z}/n) \otimes S_V^*)^{\Gamma_k} \arrow[r, "="', "\Phi"'] \arrow[r, "="] \arrow[dr, "\sim", "(\tau_U(-1), \tau_V)"'] & \mathrm{Hom}_k(S_U, S_V^*) \arrow[r, "\varepsilon"] & H^2(U \times V, \mu_n) \arrow[d] \\
& (H^1(U_{k_s}, \mathbb{Z}/n) \otimes H^1(V_{k_s}, \mu_n))^{\Gamma_k} \arrow[r, "\cup"] & H^2((U \times V)_{\bar{k}}, \mu_n),
\end{tikzcd} \tag{2-10}$$

qui est commutatif parce que, pour tous $\varphi \in \mathrm{Hom}_{k_s}(S_U, \mathbb{Z}/n)$ et $\phi \in S_V^* = \mathrm{Hom}_{k_s}(S_V, \mu_n)$, on note $\phi^* := \mathrm{Hom}_{k_s}(\phi, \mu_n) : \mathbb{Z}/n \to S_V^*$ le dual de ϕ, et on a :

$$\varepsilon(\Phi(\varphi \otimes \phi)) = \varepsilon(\phi^* \circ \varphi) = (\phi^*)_*(\varphi_*[\mathcal{T}_U]) \cup [\mathcal{T}_V] \overset{(1)}{=} \varphi_*[\mathcal{T}_U] \cup \phi_*[\mathcal{T}_V] = \tau_U(-1)(\varphi) \cup \tau_V(\phi),$$

où (1) découle du diagramme commutatif

$$\begin{tikzcd}
H^1(U \times V, S_V) \arrow[d, "\phi_*"] & \times & H^1\big(U \times V, \mathrm{Hom}_{k_s}(S_V, \mu_n)\big) \arrow[r, "\cup"] & H^2(U \times V, \mu_n) \arrow[d, "="] \\
H^1(U \times V, \mu_n) & \times & H^1\big(U \times V, \mathrm{Hom}_{k_s}(\mu_n, \mu_n)\big) \arrow[u, "(\phi^*)_* = \mathrm{Hom}_{k_s}(\phi, \mu_n)_*"] \arrow[r, "\cup"] & H^2(U \times V, \mu_n).
\end{tikzcd}$$

Si $U(k) \neq \varnothing$, alors il existe un torseur universel de n-torsion pour U. Pour un point $u \in U(k)$, notons

$$H_u^i(U, \mu_n) := \mathrm{Ker}\big(H^i(U, \mu_n) \xrightarrow{u^*} H^i(k, \mu_n)\big).$$

Corollaire 2.7. *Sous les notations et hypothèses ci-dessus, supposons que $U(k) \neq \varnothing$ avec $u \in U(k)$ et qu'il existe des torseurs universels de n-torsion $\mathcal{T}_U$ pour U* (sous le groupe S_U) *et $\mathcal{T}_V$ pour V* (sous le groupe S_V). *Alors on a un isomorphisme* :

$$H_u^2(U, \mu_n) \oplus H^2(V, \mu_n) \oplus \mathrm{Hom}_k(S_U, S_V^*) \xrightarrow{(p_1^*, p_2^*, \varepsilon)} H^2(U \times V, \mu_n).$$

Démonstration. Notons $E_2^{i,j}(U) := H^i(k, H^j(U_{k_s}, \mu_n)) \Rightarrow H^{i+j}(U, \mu_n)$ la suite spectrale de Hochschild–Serre de U et $E_2^{i,j}(V)$ (resp. $E_2^{i,j}(U \times V)$) celle de V (resp. de $U \times V$).

Notons $H_u^i(U_{k_s}, \mu_n) := \mathrm{Ker}\big(H^i(U_{k_s}, \mu_n) \xrightarrow{u^*} H^i(k_s, \mu_n)\big)$. Alors $H_u^0(U_{k_s}, \mu_n) = 0$ et $H_u^i(U_{k_s}, \mu_n) = H^i(U_{k_s}, \mu_n)$ pour $i \neq 0$. La suite spectrale de Hochschild–Serre donne canoniquement une suite spectrale :

$$E_2^{i,j}(U, u) := H^i(k, H_u^j(U_{k_s}, \mu_n)) \Rightarrow H_u^{i+j}(U, \mu_n).$$

Soit $\phi_2^{i,j} : E_2^{i,j}(U, u) \oplus E_2^{i,j}(V) \to E_2^{i,j}(U \times V)$ le morphisme de suites spectrales induit par (p_1^*, p_2^*). D'après la proposition 2.6, $\phi_2^{i,j}$ est un isomorphisme pour $j = 0, 1$ et $\phi_2^{0,2}$ est injectif. Ainsi $\phi_2^{i,j}$ induit une suite exacte par le lemme des cinq :

$$0 \to H^2_u(U, \mu_n) \oplus H^2(V, \mu_n) \xrightarrow{p_1^*, p_2^*} H^2(U \times V, \mu_n) \to \operatorname{coker}(\phi_2^{0,2}).$$

D'après la proposition 2.6 et le diagramme (2-10), on a $\operatorname{coker}(\phi_2^{0,\,2}) \cong \big(H^1(U_{\bar{k}}, \mathbb{Z}/n) \otimes H^1(V_{\bar{k}}, \mu_n)\big)^{\Gamma_k}$ et la composition

$$\operatorname{Hom}_k(S_U, S_V^*) \xrightarrow{\varepsilon} H^2(U \times V, \mu_n) \to H^2\big((U \times V)_{\bar{k}}, \mu_n\big)^{\Gamma_k} \to \operatorname{coker}(\phi_2^{0,\,2})$$

est un isomorphisme, d'où le résultat. □

3. Préliminaires sur les torseurs sous un groupe fini

Dans toute cette section, k est un corps quelconque de caractéristique 0. Sauf mention explicite du contraire, une variété est une k-variété.

Soit G un groupe algébrique connexe et X une G-variété lisse géométriquement intègre. Cette section traite trois problèmes : pour un torseur $H \to G$ sous un k-groupe fini, on montre l'existence et l'unicité de la structure de groupe sur H dans paragraphe 3A ; pour un torseur $Y \to X$ sous un k-groupe fini, on donne dans paragraphe 3B une condition nécessaire et suffisante pour le relèvement, de façon compatible, de l'action de G sur X en une action sur Y ; si ce relèvement n'existe pas, on montre dans paragraphe 3C l'existence d'une isogénie minimale $H_Y \to G$ telle que l'action de H_Y puisse être relevée en une action sur Y.

3A. ***Torseur sur un groupe algébrique.*** Pour un groupe algébrique connexe G, tout recouvrement étale fini de $G_{\bar{k}}$ est une extension centrale de $G_{\bar{k}}$ [Brion et Szamuely 2013, Proposition 1.1(1)]. Le résultat suivant généralise ce résultat au corps de base et il est aussi un analogue d'un résultat de Colliot-Thélène [2008, Theorem 5.6].

Proposition 3.1. *Soit G un groupe algébrique connexe, S un k-groupe fini commutatif et $\psi : H \to G$ un S-torseur avec H géométriquement intègre sur k. S'il existe un point $e_H \in H(k)$ avec $\psi(e_H) = e_G$, alors il existe une unique structure de k-groupe algébrique sur H telle que ψ soit un homomorphisme et que e_H soit l'unité.*

De plus, dans ce cas, $\operatorname{Ker}(\psi) = S$ *et l'action de S sur H est compatible avec la multiplication de H.*

Démonstration. L'existence d'une structure de groupe sur H est équivalente à l'existence d'un couple de morphismes (m_H, i_H) satisfaisant certaines relations où $m_H : H \times H \to H$ est la multiplication et $i_H : H \to H$ est l'inverse.

Pour l'unicité, s'il existe deux structures de groupe sur H, soient (m_H, i_H), (m'_H, i'_H) les couples de morphismes correspondants. Soient m_G la multiplication de G et i_G l'inverse de G. Alors

$$\psi \circ m_H = m_G \circ (\psi \times \psi) = \psi \circ m'_H, \quad m_H(e_H \times e_H) = e_H = m'_H(e_H \times e_H),$$
$$\psi \circ i_H = i_G \circ \psi = \psi \circ i'_H, \quad i_H(e_H) = e_H = i'_H(e_H).$$

Puisque ψ est fini étale et $H \times H$ est intègre, on a $m_H = m'_H$ et $i_H = i'_H$ [Milne 1980, Corollary I.3.13]. Ceci donne l'unicité de (m_H, i_H).

Pour l'existence de la structure de groupe (i.e., l'existence de (m_H, i_H)), par la descente galoisienne et l'unicité de (m_H, i_H), il suffit d'établir l'existence de (m_H, i_H) sur $\bar{k}$. On peut supposer que $k = \bar{k}$. Dans ce cas, ψ est fini étale galoisien avec $\mathrm{Aut}(H/G) \cong S(\bar{k})$. D'après [Brion et Szamuely 2013, Proposition 1.1(1)], il existe une structure de groupe sur H telle que $\psi : H \to G$ soit une isogénie centrale. Notons $- \cdot -$ la multiplication et $(-)^{-1}$ l'inverse de cette structure de groupe. Soit $c := e_H \cdot e_H$ et $d := e_H \cdot c^{-1}$. Les points e_H, c et d sont dans $\mathrm{Ker}(\psi)$ et donc dans le centre de H. Alors les morphismes $m'_H : H \times H \to H : (h_1, h_2) \mapsto d \cdot h_1 \cdot h_2$ et $i'_H : H \to H : h \mapsto c \cdot h^{-1}$ définissent sur H une nouvelle structure de groupe et cette structure vérifie les hypothèses ci-dessus.

Pour le dernier énoncé, puisque $S \subset \mathrm{Ker}(\psi)$, l'action de S induit une inclusion de Γ_k-module $S(\bar{k}) \subset \mathrm{Aut}(H_{\bar{k}}/G_{\bar{k}})$ et la multiplication de H induit une inclusion $\mathrm{Ker}(\psi)(\bar{k}) \subset \mathrm{Aut}(H_{\bar{k}}/G_{\bar{k}})$ de Γ_k-module. Puisque $\#\mathrm{Aut}(H_{\bar{k}}/G_{\bar{k}}) = \deg(\psi)$, les deux inclusions ci-dessus sont isomorphes, d'où le résultat. □

Corollaire 3.2. *Soit G un groupe algébrique connexe. Pour tout $\mathbb{Z}/n$-module fini M et tout homomorphisme surjectif $\pi_1(G_{\bar{k}}) \xrightarrow{\theta} M$ de noyau Γ_k-invariant, il existe un unique groupe algébrique connexe H isogène à G, i.e., muni d'un homomorphisme fini surjectif $\psi : H \to G$, tel que $(\mathrm{Ker}(\psi))(\bar{k}) \cong M$ et que la composition $\pi_1(H_{\bar{k}}) \xrightarrow{\psi_{\pi_1}} \pi_1(G_{\bar{k}}) \xrightarrow{\theta} M$ soit nulle.*

De plus, pour tout groupe algébrique connexe H_1, tout homomorphisme fini surjectif $\psi_1 : H_1 \to G$ vérifiant $\theta \circ \psi_{1,\pi_1} = 0$ se factorise par ψ.

Démonstration. Puisque $G(k) \neq \varnothing$, il existe un unique torseur universel de n-torsion $\mathcal{T}_G$ (un S_G-torseur sur G) tel que $\mathcal{T}_G|_{e_G} \cong S_G$.

D'après le corollaire 2.4, il existe un k-groupe fini commutatif S et un S-torseur $H \xrightarrow{\psi} G$ tels que $S(\bar{k}) = M$ et que l'homomorphisme $\pi_1(G_{\bar{k}}) \to S(\bar{k})$ induit par $[H_{\bar{k}}]$ soit θ. Donc la composition $\theta \circ \psi_{\pi_1}$ est nulle. Après avoir tordu par un élément de $H^1(k, S)$, on peut supposer que $[H]|_{e_G} = 0 \in H^1(k, S)$. D'après la proposition 3.1, il existe une structure de groupe sur H telle que ψ soit un homomorphisme et que $\mathrm{Ker}(\psi) = S$.

Pour tout groupe algébrique connexe H_1 et tout homomorphisme fini surjectif $\psi_1 : H_1 \to G$, le noyau ψ_1 est commutatif et on a une suite exacte de Γ_k-modules :

$$\pi_1(H_{1,\bar{k}}) \to \pi_1(G_{\bar{k}}) \to \mathrm{Ker}(\psi_1)(\bar{k}) \to 0.$$

Ceci donne un homomorphisme surjectif de Γ_k-modules $\theta_1 : \mathrm{Ker}(\psi_1)(\bar{k}) \to M \cong S(\bar{k})$ et, puisque $[H_1]|_{e_G} = 0 = [H]|_{e_G}$, on a $\theta_{1,*}([H_1]) = [H] \in H^1(X, S)$. En utilisant l'action de S, on a un $\mathrm{Ker}(\psi_1)$-morphisme $\phi : H_1 \to H$ au-dessus de G tel que $\phi(e_{H_1}) = e_H$. Soient $\chi_1, \chi_2 : H_1 \times H_1 \to H$ deux morphismes avec $\chi_1(h_1, h_2) = \phi(h_1 \cdot h_2)$ et $\chi_2(h_1, h_2) = \phi(h_1) \cdot \phi(h_2)$ pour tous $h_1, h_2 \in H_1$. Alors $\chi_1(e_{H_1}, e_{H_1}) = \chi_2(e_{H_1}, e_{H_1})$ et $\psi \circ \chi_1 = \psi \circ \chi_2$. Ceci induit :

$$\chi : H_1 \times_k H_1 \xrightarrow{\chi_1, \chi_2} H \times_G H \cong H \times_k S \xrightarrow{p_2} S.$$

Puisque H_1 est connexe, on a $\mathrm{Im}(\chi) = e_S$, $\chi_1 = \chi_2$ et ϕ est un homomorphisme. □

3B. ***Relèvement d'une action par un torseur.*** Soient G un groupe algébrique connexe et (X, ρ) une G-variété lisse géométriquement intègre. Soient F un k-groupe fini et $f : Y \to X$ un F-torseur. Notons $p_1 : G \times X \to G$, $p_2 : G \times X \to X$ les deux projections.

D'après [SGA 1 1971, X.2.2], on a deux suites exactes de groupes fondamentaux

$$1 \to \pi_1(X_{\bar{k}}) \to \pi_1(X) \to \Gamma_k \to 1 \quad \text{et} \quad 1 \to \pi_1((G \times X)_{\bar{k}}) \to \pi_1(G \times X) \to \Gamma_k \to 1.$$

D'après [SGA 1 1971, XII.5.2], on a $\pi_1((G \times X)_{\bar{k}}) \cong \pi_1(G_{\bar{k}}) \times \pi_1(X_{\bar{k}})$, car ceci vaut pour les espaces topologiques. Alors on a une suite exacte de groupes fondamentaux :

$$1 \to \pi_1(G_{\bar{k}}) \to \pi_1(G \times X) \xrightarrow{p_{2,\pi_1}} \pi_1(X) \to 1$$

qui admet une section induite par $i_e : X \to G \times X : x \mapsto (e_G, x)$ et l'action de $\pi_1(X)$ sur $\pi_1(G_{\bar{k}})$ se factorise par Γ_k. D'après (1-5), cette suite exacte induit une suite exacte d'ensembles pointés (voir [Serre 1964, §5.8])

$$1 \to H^1(X, F) \xrightarrow{p_2^*} H^1(G \times X, F) \xrightarrow{\iota} H^1(G_{\bar{k}}, F)^{\Gamma_k} \tag{3-1}$$

et p_2^* admet une section induite par i_e^*.

Proposition 3.3. *Soient G un groupe algébrique connexe et (X, ρ) une G-variété lisse géométriquement intègre. Soient F un k-groupe fini et $f : Y \to X$ un F-torseur. Alors les hypothèses ci-dessous sont équivalentes :*

(a) *on a* $\rho^*([Y]) = p_2^*([Y]) \in H^1(G \times X, F)$;

(b) *pour ι dans* (3-1), *on a* $\iota(\rho^*([Y])) = 0 \in H^1(G_{\bar{k}}, F)$;

(c) *le F-torseur Y est G-compatible, i.e., l'action de G sur X se relève en une action sur Y ;*

(d) *il existe un morphisme $\rho_Y : G \times Y \to Y$ tel que $\rho_Y|_{e_G \times Y} = \mathrm{id}_Y$ et que ρ_Y soit compatible avec ρ, i.e., $\rho \circ (\mathrm{id}_G \times f) = f \circ \rho_Y$.*

De plus, sous les hypothèses ci-dessus, on a

(1) *l'action de G sur Y pour laquelle f est un G-morphisme est unique* ;

(2) *l'action de G et celle de F commutent* ;

(3) *pour tout $\sigma \in H^1(k, F)$, le F_σ-torseur Y_σ est G-compatible.*

Démonstration. Puisque $i_e^*(p_2^*([Y])) = i_e^*(\rho^*([Y]))$ dans $H^1(X, F)$, l'équivalence (a)⇔(b) découle de la suite exacte (3-1).

Lemme 3.4. *Pour tout k-schéma de type fini Z et tous morphismes $\theta_1, \theta_2 : G \times Z \to Y$, si $f \circ \theta_1 = f \circ \theta_2$ et $\theta_1|_{e_G \times Z} = \theta_2|_{e_G \times Z}$, alors $\theta_1 = \theta_2$.*

Démonstration. En fait, θ_1, θ_2 induisent un morphisme

$$\theta : G \times Z \xrightarrow{(\theta_1,\theta_2)} Y \times_X Y \cong Y \times_k F \xrightarrow{\mathrm{pr}_F} F$$

tel que $\theta(e_G \times Z) = e_F$. Puisque G est intègre, $\theta(G \times Z) = e_F$ et donc $\theta_1 = \theta_2$. □

Pour (a)⇒(d), soient ρ^*Y le pullback de Y par ρ et $p_2^*Y := G \times Y$. Notons $\mathrm{Mor}_F(p_2^*Y, F)$ l'ensemble des morphismes $\chi : p_2^*Y \to F$ tels que $\chi(a \cdot y) = a \cdot \chi(y) \cdot a^{-1}$ pour tous $a \in F$ et $y \in p_2^*Y$. Définissons de même $\mathrm{Mor}_F(Y, F)$. Alors $Y \cong e_G \times Y \subset p_2^*Y$ induit un morphisme surjectif $\mathrm{Mor}_F(p_2^*Y, F) \xrightarrow{\mathrm{Mor}(i_e)} \mathrm{Mor}_F(Y, F)$, car il existe une section induite par p_2. Par hypothèse, on a un isomorphisme de F-torseur $p_2^*Y \xrightarrow{\phi} \rho^*Y$. Pour tout isomorphisme ϕ_1, l'argument classique montre qu'il existe un $\chi_1 \in \mathrm{Mor}_F(p_2^*Y, F)$ tel que $\phi_1 = \chi_1 \cdot \phi$. Puisque $\mathrm{Mor}(i_e)$ est surjectif, on peut supposer que $\phi|_{e_G \times X}$ est l'identité de Y. Le morphisme $\rho_Y : G \times Y \xrightarrow{\phi} \rho^*Y \to Y$ donne (d).

Pour (d)⇒(c), l'hypothèse (d) donne un diagramme commutatif :

$$\begin{tikzcd}
\mathrm{id}_Y : & e_G \times Y \arrow[r, "i_{e,Y}"] \arrow[d, "f"] & G \times Y \arrow[r, "\rho_Y"] \arrow[d, "\mathrm{id}_G \times f"] & Y \arrow[d, "f"] \\
\mathrm{id}_X : & e_G \times X \arrow[r, "i_e"] & G \times X \arrow[r, "\rho"] & X
\end{tikzcd} \tag{3-2}$$

tel que $\rho_Y \circ i_{e,Y} = \mathrm{id}_Y$. Soient $\theta_1, \theta_2 : G \times G \times Y \to Y$ les deux morphismes définis par

$$\theta_1(g_1, g_2, y) = g_1 \cdot (g_2 \cdot y) \quad \text{et} \quad \theta_2(g_1, g_2, y) = (g_1 \cdot g_2) \cdot y$$

pour tous $g_1, g_2 \in G$ et $y \in Y$. Alors $\theta_1(e_G, g_2, y) = \theta_2(e_G, g_2, y)$ et le lemme 3.4 montre que $\theta_1 = \theta_2$. Donc ρ_Y est une action et f est un G-morphisme. Ceci donne (c).

Supposons (c) et montrons (1), (2), (3) et (a).

L'hypothèse (c) donne aussi le diagramme commutatif (3-2) avec ρ_Y l'action relevée de G sur Y.

Soient θ_1, θ_2 deux actions de G sur Y telles que f soit un G-morphisme. Puisque $f \circ \theta_1 = \rho \circ (\mathrm{id}_G \times f) = f \circ \theta_2$, On applique le lemme 3.4 à $\theta_1, \theta_2 : G \times Y \to Y$ et on obtient (1).

Soient $\theta_1, \theta_2 : G \times F \times Y \to Y$ les deux morphismes définis par

$$\theta_1(g, a, y) = g \cdot (a \cdot y) \quad \text{et} \quad \theta_2(g, a, y) = a \cdot (g \cdot y)$$

pour tous $g \in G$, $a \in F$ et $y \in Y$. Alors

$$\theta_1(e_G, a, y) = a \cdot y = \theta_2(e_G, a, y) \quad \text{et} \quad (f \circ \theta_1)(g, a, y) = g \cdot f(y) = (f \circ \theta_2)(g, a, y).$$

On applique le lemme 3.4 à $\theta_1, \theta_2 : G \times F \times Y \to Y$ et on obtient (2).

Pour le F-torseur $p_2^*([Y]) = (G \times Y \to G \times X)$, l'énoncé (2) montre que l'action $G \times Y \to Y$ est un F-morphisme compatible avec ρ. Ceci induit un isomorphisme de F-torseurs $p_2^*([Y]) = \rho^*([Y])$ et on a (a).

Puisque l'énoncé (b) est un énoncé sur $\bar{k}$, on obtient (3). □

Corollaire 3.5. *Soient G un groupe algébrique connexe et (X, ρ) une G-variété lisse géométriquement intègre. Alors ρ induit un homomorphisme $\rho_{\pi_1} : \pi_1(G_{\bar{k}}) \to \pi_1(X)$ et, pour tout k-groupe fini F, il induit $\rho^*_{\pi_1} : H^1(X, F) \to H^1(G_{\bar{k}}, F)$ et on a :*

(1) *le sous-groupe* $\mathrm{Im}(\rho_{\pi_1}) \subset \pi_1(X)$ *est normal et il est contenu dans le centre de* $\pi_1(X_{\bar{k}})$;

(2) *pour tout* $\alpha \in H^1(X, F)$, *on a* $\rho^*_{\pi_1}(\alpha) = \iota(\rho^*(\alpha))$, *où* ι *est dans* (3-1) ;

(3) *pour tout* 1*-cocycle* a *de* $\pi_1(X)$ *à valeurs dans* $F(\bar{k})$, *l'homomorphisme* $a \circ \rho_{\pi_1} : \pi_1(G_{\bar{k}}) \to F(\bar{k})$ *est de noyau* Γ_k*-invariant, et il est nul si et seulement si* $\rho^*_{\pi_1}([a]) = 0$;

(4) *si X est un G-espace homogène à stabilisateur géométrique connexe, alors tout F-torseur G-compatible est constant, i.e., ce torseur est isomorphe à $M \times_k X$ avec M un F-torseur sur k.*

Démonstration. L'énoncé (1) vaut car

$$\pi_1(G_{\bar{k}}) = \mathrm{Ker}\big(\pi_1(G \times X) \xrightarrow{p_{2,*}} \pi_1(X)\big) \quad \text{et} \quad \pi_1((G \times X)_{\bar{k}}) \cong \pi_1(G_{\bar{k}}) \times \pi_1(X_{\bar{k}}).$$

Les énoncés (2) et (3) découlent par définition.

Pour (4), dans ce cas, $\mathrm{Im}(\rho_{\pi_1}) = \pi_1(X_{\bar{k}})$ [Szamuely 2009, Proposition 5.5.4]. D'après la proposition 3.3 et (2), (3) ci-dessus, tout F-torseur G-compatible est trivial sur $X_{\bar{k}}$, et donc il provient d'un F-torseur sur k. □

Corollaire 3.6. *Sous les notations et les hypothèses ci-dessus, supposons que f est G-compatible. Alors, pour tout k-schéma fini étale E, la restriction de Weil $V := R_{X \times E/X}(Y \times E)$ est un $R_{E/k}(F \times_k E)$-torseur G-compatible sur X.*

Démonstration. Notons $f_V : V \to X$. Par hypothèse, f_V est un torseur sous le groupe

$$R_{X \times E/X}(F \times X \times E) \cong R_{E/k}(F \times_k E).$$

On considère $G \times V$ comme un X-schéma par le morphisme $G \times V \xrightarrow{\mathrm{id}_G \times f_V} G \times X \xrightarrow{\rho} X$ et $G \times Y$ comme un X-schéma par $\rho \circ (\mathrm{id}_G \times f)$. Dans ce cas, tout morphisme $\rho_V \in \mathrm{Mor}_X(G \times V, V)$ satisfait $f_V \circ \rho_V = \rho \circ (\mathrm{id}_G \times f_V)$. D'après la proposition 3.3(d), il suffit de trouver un $\rho_V \in \mathrm{Mor}_X(G \times V, V)$ tel que $\rho_V|_{e_G \times V} = \mathrm{id}_V$. Puisque

$$\mathrm{Mor}_X(V, V) \xrightarrow{\sim} \mathrm{Mor}_{X \times E}(V \times E, Y \times E) \quad \text{et que} \quad \mathrm{Mor}_X(G \times V, V) \xrightarrow{\sim} \mathrm{Mor}_{X \times E}(G \times V \times E, Y \times E),$$

l'identité id_V induit un morphisme $V \times E \xrightarrow{\theta} Y \times E$. Le $X \times E$-morphisme

$$G \times V \times E \xrightarrow{\mathrm{id}_G \times \theta} G \times Y \times E \xrightarrow{\rho_Y \times \mathrm{id}_E} Y \times E$$

induit un morphisme $\rho_V \in \mathrm{Mor}_X(G \times V, V)$ qui satisfait $\rho_V|_{e_G \times V} = \mathrm{id}_V$. □

Corollaire 3.7. *Soient G un groupe algébrique connexe, Z une variété lisse géométriquement intègre et $p : X \to Z$ un G-torseur. Pour tout k-groupe fini F et tout F-torseur G-compatible $Y \to X$, il existe un F-torseur Y_Z sur Z tel que $[Y] = p^*([Y_Z]) \in H^1(X, F)$.*

Démonstration. D'après la proposition 3.3(2), Y est un $G\times F$-torseur sur Z tel que $Y/F = X$. Alors $Y_Z := Y/G$ est un F-torseur sur Z et $Y \to Y_Z$ est un F-morphisme. Donc $[Y] = p^*([Y_Z])$. □

3C. ***Le groupe minimal compatible avec un torseur.*** Soit G un groupe algébrique connexe. Soit $\mathcal{C}_G$ la catégorie des groupes algébriques connexes H isogènes à G, i.e., munis d'un homomorphisme fini surjectif $\psi : H \to G$. C'est clair que si G est linéaire, tout objet dans $\mathcal{C}_G$ est aussi linéaire.

Soit (X, ρ) une G-variété lisse géométriquement intègre. Soient F un k-groupe fini et $f : Y \to X$ un F-torseur. Soit $\mathcal{C}_G(Y)$ la sous-catégorie pleine de $\mathcal{C}_G$ dont les objets sont les groupes H isogènes à G tels que f soit H-compatible. D'après la proposition 3.3(1), tout objet $H \in \mathcal{C}_G(Y)$ admet une unique action sur Y telle que f soit un H-morphisme. Alors tout morphisme de $\mathcal{C}_G(Y)$ est compatible avec les actions ci-dessus.

Proposition 3.8. *La catégorie $\mathcal{C}_G(Y)$ admet un objet final $(H_Y \xrightarrow{\psi_Y} G)$, et un objet $(H \xrightarrow{\psi} G) \in \mathcal{C}_G(Y)$ est final si et seulement si l'action de* $\ker(\psi)$ *sur Y est libre.*

Démonstration. Dans la suite exacte (3-1), notons $\alpha := \iota(\rho^*([Y])) \in H^1(G_{\bar{k}}, F)^{\pi_1(X)}$. Soit

$$\theta \in \mathrm{Hom}_{\mathrm{cont}}(\pi_1(G_{\bar{k}}), F(\bar{k}))$$

un élément correspondant à α selon (1-5). D'après le corollaire 3.5(3), le noyau $\mathrm{Ker}(\theta)$ est Γ_k-invariant.

La fonctorialité de (3-1) et la proposition 3.3 montrent qu'un objet $(H \xrightarrow{\psi} G) \in \mathcal{C}_G$ est contenu dans $\mathcal{C}_G(Y)$ si et seulement si $\psi_*(\alpha) = 0 \in H^1(H_{\bar{k}}, F)$, i.e., $\theta \circ \psi_{\pi_1} = 0$ (corollaire 3.5(3)), où $\psi_{\pi_1} : \pi_1(H_{\bar{k}}) \to \pi_1(G_{\bar{k}})$. Puisque $\pi_1(G_{\bar{k}})$ est abélien [Miyanishi 1972, Theorem 1], le corollaire 3.2 implique l'existence de l'objet final de $\mathcal{C}_G(Y)$.

L'argument ci-dessus montre que la catégorie $\mathcal{C}_G(Y)$ est stable par changement de base, i.e., pour toute G-variété X' et tout G-morphisme $X' \to X$, on a un F-torseur $Y' := Y \times_X X' \to X'$ et $\mathcal{C}_G(Y') = \mathcal{C}_G(Y)$ comme sous-catégories de $\mathcal{C}_G$.

Soit $(H_Y \xrightarrow{\psi_Y} G)$ l'objet final de $\mathcal{C}_G(Y)$. Il est l'objet final de $\mathcal{C}_G(Y')$ aussi pour tout $Y' \to X'$ ci-dessus.

Pour montrer que l'action de $\mathrm{Ker}(\psi_Y)$ est libre, on peut supposer que $k = \bar{k}$ et que X est un espace homogène de G. Dans ce cas, Y est un espace homogène de $F \times H_Y$ (proposition 3.3(2)). Puisque $\mathrm{Ker}(\psi_Y)$ est dans le centre de $F \times H_Y$, les stabilisateurs de $\mathrm{Ker}(\psi_Y)$ en tous les points $x \in X$ sont les mêmes. La propriété de l'objet final implique que l'action de $\mathrm{Ker}(\psi_Y)$ soit libre.

Soit $(H \xrightarrow{\psi} G) \in \mathcal{C}_G(Y)$ un objet tel que l'action de $\ker(\psi)$ sur Y est libre. Soit $\phi : H \to H_Y$ l'homomorphisme canonique. Puisque ψ_Y, ψ sont finis surjectifs et que H_Y est connexe, l'homomorphisme ϕ est fini surjectif. La proposition 3.3(1) implique que ϕ est compatible avec l'action de H et de H_Y. Puisque l'action de $\mathrm{Ker}(\psi)$ sur Y est libre, ϕ est un isomorphisme. □

Définition 3.9. L'objet final $(H_Y \xrightarrow{\psi_Y} G)$ de $\mathcal{C}_G(Y)$ est appelé *le groupe minimal compatible avec le F-torseur Y.*

Remarque 3.10. Soit $\rho_{\pi_1} : \pi_1(G_{\bar{k}}) \to \pi_1(X)$ l'homomorphisme dans le corollaire 3.5 et soit α un 1-cocycle de $\pi_1(X)$ en $F(\bar{k})$ qui correspond à $[Y] \in H^1(X, F)$. Alors $\alpha|_{\pi_1(X_{\bar{k}})}$ est un homomorphisme.

Par la démonstration de la proposition 3.8, le groupe minimal compatible au F-torseur Y est déterminé par $\mathrm{Ker}(\alpha \circ \rho_{\pi_1})$, où $\alpha \circ \rho_{\pi_1} : \pi_1(G_{\bar{k}}) \to F(\bar{k})$ est un homomorphisme. Donc ceci est déterminé par $\mathrm{Ker}(\alpha|_{\mathrm{Im}(\rho_{\pi_1})})$.

D'après la proposition 3.3(3), H_Y est aussi le groupe minimal compatible au F_σ-torseur Y_σ pour tout $\sigma \in H^1(k, F)$.

Corollaire 3.11. *Sous les notations et les hypothèses ci-dessus, si Y est géométriquement intègre sur k, alors il existe un homomorphisme injectif $\phi : \mathrm{Ker}(\psi_Y) \to F$ d'image centrale compatible avec l'action de $\mathrm{Ker}(\psi_Y)$ et de F sur Y.*

Démonstration. L'action de $\mathrm{Ker}(\psi_Y)$ induit un morphisme :

$$\Phi : \mathrm{Ker}(\psi_Y) \times Y \xrightarrow{\rho_{H_Y}, \mathrm{pr}_Y} Y \times_X Y \xrightarrow{\sim} F \times_k Y \xrightarrow{\mathrm{pr}_F} F,$$

où ρ_{H_Y} est l'action de H_Y. Pour tous $h \in \mathrm{Ker}(\psi_Y)$, $y \in Y$, on a $h \cdot y = \Phi(h, y) \cdot y$.

Puisque Y est géométriquement intègre, il existe un morphisme $\phi : \mathrm{Ker}(\psi_Y) \to F$ tel que $\Phi = \phi \circ p_1$, où $p_1 : \mathrm{Ker}(\psi_Y) \times Y \to \mathrm{Ker}(\psi_Y)$ est la projection. Puisque l'action de F sur Y est libre, ϕ est un homomorphisme. La proposition 3.3(2) implique que l'image de ϕ est centrale. D'après la proposition 3.8, l'action de $\mathrm{Ker}(\psi_Y)$ est libre et donc ϕ est injectif. □

Rappelons la définition de $\mathrm{Br}_G(X)$ dans la définition 1.3.

Proposition 3.12. *Soient G un groupe algébrique connexe et X une G-variété lisse géométriquement intègre. Supposons qu'il existe un torseur universel de n-torsion $\mathcal{T}_X \xrightarrow{f} X$ sous le groupe S_X. Soit $H \xrightarrow{\psi} G$ le groupe minimal compatible au S_X-torseur $\mathcal{T}_X$. Alors, pour tout élément de n-torsion $\alpha \in \mathrm{Br}(X)$ et tout $\sigma \in H^1(k, S_X)$, on a $f_\sigma^*(\alpha) \in \mathrm{Br}_H(\mathcal{T}_{X,\sigma})$, où $f_\sigma^* : \mathrm{Br}(X) \to \mathrm{Br}(\mathcal{T}_{X,\sigma})$ est l'homomorphisme induit par $f_\sigma : \mathcal{T}_{X,\sigma} \to X$.*

Démonstration. On peut supposer que $\sigma = 0 \in H^1(k, S_X)$.

Notons $\rho_H : H \times \mathcal{T}_X \to \mathcal{T}_X$ l'action de H et $p_{1,H} : H \times \mathcal{T}_X \to H$, $p_{2,H} : H \times \mathcal{T}_X \to \mathcal{T}_X$ les deux projections. Soit $\mathcal{T}_G$ un torseur universel de n-torsion pour G sous le groupe S_G.

Appliquant le corollaire 2.7 à (G, X), on obtient : pour tout $\alpha_1 \in H^2(X, \mu_n)$, il existe un $\phi \in \mathrm{Hom}(S_G, S_X^*)$ et un $\beta \in H^2(G, \mu_n)$ tels que $(\rho^* - p_2^*)(\alpha_1) = \varepsilon(\phi) + p_1^*(\beta)$.

Puisque $f^*([\mathcal{T}_X]) = 0 \in H^1(\mathcal{T}_X, S_X)$, on a

$$(\psi \times f)^*(\varepsilon(\phi)) = (\psi \times f)^*(\phi_*([\mathcal{T}_G]) \cup [\mathcal{T}_X]) = \phi_*(\psi^*([\mathcal{T}_G])) \cup f^*([\mathcal{T}_X]) = 0.$$

Alors $(\rho_H^* - p_{2,H}^*)(f^*(\alpha_1)) = (\psi \times f)^*((\rho^* - p_2^*)(\alpha_1)) = (\psi \times f)^*(p_1^*(\beta)) = p_{1,H}^*(\psi^*(\beta))$.

D'après la suite exacte de Kummer, $(\rho_H^* - p_{2,H}^*)(f^*(\alpha)) \subset p_{1,H}^*\mathrm{Br}(H)$, d'où le résultat. □

4. Rappel sur le sous-groupe de Brauer invariant

Dans toute cette section, k est un corps quelconque de caractéristique 0. Sauf mention explicite du contraire, une variété est une k-variété.

Dans cette section, on rappelle des notions et des résultats dans [Cao 2018, §3] sur le sous-groupe de Brauer invariant.

Pour la définition du sous-groupe de Brauer invariant on renvoie le lecteur à la définition 1.3.

Soit **AB** la catégorie des groupes abéliens. Soit **GX** la catégorie des couples (G, X) avec G un groupe algébrique connexe et X une G-variété lisse, et un morphisme $(H, Y) \to (G, X)$ dans **GX** est un couple (ψ, f) avec $\psi : H \to G$ un homomorphisme et $f : Y \to X$ un H-morphisme, où l'action de H sur X est induite par ψ. Par définition,

$$\mathrm{Br}_{-}(-) : \mathbf{GX} \to \mathbf{AB} : (G, X) \mapsto \mathrm{Br}_G(X)$$

est un foncteur contravariant.

Exemple 4.1. (1) [Cao 2018, lemme 3.6] Soit G un groupe linéaire connexe. Alors $\mathrm{Br}_G(G) = \mathrm{Br}_1(G)$.

(2) [Cao 2018, proposition 3.9(3)] Soient G un groupe linéaire connexe, $G_0 \subset G$ un sous-groupe fermé connexe et $X := G/G_0$. Alors

$$\mathrm{Br}_G(X) = \mathrm{Br}_1(X, G) := \ker(\mathrm{Br}(X) \to \mathrm{Br}(G_{\bar{k}})).$$

Le groupe $\mathrm{Br}_1(X, G)$ est défini par Borovoi et Demarche [2013] pour étudier l'approximation forte de X.

(3) Soit A une variété abélienne. L'auteur ne sait pas identifier le groupe $\mathrm{Br}_A(A)$. Par exemple, l'auteur ne sait pas si $\mathrm{Br}_A(A) \subset \mathrm{Br}_1(A)$ ou si $\mathrm{Br}_A(A) \supset \mathrm{Br}_1(A)$.

Au vu de l'exemple 4.1(3), dans la suite du présent article, on suppose que G est un groupe linéaire.

Soient G un groupe linéaire connexe et X une G-variété lisse géométriquement intègre. Notons $\rho : G \times X \to X$ l'action et $p_1 : G \times X \to G$, $p_2 : G \times X \to X$ les deux projections.

(1) Puisque $\mathrm{Br}_1(G \times X) \cong \mathrm{Br}_e(G) \oplus \mathrm{Br}_1(X)$ [Sansuc 1981, lemme 6.6], on peut obtenir facilement [Cao 2018, proposition 3.2(4)] :

$$\mathrm{Br}_1(X) \subset \mathrm{Br}_G(X). \tag{4-1}$$

(2) Puisque $p_1^*|_{\mathrm{Br}_e(G)} : \mathrm{Br}_e(G) \to \mathrm{Br}(G \times X)$ est injectif, par la définition de $\mathrm{Br}_G(X)$, il existe un unique homomorphisme $\mathrm{Br}_G(X) \xrightarrow{\lambda} \mathrm{Br}_e(G)$ tel que [Cao 2018, (3.4)]

$$p_1^* \circ \lambda = \rho^* - p_2^* : \mathrm{Br}_G(X) \to \mathrm{Br}(G \times X).$$

Le $\lambda : \mathrm{Br}_G(X) \to \mathrm{Br}_e(G)$ est appelé *l'homomorphisme de Sansuc* [Cao 2018, définition 3.8].

(3) Pour toute extension de corps K/k, et tous $x \in X(K)$, $g \in G(K)$, $\alpha \in \mathrm{Br}_G(X)$, on a [Cao 2018, proposition 3.9(1)] :

$$(g \cdot x)^*(\alpha) = g^*(\lambda(\alpha)) + x^*(\alpha) \in \mathrm{Br}(K).$$

Alors, dans le cas où k est un corps de nombres, on a :

$$G(\boldsymbol{A}_k)^{\mathrm{Br}_a(G)} \cdot X(\boldsymbol{A}_k)^{\mathrm{Br}_G(X)} = X(\boldsymbol{A}_k)^{\mathrm{Br}_G(X)}. \tag{4-2}$$

La formule (4-1) et [Harari et Skorobogatov 2013, Corollary 3.6] impliquent directement :

Corollaire 4.2. *Soit $(G, X) \in \mathbf{GX}$ un objet. Si $X(\mathbf{A}_k)^{\mathrm{Br}_G(X)} \neq \varnothing$, alors, pour tout entier $n \geq 2$, il existe un torseur universel de n-torsion pour X.*

Pour un torseur sous un groupe linéaire connexe, Sansuc a construit une suite exacte dans [Sansuc 1981, proposition 6.10], qui est appelée *la suite exacte de Sansuc*. La proposition suivante dit que les sous-groupes de Brauer invariant sont compatibles avec la suite exacte de Sansuc.

Proposition 4.3 [Cao 2018, corollaire 3.11(2)]. *Soit $1 \to N \to H \xrightarrow{\psi} G \to 1$ une suite exacte de groupes linéaires connexes. Soit $(\psi, f) : (H, Y) \to (G, X)$ un morphisme dans $\mathbf{GX}$ tel que X soit géométriquement intègre sur k et $Y \to X$ soit un N-torseur, où l'action de N sur Y est induite par celle de H. Alors $f^* : \mathrm{Br}(X) \to \mathrm{Br}(Y)$ satisfait $(f^*)^{-1}\mathrm{Br}_H(Y) = \mathrm{Br}_G(X)$ et on a une suite exacte, fonctorielle en (X, Y, f, N) :*

$$\mathrm{Pic}(Y) \to \mathrm{Pic}(N) \to \mathrm{Br}_G(X) \xrightarrow{f^*} \mathrm{Br}_H(Y) \xrightarrow{\lambda} \mathrm{Br}_e(N),$$

où $\lambda : \mathrm{Br}_H(Y) \subset \mathrm{Br}_N(Y) \to \mathrm{Br}_e(N)$ est l'homomorphisme de Sansuc.

Pour une fibration $f : X \to T$ et tout $t \in T(k)$, on note $i_t : X_t \subset X$ la fibre et on a la spécialisation du groupe de Brauer $i_t^* : \mathrm{Br}(X) \to \mathrm{Br}(X_t)$. La proposition suivante dit que, si la fibration f est compatible avec des actions des groupes linéaires, alors les sous-groupes de Brauer invariants sont compatibles avec la spécialisation du groupe de Brauer.

Proposition 4.4 [Cao 2018, proposition 3.13]. *Soit $1 \to G_0 \xrightarrow{\phi} G \xrightarrow{\psi} T \to 1$ une suite exacte de groupes linéaires connexes avec T un tore. Soient X une G-variété lisse géométriquement intègre et $X \xrightarrow{f} T$ un G-morphisme. Notons $\mathrm{Br}_1(G) \xrightarrow{\phi_*} \mathrm{Br}_1(G_0)$ l'homomorphisme induit par ϕ. Alors, pour tout $t \in T(k)$, on a*

(1) *la fibre $i_t : X_t \subset X$ est G_0-invariante* ;

(2) *on a une suite exacte naturelle*

$$\mathrm{Br}_e(T) \to \mathrm{Br}_G(X) \xrightarrow{i_t^*} \mathrm{Br}_{G_0}(X_t) \to \mathrm{coker}(\phi_*);$$

(3) [Cao 2018, lemme 5.5] *si k est un corps de nombres et $H^3(k, T^*) = 0$, on a $\mathrm{coker}(\phi_*) = 0$ et i_t^* est surjectif.*

5. La descente par rapport au sous-groupe de Brauer invariant

Dans toute cette section, k est un corps de nombres. Sauf mention explicite du contraire, une variété est une k-variété.

La méthode de descente des points adéliques est établie par Colliot-Thélène et Sansuc [1987a]. Dans [Cao 2018], l'auteur étudie la méthode de descente des points adéliques orthogonaux aux sous-groupes de Brauer invariants et établit le résultat : pour un groupe linéaire connexe G, une variété lisse géométriquement intègre Z et un G-torseur $p : X \to Z$,

(1) on a [Cao 2018, théorème 5.9] :

$$Z(\boldsymbol{A}_k)^{\mathrm{Br}(Z)} = \bigcup_{\sigma \in H^1(k,G)} p_\sigma\big(X_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(X_\sigma)}\big); \tag{5-1}$$

(2) si G est un tore quasi-trivial, on a [Cao 2018, proposition 5.2]

$$Z(\boldsymbol{A}_k)^{(p^*)^{-1}B} = p(X(\boldsymbol{A}_k)^B), \tag{5-2}$$

pour tout sous-groupe $B \subset \mathrm{Br}_G(X)$, où $p^* : \mathrm{Br}(Z) \to \mathrm{Br}(X)$;

(3) pour tout homomorphisme surjectif $\psi : H \to G$ de groupes linéaires connexes, on a [Cao et al. 2019b, Theorem 5.1] :

$$G(\boldsymbol{A}_k)^{\mathrm{Br}_1(G)} = \psi(H(\boldsymbol{A}_k)^{\mathrm{Br}_1(H)}) \cdot G(k). \tag{5-3}$$

La proposition 5.1 et la proposition 5.5 suivantes sont quelques variantes de ce résultat. Plus précisément, la proposition 5.1 est une variante de (2) pour G un groupe fini commutatif et sa démonstration utilise (2) et (3) mais pas (1). La proposition 5.5 est une variante de (1) en remplaçant “Br” par “ét, Br” et en remplaçant “Br_G” par “G-ét, Br_G”, donc elle est une version limite de (1) pour tout k-torseur $Z' \to Z$ sous un k-groupe fini, et sa démonstration utilise (1) mais pas (2) et (3).

Proposition 5.1. *Soient G, H deux groupes linéaires connexes et $\psi : H \to G$ un homomorphisme surjectif de noyau S fini. Soient X* (resp. *Y*) *une G-variété* (resp. H-variété) *lisse géométriquement intègre et $f : Y \to X$ un H-morphisme tels que Y soit un S-torseur sur X, où l'action de S est induite par l'action de H. Alors, pour tout $\sigma \in H^1(k, S)$, le tordu Y_σ est une H-variété et on a* :

$$X(\boldsymbol{A}_k)^{\mathrm{Br}_G(X)} = \bigcup_{\sigma \in H^1(k,S)} f_\sigma\big(Y_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_H(Y_\sigma)}\big).$$

Démonstration. On construira les diagrammes ci-dessous

$$\begin{tikzcd}
0 \arrow[r] & S \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner"] & T_0 \arrow[r, "\varphi"] \arrow[d] & T \arrow[r] \arrow[d, "="] & 0 \\
& H \arrow[r] \arrow[dr, "\psi"'] & H_0 \arrow[r] \arrow[d, "\psi_0"] & T & \\
& & G & &
\end{tikzcd}$$

et

$$\begin{tikzcd}
Y \arrow[r, "i"] \arrow[dr, "f"'] & Y_0 \arrow[r, "\phi"] \arrow[d, "f_0"] & T \\
& X &
\end{tikzcd}$$

où le diagramme à gauche est un diagramme de groupes algébriques, le diagramme à droite est un diagramme de variétés lisses, chaque groupe dans le diagramme à gauche agit sur la variété dans le diagramme à droite avec le même position et ces actions sont compatibles avec tous les morphismes.

Puisque H est connexe, S est contenu dans le centre de H. Donc S est commutatif. Une résolution coflasque [Colliot-Thélène et Sansuc 1987b, Proposition 1.3] induit une suite exacte

$$0 \to S \to T_0 \xrightarrow{\varphi} T \to 0 \tag{5-4}$$

où T_0 est un tore quasi-trivial et T est un tore coflasque, i.e., $H^1(k', T^*) = 0$ pour toute extension k'/k. Puisque $H^3(k, T^*) \cong \prod_{v\in\infty_k} H^3(k_v, T^*) \cong \prod_{v\in\infty_k} H^1(k_v, T^*)$ [Cao 2018, lemme 5.4], on a $H^3(k, T^*) = 0$.

Soit $H_0 := H \times^S T_0$. Alors H_0 est un groupe linéaire connexe et $H \xrightarrow{\psi} G$ induit une suite exacte

$$1 \to T_0 \to H_0 \xrightarrow{\psi_0} G \to 1.$$

Soit $Y_0 := Y \times^S T_0$. Notons $i : Y \to Y_0$ l'immersion fermée canonique. Alors Y_0 est une H_0-variété et f induit un H_0-morphisme $Y_0 \xrightarrow{f_0} X$ tels que f_0 est un T_0-torseur. D'après (5-2) et la proposition 4.3, on a

$$X(\boldsymbol{A}_k)^{\mathrm{Br}_G(X)} = f_0(Y_0(\boldsymbol{A}_k)^{\mathrm{Br}_{H_0}(Y_0)}).$$

L'isomorphisme $Y_0 \times^{T_0} T \cong Y \times^S T_0 \times^{T_0} T \cong X \times T$ induit un T_0-morphisme $\phi : Y_0 \to T$ tel que $\phi^{-1}(e_T) = i(Y)$. D'après des arguments classiques (voir la démonstration de [Cao 2018, théorème 5.9]), pour tout $t \in T(k)$, on a $\phi^{-1}(t) \cong Y_{\partial(t)}$ et le morphisme $\phi^{-1}(t) \hookrightarrow Y_0 \xrightarrow{f_0} X$ est exactement $f_{\partial(t)}$, où $\partial : T(k) \to H^1(k, S)$ est l'homomorphisme induit par (5-4). Puisque $H^3(k, T^*) = 0$, d'après la proposition 4.4, $\phi^{-1}(t)$ est une H-variété et l'homomorphisme canonique $\mathrm{Br}_{H_0}(Y_0) \to \mathrm{Br}_H(\phi^{-1}(t))$ est surjectif pour tout $t \in T(k)$.

D'après (4-2), $Y_0(\boldsymbol{A}_k)^{\mathrm{Br}_{H_0}(Y_0)}$ est $T_0(\boldsymbol{A}_k)^{\mathrm{Br}_1(T_0)}$-invariant. On applique (5-3) à φ et on a

$$T(\boldsymbol{A}_k)^{\mathrm{Br}_1(T)} = \varphi(T_0(\boldsymbol{A}_k)^{\mathrm{Br}_1(T_0)}) \cdot T(k).$$

Puisque $\phi(Y_0(\boldsymbol{A}_k)^{\mathrm{Br}_{H_0}(Y_0)}) \subset T(\boldsymbol{A}_k)^{\mathrm{Br}_1(T)}$, on a :

$$Y_0(\boldsymbol{A}_k)^{\mathrm{Br}_{H_0}(Y_0)} = T_0(\boldsymbol{A}_k)^{\mathrm{Br}_1(T_0)} \cdot \Bigl(\bigsqcup_{t\in T(k)} \phi^{-1}(t)(\boldsymbol{A}_k)^{\mathrm{Br}_H(\phi^{-1}(t))}\Bigr),$$

et donc

$$X(\boldsymbol{A}_k)^{\mathrm{Br}_G(X)} = f_0\Bigl[\bigsqcup_{t\in T(k)} \phi^{-1}(t)(\boldsymbol{A}_k)^{\mathrm{Br}_H(\phi^{-1}(t))}\Bigr] = \bigcup_{t\in T(k)} f_{\partial(t)}[Y_{\partial(t)}(\boldsymbol{A}_k)^{\mathrm{Br}_H(Y_{\partial(t)})}]. \qquad \square$$

Rappelons la définition de $X(\boldsymbol{A}_k)^{G\text{-ét},\,\mathrm{Br}_G}$ dans (1-4).

Pour toute variété lisse X, définissons $X(\boldsymbol{A}_k^{\mathrm{nc}})$ l'espace des points adéliques de X hors des places complexes, i.e., on a $X(\boldsymbol{A}_k) \cong \bigl(\prod_{v \text{ complexe}} X(k_v)\bigr) \times X(\boldsymbol{A}_k^{\mathrm{nc}})$. De plus, on a :

$$X(\boldsymbol{A}_k)^{\mathrm{ob}} \cong \Bigl(\prod_{v \text{ complexe}} X(k_v)\Bigr) \times X(\boldsymbol{A}_k^{\mathrm{nc}})^{\mathrm{ob}} \tag{5-5}$$

pour l'obstruction ob $= \mathrm{Br}(X)$ ou ob $= \mathrm{Br}_1(X)$ ou ob $=$ ét, Br ou, si X est une G-variété pour un groupe linéaire connexe G, pour ob $= \mathrm{Br}_G(X)$ ou ob $= G$-ét, Br_G.

Le lemme suivant est bien connu (voir [Demarche 2009a, lemme 2.2.8] pour une variante).

Lemme 5.2. *Soient X une variété lisse et $\{X_i\}_{i\in I}$ les composantes connexes de X telles que X_i soit géométriquement intègre pour tout $i \in I$. Alors on a* :

$$X(\mathbf{A}_k^{\mathrm{nc}})^{\mathrm{Br}_1(X)} = \coprod_{i\in I} X_i(\mathbf{A}_k^{\mathrm{nc}})^{\mathrm{Br}_1(X_i)}, \qquad X(\mathbf{A}_k^{\mathrm{nc}})^{\text{ét, Br}} = \coprod_{i\in I} X_i(\mathbf{A}_k^{\mathrm{nc}})^{\text{ét, Br}}$$

et, *si X est une G-variété pour un groupe linéaire connexe G*, *on a* :

$$X(\mathbf{A}_k^{\mathrm{nc}})^{\mathrm{Br}_G(X)} = \coprod_{i\in I} X_i(\mathbf{A}_k^{\mathrm{nc}})^{\mathrm{Br}_G(X_i)} \quad \textit{et} \quad X(\mathbf{A}_k^{\mathrm{nc}})^{G\text{-ét, Br}_G} = \coprod_{i\in I} X_i(\mathbf{A}_k^{\mathrm{nc}})^{G\text{-ét, Br}_G}.$$

Démonstration. Puisque le groupe de Brauer (resp. le sous-groupe de Brauer G-invariant, resp. l'ensemble des F-torseurs, resp. l'ensemble des F-torseurs G-compatibles pour un k-groupe fini F) de X est la somme directe de celui des composantes connexes de X, on obtient l'inclusion $\supset$ dans les quatre cas ci-dessus.

Par ailleurs, soit $\pi_0(X)$ le schéma des composantes connexes géométriques de X, i.e., $\pi_0(X)$ est un k-schéma fini étale et il existe un k-morphisme surjectif $\phi : X \to \pi_0(X)$ de fibres géométriquement intègres. Pour tout k-schéma V fini étale connexe, $V(\mathbf{A}_k^{\mathrm{nc}}) \neq \varnothing$ implique $V \cong \operatorname{Spec} k$. D'après [Liu et Xu 2015, Proposition 3.3] (un résultat inspiré par Stoll), on a $\pi_0(X)(\mathbf{A}_k^{\mathrm{nc}})^{\mathrm{Br}(\pi_0(X))} = \pi_0(X)(k)$. Par définition, $\phi^*(\mathrm{Br}(\pi_0(X))) \subset \mathrm{Br}_1(X)$, $\phi^*(\mathrm{Br}(\pi_0(X))) \subset \mathrm{Br}_G(X)$ et donc on obtient l'inclusion $\subset$. □

Les deux lemmes suivants sont bien connus.

Lemme 5.3. *Soient X une variété lisse*, *L un groupe linéaire quelconque et $h : V \to X$ un L-torseur. Alors*, *pour tout $x \in X(\mathbf{A}_k)$*, *l'ensemble $\{\sigma \in H^1(k, L) : x \in h_\sigma(V_\sigma(\mathbf{A}_k))\}$ est fini.*

Démonstration. Le résultat découle du fait que, pour tout $\sigma \in H^1(k, L)$, l'ensemble $\text{Ш}^1(k, L_\sigma)$ est fini [Serre 1964, §III.4.6]. □

Voir [Skorobogatov 2001, Proposition 5.3.2 ; Cao et al. 2019a, Lemma 6.3] pour des résultats similaires.

Lemme 5.4 (M. Stoll [2007], cf. [Cao et al. 2019a, Lemma 7.1]). *Soit X une variété lisse géométriquement intègre*, *F un k-groupe fini et $f : Y \to X$ un F-torseur. Supposons qu'il existe un $x \in X(\mathbf{A}_k)^{\text{ét, Br}}$. Alors il existe un $\sigma \in H^1(k, F)$*, *un sous-groupe fermé $F' \subset F_\sigma$*, *une composante connexe $Y' \subset Y_\sigma$ tels que Y' soit géométriquement intègre et F'-invariant*, *$f' := f_\sigma|_{Y'} : Y' \to X$ soit un F'-torseur et que $x \in f'(Y'(\mathbf{A}_k)^{\mathrm{Br}(Y')})$.*

La proposition suivante est une étape intermédiaire importante dans la démonstration du théorème 1.1.

Proposition 5.5. *Soient G un groupe linéaire connexe*, *Z une variété lisse géométriquement intègre et $p : X \to Z$ un G-torseur. Alors* :

$$Z(\mathbf{A}_k)^{\text{ét, Br}} = \bigcup_{\sigma\in H^1(k,G)} p_\sigma(X_\sigma(\mathbf{A}_k)^{G_\sigma\text{-ét, Br}_{G_\sigma}}).$$

Démonstration. L'inclusion $\supset$ découle du fait que, pour tout torseur $V \to Z$ sous un k-groupe fini, l'image réciproque $X \times_Z V \to X$ est G-compatible.

Pour l'inclusion $\subset$, on peut supposer que $Z(\boldsymbol{A}_k)^{\text{ét, Br}} \neq \varnothing$.

On fixe un point $z \in Z(\boldsymbol{A}_k)^{\text{ét, Br}}$.

Soit Δ l'ensemble des $\sigma \in H^1(k, G)$ tels que $p_\sigma^{-1}(z) \cap X_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(X_\sigma)} \neq \varnothing$. Alors $\Delta \neq \varnothing$ par (5-1). Pour tout $\sigma \in \Delta$, on fixe un point $x_\sigma \in p_\sigma^{-1}(z) \cap X_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(X_\sigma)}$. Ceci induit un isomorphisme :

$$\Psi_\sigma : G(\boldsymbol{A}_k) \to p_\sigma^{-1}(z)(\boldsymbol{A}_k) : g \mapsto g \cdot x_\sigma.$$

Notons :

$$E_{0,\sigma} := \Psi_\sigma^{-1}\big(p_\sigma^{-1}(z) \cap X_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(X_\sigma)}\big) \quad \text{et} \quad E_0 := \bigsqcup_{\sigma \in \Delta} E_{0,\sigma}.$$

Pour tout $\sigma \in \Delta$, soit $G_\sigma(\boldsymbol{A}_k) \xrightarrow{a_\sigma} \mathrm{Hom}\big(\mathrm{Br}_a(G_\sigma), \mathbb{Q}/\mathbb{Z}\big)$ l'homomorphisme induit par l'accouplement de Brauer–Manin. Donc $\mathrm{Ker}(a_\sigma) = G_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_a(G_\sigma)}$. Notons

$$K_{a,\Delta} := \prod_{\sigma \in \Delta} \mathrm{Ker}(a_\sigma) \quad \text{et} \quad G_\Delta(\boldsymbol{A}_k) := \bigsqcup_{\sigma \in \Delta} G_\sigma(\boldsymbol{A}_k).$$

Définissons l'action de $\mathrm{Ker}(a_\sigma)$ sur $G_\sigma(\boldsymbol{A}_k)$ par la multiplication à gauche. Ceci induit une unique action de $K_{a,\Delta}$ sur $G_\Delta(\boldsymbol{A}_k)$ telle que l'action de $\mathrm{Ker}(\sigma_1)$ sur $G_{\sigma_2}(\boldsymbol{A}_k)$ soit l'identité pour tous $\sigma_1 \neq \sigma_2$. D'après (4-2), E_0 est $K_{a,\Delta}$-invariant.

Soit $\mathcal{S}$ l'ensemble des couples $(F, V \xrightarrow{f} Z)$ avec F un k-groupe fini et $V \xrightarrow{f} Z$ un F-torseur tel que V soit géométriquement intègre. On définit un ordre partiel : pour tous $(F_1, V_1), (F_2, V_2) \in \mathcal{S}$, on a $(F_1, V_1) \leq (F_2, V_2)$ si et seulement s'il existe un $\sigma \in H^1(k, F_1)$ et un homomorphisme surjectif $\phi : F_2 \to F_{1,\sigma}$ tels que $\phi_*([V_2]) = [V_{1,\sigma}]$.

Pour tout $(\delta, \sigma) \in H^1(k, F) \times H^1(k, G)$, soit $Y_{\sigma,\delta} := X_\sigma \times_Z V_\delta$. On a un diagramme commutatif de $F_\delta \times G_\sigma$-variétés et de $F_\delta \times G_\sigma$-morphismes :

$$\begin{tikzcd}
Y_{\sigma,\delta} \arrow[r, "f_\delta^\sigma"] \arrow[d, "p_\sigma^\delta"] \arrow[dr, phantom, "\square"] & X_\sigma \arrow[d, "p_\sigma"] \\
V_\delta \arrow[r, "f_\delta"] & Z,
\end{tikzcd}$$

tel que toute verticale soit un G_σ-torseur et que toute horizontale soit un F_δ-torseur.

Pour tout $(F, V \xrightarrow{f} Z) \in \mathcal{S}$ et tout $\sigma \in \Delta$, notons

$$E_{F,V,\sigma} := \Psi_\sigma^{-1}\left(p_\sigma^{-1}(z) \cap \left[\bigcup_{\delta \in H^1(k,F)} f_\delta^\sigma\big(Y_{\sigma,\delta}(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(Y_{\sigma,\delta})}\big)\right]\right) \subset G_\sigma(\boldsymbol{A}_k) \tag{5-6}$$

et $E_{F,V} := \bigsqcup_{\sigma \in \Delta} E_{F,V,\sigma} \subset G_\Delta(\boldsymbol{A}_k)$.

Lemme 5.6. *Pour tout $(F, V \xrightarrow{f} Z) \in \mathcal{S}$, on a :*

(1) *l'ensemble $E_{F,V}$ est un sous-ensemble non vide fermé $K_{a,\Delta}$-invariant de E_0 ;*

(2) *pour tout $(F_1, V_1) \in \mathcal{S}$ vérifiant $(F, V) \leq (F_1, V_1)$, on a $E_{F_1,V_1} \subset E_{F,V}$;*

(3) *l'ensemble $\mathcal{S}$ est un ensemble ordonné filtrant.*

Démonstration. Pour tout $\delta \in H^1(k, F)$ et tout $\sigma \in H^1(k, G)$, le morphisme f_δ^σ est fini. D'après (4-2), $Y_{\sigma,\delta}(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(Y_{\sigma,\delta})}$ est $\mathrm{Ker}(a_\sigma)$-invariant et

$$f_\delta^\sigma(Y_{\sigma,\delta}(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(Y_{\sigma,\delta})}) \subset X_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(X_\sigma)}$$

est fermé [Conrad 2012, Proposition 4.4] et $\mathrm{Ker}(a_\sigma)$-invariant. Ainsi

$$\Psi_\sigma^{-1}\big[p_\sigma^{-1}(z) \cap f_\delta^\sigma(Y_{\sigma,\delta}(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(Y_{\sigma,\delta})})\big] \subset E_{0,\sigma}$$

est fermé et $\mathrm{Ker}(a_\sigma)$-invariant.

Appliquant (5-1) et le lemme 5.3 à $Y_{\sigma,\delta} \xrightarrow{p_\sigma^\delta} V_\delta$, il existe au moins un et au plus un nombre fini de $(\delta, \sigma) \in H^1(k, F) \times H^1(k, G)$ tels que

$$(f_\delta \circ p_\sigma^\delta)^{-1}(z) \cap Y_{\sigma,\delta}(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(Y_{\sigma,\delta})} \neq \varnothing.$$

Alors $p_\sigma^{-1}(z) \cap X_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(X_\sigma)} \neq \varnothing$ et donc un tel σ est dans Δ. Alors $E_{F,V} \neq \varnothing$ et (1) découle du premier paragraphe.

L'énoncé (2) découle de la fonctorialité de l'accouplement de Brauer–Manin.

Pour tous $(F_1, V_1), (F_2, V_2) \in \mathcal{S}$, on a un $F_1 \times F_2$-torseur $V_1 \times_Z V_2 \to Z$. Par hypothèse, il existe un $(\sigma_1, \sigma_2) \in H^1(k, F_1) \times H^1(k, F_2)$ tel que $(V_{1,\sigma_1} \times_Z V_{2,\sigma_2})(\boldsymbol{A}_k)^{\mathrm{Br}(V_{1,\sigma_1} \times_Z V_{2,\sigma_2})} \neq \varnothing$. D'après le lemme 5.2 et (5-5), il existe un k-sous-groupe fermé $F_3 \subset F_{1,\sigma_1} \times F_{2,\sigma_2}$ et une composante connexe $V_3 \subset V_{1,\sigma_1} \times_Z V_{2,\sigma_2}$ tels que V_3 soit géométriquement intègre et que $V_3 \to Z$ soit un F_3-torseur compatible avec l'action de $F_{1,\sigma_1} \times F_{2,\sigma_2}$ sur $V_{1,\sigma_1} \times_Z V_{2,\sigma_2}$. Alors le morphisme $h_1 : V_3 \subset V_{1,\sigma_1} \times_Z V_{2,\sigma_2} \to V_{1,\sigma_1}$ est compatible avec $\phi_1 : F_3 \subset F_{1,\sigma_1} \times F_{2,\sigma_2} \to F_{1,\sigma_1}$. Puisque V_{1,σ_1} est géométriquement intègre, le morphisme h_1 est surjectif et donc ϕ_1 est surjectif. Alors $[V_{1,\sigma_1}] = \phi_{1,*}([V_3])$ et $(F_1, V_1) \leq (F_3, V_3)$. Par ailleurs, $(F_2, V_2) \leq (F_3, V_3)$, d'où l'énoncé (3). □

Soient $\mathcal{B} := \bigsqcup_{\sigma\in\Delta} \mathrm{Hom}\big(\mathrm{Br}_a(G_\sigma), \mathbb{Q}/\mathbb{Z}\big)$ et

$$a_\Delta : G_\Delta = \bigsqcup_{\sigma\in\Delta} G_\sigma(\boldsymbol{A}_k) \xrightarrow{\bigsqcup_{\sigma\in\Delta} a_\sigma} \bigsqcup_{\sigma\in\Delta} \mathrm{Hom}\big(\mathrm{Br}_a(G_\sigma), \mathbb{Q}/\mathbb{Z}\big) = \mathcal{B}.$$

En tant qu'ensembles, on a $\mathrm{Im}(a_\Delta) \cong K_{a,\Delta}\backslash G_\Delta$. L'espace $\mathrm{Hom}(\mathrm{Br}_a(G_\sigma), \mathbb{Q}/\mathbb{Z})$ est compact, car $\mathrm{Br}_a(G_\sigma)$ est discret. D'après le lemme 5.3, Δ est fini et donc $\mathcal{B}$ est compact. Puisque a_σ est continu et ouvert [Cao 2018, lemme 4.1], l'application a_Δ est ouverte. Donc l'image d'un sous-ensemble fermé $K_{a,\Delta}$-invariant est fermée. Alors $a_\Delta(E_{F,V}) \subset \mathcal{B}$ est fermé non vide pour tout $(F, V) \in \mathcal{S}$. Puisque $\mathcal{B}$ est compact et que $\mathcal{S}$ est un ensemble ordonné filtrant, d'après le lemme 5.6 (2), l'intersection

$$\bigcap_{(F,V)\in\mathcal{S}} a_\Delta(E_{F,V}) \neq \varnothing \quad \text{et donc} \quad E_\infty := \bigcap_{(F,V)\in\mathcal{S}} E_{F,V} \neq \varnothing.$$

Il existe un $\sigma \in \Delta$ tel que $E_\infty \cap E_\sigma \neq \varnothing$.

Soient $g \in E_\infty \cap E_\sigma$ et $x := \Psi_\sigma(g) = g \cdot x_\sigma$. Alors $p_\sigma(x) = z$ et, d'après (5-6), on a

$$x \in \bigcap_{(F,V)\in\mathcal{S}} \Bigl[\bigcup_{\delta \in H^1(k,F)} f_\delta^\sigma \bigl(Y_{\sigma,\delta}(\boldsymbol{A}_k)^{\mathrm{Br}_{G_\sigma}(Y_{\sigma,\delta})} \bigr) \Bigr].$$

D'après le corollaire 3.7, tout torseur G-compatible sous un k-groupe fini sur X provient d'un torseur sur Z. D'après le lemme de Stoll (lemme 5.4), il suffit de considérer les torseurs géométriquement intègres. Donc $x \in X_\sigma(\boldsymbol{A}_k)^{G_\sigma\text{-ét},\, \mathrm{Br}_{G_\sigma}}$, d'où le résultat. □

La proposition suivante est une généralisation de [Cao et al. 2019a, Remark 7.5].

Proposition 5.7. *Soit X une variété lisse géométriquement intègre. Soit*

$$1 \to N \to L \xrightarrow{\psi} F \to 1$$

une suite exacte de groupes linéaires avec F fini. Soient $V \to X$ un L-torseur et $Y := V/N \to X$ le F-torseur induit par ψ, i.e., $[Y] = \psi_*([V])$. Faisons l'une ou l'autre des hypothèses :

(1) *Le groupe N est connexe.*

(2) *Le groupe L est fini et N est contenu dans le centre de L.*

Alors, pour tout $\sigma \in H^1(k, F)$ avec $Y_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_1(Y_\sigma)} \neq \varnothing$, il existe un $\alpha \in H^1(k, L)$ tel que $\psi_*(\alpha) = \sigma$.

Démonstration. Le cas où N est connexe est exactement [Cao et al. 2019a, Remark 7.5].

On considère le cas (2). Dans ce cas, N est un k-groupe fini commutatif. La résolution flasque [Colliot-Thélène et Sansuc 1987b, Proposition 1.3] donne une suite exacte $0 \to N \to T \to T_0 \to 0$ avec T un tore et T_0 un tore quasi-trivial. Soit $L' := L \times^N T$. Alors L' est un groupe linéaire, car N est contenu dans le centre de L. Ceci induit un diagramme commutatif de suites exactes et de colonnes exactes :

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & & \\
1 \arrow[r] & N \arrow[r] \arrow[d] & L \arrow[r] \arrow[d, "\psi_2"] & F \arrow[r] \arrow[d, "="] & 1 \\
1 \arrow[r] & T \arrow[r] \arrow[d] & L' \arrow[r, "\psi_1"] \arrow[d] & F \arrow[r] & 1 \\
 & T_0 \arrow[r, "="] \arrow[d] & T_0 \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

Appliquons le cas (1) au L'-torseur $\psi_{2,*}([V])$. On obtient un $\beta \in H^1(k, L')$ tel que $\psi_{1,*}(\beta) = \sigma$. Puisque $H^1(k, T_0) = 0$, il existe un $\alpha \in H^1(k, L)$ tel que $\psi_{2,*}(\alpha) = \beta$ et donc $\psi_*(\alpha) = \sigma$. □

La proposition 5.7(2) et la formule (4-1) impliquent directement :

Corollaire 5.8. *Sous les hypothèses de la proposition 5.7*(2), *soit G un groupe linéaire. Pour tout $\sigma \in H^1(k, F)$, s'il existe une action de G sur Y_σ telle que $Y_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_G(Y_\sigma)} \neq \varnothing$, alors il existe un $\alpha \in H^1(k, L)$ tel que $\psi_*(\alpha) = \sigma$.*

6. Démonstration du théorème 1.4

Dans toute cette section, k est un corps de nombres. Sauf mention explicite du contraire, une variété est une k-variété.

Dans toute cette section, G est un k-groupe linéaire connexe et (X, ρ) une G-variété lisse géométriquement intègre.

Pour tout k-groupe fini F et tout F-torseur $f : Y \to X$, soit $(H_Y \xrightarrow{\psi_Y} G)$ le groupe minimal compatible au F-torseur Y (cf. définition 3.9). Pour tout $\sigma \in H^1(k, F)$, le F_σ-torseur $f_\sigma : Y_\sigma \to X$ est H_Y-compatible, i.e., il existe une unique action de H_Y sur Y_σ telle que f_σ soit un H_Y-morphisme.

Dans paragraphe 1, on a défini $X(\boldsymbol{A}_k)^{\text{ét, Br}}$ (cf. (1-1)) et $X(\boldsymbol{A}_k)^{G\text{-ét, }\mathrm{Br}_G}$ (cf. (1-4)). On définit

$$X(\boldsymbol{A}_k)^{\text{ét, }\mathrm{Br}_G} := \bigcap_{\substack{f:Y\xrightarrow{F}X \\ F \text{ fini}}} \bigcup_{\sigma\in H^1(k,F)} f_\sigma(Y_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_{H_Y}(Y_\sigma)}),$$

$$X(\boldsymbol{A}_k)^{\text{c.c., ét, }\mathrm{Br}_G} := \bigcap_{\substack{f:Y\xrightarrow{F}X \\ F \text{ fini commutatif} \\ Y \text{ géo. connexe}}} \bigcup_{\sigma\in H^1(k,F)} f_\sigma(Y_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_{H_Y}(Y_\sigma)}),$$

où géo. connexe signifie géométriquement connexe et c.c. est une abréviation de commutatif connexe. On a directement :

$$X(\boldsymbol{A}_k)^{\text{ét, }\mathrm{Br}_G} \subset X(\boldsymbol{A}_k)^{\text{c.c., ét, }\mathrm{Br}_G} \quad \text{et} \quad X(\boldsymbol{A}_k)^{\text{ét, Br}} \subset X(\boldsymbol{A}_k)^{\text{ét, }\mathrm{Br}_G} \subset X(\boldsymbol{A}_k)^{G\text{-ét, }\mathrm{Br}_G}.$$

Proposition 6.1. $$X(\boldsymbol{A}_k)^{\text{c.c., ét, }\mathrm{Br}_G} \subset X(\boldsymbol{A}_k)^{\mathrm{Br}(X)}.$$

Démonstration. Il suffit de montrer que, pour tout $\alpha \in \mathrm{Br}(X)$ et tout $x \in X(\boldsymbol{A}_k)^{\text{c.c., ét, }\mathrm{Br}_G}$, on a $\alpha(x) = 0$. On fixe un tel x et un tel α.

Il existe un entier n tel que $n \cdot \alpha = 0$. D'après le corollaire 4.2, il existe un torseur universel de n-torsion $\mathcal{T}_X \xrightarrow{f} X$ (un S_X-torseur). Soit H le groupe minimal compatible au S_X-torseur $\mathcal{T}_X$. Par hypothèse, il existe un $\sigma \in H^1(k, S_X)$ et un point adélique $t \in \mathcal{T}_{X,\sigma}(\boldsymbol{A}_k)^{\mathrm{Br}_H(\mathcal{T}_{X,\sigma})}$ tels que $f_\sigma(t) = x$. D'après la proposition 3.12, $f_\sigma^*(\alpha) \in \mathrm{Br}_H(\mathcal{T}_{X,\sigma})$. Alors $\alpha(x) = f_\sigma^*(\alpha)(t) = 0$. □

Le lemme suivant généralise un résultat de Skorobogatov [2009, Theorem 1.1] et il généralise aussi [Cao et al. 2019a, Proposition 6.6]. Sa démonstration suit l'idée de [Skorobogatov 2009, p. 506] et de [Stoll 2007, Proposition 5.17].

Lemme 6.2. *Soient F un k-groupe fini, $f : Y \to X$ un F torseur et $(H_Y \xrightarrow{\psi_Y} G)$ le groupe minimal compatible au F-torseur Y. Supposons que Y est géométriquement intègre. Alors*

(1) *on a* $X(\boldsymbol{A}_k)^{\text{ét, }\mathrm{Br}_G} = \bigcup_{\sigma\in H^1(k,F)} f_\sigma[Y_\sigma(\boldsymbol{A}_k)^{\text{ét, }\mathrm{Br}_{H_Y}}]$;

(2) *on a* $X(\boldsymbol{A}_k)^{\text{ét, Br}} = \bigcup_{\sigma\in H^1(k,F)} f_\sigma[Y_\sigma(\boldsymbol{A}_k)^{\text{ét, Br}}]$;

(3) *si* $\psi_Y : H_Y \xrightarrow{\sim} G$ *est un isomorphisme*, *on a*

$$X(\boldsymbol{A}_k)^{G\text{-ét, Br}_G} = \bigcup_{\sigma\in H^1(k,F)} f_\sigma[Y_\sigma(\boldsymbol{A}_k)^{G\text{-ét, Br}_G}].$$

Démonstration. L'inclusion $\supset$ dans les trois cas est définie par le pullback des torseurs et la fonctorialité de l'accouplement de Brauer–Manin. On considère l'inclusion $\subset$.

Dans le cas (1), il suffit de montrer que, pour tout $x \in X(\boldsymbol{A}_k)^{\text{ét, Br}_G}$, il existe un $\sigma \in H^1(k, F)$ et un $y \in Y_\sigma(\boldsymbol{A}_k)^{\text{ét, Br}_{H_Y}}$ tels que $f_\sigma(y) = x$. On fixe un tel x.

Pour tout $\sigma \in H^1(k, F)$, soient

$$\Delta_\sigma := f_\sigma^{-1}(x) \cap Y_\sigma(\boldsymbol{A}_k), \quad \Sigma := \{\sigma \in H^1(k, F) : \ \Delta_\sigma \neq \varnothing\} \quad \text{et} \quad \Delta := \bigsqcup_{\sigma\in\Sigma} \Delta_\sigma.$$

D'après le lemme 5.3, Δ et Σ sont finis.

Soit $\mathcal{S}$ l'ensemble des *X-torseurs sur Y sous k-groupes finis* i.e., l'ensemble des quintuples

$$\big(\sigma, E, E \xrightarrow{\psi} F_\sigma, V \xrightarrow{h_V} X, V \xrightarrow{h} Y_\sigma\big)$$

avec $\sigma \in H^1(k, F)$, E un k-groupe fini, ψ un homomorphisme surjectif, $V \xrightarrow{h_V} X$ un E-torseur et h un E-morphisme sur X. Alors $\psi_*([V]) = [Y_\sigma] \in H^1(k, F)$ et $h : V \to Y_\sigma$ est un $\operatorname{Ker}(\psi)$-torseur. Donc $h_\alpha : V_\alpha \to Y_{\sigma+\psi_*(\alpha)}$ est un $\operatorname{Ker}(\psi_\alpha)$-torseur pour tout $\alpha \in H^1(k, E)$. Soit

$$\Delta_V := \big\{y \in \Delta : \ \exists\alpha \in H^1(k, E) \text{ tel que } y \in h_\alpha(V_\alpha(\boldsymbol{A}_k)^{\text{Br}_{H_V}(V_\alpha)})\big\}.$$

Par l'hypothèse sur x, l'ensemble Δ_V est non vide.

On définit un ordre partiel de $\mathcal{S}$: pour tous $(\sigma_1, E_1, \psi_1, V_1, h_1), (\sigma_2, E_2, \psi_2, V_2, h_2) \in \mathcal{S}$, on a $(\sigma_1, E_1, \psi_1, V_1, h_1) \leq (\sigma_2, E_2, \psi_2, V_2, h_2)$ si et seulement si $\sigma_1 = \sigma_2$ et s'il existe un $\alpha \in H^1(k, E_1)$, un homomorphisme surjectif $\phi : E_2 \to E_{1,\alpha}$ et un E_2-morphisme $h_\phi : V_2 \to V_{1,\alpha}$ sur Y_{σ_1}. Dans ce cas, on a $\Delta_{V_2} \subset \Delta_{V_1}$.

Puisque Δ est fini, il existe un quintuple $(\sigma, E_0, \psi_0, V_0, h_0)$ dans S tel que Δ_{V_0} soit minimal. On fixe un $y \in \Delta_{V_0}$. Après avoir remplacé σ par $\sigma + \psi_{0,*}(\alpha)$ pour certain $\alpha \in H^1(k, E_0)$, on peut supposer que $y \in Y_\sigma(\boldsymbol{A}_k)$.

Pour tout torseur $Z \xrightarrow{f_1} Y_\sigma$ sous un k-groupe fini F_1, d'après [Skorobogatov 2009, Proposition 2.3 et (4)], il existe un $(\sigma, E, \psi, h_V : V \to X, h) \in \mathcal{S}$, un homomorphisme surjectif $\operatorname{Ker}(\psi) \to F_1$ et un $\operatorname{Ker}(\psi)$-morphisme $V \to Z$ sur Y_σ avec

$$V := R_{Y_\sigma\times_k F_\sigma/Y_\sigma}(Z \times_k F_\sigma) \cong R_{Y_\sigma/X}(Z) \times_X Y_\sigma \xrightarrow{h_V} X. \tag{6-1}$$

Ceci induit

$$\Delta_V \subset \bigcup_{\alpha\in H^1(k,\operatorname{Ker}(\psi))} h_\alpha(V_\alpha(\boldsymbol{A}_k)^{\text{Br}_{H_V}(V_\alpha)}) \subset \bigcup_{\alpha\in H^1(k,F_1)} f_{1,\alpha}(Z_\alpha(\boldsymbol{A}_k)^{\text{Br}_{H_Z}(Z_\alpha)}).$$

Par ailleurs, on a :

$$(\sigma, E_0, \psi_0, V_0, h_0), (\sigma, E, \psi, V, h) \leq \big(\sigma, E_0 \times_{F_\sigma} E, \psi_0 \circ (\mathrm{id}_{E_0} \times_{F_\sigma} \psi), V_0 \times_{Y_\sigma} V, h_0 \circ (\mathrm{id}_{V_0} \times_{Y_\sigma} h)\big)$$

dans $\mathcal{S}$, et donc $\Delta_{V_0} \supset \Delta_{V_0 \times_{Y_\sigma} V} \subset \Delta_V$. Puisque Δ_{V_0} est minimal, on a $\Delta_{V_0} = \Delta_{V_0 \times_{Y_\sigma} V} \subset \Delta_V$. Donc $y \in Y_\sigma(\boldsymbol{A}_k)^{\text{ét}, \mathrm{Br}_{H_Y}}$, d'où l'on déduit (1).

L'énoncé (2) découle du même argument que l'énoncé (1).

Pour (3), d'après le corollaire 3.6, le torseur $V \to X$ dans (6-1) est G-compatible. L'énoncé (3) découle du même argument que l'énoncé (1). □

La proposition suivante généralise un lemme de Stoll [2007] (cf. lemme 5.4).

Proposition 6.3. *Soient G un k-groupe linéaire connexe et (X, ρ) une G-variété lisse géométriquement intègre. Supposons que $X(\boldsymbol{A}_k)^{G\text{-ét}, \mathrm{Br}_G} \neq \varnothing$. Alors, pour tout k-groupe fini F et tout F-torseur $Y \to X$, il existe un $\sigma \in H^1(k, F)$ tel qu'il existe une composante connexe $Y' \subset Y_\sigma$ qui est géométriquement intègre.*

De plus, dans ce cas, il existe un sous k-groupe fermé $F' \subset F_\sigma$ tel que Y' soit un F'-torseur sur X, où l'action de F' sur Y' est induite par l'action de F_σ sur Y_σ.

Démonstration. Le morphisme $G \times X \xrightarrow{\rho} X$ induit un homomorphisme $\rho_{\pi_1} : \pi_1(G_{\bar{k}}) \to \pi_1(X)$. D'après le corollaire 3.5, l'image $\mathrm{Im}(\rho_{\pi_1})$ est un sous-groupe normal de $\pi_1(X)$ et elle est contenue dans le centre de $\pi_1(X_{\bar{k}})$. Pour tout k-groupe fini F_1, d'après (1-5), tout F_1-torseur $Y_1 \to X$ induit un homomorphisme $\theta_1 : \pi_1(X_{\bar{k}}) \to F_1(\bar{k})$ à conjugaison près et, d'après la proposition 3.3 et le corollaire 3.5, Y_1 est G-compatible si et seulement si $\theta_1 \circ \rho_{\pi_1} = 0$.

D'après (1-5), soit $\alpha \in H^1(\pi_1(X), F(\bar{k}))$ un 1-cocycle qui correspond à $[Y] \in H^1(X, F)$. Il existe un sous-groupe ouvert distingué $\Delta \subset \pi_1(X)$ tel que $\alpha|_\Delta = 0$. Soient $\Delta_{\bar{k}} := \Delta \cap \pi_1(X_{\bar{k}})$ et $\alpha_{\bar{k}} := \alpha|_{\pi_1(X_{\bar{k}})}$. Alors $\alpha_{\bar{k}}$ est un homomorphisme $\pi_1(X_{\bar{k}}) \to F(\bar{k})$.

Lemme 6.4. *Pour trouver Y' dans la proposition 6.3, on peut supposer que $\Delta_{\bar{k}} \cdot \mathrm{Im}(\rho_{\pi_1}) = \pi_1(X_{\bar{k}})$ et donc* $\mathrm{Im}(\alpha_{\bar{k}}) = \mathrm{Im}(\alpha_{\bar{k}} \circ \rho_{\pi_1})$.

Démonstration. Le sous-groupe $\mathrm{Im}(\rho_{\pi_1}) \cdot \Delta$ est ouvert normal dans $\pi_1(X)$. Soit $Y_2 \to X$ le revêtement galoisien correspondant. Par construction, $Y_2 \to X$ est un torseur G-compatible sous un k-groupe constant $F_2 = \pi_1(X)/(\mathrm{Im}(\rho_{\pi_1}) \cdot \Delta)$. Par hypothèse, il existe un $\sigma \in H^1(k, F_2)$ tel que $Y_{2,\sigma}(\boldsymbol{A}_k)^{\mathrm{Br}_G(Y_{2,\sigma})} \neq \varnothing$. D'après le lemme 5.2 et (5-5), il existe une composante connexe $Y_3 \subset Y_2$ telle que Y_3 est géométriquement intègre. Ainsi $Y_3 \to X$ est un torseur sous un sous-groupe fermé $F_3 \subset F_{2,\sigma}$ et on a

$$\mathrm{Im}(\pi_1(Y_{3,\bar{k}}) \hookrightarrow \pi_1(X_{\bar{k}})) = \pi_1(X_{\bar{k}}) \cap \mathrm{Im}(\pi_1(Y_2) \to \pi_1(X)) = \mathrm{Im}(\rho_{\pi_1}) \cdot \Delta_{\bar{k}}.$$

Alors $Y_3 \to X$ est G-compatible. Par le lemme 6.2(3), après avoir remplacé Y_3 par son tordu, on peut supposer que $Y_3(\boldsymbol{A}_k)^{G\text{-ét}, \mathrm{Br}_G} \neq \varnothing$.

S'il existe un $\sigma \in H^1(k, F)$ et une composante connexe Y_3' du F_σ-torseur $Y_\sigma \times_X Y_3 \to Y_3$ tels que Y_3' soit géométriquement intègre, alors l'image de Y_3' par le morphisme fini étale $Y_\sigma \times_X Y_3 \to Y_\sigma$ est une composante connexe Y' de Y_σ telle que Y' soit géométriquement intègre. Donc on peut remplacer X par

Y_3 et, après avoir remplacé X par Y_3, on peut supposer que $\Delta_{\bar{k}} \cdot \mathrm{Im}(\rho_{\pi_1}) = \pi_1(X_{\bar{k}})$. Puisque $\alpha_{\bar{k}}(\Delta_{\bar{k}}) = 0$, on a $\mathrm{Im}(\alpha_{\bar{k}}) = \mathrm{Im}(\alpha_{\bar{k}} \circ \rho_{\pi_1})$. □

Dans ce cas, puisque $\pi_1(G_{\bar{k}})$ est commutatif, $\mathrm{Im}(\alpha_{\bar{k}})$ est commutatif. D'après le corollaire 3.5, $\alpha_{\bar{k}}$ induit un homomorphisme $\pi_1(X_{\bar{k}})^{\mathrm{ab}} \to F(\bar{k})$ de noyau Γ_k-invariant, car α est défini sur k. D'après le corollaire 2.4, il existe un k-groupe fini commutatif S et un S-torseur $\mathcal{T} \to X$ tels que $\mathcal{T}$ soit géométriquement intègre, $S(\bar{k}) = \mathrm{Im}(\alpha_{\bar{k}})$ et que, dans

$$H^1(X_{\bar{k}}, S) \cong \mathrm{Hom}_{\mathrm{cont}}(\pi_1(X_{\bar{k}}), \mathrm{Im}(\alpha_{\bar{k}})),$$

on ait $[\mathcal{T}_{\bar{k}}] = \alpha_{\bar{k}}$.

Soit $(H_Y \xrightarrow{\psi_Y} G)$ le groupe minimal compatible au F-torseur Y. D'après la remarque 3.10, $(H_Y \xrightarrow{\psi_Y} G)$ est aussi le groupe minimal compatible au S-torseur $\mathcal{T}$. D'après le corollaire 3.11, $\mathrm{Ker}(\psi_Y) \cong S$. Donc $Y_4 := \mathcal{T} \times_X Y$ est une H_Y-variété et $Y_4 \to X$ est un $(S \times F)$-torseur H_Y-compatible. Donc $Y_5 := Y_4/\mathrm{Ker}(\psi_Y) \to X$ est un F-torseur G-compatible et on a un F-morphisme fini étale $\phi_5 : Y_5 \to Y/\mathrm{Ker}(\psi_Y)$. Par hypothèse, il existe un $\sigma \in H^1(k, F)$ tel que $Y_{5,\sigma}(\boldsymbol{A}_k)^{\mathrm{Br}_G(Y_{5,\sigma})} \neq \varnothing$. D'après le lemme 5.2, il existe une composante connexe Y'_5 de $Y_{5,\sigma}$ telle que Y'_5 soit géométriquement intègre. Ainsi $\phi_5(Y'_5)$ est une composante connexe de $(Y/\mathrm{Ker}(\psi_Y))_\sigma$, qui est géométriquement intègre. Puisque H_Y est connexe, les composantes connexes géométriques de $(Y/\mathrm{Ker}(\psi_Y))_\sigma$ et de Y_σ sont les mêmes, d'où le résultat. □

Lemme 6.5. $$X(\boldsymbol{A}_k)^{\text{ét}, \mathrm{Br}_G} = X(\boldsymbol{A}_k)^{G\text{-ét}, \mathrm{Br}_G}.$$

Démonstration. Il suffit de montrer que, pour tout $x \in X(\boldsymbol{A}_k)^{G\text{-ét}, \mathrm{Br}_G}$, tout k-groupe fini F et tout F-torseur $Y \xrightarrow{f} X$, il existe un $\sigma \in H^1(k, F)$, un $y \in Y_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_{H_Y}(Y_\sigma)}$ tels que $f_\sigma(y) = x$, où $(H_Y \xrightarrow{\psi_Y} G)$ est le groupe minimal compatible au F-torseur Y.

On fixe de tels x, F, Y, f.

D'après la proposition 6.3, on peut supposer que Y est géométriquement intègre.

D'après le corollaire 3.11, il existe un plongement $\phi : \mathrm{Ker}(\psi_Y) \to F$ d'image centrale compatible avec les actions de $\mathrm{Ker}(\psi_Y)$ et de F sur Y. Ceci induit une suite exacte de k-groupes finis

$$1 \to \mathrm{Ker}(\psi_Y) \xrightarrow{\phi} F \xrightarrow{\phi_1} F_1 \to 1$$

qui définit F_1. Alors $Y_1 := Y/\mathrm{Ker}(\psi_Y) \xrightarrow{f_1} X$ est un F_1-torseur G-compatible sur X. De plus, Y_1 est lisse et géométriquement intègre.

Par hypothèse, il existe un $\sigma_1 \in H^1(k, F_1)$ et un $y_1 \in Y_{1,\sigma_1}(\boldsymbol{A}_k)^{\mathrm{Br}_G(Y_{1,\sigma_1})}$ tels que $f_{1,\sigma_1}(y_1) = x$. D'après le corollaire 5.8, il existe un $\sigma_0 \in H^1(k, F)$ tel que $\phi_{1,*}(\sigma_0) = \sigma_1$. Comme l'image de ϕ est centrale dans F, on a $\mathrm{Ker}(\psi_Y)_{\sigma_0} = \mathrm{Ker}(\psi_Y)$.

L'argument ci-dessus donne un $\mathrm{Ker}(\psi_Y)$-torseur $Y_{\sigma_0} \to Y_{1,\sigma_1}$ compatible avec l'action de H_Y. D'après la proposition 5.1, il existe un $\sigma_2 \in H^1(k, \mathrm{Ker}(\psi_Y))$ et un $y \in Y_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_{H_Y}(Y_\sigma)}$ avec $\sigma := \sigma_0 + \sigma_2 \in H^1(k, F)$ tels que $f_\sigma(y) = x$. □

Lemme 6.6. $$X(\boldsymbol{A}_k)^{\text{ét}, \mathrm{Br}} = X(\boldsymbol{A}_k)^{\text{ét}, \mathrm{Br}_G}.$$

Démonstration. On peut supposer que $X(\boldsymbol{A}_k)^{\text{ét}, \operatorname{Br}_G} \neq \varnothing$. Il suffit de montrer que, pour tout k-groupe fini F et tout F-torseur $f : Y \to X$, on a

$$X(\boldsymbol{A}_k)^{\text{ét}, \operatorname{Br}_G} \subset \bigcup_{\sigma \in H^1(k,F)} f_\sigma(Y_\sigma(\boldsymbol{A}_k)^{\operatorname{Br}(Y_\sigma)}).$$

D'après la proposition 6.3, on peut supposer que Y est géométriquement intègre. L'énoncé découle de la proposition 6.1 et du lemme 6.2 (1). □

Démonstration du théorème 1.4. D'après le lemme 5.2 et (5-5), on peut supposer que X est géométriquement intègre. On obtient le théorème par combinaison du lemme 6.6 et du lemme 6.5. □

Remarque 6.7. Rappelons les catégories **AB** et **GX** dans paragraphe 4. On fixe un objet $(G, X) \in \mathbf{GX}$.

Soit $\mathbf{GX}_X$ l'ensemble des objets $(H, Y) \in \mathbf{GX}$ tels qu'il existe un morphisme $(\psi, f) : (H, Y) \to (G, X)$ dans **GX** avec ψ, f finis.

Dans toute cette section (paragraphe 6), pour établir le théorème 1.4 de (G, X), l'hypothèse que G est linéaire et la notion de sous-groupe de Brauer invariant sont utilisés seulement pour appliquer la proposition 3.12, la proposition 5.1, le corollaire 4.2, le lemme 5.2 et le corollaire 5.8 à l'élément dans $\mathbf{GX}_X$. Donc, cette section a essentiellement montré :

> pour tout foncteur contravariant $B(-,-) : \mathbf{GX} \to \mathbf{AB}$ qui associe au couple (H, Y) un sous-groupe $B(H, Y) \subset \operatorname{Br}(Y)$, si l'on peut établir la proposition 3.12, la proposition 5.1, le corollaire 4.2, le lemme 5.2 et le corollaire 5.8 pour tout élément dans $\mathbf{GX}_X$ (en remplaçant tout groupe de Brauer invariant par le $B(-,-)$ correspondant), alors on a $X(\boldsymbol{A}_k)^{\text{ét}, \operatorname{Br}} = X(\boldsymbol{A}_k)^{G\text{-ét}, B(G,-)}$, où $X(\boldsymbol{A}_k)^{G\text{-ét}, B(G,-)}$ est défini de la même façon que $X(\boldsymbol{A}_k)^{G\text{-ét}, \operatorname{Br}_G}$.

7. Démonstration des théorèmes 1.1 et 1.2

Dans toute cette section, k est un corps de nombres. Sauf mention explicite du contraire, une variété est une k-variété.

Démonstration du théorème 1.1. D'après le lemme 5.2 et (5-5), on peut supposer que Z est géométriquement intègre. Si G est connexe, l'énoncé découle du théorème 1.4 et de la proposition 5.5. Si G est fini, d'après la proposition 6.3, on peut supposer que X est géométriquement intègre, et le résultat découle du lemme 6.2(2).

Pour établir le cas général, on reprend certains arguments de [Demarche 2009b; Cao et al. 2019a]. Il existe une suite exacte

$$1 \to N \to G \xrightarrow{\psi} F \to 1$$

de k-groupes linéaires avec N un k-groupe linéaire connexe et F un k-groupe fini. Alors

$$h : U := X/N \to Z$$

est un F-torseur. Notons $q : X \to U$. Pour un $z \in Z(\boldsymbol{A}_k)^{\text{ét}, \operatorname{Br}}$, il existe un $\sigma \in H^1(k, F)$ et un $u \in U_\sigma(\boldsymbol{A}_k)^{\text{ét}, \operatorname{Br}}$ tels que $h_\sigma(u) = z$. D'après la proposition 5.7(1), il existe un $\alpha_0 \in H^1(k, G)$ tel que $\psi_*(\alpha_0) = \sigma$. Ceci induit une suite exacte

$$1 \to N' \xrightarrow{\phi} G_{\alpha_0} \xrightarrow{\psi_{\alpha_0}} F_\sigma \to 1$$

de k-groupes linéaires. Alors $N'_{\bar{k}} \cong N_{\bar{k}}$ et N' est un k-groupe linéaire connexe. Ainsi $q_{\alpha_0} : X_{\alpha_0} \to U_\sigma$ est un N'-torseur. Donc il existe un $\beta \in H^1(k, N')$ et un $x \in (X_{\alpha_0})_\beta(\boldsymbol{A}_k)^{\text{ét, Br}}$ tels que $(q_{\alpha_0})_\beta(x) = u$. Soit $\alpha := \alpha_0 + \phi_*(\beta)$. Alors $(X_{\alpha_0})_\beta = X_\alpha$ et $p_\alpha = h_\sigma \circ (q_{\alpha_0})_\beta$. Donc $x \in X_\alpha(\boldsymbol{A}_k)^{\text{ét, Br}}$ et $p_\alpha(x) = z$, d'où le résultat. □

Démonstration du théorème 1.2. Ceci découle du théorème 1.1 et de [Cao et al. 2019a, Theorem 1.5]. □

Démonstration du corollaire 1.5. Pour tout k-groupe fini F et tout F-torseur G-compatible $f : Y \to X$, d'après le corollaire 3.5(4), il existe un F-torseur M sur k tel que $Y \cong M \times_k X$ comme F-torseurs. Alors il existe un $\sigma_0 \in H^1(k, F)$ tel que $Y_{\sigma_0} \cong F \times X$. Donc

$$X(\boldsymbol{A}_k)^{\mathrm{Br}_G(X)} \subset f_{\sigma_0}(Y_{\sigma_0}(\boldsymbol{A}_k)^{\mathrm{Br}_G(Y_{\sigma_0})}) \subset \bigcup_{\sigma \in H^1(k,F)} f_\sigma(Y_\sigma(\boldsymbol{A}_k)^{\mathrm{Br}_G(Y_\sigma)}).$$

Ainsi $X(\boldsymbol{A}_k)^{G\text{-ét, Br}_G} = X(\boldsymbol{A}_k)^{\mathrm{Br}_G(X)}$ et le résultat découle du théorème 1.4. □

Remerciements

Je remercie très chaleureusement Jean-Louis Colliot-Thélène et Cyril Demarche pour leurs commentaires.

Bibliographie

[Balestrieri 2018] F. Balestrieri, "Iterating the algebraic étale-Brauer set", *J. Number Theory* **182** (2018), 284–295. MR Zbl

[Borovoi et Demarche 2013] M. Borovoi et C. Demarche, "Manin obstruction to strong approximation for homogeneous spaces", *Comment. Math. Helv.* **88**:1 (2013), 1–54. MR Zbl

[Brion et Szamuely 2013] M. Brion et T. Szamuely, "Prime-to-p étale covers of algebraic groups and homogeneous spaces", *Bull. Lond. Math. Soc.* **45**:3 (2013), 602–612. MR Zbl

[Cao 2018] Y. Cao, "Approximation forte pour les variétés avec une action d'un groupe linéaire", *Compos. Math.* **154**:4 (2018), 773–819. MR Zbl

[Cao et al. 2019a] Y. Cao, C. Demarche et F. Xu, "Comparing descent obstruction and Brauer–Manin obstruction for open varieties", *Trans. Amer. Math. Soc.* **371**:12 (2019), 8625–8650. MR Zbl

[Cao et al. 2019b] Y. Cao, Y. Liang et F. Xu, "Arithmetic purity of strong approximation for homogeneous spaces", *J. Math. Pures Appl.* (9) **132** (2019), 334–368. MR Zbl

[Colliot-Thélène 2008] J.-L. Colliot-Thélène, "Résolutions flasques des groupes linéaires connexes", *J. Reine Angew. Math.* **618** (2008), 77–133. MR Zbl

[Colliot-Thélène et Sansuc 1987a] J.-L. Colliot-Thélène et J.-J. Sansuc, "La descente sur les variétés rationnelles, II", *Duke Math. J.* **54**:2 (1987), 375–492. MR Zbl

[Colliot-Thélène et Sansuc 1987b] J.-L. Colliot-Thélène et J.-J. Sansuc, "Principal homogeneous spaces under flasque tori: applications", *J. Algebra* **106**:1 (1987), 148–205. MR Zbl

[Conrad 2012] B. Conrad, "Weil and Grothendieck approaches to adelic points", *Enseign. Math.* (2) **58**:1-2 (2012), 61–97. MR Zbl

[Demarche 2009a] C. Demarche, *Méthodes cohomologiques pour l'étude des points rationnels sur les espaces homogènes*, Ph.D. thesis, Université Paris-Sud, 2009.

[Demarche 2009b] C. Demarche, "Obstruction de descente et obstruction de Brauer–Manin étale", *Algebra Number Theory* **3**:2 (2009), 237–254. MR Zbl

[Fu 2011] L. Fu, *Étale cohomology theory*, Nankai Tracts in Math. **13**, World Sci., Hackensack, NJ, 2011. MR Zbl

[Harari et Skorobogatov 2002] D. Harari et A. N. Skorobogatov, "Non-abelian cohomology and rational points", *Compos. Math.* **130**:3 (2002), 241–273. MR Zbl

[Harari et Skorobogatov 2013] D. Harari et A. N. Skorobogatov, "Descent theory for open varieties", pp. 250–279 dans *Torsors, étale homotopy and applications to rational points* (Edinburgh, 2011), édité par A. N. Skorobogatov, Lond. Math. Soc. Lect. Note Ser. **405**, Cambridge Univ. Press, 2013. MR Zbl

[Kashiwara et Schapira 2006] M. Kashiwara et P. Schapira, *Categories and sheaves*, Grundlehren der Math. Wissenschaften **332**, Springer, 2006. MR Zbl

[Liu et Xu 2015] Q. Liu et F. Xu, "Very strong approximation for certain algebraic varieties", *Math. Ann.* **363**:3-4 (2015), 701–731. MR Zbl

[Manin 1971] Y. I. Manin, "Le groupe de Brauer–Grothendieck en géométrie diophantienne", pp. 401–411 dans *Actes du Congrès International des Mathématiciens, I* (Nice, 1970), édité par M. Berger et al., Gauthier-Villars, Paris, 1971. MR Zbl

[Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Math. Series **33**, Princeton Univ. Press, 1980. MR Zbl

[Miyanishi 1972] M. Miyanishi, "On the algebraic fundamental group of an algebraic group", *J. Math. Kyoto Univ.* **12**:2 (1972), 351–367. MR Zbl

[Poonen 2010] B. Poonen, "Insufficiency of the Brauer–Manin obstruction applied to étale covers", *Ann. of Math.* (2) **171**:3 (2010), 2157–2169. MR Zbl

[Poonen 2017] B. Poonen, *Rational points on varieties*, Grad. Studies in Math. **186**, Amer. Math. Soc., Providence, RI, 2017. MR Zbl

[Sansuc 1981] J.-J. Sansuc, "Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres", *J. Reine Angew. Math.* **327** (1981), 12–80. MR Zbl

[Serre 1964] J.-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Math. **5**, Springer, 1964.

[SGA 1 1971] A. Grothendieck, *Revêtements étales et groupe fondamental* (Séminaire de Géométrie Algébrique du Bois Marie 1960–1961), Lecture Notes in Math. **224**, Springer, 1971. MR Zbl

[SGA $4\frac{1}{2}$ 1977] P. Deligne, *Cohomologie étale* (Séminaire de Géométrie Algébrique du Bois Marie), Lecture Notes in Math. **569**, Springer, 1977. MR Zbl

[SGA 4_3 1973] M. Artin, A. Grothendieck et J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 3: Exposés IX–XIX* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Math. **305**, Springer, 1973. MR Zbl

[Skorobogatov 1999] A. N. Skorobogatov, "Beyond the Manin obstruction", *Invent. Math.* **135**:2 (1999), 399–424. MR Zbl

[Skorobogatov 2001] A. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Math. **144**, Cambridge Univ. Press, 2001. MR Zbl

[Skorobogatov 2009] A. Skorobogatov, "Descent obstruction is equivalent to étale Brauer–Manin obstruction", *Math. Ann.* **344**:3 (2009), 501–510. MR Zbl

[Skorobogatov et Zarhin 2014] A. N. Skorobogatov et Y. G. Zarhin, "The Brauer group and the Brauer–Manin set of products of varieties", *J. Eur. Math. Soc.* **16**:4 (2014), 749–769. MR Zbl

[Stoll 2007] M. Stoll, "Finite descent obstructions and rational points on curves", *Algebra Number Theory* **1**:4 (2007), 349–391. MR Zbl

[Szamuely 2009] T. Szamuely, *Galois groups and fundamental groups*, Cambridge Stud. Adv. Math. **117**, Cambridge Univ. Press, 2009. MR Zbl

Communicated by Bjorn Poonen
Received 2019-07-23 Revised 2020-02-10 Accepted 2020-04-12

yang.cao@math.uni-hannover.de *IAZD, Leibniz Universität Hannover, Germany*

ALGEBRA AND NUMBER THEORY 14:8 (2020)
https://doi.org/10.2140/ant.2020.14.2185

Most words are geometrically almost uniform

Michael Jeffrey Larsen

If w is a word in $d > 1$ letters and G is a finite group, evaluation of w on a uniformly randomly chosen d-tuple in G gives a random variable with values in G, which may or may not be uniform. It is known that if G ranges over finite simple groups of given root system and characteristic, a positive proportion of words w give a distribution which approaches uniformity in the limit as $|G| \to \infty$. In this paper, we show that the proportion is in fact 1.

1. Introduction

A *word* for the purposes of this paper is an element of the free group F_d. For any finite group G, the word w defines a word map $w_G \colon G^d \to G$ by substitution; we denote it w when G is understood. If U_G defines the uniform measure on G, we can measure the failure of random values of w to be uniform by comparing the pushforward $w_* U_{G^d}$ to the uniform distribution U_G. We say w is *almost uniform* for an infinite family of finite groups G if

$$\lim_{|G|\to\infty} \| w_* U_{G^d} - U_G \| = 0,$$

where $\|\cdot\|$ denotes the L^1 norm, and G ranges over the groups of the family. We are particularly interested in the family of finite simple groups.

When w is of the form w_0^k for some $k \geq 2$, then w is said to be a *power word*. It is easy to see that power words are not almost uniform for finite simple groups; for instance, in large symmetric groups, most elements are not k-th powers at all [Pouyanne 2002]. There has been speculation as to whether all nonpower words are almost uniform for finite simple groups (see, e.g., [Shalev 2013, Problem 4.7; Larsen 2014, Question 3.1]). Since power words are exponentially thin [Lubotzky and Meiri 2012], one could ask an easier question: is the set of words which are not almost uniform for finite simple groups thin? Or, easier still, does it have density 0? Some words are known to be almost uniform for finite simple groups: primitive words, which are exactly uniform for all groups; the commutator word $x_1 x_2 x_1^{-1} x_2^{-1}$ by [Garion and Shalev 2009], words of the form $x_1^m x_2^n$ by [Larsen and Shalev 2016], and, recently, all words of *Waring type*, i.e., words which can be written as a product of two nontrivial words involving disjoint variables [Larsen et al. 2019, Theorem 1]. The defining relation of the surface group of genus g is therefore covered for all $g \geq 1$, and, more generally, various words in which some variables appear

The author was partially supported by NSF grant DMS-1702152.
MSC2010: primary 20P05; secondary 11G25, 14G15, 20G40.
Keywords: word maps, random walks on finite simple groups, groups of Lie type.

exactly twice can also be treated by combining the idea of Parzanchevski and Schul [2014] with the method of Liebeck and Shalev [2005]. All of these words, of course, are in some sense rare and atypical.

From the point of view of algebraic geometry, the easiest families of finite simple groups to consider are those of the form $\underline{G}(\mathbb{F}_{q^n})/Z(\underline{G}(\mathbb{F}_{q^n}))$, where $\underline{G}$ is a simple, simply connected algebraic group over $\mathbb{F}_q$, and n ranges over the positive integers. We say that w is *geometrically almost uniform* for $\underline{G}$ if it is so for this family of groups. In [Larsen et al. 2019, Theorem 2], it is proved that this property is equivalent to an algebro-geometric condition on w, namely that the morphism of varieties $w_{\underline{G}}\colon \underline{G}^d \to \underline{G}$ (which by a theorem of Borel [1983] is dominant) has geometrically irreducible generic fiber. Using this criterion, it is proved in [Larsen et al. 2019, Theorem 3] that for each d, there exists a set of words of density greater than $\frac{1}{3}$ which are almost uniform for $\underline{G}$ for all $\underline{G}/\mathbb{F}_q$. (Note that this does not imply that these words are almost uniform for the family of all finite simple groups of Lie type.)

The main result of this paper is that for each $\underline{G}$ the set of words which are geometrically almost uniform for $\underline{G}$ has density 1. More explicitly:

Theorem 1.1. *Let $d \geq 2$, $\mathbb{F}_q$ and $\underline{G}$ be fixed. Let $(i_1, e_1), (i_2, e_2), \ldots$ be chosen independently and uniformly from $\{1, \ldots, d\} \times \{\pm 1\}$. Let $w = x_{i_1}^{e_1} \cdots x_{i_l}^{e_l}$ be a random word of length l defined in this way. Then the probability that w is geometrically almost uniform for $\underline{G}$ goes to 1 as $l \to \infty$.*

The idea of the proof is as follows. In [Larsen et al. 2019, Corollary 2.3], it is proved that if the image $\overline{w}$ of w under the abelianization map $F_d \to \mathbb{Z}^d$ is primitive, i.e., if $\gamma(\overline{w}) = 1$, where γ denotes the g.c.d. of its coordinates, then w is almost uniform for every $\underline{G}$, the idea being that $w_{\underline{G}(\mathbb{F}_{q^n})}$ is then surjective for all n, and this implies that $w_{\underline{G}}$ does not factor through a nonbirational generically finite morphism $\underline{X}_0 \to \underline{G}$.

Now, the image of a random walk on F_d under the abelianization map is a random walk on $\mathbb{Z}^d$. If $\mathsf{X}_{d,l}$ is the endpoint of a random walk of length l on $\mathbb{Z}^d$, then

$$\limsup_{l\to\infty} \boldsymbol{P}[\gamma(\mathsf{X}_{d,l}) = 1] < 1$$

for all d, so this is not good enough to get a result which covers almost all words. A new idea is needed.

By a probabilistic analysis, we prove that for each d,

$$\lim_{M\to\infty} \liminf_{l\to\infty} \boldsymbol{P}[1 \leq \gamma(\mathsf{X}_{d,l}) \leq M] = 1.$$

Thus, it suffices to prove that for each $d \geq 2$ and $k > 0$, in the limit as l goes to infinity, the fraction of w of length l with $\gamma(\overline{w}) = k$ for which w is almost uniform in rank $\leq r$ goes to 1. For any such w and any group G, the image of w_G contains all k-th powers in G. For $k > 1$, this no longer implies geometric irreducibility of the generic fiber of $w_{\underline{G}}$, but it puts very strong constraints on which quasifinite morphisms $\underline{X}_0 \to \underline{G}$ it can factor through.

To see how to exploit such constraints, consider the following toy problem. Suppose a polynomial map $f\colon \mathbb{A}^1 \to \mathbb{A}^1$ is defined over $\mathbb{F}_q$; for all n, $f(\mathbb{F}_{q^n})$ contains all squares in $\mathbb{F}_{q^n}$; and for some n_0, $f(\mathbb{F}_{q^{n_0}})$ contains a nonsquare. We claim this implies f is purely inseparable.

Indeed, consider the curve $\underline{C}\colon\ y^2 = f(x)$. For $\underline{C}$ to fail to be geometrically irreducible would mean that $f(x) = g(x)^2$ for some $g(x) \in \overline{\mathbb{F}}_q[x]$. Either $g(x) \in \mathbb{F}_q[x]$ or $f(x) = ah(x)^2$ for some nonsquare $a \in \mathbb{F}_q$ and some $h(x) \in \mathbb{F}_q[x]$. In the first case, $f(\mathbb{F}_{q^{n_0}})$ contains only squares in $\mathbb{F}_{q^{n_0}}$, contrary to assumption. In the second case, for all $n \geq 1$, $f(\mathbb{F}_{q^n})$ contains no nonzero square in $\mathbb{F}_{q^n}$.

Thus, the conditions on the image of f imply that $\underline{C}$ is geometrically irreducible, so it has $(1 + o(1))q^n$ points over $\mathbb{F}_{q^n}$ by the Lang–Weil estimate. Consider the y-map, that is, the morphism of degree $\deg f$ from $\underline{C}$ to the affine line given by the function y. By the Chebotarev density theorem for finite extensions of $\mathbb{F}_q(t)$, in the limit as $n \to \infty$, a fixed positive proportion of points in $\mathbb{A}^1(\mathbb{F}_{q^n})$ have preimage in $\underline{C}(\mathbb{F}_{q^n})$ consisting of $\deg_s f$ points, where $\deg_s$ denotes the separable degree of f. Since the y-map is surjective on $\mathbb{F}_{q^n}$-points, this implies that f is purely inseparable.

To apply this idea in the word map setting, one needs to find elements in $w(\underline{G}(\mathbb{F}_{q^n})^d)$ which play the role of nonsquare elements in $f(\mathbb{F}_{q^n})$. We do not need to find them for all w, just for almost all in an asymptotic sense. An approach to achieving this is to fix a d-tuple $\boldsymbol{g} \in \underline{G}(\mathbb{F}_{q^n})^d$ and estimate the probability that $w(\boldsymbol{g})$ is a “nonsquare” element. For large enough n, one can view $w(\boldsymbol{g})$ as uniformly distributed in $\underline{G}(\mathbb{F}_{q^n})$. In order to get the probability of success to approach 1, it is necessary to use not a single $\boldsymbol{g}$ but a sufficiently large number of independent choices $\boldsymbol{g}_1, \dots, \boldsymbol{g}_N$. The existence of N elements of $\underline{G}(\mathbb{F}_{q^n})^d$ which are independent in this sense (in the limit $n \to \infty$) depends on $\underline{G}(\mathbb{F}_{q^n})^N$ being d-generated. There is a substantial literature, going back to work of Philip Hall [1936], concerning the size of minimal generating sets of G^N, where G is a finite simple group. We use a recent result of Maróti and Tamburini Bellani [2013].

2. Varieties over finite fields

Throughout this section, a *variety* will always mean a geometrically integral affine scheme of finite type over a finite field. Let $A \subset B$ be an inclusion of finitely generated $\mathbb{F}_q$-algebras such that $\underline{X} := \operatorname{Spec} A$ and $\underline{Y} := \operatorname{Spec} B$ are normal varieties. Let $\phi\colon \underline{Y} \to \underline{X} = \operatorname{Spec} A$ correspond to the inclusion $A \subset B$. Let K and L denote the fraction fields of A and B respectively. Let K_0 denote the separable closure of K in L, which is a finite extension of K since L is finitely generated. Let A_0 denote the integral closure of A in K_0, $\underline{X}_0$ the spectrum of A_0, and $\psi\colon \underline{X}_0 \to \underline{X}$ the morphism corresponding to the inclusion $A \subset A_0$. As $B \supset A$ is integrally closed in $L \supset K_0$ it follows that B contains A_0, so ϕ factors through ψ.

Proposition 2.1. *For all positive integers n,*

$$\phi(\underline{Y}(\mathbb{F}_{q^n})) \subset \psi(\underline{X}_0(\mathbb{F}_{q^n})), \tag{2-1}$$

$$\textit{and} \quad |\psi(\underline{X}_0(\mathbb{F}_{q^n}))| - |\phi(\underline{Y}(\mathbb{F}_{q^n}))| = o(q^{n \dim \underline{X}}). \tag{2-2}$$

Moreover ψ is an isomorphism if and only if ϕ has geometrically irreducible generic fiber; *if not*, *there exists $\epsilon > 0$ and a positive integer m such that*

$$|\psi(\underline{X}_0(\mathbb{F}_{q^n}))| < (1 - \epsilon)q^{n \dim \underline{X}} \tag{2-3}$$

if m divides n.

Proof. As $A \subset A_0 \subset B$, the morphism ϕ factors through ψ, implying (2-1).

By [EGA IV$_2$ 1965, proposition 4.5.9], $K = K_0$ if and only if the generic fiber of ϕ is geometrically irreducible. By the same proposition, the generic fiber of $\underline{Y} \to \underline{X}_0$ is always geometrically irreducible. By [EGA IV$_3$ 1966, théorème 9.7.7], there is a dense open subset of $\underline{X}_0$ over which the fibers of $\underline{Y} \to \underline{X}_0$ are all geometrically irreducible. Let $\underline{C}$ denote the complement of this subset, endowed with its structure of reduced closed subscheme of $\underline{X}_0$.

It is well known that the Lang–Weil estimate is uniform in families. There does not seem to be a canonical reference for this fact, but a proof is sketched, for instance in [Larsen and Shalev 2012, Proposition 3.4; Tao 2012, Theorem 5]. From this, it follows that if n is sufficiently large, for every point of $\underline{X}_0(\mathbb{F}_{q^n})$ over which the morphism $\underline{Y} \to \underline{X}_0$ has geometrically irreducible fiber, there exists an $\mathbb{F}_{q^n}$-point in this fiber. In particular, every point in $\underline{X}_0(\mathbb{F}_{q^n}) \setminus \underline{C}(\mathbb{F}_{q^n})$ lies in the image of $\underline{Y}(\mathbb{F}_{q^n}) \to \underline{X}_0(\mathbb{F}_{q^n})$. By the easy part of the Lang–Weil bound,

$$|\underline{C}(\mathbb{F}_{q^n})| = O(q^{n \dim \underline{C}}) \leq O(q^{n(\dim \underline{X}_0 - 1)}).$$

Thus, the complement of the image of $\underline{Y}(\mathbb{F}_{q^n}) \to \underline{X}_0(\mathbb{F}_{q^n})$ has cardinality $o(q^{n \dim \underline{X}})$, which implies (2-2).

If ϕ is not geometrically irreducible, then $[K_0 : K] > 1$. Let K_1 denote the Galois closure of K_0/K in a fixed separable closure $\bar{K}$. We choose m so that $\mathbb{F}_{q^m}$ contains the algebraic closure of $\mathbb{F}_q$ in K_1. If we are content to limit consideration to $\mathbb{F}_{q^n}$-points of $\underline{X}$ and $\underline{X}_0$, where m divides n, we may replace $\underline{X}$ and $\underline{X}_0$ by the varieties $\underline{X}_{\mathbb{F}_{q^m}}$ and $(\underline{X}_0)_{\mathbb{F}_{q^m}}$ respectively, obtained by base change. This has the effect of replacing K, K_0, and K_1 by $K\mathbb{F}_{q^m}$, $K_0\mathbb{F}_{q^m}$, and $K_1\mathbb{F}_{q^m} = K_1$ respectively. Replacing q by q^m, we may now assume that $\mathbb{F}_q$ is algebraically closed in K_1.

Now, $\mathrm{Gal}(K_1/K)$ acts faithfully on A_1 as $\mathbb{F}_q$-algebra. As A is integrally closed in K and A_1 is the integral closure of A in K_1, it follows that

$$A \subset A_1^{\mathrm{Gal}(K_1/K)} \subset A_1 \cap K = A,$$

so $A = A_1^{\mathrm{Gal}(K_1/K)}$; likewise, $A_0 = A_1^{\mathrm{Gal}(K_1/K_0)}$. Geometrically, this means that $\underline{X}$ and $\underline{X}_0$ are the quotients of $\underline{X}_1 := \operatorname{Spec} A_1$ by $\mathrm{Gal}(K_1/K)$ and $\mathrm{Gal}(K_1/K_0)$ respectively. We denote these quotient maps π and π_0 respectively. Thus we have the diagram

$$\begin{tikzcd}
\underline{X}_1 \arrow[d, "\pi_0"'] \arrow[dd, bend left, "\pi"] \\
\underline{X}_0 \arrow[d, "\psi"'] \\
\underline{X}
\end{tikzcd}$$

As the action of $\mathrm{Gal}(K_1/K)$ on $\underline{X}_1$ is faithful and $\underline{X}_1$ is irreducible, there is a dense affine open subvariety of $\underline{X}_1$ on which $\mathrm{Gal}(K_1/K)$ acts freely. Replacing $\underline{X}_1$ by this subvariety and $\underline{X}$ and $\underline{X}_0$ by quotients of this subvariety by $\mathrm{Gal}(K_1/K)$ and $\mathrm{Gal}(K_1/K_0)$ respectively affects $o(q^{n \dim \underline{X}})$ of the

$\mathbb{F}_{q^n}$-points of $\underline{X}$, $\underline{X}_0$, and $\underline{X}_1$, so without loss of generality, we may assume that $\mathrm{Gal}(K_1/K)$ acts freely on $\underline{X}_1$. Now

$$\psi(\underline{X}_0(\mathbb{F}_{q^n})) = \psi(\underline{X}_0(\mathbb{F}_{q^n}) \setminus \pi_0(\underline{X}_1(\mathbb{F}_{q^n}))) \cup \pi(\underline{X}_1(\mathbb{F}_{q^n})). \tag{2-4}$$

By Lang–Weil, $|\underline{X}_1(\mathbb{F}_{q^n})| = (1+o(1))q^{n \dim \underline{X}}$, so

$$|\pi_0(\underline{X}_1(\mathbb{F}_{q^n}))| = ([K_1 : K_0]^{-1} + o(1))q^{n \dim \underline{X}},$$
$$|\pi(\underline{X}_1(\mathbb{F}_{q^n}))| = ([K_1 : K]^{-1} + o(1))q^{n \dim \underline{X}}.$$

By (2-4),

$$|\psi(\underline{X}_0(\mathbb{F}_{q^n}))| \le (1 - [K_1 : K_0]^{-1} + [K_1 : K]^{-1} + o(1))q^{n \dim \underline{X}},$$

which implies (2-3). □

Lemma 2.2. *Let G be a finite group acting transitively on a set S with more than one element and H a normal subgroup of G such that every element of H has at least one fixed point in S. Then for all $s \in S$, $H\,\mathrm{Stab}_G(s)$ is a proper subgroup of G.*

Proof. By a classical theorem of Jordan, every nontrivial transitive permutation group contains a derangement, so H must act intransitively. Thus, the orbit of $H\,\mathrm{Stab}_G(s)$ containing s is a proper subset of S, which implies the lemma. □

Lemma 2.3. *Let K be a field, $\overline{K}$ a separable closure of K, and K_1 and K_2 finite extensions of K in $\overline{K}$. Suppose K_1 is Galois over K and $K_2 \ne K$. If $K_1 \cap K_2 = K$, then there exists an element of* $\mathrm{Gal}(\overline{K}/K_1)$ *which does not stabilize any K-embedding of K_2 in $\overline{K}$.*

Proof. Let K_3 be the Galois closure of K_2 in $\overline{K}$ and define $G := \mathrm{Gal}(K_1K_3/K)$. Thus G acts transitively on the set S of K-embeddings of K_2 in $\overline{K}$. Let $H = \mathrm{Gal}(K_1K_3/K_1)$, which is normal in G since K_1/K is Galois. If every element of $\mathrm{Gal}(\overline{K}/K_1)$ fixes at least one element of S, then by Lemma 2.2, $H\,\mathrm{Stab}_G(s)$ is a proper subgroup of G, where s denotes the identity embedding of K_2 in $\overline{K}$. If L is the fixed field of K_1K_3 under $H\,\mathrm{Stab}_G(s)$, then L is a nontrivial extension of K contained in both $(K_1K_3)^H = K_1$ and $(K_1K_3)^{\mathrm{Stab}_G(s)} = K_2$. □

Proposition 2.4. *Let $\underline{X}$ be a variety over $\mathbb{F}_q$ with coordinate ring A with function field K. Let $K \subset K_0, K_2 \subset \overline{K}$, and let K_1* (resp. K_3) *denote the Galois closure of K_0* (resp. K_2) *in $\overline{K}$. Let A_i for $0 \le i \le 3$ denote the integral closure of A in K_i, and let $\underline{X}_i :=$* $\mathrm{Spec}\,A_i$. *If K_1 and K_2 satisfy the hypotheses of Lemma 2.3, then there exists $\epsilon > 0$ so that for all sufficiently large integers n, there are at least $\epsilon q^{n \dim \underline{X}}$ elements of $\underline{X}(\mathbb{F}_{q^n})$ which lie in the image of $\underline{X}_i(\mathbb{F}_{q^n}) \to \underline{X}(\mathbb{F}_{q^n})$ for $i = 0$ but not for $i = 2$.*

Proof. Let $K_{13} = K_1K_3$, A_{13} denote the integral closure of A in K_{13}, and $\underline{X}_{13}$ denote $\mathrm{Spec}\,A_{13}$. Let $G := \mathrm{Gal}(K_{13}/K)$. The action of G on $\underline{X}_{13}$ is faithful, and $\underline{X}_{13}$ is irreducible, so there exists a dense open affine subvariety $\underline{U}_{13} \subset \underline{X}_{13}$ on which G acts freely. Replacing $\underline{X}_{13}$, together with its quotients by subgroups of G, by $\underline{U}_{13}$ and its corresponding quotients affects only $o(q^{n \dim \underline{X}})$ $\mathbb{F}_{q^n}$-points of these quotients, and therefore does not affect the statement of the proposition. We may therefore assume that we are in the setting of [Serre 1965, Theorem 6] and can apply the Chebotarev density theorem for varieties.

By Lemma 2.3, there exists $g \in G$ such that g acts trivially on K_1 but acts without fixed points on the set of K-embeddings $K_2 \to \overline{K}$ or, equivalently, on the geometric points lying over any given geometric point of $\underline{X}$ for the covering map $\underline{X}_2 \to \underline{X}$. This implies that if $x \in \underline{X}(\mathbb{F}_{q^n})$ and g belongs to the q^n-Frobenius conjugacy class of x, then there is no q^n-Frobenius stable point lying over x on $\underline{X}_2 \to \underline{X}$, i.e., x does not lie in the image of $\underline{X}_2(\mathbb{F}_{q^n}) \to \underline{X}(\mathbb{F}_{q^n})$. On the other hand, every geometric point of $\underline{X}_0$ lying over x is stable by the q^n-Frobenius, so x lies in the image of $\underline{X}_0(\mathbb{F}_{q^n}) \to \underline{X}(\mathbb{F}_{q^n})$. By Chebotarev density [Serre 1965, Theorem 7], the proposition follows for every $\epsilon < |G|^{-1}$. □

The main technical result of this section is the following.

Proposition 2.5. *Let $\phi\colon \underline{Y} \to \underline{X}$ be a dominant morphism of normal varieties over $\mathbb{F}_q$. Then there exists a positive integer m and for every positive integer n, there exist subsets $X_{n,i} \subset \underline{X}(\mathbb{F}_{q^n})$, $1 \le i \le m$, with the following properties.*

(1) *For each i from 1 to m, we have* $\liminf_n \dfrac{|X_{n,i}|}{|\underline{X}(\mathbb{F}_{q^n})|} > 0.$

(2) *If $\theta\colon \underline{Z} \to \underline{X}$ is any dominant morphism of normal varieties over $\mathbb{F}_q$ such that*

(a) *for all $n \ge 1$, $\theta(\underline{Z}(\mathbb{F}_{q^n})) \supset \phi(\underline{Y}(\mathbb{F}_{q^n}))$, and*

(b) *there exists an integer $n_0 \ge 1$ such that $\theta(\underline{Z}(\mathbb{F}_{q^{n_0}})) \cap X_{n_0,i}$ is nonempty for each $i = 1, \ldots, m$,*

then the generic fiber of θ is geometrically irreducible.

Proof. Let A, B, C denote the coordinate rings of $\underline{X}$, $\underline{Y}$, and $\underline{Z}$ respectively. Let K, L, and M be the fields of fractions of A, B, and C respectively. We regard B and C as A-algebras via ϕ and θ respectively, so L and M are extensions of K. Let K_0 and K_2 denote the separable closures of K in L and M respectively. As B and C are finitely generated $\mathbb{F}_q$-algebras, L and M are finitely generated K-extensions, and K_0 and K_2 are finite separable extensions of K. The claimed generic irreducibility of the generic fiber of θ amounts to the equality $K = K_2$. We define $\overline{K}$, K_1, K_3, and K_{13} as in Proposition 2.4.

Let $F_1, \ldots, F_m$ denote all subfields of K_1 over K, excluding K itself. Thus, we have the following diagram of fields:

$$\begin{tikzcd}
 & & & L \arrow[ddd, dash] & \overline{K} \arrow[d, dash] & M \arrow[ddd, dash] \\
 & & & & K_{13} \arrow[dl, dash] \arrow[dr, dash] & \\
 & & & K_1 \arrow[d, dash] \arrow[dlll, dash] \arrow[dl, dash] & & K_3 \arrow[d, dash] \\
F_1 \arrow[drrrr, dash] & \cdots & F_m \arrow[drr, dash] & K_0 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
 & & & & K &
\end{tikzcd} \tag{2-5}$$

For $0 \le i \le 3$, let A_i denote the integral closure of A in K_i and $\underline{X}_i = \operatorname{Spec} A_i$; likewise for A_{13} and $\underline{X}_{13}$. For $1 \le i \le m$, let D_i denote the integral closure of A in the field F_i, and let $\underline{W}_i := \operatorname{Spec} D_i$. By (2-5), we have the following diagram of varieties:

$$\begin{tikzcd}
 & & \underline{Y} \arrow[dddr, bend right] & & & & \underline{Z} \arrow[dddl, bend left] \\
 & & & & \underline{X}_{13} \arrow[dl] \arrow[dr] & & \\
 & & & \underline{X}_1 \arrow[dlll] \arrow[dl] \arrow[d] & & \underline{X}_3 \arrow[d] & \\
\underline{W}_1 \arrow[drrrr] & \cdots & \underline{W}_m \arrow[drr] & \underline{X}_0 \arrow[dr] & & \underline{X}_2 \arrow[dl] & \\
 & & & & \underline{X} & &
\end{tikzcd}$$

Let $X_{n,i}$ denote the complement of the image of $\underline{W}_i(\mathbb{F}_{q^n})$ in $\underline{X}(\mathbb{F}_{q^n})$. By (2-3) and the Lang–Weil estimate, for $1 \le i \le m$,

$$|X_{n,i}| \ge \epsilon q^{\dim \underline{X}} > \frac{\epsilon}{2} |\underline{X}(\mathbb{F}_{q^n})| \tag{2-6}$$

if n is sufficiently large, which implies property (1).

Moreover, if $\theta \colon \underline{Z} \to \underline{X}$ is a dominant morphism satisfying condition (a), then for all $n \ge 1$, $\theta(\underline{Z}(\mathbb{F}_{q^n})) \supset \phi(\underline{Y}(\mathbb{F}_{q^n}))$, implying that

$$\begin{aligned}
&\bigl|\operatorname{im}(\underline{X}_1(\mathbb{F}_{q^n}) \to \underline{X}(\mathbb{F}_{q^n})) \setminus \operatorname{im}(\underline{X}_2(\mathbb{F}_{q^n}) \to \underline{X}(\mathbb{F}_{q^n}))\bigr| \\
&\qquad \le \bigl|\operatorname{im}(\underline{X}_0(\mathbb{F}_{q^n}) \to \underline{X}(\mathbb{F}_{q^n})) \setminus \operatorname{im}(\underline{X}_2(\mathbb{F}_{q^n}) \to \underline{X}(\mathbb{F}_{q^n}))\bigr| \\
&\qquad = \bigl|\operatorname{im}(\underline{Y}(\mathbb{F}_{q^n}) \to \underline{X}(\mathbb{F}_{q^n})) \setminus \operatorname{im}(\underline{Z}(\mathbb{F}_{q^n}) \to \underline{X}(\mathbb{F}_{q^n}))\bigr| + o(q^{n \dim \underline{X}}) \\
&\qquad = \bigl|\phi(\underline{Y}(\mathbb{F}_{q^n})) \setminus \theta(\underline{Z}(\mathbb{F}_{q^n}))\bigr| + o(q^{n \dim \underline{X}}) \\
&\qquad = o(q^{n \dim \underline{X}}).
\end{aligned}$$

If $K_2 \ne K$, Proposition 2.4 implies that $K_1 \cap K_2$ must be a nontrivial extension of K, so $F_i \subset K_2$ for some $i \in [1, m]$. Thus, for n_0 as in (b),

$$\theta(\underline{Z}(\mathbb{F}_{q^{n_0}})) \subset \operatorname{im}(\underline{X}_2(F_{q^{n_0}}) \to \underline{X}(\mathbb{F}_{q^{n_0}})) \subset \operatorname{im}(\underline{W}_i(\mathbb{F}_{q^{n_0}}) \to \underline{X}(\mathbb{F}_{q^{n_0}})),$$

contrary to the assumption that $\theta(\underline{Z}(\mathbb{F}_{q^{n_0}})) \cap X_{n_0,i}$ is nonempty for each i. We conclude that $K_2 = K$, and the proposition follows. □

3. Random walks

This section does not claim any original results. Its goal is to present well known ideas in probability theory in the form needed for the proof of Theorem 1.1.

For any positive integer d and nonnegative integer l, we define $\mathsf{X}_{d,l}$ to be the convolution of l i.i.d. random variables on $\mathbb{Z}^d$, each uniformly distributed over the $2d$-element set $\{\pm e_1, \dots, \pm e_d\}$, where $e_1, \dots, e_d$ are the standard generators of $\mathbb{Z}^d$. When $d = 2$, we write X_l for short.

The main result in this section is the following.

Proposition 3.1. *For all $d \geq 2$ and $\epsilon > 0$, there exist M and N such that for $l \geq N$,*

$$\boldsymbol{P}\Bigl[\mathsf{X}_{d,l} \in \bigcup_{i>M} i\mathbb{Z}^d\Bigr] < \epsilon.$$

We begin with a general result.

Lemma 3.2. *Let G be a finite group and S a* (not necessarily symmetric) *set of generators. Let $\mathsf{S}_1, \mathsf{S}_2, \dots$ be i.i.d. random variables on G with support S. Let $\mathsf{G}_l = \mathsf{S}_1 \cdots \mathsf{S}_l$. Suppose that there does not exist a homomorphism from G to any nontrivial cyclic group C mapping S to a single element. Then the limit as $l \to \infty$ of the distribution of G_l is the uniform distribution on G.*

Proof. Consider the Markov chain with state space G in which the probability of a transition from g to hg is $\boldsymbol{P}[\mathsf{S}_i = h]$. Since the uniform distribution is stationary, it suffices to check that this Markov chain is irreducible and periodic [Levin et al. 2009, Theorem 4.9]. Irreducibility is immediate from the condition that S generates G. If the Markov chain is periodic, then for some proper subset $X \subset G$ and some integer j, $s_1 \cdots s_j \in \mathrm{Stab}_G(X)$ for all $s_i \in S$. Let G_j denote the subgroup of G generated by

$$\{s_1 \cdots s_j \mid s_1, \dots, s_j \in S\}.$$

As $G_j \subset \mathrm{Stab}_G(X) \subsetneq G$, G_j is a proper subgroup of G.

Consider the subgroup $\widetilde{G}$ of $G \times \mathbb{Z}/j\mathbb{Z}$ generated by $\{(s, 1) \mid s \in S\}$. By definition, the kernel of projection on the second factor is G_j. By Goursat's Lemma, $\widetilde{G}$ is the pullback to $G \times \mathbb{Z}/j\mathbb{Z}$ of the graph of an isomorphism between G/G_j and a quotient of $\mathbb{Z}/j\mathbb{Z}$. This identifies G/G_j with a nontrivial cyclic group C, and all elements of S map to the same generator of C, contrary to hypothesis. □

The remaining results in this section are needed for the proof of Proposition 3.1.

Lemma 3.3. *Let $p > 2$ be prime, k a positive integer, and $\epsilon > 0$. For l sufficiently large,*

$$\boldsymbol{P}[\mathsf{X}_l \in p^k\mathbb{Z}^2] < \frac{1+\epsilon}{p^{2k}}.$$

Proof. The image under (mod p^k) reduction of our random walk on $\mathbb{Z}^2$ is a random walk on $G = (\mathbb{Z}/p^k\mathbb{Z})^2$ with generating set $S = \{\pm 1, 0), (0, \pm 1)\}$. As differences between elements of S generate G, there is no proper coset of G which contains S. By Lemma 3.2, X_l becomes uniformly distributed (mod p^k) in the limit $l \to \infty$, which implies the lemma. □

Lemma 3.4. *Let k be a positive integer, and $\epsilon > 0$. For l sufficiently large,*

$$\boldsymbol{P}[\mathsf{X}_l \in 2^k\mathbb{Z}^2] < \frac{2+\epsilon}{4^k}.$$

Proof. If l is odd, the probability that $\mathsf{X}_l \in 2\mathbb{Z}^2$ is zero. We therefore assume $l = 2l_0$, so X_l is the sum of l_0 i.i.d. random variables supported on

$$\{(\pm 2, 0), (0, \pm 2), (\pm 1, \pm 1), (0, 0)\}.$$

Reducing (mod 2^k), we obtain an irreducible aperiodic random walk on $\ker(\mathbb{Z}/2^k\mathbb{Z})^2 \to \mathbb{Z}/2\mathbb{Z}$, and the argument proceeds as before by Lemma 3.2. □

Proposition 3.5. *For all $\epsilon > 0$, there exist M and N such that for $l \geq N$,*

$$\boldsymbol{P}\Bigl[\mathsf{X}_l \in \bigcup_{i>M} i\mathbb{Z}^2\Bigr] < \epsilon.$$

Proof. By [Larsen et al. 2019, Proposition 3.2], if $p > 2$ is prime,

$$\boldsymbol{P}[\mathsf{X}_l \in p\mathbb{Z}^2 \setminus \{(0,0)\}] < \frac{4}{(p+1)^2}.$$

We choose $s \geq 2$ large enough that

$$\sum_{p>s} \frac{4}{(p+1)^2} < \frac{\epsilon}{2}$$

and choose k such that $3s/4^k < \epsilon/2$, so that if l is sufficiently large, the total probability that $\mathsf{X}_l \in p^k\mathbb{Z}^2$ for some $p \leq s$ is less than $\epsilon/2$. Note that this includes the probability that $\mathsf{X}_l = (0,0)$. Let M be larger than $s\prod_{p\leq s} p^k$. If $i > M$, then either i has a prime factor greater than s or a prime factor $\leq s$ with multiplicity at least k. The probability that there exists $i > M$ such that $G \in i\mathbb{Z}^2$ is therefore less than ϵ. □

Proof of Proposition 3.1. The projection of a random walk on $\mathbb{Z}^d$ onto the first two coordinates gives a random walk on $\mathbb{Z}^2$ where each of the four possible nonzero steps are equally likely, but a zero step is also possible in the projection if $d > 2$. Since the projection of an element of $i\mathbb{Z}^d$ is an element of $i\mathbb{Z}^2$, the conditional probability that $\mathsf{X}_{d,l} \in \bigcup_{i>M} i\mathbb{Z}^d$ if we condition on at least l_0 steps which are nonzero in the projection is less than $\epsilon/2$ if l_0 is large enough. Given l_0 the probability that there are less than l_0 steps nonzero in the projection goes to 0 as l goes to infinity, so it can be taken to be less than $\epsilon/2$, implying that $\boldsymbol{P}\bigl[\mathsf{X}_{d,l} \in \bigcup_{i>M} i\mathbb{Z}^d\bigr] < \epsilon$. □

4. Proof of Theorem 1.1

We now prove the main theorem.

Proof. Fix a simple, simply connected algebraic group $\underline{G}$ over a finite field $\mathbb{F}_q$. We apply Proposition 2.5 in the case $\underline{X} = \underline{G}$, $\underline{Y} = \underline{G}$, $\underline{Z} = \underline{G}^d$, ϕ is the k-th power map for some positive integer k, and θ is the evaluation map w for some $w \in F_d$ for which $\overline{w} = (a_1, \dots, a_d)$ and $\gamma(a_1, \dots, a_d) = k$. Given w, there exist integers $b_1, \dots, b_d$ for which $k = a_1 b_1 + \cdots + a_d b_d$, so that

$$w_{\underline{G}(\mathbb{F}_{q^n})}(g^{b_1}, \dots, g^{b_d}) = g^k$$

for all n and all $g \in \underline{G}(\mathbb{F}_{q^n})$, so $\phi(\underline{G}(\mathbb{F}_{q^n})) \subset \theta(\underline{G}(\mathbb{F}_{q^n}))$ for all $n \geq 1$.

By the main theorem of [Maróti and Tamburini Bellani 2013], for every finite simple group Γ, there exists a 2-element generating set of Γ^N whenever $N \leq 2\sqrt{|\Gamma|}$. Let n_0 be any positive integer. Defining $N_0 := q^{n_0}$ and applying this to $\Gamma := \underline{G}(\mathbb{F}_{q^{n_0}})/Z(\underline{G}(\mathbb{F}_{q^{n_0}}))$, we see that Γ^{N_0} is d-generated. As $G := \underline{G}(\mathbb{F}_{q^{n_0}})^{N_0}$ is a perfect central extension of Γ^{N_0}, lifting any set of d generators of the latter to the former, we again obtain a generating set.

We denote by

$$S = \{(g_{i1}, \dots, g_{iN_0}) \mid 1 \leq i \leq d\}$$

a generating set of G and consider an l-step random walk on this group with generating set S. By Lemma 3.2, for all $\delta > 0$, if l sufficiently large, the probability that the walk ends in any subset $T \subset G$ is at least

$$(1 - \delta/2)|T|/|G|.$$

We define $T := T_0 \cup \cdots \cup T_{\lfloor N_0/m \rfloor - 1}$, where

$$T_i := \underline{G}(\mathbb{F}_{q^{n_0}})^{im} \times X_{n_0,1} \times \cdots \times X_{n_0,m} \times \underline{G}(\mathbb{F}_{q^{n_0}})^{N_0-(i+1)m},$$

and $X_{n_0,i}$ are defined as in Proposition 2.5.

To estimate the probability that a uniformly randomly chosen element of G lies in T, we note that membership in the T_i are independent conditions. The probability of membership in each T_i is

$$\prod_{j=1}^{m} \frac{|X_{n_0,j}|}{|\underline{G}(\mathbb{F}_{q^{n_0}})|} \geq \frac{\epsilon^m}{2^m}$$

by (2-6). Therefore, the probability of membership in T for a uniformly chosen element of G is at least

$$1 - (1 - \epsilon^m/2^m)^{\lfloor N_0/m \rfloor}.$$

Taking n_0 (and therefore N_0) sufficiently large, we can guarantee this exceeds $1-\delta/2$. Thus, the probability that the random walk ends in T is greater than $1 - \delta$.

For $1 \leq j \leq N_0$, let $\boldsymbol{g}_j = (g_{1j}, \dots, g_{dj})$. We have seen that for a random word w of length n, the probability that $(w(\boldsymbol{g}_1), \dots, w(\boldsymbol{g}_{N_0})) \in T$ is greater than $1 - \delta$. Membership in T implies membership in some T_i, which implies

$$w(\boldsymbol{g}_{im+1}) \in X_{n_0,1}, \dots, w(\boldsymbol{g}_{im+m}) \in X_{n_0,m},$$

and therefore, by Proposition 2.5, if $\gamma(\overline{w}) = k$, then w is geometrically almost uniform for $\underline{G}$.

Thus, for each k, the probability is $\leq \delta$ that a random word w of length l satisfies $\gamma(\overline{w}) = k$ and that w is not geometrically almost uniform. By Proposition 3.1, for each fixed $\epsilon > 0$, there exists M such that if

l is large enough, then the probability that $\gamma(\overline{w})$ is zero or greater than M for a word of length l is less than ϵ. Therefore, the probability that w is not geometrically almost uniform for $\underline{G}$ is less than $\epsilon + M\delta$. Choosing first ϵ and then δ, we can make this quantity as small as we wish, proving the theorem. □

We remark that the proof also shows that almost all words w are almost uniform for the family of groups $\{\underline{G}(\mathbb{F}_{q^n}) \mid n \geq 1\}$. The proof, together with that of [Larsen et al. 2019, Theorem 2], implies that w is almost always uniform for all finite simple groups with fixed root system and characteristic. For instance, almost all w are almost uniform for the Suzuki and Ree groups.

5. Questions

Question 5.1. If $\mathcal{G}$ is a simple, simply connected group scheme over $\mathbb{Z}$, does the probability that a random word is almost uniform for all simple groups of the form $\mathcal{G}(\mathbb{F}_q)/Z(\mathcal{G}(\mathbb{F}_q))$ go to 1?

It seems likely that the methods of this paper will allow one to prove this for all characteristics satisfying some Chebotarev-type condition, but can one do it for all characteristics simultaneously, or even a density one set of characteristics? Even more optimistically, one can ask:

Question 5.2. Does the probability that a random word is geometrically almost uniform for all simple, simply connected algebraic groups over finite fields go to 1?

Given an e-tuple of words $w_1, \dots, w_e \in F_d$, for each G we can define a function $G^d \to G^e$, and we can ask about almost uniformity. In geometric families, this reduces again to the question of the geometric irreducibility of the generic fiber of the morphism $\underline{G}^d \to \underline{G}^e$ for simple, simply connected algebraic groups over finite fields. In the case that

$$\mathbb{Z}^d / \operatorname{Span}_{\mathbb{Z}}(\overline{w}_1, \dots, \overline{w}_e) \cong \mathbb{Z}^{d-e},$$

the function $\underline{G}(\mathbb{F}_{q^n})^d \to \underline{G}(\mathbb{F}_{q^n})^e$ is surjective. Geometric irreducibility for such words follows as before.

Question 5.3. For $e < d$, does the probability that a random e-tuple of elements of F_d of length n is geometrically almost uniform go to 1 as $n \to \infty$?

Question 5.2 has an analogue for simple, simply connected compact Lie groups. As a special case, one can ask:

Question 5.4. Does the probability that for a random word w of length n

$$\lim_{m\to\infty} \left\| w_* U_{\mathrm{SU}(m)^d} - U_{\mathrm{SU}(m)} \right\| = 0$$

go to 1 as $n \to \infty$?

Acknowledgements

I would like to thank Aner Shalev for his useful comments on an earlier version of this paper. I also want to express my gratitude to the referee for pointing out a number of inaccuracies in an earlier draft of this paper and suggesting several improvements in the exposition.

References

[Borel 1983] A. Borel, "On free subgroups of semisimple groups", *Enseign. Math.* (2) **29**:1-2 (1983), 151–164. MR Zbl

[EGA IV$_2$ 1965] A. Grothendieck, "Eléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, II", *Inst. Hautes Études Sci. Publ. Math.* **24** (1965), 5–231. MR Zbl

[EGA IV$_3$ 1966] A. Grothendieck, "Eléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, III", *Inst. Hautes Études Sci. Publ. Math.* **28** (1966), 5–255. MR Zbl

[Garion and Shalev 2009] S. Garion and A. Shalev, "Commutator maps, measure preservation, and T-systems", *Trans. Amer. Math. Soc.* **361**:9 (2009), 4631–4651. MR Zbl

[Hall 1936] P. Hall, "The Eulerian function of a group", *Q. J. Math. Oxford* (2) **7** (1936), 134–151.

[Larsen 2014] M. Larsen, "How random are word maps?", pp. 141–149 in *Thin groups and superstrong approximation* (Berkeley, 2012), edited by E. Breuillard and H. Oh, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, 2014. MR Zbl

[Larsen and Shalev 2012] M. Larsen and A. Shalev, "Fibers of word maps and some applications", *J. Algebra* **354** (2012), 36–48. MR Zbl

[Larsen and Shalev 2016] M. Larsen and A. Shalev, "On the distribution of values of certain word maps", *Trans. Amer. Math. Soc.* **368**:3 (2016), 1647–1661. MR Zbl

[Larsen et al. 2019] M. Larsen, A. Shalev, and P. H. Tiep, "Probabilistic Waring problems for finite simple groups", *Ann. of Math.* (2) **190**:2 (2019), 561–608. MR Zbl

[Levin et al. 2009] D. A. Levin, Y. Peres, and E. L. Wilmer, *Markov chains and mixing times*, Amer. Math. Soc., Providence, RI, 2009. MR Zbl

[Liebeck and Shalev 2005] M. W. Liebeck and A. Shalev, "Fuchsian groups, finite simple groups and representation varieties", *Invent. Math.* **159**:2 (2005), 317–367. MR Zbl

[Lubotzky and Meiri 2012] A. Lubotzky and C. Meiri, "Sieve methods in group theory, I: Powers in linear groups", *J. Amer. Math. Soc.* **25**:4 (2012), 1119–1148. MR Zbl

[Maróti and Tamburini Bellani 2013] A. Maróti and M. C. Tamburini Bellani, "A solution to a problem of Wiegold", *Comm. Algebra* **41**:1 (2013), 34–49. MR Zbl

[Parzanchevski and Schul 2014] O. Parzanchevski and G. Schul, "On the Fourier expansion of word maps", *Bull. Lond. Math. Soc.* **46**:1 (2014), 91–102. MR Zbl

[Pouyanne 2002] N. Pouyanne, "On the number of permutations admitting an m-th root", *Electron. J. Combin.* **9**:1 (2002), art. id. 3. MR Zbl

[Serre 1965] J.-P. Serre, "Zeta and L functions", pp. 82–92 in *Arithmetical algebraic geometry* (West Lafayette, IN, 1963), edited by O. F. G. Schilling, Harper & Row, New York, 1965. MR Zbl

[Shalev 2013] A. Shalev, "Some results and problems in the theory of word maps", pp. 611–649 in *Erdös centennial*, edited by L. Lovász et al., Bolyai Soc. Math. Stud. **25**, János Bolyai Math. Soc., Budapest, 2013. MR Zbl

[Tao 2012] T. Tao, "The Lang–Weil bound", blog post, 2012, Available at https://tinyurl.com/taolangweil.

Communicated by Ben Green
Received 2019-10-16 Revised 2020-02-17 Accepted 2020-03-25

mjlarsen@indiana.edu

Department of Mathematics, Indiana University, Rawles Hall,
Bloomington, IN, United States

ALGEBRA AND NUMBER THEORY 14:8 (2020)
https://doi.org/10.2140/ant.2020.14.2197

On a conjecture of Yui and Zagier

Yingkun Li and Tonghai Yang

We prove the conjecture of Yui and Zagier concerning the factorization of the resultants of minimal polynomials of Weber class invariants. The novelty of our approach is to systematically express differences of certain Weber functions as products of Borcherds products.

1. Introduction

In his book, Weber [1908] proved the following well-known theorem in the theory of complex multiplication. For a fundamental discriminant $d < 0$, let $\mathcal{O}_d = \mathbb{Z}[\theta]$ be the ring of integers of an imaginary quadratic field $K_d = \mathbb{Q}(\sqrt{d})$. Then the CM value of the famous j-invariant $j(\tau)$ at $\tau = \theta$ is an algebraic integer generating the Hilbert class field of K_d. The number $j(\theta)$ is called *singular moduli* and plays an important role in the arithmetic of CM elliptic curves [Gross and Zagier 1985]. Weber also considered some special modular functions h of higher levels and observed that some of their CM values $h(\theta)$ still generate the Hilbert class field of K_d (for some choices of θ), not the larger class fields as expected for general h.

These amusing observations were later studied by various authors; see, for example, [Birch 1969; Yui and Zagier 1997; Gee 1999]. In particular, Gee gave a systematic proof of these facts using Shimura's reciprocity law. One of them concerns with the CM values of the three classical Weber functions of level 48, which are defined by the following quotients of η-functions:

$$\begin{aligned}
\mathfrak{f}(\tau) &:= \zeta_{48}^{-1}\frac{\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)} = q^{-\frac{1}{48}}\prod_{n=1}^{\infty}(1+q^{n-\frac{1}{2}}),\\
\mathfrak{f}_1(\tau) &:= \frac{\eta\left(\frac{\tau}{2}\right)}{\eta(\tau)} = q^{-\frac{1}{48}}\prod_{n=1}^{\infty}(1-q^{n-\frac{1}{2}}),\\
\mathfrak{f}_2(\tau) &:= \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)} = \sqrt{2}q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1+q^{n}).
\end{aligned} \tag{1-1}$$

Together, they form a 3-dimensional, vector-valued modular function for $\mathrm{SL}_2(\mathbb{Z})$; see (2-4). In fact, the same holds for integral powers of these modular functions; see [Milas 2007, p. 50]. Furthermore, $\mathfrak{f}_2$ is a modular function for $\Gamma_0(2)$ with character χ of order 24:

$$\mathfrak{f}_2(\gamma\tau) = \chi(\gamma)\mathfrak{f}_2(\tau), \qquad \gamma \in \Gamma_0(2). \tag{1-2}$$

Li is supported by the LOEWE research unit USAG. Yang is partially supported by NSF grant DMS-1762289.
MSC2010: primary 11G18; secondary 11F03, 11F27.
Keywords: modular form, Borcherds product, Weber invariants.

The kernel of χ, denoted by $\Gamma_\chi \subset \Gamma_0(2)$, is a congruence subgroup containing $\Gamma(48)$; see (2-8). Yui and Zagier [1997] studied the CM values of these modular functions. The starting point of their work is the following result.

Proposition 1.1 [Yui and Zagier 1997, Proposition]. *Let $d < 0$ be a discriminant satisfying*

$$d \equiv 1 \bmod 8 \quad \textit{and} \quad 3 \nmid d. \tag{1-3}$$

Denote $\varepsilon_d := (-1)^{(d-1)/8}$. For each proper ideal $\mathfrak{a} = \left[a, \frac{1}{2}(-b+\sqrt{d})\right]$ of the order $\mathcal{O}_d := \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{d})\right]$ with $a > 0$, let $\tau_\mathfrak{a} = \frac{1}{2a}(-b+\sqrt{d})$ be the associated CM point and

$$f(\mathfrak{a}) = \begin{cases} \zeta_{48}^{b(a-c-ac^2)}\mathfrak{f}(\tau_\mathfrak{a}) & \textit{if } 2|(a,c), \\ \varepsilon_d \zeta_{48}^{b(a-c-ac^2)}\mathfrak{f}_1(\tau_\mathfrak{a}) & \textit{if } 2|a, 2\nmid c, \\ \varepsilon_d \zeta_{48}^{b(a-c+a^2c)}\mathfrak{f}_2(\tau_\mathfrak{a}) & \textit{if } 2\nmid a, 2|c. \end{cases} \tag{1-4}$$

Then $f(\mathfrak{a})$ is an algebraic integer depending only on the class of $\mathfrak{a}$ in the class group $\mathrm{Cl}(d)$ of $\mathcal{O}_d$, i.e., it is a class invariant. Moreover, $H_d := K_d(f(\mathfrak{a})) = K_d(j(\tau_\mathfrak{a}))$ is the ring class field of K_d corresponding $\mathcal{O}_d$.

Remark 1.2. The class invariant in [Yui and Zagier 1997] was defined using binary quadratic forms. It is a standard procedure to go between these and ideals in quadratic fields; see, e.g., [Cox 1989].

Remark 1.3. The sign ε_d in the definition of $f(\mathfrak{a})$ ensures that the class invariants behave nicely under the action of the Galois group. In particular when $d < 0$ is fundamental,

$$\sigma_{\mathfrak{a}_2}(f(\mathfrak{a}_1)) = f(\mathfrak{a}_1\mathfrak{a}_2^{-1}) \tag{1-5}$$

for any proper $\mathcal{O}_d$-ideals $\mathfrak{a}_1, \mathfrak{a}_2$, where $\sigma_\mathfrak{a} \in \mathrm{Gal}(H_d/K_d)$ is associated to the ideal class $[\mathfrak{a}] \in \mathrm{Cl}(d)$ by Artin's map. This was conjectured in [Yui and Zagier 1997] and proved in [Gee 1999, Proposition 22].

This class invariant is much better than the singular moduli in the sense that its minimal polynomial (class polynomial) has much smaller coefficients. This gives a generator of the Hilbert class field with small height, which is crucial in the speed of elliptic curve primality test [Atkin and Morain 1993]. For example, according to [Yui and Zagier 1997], the minimal polynomial of $j\left(\frac{1}{2}(1+\sqrt{-55})\right)$ is

$$x^4 + 3^3 5^3 29 \cdot 134219 x^3 - 3^7 5^3 23 \cdot 101 \cdot 32987 x^2 + 3^9 5^7 11^2 83 \cdot 101 \cdot 110641 x - 3^{12} 5^6 11^3 29^3 41^3,$$

while the minimal polynomial of $f(\mathcal{O}_{-55})$ is simply

$$x^4 + x^3 - 2x - 1.$$

Yui and Zagier [1997] made conjectures about the prime factorizations of the discriminants and resultants of such polynomials. The goal of this paper is to prove the conjecture about the factorizations of the resultants, which also clears the path to prove the conjecture about the discriminant; see Remark 1.13.

For two co-prime, fundamental discriminants d_1 and d_2, Gross and Zagier [1985] proved a beautiful factorization formula for the resultant of the class polynomials of $j\big(\frac{1}{2}(d_1+\sqrt{d_1})\big)$ and $j\big(\frac{1}{2}(d_2+\sqrt{d_2})\big)$, which is the norm of the difference $j\big(\frac{1}{2}(d_1+\sqrt{d_1})\big) - j\big(\frac{1}{2}(d_2+\sqrt{d_2})\big)$. When $\big(\frac{d_1 d_2}{p}\big) \neq -1$, set

$$\epsilon(p) = \begin{cases} \left(\dfrac{d_1}{p}\right) & \text{if } p \nmid d_1, \\ \left(\dfrac{d_2}{p}\right) & \text{if } p \nmid d_2. \end{cases}$$

Define in general $\epsilon(n) = \prod_{p \mid n} \epsilon(p)^{\operatorname{ord}_p(n)}$, where $\operatorname{ord}_p(n)$ is the power of p dividing n. For a positive integer m, if $\epsilon(m) = -1$, define

$$\mathfrak{F}(m) = \prod_{\substack{nn'=m \\ n,n'>0}} n^{\epsilon(n')} \in \mathbb{N}, \tag{1-6}$$

which is always a prime power. If $\epsilon(m) = 1$ or is not defined, define $\mathfrak{F}(m) = 1$. The result of Gross and Zagier can be stated as follows.

Theorem 1.4 [Gross and Zagier 1985, Theorem 1.3]. *Let $d_1, d_2 < 0$ be co-prime, fundamental discriminants, and $w_j = |\mathcal{O}_{d_j}^\times|$. In the notations above, we have*

$$J(d_1,d_2)^2 := \prod_{[\mathfrak{a}_j]\in \mathrm{Cl}(d_j),\, j=1,2} |j(\tau_{\mathfrak{a}_1}) - j(\tau_{\mathfrak{a}_2})|^{8/(w_1 w_2)} = \prod_{\substack{m\in\mathbb{N},\, a\in\mathbb{Z} \\ a^2+4m=d_1d_2}} \mathfrak{F}(m). \tag{1-7}$$

Inspired by this beautiful formula, Yui and Zagier [1997] gave a conjectural formula of the resultant of the minimal polynomials of the Weber class invariants defined above and provided numerical evidence. This conjecture was originally given using two tables with totally 48 entries (see [Yui and Zagier 1997, p. 1653]), but can be simplified and formulated in the following elegant way (see, e.g., $(14_?)$ in [Yui and Zagier 1997] for $d_1 \equiv d_2 \equiv 1 \bmod 24$).

Conjecture 1.5 [Yui and Zagier 1997, $(14_?)$]. *Let d_1, d_2 be co-prime, fundamental discriminants satisfying* (1-3) *and $s \mid 24$. Define the constant*

$$\kappa_3(s) := \begin{cases} \dfrac{1}{2} & \textit{if } \left(\dfrac{d_1}{3}\right) = \left(\dfrac{d_2}{3}\right) = -1 \textit{ and } 3 \mid s, \\ 1 & \textit{otherwise,} \end{cases} \tag{1-8}$$

which only depends on d_1, d_2 and s. Then

$$f_s(d_1,d_2) := \prod_{[\mathfrak{a}_j]\in \mathrm{Cl}(d_j),\, j=1,2} |f(\mathfrak{a}_1)^{24/s} - f(\mathfrak{a}_2)^{24/s}| = \prod_{\substack{m,a\in\mathbb{N},\, r \mid s \\ a^2+16mr^2=d_1d_2 \\ m\equiv 19(d_1+d_2-1) \bmod s/r}} \mathfrak{F}(m)^{\kappa_3(s)}. \tag{1-9}$$

Remark 1.6. Because of the relation $j(\tau) = (\mathfrak{f}_2^{24}(\tau) - 16)^3/\mathfrak{f}_2^{24}(\tau)$, we know that $f_s(d_1,d_2) \mid J(d_1,d_2)$ for any co-prime, fundamental discriminants d_1, d_2 satisfying (1-3). Since the invariants are algebraic integers, it is also clear that $f_{s'}(d_1,d_2) \mid f_s(d_1,d_2)$ for any $s \mid s' \mid 24$. The conjecture above also reflects such divisibilities since $\mathfrak{F}(m/r^2) \mid \mathfrak{F}(m)$ for all $m, r \in \mathbb{N}$; see, e.g., the explicit formula of $\mathfrak{F}(m)$ on [Yui and Zagier 1997, p. 1651].

When $s = 1$, it was suggested in [Yui and Zagier 1997] that one can try to prove this conjecture by adapting the analytic approach in [Gross and Zagier 1985] with $\mathrm{SL}_2(\mathbb{Z})$ replaced by $\Gamma_0(2)$. This was later carried out in [Roskam 2003]. Yang and Yin [2019] gave another analytic proof of the conjecture for $s = 1$, where the new ingredients are Borcherds' regularized theta lift [1998] and the big CM formula in [Bruinier et al. 2012]. Although the spirits of the approaches are the same, the one in [Yang and Yin 2019] is conceptually easier to understand and opens the door to attack the conjecture for $s > 1$. In this paper, we complete the proof of the conjecture for all $s \mid 24$.

Theorem 1.7. *Conjecture 1.5 is true for every $s \mid 24$.*

For $s = 1$, the proof of Theorem 1.7 in [Yang and Yin 2019] consists of three steps:

(1) Relate $\mathfrak{f}_2(z_1)^{24} - \mathfrak{f}_2(z_2))^{24}$ to a Borcherds product on the Shimura variety associated to the rational quadratic space $(M_2(\mathbb{Q}), \det)$.[1]

(2) View a pair of CM points (τ_1, τ_2) as a big CM point on this Shimura variety in the sense of [Bruinier et al. 2012]. Apply the big CM value formula [Bruinier et al. 2012, Theorem 5.2] and express the CM value in terms of Fourier coefficients of incoherent Eisenstein series.

(3) Compute the Fourier coefficients in Step (2) and obtain the formula. This is a local calculation.

In the first step for $s = 1$, one can find a vector-valued modular function $\widetilde{F}_1$ and identify $\mathfrak{f}_2(z_1)^{24} - \mathfrak{f}_2(z_2)^{24}$ with the Borcherds product $\Psi(z_1, z_2, \widetilde{F}_1)$ associated to $\widetilde{F}_1$. Note $\mathfrak{f}_2(z)^{24} = 2^{12}(\Delta(2z)/\Delta(z))$ is a Hauptmodul of $\Gamma_0(2)$, and the Borcherds product $\Psi(z_1, z_2, \widetilde{F}_1)$ is well-known in the literature on VOA and moonshine (see, e.g., [Borcherds 1992; Scheithauer 2008]). In the second step, one suitably identifies the Galois orbit of CM points with the toric orbit of big CM points, and apply Theorem 5.2 in [Bruinier et al. 2012]. This reduces the proof to the third step, where the local calculations have been completed in many special cases (see [Yang 2005; Howard and Yang 2012, Section 4.6; Kudla and Yang 2010]) and the most general result can be found in Appendix A of [Yang et al. 2019].

To execute this strategy for $s > 1$, we first need to relate $\mathfrak{f}_2(z_1)^{24/s} - \mathfrak{f}_2(z_2)^{24/s}$ to Borcherds product. Since the function $\mathfrak{f}_2(z)^{24/s}$ is invariant with respect to $\Gamma_{\chi,s} := \langle \Gamma_\chi, T^s \rangle \supset \Gamma(2s)$, one would hope to find the analog of $\widetilde{F}_1$ in $M^!(\omega_s)$, with ω_s the Weil representation of $\mathrm{SL}_2(\mathbb{Z})$ on the finite quadratic module associated to the lattice L_s (see (3-1)), which is the same as the lattice used in [Yang and Yin 2019] to produce $\Psi(z_1, z_2, \widetilde{F}_1)$, but with the quadratic form scaled by s. We have computationally decomposed the representation ω_s and analyzed the space of vector-valued modular functions. To our surprise, there is *no* modular function whose Borcherds product equals to $(\mathfrak{f}_2(z_1)^{24/s} - \mathfrak{f}_2(z_2)^{24/s})^s$! Our new idea then is to express $(\mathfrak{f}_2(z_1)^{24/s} - \mathfrak{f}_2(z_2)^{24/s})^s$ as *a product of Borcherds products*, which works out beautifully.

[1] The Shimura variety is just the product of two modular curves in this case.

Theorem 1.8 (Theorems 4.4 and 4.5). *For every* $\mathrm{d} \mid 24$, *there is a vector-valued modular function* $\widetilde{F}_{\mathrm{d}} \in M^!(\omega_{\mathrm{d}})$ *with associated Borcherds product* $\Psi_{\mathrm{d}}(z_1, z_2) := \Psi(z_1, z_2, \widetilde{F}_{\mathrm{d}})$ *such that*

$$(\mathfrak{f}_2(z_1)^{24/s} - (\varepsilon\mathfrak{f}_2(z_2))^{24/s})^s = \prod_{\mathrm{d}|s} \Psi_{\mathrm{d}}(z_1, z_2)^{\varepsilon^{\frac{24}{\mathrm{d}}}}, \tag{1-10}$$

for every $s \mid 24$ *and any* $\varepsilon = \pm 1$.

Remark 1.9. The index $r \mid s$ in the product on the right-hand side of (1-9) is *not* directly related to the index $\mathrm{d} \mid s$ in the product above! Instead, it comes out of local calculation in Section 6.

Remark 1.10. Each Borcherds product $\Psi_{\mathrm{d}}(z_1, z_2)$ comes from a different quadratic space depending on d, and is a meromorphic function on the Shimura variety X^2_{d}, which admits a natural covering map from X^2_s when $\mathrm{d} \mid s$ (see Section 4). One can then pull back Ψ_{d} to a function on X^2_s. Notice that this decomposes the divisor of the left-hand side, which is a Heegner divisor on X^2_s, into a sum of pullbacks of Heegner divisors on X^2_{d} with $\mathrm{d} \mid s$. When $s > 1$, the product $\prod_{\mathrm{d}|s} \Psi_{\mathrm{d}}(z_1, z_2)$ is itself *not* a single Borcherds product on X^2_s.

Remark 1.11. Theorem 1.8 naturally leads one to speculate a generalization of the converse theorem in [Bruinier 2014], namely every principal Heegner divisor on an orthogonal Shimura variety associated to a lattice of signature $(n, 2)$ with Witt rank greater than or equal to 2 should be the divisor of a product of Borcherds products.

To arrive at this idea, we took $s = 2$ and started from the simple observation that

$$(\mathfrak{f}_2(z_1)^{12} - \mathfrak{f}_2(z_2)^{12})^2 = (\mathfrak{f}_2(z_1)^{24} - \mathfrak{f}_2(z_2)^{24}) \cdot \frac{\mathfrak{f}_2(z_1)^{12} - \mathfrak{f}_2(z_2)^{12}}{\mathfrak{f}_2(z_1)^{12} + \mathfrak{f}_2(z_2)^{12}}. \tag{1-11}$$

We already know that the first factor on the right-hand side is a Borcherds product. If we can realize the second factor as a Borcherds product, then the left-hand side would be a product of Borcherds products (with different quadratic forms). To do that, we can read off the divisor of the second factor, and deduce the principal part of the input to Borcherds' lift. In this case, it is of the form $q^{-1/2}\mathfrak{u}_2$ for a suitable vector $\mathfrak{u}_2$ in a 64 dimensional vector space $\mathbb{C}[\mathcal{A}_2]$, where $\mathrm{SL}_2(\mathbb{Z})$ acts via the Weil representation ω_2 (see Section 3A for details). Then we find the irreducible representation in ω_2 containing $\mathfrak{u}_2$, which is 3-dimensional, and hope to find the suitable vector-valued modular function $\widetilde{F}_2$ with this principal part. Miraculously, this function exists and its three components are the $(-24/2)$-th power of the three Weber functions $\frac{\mathfrak{f}}{\sqrt{2}}, \frac{\mathfrak{f}_1}{\sqrt{2}}, \frac{\mathfrak{f}_2}{\sqrt{2}}$.

The observation (1-11) generalizes to any $s \mid 24$ by substituting $X = (\varepsilon\mathfrak{f}_2(z_2)/\mathfrak{f}_2(z_1))^{24/s}$ into the following simple identity in $\mathbb{Q}(X)$

$$(1 - X)^s = \prod_{\mathrm{d}|s} \prod_{b|\mathrm{d}} (1 - X^{s/b})^{b \cdot \mu(\mathrm{d}/b)}, \tag{1-12}$$

where μ is the Möbius function, and multiplying by $\mathfrak{f}_2(z_1)^{24}$ on both sides. Note that the identity in (1-12) holds for any $s \in \mathbb{N}$ (see Lemma 4.3). Then the miracle continues to happen, and we find a family of vectors $\{\mathfrak{u}_{\mathrm{d}} : \mathrm{d} \mid 24\}$ (see (3-12)) and vector-valued modular functions $\widetilde{F}_{\mathrm{d}} = q^{-1/\mathrm{d}}\mathfrak{u}_{\mathrm{d}} + O(q^{1/(2\mathrm{d})})$ producing the Borcherds lifts Ψ_{d} (see (2-4) and Remark 3.7). For $\mathrm{d} > 1$, the vector $\mathfrak{u}_{\mathrm{d}}$ satisfies nice invariance properties (see Proposition 3.5) and is of independent interest, whereas the components of $\widetilde{F}_{\mathrm{d}}$ are simply the $(-24/\mathrm{d})$-th power of the three Weber functions $\frac{\mathfrak{f}}{\sqrt{2}}, \frac{\mathfrak{f}_1}{\sqrt{2}}, \frac{\mathfrak{f}_2}{\sqrt{2}}$!

Remark 1.12. The $\varepsilon = \pm 1$ in Theorem 1.8 is there for a good reason. To prove the Yui–Zagier conjecture, we need to choose $\varepsilon = \varepsilon_{d_1}\varepsilon_{d_2} = (-1)^{(d_1+d_2-2)/8}$ (see Proposition 5.5 and its proof). It is also amusing to see that the same ε appears when we calculate the Fourier coefficients of derivatives of certain Eisenstein series (see Theorem 6.2).

To complete the proof, we can now apply the second step to each Borcherds product, obtain a big CM value formula, and add them together. Note that the identification of the Galois orbit of $(\tau_{\mathfrak{a}_1}, \tau_{\mathfrak{a}_2})$ used in defining $f_s(d_1, d_2)$ with the big CM cycle in [Bruinier et al. 2012] depends on the input $\widetilde{F}_{\mathrm{d}}$ in Step (1). Therefore, it is not a priori clear that this will work out. We prove this in Proposition 5.5, which crucially depends on Lemma 5.2. This unexpected result was first observed with some computer calculations, and has been reduced to a computation with finite groups in $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z})$. Finally, we apply the local calculations in [Yang et al. 2019] to finish off Step (3).

Remark 1.13. With Theorem 1.8, one can now replace the big CM value formula in [Bruinier et al. 2012] with the small CM value formula in [Schofer 2009] to prove the conjectural factorization of the discriminant of the minimal polynomials of the Weber invariants in [Yui and Zagier 1997]. We plan to carry these out as a sequel to this work [Li and Yang $\geq$ 2021].

This paper is organized as follows. After setting up notation and defining basic terms in Section 2, we study in Section 3 the action of certain subgroup $H'_{\mathrm{d}} \subset \mathrm{SO}(L_{\mathrm{d}})/\Gamma_{L_{\mathrm{d}}}$ on the finite quadratic module $\mathcal{A}_{\mathrm{d}} := L_{\mathrm{d}}^{\vee}/L_{\mathrm{d}}$ and use it to decompose the Weil representation ω_{d} of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{C}[\mathcal{A}_{\mathrm{d}}]^{H'_{\mathrm{d}}}$. The goal and main result is to construct certain element $\mathfrak{u}_{\mathrm{d}} \in \mathbb{C}[\mathcal{A}_{\mathrm{d}}]^{H'_{\mathrm{d}}}$ satisfying (3-13). This vector generates a 3-dimensional, H'_{d}-invariant subrepresentation of ω_{d}, and will be crucial in finding the input $\widetilde{F}_{\mathrm{d}}$ that produces the Borcherds product Ψ_{d}. In Section 4, we view product of two modular curves as a Shimura variety of orthogonal type $(2, 2)$ associated to L_{d}, construct the Borcherds product Ψ_{d}, and prove Theorem 1.8. In Section 5, we view the pair $(\tau_{\mathfrak{a}_1}, \tau_{\mathfrak{a}_2})$ as a big CM point on the product of two modular curves and study its Galois orbit. The upshot is Proposition 5.5, which relates the left-hand side of Conjecture 1.5 to the big CM value of Borcherds products. By the second step of strategy, Conjecture 1.5 is reduced to local calculation of certain Eisenstein series and its derivative, which we carry out in Section 6B using the results in the appendix of [Yang et al. 2019]. Finally in the Appendix, we explicitly write down the cosets in the finite quadratic module used in constructing the Borcherds products, and include a numerical example for $d_1 = -31$ and $d_2 = -127$.

2. Preliminaries

2A. ***Weil representation.*** Let (L, Q) be an even integral lattice of signature $(2, 2)$ and $V := L \otimes \mathbb{Q}$ the rational quadratic space. Denote L' the dual lattice and $\mathcal{A}_L := L'/L$ the finite quadratic module. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on $U_L := \mathbb{C}[\mathcal{A}_L]$ via the Weil representation ω_L given by

$$\omega_L(T)\mathfrak{e}_h = \mathbf{e}(-Q(h))\mathfrak{e}_h, \quad \omega_L(S)\mathfrak{e}_h = \frac{1}{\sqrt{|\mathcal{A}_L|}} \sum_{\mu \in \mathcal{A}_L} \mathbf{e}((\mu, h))\mathfrak{e}_\mu, \tag{2-1}$$

where $\{\mathfrak{e}_\mu : \mu \in \mathcal{A}_L\}$ is the standard basis of U_L and

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{2-2}$$

Note that this differs from the convention of Borcherds by complex conjugation.

Let $S(L) = \bigoplus_{\mu \in L'/L} \phi_\mu \subset S(V \otimes \mathbb{A}_f)$ with $\widehat{L} = L \otimes \widehat{\mathbb{Z}}$ and

$$\phi_\mu = \mathrm{Char}(\mu + \widehat{L}).$$

Under the isomorphism $U_L \to S(L)$ that maps $\mathfrak{e}_\mu$ to ϕ_μ, the representation ω_L becomes the restriction of the Weil representation $\omega = \omega_{V,\psi}$ (with the usual idelic character ψ of $\mathbb{Q}$) from $\mathrm{SL}_2(\mathbb{A})$ to (the diagonally embedded) $\mathrm{SL}_2(\mathbb{Z})$. We will sometimes switch the representation spaces between U_L and $S(L)$. Note that $S(L_1 \oplus L_2) = S(L_1) \otimes S(L_2)$ for any two sublattices $L_1, L_2 \subset L$ orthogonal to each other.

2B. ***Weber functions.*** For any finite-dimensional, $\mathbb{C}$-representation $\rho : \Gamma \to V$ of a finite index subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, denote $M^!(\rho, \Gamma)$ the space of weakly holomorphic, vector-valued modular function with respect to ρ. We drop ρ (resp. Γ) from the notation if ρ is trivial (resp. $\Gamma = \mathrm{SL}_2(\mathbb{Z})$). For example, the three Weber functions defined by (1-1) form a vector-valued modular function

$$\begin{pmatrix} \mathfrak{f}_2 \\ \mathfrak{f}_1 \\ \mathfrak{f} \end{pmatrix} \in M^!(\overline{\varrho_{24}}).$$

Here, for a positive integer d and $j \in (\mathbb{Z}/2\mathrm{d}\mathbb{Z})^\times$, the representation $\varrho_{\mathrm{d},j} : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{GL}_3(\mathbb{C})$ is defined by

$$\varrho_{\mathrm{d},j}(T) := \begin{pmatrix} \zeta_{\mathrm{d}}^{-j} & 0 & 0 \\ 0 & 0 & \zeta_{2\mathrm{d}}^{j} \\ 0 & \zeta_{2\mathrm{d}}^{j} & 0 \end{pmatrix}, \quad \varrho_{\mathrm{d},j}(S) := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{2-3}$$

We simply write ϱ_{d} for $\varrho_{\mathrm{d},1}$. Finally, $\bar{\rho}(g) := \overline{\rho(g)}$. Later, the modular function

$$F_{\mathrm{d}}(\tau) := \sqrt{2}^{24/\mathrm{d}} \begin{pmatrix} \mathfrak{f}_2^{-24/\mathrm{d}}(\tau) \\ \mathfrak{f}_1^{-24/\mathrm{d}}(\tau) \\ \mathfrak{f}^{-24/\mathrm{d}}(\tau) \end{pmatrix} \in M^!(\varrho_{\mathrm{d}}), \ \mathrm{d} \mid 24 \tag{2-4}$$

will play an important role for us as the representation ϱ_{d} defined above is a subrepresentation of certain Weil representation that we will consider.

Remark 2.1. For convenience later, we will denote

$$\sqrt{2}^{24/\mathrm{d}} \mathfrak{f}_2^{-24/\mathrm{d}}(\tau) = \left(\frac{\eta(\tau)}{\eta(2\tau)} \right)^{24/\mathrm{d}} = \sum_{l \geq -1,\, l \equiv -1 \bmod \mathrm{d}} c_{\mathrm{d}}(l) q^{l/\mathrm{d}} \in q^{-1/\mathrm{d}}\mathbb{Z}[\![q]\!]. \tag{2-5}$$

Clearly $c_{\mathrm{d}}(-1)=1$ for every $\mathrm{d}\mid 24$. We will also denote $c_{-1}(l)$ the l-th Fourier coefficient of

$$2^{12}\mathfrak{f}_1^{-24}(2\tau)=\mathfrak{f}_2^{24}(\tau)=2^{12}\frac{\Delta(2\tau)}{\Delta(\tau)}.$$

Let $\chi:\Gamma_0(2)\to\mathbb{C}^\times$ be the character defined in (1-2). On the generators T, S^2 and TB of $\Gamma_0(2)$, where

$$B:=ST^2S^{-1}=\begin{pmatrix}1&0\\-2&1\end{pmatrix},\tag{2-6}$$

the character χ is explicitly given by

$$\chi(T)=\zeta_{24},\quad \chi(S^2)=1,\quad\text{and}\quad \chi(TB)=1.\tag{2-7}$$

The kernel of χ is a normal subgroup of $\Gamma_0(2)$ defined by

$$\Gamma_\chi:=\langle\Gamma_0(2)^{\mathrm{der}},T^{24},S^2,TB\rangle\subset\Gamma_0(2),\tag{2-8}$$

where $\Gamma_0(2)^{\mathrm{der}}$ is the derived subgroup of $\Gamma_0(2)$. We remark that Γ_χ is the group $\Phi_0^0(24)$ in [Yang and Yin 2016]. Furthermore, it contains the congruence subgroup $\Gamma_0(48)\cap\Gamma(24)$ and $\Gamma_0(2)/\Gamma_\chi\cong\mathbb{Z}/24$. More generally, for any divisor $\mathrm{d}\mid 24$, denote the kernel of $\chi^{24/\mathrm{d}}$ by

$$\Gamma_{\chi,\mathrm{d}}:=\langle\Gamma_\chi,T^{\mathrm{d}}\rangle\subset\Gamma_0(2).\tag{2-9}$$

It has index d in $\Gamma_0(2)$ and contains $\Gamma_\chi=\Gamma_{\chi,24}$, as well as the congruence subgroup

$$\Gamma_{\mathrm{d}}:=\Gamma_1(2\mathrm{d})\cap\Gamma(\mathrm{d}).\tag{2-10}$$

In particular, $\Gamma_0(2)=\Gamma_{\chi,1}$. More generally for $\mathrm{d}\mid\mathrm{d}'\mid 24$, we have $\Gamma_{\mathrm{d}}\supset\Gamma_{\mathrm{d}'}$. For future convenience, we also write d_p for the p-primary part of d. Then clearly $\mathrm{d}=\mathrm{d}_2\mathrm{d}_3$.

3. Decomposition of Weil representations

3A. ***Lattice.*** For a divisor $\mathrm{d}\mid 24$, consider the quadratic lattice

$$L_{\mathrm{d}}=\left\{\lambda=\begin{pmatrix}\lambda_{00}&\lambda_{01}\\2\lambda_{10}&\lambda_{11}\end{pmatrix}:\lambda_{ij}\in\mathbb{Z}\right\},\qquad Q_{\mathrm{d}}(\lambda):=\mathrm{d}\det(\lambda).\tag{3-1}$$

The dual lattice is given by

$$L'_{\mathrm{d}}=\left\{\lambda=\frac{1}{\mathrm{d}}\begin{pmatrix}\lambda_{00}&\lambda_{01}/2\\\lambda_{10}&\lambda_{11}\end{pmatrix}:\lambda_{ij}\in\mathbb{Z}\right\}.\tag{3-2}$$

The finite quadratic module $L'_{\mathrm{d}}/L_{\mathrm{d}}$ is then isomorphic to

$$\mathcal{A}_{\mathrm{d}}:=\{h=[h_0,h_1,h_2,h_3]:h_0,h_3\in\mathbb{Z}/\mathrm{d}\mathbb{Z},\,h_1,h_2\in\mathbb{Z}/(2\mathrm{d}\mathbb{Z})\},\tag{3-3}$$

where the isomorphism is fixed throughout and given by

$$L'_{\mathrm{d}}/L_{\mathrm{d}}\cong\mathcal{A}_{\mathrm{d}},\qquad \frac{1}{\mathrm{d}}\begin{pmatrix}\lambda_{00}&\lambda_{01}/2\\\lambda_{10}&\lambda_{11}\end{pmatrix}+L_{\mathrm{d}}\mapsto[\lambda_{00},\lambda_{01},\lambda_{10},\lambda_{11}].\tag{3-4}$$

Via this isomorphism, the quadratic form Q_{d} on $\mathcal{A}_{\mathrm{d}}$ becomes

$$Q_{\mathrm{d}}(h) := \frac{2h_0h_3 - h_1h_2}{2\mathrm{d}} \in \frac{1}{2\mathrm{d}}\mathbb{Z}/\mathbb{Z} \tag{3-5}$$

for $h = [h_0, h_1, h_2, h_3] \in \mathcal{A}_{\mathrm{d}}$. We denote $U_{\mathrm{d}} := \mathbb{C}[\mathcal{A}_{\mathrm{d}}]$, which is acted on by $\mathrm{SL}_2(\mathbb{Z})$ via the Weil representation $\omega_{\mathrm{d}} := \omega_{L_{\mathrm{d}}}$.

Now, we can map L_{d} into $L'_{\mathrm{d}}/L_{\mathrm{d}} \cong \mathcal{A}_{\mathrm{d}}$ via

$$\kappa_{\mathrm{d}} : L_{\mathrm{d}} \to L'_{\mathrm{d}}/L_{\mathrm{d}}, \quad \lambda \mapsto \frac{1}{\mathrm{d}}\lambda + L_{\mathrm{d}}, \tag{3-6}$$

which is compatible with the left and right action of $\Gamma_0(2)$, i.e.,

$$g_1 \cdot \kappa_{\mathrm{d}}(\lambda \cdot g_2) = \kappa_{\mathrm{d}}(g_1 \cdot \lambda \cdot g_2) = \kappa_{\mathrm{d}}(g_1 \cdot \lambda) \cdot g_2 \tag{3-7}$$

for all $g_1, g_2 \in \Gamma_0(2)$ and $\lambda \in L_{\mathrm{d}}$. By viewing $\Gamma_{\chi,1} = \Gamma_0(2)$ as a subset of L_{d}, we can send it to a subset in $\mathcal{A}_{\mathrm{d}}$. If we denote

$$\mathcal{A}^0_{\mathrm{d}} := \{[h_0, h_1, h_2, h_3] \in \mathcal{A}_{\mathrm{d}} : h_2 = 0 \in \mathbb{Z}/(2\mathrm{d}\mathbb{Z})\}, \tag{3-8}$$

it will be helpful to know the parts of $\Gamma_0(2)$ that land in $\mathcal{A}^0_{\mathrm{d}}$ under κ_{d} when we simplify the expression of Borcherds products. For this we need the following lemma, whose proof will follow from combining the corresponding local results in Lemmas 3.8 and 3.12.

Lemma 3.1. *For any $j \in \mathbb{Z}/\mathrm{d}\mathbb{Z}$, we have* (*viewing* $\Gamma_0(2) \subset L_{\mathrm{d}}$)

$$\kappa_{\mathrm{d}}(T^j\Gamma_{\chi,\mathrm{d}}) \cap \mathcal{A}^0_{\mathrm{d}} = \{\mathrm{d}_3^{-1}[r, r(2j + (r^2 - 1)), 0, r] : r \in (\mathbb{Z}/\mathrm{d}\mathbb{Z})^\times\}.$$

Remark 3.2. Note that $r^3 - r \mod 2\mathrm{d}$ is well-defined for $r \in (\mathbb{Z}/\mathrm{d}\mathbb{Z})^\times$ when $\mathrm{d} \mid 24$. Furthermore

$$r^3 - r \equiv \begin{cases} \mathrm{d} \mod 2\mathrm{d} & \text{if } 8 \mid \mathrm{d} \text{ and } r \equiv \pm 3 \mod 8, \\ 0 \mod 2\mathrm{d} & \text{otherwise.} \end{cases}$$

Let $\mathrm{GL}_2(\mathbb{Q}) \times \mathrm{GL}_2(\mathbb{Q})$ acts on $V_{\mathrm{d}} = L_{\mathrm{d}} \otimes \mathbb{Q} = M_2(\mathbb{Q})$ via

$$(g_1, g_2) \cdot X = g_1 X g_2^{-1}.$$

This action gives an identification of $\mathrm{GSpin}(V)$ with $H = \{(g_1, g_2) : \det g_1 = \det g_2\}$, and a commutative diagram of exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & \{\pm 1\} \arrow[r] \arrow[d] & \mathrm{SL}_2 \times \mathrm{SL}_2 \arrow[r] \arrow[d] & \mathrm{SO}(V) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbb{G}_m \arrow[r] & H \arrow[r] & \mathrm{SO}(V) \arrow[r] & 1.
\end{tikzcd}$$

For the particular lattice L_{d}, we have

$$\mathrm{SO}(L_{\mathrm{d}}) = \overline{\Gamma_0(2) \times \Gamma_0(2)} = \Gamma_0(2) \times \Gamma_0(2)/\{\pm(I_2, I_2)\}, \tag{3-9}$$

As $\{\pm(I_2, I_2)\}$ does not matter in this paper, we will simply identify $\mathrm{SO}(L_\mathrm{d})$ with $\Gamma_0(2)\times\Gamma_0(2)$ and drop the overline. Under this identification, we have $\Gamma_{L_\mathrm{d}} = \Gamma_\mathrm{d}\times\Gamma_\mathrm{d}$, where Γ_d is defined in (2-10). In particular, we are interested in the action of the subgroup of $\mathrm{SO}(L_\mathrm{d})$ generated by the images of (T, T) and $\Gamma_{\chi,\mathrm{d}}\times\Gamma_{\chi,\mathrm{d}}$. We let H'_d be its image in $H_\mathrm{d} := N_\mathrm{d}\times N_\mathrm{d}$, where $N_\mathrm{d} := \Gamma_0(2)/\Gamma_\mathrm{d}$. Let $N'_\mathrm{d} := \Gamma_{\chi,\mathrm{d}}/\Gamma_\mathrm{d}$. Then

$$N'_\mathrm{d}\times N'_\mathrm{d}\subset H'_\mathrm{d}\subset H_\mathrm{d} = N_\mathrm{d}\times N_\mathrm{d}. \tag{3-10}$$

Since $\Gamma_0(2)/\Gamma_{\chi,\mathrm{d}}\cong\mathbb{Z}/\mathrm{d}\mathbb{Z}$, the quotient group $H_\mathrm{d}/H'_\mathrm{d}$ is isomorphic to $\mathbb{Z}/\mathrm{d}\mathbb{Z}$. For prime p, let $N_{\mathrm{d},p}$ denote the quotient of the subgroups generated respectively by $\Gamma_0(2)$ and Γ_d in $\mathrm{SL}_2(\mathbb{Z}_p)$. Similarly, we can also define K_p for $K\in\{N_\mathrm{d}, N'_\mathrm{d}, H_\mathrm{d}, H'_\mathrm{d}\}$. Since d is only divisible by 2 and 3 in our case, the Chinese remainder theorem implies

$$H_\mathrm{d}\cong H_{\mathrm{d},2}\times H_{\mathrm{d},3},\quad H'_\mathrm{d}\cong H'_{\mathrm{d},2}\times H'_{\mathrm{d},3},\quad N'_{\mathrm{d},p}\times N'_{\mathrm{d},p}\subset H'_{\mathrm{d},p}\subset H_{\mathrm{d},p} = N_{\mathrm{d},p}\times N_{\mathrm{d},p}.$$

For the same reason, we have the decomposition

$$\mathcal{A}_\mathrm{d}\cong\mathcal{A}_{\mathrm{d},2}\times\mathcal{A}_{\mathrm{d},3},\quad \mathcal{A}_{\mathrm{d},p} := \mathcal{A}_\mathrm{d}\otimes_\mathbb{Z}\mathbb{Z}_p. \tag{3-11}$$

Using this isomorphism, we can write $\omega_\mathrm{d}\cong\omega_{\mathrm{d},2}\otimes\omega_{\mathrm{d},3}$ and $U_\mathrm{d}\cong U_{\mathrm{d},2}\otimes U_{\mathrm{d},3}$, where $\omega_{\mathrm{d},p}$ is the Weil representation of $\mathrm{SL}_2(\mathbb{Z}_p)$ acting on $U_{\mathrm{d},p}$ associated to $\mathcal{A}_{\mathrm{d},p}$.

Now, we introduce the vector $\mathfrak{u}_\mathrm{d}\in U_\mathrm{d}$.

$$\begin{aligned}\mathfrak{u}_\mathrm{d} &:= \mathfrak{u}_{\mathrm{d},2}\otimes\mathfrak{u}_{\mathrm{d},3} = \sum_{j\in\mathbb{Z}/\mathrm{d}\mathbb{Z}} a_\mathrm{d}(j)\Bigg(\sum_{h\in\kappa_\mathrm{d}(T^j\Gamma_{\chi,\mathrm{d}})}\mathfrak{e}_h\Bigg),\\ a_\mathrm{d}(j) &:= \Bigg(\sum_{s\in(\mathbb{Z}/\mathrm{d}\mathbb{Z})^\times}\zeta_\mathrm{d}^{sj}\Bigg) = \mu\bigg(\frac{\mathrm{d}}{(\mathrm{d},j)}\bigg)\frac{\varphi(\mathrm{d})}{\varphi(\mathrm{d}/(\mathrm{d},j))}\in\mathbb{Z},\end{aligned} \tag{3-12}$$

where $\mathfrak{u}_{\mathrm{d},p} = \mathfrak{u}_{\mathrm{d},p}(1,\dots,1)\in U'_{\mathrm{d},p}\subset U_{\mathrm{d},p}$ is the vector defined in (3-23) and (3-33), μ and φ are the Möbius and Euler φ-function respectively. Note that $a_\mathrm{d}(j)$ is defined for any $\mathrm{d}\in\mathbb{N}$ and $j\in\mathbb{Z}/\mathrm{d}\mathbb{Z}$.

Remark 3.3. A natural question is where the element $\mathfrak{u}_{\mathrm{d},p}$ comes from and what it is good for? In the next two subsections, we will give some ideas where they come from. For now, we are satisfied to give its nice properties as below. See Proposition 3.6 below.

Lemma 3.4. *For any* $\mathrm{d}, r\mid 24$, *the vector* $\mathfrak{u}_\mathrm{d}\in\mathbb{Z}[\mathcal{A}_\mathrm{d}]$ *is invariant with respect to* $\Gamma_{\chi,r}\times\Gamma_{\chi,r}$ *if and only if* $\mathrm{d}\mid r$.

Proof. If $\mathrm{d}\mid r$, then $\Gamma_{\chi,r}\subset\Gamma_{\chi,\mathrm{d}}$ and we just need to prove the case when $r = \mathrm{d}$. Let $(g_1, g_2)\in\mathrm{SO}(L_\mathrm{d})$ with $g_j\in\Gamma_{\chi,\mathrm{d}}$. Then

$$(g_1, g_2)\cdot\mathfrak{u}_\mathrm{d} = \sum_{j\in\mathbb{Z}/\mathrm{d}\mathbb{Z}} a_\mathrm{d}(j)\Bigg(\sum_{h\in\kappa_\mathrm{d}(g_1T^j\Gamma_{\chi,\mathrm{d}}g_2^{-1})}\mathfrak{e}_h\Bigg) = \mathfrak{u}_\mathrm{d},$$

where we have used the fact that $\Gamma_{\chi,\mathrm{d}}$ is normal in $\Gamma_0(2)$ with coset representatives $\{T^j : j \in \mathbb{Z}/\mathrm{d}\mathbb{Z}\}$. Similarly, $(T, T)\cdot\mathfrak{u}_\mathrm{d} = \mathfrak{u}_\mathrm{d}$. Thus $\mathfrak{u}_\mathrm{d}$ is $\Gamma_{\chi,\mathrm{d}} \times \Gamma_{\chi,\mathrm{d}}$-invariant. If $\mathrm{d} \nmid r$, then $(T^r, 1) \in (\Gamma_{\chi,r} \times \Gamma_{\chi,r})\backslash(\Gamma_{\chi,\mathrm{d}} \times \Gamma_{\chi,\mathrm{d}})$. It is easy to see that

$$(T^r, 1)\cdot\mathfrak{u}_\mathrm{d} = \sum_{j\in\mathbb{Z}/\mathrm{d}\mathbb{Z}} a_\mathrm{d}(j-r)\Bigg(\sum_{h\in\kappa_\mathrm{d}(T^jN'_\mathrm{d})} \mathfrak{e}_h\Bigg) \neq \mathfrak{u}_d$$

since

$$\frac{a_\mathrm{d}(-r)}{\varphi(\mathrm{d})} = \frac{\mu(\mathrm{d}/(\mathrm{d},r))}{\varphi(\mathrm{d}/(\mathrm{d},r))} \neq 1 = \frac{a_\mathrm{d}(0)}{\varphi(\mathrm{d})}$$

when $\mathrm{d} \nmid r$. □

Proposition 3.5. *For any* $\mathrm{d} \mid 24$, *we have*

$$\omega_\mathrm{d}(g)\mathfrak{u}_\mathrm{d} = \chi(g)^{-24/\mathrm{d}}\mathfrak{u}_\mathrm{d} \tag{3-13}$$

for all $g \in \Gamma_0(2)$.

Proof. This follows directly from the local results 3.10 and 3.16 as

$$\omega_\mathrm{d}(g)\mathfrak{u}_\mathrm{d} = (\omega_{\mathrm{d},2}(g)\mathfrak{u}_{\mathrm{d},2}) \otimes (\omega_{\mathrm{d},3}(g)\mathfrak{u}_{\mathrm{d},3}) = \chi(g)^{-24(\mathrm{d}_2/\mathrm{d}_3+\mathrm{d}_3/\mathrm{d}_2)}\mathfrak{u}_{\mathrm{d},2} \otimes \mathfrak{u}_{\mathrm{d},3} = \chi(g)^{-24/\mathrm{d}}\mathfrak{u}_\mathrm{d}.$$

for all $g \in \Gamma_0(2)$. Here we have used $\frac{1}{\mathrm{d}} - \left(\frac{\mathrm{d}_2}{\mathrm{d}_3} + \frac{\mathrm{d}_3}{\mathrm{d}_2}\right) \in \mathbb{Z}$ when $\mathrm{d} \mid 24$. □

Now, define two further vectors

$$\mathfrak{v}_\mathrm{d} := \omega_\mathrm{d}(S)\mathfrak{u}_\mathrm{d}, \quad \mathfrak{w}_\mathrm{d} := \zeta_{2\mathrm{d}}^{-1}\omega_\mathrm{d}(T)\mathfrak{v}_\mathrm{d}. \tag{3-14}$$

Note that $\mathfrak{u}_\mathrm{d}$, $\mathfrak{v}_\mathrm{d}$ and $\mathfrak{w}_\mathrm{d}$ are linearly independent for all $\mathrm{d} \mid 24$. The key to the input of Borcherds lifting is then constructed using these vectors in the following result.

Proposition 3.6. *The representations* ϱ_d *defined in* (2-3) *is a subrepresentation of the Weil representation* ω_d *via the map*

$$\iota_\mathrm{d} : \mathbb{C}^3 \to U_\mathrm{d}^{H'_\mathrm{d}} \subset U_\mathrm{d}, \quad \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto a\mathfrak{u}_\mathrm{d} + b\mathfrak{v}_\mathrm{d} + c\mathfrak{w}_\mathrm{d}. \tag{3-15}$$

Let F_d *be the modular function defined in* (2-4). *The function* $\iota_\mathrm{d} \circ F_\mathrm{d}$ *is then in* $M^!(\omega_\mathrm{d})$ *and invariant with respect to the orthogonal group* $H'_\mathrm{d} \subset \mathrm{SO}(L_\mathrm{d})/\Gamma_{L_\mathrm{d}}$. *Furthermore, it has the principal part*

$$\iota_d \circ F_\mathrm{d}(\tau) = q^{-1/\mathrm{d}}\mathfrak{u}_\mathrm{d} + \begin{cases} O(q^{1/2}) & \textit{if } \mathrm{d} > 1, \\ O(1) & \textit{if } \mathrm{d} = 1, \end{cases} \tag{3-16}$$

Remark 3.7. When $\mathrm{d} = 1$, the function $\iota_\mathrm{d} \circ F_\mathrm{d}$ differs from the input in [Yang and Yin 2019] by a constant vector. To simplify the notation, we will write

$$\widetilde{F}_\mathrm{d} := \iota_\mathrm{d} \circ F_\mathrm{d} + \begin{cases} 24(\mathfrak{e}_{(0,0)} + \mathfrak{e}_{(1/2,0)}) & \text{if } \mathrm{d} = 1, \\ 0 & \text{if } \mathrm{d} > 1, \end{cases} \tag{3-17}$$

which is an element in $M^!(\omega_\mathrm{d})$ invariant with respect to H'_d.

Proof. It suffices to check on the generators T, S of $\mathrm{SL}_2(\mathbb{Z})$. From the definition and Proposition 3.5, it is clear that

$$\begin{gathered}\omega_{\mathrm{d}}(T)\mathfrak{u}_{\mathrm{d}}=\zeta_{\mathrm{d}}^{-1}\mathfrak{u}_{\mathrm{d}},\qquad \omega_{\mathrm{d}}(T)\mathfrak{v}_{\mathrm{d}}=\zeta_{2\mathrm{d}}\mathfrak{w}_{\mathrm{d}},\\ \omega_{\mathrm{d}}(T)\mathfrak{w}_{\mathrm{d}}=\zeta_{2\mathrm{d}}^{-1}\omega_{\mathrm{d}}(T^2S)\mathfrak{u}_{\mathrm{d}}=\zeta_{2\mathrm{d}}^{-1}\omega_{\mathrm{d}}(SB)\mathfrak{u}_{\mathrm{d}}=\zeta_{2\mathrm{d}}\omega_{\mathrm{d}}(S)\mathfrak{u}_{\mathrm{d}}=\zeta_{2\mathrm{d}}\mathfrak{v}_{\mathrm{d}},\\ \omega_{\mathrm{d}}(S)\mathfrak{u}_{\mathrm{d}}=\mathfrak{v}_{\mathrm{d}},\qquad \omega_{\mathrm{d}}(S)\mathfrak{v}_{\mathrm{d}}=\mathfrak{u}_{\mathrm{d}},\\ \omega_{\mathrm{d}}(S)\mathfrak{w}_{\mathrm{d}}=\zeta_{2\mathrm{d}}^{-1}\omega_{\mathrm{d}}(STS)\mathfrak{u}_{\mathrm{d}}=\zeta_{2\mathrm{d}}^{-1}\omega_{\mathrm{d}}((ST)^2BS^2)\mathfrak{u}_{\mathrm{d}}=\zeta_{2\mathrm{d}}^{-1}\omega_{\mathrm{d}}(S(TS)^3)\mathfrak{u}_{\mathrm{d}}=\zeta_{2\mathrm{d}}^{-1}\omega_{\mathrm{d}}(S)\mathfrak{u}_{\mathrm{d}}=\mathfrak{w}_{\mathrm{d}}.\end{gathered}$$ □

In the following two subsections, we work at the 2-part and 3-part separately and construct $\mathfrak{u}_{\mathrm{d},p}$ for $p=2,3$. This will shed some light on where $\mathfrak{u}_{\mathrm{d}}$ comes from.

3B. ***The case p = 3.*** There are two possibilities for $\mathcal{A}_{\mathrm{d},3}$. If $3\nmid \mathrm{d}$, then $\mathcal{A}_{\mathrm{d},3}$ is trivial. If $3\mid \mathrm{d}$, we can identify the groups $\mathcal{A}_{\mathrm{d},3}$ and $\mathcal{A}:=M_2(\mathbb{F}_3)$ via

$$\kappa_{\mathrm{d},3}:M_2(\mathbb{F}_3)\cong\mathcal{A}_{\mathrm{d},3},\qquad \begin{pmatrix}h_0&-h_1\\h_2&h_3\end{pmatrix}\bmod 3\mapsto h=[h_0,h_1,h_2,h_3]\otimes\mathbb{Z}_3,\tag{3-18}$$

which is just the map κ_{d} in (3-6) tensored with $\mathbb{Z}_3$. This is an isomorphism of finite quadratic modules if we equip $M_2(\mathbb{F}_3)$ with the quadratic form $Q_{\mathrm{d},3}:=(3\mathrm{d}_2)^{-1}\det$, which has value in $\frac{1}{3}\mathbb{Z}/\mathbb{Z}$. Then $H_3\cong\mathrm{SL}_2(\mathbb{F}_3)\times\mathrm{SL}_2(\mathbb{F}_3)$, $H_3'=\langle N_3'\times N_3',(T,T)\rangle$, where

$$\begin{aligned}N_{\mathrm{d},3}'&:=\left\{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}-1&-1\\-1&1\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}-1&1\\1&1\end{smallmatrix}\right),\left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\1&-1\end{smallmatrix}\right),\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}1&-1\\-1&-1\end{smallmatrix}\right)\right\}\\&=\left\langle\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\1&-1\end{smallmatrix}\right)\right\rangle\subset\mathrm{SL}_2(\mathbb{F}_3)\subset M_2(\mathbb{F}_3)\end{aligned}\tag{3-19}$$

is isomorphic to the group of quaternions. Another way to characterize $N_{\mathrm{d},3}'$ is

$$N_{\mathrm{d},3}'=\left\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\right\}\cup\left\{g\in\mathrm{SL}_2(\mathbb{F}_3):\mathrm{Tr}(g)=0\right\}.\tag{3-20}$$

From this, it is easy to check the following local analog of Lemma 3.1 at 3.

Lemma 3.8. *For any $j\in\mathbb{Z}/\mathrm{d}_3\mathbb{Z}$, we have*

$$\kappa_{\mathrm{d},3}(T^jN_{\mathrm{d},3}')\cap\mathcal{A}_{\mathrm{d},3}^0=\{\pm[1,-j,0,1]\}.$$

Denote $\mathbf{0}_3\in\mathcal{A}$ the zero matrix. Then $H_{\mathrm{d},3}$ acts on the set $\mathcal{A}\backslash\mathbf{0}_3$, and decomposes it into 3 orbits according to the norm of the elements. The subgroup $H_{\mathrm{d},3}'\subset H_{\mathrm{d},3}$ acts on $\mathcal{A}\backslash\mathbf{0}_3$ similarly and decomposes the three orbits into 5 orbits. We denote the sum of elements in each orbit by $\mathfrak{w}_i$ for $i=0,1,2,3,4$. They are explicitly given as follows:

$$\mathfrak{w}_i:=\begin{cases}\sum_{h\in\kappa_{\mathrm{d},3}(T^iN_{\mathrm{d},3}')}\mathfrak{e}_h & \text{if } i=0,1,2.\\ \sum_{h\in\mathcal{A}\backslash\mathbf{0}_3,\,\det(h)\equiv -i \bmod 3}\mathfrak{e}_h & \text{if } i=3,4.\end{cases}\tag{3-21}$$

This gives $U_{\mathrm{d},3}^{H_{\mathrm{d},3}'}\cong\mathbb{C}\mathfrak{e}_{\mathbf{0}_3}+\sum_{j=0}^4\mathbb{C}\mathfrak{w}_j\subset\mathbb{C}[\mathcal{A}]$. Moreover, $U_{\mathrm{d},3}^{H_{\mathrm{d},3}'}$ contains an $\mathrm{SL}_2(\mathbb{Z})$-invariant vector $4\mathfrak{e}_{\mathbf{0}_3}+\mathfrak{w}_3$, which is also in $U_{\mathrm{d},3}^{H_{\mathrm{d},3}}$. Its orthogonal complement in $U_{\mathrm{d},3}^{H_{\mathrm{d},3}'}$ is 5-dimensional and decomposes into $\chi_3^{-\mathrm{d}_2} \oplus \chi_3^{-\mathrm{d}_2} \oplus \varrho^{-\mathrm{d}_2}$, where χ_3 and ϱ are irreducible representations of $\mathrm{SL}_2(\mathbb{Z})$ given by

$$\chi_3(T) = \zeta_3, \quad \chi_3(S) = 1, \quad \varrho(T) = \begin{pmatrix} 1 & & \\ & \zeta_3 & \\ & & \zeta_3^2 \end{pmatrix}, \quad \varrho(S) = \frac{1}{3}\begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}, \tag{3-22}$$

with respect to the basis $\{\mathfrak{w}_0 - \mathfrak{w}_1, \mathfrak{w}_0 - \mathfrak{w}_2, 8\mathfrak{e}_{\mathbf{0}_3} - \mathfrak{w}_3, \mathfrak{w}_0 + \mathfrak{w}_1 + \mathfrak{w}_2, 2\mathfrak{w}_4\}$. For any $m \in \mathbb{Z}$, we use $\varrho^{[m]}$ and $\chi_3^{[m]}$ to denote the representations of $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$\varrho^{[m]}(g) := \varrho(g)^m, \quad \chi_3^{[m]}(g) := \chi_3(g)^m.$$

Note that $\varrho^{[m]}$ and $\chi_3^{[m]}$ are well-defined and only depend on m mod 3. We remark $\chi_3|_{\Gamma_0(2)} = \chi^8$. In summary, we have:

Lemma 3.9. (1) *The subrepresentation $\omega_{\mathrm{d},3}^{H_{\mathrm{d},3}} \subset \omega_{\mathrm{d},3}$ fixed by $H_{\mathrm{d},3}$ decomposes as*

$$\omega_{\mathrm{d},3}^{H_{\mathrm{d},3}} \cong \mathbb{1} \oplus \varrho^{[-\mathrm{d}_2]}$$

with respect to the basis $\{4\mathfrak{e}_{\mathbf{0}_3} + \mathfrak{w}_3, 8\mathfrak{w}_0 - \mathfrak{w}_3, \mathfrak{w}_0 + \mathfrak{w}_1 + \mathfrak{w}_2, 2\mathfrak{w}_4\}$.

(2) *Denote $U'_{\mathrm{d},3}$ the orthogonal complement of $U_{\mathrm{d},3}^{H_{\mathrm{d},3}}$ in $U_{\mathrm{d},3}^{H'_{\mathrm{d},3}}$ and $\omega'_{\mathrm{d},3}$ the restriction of $\omega_{\mathrm{d},3}$ to $U'_{\mathrm{d},3}$. Then*

$$U'_{\mathrm{d},3} = \left\{ \sum_{j=0}^{2} a_j \mathfrak{w}_j : a_j \in \mathbb{C}, \sum_j a_j = 0 \right\}$$

and $\omega'_{\mathrm{d},3} \cong (\chi_3^{[-\mathrm{d}_2]})^{\oplus 2}$.

(3) *Under this identification, $M^!(\omega_{\mathrm{d},3})^{H_{\mathrm{d},3}} \cong M^! \oplus M^!(\varrho^{[-\mathrm{d}_2]})$ and*

$$M^!(\omega_{\mathrm{d},3})^{H'_{\mathrm{d},3}} \cong M^!(\omega_{\mathrm{d},3})^{H_{\mathrm{d},3}} \oplus M^!(\chi_3^{[-\mathrm{d}_2]})^{\oplus 2}.$$

The analog of $\mathfrak{u}_{\mathrm{d}}$ satisfying Lemma 3.4 and Proposition 3.5 is in the subspace

$$U'_{\mathrm{d},3} = \{\mathfrak{u}_{\mathrm{d},3}(\vec{c}) : \vec{c} = (c_s) \in \mathbb{C}^{\varphi(\mathrm{d}_3)}\},$$

where

$$\mathfrak{u}_{\mathrm{d},3}(\vec{c}) := \sum_{j \in \mathbb{Z}/\mathrm{d}_3\mathbb{Z}} \biggl(\sum_{s \in (\mathbb{Z}/\mathrm{d}_3\mathbb{Z})^\times} c_s \zeta_{\mathrm{d}_3}^{sj} \biggr) \biggl(\sum_{h \in \kappa_{\mathrm{d},3}(T^j N'_{\mathrm{d},3})} \mathfrak{e}_h \biggr). \tag{3-23}$$

As a consequence of Lemma 3.4, we have the following local analog of Proposition 3.5 at $p = 3$.

Proposition 3.10. *For any* $\mathrm{d} \mid 24$ *and $\vec{c} \in \mathbb{C}^{\varphi(\mathrm{d}_3)}$, we have*

$$\omega_{\mathrm{d},3}(g)\mathfrak{u}_{\mathrm{d},3}(\vec{c}) = \chi(g)^{-24\mathrm{d}_2/\mathrm{d}_3}\mathfrak{u}_{\mathrm{d},3}(\vec{c}) \tag{3-24}$$

for all $g \in \Gamma_0(2)$.

Proof. If $\mathrm{d}_3 = 1$, this is clear. Otherwise,

$$\omega_{\mathrm{d},3}(g)\mathfrak{u}_{\mathrm{d},3}(\vec{c}) = \chi_3(g)^{-\mathrm{d}_2}\mathfrak{u}_{\mathrm{d},3}(\vec{c}) = \chi(g)^{-8\mathrm{d}_2}\mathfrak{u}_{\mathrm{d},3}(\vec{c}). \qquad \square$$

If $\vec{c} = (1, \dots, 1) \in \mathbb{C}^{\varphi(\mathrm{d}_3)}$, then we simply denote $\mathfrak{u}_{\mathrm{d},3}(\vec{c})$ by $\mathfrak{u}_{\mathrm{d},3}$, which is explicitly given by

$$\mathfrak{u}_{\mathrm{d},3} = \begin{cases} 2\mathfrak{w}_0 - \mathfrak{w}_1 - \mathfrak{w}_2 & \text{if } \mathrm{d}_3 = 3, \\ \mathfrak{e}_{\mathbf{0}_3} & \text{if } \mathrm{d}_3 = 1. \end{cases} \tag{3-25}$$

3C. ***The case $p = 2$.*** In this case, the finite quadratic module

$$\mathcal{A}_{\mathrm{d},2} = \mathbb{Z}/\mathrm{d}_2\mathbb{Z} \times \mathbb{Z}/(2\mathrm{d}_2)\mathbb{Z} \times \mathbb{Z}/(2\mathrm{d}_2)\mathbb{Z} \times \mathbb{Z}/\mathrm{d}_2\mathbb{Z}$$

has the quadratic form

$$Q_{\mathrm{d},2}([h_0, h_1, h_2, h_3]) := \frac{\mathrm{d}_3^{-1}}{2\mathrm{d}_2}(2h_0h_3 - h_1h_2) \in \frac{1}{2\mathrm{d}_2}\mathbb{Z}/\mathbb{Z}. \tag{3-26}$$

Even though the size of $\mathcal{A}_{\mathrm{d},2}$ can be large, the number of orbits under the suitable orthogonal group $H'_{\mathrm{d},2}$ is much smaller. More precisely, we have $H_{\mathrm{d},2} = N_{\mathrm{d},2} \times N_{\mathrm{d},2}$ and $H'_{\mathrm{d},2} \supset N'_{\mathrm{d},2} \times N'_{\mathrm{d},2}$, where

$$\begin{aligned} N_{\mathrm{d},2} &:= \left\{ \begin{pmatrix} a & b \\ 2c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/(2\mathrm{d}_2\mathbb{Z})) \right\} / \langle T^{\mathrm{d}_2}, C^{\mathrm{d}_2/(2,\mathrm{d}_2)} \rangle, \\ N'_{\mathrm{d},2} &:= \langle A, C, D \rangle \cong (\mathbb{Z}/(\mathrm{d}_2(2,\mathrm{d}_2)/(4,\mathrm{d}_2))\mathbb{Z} \times \mathbb{Z}/(\mathrm{d}_2/(2,\mathrm{d}_2))\mathbb{Z}) \rtimes \mathbb{Z}/(4,\mathrm{d}_2)\mathbb{Z}. \end{aligned} \tag{3-27}$$

Here $A := \left(\begin{smallmatrix} 3 & 2 \\ 4 & 3 \end{smallmatrix}\right)$, $C := \left(\begin{smallmatrix} 5 & 4 \\ 16 & 13 \end{smallmatrix}\right)$, $D := \left(\begin{smallmatrix} -1 & 1 \\ -2 & 1 \end{smallmatrix}\right)$ are elements in $\mathrm{SL}_2(\mathbb{Z})$ projected into $N_{\mathrm{d},2}$. The commutation relation is given by $DAD^{-1} = A^3$. In particular $N'_{\mathrm{d},2}$ has size d_2^2 and is abelian for $\mathrm{d}_2 = 1, 2, 4$.

The group $N_{\mathrm{d},2}$ acts on the left on $\mathcal{A}_{\mathrm{d},2}$ via (simply coming from matrix multiplication)

$$\begin{pmatrix} a & b \\ 2c & d \end{pmatrix} \cdot [h_0, h_1, h_2, h_3] := [ah_0 + bh_2, ah_1 + 2(bh_3), 2(ch_0) + dh_2, ch_1 + dh_3] \tag{3-28}$$

for $\left(\begin{smallmatrix} a & b \\ 2c & d \end{smallmatrix}\right) \in N_{\mathrm{d},2}$ and $[h_0, h_1, h_2, h_3] \in \mathcal{A}_{\mathrm{d},2}$. The same holds for the right action. We can embed $N_{\mathrm{d},2}$ into $\mathcal{A}_{\mathrm{d},2}$ using the map $\kappa_{\mathrm{d},2} : N_{\mathrm{d},2} \to \mathcal{A}_{\mathrm{d},2}$ defined by

$$\kappa_{\mathrm{d},2}\left(\begin{pmatrix} a & b \\ 2c & d \end{pmatrix}\right) := \mathrm{d}_3^{-1}[a \bmod \mathrm{d}_2, 2b, 2c, d \bmod \mathrm{d}_2]. \tag{3-29}$$

It is then easy to check that

$$\begin{aligned} \kappa_{\mathrm{d},2}(g_1g_2) &= g_1 \cdot \kappa_{\mathrm{d},2}(g_2) = \kappa_{\mathrm{d},2}(g_1) \cdot g_2, \\ Q_{\mathrm{d},2}(\kappa_{\mathrm{d},2}(g)) &= \frac{\mathrm{d}_3^{-1}\det(g) \bmod \mathrm{d}_2}{\mathrm{d}_2} \in \frac{2}{2\mathrm{d}_2}\mathbb{Z}/\mathbb{Z} \end{aligned} \tag{3-30}$$

for all $g, g_1, g_2 \in N_{\mathrm{d},2}$. From this, when $2 \mid \mathrm{d}$, it is easy to check that $\kappa_{\mathrm{d},2}$ is a two-to-one map since $(\mathrm{d}_2 + 1)\left(\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right) \in N'_{\mathrm{d},2}$ and

$$\kappa_{\mathrm{d},2}\left((\mathrm{d}_2 + 1)\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}\right) = \kappa_{\mathrm{d},2}\left(\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}\right).$$

To better describe $\kappa_{\mathrm{d},2}(N_{\mathrm{d},2})$, it is useful to know the smallest additive subgroup of $\mathcal{A}_{\mathrm{d},2}$ containing it. We describe it in the following lemma.

Lemma 3.11. *Let $\mathcal{A}'_{\mathrm{d},2} \subset \mathcal{A}_{\mathrm{d},2}$ be the smallest* (*additive*) *subgroup containing $\kappa_{\mathrm{d},2}(N'_{\mathrm{d},2})$.*

(1) *When $8 \mid \mathrm{d}$, $\mathcal{A}'_{\mathrm{d},2} \cong (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/8\mathbb{Z})^2$ is the orthogonal complement of the subgroup generated by* $[6, 4, 0, 2]$, $[0, 8, 0, 0]$, $[0, 2, 2, 0] \in \mathcal{A}_{\mathrm{d},2}$, *and*

$$\kappa_{\mathrm{d},2}^{-1}(\mathcal{A}'_{\mathrm{d},2}) = N'_{\mathrm{d},2} \sqcup T^4 N'_{\mathrm{d},2}.$$

Furthermore, we can distinguish the elements in $N'_{\mathrm{d},2}$ and $T^4 N'_{\mathrm{d},2}$ via

$$\begin{aligned} N'_{\mathrm{d},2} &= \kappa_{\mathrm{d},2}^{-1}(\{[h_0, h_1, h_2, h_3] \in \mathcal{A}'_{\mathrm{d},2} : h_0^2 - \mathrm{d}_3^2 \equiv h_1 + h_2 \bmod 16\}), \\ T^4 N'_{\mathrm{d},2} &= \kappa_{\mathrm{d},2}^{-1}(\{[h_0, h_1, h_2, h_3] \in \mathcal{A}'_{\mathrm{d},2} : h_0^2 - \mathrm{d}_3^2 \equiv h_1 + h_2 + 8 \bmod 16\}). \end{aligned} \tag{3-31}$$

(2) *When $8 \nmid \mathrm{d}$, $\mathcal{A}'_{\mathrm{d},2} \cong (\mathbb{Z}/\mathrm{d}_2\mathbb{Z})^2$ is generated by $\kappa_{\mathrm{d},2}\big(\big(\begin{smallmatrix}1 & \\ & 1\end{smallmatrix}\big)\big)$, $\kappa_{\mathrm{d},2}\big(\big(\begin{smallmatrix}-1 & 1 \\ -2 & 1\end{smallmatrix}\big)\big)$ and*

$$\kappa_{\mathrm{d},2}^{-1}(\mathcal{A}'_{\mathrm{d},2}) = N'_{\mathrm{d},2}.$$

Proof. This can be verified using the Appendix and some computer calculation. □

In addition, we record the following local analog of Lemma 3.1 at the prime 2.

Lemma 3.12. *For any $j \in \mathbb{Z}/\mathrm{d}_2\mathbb{Z}$, we have*

$$\kappa_{\mathrm{d},2}(T^j N'_{\mathrm{d},2}) \cap \mathcal{A}^0_{\mathrm{d},2} = \{[r, r(2j + (\mathrm{d}_3 r)^2 - 1), 0, r] : r \in (\mathbb{Z}/\mathrm{d}_2\mathbb{Z})^\times\}.$$

Proof. For $j = 0$, this follows directly from Lemma 3.11. In general, it is easy to check that

$$T^j(\kappa_{\mathrm{d},2}(N'_{\mathrm{d},2}) \cap \mathcal{A}^0_{\mathrm{d},2}) = \kappa_{\mathrm{d},2}(T^j N'_{\mathrm{d},2}) \cap \mathcal{A}^0_{\mathrm{d},2}$$

for any j since the action of T preserves $\mathcal{A}^0_{\mathrm{d}}$. □

Since $T^{\mathrm{d}_2} = 0 \in N'_{\mathrm{d},2}$ and $H'_{\mathrm{d},2}$ is generated by $N'_{\mathrm{d},2} \times N'_{\mathrm{d},2}$ and (T, T), the index of $H'_{\mathrm{d},2}$ in $H_{\mathrm{d},2}$ is d_2 and the sizes of $H_{\mathrm{d},2}$ and $H'_{\mathrm{d},2}$ are $\mathrm{d}_2^6/(2, \mathrm{d}_2)$ and $\mathrm{d}_2^5/(2, \mathrm{d}_2)$ respectively. The dimension of $U_{\mathrm{d},2}^{H'_{\mathrm{d},2}}$ is the number of orbits in $\mathcal{A}_{\mathrm{d},2}$ under the action of $H'_{\mathrm{d},2}$. Since the finite group $H'_{\mathrm{d},2}$ is explicitly given in (3-27), it is straightforward to calculate these orbits on a computer in practice. We did this in Sage [2019] and received the following results:

$$\dim U_{\mathrm{d},2}^{H'_{\mathrm{d},2}} = \begin{cases} 4 & \text{if } \mathrm{d}_2 = 1, \\ 16 & \text{if } \mathrm{d}_2 = 2, \\ 46 & \text{if } \mathrm{d}_2 = 4, \\ 118 & \text{if } \mathrm{d}_2 = 8. \end{cases} \tag{3-32}$$

With these calculations, one can already explicitly decompose the representation $\omega_{\mathrm{d},2}^{H'_{\mathrm{d},2}}$ on $U_{\mathrm{d},2}^{H'_{\mathrm{d},2}}$. To find the desired vectors, we need to consider the following subspace of $U_{\mathrm{d},2}^{H'_{\mathrm{d},2}}$.

For $\mathrm{d}_2 = 1$, the vector $\mathfrak{e}_{(1/2,0)} - \mathfrak{e}_{(0,1/2)}$ generates a 1-dimensional $\mathrm{SL}_2(\mathbb{Z})$-invariant subspace. Denote $U'_{\mathrm{d},2} \subset U_{\mathrm{d},2}^{H'_{\mathrm{d},2}}$ its orthogonal complement. For $\mathrm{d}_2 \geq 2$, the subgroup $H'_{\mathrm{d},2}$ has index 2 in $H'_{\mathrm{d}/2,2} = \langle T^{\mathrm{d}_2/2}, H'_{\mathrm{d},2}\rangle$. Denote $U'_{\mathrm{d},2} \subset U_{\mathrm{d},2}^{H'_{\mathrm{d},2}}$ the orthogonal complement of $U_{\mathrm{d},2}^{H'_{\mathrm{d}/2,2}} \subset U_{\mathrm{d},2}^{H'_{\mathrm{d},2}}$. Then it is clear that

$$\dim U'_{\mathrm{d},2} = \tfrac{1}{2}\big(\text{numbers of } H'_{\mathrm{d},2}\text{-orbits of } \mathcal{A}_{\mathrm{d},2} - \text{numbers of } H'_{\mathrm{d}/2,2}\text{-orbits of } \mathcal{A}_{\mathrm{d},2}\big).$$

The following result comes out of the computer calculations.

Lemma 3.13. *For any* $\mathrm{d} \mid 24$, *the dimension of* $U'_{\mathrm{d},2}$ *is* $3\varphi(\mathrm{d}_2)$. *Furthermore, the support of any elements in* $U'_{\mathrm{d},2}$ *is contained in the union of* $\{h \in \mathcal{A}_{\mathrm{d},2} : 2Q_{\mathrm{d}}(h) = -\mathrm{d}_3^{-1}/\mathrm{d}_2\}$ *and* $\bigcup_{j \in \mathbb{Z}/\mathrm{d}_2\mathbb{Z}} \kappa_{\mathrm{d},2}(T^j N'_{\mathrm{d},2})$.

Now for $\mathrm{d} \mid 24$, define the following vectors

$$\begin{aligned} \mathfrak{u}_{\mathrm{d},2}(\vec{c}) &:= \sum_{j \in \mathbb{Z}/\mathrm{d}_2\mathbb{Z}} \Bigg(\sum_{s \in (\mathbb{Z}/\mathrm{d}_2\mathbb{Z})^\times} c_s \zeta_{\mathrm{d}_2}^{js} \Bigg) \Bigg(\sum_{h \in \kappa_{\mathrm{d},2}(T^j N'_{\mathrm{d},2})} \mathfrak{e}_h \Bigg), \\ \mathfrak{v}_{\mathrm{d},2}(\vec{c}) &:= \omega_{\mathrm{d},2}(S)\mathfrak{u}_{\mathrm{d},2}(\vec{c}), \qquad \mathfrak{w}_{\mathrm{d},2}(\vec{c}) := \zeta_{\mathrm{d}_2}^{-\mathrm{d}_3} \omega_{\mathrm{d},2}(T)\mathfrak{v}_{\mathrm{d},2}(\vec{c}) \end{aligned} \tag{3-33}$$

for all $\vec{c} = (c_s) \in \mathbb{C}^{\varphi(\mathrm{d}_2)}$. From Lemma 3.13, we can show that these vectors give a basis of $U'_{\mathrm{d},2}$.

Lemma 3.14. *For any* $\mathrm{d} \mid 24$ *with* $2 \mid \mathrm{d}$ *and* $\vec{c} \in \mathbb{C}^{\varphi(\mathrm{d}_2)}$, *the vectors* $\mathfrak{v}_{\mathrm{d},2}(\vec{c})$, $\mathfrak{w}_{\mathrm{d},2}(\vec{c})$ *have the same support, which is disjoint from that of* $\mathfrak{u}_{\mathrm{d},2}(\vec{c_1})$ *for any* $\vec{c_1} \in \mathbb{C}^{\varphi(\mathrm{d}_2)}$.

Proof. Since the action of $\omega_{\mathrm{d},2}(T)$ does not change the support, we know that $\mathfrak{v}_{\mathrm{d},2}(\vec{c})$ and $\mathfrak{w}_{\mathrm{d},2}(\vec{c})$ have the same support. Now we have by definition

$$\mathfrak{v}_{\mathrm{d},2}(\vec{c}) = (2\mathrm{d}_2^2)^{-1} \sum_{s \in (\mathbb{Z}/\mathrm{d}_2\mathbb{Z})^\times} c_s \sum_{\mu \in \mathcal{A}_{\mathrm{d},2}} \sum_{j \in \mathbb{Z}/\mathrm{d}_2\mathbb{Z}} \zeta_{\mathrm{d}_2}^{js} \Bigg(\sum_{h \in \kappa_{\mathrm{d},2}(T^j N'_{\mathrm{d},2})} \mathbf{e}((\mu, h)) \mathfrak{e}_\mu \Bigg).$$

We want to show that the coefficient of $\mathfrak{e}_\mu$ is zero if $\mu = \kappa_{\mathrm{d},2}(T^{j'} g')$ with $j' \in \mathbb{Z}/\mathrm{d}_2\mathbb{Z}$ and $g' \in N'_{d,2}$. Now if $h = \kappa_{\mathrm{d},2}(g)$ with $g \in T^j N'_{d,2}$, then

$$(\mu, h) = \frac{\mathrm{d}_3^{-1} \operatorname{Tr}(g(T^{j'} g')^{-1})}{\mathrm{d}_2}$$

by (3-30). Since $N'_{\mathrm{d},2}$ is normal in $N_{\mathrm{d},2}$, which contains T, we have $T^j N'_{\mathrm{d},2} T^{-j'} = T^{j-j'} N'_{\mathrm{d},2}$. Therefore, it suffices to show that the sum below vanishes

$$\sum_{j \in \mathbb{Z}/\mathrm{d}_2\mathbb{Z}} \zeta_{\mathrm{d}_2}^{js} \sum_{h \in \kappa_{\mathrm{d},2}(T^j N'_{\mathrm{d},2})} \mathbf{e}((\mu, h)) = \zeta_{\mathrm{d}_2}^{j's} \sum_{j'' \in \mathbb{Z}/\mathrm{d}_2\mathbb{Z}} \zeta_{\mathrm{d}_2}^{j''s} \sum_{h \in \kappa_{\mathrm{d},2}(T^{j''} N'_{\mathrm{d},2})} \zeta_{\mathrm{d}_2}^{\mathrm{d}_3^{-1} \operatorname{Tr}(h)}$$

with $j'' := j - j'$. Also for $h = [h_0, h_1, h_2, h_3] \in \kappa_{\mathrm{d},2}(N'_{\mathrm{d},2})$, we have $\operatorname{Tr}(T^j \cdot h) = \operatorname{Tr}(h) + j \cdot h_1$. Using this, we can rewrite

$$\sum_{j'' \in \mathbb{Z}/\mathrm{d}_2\mathbb{Z}} \zeta_{\mathrm{d}_2}^{j''s} \sum_{h \in \kappa_{\mathrm{d},2}(T^{j''} N'_{\mathrm{d},2})} \zeta_{\mathrm{d}_2}^{\mathrm{d}_3^{-1} \operatorname{Tr}(h)} = \sum_{h \in \kappa_{\mathrm{d},2}(N'_{\mathrm{d},2})} \zeta_{\mathrm{d}_2}^{\mathrm{d}_3^{-1} \operatorname{Tr}(h)} \sum_{j'' \in \mathbb{Z}/\mathrm{d}_2\mathbb{Z}} \zeta_{\mathrm{d}_2}^{j''(s + \mathrm{d}_3^{-1} h_1)}$$

By Lemma 3.11 (or inspecting the Appendix), we know that $h_1 \in 2\mathbb{Z}/2\mathrm{d}_2\mathbb{Z}$ for all $h \in \kappa_{\mathrm{d},2}(N'_{\mathrm{d},2})$. So $s + \mathrm{d}_3^{-1}h_1 \in (\mathbb{Z}/\mathrm{d}_2\mathbb{Z})^\times$ and the sum above vanishes. □

Lemma 3.15. *For any* $\mathrm{d} \mid 24$ *and any basis* $\mathcal{B}$ *of* $\mathbb{C}^{\varphi(\mathrm{d}_2)}$*, the set*

$$\bigcup_{\vec{c}\in\mathcal{B}} \{\mathfrak{u}_{\mathrm{d},2}(\vec{c}), \mathfrak{v}_{\mathrm{d},2}(\vec{c}), \mathfrak{w}_{\mathrm{d},2}(\vec{c})\} \tag{3-34}$$

is a basis of $U'_{\mathrm{d},2}$.

Proof. We know that dimension of $U'_{\mathrm{d},2}$ is $3\varphi(\mathrm{d}_2)$ from Lemma 3.13, and need to check linear independence of the vectors in the set above. Since the vectors $\mathfrak{u}_{\mathrm{d},2}(\vec{c})$, $\mathfrak{v}_{\mathrm{d},2}(\vec{c})$, $\mathfrak{w}_{\mathrm{d},2}(\vec{c})$ are defined linearly, it suffices to prove the lemma for $\mathcal{B} = \{\vec{e}(s_0) : s_0 \in (\mathbb{Z}/\mathrm{d}_2\mathbb{Z})^\times\}$ with $\vec{e}(s_0) \in \mathbb{C}^{\varphi(\mathrm{d}_2)}$ the standard basis vector with 0 everywhere except 1 at the s_0-th entry. It is easily checked from the definition that $\mathfrak{u}_{\mathrm{d},2}(\vec{c})$, $\mathfrak{v}_{\mathrm{d},2}(\vec{c})$, $\mathfrak{w}_{\mathrm{d},2}(\vec{c})$ are in $U'_{\mathrm{d},2}$ are eigenvectors of T with eigenvalue $\zeta_{\mathrm{d}_2}^{-s_0}$ when $\vec{c} = \vec{e}(s_0)$. Therefore, it suffices to check that the three vectors $\mathfrak{u}_{\mathrm{d},2}(\vec{c})$, $\mathfrak{v}_{\mathrm{d},2}(\vec{c})$, $\mathfrak{w}_{\mathrm{d},2}(\vec{c})$ are linearly independent whenever $\vec{c} = \vec{e}(s_0)$.

When $\mathrm{d}_2 = 1$, this is easily checked by hand. When $\mathrm{d}_2 \geq 2$, it suffices to show that $\mathfrak{v}_{\mathrm{d},2}(\vec{e}(s_0))$ and $\mathfrak{w}_{\mathrm{d},2}(\vec{e}(s_0))$ are linearly independent by Lemma 3.14. Let us assume otherwise. Then the restriction of $\omega_{\mathrm{d},2}$ to $\mathbb{C}\mathfrak{u}_{\mathrm{d},2}(\vec{e}(s_0)) + \mathbb{C}\mathfrak{v}_{\mathrm{d},2}(\vec{e}(s_0))$ is a 2-dimensional representation of $\mathrm{SL}_2(\mathbb{Z})$. In the basis $\{\mathfrak{u}_{\mathrm{d},2}(\vec{e}(s_0)), \mathfrak{v}_{\mathrm{d},2}(\vec{e}(s_0))\}$, it is given by the map

$$T \mapsto \begin{pmatrix} \zeta_{\mathrm{d}_2}^{-1} & \\ & \pm\zeta_{2\mathrm{d}_2} \end{pmatrix}, \quad S \mapsto \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}.$$

However, $(T \cdot S)^6$ is the identity, whereas

$$\left(\begin{pmatrix} \zeta_{\mathrm{d}_2}^{-1} & \\ & \pm\zeta_{2\mathrm{d}_2} \end{pmatrix}\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}\right)^6 = \left(\pm\begin{pmatrix} \zeta_{2\mathrm{d}_2}^{-1} & \\ & \zeta_{2\mathrm{d}_2}^{-1} \end{pmatrix}\right)^3$$

is not the identity since $2 \mid \mathrm{d}_2$. This is a contradiction and finishes the proof. □

Proposition 3.16. *For* $\mathrm{d} \mid 24$, *let* $\omega'_{\mathrm{d},2}$ *denote the restriction of* $\omega_{\mathrm{d},2}$ *to* $U'_{\mathrm{d},2} \subset U_{\mathrm{d},2}^{H'_{\mathrm{d},2}}$. *Then* $\mathfrak{u}_{\mathrm{d},2}(\vec{c})$ *satisfies*

$$\omega'_{\mathrm{d},2}(g)\mathfrak{u}_{\mathrm{d},2}(\vec{c}) = \chi(g)^{-24\mathrm{d}_3/\mathrm{d}_2}\mathfrak{u}_{\mathrm{d},2}(\vec{c}) \tag{3-35}$$

for all $g \in \Gamma_0(2)$ *and* $\vec{c} \in \mathbb{C}^{\varphi(\mathrm{d}_2)}$. *Furthermore with respect to the basis in* (3-34), *we have*

$$\omega'_{\mathrm{d},2} \cong \varrho_{\mathrm{d}_2,\mathrm{d}_3}^{\oplus\varphi(\mathrm{d}_2)} \tag{3-36}$$

Here $\varrho_{\mathrm{d}_2,\mathrm{d}_3}$ *is the* 3*-dimensional representation defined in* (2-3).

Remark 3.17. If $\vec{c} = (1, \dots, 1) \in \mathbb{C}^{\varphi(\mathrm{d}_2)}$, we simply write $\mathfrak{u}_{\mathrm{d},2}$ for $\mathfrak{u}_{\mathrm{d},2}(\vec{c})$. They are explicitly given by

$$\mathfrak{u}_{\mathrm{d},2} = \begin{cases} \mathfrak{e}_{0_2} & \text{if } \mathrm{d}_2 = 1, \\ 2^{\mathrm{d}_2/2}\big(\sum_{\kappa_{\mathrm{d},2}(N'_{\mathrm{d},2})} \mathfrak{e}_h - \sum_{\kappa_{\mathrm{d},2}(T^{\mathrm{d}_2/2}N'_{\mathrm{d},2})} \mathfrak{e}_h\big) & \text{if } \mathrm{d}_2 = 2, 4, 8. \end{cases} \tag{3-37}$$

Proof. For the first claim, it suffices to prove the cases $g = T, S^2, TB$, which are generators of $\Gamma_0(2)$. If $g = T$, then $\omega'_{\mathrm{d},2}(T)\mathfrak{e}_h = \mathbf{e}(-Q_{\mathrm{d},2}(h))\mathfrak{e}_h$. For $h \in \kappa_{\mathrm{d},2}(T^jN'_{\mathrm{d},2})$, we have $Q_{\mathrm{d},2}(h) = \mathrm{d}_3^{-1}/\mathrm{d}_2 =$

$\mathrm{d}_3/\mathrm{d}_2 \in \frac{1}{\mathrm{d}_2}\mathbb{Z}/\mathbb{Z}$. Therefore (3-35) holds for $g = T$. When $g = S^2$, since $\omega_{\mathrm{d}}(S^2)\mathfrak{e}_h = \mathfrak{e}_{-h}$ for all $h \in \mathcal{A}_{\mathrm{d}}$ and $-\left(\begin{smallmatrix}1 & \\ & 1\end{smallmatrix}\right) \in N'_{\mathrm{d},2}$, we know that $-\kappa_{\mathrm{d}}(T^j N'_{\mathrm{d},2}) = \kappa_{\mathrm{d}}(T^j N'_{\mathrm{d},2})$ and (3-35) holds for $g = S^2$.

For $g = TB = TST^2S^{-1}$, it suffices to show the middle equation below

$$\omega'_{\mathrm{d},2}(S)\omega_{\mathrm{d},2}(T^{-1})\mathfrak{u}_{\mathrm{d},2}(\vec{c}) = \zeta_{\mathrm{d}_2}^{\mathrm{d}_3^{-1}}\mathfrak{v}_{\mathrm{d},2}(\vec{c}) = \omega_{\mathrm{d},2}(T^2)\mathfrak{v}_{\mathrm{d},2}(\vec{c}) = \omega_{\mathrm{d},2}(T^2)\omega'_{\mathrm{d},2}(S)\mathfrak{u}_{\mathrm{d},2}(\vec{c}).$$

This is easily checked by hand when $\mathrm{d}_2 = 1$. If $2 \mid \mathrm{d}_2$, we know by Lemmas 3.13 and 3.14 that the support of $\mathfrak{v}_{\mathrm{d},2}(\vec{c})$ is contained in $\{h \in \mathcal{A}_{\mathrm{d},2} : 2Q_{\mathrm{d}}(h) = -\mathrm{d}_3^{-1}/\mathrm{d}_2\}$. It is therefore an eigenvector of $\omega'_{\mathrm{d},2}(T^2)$ with eigenvalue $\zeta_{\mathrm{d}_2}^{\mathrm{d}_3^{-1}}$. This proves the first claim. As in the proof of Proposition 3.6, the vectors $\{\mathfrak{u}_{\mathrm{d},2}(\vec{c}), \mathfrak{v}_{\mathrm{d},2}(\vec{c}), \mathfrak{w}_{\mathrm{d},2}(\vec{c})\}$ generate a 3-dimensional subrepresentation of $\omega_{\mathrm{d},2}$ isomorphic to $\varrho_{\mathrm{d}_2,\mathrm{d}_3}$. The second claim then follows from Lemma 3.15. □

4. Borcherds liftings

4A. ***Brief review of Borcherds liftings.*** We first set up notation and briefly review the Borcherds lifting, following [Yang and Yin 2019, Section 3]. Let $V = V_{\mathrm{d}}$ and H be as in Section 3.

Let

$$\mathcal{L} = \{w \in V_{\mathbb{C}} : (w, w) = 0,\ (w, \bar{w}) < 0\}. \tag{4-1}$$

and let $\mathbb{D}$ be the Hermitian symmetric domain of oriented negative 2-planes in $V_{\mathbb{R}} = V \otimes_{\mathbb{Q}} \mathbb{R}$. Then one has an isomorphism

$$pr : \mathcal{L}/\mathbb{C}^\times \cong \mathbb{D}, \quad w = u + iv \mapsto \mathbb{R}u + \mathbb{R}(-v).$$

For the isotropic matrix $\ell = \left(\begin{smallmatrix}0 & -1\\ 0 & 0\end{smallmatrix}\right) \in L$ and $\ell' = \left(\begin{smallmatrix}0 & 0\\ 1/\mathrm{d} & 0\end{smallmatrix}\right) \in V$ with $(\ell, \ell') = 1$. We also have the associated tube domain

$$\mathcal{H}_{\ell,\ell'} = \left\{\begin{pmatrix}z_1 & 0\\ 0 & -z_2\end{pmatrix} : y_1y_2 > 0\right\}, \quad y_i = \mathrm{Im}(z_i),$$

together with

$$w : \mathcal{H}_{\ell,\ell'} \to \mathcal{L}, \quad w\left(\begin{pmatrix}z_1 & 0\\ 0 & -z_2\end{pmatrix}\right) = \begin{pmatrix}z_1 & -\mathrm{d}z_1z_2\\ 1/\mathrm{d} & -z_2\end{pmatrix}.$$

This gives an isomorphism $\mathcal{H}_{\ell,\ell'} \cong \mathcal{L}/\mathbb{C}^\times$. We also identity $\mathbb{H}^2 \cup (\mathbb{H}^-)^2$ with $\mathcal{H}_{\ell,\ell'}$ by

$$\psi_{\mathrm{d}} : z = (z_1, z_2) \mapsto \begin{pmatrix}z_1/\mathrm{d} & 0\\ 0 & -z_2/\mathrm{d}\end{pmatrix}.$$

Note that we use this identification in order to have the following compatibility property and it is also the identification used in the computation of Borcherds products. The following is a special case of [Yang and Yin 2019, Proposition 3.1].

Proposition 4.1. *Define*

$$w_{\mathrm{d}} : \mathbb{H}^2 \cup (\mathbb{H}^-)^2 \to \mathcal{L}, \quad w_{\mathrm{d}}(z_1, z_2) = w \circ \psi_{\mathrm{d}}(z_1, z_2) = \begin{pmatrix}z_1/\mathrm{d} & -z_1z_2/\mathrm{d}\\ 1/\mathrm{d} & -z_2/\mathrm{d}\end{pmatrix}.$$

Then the composition $pr \circ w_{\mathrm{d}}$ *gives an isomorphism between* $\mathbb{H}^2 \cup (\mathbb{H}^-)^2$ *and* $\mathbb{D}$. *Moreover*, w_{d} *is* $H(\mathbb{R})$*-equivariant, where* $H(\mathbb{R})$ *acts on* $\mathbb{H}^2 \cup (\mathbb{H}^-)^2$ *via the usual linear fraction*:

$$(g_1, g_2)(z_1, z_2) = (g_1(z_1), g_2(z_2)),$$

and acts on $\mathcal{L}$ *and* $\mathbb{D}$ *naturally via its action on* V. *Moreover, one has*

$$(g_1, g_2)w_{\mathrm{d}}(z_1, z_2) = \frac{j(g_1, z_1)j(g_2, z_2)}{\nu(g_1, g_2)} w_{\mathrm{d}}(g_1(z_1), g_2(z_2)), \tag{4-2}$$

where $\nu(g_1, g_2) = \det g_1 = \det g_2$ *is the spin character of* $H \cong \mathrm{GSpin}(V)$, *and*

$$j(g, z) := cz + d, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is the automorphy factor of weight 1.

For a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, let X_Γ be the associated open modular curve over $\mathbb{Q}$ such that $X_\Gamma(\mathbb{C}) = \Gamma\backslash\mathbb{H}$. Assume $\Gamma \supset \Gamma(M)$ for some integer $M \geq 1$. Let

$$\nu : \mathbb{A}^\times \hookrightarrow \mathrm{GL}_2(\mathbb{A}), \quad \nu(d) = \mathrm{diag}(1, d).$$

Let $K(\Gamma)$ be the product of $\nu(\widehat{\mathbb{Z}}^\times)$ and the preimage of $\Gamma/\Gamma(M)$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ (under the map $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$). Let $K = (K(\Gamma) \times K(\Gamma)) \cap H(\mathbb{A}_f)$. Then one has by the strong approximation theorem

$$X_K \cong X_\Gamma \times X_\Gamma.$$

In this way, we have identified the product of two copies of a modular curve X_Γ with a Shimura variety X_K.

Suppose that Γ acts on L'/L trivially, then for each $\mu \in L'/L$ and $m \in Q(\mu) + L$, the associated special divisor $Z_\Gamma(m, \mu)$ is given by

$$Z_\Gamma(m, \mu) = (\Gamma \times \Gamma)\backslash\{(z_1, z_2) : w_{\mathrm{d}}(z_1, z_2) \perp x \text{ for some } x \in \mu + L,\ Q(x) = m\}.$$

More generally, assume $\Gamma \supset \Gamma(M)$ preserves L, and $\mathfrak{u} = \sum a_\mu \mathfrak{e}_\mu \in \mathbb{C}[L'/L]$ is $\Gamma \times \Gamma$-invariant, the cycle

$$Z_{\Gamma(M)}(m, \mathfrak{u}) = \sum a_\mu Z_{\Gamma(M)}(m, \mu)$$

descends to a cycle $Z_\Gamma(m, \mathfrak{u})$ in $X_\Gamma \times X_\Gamma$. For our purpose, we will take

$$\mathrm{d} \mid 24, \quad \Gamma = \Gamma_{\chi,\mathrm{d}} \supset \Gamma_{\mathrm{d}} \supset \Gamma(2\mathrm{d}) \supset \Gamma(48)$$

from now on and write $X_{\mathrm{d}} := X_\Gamma = X_{\Gamma_{\chi,\mathrm{d}}}$. Notice that $X_1 = X_0(2)$ has two cusps, $i\infty$ and 0. Since $\{T^j : 1 \leq j \leq \mathrm{d}\}$ are coset representatives of $\Gamma_{\chi,\mathrm{d}}$ in $\Gamma_{\chi,1}$, the modular curve X_{d} has the same cusps as X_1.

Lemma 4.2 [Yang and Yin 2019, Corollary 3.3]. *For* $\mathrm{d} \mid \mathrm{d}' \mid 24$, *let* $\pi : X_{\Gamma(2\mathrm{d}')} \to X_{\mathrm{d}}$ *be the natural projection. Then*

$$(\pi \times \pi)^*(X_{\mathrm{d}}^\Delta) = \sum_{\gamma \in \Gamma/\Gamma(2\mathrm{d}')} Z_{\Gamma(2\mathrm{d}')}\Big(\frac{1}{\mathrm{d}'}, \frac{1}{\mathrm{d}'}\gamma + L\Big) \tag{4-3}$$

and the group $\Gamma(2\mathrm{d}')$ *can be replaced by* $\Gamma_{\mathrm{d}'}$.

Since Γ is normal in $\Gamma_0(2) = \Gamma_{\chi,1}$, the action of $T = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \in \Gamma_0(2)$ on $\mathbb{H}$ factors through X_{d} and defines an isomorphism $X_{\mathrm{d}} \to X_{\mathrm{d}}$, which we also denote by T. Using this, we can define translates of the diagonal

$$X_{\mathrm{d}}^{\Delta}(j) := (T^j \times \mathbb{1})^*(X_{\mathrm{d}}^{\Delta}) \subset X_{\mathrm{d}} \times X_{\mathrm{d}} \tag{4-4}$$

for $j \in \mathbb{Z}/\mathrm{d}\mathbb{Z}$. Equation (4-3) also generalizes to

$$(\pi \times \pi)^*(X_{\mathrm{d}}^{\Delta}(j)) = \sum_{\gamma \in \Gamma/\Gamma(2\mathrm{d}')} Z_{\Gamma(2\mathrm{d}')}\Big(\frac{1}{\mathrm{d}'}, \frac{1}{\mathrm{d}'} T^j \gamma + L\Big), \tag{4-5}$$

where one can replace $\Gamma(2\mathrm{d}')$ with $\Gamma_{\mathrm{d}'}$. From this, we see that the pull back of $X_{\mathrm{d}}^{\Delta}(j)$ along natural projection $X_{\mathrm{d}'} \times X_{\mathrm{d}'} \to X_{\mathrm{d}} \times X_{\mathrm{d}}$ is $\bigcup_{l \in \mathrm{d}\mathbb{Z}/\mathrm{d}'\mathbb{Z}} X_{\mathrm{d}'}^{\Delta}(j+l)$. Before proceeding further to state and prove the main result of this section, we record the following identity for convenience.

Lemma 4.3. *For any* $\mathrm{d} \in \mathbb{N}$, *we have the following identity in* $\mathbb{Q}(X)$

$$\mathrm{p}_{\mathrm{d}}(X) := \prod_{j \in \mathbb{Z}/\mathrm{d}\mathbb{Z}} (1 - \zeta_{\mathrm{d}}^j X)^{a_{\mathrm{d}}(j)} = \prod_{b \mid \mathrm{d}} (1 - X^{\mathrm{d}/b})^{b \cdot \mu(\mathrm{d}/b)}, \tag{4-6}$$

where $a_{\mathrm{d}}(j)$ *is the constant defined in* (3-12). *Furthermore for any* $s \in \mathbb{N}$, *we have*

$$\prod_{\mathrm{d} \mid s} \mathrm{p}_{\mathrm{d}}(X^{s/\mathrm{d}}) = (1 - X)^s. \tag{4-7}$$

Proof. To prove (4-6), it suffices to check that both sides have the same roots counting multiplicity, since they agree at $X = 0$. The multiplicity of $X = \zeta_{\mathrm{d}}^j$ on the left-hand side is $a_{\mathrm{d}}(-j) = a_{\mathrm{d}}(j)$, whereas it is $\sum_{b \mid (\mathrm{d}, j)} b \cdot \mu(\mathrm{d}/b)$ on the right-hand side. The equality is then a consequence of the identity

$$\sum_{b \mid n} b \cdot \mu\Big(\frac{\mathrm{d}}{b}\Big) = \mu(\mathrm{d}/n) \frac{\varphi(\mathrm{d})}{\varphi(\mathrm{d}/n)}, \quad n \mid \mathrm{d},$$

which is a standard exercise that we leave, along with (4-7), to the curious readers. □

Now, we can specialize Borcherds' far reaching lifting theorem [1998, Theorem 13.3] (see also [Yang and Yin 2019, Theorems 2.1 and 2.2]) to the modular function $\widetilde{F}_{\mathrm{d}}$ in (3-17) and the result below.

Theorem 4.4. *For every* $\mathrm{d} \mid 24$, *recall the modular function in* $M^!(\omega_{\mathrm{d}})^{H'_{\mathrm{d}}}$

$$\widetilde{F}_{\mathrm{d}}(\tau) = \sqrt{2}^{\mathrm{d}} (\mathfrak{f}_2^{-24/\mathrm{d}}(\tau)\mathfrak{u}_{\mathrm{d}} + \mathfrak{f}_1^{-24/\mathrm{d}}(\tau)\mathfrak{v}_{\mathrm{d}} + \mathfrak{f}^{-24/\mathrm{d}}(\tau)\mathfrak{w}_{\mathrm{d}}) + \begin{cases} 24(\mathfrak{e}_{(0,0)} + \mathfrak{e}_{(1/2,0)}) & \textit{if } \mathrm{d} = 1, \\ 0 & \textit{if } \mathrm{d} > 1, \end{cases}$$

defined in (3-17) *with* $\mathfrak{u}_{\mathrm{d}}, \mathfrak{v}_{\mathrm{d}}, \mathfrak{w}_{\mathrm{d}} \in U_{\mathrm{d}}$ *vectors defined in* (3-12) *and* (3-14). *Let* $\Psi_{\mathrm{d}}(z)$ *be the meromorphic modular function on* $X_{\mathrm{d}} \times X_{\mathrm{d}}$ (*with some characters*) *associated to* $\widetilde{F}_{\mathrm{d}}$ *via Borcherds multiplicative lifting, i.e.*, $-\log\|\Psi_{\mathrm{d}}(z)\|_{\mathrm{Pet}}^2$ *is the regularized theta lift of* $\widetilde{F}_{\mathrm{d}}$ *with* $\|\cdot\|_{\mathrm{Pet}}$ *a suitably normalized Petersson norm* (*see, e.g., Theorem 2.1 in* [*Yang and Yin 2019*]). *Then* $\Psi_{\mathrm{d}}(z)$ *has the following properties*:

(1) *On* $X_{\mathrm{d}} \times X_{\mathrm{d}}$,

$$\mathrm{Div}(\Psi_{\mathrm{d}}(z)) = \sum_{j \in \mathbb{Z}/\mathrm{d}\mathbb{Z}} a_{\mathrm{d}}(j) X_{\mathrm{d}}^{\Delta}(j).$$

(2) *When* $\mathrm{d} = 1$, $\Psi_{\mathrm{d}}(z)$ *has a product expansion of the form*

$$\Psi_1(z) = 2^{12}(q_1 - q_2) \prod_{m,n \geq 1} (1 - q_1^n q_2^m)^{c_1(mn)} (1 - q_1^{2n} q_2^{2m})^{c_{-1}(2mn)}$$

near the cusp $\mathbb{Q}\ell$ *of* X_K, *where* $q_j := e^{2\pi i z_j}$ *and* $c_{\mathrm{d}}(l)$ *are the Fourier coefficients defined in Remark 2.1.*

(3) *When* $\mathrm{d} > 1$, $\Psi_{\mathrm{d}}(z)$ *has a product expansion of the form*

$$\Psi_{\mathrm{d}}(z) = \prod_{b \mid \mathrm{d}} (q_1^{1/b} - q_2^{1/b})^{b \cdot \mu(\mathrm{d}/b)} \prod_{\substack{m,n \in \mathbb{N} \\ mn \equiv -1 \bmod \mathrm{d}}} \left(\prod_{b \mid \mathrm{d}} (1 - q_1^{n/b} q_2^{m/b})^{b \cdot \mu(\mathrm{d}/b)} \right)^{c_{\mathrm{d}}(mn)(-1)^{(n^2-1)/\mathrm{d}_2}}$$

near the cusp $\mathbb{Q}\ell$ *of* X_K, *where* μ *and* φ *are the Möbius and Euler* φ*-function respectively.*

Proof. This is a specialization of Borcherds' result to the input $\widetilde{F}_{\mathrm{d}} \in M^!(\omega_{\mathrm{d}})$. For this, we need to substitute the suitable parameters into Borcherds' result, which has been specialized to this case in Theorems 2.1 and 2.2 in [Yang and Yin 2019]. Using the specialization there, we see that the divisor of Ψ_{d} is

$$\sum_{j \in \mathbb{Z}/\mathrm{d}\mathbb{Z}} a_{\mathrm{d}}(j) \sum_{\mu \in \kappa(T^j N_{\mathrm{d}}')} Z_{\Gamma_{\mathrm{d}}}\Big(-\frac{1}{\mathrm{d}}, \mu\Big) = \sum_{j \in \mathbb{Z}/\mathrm{d}\mathbb{Z}} a_{\mathrm{d}}(j) \sum_{\gamma \in \Gamma/\Gamma(2\mathrm{d})} Z_{\Gamma(2\mathrm{d})}\Big(-\frac{1}{\mathrm{d}}, \frac{1}{\mathrm{d}} T^j \gamma + L\Big),$$

which gives us the first claim after applying Lemma 4.2.

For the second and third claim, we specialize Theorem 2.2 in [Yang and Yin 2019] and use the notations there. When $\mathrm{d} = 1$, this is rather classical and can be found in [Scheithauer 2008] (see also Proposition 5.3 in [Yang and Yin 2019]).[2] For $\mathrm{d} > 1$, the Weyl chambers for $\widetilde{F}_{\mathrm{d}}$ are the same as in the case $\mathrm{d} = 1$, and we choose the one $W = \mathbb{R}\big\{\big(\begin{smallmatrix} a & \\ & -1 \end{smallmatrix}\big) : a > 1\big\}$. Since $\mathfrak{u}_{\mathrm{d}}$, $\mathfrak{v}_{\mathrm{d}}$ and $\mathfrak{w}_{\mathrm{d}}$ do not have support on any isotropic vector, the associated form $\widetilde{F}_{\mathrm{d},P}$ is identically zero, and the Weyl vector $\rho(W, \widetilde{F}_{\mathrm{d}})$ is 0. Since $\widetilde{F}_{\mathrm{d}}$ does not have any constant term, the constant C in the product expansion is 1, For the infinite product, suppose $\lambda = \frac{1}{\mathrm{d}}\big(\begin{smallmatrix} -m & \\ & n \end{smallmatrix}\big)$ with $m, n \in \mathbb{Z}$. Then $(\lambda, W) > 0$ if and only if $m \geq -n$, $n \geq 0$ and $(m, n) \neq (0, 0)$.

The set of $\mu \in L_0'/L$ with $p(\mu) = \lambda$ consists then of $\frac{1}{\mathrm{d}}\big(\begin{smallmatrix} -m & -j \\ 0 & n \end{smallmatrix}\big)$ with $j \in \frac{1}{2}\mathbb{Z}/\mathrm{d}\mathbb{Z}$. For such λ, μ, we have

$$1 - e((\lambda, z) + (\mu, \ell')) = 1 - \zeta_{\mathrm{d}}^j q_1^{n/\mathrm{d}} q_2^{m/\mathrm{d}}.$$

By inspecting the q-expansion of F_{d}, we notice that

$$F_{\mathrm{d}}(\tau) = \Bigg(q^{-1/\mathrm{d}} + \sum_{l \in \mathbb{N}, l \equiv -1 \bmod \mathrm{d}} c_{\mathrm{d}}(l) q^{l/\mathrm{d}} \Bigg) \mathfrak{u}_{\mathrm{d}} + \sum_{\mu \in L'/L,\, Q_{\mathrm{d}}(\mu) \in \left\{ \frac{1}{2\mathrm{d}}, \frac{1}{2\mathrm{d}} + \frac{1}{2} \right\}} F_{\mathrm{d},\mu}(\tau) \mathfrak{e}_{\mu}.$$

[2] Note that the Fourier expansion of f in [loc. cit.] is incorrect.

Therefore, the only pairs of (m, n) with $m < 0$ is $m = -n = -1$, and the only $\mu \in L_0'/L$ where $F_{\mathrm{d},\mu}$ could be nonzero are contained in the support of $\mathfrak{u}_{\mathrm{d}}$, hence

$$\mu = \frac{1}{\mathrm{d}}\begin{pmatrix} -m & j \\ 0 & n \end{pmatrix} + L \in \frac{1}{\mathrm{d}} T^{j'} \Gamma_{\chi,\mathrm{d}} + L$$

with $mn \equiv -1 \mod \mathrm{d}$ and $j' := nj - \frac{1}{2}(n^2-1) \in \mathbb{Z}/\mathrm{d}\mathbb{Z}$ by Lemma 3.1. The Fourier coefficient $c(-Q(\lambda), \mu)$ of the input is then $c_{\mathrm{d}}(mn)a_{\mathrm{d}}(j')$. It is easy to check that $a_{\mathrm{d}}(j') = a_{\mathrm{d}}(j)(-1)^{(n^2-1)/\mathrm{d}_2}$. By Theorem 2.2 in [Yang and Yin 2019], $\Psi_{\mathrm{d}}(z)$ has the product expansion

$$\Psi_{\mathrm{d}}(z) = \prod_{\substack{m \in \mathbb{Z}_{\geq -1}, n \in \mathbb{N} \\ mn \equiv -1 \bmod \mathrm{d}}} \prod_{j \in \mathbb{Z}/\mathrm{d}\mathbb{Z}} (1 - \zeta_{\mathrm{d}}^{j} q_1^{n/\mathrm{d}} q_2^{m/\mathrm{d}})^{c_{\mathrm{d}}(mn)a_{\mathrm{d}}(j)(-1)^{(n^2-1)/8}}$$

Finally, applying Lemma 4.3 finishes the proof. □

4B. ***The Weber function differences as Borcherds liftings.*** Now, we are ready to state and prove the following main result of this section.

Theorem 4.5. *For* $\mathrm{d} \mid 24$, *let* $\Psi_{\mathrm{d}}(z_1, z_2)$ *be the Borcherds product of* $\widetilde{F}_{\mathrm{d}} \in M^!(\omega_{\mathrm{d}})$ *as in Theorem 4.4. Then for any* $s \mid 24$ *and* $\varepsilon \in \{\pm 1\}$, *we have*

$$(\mathfrak{f}_2(z_1)^{24/s} - (\varepsilon \mathfrak{f}_2(z_2))^{24/s})^s = \prod_{\mathrm{d} \mid s} \Psi_{\mathrm{d}}(z_1, z_2)^{\varepsilon^{24/\mathrm{d}}}. \tag{4-8}$$

Proof. We first look at their divisors in the open Shimura varieties $X_s \times X_s$. Suppose $\varepsilon = 1$. The left-hand side clearly has $s \cdot [X_s^{\Delta}]$ as its divisor, whereas the right-hand side has the divisor

$$\sum_{\mathrm{d} \mid s} \sum_{j \in \mathbb{Z}/\mathrm{d}\mathbb{Z}} a_{\mathrm{d}}(j) \sum_{l \in \mathrm{d}\mathbb{Z}/s\mathbb{Z}} [X_s^{\Delta}(j + l)] = \sum_{k \in \mathbb{Z}/s\mathbb{Z}} \left(\sum_{\mathrm{d} \mid s} a_{\mathrm{d}}(k) \right) [X_s^{\Delta}(k)] = s \cdot [X_s^{\Delta}],$$

as

$$\sum_{\mathrm{d} \mid s} a_{\mathrm{d}}(k) = \sum_{\mathrm{d} \mid s} \mu(\mathrm{d}/(\mathrm{d}, k)) \varphi(\mathrm{d})/\varphi(\mathrm{d}/(\mathrm{d}, k)) = \begin{cases} s & \text{if } k = 0, \\ 0 & \text{otherwise.} \end{cases}$$

When $\varepsilon = -1$, the argument is the same unless $8 \mid s$. In that case, the divisor of the left-hand side is $s \cdot [X_s^{\Delta}(s/2)]$, whereas the divisor of the right-hand side is

$$\mathrm{Div} \prod_{\mathrm{d} \mid s/2} \Psi_{\mathrm{d}}(z_1, z_2)^2 - \mathrm{Div} \prod_{\mathrm{d} \mid s} \Psi_{\mathrm{d}}(z_1, z_2) = s \cdot ([X_s^{\Delta}] + [X_s^{\Delta}(s/2)]) - s \cdot [X_s^{\Delta}] = s \cdot [X_s^{\Delta}(s/2)].$$

Now let

$$g(z_1, z_2) = \frac{\prod_{\mathrm{d} \mid s} \varepsilon^{24/(\mathrm{d},s)} \Psi_{\mathrm{d}}(z_1, z_2)^2}{(\mathfrak{f}_2(z_1)^{24/s} - (\varepsilon \mathfrak{f}_2(z_2))^{24/s})^s}.$$

Then it is holomorphic and has no zeros on $X_s \times X_s$. So

$$\mathrm{Div}(g(z_1, z_2)) = a_{\infty,1}(\{\infty\} \times X_s) + a_{\infty,2}(X_s \times \{\infty\}) + a_{0,1}(\{0\} \times X_s) + a_{0,2}(X_s \times \{0\})$$

is supported on the boundary with $a_{i,j} \in \mathbb{Z}$. The product expansion of Ψ_d and the definition of $\mathfrak{f}_2$ imply that $a_{\infty,1} = a_{\infty,2} = 0$.

Next, fix $z_2 \in X_s$ the above argument shows that $g(z_1, z_2)$, as a function of z_1 on $X_s \cup \{0, \infty\}$ has only zeros or poles at the cusp $\{0\}$, which is impossible. So $g(z_1, z_2)$ has no zeros or poles in z_1, and is therefore independent of z_1, i.e, $g(z_1, z_2) = g(z_2)$ is purely a function of z_2 with no zeros or poles in $X_s \cup \{\infty\}$. This implies that $g(z_1, z_2) = g(z_2) = C$ is a constant.

Finally, looking at the q_1-leading term of the Fourier expansion, we see $C = 1$ and this proves the theorem. The last part of the proof follows from the argument in the proof of [Yang and Yin 2019, Theorem 3.4]. □

5. Big CM values

5A. ***Products of CM cycles as big CM cycles.*** Yang and Yin [2019, Section 3.2] have described how to view a pair of CM points as a big CM point, which we now briefly review for convenience and set up necessary notation. We modify a little for use in this paper. For $j = 1, 2$, let $d_j < 0$ be co-prime, fundamental discriminants satisfying (1-3). Denote $E_j = \mathbb{Q}(\sqrt{d_j})$ with ring of integers $\mathcal{O}_j = \mathbb{Z}\big[\frac{1}{2}(1 + \sqrt{d_j})\big]$, and class group $\mathrm{Cl}(d_j)$. Let $E = E_1 \otimes_{\mathbb{Q}} E_2 = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ with ring of integers $\mathcal{O}_E = \mathcal{O}_1 \otimes_{\mathbb{Z}} \mathcal{O}_2$. Then E is a biquadratic CM number field with real quadratic subfield $F = \mathbb{Q}(\sqrt{D})$ and $D = d_1 d_2$.

For a positive integer d, we define $W = W_{\mathrm{d}} = E$ with the F-quadratic form $Q_F(x) = \mathrm{d}x\bar{x}/\sqrt{D}$. Let $W_{\mathbb{Q}} = W$ with the $\mathbb{Q}$-quadratic form $Q_{\mathbb{Q}}(x) = \mathrm{Tr}_{F/\mathbb{Q}}\, Q_F(x)$. Let σ_1 and σ_2 be two real embeddings of F with $\sigma_j(\sqrt{D}) = (-1)^{j-1}\sqrt{D}$. Then W has signature $(0, 2)$ at σ_2 and $(2, 0)$ at σ_1 respectively, and so $W_{\mathbb{Q}}$ has signature $(2, 2)$. Choose a $\mathbb{Z}$-basis of $\mathcal{O}_E$ as follows

$$e_1 = 1 \otimes 1, \quad e_2 = \frac{-1+\sqrt{d_1}}{2} = \frac{-1+\sqrt{d_1}}{2} \otimes 1, \quad e_3 = \frac{1+\sqrt{d_2}}{2} = 1 \otimes \frac{1+\sqrt{d_2}}{2}, \quad e_4 = e_2 e_3.$$

We will drop $\otimes$ when there is no confusion. Then it is easy to check that

$$(W_{\mathbb{Q}}, Q_{\mathbb{Q}}) \cong (V, Q) = (M_2(\mathbb{Q}), \mathrm{d}\det), \qquad \sum x_i e_i \mapsto \begin{pmatrix} x_3 & x_1 \\ x_4 & x_2 \end{pmatrix}. \tag{5-1}$$

We will identify $(W_{\mathbb{Q}}, Q_{\mathbb{Q}})$ with the quadratic space $(V, Q) = (M_2(\mathbb{Q}), \mathrm{d}\det)$. Under this identification, the lattice $M_2(\mathbb{Z})$ becomes $\mathcal{O}_E$, and the lattice L_{d} becomes $\mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 + \mathbb{Z}2e_4 \subset \mathcal{O}_E$, which we still denote by $L = L_{\mathrm{d}}$. Define T to be the maximal torus in H given by the following diagram:

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[d] & T \arrow[r] \arrow[d] & \mathrm{Res}_{F/\mathbb{Q}}\, \mathrm{SO}(W) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbb{G}_m \arrow[r] & H \arrow[r] & \mathrm{SO}(V) \arrow[r] & 1
\end{tikzcd} \tag{5-2}$$

Then T can be identified with ([Howard and Yang 2012; Bruinier et al. 2012, Section 6])

$$T(R) = \{(t_1, t_2) \in (E_1 \otimes_{\mathbb{Q}} R)^\times \times (E_2 \otimes_{\mathbb{Q}} R)^\times : t_1\bar{t_1} = t_2\bar{t_2}\},$$

for any $\mathbb{Q}$-algebra R, and the map from T to $\mathrm{SO}(W)$ is given by $(t_1, t_2) \mapsto t_1/\bar{t_2}$. The map from T to H is explicitly given as follows. Define the embeddings $\iota_j : E_j \to M_2(\mathbb{Q})$ by

$$(e_1, e_2)\iota_1(r) = (re_1, re_2), \quad \iota_2(r)(e_3, e_1)^t = (\bar{r}e_3, \bar{r}e_1)^t. \tag{5-3}$$

Then $\iota = (\iota_1, \iota_2)$ gives the embedding from T to H. If $r_j = \alpha_j e_1 + (-1)^{j+1}\beta_j e_{j+1} \in E_j$, then

$$\iota_j(r_j) = \alpha_j \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \beta_j \begin{pmatrix} 0 & \frac{1}{4}(d_j - 1) \\ 1 & -1 \end{pmatrix}. \tag{5-4}$$

Extend the two real embeddings of F into a CM type $\Sigma = \{\sigma_1, \sigma_2\}$ of E via

$$\sigma_1(\sqrt{d_i}) = \sqrt{d_i} \in \mathbb{H}, \quad \sigma_2(\sqrt{d_1}) = \sqrt{d_1}, \quad \sigma_2(\sqrt{d_2}) = -\sqrt{d_2}.$$

Since $W_{\sigma_2} = W \otimes_{F,\sigma_2} \mathbb{R} \subset V_{\mathbb{R}}$ has signature $(0, 2)$, it gives two points $z_{\sigma_2}^{\pm}$ in $\mathbb{D}$. In this case, the big CM cycles associated to T as defined in [Bruinier et al. 2012; Yang and Yin 2019] are given by

$$Z(W, z_{\sigma_2}^{\pm}) = \{z_{\sigma_2}^{\pm}\} \times T(\mathbb{Q})\backslash T(\mathbb{A}_f)/K_T \in Z^2(X_K), \tag{5-5}$$

and

$$Z(W) = Z(W, z_{\sigma_2}^{\pm}) + \sigma_2(Z(W, z_{\sigma_2}^{\pm})). \tag{5-6}$$

For simplicity, we will denote z_{σ_2} for $z_{\sigma_2}^{+}$. The same calculation as in the proof of [Yang and Yin 2019, Lemma 3.4] gives the following result.

Lemma 5.1. *On $\mathbb{H}^2 \cup (\mathbb{H}^-)^2$, one has $z_{\sigma_2} = (\tau_1, \tau_2) \in \mathbb{H}^2$ and $z_{\sigma_2}^- = (\bar{\tau}_1, \bar{\tau}_2) \in (\mathbb{H}^-)^2$, where*

$$\tau_j = \frac{1+\sqrt{d_j}}{2}.$$

For $\mathrm{d} \mid 24$, let $K_{\mathrm{d}} \subset H(\mathbb{A}_f)$ be the compact open subgroup generated by (T, T), $(\Gamma_{\chi,\mathrm{d}} \times \Gamma_{\chi,\mathrm{d}}) \otimes \hat{\mathbb{Z}} \subset H(\mathbb{A}_f)$ and $(\nu(\hat{\mathbb{Z}}^\times) \times \nu(\hat{\mathbb{Z}}^\times)) \cap H(\mathbb{A}_f)$. By the choice of $\Gamma_{\chi,\mathrm{d}}$, we actually have the following result.

Lemma 5.2. *Suppose $d_j < 0$ are discriminants satisfying* (1-3) *for $j = 1, 2$. Then for any* $\mathrm{d} \mid 24$, *the preimage $\iota^{-1}(K_{\mathrm{d}})$ is independent of* $\mathrm{d} \mid 24$.

Remark 5.3. We will simply denote $\iota^{-1}(K_{\mathrm{d}})$ by K_T.

Remark 5.4. The lemma does not require d_j to be fundamental or co-prime.

Proof. Since $K_{24} \subset K_{\mathrm{d}} \subset K_1$ for any $\mathrm{d} \mid 24$, it suffices to check that $\iota^{-1}(K_1) = \iota^{-1}(K_{24})$. Furthermore, we know that $\Gamma(48) \subset \Gamma_{\chi,24} \subset \Gamma_{\chi,1} = \Gamma_0(2)$, so we only need to check the equality when tensoring with $\mathbb{Z}/3\mathbb{Z}$ and with $\mathbb{Z}/16\mathbb{Z}$. This then boils down to a short calculation with finite groups.

To check the case modulo 3, it suffices to show that $\iota(\iota^{-1}(K_1)\otimes\mathbb{Z}/3\mathbb{Z})\subset K_{24}\subset \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})\times\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. Since $\Gamma_{\chi,1}\otimes\mathbb{Z}/3=\Gamma_0(2)\otimes\mathbb{Z}/3=\mathrm{SL}_2(\mathbb{Z}_3)$, we have $\iota^{-1}(K_1)\otimes\mathbb{Z}/3=\iota^{-1}(H(\mathbb{Z}/3\mathbb{Z}))$. Thus (5-4) implies

$$\iota(\iota^{-1}(K_1)\otimes\mathbb{Z}/3)=\left\{\left(\begin{pmatrix}\alpha_j & \beta_j(d_j-1)/4\\ \beta_j & \alpha_j-\beta_j\end{pmatrix}\right)_{j=1,2}\in H(\mathbb{Z}/3\mathbb{Z}):\alpha_j,\beta_j\in\mathbb{Z}/3\mathbb{Z},\right\}$$

and we need to show that this is contained in

$$\begin{aligned}K_{24}\otimes\mathbb{Z}/3\mathbb{Z}&=\langle\Gamma_{\chi,24}\times\Gamma_{\chi,24},(T,T),\nu(\hat{\mathbb{Z}}^\times)\times\nu(\hat{\mathbb{Z}}^\times)\rangle\otimes\mathbb{Z}/3\mathbb{Z}\\&=\langle\Gamma_{\chi,3}\times\Gamma_{\chi,3},(T,T),\nu(\hat{\mathbb{Z}}^\times)\times\nu(\hat{\mathbb{Z}}^\times)\rangle\otimes\mathbb{Z}/3\mathbb{Z}\\&=\left\langle N'_{\mathrm{d},3}\times N'_{\mathrm{d},3},(T,T),\left(\left(\begin{smallmatrix}1&\\&-1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&\\&-1\end{smallmatrix}\right)\right)\right\rangle\subset H(\mathbb{Z}/3\mathbb{Z}).\end{aligned}$$

Now given $r=(r_1,r_2)\in\iota^{-1}(K_1)\otimes\mathbb{Z}/3\mathbb{Z}$ with $\iota_j(r_j)=\left(\begin{smallmatrix}\alpha_j&\beta_j(d_j-1)/4\\ \beta_j&\alpha_j-\beta_j\end{smallmatrix}\right)$, we know that

$$\delta:=\det(\iota_j(r_j))=\mathrm{Tr}(\iota_j(r_j))^2-\beta_j^2d_j\in(\mathbb{Z}/3\mathbb{Z})^\times \tag{5-7}$$

is independent of j. If $\beta_j=0$, then $\iota_j(r_j)=\pm\left(\begin{smallmatrix}1&\\&1\end{smallmatrix}\right)\in N'_{\mathrm{d},3}$ and $\iota(r)\in K_{24}\otimes\mathbb{Z}/3\mathbb{Z}$. If $\beta_1=0$ and $\beta_2\neq0$, then $\iota_1(r_1)\in N'_{\mathrm{d},3}$ and $\delta=1$, which implies $\mathrm{Tr}(\iota_2(r_2))=0$ by (5-7). That means $\iota_2(r_2)\in N'_{\mathrm{d},3}$ by (3-20). Finally suppose $\beta_j\neq0$, then we can use $3\nmid d_j$ to show that $\epsilon:=\alpha_j\beta_j(\delta+1)$ is independent of j. It is then straightforward to check that $T^{1-\epsilon}\left(\begin{smallmatrix}1&\\&\delta\end{smallmatrix}\right)\iota_j(r_j)\in N'_{\mathrm{d},3}$. Therefore $\iota(r)\in K_{24}\otimes\mathbb{Z}/3\mathbb{Z}$.

To check the case modulo 16, suppose

$$r=(r_1,r_2)\in\iota^{-1}(K_1)\otimes\mathbb{Z}/16\mathbb{Z}$$

with $r_j=\alpha_je_1+(-1)^{j+1}\beta_je_{j+1}$, $\alpha_j,\beta_j\in\mathbb{Z}/16\mathbb{Z}$. Then simple calculation shows that $\alpha_j-1,\beta_j\in2\mathbb{Z}/16\mathbb{Z}$. Furthermore, $\det(\iota_j(r_j))=\alpha_j(\alpha_j-\beta_j)-\beta_j^2(d_j-1)/4\in(\mathbb{Z}/16\mathbb{Z})^\times$ is independent of j since $\iota(r)\in H(\mathbb{A}_f)$, and $\beta_j^2(d_j-1)/4\equiv0 \bmod 8$ since $d_j\equiv1 \bmod 8$ and $\beta_j\in2\mathbb{Z}/16\mathbb{Z}$. Therefore,

$$\det(\iota_j(r_j))^{-1}=\alpha_j^{-1}(\alpha_j-\beta_j)^{-1}+\beta_j^2(d_j-1)/4.$$

Now $r\in\iota^{-1}(K_{24})$ if and only if $\iota(r)\in K_{24}\otimes\mathbb{Z}/16\mathbb{Z}$, which is generated by $\nu((\mathbb{Z}/16\mathbb{Z})^\times)\times\nu((\mathbb{Z}/16\mathbb{Z})^\times)$, $(T,T)\otimes\mathbb{Z}/16\mathbb{Z}$ and $(\Gamma_{\chi,24}\times\Gamma_{\chi,24})\otimes\mathbb{Z}/16\mathbb{Z}\cong(\Gamma_{\chi,8}/\Gamma(16)\times\Gamma_{\chi,8}/\Gamma(16))$. From the natural surjection $\Gamma_{\chi,8}/\Gamma(16)\to\Gamma_{\chi,8}/\Gamma_8=N'_8=N'_{8,2}$, we see that the following claim will finish the proof: the element

$$g_j:=\nu(\det(\iota_j(r_j)))^{-1}T^{\det(\iota_j(r_j)-1)/2}\iota_j(r_j)$$

is in $N'_8=N'_{8,2}$ for all $r_j=\alpha_je_j+(-1)^{j+1}\beta_je_{j+1}$ with $\alpha_j-1,\beta_j\in2\mathbb{Z}/16\mathbb{Z}$. By dropping the subscript j in d_j,g_j,α_j and β_j, we can write

$$g=\alpha\begin{pmatrix}1&\frac{\alpha(\alpha-\beta)-1-\beta^2(d-1)/4}{2}\\0&\alpha^{-1}(\alpha-\beta)^{-1}+\frac{\beta^2(d-1)}{4}\end{pmatrix}+\beta\begin{pmatrix}\frac{\alpha(\alpha-\beta)-1-\beta^2(d-1)/4}{2}&\frac{d-1}{4}-\frac{\alpha(\alpha-\beta)-1-\beta^2(d-1)/4}{2}\\ \alpha^{-1}(\alpha-\beta)^{-1}&-\alpha^{-1}(\alpha-\beta)^{-1}\end{pmatrix},$$

which is an element in $N_8 = N_{8,2}$. Denote $h = [h_0, h_1, h_2, h_3] := \kappa_{8,2}(g) \in \mathcal{A}_{8,2}$. To show that $g \in N'_8 = N'_{8,2}$, it suffices check that $h \in \mathcal{A}'_{8,2}$, i.e.,

$$h \perp [6, 4, 0, 2], \quad h \perp [0, 2, 2, 0]$$

and $h_0^2 - 1 \equiv h_1 + h_2 \mod 16$ by Lemma 3.11. All of these can be checked by hand (assuming $d \equiv 1 \mod 8$ and $\alpha - 1 \equiv \beta \equiv 0 \mod 2$), and we leave the details to the reader. □

By [Yang and Yin 2019, Lemma 3.5], the map

$$p : T(\mathbb{Q})\backslash T(\mathbb{A}_f)/K_T \to \mathrm{Cl}(d_1) \times \mathrm{Cl}(d_2), \quad [t_1, t_2] \mapsto ([t_1], [t_2]) = ([\mathfrak{a}_1], [\mathfrak{a}_2]) \tag{5-8}$$

is injective. Here $\mathfrak{a}_j$ is the ideal of E_j associated to t_j. If d_1, d_2 are co-prime, then [Yang and Yin 2019, Lemma 3.8] tells us that it is an isomorphism. If $d_1 d_2$ is not a perfect square, this subgroup can be identified with $\mathrm{Gal}(H/E)$ with H the composite of the ring class fields H_{d_j} associated to the order of discriminant d_j (see Proposition 3.2 in [Li 2018]). This observation and the above lemma give the following corollary.

Proposition 5.5. *Let $d_j < 0$ be co-prime, fundamental discriminants satisfying* (1-3). *For $[\mathfrak{a}_j] \in \mathrm{Cl}(d_j)$, recall the class invariant $f(\mathfrak{a}_j)$ defined in* (1-4). *Then for any $s \mid 24$*

$$4s \sum_{[\mathfrak{a}_j] \in \mathrm{Cl}(d_j),\, j=1,2} \log |f(\mathfrak{a}_1)^{24/s} - f(\mathfrak{a}_2)^{24/s}| = \sum_{\mathrm{d} \mid s} \varepsilon^{24/\mathrm{d}} \log |\Psi_{\mathrm{d}}(Z(W))|, \tag{5-9}$$

where $\varepsilon := \varepsilon_{d_1}\varepsilon_{d_2} = (-1)^{(d_1+d_2-2)/8}$ and $Z(W)$ is the big CM cycle defined in (5-6).

Proof. We may assume $s = 24$ for simplicity, as the other cases are the same. By applying Shimura's reciprocity law, Proposition 22 in [Gee 1999] showed that class invariants $f(\mathfrak{a}_j)$ for $[\mathfrak{a}_j] \in \mathrm{Cl}(d_j)$ are conjugates of each other under the Galois group. In particular, [loc. cit., (18)] implies

$$f(\mathfrak{a}_j) = \varepsilon_{d_j}(\zeta_{48}^{-1}\mathfrak{f}_2(\tau_j))^{\sigma_{t_j}} = \varepsilon_{d_j}\zeta_{48}^{-\sigma_{t_j}}\mathfrak{f}_2^{\sigma_{t_j}}(\tau_j^{\sigma_{t_j}}) = \varepsilon_{d_j}\zeta_{48}^{-t_j\bar{t}_j}\delta(t_j)\mathfrak{f}_2(\tau_j^{\sigma_{t_j}})$$

where the class $t_j \in (E_j \otimes \mathbb{A}_f)^\times$ in $\mathrm{Cl}(d_j)$ is $[\mathfrak{a}_j]$. Here $t_j\bar{t}_j$ can be understood to be an integer modulo 48, and

$$\delta(t_j) = \frac{(\sqrt{2})^{\sigma_{t_j\bar{t}_j}}}{\sqrt{2}}$$

is an 8-th root of unit depending only on $t_j\bar{t}_j$ mod 8, coming from the Fourier coefficients of $\mathfrak{f}_2$. Note that $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$. Thus for $t = (t_1, t_2) \in T(\mathbb{A}_f)$, we have $t_1\bar{t}_1 = t_2\bar{t}_2$ and

$$\log |f(\mathfrak{a}_1) - f(\mathfrak{a}_2)| = \log |(\zeta_{48}^{-1}\mathfrak{f}_2(\tau_1))^{\sigma_{t_1}} - \varepsilon(\zeta_{48}^{-1}\mathfrak{f}_2(\tau_2))^{\sigma_{t_2}}| = \log |\mathfrak{f}_2(\tau_1^{\sigma_{t_1}}) - \varepsilon\mathfrak{f}_2(\tau_2^{\sigma_{t_2}})|,$$

which depends only on the image $p(t) = ([\mathfrak{a}_1], [\mathfrak{a}_2]) \in \mathrm{Cl}(d_1) \times \mathrm{Cl}(d_2)$. So by the isomorphism (5-8),

$$\sum_{[\mathfrak{a}_j]\in \mathrm{Cl}(d_j),\, j=1,2} \log |f(\mathfrak{a}_1) - f(\mathfrak{a}_2)| = \sum_{t\in T(\mathbb{Q})\backslash T(\mathbb{A}_f)/K_T} \log |\mathfrak{f}_2(\tau_1^{\sigma_{t_1}}) - \varepsilon \mathfrak{f}_2(\tau_2^{\sigma_{t_2}})|$$

$$= \sum_{(z,t)\in Z(W,\sigma_2^+)} \log |\mathfrak{f}_2(z_1) - \varepsilon \mathfrak{f}_2(z_2)|_{(z_1 z_2)=[(z,t)]}.$$

As the other three orbits are Galois conjugates of $Z(W, \sigma_2^+)$, the sums over the other orbits are the same as this one. Now the desired identity follows from Theorem 4.5. □

6. Incoherent Eisenstein Series and the proof of the Yui–Zagier conjecture

In this section, we will use the big CM value formula of Bruinier, Kudla and Yang [Bruinier et al. 2012] (see also [Yang and Yin 2019, Theorem 2.6]) to prove the factorization formula for $\Psi_{\mathrm{d}}(Z(W))$ and the Yui–Zagier conjecture. To do so, we need to review the associated incoherent Eisenstein series and compute their Fourier coefficients.

6A. ***Incoherent Eisenstein series.*** Let $F = \mathbb{Q}(\sqrt{D})$, $E = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, and $W = E$ with F-quadratic form $Q_F(x) = \mathrm{d}x\bar{x}/\sqrt{D}$ as in Section 5. Here $D = d_1 d_2$. Let $\chi_{E/F}$ be the quadratic Hecke character of F associated to E/F. Then there is a $\mathrm{SL}_2(\mathbb{A}_F)$-equivariant map

$$\lambda = \prod \lambda_v : S(W(\mathbb{A}_F)) \to I(0, \chi_{E/F}), \quad \lambda(\phi)(g) = \omega(g)\phi(0). \tag{6-1}$$

Here $I(s, \chi_{E/F}) = \mathrm{Ind}_{B_{\mathbb{A}_F}}^{\mathrm{SL}_2(\mathbb{A}_F)} \chi_{E/F}| \cdot |^s$ is the principal series, whose sections (elements) are smooth functions Φ on $\mathrm{SL}_2(\mathbb{A}_F)$ satisfying the condition

$$\Phi(n(b)m(a)g, s) = \chi(a)|a|^{s+1}\Phi(g, s), \quad b \in \mathbb{A}_F,\ a \in \mathbb{A}_F^\times.$$

Here $B = NM$ is the standard Borel subgroup of SL_2. Such a section is called factorizable if $\Phi = \bigotimes \Phi_v$ with $\Phi_v \in I(s, \chi_v)$. It is called standard if $\Phi|_{\mathrm{SL}_2(\widehat{\mathcal{O}}_F)\mathrm{SO}_2(\mathbb{R})^2}$ is independent of s. For a standard section $\Phi \in I(s, \chi)$, its associated Eisenstein series is defined as

$$E(g, s, \Phi) = \sum_{\gamma\in B_F\backslash \mathrm{SL}_2(F)} \Phi(\gamma g, s)$$

for $\Re(s) \gg 0$.

For $\phi \in S(V_f) = S(W_f)$, let Φ_f be the standard section associated to $\lambda_f(\phi) \in I(0, \chi_f)$. For each real embedding $\sigma_i : F \hookrightarrow \mathbb{R}$, let $\Phi_{\sigma_i} \in I(s, \chi_{\mathbb{C}/\mathbb{R}}) = I(s, \chi_{E_{\sigma_i}/F_{\sigma_i}})$ be the unique “weight one” eigenvector of $\mathrm{SL}_2(\mathbb{R})$ given by

$$\Phi_{\sigma_i}(n(b)m(a)k_\theta) = \chi_{\mathbb{C}/\mathbb{R}}(a)|a|^{s+1}e^{i\theta},$$

for $b \in \mathbb{R}$, $a \in \mathbb{R}^\times$, and $k_\theta = \left(\begin{smallmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{smallmatrix}\right) \in \mathrm{SO}_2(\mathbb{R})$. We define for $\vec{\tau} = (\tau_1, \tau_2) \in \mathbb{H}^2$

$$E(\vec{\tau}, s, \phi) = \mathrm{N}(\vec{v})^{-1/2} E\Big(g_{\vec{\tau}}, s, \Phi_f \otimes \Big(\bigotimes_{1\le i\le 2} \Phi_{\sigma_i}\Big)\Big),$$

where $\vec{v}=\mathrm{Im}(\vec{\tau})$, $\mathrm{N}(\vec{v})=\prod_i v_i$, and $g_{\vec{\tau}}=(n(u_i)m(\sqrt{v_i}))_{1\le i\le 2}$. It is a (nonholomorphic) Hilbert modular form of parallel weight 1 for some congruence subgroup of $\mathrm{SL}_2(\mathcal{O}_F)$. Following [Bruinier et al. 2012], we further normalize

$$E^*(\vec{\tau},s,\phi)=\Lambda(s+1,\chi_{E/F})E(\vec{\tau},s,\phi),$$

where

$$\Lambda(s,\chi)=D^{s/2}\bigl(\pi^{-(s+1)/2}\Gamma\bigl(\tfrac{1}{2}(s+1)\bigr)\bigr)^2L(s,\chi_{E/F}). \tag{6-2}$$

According to [Yang and Yin 2019], this Eisenstein series is incoherent in the sense of Kudla, and $E^*(\vec{\tau},0,\phi)=0$ automatically. Write its central derivative via Fourier expansion

$$E^{*,\prime}(\vec{\tau},0,\phi)=\sum_{t\in F}a(\vec{v},t,\phi)q^t,\quad q^t=\mathbf{e}(\mathrm{Tr}(t\tau)), \tag{6-3}$$

with $\vec{v}$ the imaginary part of $\vec{\tau}\in\mathbb{H}^2$. Then it is known that $a(t,\phi)=a(\vec{v},t,\phi)$ is independent of $\vec{v}$ when t is totally positive. Finally, when $\phi=\bigotimes_{\mathfrak{p}}\phi_{\mathfrak{p}}\in S(V_f)$ is factorizable, one has for $t\gg 0$ (the factor -4 comes from [Yang and Yin 2019, Proposition 2.7(1)(2)])

$$a(t,\phi)=-4\frac{d}{ds}\biggl(\prod_{\mathfrak{p}}W_{t,\mathfrak{p}}(s,\phi)\biggr)\biggr|_{s=0} \tag{6-4}$$

where

$$W_{t,\mathfrak{p}}(s,\phi):=\int_{F_{\mathfrak{p}}}\omega(wn(b))(\phi_{\mathfrak{p}})(0)|a(wn(b))|_{\mathfrak{p}}^s\psi_{\mathfrak{p}}(-tb)\,db \tag{6-5}$$

are the local Whittaker functions. Specializing Theorem 5.2 in [Bruinier et al. 2012] gives us the following result.

Theorem 6.1 (Bruinier–Kudla–Yang). *Let $d_j<0$ be fundamental discriminants satisfying $d_j\equiv 1 \bmod 8$ and $3\nmid d_j$. For any $1\neq \mathrm{d}\mid 24$, let $\phi_{\mathrm{d}}\in S(V_{\mathrm{d}}(\mathbb{A}_f)$ be associated to $\mathfrak{u}_{\mathrm{d}}$. Then we have*

$$-\log|\Psi_{\mathrm{d}}(Z(W))|^4=C(W,K)\sum_{t\in F^\times,t\gg 0,\mathrm{Tr}(t)=1/\mathrm{d}}a(t,\phi_{\mathrm{d}}), \tag{6-6}$$

where $Z(W)$ is the big CM 0-cycle associated to d_1,d_2 defined in (5-6), *and*

$$C(W,K)=\frac{\deg(Z(W,z_{\sigma_2}^{\pm}))}{\Lambda(0,\chi)}=2.$$

The rest of this section is to compute $a(t,\phi_{\mathrm{d}})$ and prove the Yui–Zagier conjecture. Unfortunately, ϕ_{d} is not factorizable over F at the places dividing $(\mathrm{d},6)$. Instead, we have

$$\phi_{\mathrm{d}}=\phi_{\mathrm{d},2}\phi_{\mathrm{d},3}\otimes_{\mathfrak{p}\nmid 6}\phi_{\mathrm{d},\mathfrak{p}}.$$

Then for $\mathfrak{p}\nmid 6$, the contribution of $W_{t,\mathfrak{p}}(s,\phi_{\mathrm{d}})$ is the same as in the case of Gross-Zagier (see [Yang and Yin 2019]). Therefore, we are left with the local calculations at 2 and 3. Since 2 splits completely in $E/\mathbb{Q}$, we denote $\mathfrak{p}_1,\mathfrak{p}_2$ the two primes in F above 2. Also denote $\mathfrak{p}_3,\mathfrak{p}_3'$ the primes in F above 3. They are the same if and only if $\bigl(\frac{D}{3}\bigr)=-1$. The local calculations in Section 6B lead to the following result.

Theorem 6.2. *Let $d_j < 0$ and d be the same as in Theorem 6.1, and let $\varepsilon = \varepsilon_1\varepsilon_2 = (-1)^{(d_1+d_2-2)/8}$. Suppose $t = (a+\sqrt{D})/(2\mathrm{d}\sqrt{D}) \in F^\times$ is totally positive with $a \in \mathbb{Q}$. Then*

$$a(t,\phi_{\mathrm{d}}) = -\mathrm{d}_2\varepsilon^{24/\mathrm{d}}\delta_2(\mathrm{d}_2,t)\times\left\{\sum_{\substack{\mathfrak{p}\ \textit{inert in } E/F\\ \mathfrak{p}\nmid 3}}(1+\mathrm{ord}_{\mathfrak{p}}(t\sqrt{D}))\rho^{(6)}(t\sqrt{D}\mathfrak{p}^{-1})\delta_3(\mathrm{d}_3,t)\log(\mathrm{Nm}(\mathfrak{p}))\right.$$
$$\left. +\log 3\sum_{\substack{\mathfrak{p}\ \textit{inert in } E/F\\ \mathfrak{p}\mid 3}}\rho^{(2)}(t\sqrt{D}\mathfrak{p}^{-1})\delta_3'(\mathrm{d}_3,t)\right\} \tag{6-7}$$

if $a \in \mathbb{Z}$ and zero otherwise. The functions $\delta_p(\mathrm{d}_p,t)$ and $\delta_3'(\mathrm{d}_3,t)$ are defined by

$$\delta_2(1,t) := 2(v_2(\mathrm{Nm}(t))-1), \qquad v_2(\mathrm{Nm}(t)) \geq 2,$$

$$\delta_2(2,t) := \begin{cases} 1 & \textit{if } v_2(\mathrm{Nm}(t)) = 0,\\ v_2(\mathrm{Nm}(t))-3 & \textit{if } v_2(\mathrm{Nm}(t)) \geq 1,\end{cases}$$

$$\delta_2(4,t) := \begin{cases} \mp 1 & \textit{if } \mathrm{Nm}(2t) \equiv \pm 1 \bmod 4,\\ 1 & \textit{if } v_2(\mathrm{Nm}(t)) = 0,\\ v_2(\mathrm{Nm}(t))-3 & \textit{if } v_2(\mathrm{Nm}(t)) \geq 1,\end{cases}$$

$$\delta_2(8,t) := \begin{cases} 1 & \textit{if } \mathrm{Nm}(4t) \equiv 3 \bmod 8,\\ -1 & \textit{if } \mathrm{Nm}(4t) \equiv 7 \bmod 8,\\ \mp 1 & \textit{if } \mathrm{Nm}(2t) \equiv \pm 1 \bmod 4,\\ 1 & \textit{if } v_2(\mathrm{Nm}(t)) = 0,\\ v_2(\mathrm{Nm}(t))-3 & \textit{if } v_2(\mathrm{Nm}(t)) \geq 1,\end{cases}$$

$$\delta_3(1,t) := \rho_3(t), \qquad v_3(\mathrm{Nm}(t)) \geq 0,$$

$$\delta_3(3,t) := \begin{cases} 2-\frac{3}{4}\left(1-\left(\frac{d_1}{3}\right)\right)\left(1-\left(\frac{d_2}{3}\right)\right) & \textit{if } \mathrm{Nm}(3t) \equiv 1 \bmod 3,\\ -1 & \textit{if } \mathrm{Nm}(3t) \equiv 2 \bmod 3,\\ \left(1+\left(\frac{d_1}{3}\right)\right)v_3(\mathrm{Nm}(t))+1-\left(\frac{d_1}{3}\right)^{v_3(\mathrm{Nm}(t))-1} & \textit{if } v_3(\mathrm{Nm}(3t)) \geq 1,\end{cases}$$

$$\delta_3'(\mathrm{d}_3,t) := \begin{cases} v_3(\mathrm{Nm}(t))+1 & \textit{if } \mathrm{d}_3 = 1,\\ 2v_3(\mathrm{Nm}(t))+3 & \textit{if } \mathrm{d}_3 = 3,\end{cases}$$

and zero otherwise. Here $\rho^{(M)}(\mathfrak{a}) := \rho(\mathfrak{a}^{(M)})$ is the number of integral ideals of E with relative norm (to F) $\mathfrak{a}^{(M)}$, $\rho_M(\mathfrak{a}) := \rho(\mathfrak{a}/\mathfrak{a}^{(M)})$, and $\mathfrak{a}^{(M)}$ is the prime to M part of an ideal $\mathfrak{a}$.

Proof. To evaluate $a(t,\phi)$, it is convenient to introduce the "Diff" set of Kudla. For a totally positive $t \in F^\times$, define

$$\mathrm{Diff}(W,t) := \{\mathfrak{p} : W_{\mathfrak{p}} \text{ does not represent } t\}.$$

Then $|\mathrm{Diff}(W,t)|$ is finite and odd. Furthermore if $\#\mathrm{Diff}(W,t) > 1$, then $a(t,\phi)$ vanishes. This is also the case with the expression on the right-hand side of (6-7), since $\delta_3(\mathrm{d}_3,t) = 0$ if $\mathfrak{p}_3, \mathfrak{p}_3' \in \mathrm{Diff}(W,t)$ and $\rho^{(6)}(t\sqrt{D}\mathfrak{p}) = 0$ for every inert $\mathfrak{p}$ if $\mathrm{Diff}(W,t)$ contains two primes coprime to 6. Therefore, we can suppose that $\mathrm{Diff}(W, t) = \{\mathfrak{p}_0\}$ for a single prime $\mathfrak{p}_0$ of F. In that case, every term with $\mathfrak{p} \neq \mathfrak{p}_0$ on the right-hand side of (6-7) vanishes. Given $t = (a + \sqrt{D})/(2\mathrm{d}\sqrt{D}) \in F$ totally positive, the Fourier coefficient $a(t, \phi)$ is given by

$$a(t, \phi_{\mathrm{d}}) = -4\frac{d}{ds}\left(\frac{W^*_{t,2}(s, \phi_{\mathrm{d},2})}{\gamma(W_2)}\frac{W^*_{t,3}(s, \phi_{\mathrm{d},3})}{\gamma(W_3)}\prod_{\mathfrak{p}\nmid 6\infty}\frac{W^*_{t,\mathfrak{p}}(s, \phi_{\mathfrak{p}})}{\gamma(W_{\mathfrak{p}})}\right)\Bigg|_{s=0},$$

where $\gamma(W_{\mathfrak{p}})$ is the Weil index of $W_{\mathfrak{p}}$ (see, e.g., Proposition 2.7 in [Yang and Yin 2019]).

Recall that $\mathfrak{p}_1, \mathfrak{p}_2$ and $\mathfrak{p}_3, \mathfrak{p}'_3$ are primes in F above 2 and 3 respectively. Since $\mathfrak{p}_1, \mathfrak{p}_2$ splits in E, they are not in $\mathrm{Diff}(W, t)$ for any t. However, $\mathfrak{p}_3$ and $\mathfrak{p}'_3$ could appear in some Diff set if they are inert in E/F. Now, if $\mathfrak{p}_0 \nmid 3$, then we can proceed as in the proof of Theorem 1.1 in [Yang and Yin 2019] to obtain

$$a(t, \phi_{\mathrm{d}}) = -2\frac{W^*_{t,2}(0, \phi_{\mathrm{d},2})}{\gamma(W_2)}\frac{W^*_{t,3}(0, \phi_{\mathrm{d},3})}{\gamma(W_3)}\rho^{(6)}(\mathrm{d}\sqrt{D}t\mathfrak{p}_0^{-1})(1 + \mathrm{ord}_{\mathfrak{p}_0}(t\sqrt{D}))\log \mathrm{Nm}(\mathfrak{p}_0).$$

By Lemma 6.5 and (6-13), we can replace $2W^*_{t,2}(0, \phi_{\mathrm{d},2})/\gamma(W_2)$ with $\varepsilon^{24/\mathrm{d}}\mathrm{d}_2\delta_2(\mathrm{d}_2, t)$. By Lemmas 6.7, 6.10 and 6.12, we can replace $W^*_{t,3}(0, \phi_{\mathrm{d},3})/\gamma(W_3)$ with $\delta_3(\mathrm{d}_3, t)$ and arrive at the right-hand side.

If $\mathrm{Diff}(W, t) = \{\mathfrak{p}_0\}$ with $\mathfrak{p}_0 \mid 3$, then $\left(\frac{d_j}{3}\right) = -1$ and we can write

$$a(t, \phi_{\mathrm{d}}) = -4\frac{W^*_{t,2}(0, \phi_{\mathrm{d},2})}{\gamma(W_2)}\frac{W^{*,\prime}_{t,3}(0, \phi_{\mathrm{d},3})}{\gamma(W_3)}\rho^{(6)}(\mathrm{d}\sqrt{D}t).$$

We can again replace $2W^*_{t,2}(0, \phi_{\mathrm{d},2})/\gamma(W_2)$ with $\varepsilon^{24/\mathrm{d}}\mathrm{d}_2\delta_2(\mathrm{d}_2, t)$ and apply Lemma 6.12 to replace $2W^{*,\prime}_{t,3}(0, \phi_{\mathrm{d},3})/\gamma(W_3)$ with $\delta'_3(3, t)\log 3$. This finishes the proof. □

Yui and Zagier [1997] derived the conjectural factorization of $\mathrm{Nm}_{H/\mathbb{Q}}(f(\tau_1)^{24/s} - f(\tau_2)^{24/s})$ from the conjectural factorization of $\mathrm{Nm}_{H/\mathbb{Q}}(\Phi_{24/s}(f(\tau_1), f(\tau_2)))$, where Φ_r the r-th cyclotomic polynomial. Since $\mathfrak{F}(m)$ is the power of a rational prime ℓ, we can define

$$\mathfrak{F}(m) = \ell^{\gamma(m)}, \tag{6-8}$$

where $\gamma(m) = \prod_{p\mid m}\gamma_p(m)$ with

$$\gamma_p(m) := \begin{cases} \mathrm{ord}_p(m) + 1 & \text{if } \varepsilon(p) = 1, \\ 1 & \text{if } \varepsilon(p) = -1 \text{ and } 2 \mid \mathrm{ord}_p(m), \\ \frac{1}{2}(\mathrm{ord}_p(m) + 1) & \text{if } \varepsilon(p) = -1 \text{ and } 2 \nmid \mathrm{ord}_p(m) \text{ (i.e., } p = \ell). \end{cases} \tag{6-9}$$

The conjecture is then expressed in terms of how $\gamma_2(m)$ and $\gamma_3(m)$ decomposes, which are summarized in two tables (see [Yui and Zagier 1997, p. 1653]). The theorem above is equivalent to this formulation of the conjecture. As in [Yui and Zagier 1997], one can give a conjecture with an equivalent, but simplified, expression. This is the content of Conjecture 1.5, which we prove now.

Proof of Theorem 1.7. By Proposition 5.5 and Theorems 6.1, 6.2, we can write

$$
\begin{aligned}
4s & \sum_{[\mathfrak{a}_j]\in \mathrm{Cl}(d_j),\, j=1,2} \log |f(\mathfrak{a}_1)^{24/s} - f(\mathfrak{a}_2)^{24/s})|^4 \\
&= -2 \sum_{\mathrm{d}|s} \varepsilon^{24/\mathrm{d}} \sum_{t\in F^\times, t\gg 0, \mathrm{Tr}(t)=1/\mathrm{d}} a(t, \phi_{\mathrm{d}}) \\
&= 2 \sum_{\mathrm{d}|s} \sum_{t\in F^\times, t\gg 0, \mathrm{Tr}(t)=1/\mathrm{d}} \mathrm{d}_2 \delta_2(\mathrm{d}_2, t) \\
&\qquad \times \Bigg\{ \log 3 \sum_{\substack{\mathfrak{p} \text{ inert in } E/F \\ \mathfrak{p}|3}} \rho^{(2)}(t\sqrt{D}\mathfrak{p}^{-1}) \delta_3'(\mathrm{d}_3, t) \\
&\qquad\qquad + \sum_{\substack{\mathfrak{p} \text{ inert in } E/F \\ \mathfrak{p}\nmid 3}} (1+\mathrm{ord}_{\mathfrak{p}}(t\sqrt{D}))\rho^{(6)}(t\sqrt{D}\mathfrak{p}^{-1})\delta_3(\mathrm{d}_3, t)\log(\mathrm{Nm}(\mathfrak{p})) \Bigg\} \\
&= 2 \sum_{4\sqrt{D}\tilde{t}\in \mathcal{O}_F, \tilde{t}\gg 0, \mathrm{Tr}(\tilde{t})=1/2} \sum_{\mathrm{d}|s} \mathrm{d}_2 \delta_2\big(\mathrm{d}_2, \tfrac{2\tilde{t}}{\mathrm{d}}\big) \\
&\qquad \times \Bigg\{ \log 3 \sum_{\substack{\mathfrak{p} \text{ inert in } E/F \\ \mathfrak{p}|3}} \rho^{(2)}\big(\tfrac{2\tilde{t}}{\mathrm{d}}\sqrt{D}\mathfrak{p}^{-1}\big) \delta_3'\big(\mathrm{d}_3, \tfrac{2\tilde{t}}{\mathrm{d}}\big) \\
&\qquad\qquad + \sum_{\substack{\mathfrak{p} \text{ inert in } E/F \\ \mathfrak{p}\nmid 3}} (1+\mathrm{ord}_{\mathfrak{p}}(\tilde{t}\sqrt{D}))\rho^{(6)}(\tilde{t}\sqrt{D}\mathfrak{p}^{-1})\delta_3\big(\mathrm{d}_3, \tfrac{2\tilde{t}}{\mathrm{d}}\big)\log(\mathrm{Nm}(\mathfrak{p})) \Bigg\}
\end{aligned}
$$

By Theorem 6.2, we have

$$
\begin{aligned}
\sum_{\mathrm{d}_2|s_2} \mathrm{d}_2\delta_2\big(\mathrm{d}_2, \tfrac{2\tilde{t}}{\mathrm{d}}\big) &= \sum_{\mathrm{d}_2|s_2} \mathrm{d}_2\delta_2\big(\mathrm{d}_2, \tfrac{2\tilde{t}}{\mathrm{d}_2}\big), \\
\sum_{\mathrm{d}_2|1} \mathrm{d}_2\delta_2\big(\mathrm{d}_2, \tfrac{2\tilde{t}}{\mathrm{d}_2}\big) &= 2(v_2(\mathrm{Nm}(\tilde{t}))+1) = 2\gamma_2(\mathrm{Nm}(\tilde{t})), \\
\sum_{\mathrm{d}_2|2} \mathrm{d}_2\delta_2\big(\mathrm{d}_2, \tfrac{2\tilde{t}}{\mathrm{d}_2}\big) &= 4 \begin{cases} 1 & \text{if } v_2(\mathrm{Nm}(\tilde{t}))=0, \\ v_2(\mathrm{Nm}(\tilde{t}))-1 & \text{if } v_2(\mathrm{Nm}(\tilde{t}))\geq 1, \end{cases} \\
\sum_{\mathrm{d}_2|4} \mathrm{d}_2\delta_2\big(\mathrm{d}_2, \tfrac{2\tilde{t}}{\mathrm{d}_2}\big) &= 8 \begin{cases} 1 & \text{if } v_2(\mathrm{Nm}(\tilde{t}))\equiv -1 \bmod 4 \\ & \text{or } v_2(\mathrm{Nm}(\tilde{t}))=2, \\ v_2(\mathrm{Nm}(\tilde{t}))-3 & \text{if } v_2(\mathrm{Nm}(\tilde{t}))\geq 3, \end{cases} \\
\sum_{\mathrm{d}_2|8} \mathrm{d}_2\delta_2\big(\mathrm{d}_2, \tfrac{2\tilde{t}}{\mathrm{d}_2}\big) &= 16 \begin{cases} 1 & \text{if } v_2(\mathrm{Nm}(\tilde{t}))=4 \\ & \text{or } v_2(\mathrm{Nm}(\tilde{t}))\equiv 12 \bmod 16 \\ & \text{or } v_2(\mathrm{Nm}(\tilde{t}))\equiv 3 \bmod 8, \\ v_2(\mathrm{Nm}(\tilde{t}))-5 & \text{if } v_2(\mathrm{Nm}(\tilde{t}))\geq 5. \end{cases}
\end{aligned}
$$

From this, it is easy to check that

$$\sum_{\mathrm{d}_2 \mid s_2} \mathrm{d}_2 \delta_2\big(\mathrm{d}_2, \tfrac{2\tilde{t}}{\mathrm{d}}\big) = 2 s_2 \sum_{\substack{r_2 \mid s_2,\, m := D\mathrm{Nm}(\tilde{t}/r_2) \in \mathbb{Z}, \\ m \equiv 3 \bmod s_2/r_2}} \gamma_2(m), \tag{6-10}$$

where we write $s = s_2 s_3$ with s_p the p-part of s. Similarly, we also have

$$\begin{aligned} &\kappa_3(s) s_3 \sum_{\substack{r_3 \mid s_3,\, m := D\mathrm{Nm}(\tilde{t}/r_3) \in \mathbb{Z}, \\ m \equiv d_1 + d_2 - 1 \bmod s_3/r_3}} \gamma_3(m) \\ &\qquad = \begin{cases} \frac{1}{2} \sum_{\mathrm{d}_3 \mid s_3} \sum_{\mathfrak{p} \mid 3} \rho_3(\mathfrak{p}^{-1}\tilde{t}/3) \delta_3'\big(\mathrm{d}_3, \frac{2\tilde{t}}{\mathrm{d}}\big) & \text{if } \big(\frac{d_1}{3}\big) = \big(\frac{d_2}{3}\big) = -1 \text{ and } 2 \nmid v_3(\mathrm{Nm}(\tilde{t})), \\ \sum_{\mathrm{d}_3 \mid s_3} \delta_3\big(\mathrm{d}_3, \frac{2\tilde{t}}{\mathrm{d}}\big) & \text{otherwise,} \end{cases} \end{aligned} \tag{6-11}$$

where $\kappa_3(s) \in \big\{1, \frac{1}{2}\big\}$ is the constant defined in (1-8). So suppose $\mathrm{Diff}(W, \tilde{t}) = \{\mathfrak{p}_0\}$ with $\ell = \mathrm{Nm}(\mathfrak{p}_0)$. Then substituting in these gives us

$$\begin{aligned} \sum_{\mathrm{d} \mid s} \mathrm{d}_2 \delta_2\big(\mathrm{d}_2, \tfrac{2\tilde{t}}{\mathrm{d}}\big) \Bigg\{ &\log 3 \sum_{\substack{\mathfrak{p} \text{ inert in } E/F \\ \mathfrak{p} \mid 3}} \rho^{(2)}\big(\tfrac{2\tilde{t}}{\mathrm{d}} \sqrt{D} \mathfrak{p}^{-1}\big) \delta_3'\big(\mathrm{d}_3, \tfrac{2\tilde{t}}{\mathrm{d}}\big) \\ &+ \sum_{\substack{\mathfrak{p} \text{ inert in } E/F \\ \mathfrak{p} \nmid 3}} (1 + \mathrm{ord}_{\mathfrak{p}}(\tilde{t}\sqrt{D})) \rho^{(6)}(\tilde{t}\sqrt{D}\mathfrak{p}^{-1}) \delta_3\big(\mathrm{d}_3, \tfrac{2\tilde{t}}{\mathrm{d}}\big) \log(\mathrm{Nm}(\mathfrak{p})) \Bigg\} \\ &= 4s \sum_{\substack{r \mid s,\, m := D\mathrm{Nm}(\tilde{t}/r) \in \mathbb{Z} \\ m \equiv 19D \bmod s/r}} \log(\ell) \prod_{p \mid m} \gamma_p(m) = 4s \sum_{\substack{r \mid s,\, m := D\mathrm{Nm}(\tilde{t}/r) \in \mathbb{Z} \\ m \equiv 19D \bmod s/r}} \log \mathfrak{F}(m). \end{aligned}$$

After writing $\tilde{t} = (\sqrt{D} + a)/(4\sqrt{D})$ with $a \in \mathbb{Z}$ in the summation, we obtain (1-9). □

6B. ***Local Calculations.*** We first need to write $\phi_{\mathrm{d},p}$ as a linear combination of $\bigotimes_{\mathfrak{p} \mid p} \phi_{\mathfrak{p}}$ for some $\phi_{\mathfrak{p}} \in S(E_{\mathfrak{p}}) = S(W_{\mathfrak{p}})$.

6B1. $p = 2$. In this subsection, we deal with the case $p = 2$. Since $d_j \equiv 1 \bmod 8$, the prime 2 splits completely. We fix $\delta, \delta_j \in \mathbb{Z}_2^\times$ such that

$$\delta^2 = D, \quad \delta_j^2 = d_j, \quad \delta_1 \delta_2 = \delta. \tag{6-12}$$

We also denote

$$\overline{\delta_j} := -\delta_j, \quad \delta' := -\delta.$$

Note that

$$\varepsilon_{d_1} \varepsilon_{d_2} = \Big(\frac{2}{\delta}\Big). \tag{6-13}$$

For $i = 1, 2$, let $\mathfrak{p}_i$ be the two primes in F above 2, and $\mathfrak{P}_i, \overline{\mathfrak{P}_i}$ the two primes in E above $\mathfrak{p}_i$. Then the local fields $E_{\mathfrak{P}_i}$ and $E_{\overline{\mathfrak{P}_i}}$ are isomorphic to $\mathbb{Q}_2$ via the map

$$\begin{aligned}
\sigma_i &: F_{\mathfrak{p}_i} \cong \mathbb{Q}_2, \quad \sqrt{D} \mapsto (-1)^i \delta, \\
\sigma_i &: E_{\mathfrak{P}_i} \cong \mathbb{Q}_2, \quad \sqrt{D} \mapsto (-1)^i \delta, \quad \sqrt{d_j} \mapsto (-1)^{(i-1)(j-1)}\delta_j, \\
\sigma_i &: E_{\overline{\mathfrak{P}_i}} \cong \mathbb{Q}_2, \quad \sqrt{D} \mapsto (-1)^i \delta, \quad \sqrt{d_j} \mapsto -(-1)^{(i-1)(j-1)}\delta_j.
\end{aligned}$$

Under these identifications, $W_2 = W \otimes_{\mathbb{Q}} \mathbb{Q}_2 = W_{\mathfrak{p}_1} \times W_{\mathfrak{p}_2}$ with

$$W_{\mathfrak{p}_i} = E_{\mathfrak{p}_i} = E_{\mathfrak{P}_i} \times E_{\overline{\mathfrak{P}_i}} \cong \mathbb{Q}_2^2, \quad Q_{\mathfrak{p}_i}(y_1, y_2) = (-1)^i \frac{\mathrm{d}}{\delta} y_1 y_2.$$

Now we identify the $\mathbb{Q}_2$-quadratic space

$$\sigma : (V \otimes_{\mathbb{Q}} \mathbb{Q}_2, Q) \cong (E_{\mathfrak{p}_1}, Q_{\mathfrak{p}_1}) \times (E_{\mathfrak{p}_2}, Q_{\mathfrak{p}_2}), \quad \begin{pmatrix} x_3 & x_1 \\ x_4 & x_2 \end{pmatrix} \mapsto (\sigma_1(x), \sigma_1(\bar{x}), \sigma_2(x), \sigma_2(\bar{x})), \tag{6-14}$$

with

$$x = x_1 + x_2 \frac{-1+\sqrt{d_1}}{2} + x_3 \frac{1+\sqrt{d_2}}{2} + x_4 \frac{-1+\sqrt{d_1}}{2}\frac{1+\sqrt{d_2}}{2} \in W_2.$$

Under this isomorphism, we can identify $S(V \otimes \mathbb{Q}_2)$ with $S(E_{\mathfrak{p}_1} \times E_{\mathfrak{p}_2}) \cong S(E_{\mathfrak{p}_1}) \otimes S(E_{\mathfrak{p}_2})$, and map the lattice $L_{\mathrm{d},2} := L_{\mathrm{d}} \otimes \mathbb{Z}_2$ onto

$$\widetilde{L} := \Big\{ y = (y_1, y_2, y_3, y_4) \in \mathbb{Z}_2^4 : \sum y_i \in 2\mathbb{Z}_2 \Big\},$$

The $\mathbb{Q}_2$-quadratic form $\widetilde{Q}_{\mathrm{d}}$ on $\widetilde{L}$ is given by

$$\widetilde{Q}_{\mathrm{d}}(y) := -\frac{\mathrm{d}}{\delta}(y_1 y_2 - y_3 y_4) = Q_{\mathfrak{p}_1}(y_1, y_2) + Q_{\mathfrak{p}_2}(y_3, y_3).$$

Let

$$L_0 = (2\mathbb{Z}_2)^4 = 2\mathcal{O}_{E_{\mathfrak{p}_1}} \times 2\mathcal{O}_{E_{\mathfrak{p}_2}} = \widetilde{M}_1 \times \widetilde{M}_2$$

with $\widetilde{M}_i$ being the $\mathcal{O}_{F_{\mathfrak{p}_i}}$-lattice $2\mathcal{O}_{E_{\mathfrak{p}_i}}$. Then

$$L_0 \subset \widetilde{L} \subset \widetilde{L}' \subset L_0' = \frac{1}{4\mathrm{d}_2} L_0 \quad \text{and} \quad \widetilde{L}' = \left\{ y = \frac{1}{2\mathrm{d}_2}(y_1, y_2, y_3, y_4) \in \frac{1}{2\mathrm{d}_2}\mathbb{Z}_2^4 : y_i + y_j \equiv 0 \bmod 2 \right\}.$$

Notice that

$$\phi_{\widetilde{L}} \circ \sigma^{-1} = \sum_{\substack{y_i \in \mathbb{Z}/2\mathbb{Z} \\ \sum y_i = 0}} \phi_{(y_1, y_2) + \widetilde{M}_1} \otimes \phi_{(y_3, y_4) + \widetilde{M}_2},$$

where $\phi_A = \mathrm{Char}(A)$ for $A \subset W_2$. To apply the general formula in [Yang et al. 2019], we define $M_i = \mathbb{Z}_2^2$ with quadratic form $Q_i(y_1 y_2) = (-1)^i \frac{4\mathrm{d}}{\delta} y_1 y_2$. Then $(M_i, Q_i) \cong (\widetilde{M}_i, Q_{\mathfrak{p}_i})$ via scaling by 2. For any $\mu \in (\mathbb{Q}_2/\mathbb{Z}_2)^2$, we denote

$$\phi_\mu = \mathrm{char}(\mu + \mathbb{Z}_2^2)$$

and view it as an element in $S(M_i)$ for both $i = 1, 2$ if $\mu \in \big(\frac{1}{4\mathrm{d}_2}\mathbb{Z}_2/\mathbb{Z}_2\big)^2$.

Now, we can apply this scaling map to $\phi_{\mathrm{d},2}\circ\sigma^{-1}$, where $\phi_{\mathrm{d},2}\in S(L_{\mathrm{d},2})$ is the Schwartz function associated to $\mathfrak{u}_{\mathrm{d},2}$. We denote the result by $\widetilde{\phi}_{\mathrm{d},2}\in S(M_1\times M_2)\cong S(M_1)\otimes S(M_2)$, which will depend on the choice of $\delta \bmod \mathrm{d}_2$. We have listed them as follows.

Lemma 6.3. *For $\delta_j\in\mathbb{Z}_2^\times$ and $\delta=\delta_1\delta_2\in\mathbb{Z}_2^\times$, we have*

$$\widetilde{\phi}_{\mathrm{d},2}=\begin{cases} \phi_{\widetilde{L}}, & \mathrm{d}_2=1,\\ \phi_0\otimes\phi_{1,\delta}+\phi_{1,-\delta}\otimes\phi_0, & \mathrm{d}_2=2,\\ 2\big((\phi_0+\phi_{1,-\delta})\otimes\phi_{2,\delta}+\phi_{2,-\delta}\otimes(\phi_0+\phi_{1,\delta})\big), & \mathrm{d}_2=4,\\ \Big(\frac{2}{\delta\mathrm{d}_3}\Big)4\big((\phi_0+\phi_{1,\delta})\otimes\phi_{3,\delta}+\phi_{3,-\delta}\otimes(\phi_0+\phi_{1,-\delta})+\phi_{2,\delta}\otimes\phi_{3,5\delta}+\phi_{3,-5\delta}\otimes\phi_{2,-\delta}\big), & \mathrm{d}_2=8, \end{cases} \tag{6-15}$$

where for $j=1,2,3,\ r\in(\mathbb{Z}/2^{j+1}\mathbb{Z})^\times$

$$\phi_0:=\sum_{k\in\mathbb{Z}/2\mathbb{Z}}\phi_{\frac{1}{2}(k,k)}-\phi_{\frac{1}{2}(k,k+1)},\qquad \phi_{j,r}:=\sum_{a\in(\mathbb{Z}/2^{j+1})^\times}\phi_{\mu(a;r,j)}-\phi_{\mu(a;r+2^j;j)},$$

are elements in $S(M_i)$ with

$$\mu(a;r,j):=\frac{1}{2^{j+1}}(a,ra^{-1})\in(\mathbb{Q}_2/\mathbb{Z}_2)^2.$$

Remark 6.4. Note that the support of $\mathfrak{u}_{24,2}$ is the support of $\mathfrak{u}_{8,2}$ after scaling by d_3. This does not affect $\phi_{j,r}$ for $j=1,2$ but introduces the factor $\big(\frac{2}{\mathrm{d}_3}\big)$ when $j=3$, since $\phi_{3,rc^2}=\big(\frac{2}{c}\big)\phi_{3,r}$ for any odd integer c. Therefore this factor appears above when $\mathrm{d}_2=8$.

Proof. One can use Lemma 3.11 to check that the cosets on the right indeed appear. Then we have all of them by counting. □

Now, we can apply the general Whittaker function formulas in [Yang et al. 2019] to obtain:

Lemma 6.5. *Let $\delta_2(\mathrm{d}_2,t)$ be defined as in Theorem 6.2. Then we have*

$$\frac{W_t^*(0,\widetilde{\phi}_{\mathrm{d},2})}{\gamma(W_2)}=\Big(\frac{2}{\delta}\Big)^{24/\mathrm{d}}\frac{\mathrm{d}_2}{2}\delta_2(\mathrm{d}_2,t)$$

for all totally positive $t\in F^\times$ with $\mathrm{Tr}(t)=\frac{1}{\mathrm{d}}$.

Proof. This can be checked case by case. For $\mathrm{d}_2=1$, this was already done in [Yang and Yin 2019]. Otherwise, we can apply Propositions 5.3 and 5.7 in [Yang et al. 2019] after scaling the lattice by 2 and the quadratic form by 4 (i.e., variant 2 in [Yang et al. 2019]). We write $t_i=\sigma_i(t)\in\mathbb{Q}_2$ and suppose $o(t_1)\geq o(t_2)$ with $o(t_i)$ the 2-adic valuation of $t_i\in\mathbb{Q}_2$. The case $o(t_1)\leq o(t_2)$ will be exactly the same. Tables 1–6 contain the nonzero values of $W_{t_i}^*(0,\phi_{\mu_i})/\gamma(W_{\mathfrak{p}_i})$ for $i=1$.

$o(t_1)$	$\mu_1 = (0,0)$	$\left(\frac{1}{2},\frac{1}{2}\right)$	$\left(\frac{1}{2},0\right)$
1	0	1	0
≥ 2	$o(t_1)-2$	0	1

Table 1. $\mathrm{d}_2 = 2$, $\beta = -8\mathrm{d}_3\delta^{-1}$.

$o(t_1)$	$\mu_1 = (0,0)$	$\left(\frac{1}{2},\frac{1}{2}\right)$	$\left(\frac{1}{2},0\right)$	$\left(\frac{a}{4},-\frac{a^{-1}\delta}{4}\right)$	$\left(\frac{a}{4},\frac{a^{-1}(-\delta+2)}{4}\right)$
$t_1 \in \mathrm{d}_3 + 4\mathbb{Z}_2$	0	0	0	$\frac{1}{2}$	0
$t_1 \in -\mathrm{d}_3 + 4\mathbb{Z}_2$	0	0	0	0	$\frac{1}{2}$
2	0	1	0	0	0
≥ 3	$o(t_1)-3$	0	1	0	0

Table 2. $\mathrm{d}_2 = 4$, $\beta = -16\mathrm{d}_3\delta^{-1}$.

$o(t_1)$	$\mu_1 = (0,0)$	$\left(\frac{1}{2},\frac{1}{2}\right)$	$\left(\frac{1}{2},0\right)$	$\left(\frac{a}{4},\frac{a^{-1}\delta}{4}\right)$	$\left(\frac{a}{4},\frac{a^{-1}(\delta+2)}{4}\right)$	$\left(\frac{a}{8},\frac{a^{-1}\delta^{-1}}{8}\right)$	$\left(\frac{a}{8},\frac{a^{-1}(\delta^{-1}+4)}{8}\right)$
$t_1 \in \frac{1}{2}(-\mathrm{d}_3 + 8\mathbb{Z}_2)$	0	0	0	0	0	$\frac{1}{4}$	0
$t_1 \in \frac{1}{2}(3\mathrm{d}_3 + 8\mathbb{Z}_2)$	0	0	0	0	0	0	$\frac{1}{4}$
$t_1 \in 2(-\mathrm{d}_3 + 4\mathbb{Z}_2)$	0	0	0	$\frac{1}{2}$	0	0	0
$t_1 \in 2(\mathrm{d}_3 + 4\mathbb{Z}_2)$	0	0	0	0	$\frac{1}{2}$	0	0
3	0	1	0	0	0	0	0
≥ 4	$o(t_1)-4$	0	1	0	0	0	0

Table 3. $\mathrm{d}_2 = 8$, $\beta = -32\mathrm{d}_3\delta^{-1}$.

$o(t_1)$	$\mu_2 = \left(\frac{a}{4},\frac{a^{-1}\delta}{4}\right)$	$\left(\frac{a}{4},\frac{a^{-1}(\delta+2)}{4}\right)$
≥ 1	$\frac{1}{2}$	0

Table 4. $\mathrm{d}_2 = 2$, $\beta = 8\mathrm{d}_3\delta^{-1}$.

$o(t_1)$	$\mu_2 = \left(\frac{a}{8},\frac{a^{-1}\delta}{8}\right)$	$\left(\frac{a}{8},\frac{a^{-1}(\delta+4)}{8}\right)$
0	0	$\frac{1}{4}$
≥ 1	$\frac{1}{4}$	0

Table 5. $\mathrm{d}_2 = 4$, $\beta = 16\mathrm{d}_3\delta^{-1}$.

$o(t_1)$	$\mu_2 = \left(\frac{a}{16},\frac{a^{-1}\delta\mathrm{d}_3^2}{16}\right)$	$\left(\frac{a}{16},\frac{a^{-1}(\delta\mathrm{d}_3^2+8)}{16}\right)$	$\left(\frac{a}{16},\frac{5a^{-1}\delta\mathrm{d}_3^2}{16}\right)$	$\left(\frac{a}{16},\frac{a^{-1}(5\delta\mathrm{d}_3^2+8)}{16}\right)$
-1	0	0	$\frac{1}{8}$	0
≥ 1	$\frac{1}{8}$	0	0	0

Table 6. $\mathrm{d}_2 = 8$, $\beta = 32\mathrm{d}_3\delta^{-1}$.

For $i=2$, we write $\alpha(\mu_2, t_2) := \beta\mu_2\overline{\mu_2} - t_2$ in the notation of [Yang et al. 2019]. When $\mathrm{d}_2 = 2$, we have $t_2 \in \frac{1}{2}(\mathrm{d}_3^{-1} + 4\mathbb{Z}_2)$ if $o(t_1) \geq 1$, since $t_1 + t_2 = 1/(2\mathrm{d}_3)$. Then with $\beta = 8\mathrm{d}_3\delta^{-1}$, we have $\alpha(\mu(a;\delta,1), t_2) = \beta\frac{a}{4}\frac{a^{-1}\delta}{4} - t_2 \in 2\mathbb{Z}_2$. When $\mathrm{d}_2 = 4$, we have

$$t_2 \in \begin{cases} \frac{1}{4}\mathrm{d}_3^{-1} + 1 + 2\mathbb{Z}_2 & \text{if } o(t_1) = 0, \\ \frac{1}{4}\mathrm{d}_3^{-1} + 2\mathbb{Z}_2 & \text{if } o(t_1) \geq 1, \end{cases}$$

since $t_1+t_2 = 1/(4\mathrm{d}_3)$. Then with $\beta = 16\mathrm{d}_3\delta^{-1}$, we have $\alpha(\mu(a;\delta,2),t_2) \in \mathbb{Z}_2^\times$, $\alpha(\mu(a;\delta+4,2),t_2) \in 2\mathbb{Z}_2$ if $o(t_1)=0$, and $\alpha(\mu(a;\delta,2),t_2) \in 2\mathbb{Z}_2$, $\alpha(\mu(a;\delta+4,2),t_2) \in \mathbb{Z}_2^\times$ if $o(t_1) \geq 1$. When $\mathrm{d}_2 = 8$, we have

$$t_2 \in \begin{cases} \frac{1}{8}\mathrm{d}_3^{-1} + \frac{1}{2}\mathrm{d}_3 + 2\mathbb{Z}_2 & \text{if } o(t_1) = -1, \\ \frac{1}{8}\mathrm{d}_3^{-1} + 2\mathbb{Z}_2 & \text{if } o(t_1) \geq 1, \end{cases}$$

since $t_1 + t_2 = 1/(8\mathrm{d}_3)$. Then with $\beta = 32\mathrm{d}_3\delta^{-1}$, we have

$$\alpha(\mu(a;\delta\mathrm{d}_3^2,3),t_2) \in \begin{cases} \frac{1}{2}\mathbb{Z}_2^\times & \text{if } o(t_1) = -1, \\ 2\mathbb{Z}_2 & \text{if } o(t_1) \geq 1, \end{cases}$$

$$\alpha(\mu(a;5\delta\mathrm{d}_3^2,3),t_2) \in \begin{cases} 2\mathbb{Z}_2 & \text{if } o(t_1) = -1, \\ \frac{1}{2}\mathbb{Z}_2^\times & \text{if } o(t_1) \geq 1, \end{cases}$$

and $\alpha(\mu(a;\delta\mathrm{d}_3^2+8,3),t_2), \alpha(\mu(a;5\delta\mathrm{d}_3^2+8,3),t_2) \notin 2\mathbb{Z}_2$.

Putting these together, we see that when $\mathrm{d}_2 = 2$, we have

$$\frac{W_t^*(0,\widetilde{\phi}_{\mathrm{d},2})}{\gamma(W_2)} = \begin{cases} 1 & \text{if } o(t_1) = 1, \\ o(t_1) - 4 & \text{if } o(t_1) \geq 2. \end{cases}$$

Notice that $v_2(\mathrm{Nm}(t)) = o(t_1t_2) = o(t_1) - 1$. This proves the lemma for $\mathrm{d}_2 = 2$. When $\mathrm{d}_2 = 4$, we have

$$\frac{W_t^*(0,\widetilde{\phi}_{\mathrm{d},2})}{\gamma(W_2)} = \begin{cases} \mp 1 & \text{if } t_1 \in \pm\mathrm{d}_3 + 4\mathbb{Z}_2, \\ 1 & \text{if } o(t_1) = 2, \\ o(t_1) - 5 & \text{if } o(t_1) \geq 3. \end{cases}$$

Notice that $v_2(\mathrm{Nm}(t)) = o(t_1t_2) = o(t_1) - 2$. If $t_1 \in \pm\mathrm{d}_3 + 4\mathbb{Z}_2$, then $4t_2 \in \mathrm{d}_3^{-1} + 4\mathbb{Z}_2$ and $\mathrm{Nm}(2t) = 4t_1t_2 \equiv \pm 1 \bmod 4$. This proves the lemma for $\mathrm{d}_2 = 4$. Finally when $\mathrm{d}_2 = 8$, we have

$$\left(\frac{2}{\delta}\right)\frac{W_t^*(0,\widetilde{\phi}_{\mathrm{d},2})}{\gamma(W_2)} = \begin{cases} 1 & \text{if } t_1 \in \frac{1}{2}(-\mathrm{d}_3 + 8\mathbb{Z}_2), \\ -1 & \text{if } t_1 \in \frac{1}{2}(3\mathrm{d}_3 + 8\mathbb{Z}_2), \\ \mp 1 & \text{if } t_1 \in 2(\pm\mathrm{d}_3 + 4\mathbb{Z}_2), \\ 1 & \text{if } o(t_1) = 3, \\ o(t_1) - 6 & \text{if } o(t_1) \geq 4. \end{cases}$$

Notice that $v_2(\mathrm{Nm}(t)) = o(t_1t_2) = o(t_1) - 3$. If $t_1 \in \frac{1}{2}(-\mathrm{d}_3 + 4\mathbb{Z}_2)$, then $8t_2 \in \mathrm{d}_3^{-1} + 4 + 8\mathbb{Z}_2$ and $\mathrm{Nm}(4t) = 16t_1t_2 \equiv 3 \bmod 8$. Similarly, if $t_1 \in \frac{1}{2}(3\mathrm{d}_3 + 4\mathbb{Z}_2)$, then $8t_2 \in \mathrm{d}_3^{-1} + 4 + 8\mathbb{Z}_2$ and $\mathrm{Nm}(4t) = 16t_1t_2 \equiv 7 \bmod 8$. If $t_1 \in 2(\pm\mathrm{d}_3 + 4\mathbb{Z}_2)$, then $8t_2 \in \mathrm{d}_3^{-1} + 8\mathbb{Z}_2$ and $\mathrm{Nm}(2t) = 4t_1t_2 \equiv \pm 1 \bmod 4$. This completes the proof. □

6B2. $p = 3$. If $\mathrm{d}_3 = 1$, then $\phi_{\mathrm{d},3} = \mathrm{Char}(\mathcal{O}_E \otimes \mathbb{Z}_3)$ and the calculations have been done before. So suppose $\mathrm{d}_3 = 3$. There are 3 cases to consider.

$$\bullet\ \left(\frac{d_i}{3}\right) = 1. \qquad \bullet\ \left(\frac{d_1}{3}\right) \neq \left(\frac{d_2}{3}\right). \qquad \bullet\ \left(\frac{d_i}{3}\right) = -1.$$

The first case is similar to the case $p = 2$ considered above. We again fix $\delta_i \in \mathbb{Z}_3^\times$ square roots of d_i and denote $\delta := \delta_1\delta_2$. Then the analog of the map in (6-14) for $p = 3$, which we also call σ, identifies $L_{\mathrm{d},3} = M_2(\mathbb{Z}_3)$ with $\widetilde{L}_3 := \mathbb{Z}_3^4$, which has the quadratic form $\widetilde{Q}_{\mathrm{d}}(y) = -\frac{3\mathrm{d}_2}{\delta}(y_1y_2 - y_3y_4)$. Denote $\widetilde{\phi}_{\mathrm{d},3} := \phi_{\mathrm{d},3} \circ \sigma^{-1} \in S(\widetilde{L}_3)$, where $\phi_{\mathrm{d},3}$ is the Schwartz function associated to $\mathfrak{u}_{\mathrm{d},3} \in \mathbb{C}[\mathcal{A}_{\mathrm{d},3}]$. Then the analog of Lemma 6.3 is as follows.

Lemma 6.6. *For* $\delta_i \in \mathbb{Z}_3^\times$ *and* $\delta = \delta_1\delta_2 \equiv \pm 1 \bmod 3$, *we have*

$$\widetilde{\phi}_{\mathrm{d},3} = \phi_0 \otimes \phi_\delta + \phi_{-\delta} \otimes \phi_0 + 2\phi_\delta \otimes \phi_{-\delta},$$

where

$$\phi_0 := 2\phi_{(0,0)} - (\phi_{\frac{1}{3}(0,1)} + \phi_{\frac{1}{3}(1,0)} + \phi_{\frac{1}{3}(0,2)} + \phi_{\frac{1}{3}(0,2)}), \quad \phi_{\pm 1} := \phi_{\frac{1}{3}(1,\pm 1)} + \phi_{\frac{1}{3}(2,\pm 2)}.$$

are in $S(\mathbb{Z}_3^2)$.

Proof. This follows from a straightforward calculations as in the case $p = 2$. □

Lemma 6.7. *Suppose* $\left(\frac{d_i}{3}\right) = 1$. *Then we have*

$$\frac{W_t^*(0, \widetilde{\phi}_{\mathrm{d},3})}{\gamma(W_3)} = \begin{cases} 2 & \text{if } v_3(\mathrm{Nm}(t)) = -2, \\ 2v_3(\mathrm{Nm}(t)) & \text{if } v_3(\mathrm{Nm}(t)) \geq -1, \end{cases}$$

for all totally positive $t \in F^\times$ *with* $\mathrm{Tr}(t) = \frac{1}{\mathrm{d}}$.

Proof. Apply Lemma 6.6 and Propositions 5.3, 5.7 in [Yang et al. 2019]. □

In the second case, the prime 3 is inert in F and splits into two primes $\mathfrak{P}, \overline{\mathfrak{P}}$ in E. We therefore fix $\delta \in \overline{\mathbb{Q}_3}$ such that $\delta^2 = D$, and denote $F_\delta := \mathbb{Q}_3(\delta)$ the quadratic extension of $\mathbb{Q}_3$ with $\mathcal{O}_\delta \subset F_\delta$ its ring of integers, where 3 is inert. For any choice of $\delta_j \in F_\delta$ such that $\delta_j^2 = d_j$ and $\delta_1\delta_2 = \delta$, we can identify $W \otimes \mathbb{Q}_3$ with $F_\delta \times F_\delta$ via

$$(a_1 + b_1\sqrt{d_1}) \otimes (a_2 + b_2\sqrt{d_2}) \mapsto ((a_1 + b_1\delta_1)(a_2 + b_2\delta_2), (a_1 - b_1\delta_1)(a_2 - b_2\delta_2)).$$

This identifies the $\mathbb{Q}_3$-vector spaces $V \otimes \mathbb{Q}_3$ and $F_\delta \times F_\delta$. The $\mathbb{Z}_3$-lattice $L_{3\mathrm{d}_2} \otimes \mathbb{Z}_3$ and its dual lattice $L'_{3\mathrm{d}_2} \otimes \mathbb{Z}_3$ in $V \otimes \mathbb{Q}_3$ are then mapped to

$$\widetilde{L}_3 := \mathcal{O}_\delta \times \mathcal{O}_\delta \quad \text{and} \quad \widetilde{L}'_3 := 3^{-1}\mathcal{O}_\delta \times 3^{-1}\mathcal{O}_\delta,$$

respectively. The finite $\mathbb{Z}_3$-modules $(L'_{3\mathrm{d}_2}/L_{3\mathrm{d}_2}) \otimes \mathbb{Z}_3$ and $\mathcal{O}_\delta/3\mathcal{O}_\delta \times \mathcal{O}_\delta/3\mathcal{O}_\delta$ are explicitly identified via

$$\begin{aligned}\frac{1}{3\mathrm{d}_2}\begin{pmatrix} x_3 & x_1 \\ x_4 & x_2 \end{pmatrix} \otimes \mathbb{Z}_3 \mapsto \Big(&\mathrm{d}_2^{-1}(x_1 + x_2 - x_3 - x_4 + (x_4 - x_2)\delta_1 - (x_3 + x_4)\delta_2 + x_4\delta), \\ &\mathrm{d}_2^{-1}(x_1 + x_2 - x_3 - x_4 - (x_4 - x_2)\delta_1 + (x_3 + x_4)\delta_2 + x_4\delta)\Big). \qquad (6\text{-}16)\end{aligned}$$

The latter can be viewed as the finite quadratic module of the $\mathcal{O}_\delta$-lattice $\mathcal{O}_E \otimes \mathbb{Z}_3 \cong \mathcal{O}_\delta \times \mathcal{O}_\delta$ with the F_δ-quadratic form $Q_{\mathrm{d},\delta}(y) := -\frac{3\mathrm{d}_2}{\delta} y_1 y_2$ for $y = (y_1, y_2) \in F_\delta \times F_\delta$. Note that $\mathcal{O}_\delta / 3\mathcal{O}_\delta = (\mathbb{Z}/3\mathbb{Z})[\delta]$ is a finite field of size 9.

Now let $\widetilde{\phi}_{\mathrm{d},3} \in S(\mathcal{O}_E \otimes \mathbb{Z}_3)$ be the Schwartz function associated to $\phi_{\mathrm{d},3} \in S(L_{\mathrm{d},3})$ under the map in (6-16). It is easy to check by hand the following lemma.

Lemma 6.8. *Let $\delta, \delta_1, \delta_2 \in \overline{\mathbb{Q}_3}$ be as above. Then*

$$\widetilde{\phi}_{\mathrm{d},3} = 2 \sum_{\mu \in S_0} \phi_\mu - \sum_{\mu \in S_1} \phi_\mu - \sum_{\mu \in S_{-1}} \phi_\mu, \tag{6-17}$$

where $S_j := \left\{ \mu \in \left(\tfrac{1}{3}\mathbb{Z}/\mathbb{Z}\right)[\delta] \times \left(\tfrac{1}{3}\mathbb{Z}/\mathbb{Z}\right)[\delta] : Q_{\mathrm{d},\delta}(\mu) = \tfrac{1}{3}(-\mathrm{d}_2 + j\delta) \in \left(\tfrac{1}{3}\mathbb{Z}/\mathbb{Z}\right)[\delta] \right\}$ *for* $j = 0, \pm 1$.

Remark 6.9. The size of S_j is 8 for every j.

We can now apply Proposition 5.3 in [Yang et al. 2019] to find the value of the Whittaker function.

Lemma 6.10. *Suppose $\left(\frac{d_1}{3}\right) \neq \left(\frac{d_1}{3}\right)$. Then we have*

$$\frac{W_t^*(0, \widetilde{\phi}_{\mathrm{d},3})}{\gamma(W_3)} = \begin{cases} 2 & \textit{if}\, \mathrm{Nm}(3t) \equiv 1 \bmod 3, \\ -1 & \textit{if}\, \mathrm{Nm}(3t) \equiv 2 \bmod 3, \end{cases}$$

for all totally positive $t \in F^\times$ with $\mathrm{Tr}(t) = \frac{1}{\mathrm{d}}$.

Proof. First, $\beta = -3\mathrm{d}_2/\delta$, the normalizing L-factor is $L(1, \chi) = \frac{9}{8}$ and the volume $\mathrm{vol}(\mathcal{O}_E, d_\beta x) = \frac{1}{9}$. Suppose $t = (\delta + a)/(6\mathrm{d}_2\delta) \in F_\delta$. For $\mu \in S_j$, the quantity $3\alpha(\mu, t)$ is

$$3\alpha(\mu, t) := 3(Q_{\mathrm{d},\delta}(\mu) - t) \equiv (-\mathrm{d}_2 + j\delta) - 2(\mathrm{d}_2\delta)^{-1}(\delta + a) \equiv (j - \mathrm{d}_2 a)\delta \bmod 3$$

since $\delta^2 = D \equiv 2 \bmod 3$. Now $3\alpha(\mu, t) \equiv 0 \bmod 3$ if and only if $3 \mid (j - \mathrm{d}_2 a)$. This happens when $3 \mid (j, a)$, in which case $\mu \in S_0$ and $\mathrm{Nm}(3t) \equiv 1 + a^2 \equiv 1 \bmod 3$. The value of $W_t^*(0, \widetilde{\phi}_{\mathrm{d},3})/\gamma(W_3)$ is 2. Otherwise if $3 \nmid a$ and $3 \mid (j - \mathrm{d}_2 a)$, then $\mu \in S_{\mathrm{d}_2 a}$ and $\mathrm{Nm}(3t) \equiv 2 \bmod 3$. The value of $W_t^*(0, \widetilde{\phi}_{\mathrm{d},3})/\gamma(W_3)$ is then -1. This finishes the proof. □

In the last case, we need to calculate both the value and derivative of the Whittaker function at $s = 0$ since 3 splits into the product of two inert primes $\mathfrak{p}_1, \mathfrak{p}_2$ in F. As in the setup of the previous two cases, we fix $\delta, \delta_i \in \overline{\mathbb{Q}_3}$ such that $\delta_i^2 = d_i$ and $\delta = \delta_1\delta_2 \in \mathbb{Z}_3$. Denote $\widetilde{E} := \mathbb{Q}_3(\delta_1) = \mathbb{Q}_3(\delta_2)$ the quadratic extension of $\mathbb{Q}_3$ with ring of integers $\widetilde{\mathcal{O}}$. This gives an identification

$$\sigma_i : F \otimes \mathbb{Q}_3 \cong \mathbb{Q}_3 : \sqrt{D} \mapsto (-1)^i \delta, \quad \sigma_i : E_{\mathfrak{p}_i} \cong \widetilde{E} : \sqrt{d_j} \mapsto (-1)^{(i-1)(j-1)} \delta_j.$$

Then the isomorphism in (5-1) induces $V \otimes \mathbb{Q}_3 \cong W \otimes \mathbb{Q}_3 = E_{\mathfrak{p}_1} \times E_{\mathfrak{p}_2} \cong \widetilde{E} \times \widetilde{E}$, with the quadratic form on $y \in E_{\mathfrak{p}_i}$ given by $Q_i(y) := (-1)^{i-1}(3\mathrm{d}_2)/(\sqrt{D})\mathrm{Nm}(y)$. The lattice $L_{\mathrm{d},3}$ is then isometric to

$$\widetilde{L}_{\mathrm{d},3} := \widetilde{\mathcal{O}} \times \widetilde{\mathcal{O}} \subset \widetilde{E} \times \widetilde{E},$$

whose dual lattice is $\widetilde{L}'_{\mathrm{d},3} := \frac{1}{3}\widetilde{\mathcal{O}} \times \frac{1}{3}\widetilde{\mathcal{O}} \subset \widetilde{E} \times \widetilde{E}$, with respect to the quadratic form $\widetilde{Q}_{\mathrm{d},\delta}(y) := -(3\mathrm{d}_2/\delta)(\mathrm{Nm}(y_1) - \mathrm{Nm}(y_2))$ for $y = (y_1, y_2) \in \widetilde{E} \times \widetilde{E}$. Under this identification, the Schwartz function $\widetilde{\phi}_{\mathrm{d},3} \in S(\widetilde{L}_{\mathrm{d},3})$ associated to $\phi_{\mathrm{d},3} \in S(L_{\mathrm{d},3})$ has the following decomposition.

Lemma 6.11. *Let $\delta, \delta_1, \delta_2 \in \overline{\mathbb{Q}_3}$ be as above. Then*

$$\widetilde{\phi}_{\mathrm{d},3} = 2\sum_{\mu\in S_1} \phi_\mu \otimes \phi_0 + 2\sum_{\mu\in S_{-1}} \phi_0 \otimes \phi_\mu - \sum_{\mu_1\in S_{-1},\mu_2\in S_1} \phi_{\mu_1}\otimes\phi_{\mu_2} \tag{6-18}$$

where $S_j := \left\{\mu \in \frac{1}{3}\widetilde{\mathcal{O}}/\widetilde{\mathcal{O}} : -\frac{3}{\delta}\mathrm{Nm}(\mu) \equiv \frac{j}{3} \bmod \mathbb{Z}_3\right\}$ *for* $j = \pm 1$.

Now, we can again apply Proposition 5.3 in [Yang et al. 2019] to calculate the values and derivatives of the Whittaker function.

Lemma 6.12. *Suppose* $\left(\frac{d_1}{3}\right) = \left(\frac{d_1}{3}\right) = -1$. *Then we have*

$$\frac{W_t^*(0,\phi_{\mathrm{d},3})}{\gamma(W_3)} = \begin{cases} -1 & \textit{if } v_3(\mathrm{Nm}(t)) = -2, \\ 2 & \textit{if } v_3(\mathrm{Nm}(t)) \geq 0 \textit{ is even}, \\ 0 & \textit{otherwise}, \end{cases}$$

$$\frac{W^{*,\prime}_t(0,\phi_{\mathrm{d},3})}{\gamma(W_3)} = \left(v_3(\mathrm{Nm}(t)) + \frac{3}{2}\right)\log 3 \quad \textit{if } v_3(\mathrm{Nm}(t)) \geq -1 \textit{ is odd},$$

for all totally positive $t \in F^\times$ *with* $\mathrm{Tr}(t) = \frac{1}{\mathrm{d}}$.

Proof. Denote $t_i := \sigma_i(t) \in \mathbb{Q}_3$ and $o(t_i)$ its valuation. Since $\mathrm{Tr}(t) = 1/(3\mathrm{d}_2)$, either $o(t_i) = -1$ for both $i = 1, 2$, or $o(t_i) \geq 0$ for exactly one of $i = 1, 2$. In the first case, it is easy to check that $W_{t_i}(s, \phi_\mu \otimes \phi_0)$ and $W_{t_i}(s, \phi_0 \otimes \phi_\mu)$ are identically zero by Proposition 5.7 in [Yang et al. 2019]. If we write $t_1 = (\delta - a)/(2\mathrm{d}_2 3\delta)$, $t_2 = (\delta + a)/(2\mathrm{d}_2 3\delta)$ with $a \in \mathbb{Z}_3$, then we must have $a \in 3\mathbb{Z}_3$ since $\delta^2 = D \in 1 + 3\mathbb{Z}_3$ and

$$-2 = o(t_1) + o(t_2) = o(t_1 t_2) = -2 + o(\delta^2 - a^2) = -2 + o(1 - a^2).$$

That means for $\mu_1 \in S_{-1}$ and $\mu_2 \in S_1$, we have

$$\alpha(\mu_1, t_1) = -\frac{3\mathrm{d}_2}{\delta}\mathrm{Nm}(\mu_1) - t_1 \equiv -\frac{\mathrm{d}_2}{3} - \frac{\delta - a}{2\mathrm{d}_2 3\delta} \equiv 0 \bmod \mathbb{Z}_3,$$
$$\alpha(\mu_2, t_2) = \frac{3\mathrm{d}_2}{\delta}\mathrm{Nm}(\mu_2) - t_2 \equiv -\frac{\mathrm{d}_2}{3} - \frac{\delta + a}{2\mathrm{d}_2 3\delta} \equiv 0 \bmod \mathbb{Z}_3.$$

By Proposition 5.3 in [Yang et al. 2019], $\gamma(W_3)^{-1} W_{t_i}(0, \phi_{\mu_1} \otimes \phi_{\mu_2}) = \frac{1}{16}$ for any $(\mu_1, \mu_2) \in S_{-1} \times S_1$. Since S_j has size 4 for $j = \pm 1$, we obtain

$$\frac{W_t(0, \phi_{\mathrm{d},3})}{\gamma(W_3)} = -1$$

when $v_3(\mathrm{Nm}(t)) = o(t_1) + o(t_2) = -2$.

In the second case, suppose $o(t_1) \geq 0$. Then Propositions 5.3 and 5.7 in [Yang et al. 2019] imply that $W_{t_i}(s, \phi_{\mu_1} \otimes \phi_{\mu_2})$ vanishes identically for $(\mu_1, \mu_2) \in S_{-1} \times S_1$ and

$$\frac{W_{t_1}^*(0, \phi_0)}{\gamma(W_{\mathfrak{p}_1})} = \frac{1 + (-1)^{o(t_1)-1}}{2}, \quad \frac{W_{t_2}^*(0, \phi_\mu)}{\gamma(W_{\mathfrak{p}_2})} = L(1, \chi_{\mathfrak{p}_2})3^{-1} = \frac{1}{4},$$

$$\frac{W^{*,\prime}_{t_1}(0,\phi_0)}{\gamma(W_{\mathfrak{p}_1})} = \frac{2o(t_1)+1}{2}\log(3) \qquad \text{when } 2 \mid o(t_1)$$

when $\mu \in S_1$ as $\alpha(\mu, t_2) = -(\mathrm{d}_2\mathrm{Nm}(\mu))/(3\delta) - t_2 \in \frac{\mathrm{d}_2}{3} - t_2 + \mathbb{Z}_3 = \mathbb{Z}_3$. Since $v_3(\mathrm{Nm}(t)) = o(t_1t_2) = o(t_1) - 1$, we obtain the lemma when $o(t_1) \geq 0$. The case $o(t_2) \geq 0$ holds similarly. □

Appendix

We record here the set $\kappa_{\mathrm{d},2}(N'_{\mathrm{d},2}) \subset \mathcal{A}_{\mathrm{d},2} = \mathbb{Z}/\mathrm{d}_2\mathbb{Z} \times \mathbb{Z}/2\mathrm{d}_2\mathbb{Z} \times \mathbb{Z}/2\mathrm{d}_2\mathbb{Z} \times \mathbb{Z}/\mathrm{d}_2\mathbb{Z}$. Note that the group $N'_{\mathrm{d},2}$ and the map $\mathrm{d}_3 \cdot \kappa_{\mathrm{d},2}$ only depend on d_2. This helps with checking Lemma 3.11.

$$\kappa_{1,2}(N'_{1,2}) = \kappa_{3,2}(N'_{3,2}) = \{[0,0]\}, \quad \kappa_{2,2}(N'_{2,2}) = \kappa_{6,2}(N'_{6,2}) = \{[1,0,0,1],[1,2,2,1]\},$$

$$\begin{aligned}&\kappa_{4,2}(N'_{4,2}) = \kappa_{12,2}(N'_{12,2}) = \\ &\quad \big\{[1,2,6,3],[1,6,2,3],[1,0,0,1],[1,4,4,1],[3,6,2,1],[3,2,6,1],[3,0,0,3],[3,4,4,3]\big\}.\end{aligned}$$

$$\begin{aligned}&\kappa_{8,2}(N'_{8,2}) = \\ &\Big\{[1,2,14,7],[1,6,10,7],[1,10,6,7],[1,14,2,7],[1,0,0,1],[1,4,12,1],[1,8,8,1],[1,12,4,1],\\ &[3,14,10,5],[3,2,6,5],[3,6,2,5],[3,10,14,5],[3,8,0,3],[3,12,12,3],[3,0,8,3],[3,4,4,3],\\ &[5,2,6,3],[5,6,2,3],[5,10,14,3],[5,14,10,3],[5,8,0,5],[5,12,12,5],[5,0,8,5],[5,4,4,5],\\ &[7,14,2,1],[7,2,14,1],[7,6,10,1],[7,10,6,1],[7,0,0,7],[7,4,12,7],[7,8,8,7],[7,12,4,7]\Big\}.\end{aligned}$$

$$\begin{aligned}&\kappa_{24,2}(N'_{24,2}) = \kappa_{24,2}(N'_{8,2}) = 3^{-1}\cdot\kappa_{8,2}(N'_{8,2}) = \\ &\Big\{[3,6,10,5],[3,2,14,5],[3,14,2,5],[3,10,6,5],[3,0,0,3],[3,12,4,3],[3,8,8,3],[3,4,12,3],\\ &[1,10,14,7],[1,6,2,7],[1,2,6,7],[1,14,10,7],[1,8,0,1],[1,4,4,1],[1,0,8,1],[1,12,12,1],\\ &[7,6,2,1],[7,2,6,1],[7,14,10,1],[7,10,14,1],[7,8,0,7],[7,4,4,7],[7,0,8,7],[7,12,12,7],\\ &[5,10,6,3],[5,6,10,3],[5,2,14,3],[5,14,2,3],[5,0,0,5],[5,12,4,5],[5,8,8,5],[5,4,12,5]\Big\}.\end{aligned}$$

Here we also include an explicit example for Theorem 1.7. Let $d_1 = -31$, $d_2 = -127$, which have class numbers 3 and 5 respectively and satisfy $d_j \equiv 17 \bmod 24$. Then the minimal polynomials of the invariants $f\big(\big[1, \frac{1}{2}(1+\sqrt{d_j})\big]\big)$ are

$$g_1(x) = x^3 + x - 1, \quad g_2(x) = x^5 - x^4 - 2x^3 + x^2 + 3x - 1. \tag{6-19}$$

Table 7 lists the values of $\mathfrak{F}(m)$ for various m. By the Gross–Zagier theorem, one obtains $J(d_1, d_2)$ by simply takes the product of all the numbers in the fourth column. For $f_s(d_1, d_2)$, one takes product of the entries $\mathfrak{F}\big(\frac{m}{4r^2}\big)$ over all the m's in the table and $r \mid s$ satisfying $m \equiv 4\cdot 19(d_1 + d_2 - 1) \bmod 4sr$. This congruence condition eliminates many entries, especially if s is large. For example, we have

$$f_{24}(d_1,d_2) = \left(\mathfrak{F}\Big(\frac{2^2 3^5}{4}\Big)\mathfrak{F}\Big(\frac{2^4 3^3}{4\cdot 2^2}\Big)\mathfrak{F}\Big(\frac{2^2 3^5}{4\cdot 3^2}\Big)\mathfrak{F}\Big(\frac{2^4 3^3}{4\cdot 6^2}\Big)\right)^{1/2} = 3^4$$

by Theorem 1.7. One can then immediately check that this is the absolute value of the resultant of the minimal polynomials g_1, g_2 in (6-19).

a	m	m mod 96	$\mathfrak{F}(m)$	$\mathfrak{F}\left(\frac{m}{2^2}\right)$	$\mathfrak{F}\left(\frac{m}{4^2}\right)$	$\mathfrak{F}\left(\frac{m}{8^2}\right)$	$\mathfrak{F}\left(\frac{m}{16^2}\right)$	$\mathfrak{F}\left(\frac{m}{6^2}\right)$	$\mathfrak{F}\left(\frac{m}{12^2}\right)$	$\mathfrak{F}\left(\frac{m}{24^2}\right)$	$\mathfrak{F}\left(\frac{m}{48^2}\right)$
1	$2^3 \cdot 3 \cdot 41$	24	3^8	3^4	1	1	1	1	1	1	1
3	$2 \cdot 491$	22	491^2	1	1	1	1	1	1	1	1
5	$2 \cdot 3 \cdot 163$	18	3^4	1	1	1	1	1	1	1	1
7	$2^2 \cdot 3^5$	12	3^9	3^3	1	1	1	3^2	1	1	1
9	$2^2 \cdot 241$	4	241^3	241	1	1	1	1	1	1	1
11	$2 \cdot 3^2 \cdot 53$	90	53^2	1	1	1	1	1	1	1	1
13	$2 \cdot 3 \cdot 157$	78	3^4	1	1	1	1	1	1	1	1
15	$2^5 \cdot 29$	64	29^6	29^4	29^2	1	1	1	1	1	1
17	$2^4 \cdot 3 \cdot 19$	48	3^{10}	3^6	3^2	1	1	1	1	1	1
19	$2 \cdot 3 \cdot 149$	30	3^4	1	1	1	1	1	1	1	1
21	$2 \cdot 19 \cdot 23$	10	23^4	1	1	1	1	1	1	1	1
23	$2^2 \cdot 3 \cdot 71$	84	3^6	3^2	1	1	1	1	1	1	1
25	$2^2 \cdot 3^2 \cdot 23$	60	23^3	23	1	1	1	23	1	1	1
27	$2 \cdot 401$	34	401^2	1	1	1	1	1	1	1	1
29	$2 \cdot 3^2 \cdot 43$	6	43^2	1	1	1	1	1	1	1	1
31	$2^3 \cdot 3 \cdot 31$	72	3^8	3^4	1	1	1	1	1	1	1
33	$2^3 \cdot 89$	40	89^4	89^2	1	1	1	1	1	1	1
35	$2 \cdot 3 \cdot 113$	6	3^4	1	1	1	1	1	1	1	1
37	$2 \cdot 3 \cdot 107$	66	3^4	1	1	1	1	1	1	1	1
39	$2^2 \cdot 151$	28	151^3	151	1	1	1	1	1	1	1
41	$2^2 \cdot 3 \cdot 47$	84	3^6	3^2	1	1	1	1	1	1	1
43	$2 \cdot 3^2 \cdot 29$	42	29^2	1	1	1	1	1	1	1	1
45	$2 \cdot 239$	94	239^2	1	1	1	1	1	1	1	1
47	$2^4 \cdot 3^3$	48	3^{10}	3^6	3^2	1	1	3^3	3	1	1
49	$2^7 \cdot 3$	0	3^8	3^6	3^4	3^2	1	1	1	1	1
51	$2 \cdot 167$	46	167^2	1	1	1	1	1	1	1	1
53	$2 \cdot 3 \cdot 47$	90	3^4	1	1	1	1	1	1	1	1
55	$2^2 \cdot 3 \cdot 19$	36	3^6	3^2	1	1	1	1	1	1	1
57	$2^2 \cdot 43$	76	43^3	43	1	1	1	1	1	1	1
59	$2 \cdot 3 \cdot 19$	18	3^4	1	1	1	1	1	1	1	1
61	$2 \cdot 3^3$	54	3^4	1	1	1	1	1	1	1	1

Table 7. Values of $\mathfrak{F}$ for $(d_1, d_2) = (-31, -127)$.

Acknowledgement

We thank Hongbo Yin for a careful reading and helpful comments of an earlier version of this paper.

References

[Atkin and Morain 1993] A. O. L. Atkin and F. Morain, "Elliptic curves and primality proving", *Math. Comp.* **61**:203 (1993), 29–68. MR Zbl

[Birch 1969] B. J. Birch, "Weber's class invariants", *Mathematika* **16** (1969), 283–294. MR Zbl

[Borcherds 1992] R. E. Borcherds, "Monstrous moonshine and monstrous Lie superalgebras", *Invent. Math.* **109**:2 (1992), 405–444. MR Zbl

[Borcherds 1998] R. E. Borcherds, "Automorphic forms with singularities on Grassmannians", *Invent. Math.* **132**:3 (1998), 491–562. MR Zbl

[Bruinier 2014] J. H. Bruinier, "On the converse theorem for Borcherds products", *J. Algebra* **397** (2014), 315–342. MR Zbl

[Bruinier et al. 2012] J. H. Bruinier, S. S. Kudla, and T. Yang, "Special values of Green functions at big CM points", *Int. Math. Res. Not.* **2012**:9 (2012), 1917–1967. MR Zbl

[Cox 1989] D. A. Cox, *Primes of the form x^2+ny^2: Fermat, class field theory and complex multiplication*, Wiley, New York, 1989. MR Zbl

[Gee 1999] A. Gee, "Class invariants by Shimura's reciprocity law", *J. Théor. Nombres Bordeaux* **11**:1 (1999), 45–72. MR Zbl

[Gross and Zagier 1985] B. H. Gross and D. B. Zagier, "On singular moduli", *J. Reine Angew. Math.* **355** (1985), 191–220. MR Zbl

[Howard and Yang 2012] B. Howard and T. Yang, *Intersections of Hirzebruch–Zagier divisors and CM cycles*, Lecture Notes in Math. **2041**, Springer, 2012. MR Zbl

[Kudla and Yang 2010] S. S. Kudla and T. Yang, "Eisenstein series for SL(2)", *Sci. China Math.* **53**:9 (2010), 2275–2316. MR Zbl

[Li 2018] Y. Li, "Singular units and isogenies between CM elliptic curves", preprint, 2018. arXiv

[Li and Yang $\geq$ 2021] Y. Li and T. Yang, "On a conjecture of Yui and Zagier, II", in preparation.

[Milas 2007] A. Milas, "Characters, supercharacters and Weber modular functions", *J. Reine Angew. Math.* **608** (2007), 35–64. MR Zbl

[Roskam 2003] H. Roskam, "On singular moduli for level 2 and 3", preprint, 2003. arXiv

[Sage 2019] W. A. Stein et al., "Sage mathematics software", 2019, available at http://www.sagemath.org. Version 8.8.

[Scheithauer 2008] N. R. Scheithauer, "Generalized Kac–Moody algebras, automorphic forms and Conway's group, II", *J. Reine Angew. Math.* **625** (2008), 125–154. MR Zbl

[Schofer 2009] J. Schofer, "Borcherds forms and generalizations of singular moduli", *J. Reine Angew. Math.* **629** (2009), 1–36. MR Zbl

[Weber 1908] H. Weber, *Lehrbuch der Algebra, III: Elliptische Funktionen und algebraische Zahlen*, 2nd ed., Vieweg & Sohn, Braunschweig, Germany, 1908. Zbl

[Yang 2005] T. Yang, "CM number fields and modular forms", *Pure Appl. Math. Q.* **1**:2 (2005), 305–340. MR Zbl

[Yang and Yin 2016] T. Yang and H. Yin, "Some non-congruence subgroups and the associated modular curves", *J. Number Theory* **161** (2016), 17–48. MR Zbl

[Yang and Yin 2019] T. Yang and H. Yin, "Difference of modular functions and their CM value factorization", *Trans. Amer. Math. Soc.* **371**:5 (2019), 3451–3482. MR Zbl

[Yang et al. 2019] T. Yang, H. Yin, and P. Yu, "The lambda invariants at CM points", *Int. Math. Res. Not.* (online publication November 2019).

[Yui and Zagier 1997] N. Yui and D. Zagier, "On the singular values of Weber modular functions", *Math. Comp.* **66**:220 (1997), 1645–1662. MR Zbl

Communicated by Richard Borcherds
Received 2019-12-17 Accepted 2020-03-25

li@mathematik.tu-darmstadt.de *Technische Universität Darmstadt, Darmstadt, Germany*

thyang@math.wisc.edu *University of Wisconsin, Madison, Madison, WI, United States*

ALGEBRA AND NUMBER THEORY 14:8 (2020)
https://doi.org/10.2140/ant.2020.14.2239

On iterated product sets with shifts, II

Brandon Hanson, Oliver Roche-Newton and Dmitrii Zhelezov

The main result of this paper is the following: for all $b \in \mathbb{Z}$ there exists $k = k(b)$ such that

$$\max\{|A^{(k)}|, |(A+u)^{(k)}|\} \geq |A|^b,$$

for any finite $A \subset \mathbb{Q}$ and any nonzero $u \in \mathbb{Q}$. Here, $|A^{(k)}|$ denotes the k-fold product set $\{a_1 \cdots a_k : a_1, \dots, a_k \in A\}$.

Furthermore, our method of proof also gives the following l_∞ sum-product estimate. For all $\gamma > 0$ there exists a constant $C = C(\gamma)$ such that for any $A \subset \mathbb{Q}$ with $|AA| \leq K|A|$ and any $c_1, c_2 \in \mathbb{Q} \setminus \{0\}$, there are at most $K^C|A|^\gamma$ solutions to

$$c_1x + c_2y = 1, \quad (x, y) \in A \times A.$$

In particular, this result gives a strong bound when $K = |A|^\epsilon$, provided that $\epsilon > 0$ is sufficiently small, and thus improves on previous bounds obtained via the Subspace Theorem.

In further applications we give a partial structure theorem for point sets which determine many incidences and prove that sum sets grow arbitrarily large by taking sufficiently many products.

We utilize a query-complexity analogue of the polynomial Freiman–Ruzsa conjecture, due to Pälvölgyi and Zhelezov (2020). This new tool replaces the role of the complicated setup of Bourgain and Chang (2004), which we had previously used. Furthermore, there is a better quantitative dependence between the parameters.

1. Introduction

1.1. ***Background and statement of main results.*** Let A be a finite set of rational numbers and let $u \in \mathbb{Q}$ be nonzero. In this article we wish to investigate the sizes of the k-fold product sets

$$A^{(k)} := \{a_1 \cdots a_k : a_1, \dots, a_k \in A\} \quad \text{and} \quad (A+u)^{(k)} = \{(a_1+u) \cdots (a_k+u) : a_1, \dots, a_k \in A\}.$$

This is an instance of a sum-product problem. Recall that the Erdős and Szemerédi [1983] sum-product conjecture states that, for all $\epsilon > 0$ there exists a constant $c(\epsilon) > 0$ such that

$$\max\{|A+A|, |AA|\} \geq c(\varepsilon)|A|^{2-\varepsilon}$$

holds for any $A \subset \mathbb{Z}$. Here $A + A := \{a + b : a, b \in A\}$ is the *sum set* of A, and AA is another notation for $A^{(2)}$. Erdős and Szemerédi also made the more general conjecture that for any finite $A \subset \mathbb{Z}$,

$$\max\{|kA|, |A^k|\} \geq c(\epsilon)|A|^{k-\epsilon},$$

MSC2010: primary 11B99; secondary 11D72.
Keywords: sum-product problem, S-units, weak Erdős–Szemerédi, unbounded growth conjecture, subspace theorem.

where $kA := \{a_1 + \cdots + a_k : a_1, \ldots, a_k \in A\}$ is the *k-fold sum set*. Both of these conjectures are wide open, and it is natural to also consider them for the case when A is a subset of $\mathbb{R}$ or indeed other fields. The case when $k = 2$ has attracted the most interest. See, for example, [Konyagin and Shkredov 2015; 2016; Solymosi 2009; Tao and Vu 2006] for more background on the original Erdős–Szemerédi sum-product problem.

Most relevant to our problem is the case of general (large) k. Little is known about the Erdős–Szemerédi conjecture in this setting, with the exception of the remarkable series of work of Chang [2003] and Bourgain and Chang [2004]. This culminated in the main theorem of [Bourgain and Chang 2004]: for all $b \in \mathbb{R}$ there exists $k = k(b) \in \mathbb{Z}$ such that

$$\max\{|kA|, |A^k|\} \geq |A|^b \tag{1}$$

holds for any $A \subset \mathbb{Q}$. On the other hand, it appears that we are not close to proving such a strong result for $A \subset \mathbb{R}$.

In the same spirit as the Erdős–Szemerédi conjecture, it is expected that an additive shift will destroy multiplicative structure present in A. In particular, one expects that, for a nonzero u, at least one of $|A^{(k)}|$ or $|(A+u)^{(k)}|$ is large. The $k = 2$ version of this problem was considered in [Garaev and Shen 2010] and [Jones and Roche-Newton 2013]. The main result of this paper is the following analogue of the Bourgain–Chang theorem.

Theorem 1.1. *For all $b \in \mathbb{Z}$, there exists $k = k(b)$ such that for any finite set $A \subset \mathbb{Q}$ and any nonzero rational u,*

$$\max\{|A^k|, |(A+u)^k|\} \geq |A|^b.$$

This paper is a sequel to [Hanson et al. 2019], in which the main result was the following:

Theorem 1.2. *For any finite set $A \subset \mathbb{Q}$ with $|AA| \leq K|A|$, any nonzero $u \in \mathbb{Q}$ and any positive integer k,*

$$|(A+u)^{(k)}| \geq \frac{|A|^k}{(8k^4)^{kK}}.$$

The proof of this result was based on an argument that Chang [2003] introduced to give similar bounds for the k-fold sum set of a set with small product set. Theorem 1.2 is essentially optimal when K is of the order $c \log|A|$, for a sufficiently small constant $c = c(k)$. However, the result becomes trivial when K is larger, for example if $K = |A|^\epsilon$ and $\varepsilon > 0$. The bulk of this paper is devoted to proving the following theorem, which gives a near optimal bound for the size of $(A+u)^{(k)}$ when $K = |A|^\varepsilon$, for a sufficiently small but positive ε.

Theorem 1.3. *Given $0 < \gamma < \frac{1}{2}$, there exists a positive constant $C = C(\gamma, k)$ such that for any finite $A \subset \mathbb{Q}$ with $|AA| = K|A|$ and any nonzero rational u,*

$$|(A+u)^{(k)}| \geq \frac{|A|^{k(1-\gamma)-1}}{K^{Ck}}.$$

In fact, we prove a more general version of Theorem 1.3 in terms of certain weighted energies and so-called Λ-constants (see Theorem 3.6 for the general statement that implies Theorem 1.3 — see Sections 2 and 3 for the relevant definitions of energy and Λ-constants). This more general result is what allows us to deduce Theorem 1.1.

1.2. ***A subspace type theorem — an l_∞ sum-product estimate.*** It appears that Theorem 1.1, as well as the forthcoming generalized form of Theorem 1.3, lead to some interesting new applications. To illustrate the strength of these sum-product results, we present three applications in this paper.

Our main application concerns a variant of the celebrated subspace theorem by Evertse, Schmidt and Schlikewei [Evertse et al. 2002] which, after quantitative improvements by Amoroso and Viada [2009], reads as follows: Suppose $a_1, \dots, a_k \in \mathbb{C}^*$, $\alpha_1, \dots, \alpha_r \in \mathbb{C}^*$ and define

$$\Gamma = \{\alpha_1^{z_1} \cdots \alpha_r^{z_r}, z_i \in \mathbb{Z}\},$$

so Γ is a free multiplicative group of rank r.[1] Consider the equation

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = 1 \tag{2}$$

with $a_i \in \mathbb{C}^*$ viewed as fixed coefficients and $x_i \in \Gamma$ as variables. A solution $(x_1, \dots, x_k)$ to (2) is called *nondegenerate* if for any nonempty $J \subsetneq \{1, \dots, k\}$

$$\sum_{i \in J} a_i x_i \neq 0.$$

Theorem 1.4 (the subspace theorem [Evertse et al. 2002; Amoroso and Viada 2009]). *The number $A(k, r)$ of nondegenerate solutions to* (2) *satisfies the bound*

$$A(k, r) \leq (8k)^{4k^4(k+kr+1)}. \tag{3}$$

The subspace theorem dovetails nicely to the following version of the Freiman lemma.

Theorem 1.5. *Let $(G, \cdot)$ be a torsion-free abelian group and $A \subset G$ with $|AA| < K|A|$. Then A is contained in a subgroup $G' < G$ of rank at most K.*

Now assume for simplicity that $A \subset \mathbb{Q}$ and $|AA| \leq K|A|$. Let us call such sets (this definition generalizes of course to an arbitrary ambient group) *K-almost subgroups*.[2]

We now show that it is natural to expect that the subspace theorem generalizes to K-almost subgroups with K taken as a proxy for the group rank. A straightforward corollary of Theorems 1.5 and 1.4 is as follows.

[1] The original theorem is formulated in a more general setting, namely for the division group of Γ, but we will stick to the current formulation for simplicity.

[2] One could have used a more general framework of *K-approximate subgroups* introduced by Tao. We decided to introduce a simpler definition in order to avoid technicalities. However, in the abelian setting the definitions are essentially equivalent.

Corollary 1.6 (subspace theorem for K-almost subgroups). *Let A be a K-almost subgroup. Then the number $A(k, K)$ of nondegenerate solutions $(x_1, x_2, \dots, x_k) \in A^k$ to*

$$c_1x_1 + c_2x_2 + \cdots + c_kx_k = 1$$

with fixed coefficients $c_i \in \mathbb{C}^*$ is bounded by

$$A(k, K) \leq (8k)^{4k^4(k+kK+1)}.$$

Similarly to (1), the bound of Corollary 1.6 becomes trivial when A is large and K is larger than $c \log|A|$ for some small $c > 0$.

We conjecture that a much stronger polynomial bound holds.

Conjecture 1. There is a constant $c(k)$ such that Corollary 1.6 holds with the bound

$$A(k, K) \leq K^{c(k)}.$$

We can support Conjecture 1 with a special case $k = 2$ and $A \subset \mathbb{Q}$, $c_i \in \mathbb{Q}$ and a somewhat weaker estimate, which we see as a proxy for the Beukers–Schlikewei theorem [Beukers and Schlickewei 1996].

Theorem 1.7 (weak Beukers–Schlikewei for K-almost subgroups). *For any $\gamma > 0$ there is $C(\gamma) > 0$ such that for any K-almost subgroup $A \subset \mathbb{Q}$ and fixed nonzero $c_1, c_2 \in \mathbb{Q}$ the number $A(2, K)$ of solutions $(x_1, x_2) \in A^2$ to*

$$c_1x_1 + c_2x_2 = 1$$

is bounded by

$$A(2, K) \leq |A|^{\gamma} K^C.$$

One can view Theorem 1.7 as an l_∞ version of the weak Erdős–Szemerédi sum-product conjecture. The *weak Erdős–Szemerédi conjecture* is the statement that, if $|AA| \leq K|A|$ then $|A + A| \geq K^{-C}|A|^2$ for some positive absolute constant C. For $A \subset \mathbb{Z}$, this result was proved in [Bourgain and Chang 2004], but the conjecture remains open over the reals.

A common approach to proving sum-product estimates is to attempt to show that, for a set A with small product set, the *additive energy* of A, which is defined as the quantity

$$E_+(A) := |\{(a, b, c, d) \in A^4 : a + b = c + d\}|,$$

is small. Indeed, this was the strategy implemented in [Chang 2003] and [Bourgain and Chang 2004], the latter of which showed that,[3] for all $\gamma > 0$, there is a constant $C = C(\gamma)$ such that for any $A \subset \mathbb{Q}$ with $|AA| \leq K|A|$,

$$E_+(A) \leq K^C|A|^{2+\gamma}. \tag{4}$$

[3] This is something of an over-simplification, as [Bourgain and Chang 2004] in fact proved a much more general result which bounded the multifold additive energy with weights attached.

Since there are at least $|A|^2$ trivial solutions when $\{a, b\} = \{c, d\}$, this bound is close to best possible. It then follows from a standard application of the Cauchy–Schwarz inequality that

$$|A + A| \geq \frac{|A|^{2-\gamma}}{K^C}.$$

Defining the representation function $r_{A+A}(c) = |\{(a_1, a_2) \in A \times A : a_1 + a_2 = c\}|$, it follows that

$$E_+(A) = \sum_x r_{A+A}(x)^2,$$

and so bounds for the additive energy can be viewed as l_2 estimates for this representation function.

Theorem 1.7 gives the stronger l_∞ estimate: it says that, if $|AA| \leq K|A|$ then $r_{A+A}(c) \leq K^C|A|^\gamma$ for all $c \neq 0$. This implies (4), and thus in turn the weak Erdős–Szemerédi sum-product conjecture. We prove Theorem 1.7 in Section 4.

Remark. It is highly probable that our method can be combined with the ideas of [Bourgain and Chang 2009] which would generalize Theorem 1.7 to K-almost subgroups consisting of algebraic numbers of degree at most d (though not necessarily contained in the same field extension). The upper power C is going to depend on d then, so the putative bound (using the notation of Theorem 1.7) is

$$A(2, K) \leq C'(d)|A|^\gamma K^{C(\gamma,d)}$$

with some $C, C' > 0$. We are going to consider this matter in detail elsewhere. Note, however, that proving a similar statement with no dependence on d seems to be a significantly harder problem.

1.3. *Further applications.*

1.3.1. *An inverse Szemerédi–Trotter theorem.* Theorem 1.7 can be interpreted as a partial inverse to the Szemerédi–Trotter theorem. The Szemerédi–Trotter theorem states that, if P is a finite set of points and L is a finite set of lines in $\mathbb{R}^2$, then the number of incidences $I(P, L)$ between P and L satisfies the bound

$$I(P, L) := |\{(p, l) \in P \times L : p \in l\}| = O(|P|^{2/3}|L|^{2/3} + |P| + |L|). \tag{5}$$

The term $|P|^{2/3}|L|^{2/3}$ above is dominant unless the sizes of P and L are rather imbalanced. The Szemerédi–Trotter theorem is tight, up to the multiplicative constant.

It is natural to consider the inverse question: for what sets P and L is it possible that $I(P, L) = \Omega(|P|^{2/3}|L|^{2/3})$? The known constructions of point sets which attain many incidences appear to all have some kind of lattice like structure. This perhaps suggests the loose conjecture that point sets attaining many incidences must always have some kind of additive structure, although such a conjecture seems to be far out of reach to the known methods.

However, with an additional restriction that $P = A \times A$ with $A \subset \mathbb{Q}$, Theorem 1.1 leads to the following partial inverse theorem, which states that if A has small product set then $I(P, L)$ cannot be maximal.

Theorem 1.8. *For all $\gamma \geq 0$ there exists a constant $C = C(\gamma)$ such that the following holds. Let A be a finite set of rationals such that $|AA| \leq K|A|$ and let $P = A \times A$. Then, for any finite set L of lines in the plane, $I(P, L) \leq 3|P| + |A|^{\gamma} K^{C} |L|$.*

In fact, not only does this show that $I(A \times A, L)$ cannot be maximal when $|AA|$ is small, but better still the number of incidences is almost bounded by the trivial linear terms in (5). The insistence that the point set is a direct product is rather restrictive. However, since many applications of the Szemerédi–Trotter Theorem make use of direct products, it seems likely that Theorem 1.8 could be useful. The proof is given in Section 5.

1.3.2. *Improved bound for the size of an additive basis of a set with small product set.* Theorem 1.7 also yields the following application concerning the problem of bounding the size of an additive basis considered in [Shkredov and Zhelezov 2018]. We can significantly improve the bound in the rational setting, pushing the exponent in (6) from $\frac{1}{2} + \frac{1}{442} - o_{\epsilon}(1)$ to $\frac{2}{3} - o_{\epsilon}(1)$ in the limiting case $K = |A|^{\epsilon}$.

Theorem 1.9. *For any $\gamma > 0$ there exists $C(\gamma)$ such that for an arbitrary $A \subset \mathbb{Q}$ with $|AA| = K|A|$ and $B, B' \subset \mathbb{Q}$,*

$$S := |\{(b, b') \in B \times B' : b + b' \in A\}| \leq 2|A|^{\gamma} K^{C} \min\{|B|^{1/2}|B'| + |B|, |B'|^{1/2}|B| + |B'|\}.$$

In particular, for any $\gamma > 0$ there exists $C(\gamma)$ such that if $A \subset B + B$ then

$$|B| \geq |A|^{2/3-\gamma} K^{-C}. \tag{6}$$

The proof of Theorem 1.9 is given in Section 5.

Remark. During the preparation of the manuscript we became aware that Cosmin Pohoata has independently proved Theorem 1.9 using an earlier result of Chang and by a somewhat different method.

1.3.3. *Unlimited growth for products of difference sets.* It was conjectured in [Balog et al. 2017] that for any $b \in \mathbb{R}$ there exists $k = k(b) \in \mathbb{N}$ such that for all $A \subset \mathbb{R}$

$$|(A - A)^{k}| \geq |A|^{b}.$$

In another application of Theorem 1.1, we give a positive answer to this question under the additional restriction that $A \subset \mathbb{Q}$. In fact, we prove the following stronger statement.

Theorem 1.10. *For any $b \in \mathbb{R}$ there exists $k = k(b) \in \mathbb{N}$ such that for all $A \subset \mathbb{Q}$ and $B \subset \mathbb{Q}$ with $|B| \geq 2$,*

$$|(A + B)^{k}| \geq |A|^{b}.$$

The proof is given in Section 5.

1.4. ***Asymptotic notation.*** Throughout the paper, the standard notation $\ll$, $\gg$ is applied to positive quantities in the usual way. Saying $X \gg Y$ or $Y \ll X$ means that $X \geq cY$, for some absolute constant $c > 0$. The expression $X \approx Y$ means that both $X \gg Y$ and $X \ll Y$ hold.

1.5. ***The structure of the rest of this paper.*** In Section 2, we introduce a new kind of mixed energy, and establish some initial bounds on this energy which are strong when the set A is defined by relatively few primes ($c \log|A|$ for a sufficiently small constant c). The structure of these arguments are similar to those introduced by Chang [2003], and also used by the authors in [Hanson et al. 2019].

The goal of Section 3 is to prove the main technical result of the paper, Theorem 3.6. The statement uses the language of Λ-constants, which is a robust generalization of additive energy, and so we must first define what these constants are and identify some of their crucial properties. We also introduce the notion of query complexity, which is nicely tuned in to the techniques used and results established in Section 2. An essential tool in converting the bounds from Section 2 into strong bounds for Λ-constants is a deep new result of Zhelezov and Pálvölgyi [2020].

In Section 4, we use Theorem 3.6 to conclude the proofs of the main results of this paper, Theorems 1.1, 1.3 and 1.7. Finally, in Section 5, we give proofs of further applications of our main results.

2. A Chang-type bound for the mixed energy

Different kinds of energies play a pivotal role in the work of Chang [2003] and Bourgain and Chang [2004], as well as [Hanson et al. 2019]. In [Chang 2003], it was proved that, for any finite set of rationals A with $|AA| \leq K|A|$, the *k-fold additive energy*, which is defined as the number of solutions to

$$a_1 + \cdots + a_k = a_{k+1} + \cdots a_{2k}, \quad (a_1, \dots, a_{2k}) \in A^{2k}, \tag{7}$$

is at most $(2k^2 - k)^{kK}|A|^k$. A simple application of the Cauchy–Schwarz inequality then implies that the *k-fold sum set* satisfies the bound

$$|kA| \geq \frac{|A|^k}{(2k^2 - k)^{kK}}.$$

Bound (7) is close to optimal when $K = c \log|A|$, but becomes trivial when $K = |A|^{\varepsilon}$. In [Bourgain and Chang 2004], (a weighted version of) this bound was used as a foundation, and developed considerably courtesy of some intricate decoupling arguments, in order to prove a bound for the k-fold additive energy which remains very strong when K is of the order $|A|^{\varepsilon}$.

In [Hanson et al. 2019], we followed a similarly strategy to that of [Chang 2003], proving that for any finite set of rationals A with $|AA| \leq K|A|$ and any nonzero rational u, the *k-fold multiplicative energy* of $A + u$, which is defined as the number of solutions to

$$(a_1 + u) \cdots (a_k + u) = (a_{k+1} + u) \cdots (a_{2k} + u), \quad (a_1, \dots, a_{2k}) \in A^{2k}, \tag{8}$$

is at most $(Ck^2)^{kK}|A|^k$. Unfortunately, in adapting the approach of [Chang 2003] in order to bound the number of solutions to (8) in [Hanson et al. 2019], we encountered some difficulties with dilation invariance which made the argument rather more complicated, and we were unable to marry our methods with those of [Bourgain and Chang 2004] to obtain a strong bound when K is of order $|A|^{\varepsilon}$.

In this paper, we modify the approach of [Hanson et al. 2019] by working with a different form of energy. Consider the following representation function:

$$r_k(x,y) = |\{(a_1,\dots,a_k)\in A^k : a_1\cdots a_k = x,\ (a_1+u)\cdots(a_k+u)=y\}|.$$

Then, because r_k is supported on $A^{(k)}\times(A+u)^{(k)}$, it follows from the Cauchy–Schwarz inequality that

$$|A|^{2k} = \biggl(\sum_{(x,y)\in A^{(k)}\times(A+u)^{(k)}} r_k(x,y)\biggr)^2 \le |A^{(k)}||(A+u)^{(k)}| \sum_{(x,y)\in A^{(k)}\times(A+u)^{(k)}} r_k(x,y)^2. \tag{9}$$

The latter sum is the quantity

$$\tilde{E}_k(A;u) := \biggl|\biggl\{(a_1,\dots,a_k,b_1,\dots,b_k)\in A^{2k} : \prod_{i=1}^k a_i = \prod_{i=1}^k b_i,\ \prod_{i=1}^k (a_i+u) = \prod_{i=1}^k (b_i+u)\biggr\}\biggr|.$$

We summarize this in the following lemma.

Lemma 2.1. *For any finite set $A\subset\mathbb{R}$, any $u\in\mathbb{R}\setminus\{0\}$ and any integer $k\ge 2$, we have*

$$|A|^{2k} \le |A^{(k)}||(A+u)^{(k)}|\tilde{E}_k(A;u).$$

In particular,

$$\frac{|A|^k}{\tilde{E}_k(A;u)^{1/2}} \le \max\{|A^{(k)}|, |(A+u)^{(k)}|\}.$$

Our goal is to estimate this energy and to show that, at least for sets of rationals, it cannot ever be too big.

In this section we seek to give an initial upper bound for $\tilde{E}_k(A;u)$. The strategy is close to that of Chang [2003]. There are also clear similarities with the prequel to this paper [Hanson et al. 2019].

To do this, as in [Hanson et al. 2019], we will write $\tilde{E}_k(A;u)$ in terms of Dirichlet polynomials. In this case, our Dirichlet polynomials will be functions of the form

$$F(s_1,s_2) = \sum_{(a,b)\in\mathbb{Q}^2} \frac{f(a,b)}{a^{s_1}b^{s_2}}$$

where $f:\mathbb{Q}^2\to\mathbb{C}$ is some function of finite support. It will also be more convenient to count weighted energy. For w_a a sequence of nonnegative weights on A, let

$$\tilde{E}_{k,w}(A;u) = \sum_{\substack{a_1\cdots a_k = b_1\cdots b_k\\ (a_1+u)\cdots(a_k+u)=(b_1+u)\cdots(b_k+u)}} w_{a_1}\cdots w_{a_k}w_{b_1}\cdots w_{b_k}.$$

Lemma 2.2. *Let A be a finite set of rational numbers and let u be a nonzero rational number. Then, for any integer $k\ge 2$, we have*

$$\tilde{E}_{k,w}(A;u) = \lim_{T\to\infty}\frac{1}{T^2}\int_0^T\int_0^T \biggl|\sum_{a\in A} w_a a^{it_1}(a+u)^{it_2}\biggr|^{2k} dt_1 dt_2.$$

Proof. Expanding, the double integral on the right hand side is equal to

$$\sum_{a_1,\dots,a_k\in A}\sum_{b_1,\dots,b_k\in A} w_{a_1}\cdots w_{a_k}w_{b_1}\cdots w_{b_k}$$
$$\cdot\int_0^T (a_1\cdots a_k b_1^{-1}\cdots b_k^{-1})^{it_1}\,dt_1\int_0^T((a_1+u)\cdots(a_k+u)(b_1+u)^{-1}\cdots(b_k+u)^{-1})^{it_2}\,dt_2.$$

Now

$$\frac{1}{T}\int_0^T (u/v)^{it}\,dt=\begin{cases}1 & \text{if } u=v,\\ O_{u,v}(T^{-1}) & \text{if } u\neq v.\end{cases}$$

From this, the lemma follows. □

Let $\|\cdot\|_{2k}$ be the standard norm in $L^{2k}([0,T]^2)$, normalized such that $\|1\|_{2k}=1$. So,

$$\|f\|_{2k}:=\left(\frac{1}{T^2}\int_0^T\int_0^T|f(t)|^{2k}dt\right)^{1/2k}.$$

Lemma 2.3. *Let $\mathcal{J}$ be a set of integers and decompose it as $\mathcal{J}=\mathcal{J}_1\cup\cdots\cup\mathcal{J}_N$. For each $j\in\mathcal{J}$ let $f_j:\mathbb{R}\times\mathbb{R}\to\mathbb{C}$ be a function belonging to $L^{2k}(\mathbb{R}^2)$ for every integer $k\ge 2$. Then, for every integer $k\ge 2$,*

$$\lim_{T\to\infty}\left(\frac{1}{T^2}\int_0^T\int_0^T\left|\sum_{j\in\mathcal{J}}f_j(t_1,t_2)\right|^{2k}dt_1dt_2\right)^{1/k}$$
$$\le N\sum_{n=1}^{N}\lim_{T\to\infty}\left(\frac{1}{T^2}\int_0^T\int_0^T\left|\sum_{j\in\mathcal{J}_n}f_j(t_1,t_2)\right|^{2k}dt_1dt_2\right)^{1/k}. \quad (10)$$

Proof. It suffices to prove the inequality for all sufficiently large T, which we assume fixed for now. Then

$$\left(\frac{1}{T^2}\int_0^T\int_0^T\left|\sum_{j\in\mathcal{J}}f_j(t_1,t_2)\right|^{2k}dt_1dt_2\right)^{1/k}=\left(\left\|\sum_{n=1}^{N}\sum_{j\in\mathcal{J}_n}f_j\right\|_{2k}\right)^2\le\left(\sum_{n=1}^{N}\left\|\sum_{j\in\mathcal{J}_n}f_j\right\|_{2k}\right)^2, \quad (11)$$

by the triangle inequality. By the Cauchy–Schwarz inequality, (11) is bounded by

$$N\sum_{n=1}^{N}\left\|\sum_{j\in\mathcal{J}_n}f_j\right\|_{2k}^2. \quad (12)$$

Letting $T\to\infty$ we get the claim of the lemma. □

Corollary 2.4. *Let A be a finite set of rational numbers, partitioned as $A=A_1\cup\cdots\cup A_N$, let w be a set of nonnegative weights, and let u be a nonzero rational number. Then for any integer $k\ge 2$*

$$\tilde{E}_{k,w}(A;u)^{1/k}\le N\sum_{j=1}^{N}\tilde{E}_{k,w}(A_j;u)^{1/k}.$$

Now let p be a fixed prime. For $a\in\mathbb{Q}$, let $v_p(a)$ denote the p-adic valuation of a. For a set A of rational numbers and an integer t, we let $A_t=\{a\in A:v_p(a)=t\}$.

Lemma 2.5. *Let p be a prime number. Suppose A is a finite set of rational numbers and let u be a nonzero rational number. Then for any w, a set of nonnegative weights on A, and any integer $k \geq 2$,*

$$\tilde{E}_{k,w}(A;u)^{1/k} \leq 2\binom{2k}{2}\sum_{d\in\mathbb{Z}} \tilde{E}_{k,w}(A_d;u)^{1/k}.$$

Proof. First, let $A = A_+ \cup A_-$ where $A_+ = \{a \in A : v_p(a) \geq v_p(u)\}$ and $A_- = \{a \in A : v_p(a) < v_p(u)\}$. By Corollary 2.4, we have

$$\tilde{E}_{k,w}(A;u)^{1/k} \leq 2\tilde{E}_{k,w}(A_+;u)^{1/k} + 2\tilde{E}_{k,w}(A_-;u)^{1/k}. \tag{13}$$

These two terms will be dealt with in turn, starting with $E_{k,w}(A_+;u)^{1/k}$. To do this, we first set up some more notation. For an integer d, define the function

$$f_d(t_1,t_2) := \sum_{a\in A_d} w_a a^{it_1}(a+u)^{it_2}.$$

Then, by Lemma 2.2

$$\tilde{E}_{k,w}(A_+;u) = \lim_{T\to\infty}\frac{1}{T^2}\int_0^T\int_0^T\left|\sum_{d\geq v_p(u)} f_d(t_1,t_2)\right|^{2k} dt_1dt_2.$$

Expanding this expression, as in the proof of Lemma 2.2, we obtain that $\tilde{E}_{k,w}(A_+;u)$ is equal to

$$\sum_{d_1,\dots,d_{2k}\geq v_p(u)} \lim_{T\to\infty}\frac{1}{T^2}\int_0^T\int_0^T f_{d_1}(t_1,t_2)\cdots f_{d_k}(t_1,t_2)\overline{f_{d_{k+1}}(t_1,t_2)}\cdots\overline{f_{d_{2k}}(t_1,t_2)}\,dt_1dt_2. \tag{14}$$

For fixed $d_1,\dots,d_{2k}$, the quantity

$$\lim_{T\to\infty}\frac{1}{T^2}\int_0^T\int_0^T f_{d_1}(t_1,t_2)\cdots f_{d_k}(t_1,t_2)\overline{f_{d_{k+1}}(t_1,t_2)}\cdots\overline{f_{d_{2k}}(t_1,t_2)}\,dt_1dt_2.$$

gives a weighted count of the number of solutions to the system of simultaneous equations

$$a_1\cdots a_k = a_{k+1}\cdots a_{2k} \tag{15}$$

$$(a_1+u)\cdots(a_k+u) = (a_{k+1}+u)\cdots(a_{2k}+u), \tag{16}$$

such that $a_i \in A_{d_i}$.

We claim that there are no solutions to (16), and thus also no solutions to the above system, if all of the d_i are distinct. Indeed, suppose we have a solution

$$(a_1+u)\cdots(a_k+u) = (a_{k+1}+u)\cdots(a_{2k}+u)$$

and so

$$(a_1u^{-1}+1)\cdots(a_ku^{-1}+1) = (b_{k+1}u^{-1}+1)\cdots(b_{2k}u^{-1}+1). \tag{17}$$

Since $v_p(a_iu^{-1}) \geq 0$, expanding out both sides of (17) and simplifying gives

$$u^{-1}(a_1+\cdots+a_k) + \text{higher terms} = u^{-1}(b_{k+1}+\cdots+b_{2k}) + \text{higher terms}. \tag{18}$$

If all of the d_i are distinct, then there is some unique smallest d_i, and thus a unique smallest value of $v_p(a_i)$. But then the left hand side and the right hand side are divisible by distinct powers of p, a contradiction.

So returning to (14), we need only consider the cases in which one or more of the d_i are repeated. There are three kinds of ways in which this can happen:

(1) $d_i = d_i'$ with $1 \le i \le k$ and $k+1 \le i' \le 2k$. There are k^2 possible positions for such a pair (i, i').

(2) $d_i = d_i'$ with $1 \le i, i' \le k$. There are $\binom{k}{2}$ possible positions for such a pair (i, i').

(3) $d_i = d_i'$ with $k+1 \le i, i' \le 2k$. There are $\binom{k}{2}$ possible positions for such a pair (i, i').

Suppose we are in situation (1) above. Specifically, suppose that $d_1 = d_{2k}$. The other $k^2 - 1$ cases can be dealt with by the same argument. Then these terms in (14) can be rewritten as

$$\begin{aligned}\sum_{d_1 \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T & f_{d_1}(t_1, t_2)\overline{f_{d_1}(t_1, t_2)} \\ & \sum_{d_2,\dots,d_{2k-1} \ge v_p(u)} f_{d_2}(t_1, t_2) \cdots f_{d_k}(t_1, t_2)\overline{f_{d_{k+1}}(t_1, t_2)} \cdots \overline{f_{d_{2k-1}}(t_1, t_2)}\, dt_1 dt_2 \\ & = \sum_{d \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1, t_2)|^2 \Big| \sum_{d \ge v_p(u)} f_d(t_1, t_2)\Big|^{2(k-1)} dt_1 dt_2. \quad (19)\end{aligned}$$

Suppose we are in situation (2). Specifically, suppose that $d_1 = d_2$. The other $\binom{k}{2} - 1$ cases can be dealt with by the same argument. Then these terms in (14) can be rewritten as

$$\begin{aligned}\sum_{d_1 \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T f_{d_1}^2(t_1, t_2) & \sum_{d_3,\dots,d_{2k} \ge v_p(u)} f_{d_3}(t_1, t_2) \cdots f_{d_k}(t_1, t_2)\overline{f_{d_{k+1}}(t_1, t_2)} \cdots \overline{f_{d_{2k}}(t_1, t_2)}\, dt_1 dt_2 \\ & \le \sum_{d \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1, t_2)|^2 \Big| \sum_{d \ge v_p(u)} f_d(t_1, t_2)\Big|^{k-2} \Big| \sum_{d} f_d(t_{\bar{1}}, t_2)\Big|^{k} dt_1 dt_2 \\ & = \sum_{d \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1, t_2)|^2 \Big| \sum_{d \ge v_p(u)} f_d(t_1, t_2)\Big|^{2(k-1)} dt_1 dt_2.\end{aligned}$$

The same argument also works in case (3). Returning to (14), we then have

$$\begin{aligned}\tilde{E}_{k,w}(A_+; u) & \le \binom{2k}{2} \sum_{d \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1, t_2)|^2 \Big| \sum_{d \ge v_p(u)} f_d(t_1, t_2)\Big|^{2(k-1)} dt_1 dt_2 \\ & \le \binom{2k}{2} \sum_{d \ge v_p(u)} \tilde{E}_{k,w}(A_d; u)^{1/k} E_{k,w}(A_+; u)^{1-1/k},\end{aligned}$$

the last inequality being Hölder's. It therefore follows that

$$\tilde{E}_{k,w}(A_+; u)^{1/k} \le \binom{2k}{2} \sum_{d \ge v_p(u)} \tilde{E}_{k,w}(A_d; u)^{1/k}. \quad (20)$$

Now we proceed to $E_{k,w}(A_-;u)^{1/k}$. For any solution to the pair of equations

$$a_1 \cdots a_k = a_{k+1} \cdots a_{2k} \quad \text{and} \quad (a_1+u)\cdots(a_k+u) = (a_{k+1}+u)\cdots(a_{2k}+u)$$

we have a solution to the equation

$$(1+ua_1^{-1})\cdots(1+ua_k^{-1}) = (1+ua_{k+1}^{-1})\cdots(1+ua_{2k}^{-1}).$$

Again, we expand and simplify, using this time that $v_p(ua_i^{-1})$ is positive, and get

$$u(a_1^{-1}+\cdots a_k^{-1}) + \text{higher terms} = u(a_{k+1}^{-1}+\cdots a_{2k}^{-1}) + \text{higher terms}.$$

As in the previous case,[4] we cannot have a unique smallest $v_p(ua_i^{-1})$. We can therefore repeat the arguments that gave us (20) in order to deduce that

$$\tilde{E}_{k,w}(A_-;u)^{1/k} \le \binom{2k}{2} \sum_{d<v_p(u)} \tilde{E}_{k,w}(A_d;u)^{1/k}. \tag{21}$$

Inserting (20) and (21) into (13) completes the proof. □

Next, this is used as a base case to give an analogous result with more primes.

Lemma 2.6. *Let $p_1,\ldots,p_K$ be a prime numbers. Suppose A is a finite set of rational numbers and let u be a nonzero rational number. For a vector $\boldsymbol{d}=(d_1,\ldots,d_K)$, define*

$$A_{\boldsymbol{d}} = \{a \in A : v_{p_1}(a)=d_1,\ldots,v_{p_K}(a)=d_K\}.$$

Then for any w, a set of nonnegative weights on A, and for any integer $k \ge 2$,

$$\tilde{E}_{k,w}(A;u)^{1/k} \le \left(2\binom{2k}{2}\right)^K \sum_{\boldsymbol{d}\in\mathbb{Z}^K} \tilde{E}_{k,w}(A_{\boldsymbol{d}};u)^{1/k}.$$

Proof. The aim is to prove that

$$\lim_{T\to\infty}\left(\frac{1}{T^2}\int_0^T\int_0^T \left|\sum_{\boldsymbol{d}\in\mathbb{Z}^K}\sum_{a\in A_{\boldsymbol{d}}} w_a a^{it_1}(a+u)^{it_2}\right|^{2k} dt_1dt_2\right)^{1/k}$$
$$\le \left(2\binom{2k}{2}\right)^K \sum_{\boldsymbol{d}\in\mathbb{Z}^K} \lim_{T\to\infty}\left(\frac{1}{T^2}\int_0^T\int_0^T \left|\sum_{a\in A_{\boldsymbol{d}}} w_a a^{it_1}(a+u)^{it_2}\right|^{2k} dt_1dt_2\right)^{1/k}. \tag{22}$$

[4] Note that here we have used the information that $a_1\cdots a_k = a_{k+1}\cdots a_{2k}$, whereas we did not use this when bounding $\tilde{E}_{k,w}(A_+;u)$.

We proceed by induction on K, the base case $K = 1$ being given by Lemma 2.5. Then

$$\begin{aligned}
&\lim_{T\to\infty}\biggl(\frac{1}{T^2}\int_0^T\int_0^T\biggl|\sum_{\boldsymbol{d}\in\mathbb{Z}^K}\sum_{a\in A_{\boldsymbol{d}}} w_a a^{it_1}(a+u)^{it_2}\biggr|^{2k} dt_1dt_2\biggr)^{1/k}\\
&\quad= \lim_{T\to\infty}\biggl(\frac{1}{T^2}\int_0^T\int_0^T\biggl|\sum_{d_K\in\mathbb{Z}}\biggl(\sum_{\boldsymbol{d}'\in\mathbb{Z}^{K-1}}\sum_{a\in A_{(\boldsymbol{d}',d)}} w_a a^{it_1}(a+u)^{it_2}\biggr)\biggr|^{2k} dt_1dt_2\biggr)^{1/k}\\
&\quad\le 2\binom{2k}{2}\sum_{d_K\in\mathbb{Z}}\lim_{T\to\infty}\biggl(\frac{1}{T^2}\int_0^T\int_0^T\biggl|\sum_{\boldsymbol{d}'\in\mathbb{Z}^{K-1}}\sum_{a\in A_{(\boldsymbol{d}',d)}} w_a a^{it_1}(a+u)^{it_2}\biggr|^{2k} dt_1dt_2\biggr)^{1/k}\\
&\quad\le 2\binom{2k}{2}\sum_{d_K\in\mathbb{Z}}\biggl(2\binom{2k}{2}\biggr)^{K-1}\sum_{\boldsymbol{d}'\in\mathbb{Z}^{K-1}}\lim_{T\to\infty}\biggl(\frac{1}{T^2}\int_0^T\int_0^T\biggl|\sum_{a\in A_{(\boldsymbol{d}',d)}} w_a a^{it_1}(a+u)^{it_2}\biggr|^{2k} dt_1dt_2\biggr)^{1/k}\\
&\quad= \biggl(2\binom{2k}{2}\biggr)^{K}\sum_{\boldsymbol{d}\in\mathbb{Z}^K}\lim_{T\to\infty}\biggl(\frac{1}{T^2}\int_0^T\int_0^T\biggl|\sum_{a\in A_{\boldsymbol{d}}} w_a a^{it_1}(a+u)^{it_2}\biggr|^{2k} dt_1dt_2\biggr)^{1/k}.
\end{aligned}$$

The first inequality above follows from an application of Lemma 2.5. The second inequality follows from the induction hypothesis. □

3. Lambda-constants and query complexity

3.1. ***Lambda constants.*** In order to extract as much as possible from the Lemma 2.6, it will be convenient to use the language of Λ-*constants*. The main motivation behind Λ-constants is the stability property given by the forthcoming Corollary 3.2, which is absent in the nonweighted version of the energy.

We also encourage the interested reader to consult our preceding paper [Hanson et al. 2019] for a slightly more gentle introduction to Λ-constants in the setting of Dirichlet polynomials and more in-depth motivation behind this concept.

Let $A \subset \mathbb{Q}$ be a finite set and let u be a nonzero rational. Define

$$\Lambda_k(A; u) := \max \tilde{E}_{k,w}(A; u)^{1/k},$$

where the maximum is taken over all weights w on A such that

$$\sum_{a\in A} w(a)^2 = 1. \tag{23}$$

An equivalent definition is

$$\Lambda_k(A; u) := \max \lim_{T\to\infty}\biggl\|\sum_{a\in A} w_a a^{it_1}(a+u)^{it_2}\biggr\|_{2k}^2 .$$

where the maximum is taken over the same range of weights.

Lemma 3.1. *Let $A \subset \mathbb{Q}$ be a finite set with some nonnegative real weights w_a assigned to each element $a \in A$ and let u be a nonzero rational. Then*

$$\Bigl\| \sum_{a \in A} w_a a^{it_1}(a+u)^{it_2} \Bigr\|_{2k}^2 \le \Lambda_k(A;u)\Bigl(\sum_{a\in A} w_a^2\Bigr) + o_{T\to\infty}(1). \tag{24}$$

Proof. If $\sum_{a\in A} w_a^2 = 0$ the claim of the lemma is trivial. Otherwise, define new weights

$$w'_a := \frac{w_a}{\bigl(\sum_{a\in A} w_a^2\bigr)^{1/2}}$$

which satisfy (23). It thus suffices to show that

$$\Bigl\| \sum_{a \in A} w'_a a^{it_1}(a+u)^{it_2} \Bigr\|_{2k}^2 \le \Lambda_k(A;u) + o_{T\to\infty}(1),$$

which is a straightforward consequence of our definition of $\Lambda_k(A;u)$. □

We will use the following stability property of Λ-constants which helps us to work with subsets.

Corollary 3.2. *Suppose that $A \subset \mathbb{Q}$, that u is a nonzero rational and $A' \subset A$. Then*

$$\Lambda_k(A';u) \le \Lambda_k(A;u).$$

In particular,

$$\tilde{E}_k^{1/k}(A';u) \le \Lambda_k(A;u)|A'| \quad \textit{and} \quad \tilde{E}_k(A;u) \le \Lambda_k^k(A;u)|A|^k.$$

Proof. The first claim follows from the observation that any set of weights $\{w_a\}_{a\in A'}$ with $\sum w_a^2 = 1$ can be trivially extended to a set of weights $\{w_a\}_{a\in A}$ by assigning zero weight to the elements in $A \setminus A'$. Next observe that E_k is just $E_{k,w}$ with all the weights being one and apply Lemma 3.1. □

3.2. *Query complexity.*

The ideas of Section 2 dovetail perfectly with the notion of the *query-complexity* of a set of rationals. Given a set $A \subset \mathbb{Q}$, we define its query complexity $q(A)$ to be the smallest integer t such that there are functions $f_i : \mathbb{Z} \to \mathbb{P}$, $i = 1, \dots, t-1$ and a fixed prime p_0 such that the vectors

$$(v_{p_0}(a), v_{p_1}(a), \dots, v_{p_{t-1}}(a)), \quad a \in A$$

are pairwise distinct, with the primes p_i defined recursively as

$$p_i = f_i(v_{p_{i-1}}(a)). \tag{25}$$

In the language of computational complexity, suppose that Alice and Bob agree on a set $A \subset \mathbb{Q}$, and then Alice secretly chooses an element $a \in A$. Bob can recover the value $a \in A$ by querying Alice iteratively at most t times, at step i evaluating p_i using (25) and asking Alice for $v_{p_i}(a)$.

The following result was recently proven by Zhelezov and Pálvölgyi [2020], building on work of Matolsci, Ruzsa, Shakan and Zhelezov [Matolcsi et al. 2020].[5]

[5] We state a version of the result which is geared towards the particular considerations of our problem; see [Zhelezov and Pálvölgyi 2020, Theorem 1.1] for a more general statement.

Theorem 3.3. *For any $\epsilon > 0$, and any set $A \subset \mathbb{Q}$ with $|AA| \leq K|A|$, there exists a subset $A' \subset A$ with $|A'| \geq K^{-2/\epsilon}|A|$ and $q(A) \leq \epsilon \log_2|A|$.*

The next lemma records that any set with small query complexity also has a small Λ-constant.

Lemma 3.4. *Let $A \subset \mathbb{Q}$ with $q(A) \leq t$. Then for any $u \in \mathbb{Q} \setminus \{0\}$*

$$\Lambda_k(A; u) \leq \left(2\binom{2k}{2}\right)^t.$$

Proof. Write $t = q(A)$. Let w be any set of weights on A that satisfy (23). Let $a \in A$ be arbitrary. In the notation of Lemma 2.6, we have a list of primes $p_1, p_2, \dots, p_t$ defined by (25) such that the set

$$A_{\boldsymbol{a}} = \{a' \in A : v_{p_1}(a') = v_{p_1}(a), \dots, v_{p_t}(a') = v_{p_t}(a)\}$$

has cardinality exactly 1. For any singleton $\{a\} \in A$, $\tilde{E}_{k,w}(\{a\}; u) = w_a^{2k}$. Therefore, by Lemma 2.6,

$$\tilde{E}_{k,w}(A'; u)^{1/k} \leq \left(2\binom{2k}{2}\right)^t \sum_{a \in A'} w_a^2 = \left(2\binom{2k}{2}\right)^t. \qquad \square$$

The following result is important generalization of the previous one; it shows that if A contains a large subset with small query complexity then A itself has small Λ-constant.

Lemma 3.5. *Let $A \subset \mathbb{Q}^*$ be a finite set with $|AA| \leq K|A|$ and let u be a nonzero rational number. Suppose that $A' \subset A$ and $q(A') = t$. Then*

$$\Lambda_k(A; u) \leq K^4 \left(\frac{|A|}{|A'|}\right)^2 \left(2\binom{2k}{2}\right)^t.$$

Proof. Let w be an arbitrary set of weights on A such that $\sum_{a \in A} w(a)^2 = 1$. We seek a suitable upper bound for

$$\left\| \sum_{a \in A} w_a a^{it_1} (a+u)^{it_2} \right\|_{2k}^2.$$

For a fixed $z \in A/A'$, define a set of weights $w^{(z)}$ on zA' by taking $w^{(z)}(za') = w(za')$ if $za' \in A$ and $w^{(z)}(za') = 0$ otherwise. Define

$$R_{(A/A'),A'}(x) := |\{(s, a) \in (A/A') \times A' : sa = x\}|$$

and note that $R_{(A/A'),A'}(x) \geq |A'|$ for all $x \in A$. This is because, for all $a' \in A'$, $x = (x/a')a'$. Therefore,

$$\begin{aligned}\left\| \sum_{z \in A/A'} \sum_{a' \in A'} w^{(z)}(za')(za')^{it_1}(za'+u)^{it_2} \right\|_{2k} &= \left\| \sum_{a \in A} R_{(A/A'),A'}(a) w(a) a^{it_1}(a+u)^{it_2} \right\|_{2k} \\ &\geq |A'| \left\| \sum_{a \in A} w_a a^{it_1}(a+u)^{it_2} \right\|_{2k}.\end{aligned}$$

On the other hand, by the triangle inequality and Lemma 3.1

$$\begin{aligned}\Bigl\| \sum_{z\in A/A'} \sum_{a'\in A'} w^{(z)}(za')(za')^{it_1}(za'+u)^{it_2} \Bigr\|_{2k} &\le \sum_{z\in A/A'} \Bigl\| \sum_{a'\in A'} w^{(z)}(za')(za')^{it_1}(za'+u)^{it_2} \Bigr\|_{2k} \\ &\le \sum_{z\in A/A'} \Lambda_k(zA';u)^{1/2} + o_{T\to\infty}(1).\end{aligned}$$

Since $q(A')=t$, it follows from Lemma 3.4 that $\Lambda_k(zA';u)=\Lambda_k(A';u/z)\le \bigl(2\binom{2k}{2}\bigr)^t$. We also have

$$|A/A'| \le |A/A| \le \frac{|AA|^2}{|A|} \le K^2|A|,$$

by the Ruzsa triangle inequality (see [Tao and Vu 2006]). It therefore follows that

$$\Bigl\| \sum_{a\in A} w_a a^{it_1}(a+u)^{it_2} \Bigr\|_{2k} \le K^2 \biggl(\frac{|A|}{|A'|}\biggr) \biggl(2\binom{2k}{2}\biggr)^{t/2} + o_{T\to\infty}(1),$$

and the result follows. □

Combining this with Theorem 3.3 gives the following, which is our main result concerning Λ-constants.

Theorem 3.6. *Given $0<\gamma<\frac{1}{2}$, there exists a positive constants $C=C(\gamma,k)$ such that for any finite $A\subset\mathbb{Q}^*$ with $|AA|=K|A|$ and any nonzero rational u,*

$$\Lambda_k(A;u) \le K^C|A|^{\gamma}.$$

Proof. Apply Theorem 3.3 with $\epsilon=\gamma/\log_2(4k)$. There exists $A'\subset A$ with $|A'|\ge K^{-2/\epsilon}|A|$ and $q(A)\le \epsilon\log_2|A|$. Then by Lemma 3.5

$$\Lambda_k(A;u) \le K^4 \biggl(\frac{|A|}{|A'|}\biggr)^2 \biggl(2\binom{2k}{2}\biggr)^{\epsilon\log_2|A|} \le K^{4+4/\epsilon}|A|^{\epsilon\log_2(4k)}.$$ □

Observe that we can in fact take $C(\gamma,k)$ in Theorem 3.6 to be $4+4\log_2(4k)/\gamma$.

4. Concluding the proofs

In this section we conclude the proof of Theorem 1.1, which is the main theorem of this paper, and Theorem 1.7 announced in the introduction.

We will use the Plünnecke–Ruzsa theorem. See [Petridis 2012] for a simple inductive proof. Following convention, we state it using additive notation, although it will be used in the multiplicative setting.

Theorem 4.1. *Let A be a subset of a commutative additive group G with $|A+A|\le K|A|$. Then for any $h\in\mathbb{N}$,*

$$|hA| \le K^h|A|.$$

For the convenience of the reader, we restate Theorem 1.1.

Theorem 4.2. *For all $b \in \mathbb{Z}$, there exists $k = k(b)$ such that for any finite set $A \subset \mathbb{Q}^*$ and any nonzero rational u,*

$$\max\{|A^{(k)}|, |(A+u)^{(k)}|\} \geq |A|^b$$

Proof. Fix b and assume that

$$|A^{(k)}| < |A|^b$$

for some sufficiently large $k = 2^l$. The value of l (and thus also that of k) will be specified at the end of the proof. Since $|A^{(2^l)}| < |A|^b$, it follows that

$$\frac{|A^{(2^l)}|}{|A^{(2^{l-1})}|}\frac{|A^{(2^{l-1})}|}{|A^{(2^{l-2})}|}\cdots\frac{|A^{(2)}|}{|A|} < |A|^{b-1}$$

and thus there is some integer $l_0 \leq l$ such that

$$\frac{|A^{(2^{l_0+1})}|}{|A^{(2^{l_0})}|} < |A|^{(b-1)/l}.$$

Therefore, writing $k_0 = 2^{l_0}$ and $B = A^{(k_0)}$, we have

$$|BB| < |B||A|^{(b-1)/l}.$$

Also, for any nonzero $\lambda \in \mathbb{Q}$, $|(\lambda B)(\lambda B)| < |B||A|^{(b-1)/l}$. Therefore, by Theorem 3.6,

$$\Lambda_h(\lambda B; u) \leq |A|^{C(b-1)/l}|B|^{\gamma} \leq |A|^{C(b-1)/l+\gamma b}$$

where $C = C(h,\gamma)$ and h, γ will be specified later.

Now, for some $\lambda \in \mathbb{Q}$, we have $A \subset \lambda B$, and thus by Corollary 3.2 and Lemma 2.1

$$\frac{|A|^2}{\max\{|A^{(h)}|, |(A+u)^{(h)}|\}^{2/h}} \leq \tilde{E}_h^{1/h}(A;u) \leq |A|\Lambda_h(\lambda B; u) \leq |A|^{1+C(b-1)/l+\gamma b}.$$

This rearranges to

$$\max\{|A^{(h)}|, |(A+u)^{(h)}|\} \geq |A|^{h/2(1-C(b-1)/l-\gamma b)}.$$

Choose $\gamma = 1/100b$ and $h = 4b$. Then $C = C(h,\gamma) = C(b)$ and we have

$$\max\{|A^{(h)}|, |(A+u)^{(h)}|\} \geq |A|^{h/2(99/100-C(b)(b-1)/l)}.$$

Then choose $l = (b-1)4C$ to get

$$\max\{|A^{(h)}|, |(A+u)^{(h)}|\} \geq |A|^{h/4} = |A|^b.$$

Note that the choice of l depends only on b and thus $k = 2^{4C(b-1)} = k(b)$. In particular, since $k > h$, we conclude that

$$\max\{|A^{(k)}|, |(A+u)^{(k)}|\} \geq |A|^b,$$

as required. □

If we use the value of $C(\gamma, k)$ indicated at the end of the proof of Theorem 3.6 to keep track of the constants in this argument, it follows that we can take $k = 2^{O(b^2 \log b)}$. To be even more precise, it gives

$$k = (16b)^{1616b^2}.$$

This compares favorably with the dependency in the corresponding sum-product bound of Bourgain and Chang [2004], where they commented that it was possible to take $k = 2^{O(b^4)}$. A similar quantitative improvement for the classical iterated sum-product problem is possible by studying the recent paper of Zhelezov and Pálvölgyi [2020] and filling in some extra details.

Theorem 3.6 also implies Theorem 1.3. The statement is repeated below for the convenience of the reader.

Theorem 4.3. *Given $0 < \gamma < \frac{1}{2}$ and any integer $k \geq 2$, there exists a positive constant $C = C(\gamma, k)$ such that for any finite $A \subset \mathbb{Q}^*$ with $|AA| = K|A|$ and any nonzero rational u,*

$$|(A+u)^{(k)}| \geq \frac{|A|^{k(1-\gamma)-1}}{K^{Ck}}.$$

Proof. Define $w(a) = 1/|A|^{1/2}$ for all $a \in A$ and note that (23) is satisfied. Furthermore, for this set of weights w,

$$\tilde{E}_{k,w}(A; u) = \frac{\tilde{E}_k(A; u)}{|A|^k} \geq \frac{|A|^k}{|A^{(k)}||(A+u)^{(k)}|}, \tag{26}$$

where the inequality comes from Lemma 2.1. It follows from Theorem 3.6 that there exists a constant $C = C(\gamma, k)$ such that for any $u \in \mathbb{Q} \setminus \{0\}$, $\Lambda_k(A; u) \leq K^C |A|^\gamma$. Consequently, by the definition of $\Lambda_k(A; u)$,

$$\tilde{E}_{k,w}(A; u) \leq K^{Ck} |A|^{\gamma k}.$$

Combining this with (26), it follows that

$$|A^{(k)}||(A+u)^{(k)}| \geq \frac{|A|^{k(1-\gamma)}}{K^{Ck}}. \tag{27}$$

Finally, since $|AA| \leq K|A|$, it follows from the Plünnecke–Ruzsa Theorem that $|A^{(k)}| \leq K^k |A|$. Inserting this into (27) completes the proof. □

We now turn to the proof of Theorem 1.7. Recall its statement.

Theorem 4.4. *For any $\gamma > 0$ there is $C(\gamma) > 0$ such that for any K-almost subgroup $A \subset \mathbb{Q}^*$ and fixed nonzero $c_1, c_2 \in \mathbb{Q}$ the number $A(2, K)$ of solutions $(x_1, x_2) \in A^2$ to*

$$c_1 x_1 + c_2 x_2 = 1$$

is bounded by

$$A(2, K) \leq |A|^\gamma K^C.$$

Proof. Let $S \subset A$ be the set of $x_1 \in A$ such that $c_1 x_1 + c_2 x_2 = 1$ for some $x_2 \in A$. Since the projection $(x_1, x_2) \to x_1$ is injective, it suffices to bound the size of S.

Since $S \subset A$, by Theorem 3.6 and Corollary 3.2 for any nonzero u

$$\tilde{E}_k(S; u) \le K^{kC(\gamma',k)} |A|^{k\gamma'} |S|^k$$

with the parameters $0 < \gamma' < \frac{1}{2}$, $k \ge 2$ to be taken in due course.

In particular, by Lemma 2.1

$$|S|^k \le (K^{kC(\gamma',k)} |A|^{k\gamma'} |S|^k)^{1/2} \max\{|S^k|, |(S - 1/c_1)^k|\}.$$

On the other hand, $S \subseteq A$ and $(S - 1/c_1) \subseteq -(c_2/c_1)A$, so by the Plünnecke–Ruzsa inequality

$$\max\{|S^k|, |(S - 1/c_1)^k|\} \le |A^{(k)}| \le K^k |A|.$$

We then have

$$|S| \le |A|^{\gamma' + 2/k} K^{C+2},$$

and taking $k = \lfloor 2/\gamma' \rfloor + 1$ and $\gamma' = \gamma/2$, the claim follows. □

5. Further applications

Proof of Theorem 1.8. Recall that Theorem 1.8 is the following statement. For all $\gamma \ge 0$ there exists a constant $C = C(\gamma)$ such that for any finite $A \subset \mathbb{Q}$ with $|AA| \le K|A|$ and any finite set L of lines in the plane, $I(P, L) \le 3|P| + |A|^\gamma K^C |L|$, where $P = A \times A$.

First of all, observe that horizontal and vertical lines contribute a total of at most $2|P|$. This is because each point $p \in P$ can belong to at most one horizontal and one vertical line. Similarly, lines through the origin contribute at most $|P| + |L|$ incidences, since each point aside from the origin belongs to at most one such line, and the origin itself may contribute $|L|$ incidences.

It remains to bound incidences with lines of the form $y = mx + c$, with $m, c \ne 0$. Let $l_{m,c}$ denote the line with equation $y = mx + c$. Note that, if $m \notin \mathbb{Q}$ then $l_{m,c}$ contains at most one point from P. Indeed, suppose $l_{m,c}$ contains two distinct points (x, y) and (x', y') from P. In particular, since $A \subset \mathbb{Q}$, $x, y, x', y' \in \mathbb{Q}$. Then $l_{m,c}$ has direction $m = (y - y')/(x - x')$. Therefore, lines $l_{m,c}$ with irrational slope m contribute at most $|L|$ incidences.

Next, suppose that $m \in \mathbb{Q}$ and $c \notin \mathbb{Q}$. Then $l_{m,c}$ does not contain any points from P, since if it did then we would have a solution to $y = mx + c$, but the left hand side is rational and the right hand side is irrational.

It remains to consider the case when $m, c \in \mathbb{Q}^*$. An application of Theorem 1.7 implies that $|l_{m,c} \cap P| \le K^C |A|^\gamma$. Therefore, these lines contribute a total of at most $|L| K^C |A|^\gamma$ incidences.

Adding together the contributions from these different types of lines completes the proof. □

Proof of Theorem 1.9. Recall that Theorem 1.9 states that, for any $\gamma > 0$ there exists $C(\gamma)$ such that for an arbitrary $A \subset \mathbb{Q}$ with $|AA| = K|A|$ and $B, B' \subset \mathbb{Q}$,

$$S := |\{(b, b') \in B \times B' : b + b' \in A\}| \leq 2|A|^{\gamma} K^{C} \min\{|B|^{1/2}|B'| + |B|, |B'|^{1/2}|B| + |B'|\}.$$

We will prove that

$$S \leq 2|A|^{\gamma} K^{C}(|B'|^{1/2}|B| + |B'|). \tag{28}$$

Since the roles of B and B' are interchangeable, (28) also implies that $S \leq 2|A|^{\gamma} K^{C}(|B|^{1/2}|B'| + |B|)$, and thus completes the proof.

Let $\gamma > 0$ and $C(\gamma)$, given by Theorem 1.7, be fixed. Without loss of generality assume that $S \geq 2|B'|$ as otherwise the claimed bound is trivial.

For each $b \in B$ define

$$S_b := \{b' \in B' : b + b' \in A\},$$

and similarly for $b' \in B'$

$$T_{b'} := \{b \in B : b' + b \in A\}.$$

It follows from Theorem 1.7 that for $b_1, b_2 \in B$ with $b_1 \neq b_2$

$$|S_{b_1} \cap S_{b_2}| \leq |A|^{\gamma} K^{C}$$

since each $x \in S_{b_1} \cap S_{b_2}$ gives a solution $(a, a') := (b_1 + x, b_2 + x)$ to

$$a - a' = b_1 - b_2$$

with $a, a' \in A$.

On the other hand, by double-counting and the Cauchy–Schwarz inequality,

$$\sum_{b \in B} |S_b| + \sum_{b_1, b_2 \in B : b_1 \neq b_2} |S_{b_1} \cap S_{b_2}| = \sum_{b' \in B'} |T_{b'}|^2 \geq |B'|^{-1} \Bigl(\sum_{b' \in B'} |T_{b'}|\Bigr)^2 = |B'|^{-1} S^2.$$

Therefore,

$$\sum_{b_1, b_2 \in B : b_1 \neq b_2} |S_{b_1} \cap S_{b_2}| \geq |B'|^{-1} S^2 - \sum_{b \in B} |S_b| = |B'|^{-1} S^2 - S \geq \tfrac{1}{2} |B'|^{-1} S^2$$

by our assumption.

The left-hand side is at most $|B|^2 |A|^{\gamma} K^{C}$, and so

$$S \leq (2|A|^{\gamma} K^{C})^{1/2} |C|^{1/2} |B'|,$$

which completes the proof. □

Proof of Theorem 1.10. Recall that Theorem 1.10 states that for all b there exists k such that for all $A, B \subset \mathbb{Q}$ with $|B| \geq 2$, $|(A + B)^k| \geq |A|^b$.

Since $|B| \geq 2$, there exist two distinct elements $b_1, b_2 \in B$. Apply Theorem 1.1 to conclude that for all b there exists $k = k(b)$ with

$$|(A+B)^k| \geq \max\{|(A+b_1)^k|, |((A+b_1)+(b_2-b_1))^k|\} \geq |A|^b. \qquad \square$$

Acknowledgements

Oliver Roche-Newton was partially supported by the Austrian Science Fund FWF Project P 30405-N32. Dmitrii Zhelezov was supported by the Knut and Alice Wallenberg Foundation Program for Mathematics 2017.

We thank Brendan Murphy, Cosmin Pohoata, Imre Ruzsa and Endre Szemerédi for helpful conversations.

References

[Amoroso and Viada 2009] F. Amoroso and E. Viada, “Small points on subvarieties of a torus”, *Duke Math. J.* **150**:3 (2009), 407–442. MR Zbl

[Balog et al. 2017] A. Balog, O. Roche-Newton, and D. Zhelezov, “Expanders with superquadratic growth”, *Electron. J. Combin.* **24**:3 (2017), art. id. 3.14. MR Zbl

[Beukers and Schlickewei 1996] F. Beukers and H. P. Schlickewei, “The equation $x + y = 1$ in finitely generated groups”, *Acta Arith.* **78**:2 (1996), 189–199. MR Zbl

[Bourgain and Chang 2004] J. Bourgain and M.-C. Chang, “On the size of k-fold sum and product sets of integers”, *J. Amer. Math. Soc.* **17**:2 (2004), 473–497. MR Zbl

[Bourgain and Chang 2009] J. Bourgain and M.-C. Chang, “Sum-product theorems in algebraic number fields”, *J. Anal. Math.* **109** (2009), 253–277. MR Zbl

[Chang 2003] M.-C. Chang, “The Erdős–Szemerédi problem on sum set and product set”, *Ann. of Math.* (2) **157**:3 (2003), 939–957. MR Zbl

[Erdős and Szemerédi 1983] P. Erdős and E. Szemerédi, “On sums and products of integers”, pp. 213–218 in *Studies in pure mathematics*, edited by P. Erdős, Birkhäuser, Basel, 1983. MR Zbl

[Evertse et al. 2002] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt, “Linear equations in variables which lie in a multiplicative group”, *Ann. of Math.* (2) **155**:3 (2002), 807–836. MR Zbl

[Garaev and Shen 2010] M. Z. Garaev and C.-Y. Shen, “On the size of the set $A(A + 1)$”, *Math. Z.* **265**:1 (2010), 125–132. MR Zbl

[Hanson et al. 2019] B. Hanson, O. Roche-Newton, and D. Zhelezov, “On iterated product sets with shifts”, *Mathematika* **65**:4 (2019), 831–850. MR Zbl

[Jones and Roche-Newton 2013] T. G. F. Jones and O. Roche-Newton, “Improved bounds on the set $A(A + 1)$”, *J. Combin. Theory Ser. A* **120**:3 (2013), 515–526. MR Zbl

[Konyagin and Shkredov 2015] S. V. Konyagin and I. D. Shkredov, “On sum sets of sets having small product set”, *Proc. Steklov Inst. Math.* **290**:1 (2015), 288–299. MR Zbl

[Konyagin and Shkredov 2016] S. V. Konyagin and I. D. Shkredov, “New results on sums and products in $\mathbb{R}$”, *Proc. Steklov Inst. Math.* **294**:1 (2016), 78–88. Zbl

[Matolcsi et al. 2020] D. Matolcsi, I. Ruzsa, G. Shakan, and D. Zhelezov, “An analytic approach to cardinalities of sumsets”, preprint, 2020. arXiv

[Petridis 2012] G. Petridis, “New proofs of Plünnecke-type estimates for product sets in groups”, *Combinatorica* **32**:6 (2012), 721–733. MR Zbl

[Shkredov and Zhelezov 2018] I. D. Shkredov and D. Zhelezov, "On additive bases of sets with small product set", *Int. Math. Res. Not.* **2018**:5 (2018), 1585–1599. MR Zbl

[Solymosi 2009] J. Solymosi, "Bounding multiplicative energy by the sumset", *Adv. Math.* **222**:2 (2009), 402–408. MR Zbl

[Tao and Vu 2006] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math. **105**, Cambridge Univ. Press, 2006. MR Zbl

[Zhelezov and Pálvölgyi 2020] D. Zhelezov and D. Pálvölgyi, "Query complexity and the polynomial Freiman–Ruzsa conjecture", preprint, 2020. arXiv

Communicated by Andrew Granville
Received 2020-01-28 Revised 2020-03-30 Accepted 2020-05-01

brandon.w.hanson@gmail.com *Department of Mathematics, University of Georgia, Boyd Graduate Studies Research Center, Athens, GA, United States*

o.rochenewton@gmail.com *Johann Radon Institute for Computational and Applied Mathematics, Linz, Austria*

dzhelezov@gmail.com *Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Budapest, Hungary*

ALGEBRA AND NUMBER THEORY 14:8 (2020)
https://doi.org/10.2140/ant.2020.14.2261

The dimension growth conjecture, polynomial in the degree and without logarithmic factors

Wouter Castryck, Raf Cluckers, Philip Dittmann and Kien Huu Nguyen

We study Heath-Brown's and Serre's dimension growth conjecture (proved by Salberger) when the degree d grows. Recall that Salberger's dimension growth results give bounds of the form $O_{X,\varepsilon}(B^{\dim X+\varepsilon})$ for the number of rational points of height at most B on any integral subvariety X of $\mathbb{P}^n_{\mathbb{Q}}$ of degree $d \geq 2$, where one can write $O_{d,n,\varepsilon}$ instead of $O_{X,\varepsilon}$ as soon as $d \geq 4$. We give the following simplified and strengthened forms of these results: we remove the factor B^ε as soon as $d \geq 5$, we obtain polynomial dependence on d of the implied constant, and we give a simplified, self-contained approach for $d \geq 16$. Along the way, we improve the well-known bounds due to Bombieri and Pila on the number of integral points of bounded height on affine curves and those by Walsh on the number of rational points of bounded height on projective curves. This leads to a slight sharpening of a recent estimate due to Bhargava, Shankar, Taniguchi, Thorne, Tsimerman and Zhao on the size of the 2-torsion subgroup of the class group of a degree d number field. Our treatment builds on recent work by Salberger, who brings in many primes in Heath-Brown's variant of the determinant method, and on recent work by Walsh and by Ellenberg and Venkatesh who bring in the size of the defining polynomial. We also obtain lower bounds showing that one cannot do better than polynomial dependence on d.

1. Introduction and main results

1.1. Following a question raised by Heath-Brown [1983, page 227] in the case of hypersurfaces, Serre [1992, page 27; 1989, page 178] twice formulated a question about rational points on a projective variety X of degree d, which was dubbed the dimension growth conjecture by Browning [2009]. The question puts forward concrete upper bounds on the number of such points with height at most B, as a function of B. This dimension growth conjecture is now a theorem due to Salberger [2013] (and others under various conditions on d); moreover, for $d \geq 4$ Salberger obtains complete uniformity in X, keeping only

The authors would like to thank Gal Binyamini, Jonathan Pila, Arne Smeets, Jan Tuitman, and Alex Wilkie for interesting discussions on the topics of the paper; Per Salberger for sharing his preprint with us and for interesting exchanges of ideas; and Floris Vermeulen for a number of helpful remarks on earlier versions of this article. Castryck, Cluckers, and Nguyen were partially supported by the European Research Council under the European Community's Seventh Framework Programme (FP7/2007-2013) with ERC Grant Agreement nr. 615722 MOTMELSUM and thank the Labex CEMPI (ANR-11-LABX-0007-01). Castryck is affiliated on a voluntary basis with the Department of Mathematics: Algebra and Geometry at Ghent University. Cluckers and Dittmann were partially supported by KU Leuven IF C14/17/083. Nguyen is partially supported by the Fund for Scientific Research – Flanders (Belgium) (FWO) 12X3519N.

MSC2010: primary 11D45; secondary 11G35, 14G05.

Keywords: dimension growth conjecture, rational points of bounded height.

d and the dimension of the ambient projective space fixed, thereby confirming a variant that had been proposed by Heath-Brown.

We remove from these bounds the factors of the form B^{ε} when the degree d is at least 5, without creating a factor $\log B$, while moreover obtaining polynomial dependence on d of the constants. The approach with polynomial dependence on d is implemented in all auxiliary results as well, and this has the pleasant consequence of yielding a more direct and self-contained proof of the dimension growth conjecture for d at least 16 (our treatment of dimension growth for $5 \le d \le 15$ is not self-contained and uses [Browning et al. 2006] when $d > 5$ and [Salberger 2013] for $d = 5$). Theorems 2 and 3 below give such improvements to bounds by Walsh [2015] on the number of rational points of bounded height on integral projective curves, and to bounds of Bombieri and Pila [1989, Theorem 5] on the number of integral points of bounded height on affine irreducible curves, with rather low powers of d, compared to [Walkowiak 2005]. Polynomial dependence on d for projective curves as in Theorem 2 is useful for effective versions of Hilbert's irreducibility theorem and for Malle's conjecture; see [Dèbes and Walkowiak 2008; Motte 2018; Walkowiak 2005].

The possibility of polynomial dependence on d came to us via a question raised by Yomdin (see below Remark 3.8 of [Burguet et al. 2015]) in combination with the determinant method with smooth parametrizations as in [Pila 2010], refined in [Cluckers et al. 2020b], and via the work by Binyamini and Novikov [2019, Theorem 6]. The removal of the factor B^{ε} without needing $\log B$ was recently achieved by Walsh [2015, Theorems 1.1, 1.2, 1.3] who combines ideas by Ellenberg and Venkatesh [2005] with the determinant method based on p-adic approximation (rather than on smooth maps) due to Heath-Brown [2002], refined in [Salberger 2013]. In fact, polynomial dependence on d for the case of projective curves was also achieved in [Motte 2018] and [Walkowiak 2005], with a higher exponent. One cannot achieve dependence on d better than polynomial, as shown by the lower bounds from Proposition 5 below. Let us mention that positive characteristic analogues, over $\mathbb{F}_q[t]$, are obtained in [Cluckers et al. 2020a] and [Sedunova 2017] for curves, and in [Vermeulen 2020] for dimension growth.

1.2. Let us make all this more precise. We study the number

$$N(X, B)$$

of rational points of height at most B on subvarieties X of $\mathbb{P}^n$ defined over $\mathbb{Q}$. Here, the height $H(x)$ of a $\mathbb{Q}$-rational point x in $\mathbb{P}^n$ is given by

$$H(x) = \max(|x_0|, \dots, |x_n|)$$

for an $(n+1)$-tuple $(x_0, \dots, x_n)$ of integers x_i which are homogeneous coordinates for x and have greatest common divisor equal to 1.

Salberger [2013] proved the so-called dimension growth conjecture raised as a question by Serre [1992, page 27] following a question of Heath-Brown [1983, page 227].

Dimension growth [Salberger 2013, Theorem 0.1]. *If X is an integral projective variety of degree $d \geq 2$ defined over $\mathbb{Q}$, then*

$$N(X, B) \leq O_{X,\varepsilon}(B^{\dim X+\varepsilon}).$$

One should compare the bound for $N(X, B)$ from this theorem to the trivial upper bound $O_{d,n}(B^{\dim X+1})$ that follows from Lemma 4.1.1 below.

A variant of this question from [Serre 1989, page 178] replaces the factor B^{ε} by $\log(B)^c$ for some c depending on X, see Section 1.4 below.

Heath-Brown [2002] introduces a form of this conjecture with uniformity in X for fixed d and n, and he develops a new variant of the determinant method using p-adic approximation instead of smooth parametrizations as in [Bombieri and Pila 1989; Binyamini and Novikov 2019; Pila 2010; Cluckers et al. 2020b]. In [Salberger 2013], Salberger proves this uniform version of the dimension growth conjecture for $d \geq 4$.

Uniform dimension growth [Salberger 2013, Theorem 0.3]. *For $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$ an integral projective variety of degree $d \geq 4$, one has*

$$N(X, B) \leq O_{d,n,\varepsilon}(B^{\dim X+\varepsilon}).$$

Almost all situations of this uniform dimension growth had been obtained previously in [Heath-Brown 2002] and [Browning et al. 2006], including the case $d = 2$ but without the (difficult) cases $d = 4$ and $d = 5$. Our main contributions are to make the dependence on d polynomial, to remove the factor B^{ε} without having to use factors $\log B$, and to provide relatively self-contained proofs for large degree, with main result as follows.

Theorem 1 (uniform dimension growth). *Given $n > 1$, there exist constants $c = c(n)$ and $e = e(n)$, such that for all integral projective varieties $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$ of degree $d \geq 5$ and all $B \geq 1$ one has*

$$N(X, B) \leq cd^e B^{\dim X}. \tag{1-2-1}$$

As mentioned earlier, one cannot do better than polynomial dependence on d, see the lower bounds from Proposition 5 and Section 6 below.

We heavily rework results and methods of Salberger, Walsh, Ellenberg and Venkatesh, Heath-Brown, and Browning, and use various explicit estimates for Hilbert functions, for certain universal Noether polynomials as in [Ruppert 1986], and for solutions of linear systems of equations over $\mathbb{Z}$ from [Bombieri and Vaaler 1983].

1.3. ***Rational points on curves and hypersurfaces.*** Let us make precise some of our improvements for counting points on curves and surfaces, which are key to Theorem 1. We obtain the following improvement of Walsh's Theorem 1.1 [2015].

Theorem 2 (projective curves). *Given $n > 1$, there exists a constant $c = c(n)$ such that for all $d > 0$ and all integral projective curves $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$ of degree d and all $B \geq 1$ one has*

$$N(X, B) \leq cd^4 B^{2/d}.$$

In view of Proposition 5 below, the exponent 4 of d in Theorem 2 can perhaps be lowered, but cannot become lower than 2 in general. Several adaptations of results and proofs of [Walsh 2015] are key to our treatment and are developed in Section 3.

For affine counting we use the following notation for a variety $X \subseteq \mathbb{A}^n_{\mathbb{Q}}$ and a polynomial f in $\mathbb{Z}[y_1, \dots, y_n]$:

$$N_{\text{aff}}(X, B) := \#\{x \in \mathbb{Z}^n \mid |x_i| \leq B \text{ for each } i \text{ and } x \in X(\mathbb{Q})\},$$

and

$$N_{\text{aff}}(f, B) := \#\{x \in \mathbb{Z}^n \mid |x_i| \leq B \text{ for each } i \text{ and } f(x) = 0\}.$$

By a careful elaboration of the argument from [Ellenberg and Venkatesh 2005, Remark 2.3] and an explicit but otherwise classical projection argument, we find the following improvement of bounds by Bombieri and Pila [1989, Theorem 5] and later sharpenings by Pila [1995; 1996], Walkowiak [2005], Ellenberg and Venkatesh [2005, Remark 2.3], Binyamini and Novikov [2019, Theorem 6], and others.

Theorem 3 (affine curves). *Given $n > 1$, there exists a constant $c = c(n)$ such that for all $d > 0$, all integral affine curves $X \subseteq \mathbb{A}^n_{\mathbb{Q}}$ of degree d, and all $B \geq 1$ one has*

$$N_{\text{aff}}(X, B) \leq cd^3 B^{1/d}(\log B + d).$$

A variant of Theorem 3 is given in Section 4, where $\log B$ is absent and instead the size of the coefficients of the polynomial f defining the affine planar curve comes in.

It is well-known that Theorems 1, 2, and 3 imply similar bounds for varieties defined and integral over $\overline{\mathbb{Q}}$ (instead of $\mathbb{Q}$), by intersecting with a Galois conjugate and using a trivial bound, see Lemma 4.1.3. The following improves Theorem 0.4 of [Salberger 2013] and is key to Theorem 1. It can be seen as an affine form of the dimension growth theorem, for hypersurfaces.

Theorem 4 (affine hypersurfaces). *Given $n > 2$, there exist constants $c = c(n)$ and $e = e(n)$, such that for all polynomials f in $\mathbb{Z}[y_1, \dots, y_n]$ whose homogeneous part of highest degree $h(f)$ is irreducible over $\overline{\mathbb{Q}}$ and whose degree d is at least 5, one has*

$$N_{\text{aff}}(f, B) \leq cd^e B^{n-2}.$$

One should compare the bound from this theorem to the trivial upper bound $O_{d,n}(B^{n-1})$ from Lemma 4.1.1.

1.4. ***Example and a question.*** In Serre's example [1989, page 178] of the degree 2 surface in $\mathbb{P}^3$ given by the equation $xy = zw$, the logarithmic factor $\log B$ cannot be dispensed with in the upper bound. Hence, (1-2-1) of Theorem 1 cannot hold for $d = 2$ in general. For $d = 3$, the bound from (1-2-1) remains wide open since already uniformity in $X \subseteq \mathbb{P}^n$ of degree 3 is not known for the uniform dimension growth with $O_{d,n,\varepsilon}(B^{\dim X+\varepsilon})$ as upper bound (see [Salberger 2015; 2013] for subtleties when $d = 3$). For $d = 4$, one may investigate whether (1-2-1) of Theorem 1 remains true, that is, without involving a factor B^ε or $\log B$.

1.5. ***Lower bounds.*** In Section 6 we discuss the necessity of the polynomial dependence on d in the above theorems.

Proposition 5. *For each integer $d > 0$ there is an integral projective curve $X \subseteq \mathbb{P}^2$ of degree d and an integer $B \geq 1$ such that*

$$\tfrac{1}{5} d^2 B^{2/d} \leq N(X, B).$$

In particular, in the statement of Theorem 2 it is impossible to replace the factor d^4 with an expression in d which is $o(d^2)$.

Similarly we show that it is impossible to replace the quartic dependence on d of the bound from Theorem 3 by a function in $o(d^2/\log d)$. We also show that in Theorems 1 and 4 we cannot take $e < 1$ or $e < 2$, respectively.

1.6. ***An application.*** Our bounds with improved exponent can be used as substitutes for those by Salberger, Bombieri and Pila, and Walsh upon which they improve, potentially leading to stronger statements. A very recent example of such an application is Bhargava, Shankar, Taniguchi, Thorne, Tsimerman and Zhao's bound [Bhargava et al. 2020, Theorem 1.1] on the number $h_2(K)$ of 2-torsion elements in the class group of a degree $d > 2$ number field K, in terms of its discriminant Δ_K. Precisely, they show that

$$h_2(K) \leq O_{d,\varepsilon}(|\Delta_K|^{1/2-1/(2d)+\varepsilon}),$$

thereby obtaining a power saving over the trivial bound coming from the Brauer–Siegel theorem. This power saving is mainly accounted for by an application of Bombieri and Pila's bound [1989, Theorem 5]. In Section 4 we explain how our improved bound stated in Theorem 3, or rather its refinement stated in Corollary 4.2.4, allows for removal of the factor $|\Delta_K|^\varepsilon$ as soon as d is odd; if d is even then we can replace it by $\log|\Delta_K|$.

Theorem 6. *For all degree $d > 2$ number fields K we have*

$$h_2(K) \leq O_d(|\Delta_K|^{1/2-1/(2d)}(\log|\Delta_K|)^{1-(d \bmod 2)}).$$

It is possible to make the hidden constant explicit, but targeting polynomial growth seems of lesser interest since $|\Delta_K|$ is itself bounded from below by an exponential expression in d, coming from Minkowski's bound.

1.7. ***Structure of the paper.*** In Section 2 we render several results of Salberger [2007] explicit in terms of the degrees and dimensions involved. In Section 3 we similarly adapt the results of Walsh [2015]. Section 4 completes the proofs of our main results in the hypersurface case, which is complemented by

Section 5, in which we discuss projection arguments from [Browning et al. 2006], explicit in the degrees and dimensions, and thus finish the proofs of our main theorems. Finally, in Section 6, we provide lower bounds showing the necessity of polynomial dependence on d in our main results.

2. The determinant method for hypersurfaces

With the aim of improving the results of [Walsh 2015] in the next section, we sharpen some results from Salberger's global determinant method. The main result of this section is Corollary 2.9, which improves on [Salberger 2013, Lemmas 1.4, 1.5] (see also [Walsh 2015, Theorem 2.2]). This mainly depends on making [Salberger 2007, Main Lemma 2.5] in the case of hypersurfaces explicit in its independence of the degree.

Let f be an absolutely irreducible homogeneous polynomial in $\mathbb{Z}[x_0, \dots, x_{n+1}]$ which is primitive, and let X be the hypersurface in $\mathbb{P}^{n+1}_{\mathbb{Q}}$ defined by f. For p a prime number, let X_p denote the reduction of X modulo p, i.e., the hypersurface in $\mathbb{P}^{n+1}_{\mathbb{F}_p}$ described by the reduction of f mod p.

Lemma 2.1 (Lemma 2.3 of [Salberger 2007], explicit for hypersurfaces). *Let A be the stalk of X_p at some $\mathbb{F}_p$-point P of multiplicity μ and let $\mathfrak{m}$ be the maximal ideal of A. Let $g_{X,P} : \mathbb{Z}_{>0} \to \mathbb{Z}$ be the function given by $g_{X,P}(k) = \dim_{A/\mathfrak{m}} \mathfrak{m}^k/\mathfrak{m}^{k+1}$ for $k > 0$. Then one has*

$$g(k) = \binom{n+k}{n} \text{ for } k < \mu$$

and

$$g(k) = \binom{n+k}{n} - \binom{n+k-\mu}{n} \text{ for } k \geq \mu.$$

In particular,

$$g(k) \leq \frac{\mu k^{n-1}}{(n-1)!} + O_n(k^{n-2})$$

for all $k \geq 1$, where the implied constant depends only on n, as indicated.

Proof. The function g is identical to the Hilbert function of the projectivized tangent cone of X_p at P, which is a degree μ hypersurface in $\mathbb{P}^n$. This gives the explicit expression for g, so it only remains to prove the estimate.

Consider first $k < \mu$. Then

$$g(k) = \binom{n+k}{n} = \frac{k^n}{n!} + \frac{(n+1)k^{n-1}}{2(n-1)!} + O_n(k^{n-2}).$$

Since $\mu > k$, for $k \geq n$ we immediately obtain the desired inequality, and the k between 1 and n are covered by choosing the constant large enough.

Now consider $k \geq \mu$. Write $p(X)$ for the polynomial $\binom{n+X}{n}$ and a_i for its coefficients. Then

$$p(k) - p(k-\mu) = a_n(k^n - (k-\mu)^n) + a_{n-1}(k^{n-1} - (k-\mu)^{n-1}) + O_n(k^{n-2}).$$

Observe that $a_n = 1/n!$, $a_{n-1} = (n+1)/(2(n-1)!) = a_n(n+1)n/2$, and write

$$k^n - (k-\mu)^n = \mu(k^{n-1} + (k-\mu)k^{n-2} + \cdots + (k-\mu)^{n-1})$$

as well as

$$k^{n-1} - (k-\mu)^{n-1} = \mu(k^{n-2} + \cdots + (k-\mu)^{n-2}).$$

Considering $\mu \geq n(n+1)/2$, we have

$$(k-\mu)^i k^{n-1-i} + \frac{(n+1)n}{2}(k-\mu)^{i-1}k^{n-1-i} \leq k^{n-1}$$

for $i \geq 1$, and hence

$$a_n(k^n - (k-\mu)^n) + a_{n-1}(k^{n-1} - (k-\mu)^{n-1}) \leq \frac{\mu}{n!}(k^{n-1} + \cdots + k^{n-1}) = \mu\frac{k^{n-1}}{(n-1)!}$$

as desired.

For μ less than $n(n+1)/2$, one simply bounds $k^{n-1} - (k-\mu)^{n-1} \leq O_n(k^{n-2})$ and the statement follows. □

Lemma 2.2. *Let $c, n, \mu > 0$ be integers. Let $g\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{>0}$ be a function with $g(0) = 1$ and satisfying $g(k) \leq \mu k^{n-1}/(n-1)! + c\mu k^{n-2}$ for $k > 0$. Let $(n_i)_{i\geq 1}$ be the nondecreasing sequence of integers $m \geq 0$ where m occurs exactly $g(m)$ times. Then for any $s \geq 0$ we have*

$$n_1 + \cdots + n_s \geq \left(\frac{n!}{\mu}\right)^{1/n} \frac{n}{n+1} s^{1+1/n} - O_{n,c}(s).$$

This statement is implicitly contained in the proof of [Salberger 2007, Main Lemma 2.5], but we give the full proof to stress that the error term does not depend on μ.

Proof. Note that replacing g by a function which is pointwise larger than g at any point only strengthens the claim, so we may as well assume that

$$g(k) = \frac{\mu}{n!}(k^n - (k-1)^n) + c\mu(k^{n-1} - (k-1)^{n-1})$$

for $k > 0$. Let $G\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ be given by $G(k) = g(0) + \cdots + g(k) = \frac{\mu}{n!}k^n + c\mu k^{n-1} + 1$. Now

$$\left(\frac{n!}{\mu}\right)^{1/n} \frac{n}{n+1} G(k)^{1+1/n} = \frac{\mu k^{n+1}}{(n-1)!(n+1)} + O_{n,c}(\mu k^n),$$

and

$$0g(0) + \cdots + kg(k) \geq \frac{\mu}{(n-1)!}\sum_{i\leq k}(i^n + O_n(ci^{n-1})) = \frac{\mu}{(n-1)!(n+1)}k^{n+1} + O_{n,c}(\mu k^n).$$

This proves the lemma for $s = G(k)$.

To deduce the result for general $s > 0$, let k be the unique integer with $G(k-1) < s \le G(k)$, and use

$$\begin{aligned} n_1 + \cdots + n_s \ge n_1 + \cdots + n_{G(k)} - kg(k) &\ge \left(\frac{n!}{\mu}\right)^{1/n} \frac{n}{n+1} G(k)^{1+1/n} - O_{n,c}(\mu k^n) \\ &\ge \left(\frac{n!}{\mu}\right)^{1/n} \frac{n}{n+1} s^{1+1/n} - O_{n,c}(s). \end{aligned}$$ □

Lemma 2.3. *Consider A as in Lemma 2.1, and let $(n_i(A))_{i\ge 1}$ be the nondecreasing sequence of integers $m \ge 0$ where m occurs exactly $\dim_{A/\mathfrak{m}} \mathfrak{m}^k/\mathfrak{m}^{k+1}$ times. Write $A(s) = n_1(A) + \cdots + n_s(A)$. Then*

$$A(s) \ge \left(\frac{n!}{\mu}\right)^{1/n} \left(\frac{n}{n+1}\right) s^{1+1/n} - O_n(s),$$

where the implied constant only depends on n.

Proof. This is immediate from the last two lemmas. □

As usual, write $\mathbb{Z}_{(p)}$ for the localization of $\mathbb{Z}$ at (the complement of) the prime ideal (p).

Lemma 2.4 (Lemma 2.4 of [Salberger 2007], cited as in the Appendix of [Browning et al. 2006]). *Let R be a noetherian local ring containing $\mathbb{Z}_{(p)}$, $A = R/pR$, and consider ring homomorphisms $\psi_1, \dots, \psi_s \colon R \to \mathbb{Z}_{(p)}$. Let $r_1, \dots, r_s$ be elements of R. Then the determinant of the $s \times s$-matrix $(\psi_i(r_j))$ is divisible by $p^{A(s)}$.*

Corollary 2.5 (Main Lemma 2.5 of [Salberger 2007]). *Let $\mathcal{X} \to \operatorname{Spec} \mathbb{Z}$ be the hypersurface in $\mathbb{P}^{n+1}_{\mathbb{Z}}$ cut out by the homogeneous polynomial f as above, so X is the generic fiber of $\mathcal{X}$ and X_p is the special fiber of $\mathcal{X}$ over p.*

Let P be an $\mathbb{F}_p$-point of multiplicity μ on X_p and let $\xi_1, \dots, \xi_s$ be $\mathbb{Z}$-points on $\mathcal{X}$, given by some primitive integer tuples, with reduction P. Let $F_1, \dots, F_s$ be homogeneous polynomials in $x_0, \dots, x_{n+1}$ with integer coefficients.

Then $\det(F_j(\xi_i))$ is divisible by p^e where

$$e \ge \left(\frac{n!}{\mu}\right)^{1/n} \frac{n}{n+1} s^{1+1/n} - O_n(s).$$

Proof. Let P' be the image of P under the closed embedding $X_p \hookrightarrow \mathcal{X}$, and R the stalk of $\mathcal{X}$ at P'. Then R is a noetherian local ring containing $\mathbb{Z}_{(p)}$, and R/pR is the stalk of X_p at P. Since P' is a specialization of all the ξ_i (this is precisely what it means that the ξ_i have reduction P), it makes sense to evaluate an element of R at each ξ_i, giving s ring homomorphisms $R \to \mathbb{Z}_{(p)}$.

The F_i induce $\mathbb{Z}_{(p)}$-valued polynomial functions on an affine neighborhood of P', and hence give elements of R. The statement now follows from the preceding two lemmas. □

Proposition 2.6. *Let $\mathcal{X}$ be as above. Let $\xi_1, \dots, \xi_s$ be $\mathbb{Z}$-points on $\mathcal{X}$, and $F_1, \dots, F_s$ be homogeneous polynomials in $n+1$ variables with integer coefficients. Then the determinant Δ of the $s \times s$-matrix*

$(F_i(\xi_j))$ is divisible by p^e, where

$$e \geq (n!)^{1/n} \frac{n}{n+1} \frac{s^{1+1/n}}{n_p^{1/n}} - O_n(s),$$

and where n_p is the number of $\mathbb{F}_p$-points on X_p, counted with multiplicity.

Proof. This is identical to the proof of [Salberger 2013, Lemma 1.4], see also the appendix of [Walsh 2015] — but we have eliminated the dependence of the constant on d. □

Lemma 2.7. *In the situation above, if $p > 27d^4$ and X_p is geometrically integral, i.e., the defining polynomial f has absolutely irreducible reduction modulo p, then $n_p \leq p^n + O_n(d^2 p^{n-1/2})$.*

Proof. By [Cafure and Matera 2006, Corollary 5.6] the number of $\mathbb{F}_p$-points of X_p counted without multiplicity is bounded by

$$\frac{p^{n+1} + (d-1)(d-2)p^{n+1/2} + (5d^2+d+1)p^n - 1}{p-1} \leq p^n + O_n(d^2 p^{n-1/2}).$$

(This uses the lower bound on p and the condition on X_p.)

The singular points of X_p all lie in the algebraic set cut out by f and $\frac{\partial f}{\partial x_0}$, which can be assumed to be nonzero without loss of generality. This is an algebraic set all of whose components have codimension 2 and the sum of the degrees of these components is bounded by d^2. The standard Lang–Weil estimate yields that there are $O_n(d^2 p^{n-1}) \leq O_n(dp^{n-1/2})$ points on this algebraic set and hence at most that many singular points, each of which has multiplicity at most d. Adding this term to the number of points counted without multiplicity yields the claim. □

Lemma 2.8. *In the situation above, with $p > 27d^4$ and X_p geometrically integral, we have $n_p^{1/n}/p - 1 \leq O_n(d^2 p^{-1/2})$.*

Proof. Apply the general inequality $x^{1/n} - 1 \leq x - 1$ for $x \geq 1$. □

We immediately obtain the following from Proposition 2.6.

Corollary 2.9. *The determinant Δ from Proposition 2.6 is divisible by p^e, where*

$$e \geq (n!)^{1/n} \frac{n}{n+1} \frac{s^{1+1/n}}{p + O_n(d^2 p^{1/2})} - O_n(s).$$

This is stated as Theorem 2.2 in [Walsh 2015], but our statement is more precise in terms of the implied constants.

3. Points on projective hypersurfaces à la Walsh

3.1. ***Formulation of main result.*** The following result is the goal of this section and an improvement to Theorem 1.3 of [Walsh 2015]. Call a polynomial f over $\mathbb{Z}$ primitive if the greatest common divisor of its coefficients equals 1. For any f, we write $\|f\|$ for the maximum of the absolute values of the coefficients of f.

Theorem 3.1.1. *Let $n > 0$ be an integer. Then there exists c (depending on n) such that the following holds for all choices of f, d, B. Let f be a primitive irreducible homogeneous polynomial in $\mathbb{Z}[x_0, \dots, x_{n+1}]$ of degree $d \geq 1$, and write X for the hypersurface in $\mathbb{P}^{n+1}_{\mathbb{Q}}$ cut out by f. Choose $B \geq 1$. Then there exists a homogeneous g in $\mathbb{Z}[x_0, \dots, x_{n+1}]$ of degree at most*

$$cB^{(n+1)/(nd^{1/n})} \frac{d^{4-1/n} b(f)}{\|f\|^{1/n \cdot 1/d^{1+1/n}}} + cd^{1-1/n} \log B + cd^{4-1/n},$$

not divisible by f, and vanishing at all points on X of height at most B.

Here the quantity $b(f)$ is defined in Definition 3.2.1; it always satisfies $b(f) \leq O(\max(d^{-2} \log\|f\|, 1))$. The main improvement over [Walsh 2015] lies in the polynomial dependence on the degree d.

We also immediately obtain the following, which is the essential tool for proving Theorem 2.

Corollary 3.1.2. *For any primitive irreducible polynomial $f \in \mathbb{Z}[x_0, x_1, x_2]$ homogeneous of degree d and any $B \geq 1$ we have*

$$N(f, B) \leq cB^{2/d} \frac{d^4 b(f)}{\|f\|^{1/d^2}} + cd \log B + cd^4 \leq c' d^4 B^{2/d},$$

where c, c' are absolute constants.

Proof. Apply Theorem 3.1.1 to obtain a polynomial g, and then apply Bézout's theorem to the curves defined by f and g. This yields the first inequality. For the second inequality we can use that $b(f)/\|f\|^{1/d^2}$ is bounded because $b(f) \leq O(\max(d^{-2} \log\|f\|, 1))$. □

3.2. *A determinant estimate.* In this section we want to use the results of Section 2 for a number of primes simultaneously. It is useful to introduce the following measure of the set of primes modulo which an absolutely irreducible polynomial over the integers ceases to be absolutely irreducible.

Definition 3.2.1. For an integer polynomial f in an arbitrary number of variables we set $b(f) = 0$ if f is not absolutely irreducible, and

$$b(f) = \prod_p \exp\left(\frac{\log p}{p}\right)$$

otherwise, where the product is over those primes $p > 27d^4$ such that the reduction of f modulo p is not absolutely irreducible.

For now we work with a degree d hypersurface in $\mathbb{P}^{n+1}$ defined by a primitive polynomial $f \in \mathbb{Z}[x_0, \dots, x_{n+1}]$ which is absolutely irreducible. We first establish a basic estimate on $b(f)$, showing in particular that it is finite.

Theorem 3.2.2 (explicit Noether polynomials, [Ruppert 1986, Satz 4]). *Let $d \geq 2$, $n \geq 3$. There is a collection of homogeneous polynomials Φ in $\binom{n+d}{n}$ variables over $\mathbb{Z}$ of degree $d^2 - 1$, such that*

$$\|\Phi\|_1 \leq d^{3d^2-3} \left[\binom{n+d}{n} 3^d \right]^{d^2-1}$$

(*where* $\|\cdot\|_1$ *denotes the sum of the absolute values of the coefficients*), *and such that the following holds for any polynomial F in $n+1$ variables homogeneous of degree d over any field*:

- *If F is not absolutely irreducible*, *then all the Φ vanish when applied to the coefficients of F*, *reducing modulo the characteristic of the ground field if necessary.*
- *If F is absolutely irreducible over a field of characteristic* 0, *then one of the Φ does not vanish when applied to the coefficients of F.*

Corollary 3.2.3. $b(f) \leq O(\max(d^{-2}\log\|f\|, 1))$.

Proof. Write $\mathcal{P}$ for the set of prime numbers $p > 27d^4$ modulo which f is not absolutely irreducible. There exists a Noether form Φ with coefficients in $\mathbb{Z}$ such that Φ applied to the coefficients of f is nonzero, but is divisible by any prime in $\mathcal{P}$. In particular, the product of such p is bounded by $c := \|\Phi\|_1\|f\|^{\deg\Phi}$. Now

$$\begin{aligned}\log b(f) &= \sum_{p\in\mathcal{P}} \frac{\log p}{p}\\ &\leq \sum_{27d^4<p\leq\log c} \frac{\log p}{p} + \sum_{\log c<p\in\mathcal{P}} \frac{\log p}{\log c}\\ &\leq \max(\log\log c - 4\log d, 0) + O(1) + \frac{\log c}{\log c}\\ &\leq \max(\log\log c - 4\log d, 0) + O(1)\\ &\leq \max(\log(\deg\Phi\log\|f\|) - 4\log d, \log\log\|\Phi\|_1 - 4\log d, 0) + O(1),\end{aligned}$$

where we have used that the function $\log x - \sum_{p\leq x}\log p/p$ is bounded (Mertens' first theorem). Since $\log\log\|\Phi\|_1 - 4\log d$ is bounded above, the claim follows. □

We now adapt [Walsh 2015, Theorem 2.3], keeping track of the dependency on the degree and on $b(f)$.

Lemma 3.2.4. *For any $x > 0$, $\sum_{p\leq x}\log p \leq 2x$, where the sum extends over prime numbers not exceeding x.*

Proof. This is a classical estimate on the first Chebyshev function. □

Lemma 3.2.5. *As x varies over positive real numbers we have $\sum_{p>x}\log p/p^{3/2} = O(x^{-1/2})$, where the sum extends over prime numbers greater than x.*

Proof. Estimate the density of prime numbers using the prime number theorem and compare the sum with an integral. □

Proposition 3.2.6. *Let $(\xi_1, \ldots, \xi_s)$ be a tuple of rational points in X, let $F_{li} \in \mathbb{Z}[x_0, \ldots, x_{n+1}]$, $1 \leq l \leq L$, $1 \leq i \leq s$, be homogeneous polynomials with integer coefficients, and write Δ_l for the determinant of*

$(F_{li}(\xi_j))_{ij}$. Let Δ be the greatest common divisor of the Δ_l, and assume that $\Delta \neq 0$. Then we have the bound

$$\log|\Delta| \geq \frac{n!^{1/n}}{n+1} s^{1+1/n}(\log s - O_n(1) - n(4\log d + \log b(f))).$$

This is a more explicit variant of [Walsh 2015, Theorem 2.3].

Proof. Let $\mathcal{P}$ be the collection of prime numbers p such that either $p \leq 27d^4$ or X_p is not geometrically integral.

We now apply Corollary 2.9 to all prime numbers $p \leq s^{1/n}$ not in $\mathcal{P}$, yielding

$$\log|\Delta| \geq \frac{n!^{1/n} n}{n+1} s^{1+1/n} \sum_{\mathcal{P} \not\ni p \leq s^{1/n}} \frac{\log p}{p + O_n(d^2 p^{1/2})} - O_n(s) \sum_{p \leq s^{1/n}} \log p.$$

The last term is bounded by $O_n(1) s^{1+1/n}$.

In estimating the main term, we may use that $1/(p + O_n(d^2 p^{1/2})) \geq 1/p - O_n(d^2)/p^{3/2}$. We can then bound

$$\begin{aligned}
\sum_{\mathcal{P} \not\ni p \leq s^{1/n}} \frac{\log p}{p + O_n(d^2 p^{1/2})} &\geq \sum_{p \leq s^{1/n}} \frac{\log p}{p} - \sum_{p \in \mathcal{P}} \frac{\log p}{p} - O_n(d^2) \sum_{\mathcal{P} \not\ni p \leq s^{1/n}} \frac{\log p}{p^{3/2}} \\
&\geq \frac{\log s}{n} - \sum_{p \leq 27d^4} \frac{\log p}{p} - \log b(f) - O(1) - O_n\biggl(d^2 \sum_{p > 27d^4} \frac{\log p}{p^{3/2}}\biggr) \\
&\geq \frac{\log s}{n} - \log(27d^4) - \log b(f) - O(1) - O_n(d^2 (27d^4)^{-1/2}) \\
&\geq \frac{\log s}{n} - 4\log d - \log b(f) - O_n(1).
\end{aligned}$$

□

3.3. *The main estimates.* We first establish that we can reduce to the case of absolutely irreducible f in the proof of Theorem 3.1.1.

Lemma 3.3.1. *If $f \in \mathbb{Z}[x_0, \dots, x_{n+1}]$ is homogeneous of degree $d \geq 1$ and irreducible but not absolutely irreducible, then there exists another polynomial $g \in \mathbb{Z}[x_0, \dots, x_{n+1}]$ of degree d, not divisible by f, which vanishes on all rational zeroes of f.*

Proof. This is established in the first paragraph of Section 4 of [Walsh 2015]. □

Let us now work with a restricted class of homogeneous polynomials f, namely those which are absolutely irreducible and for which the leading coefficient c_f, i.e., the coefficient of the monomial x_{n+1}^d, satisfies

$$c_f \geq \|f\| C^{-nd^{1+1/n}}$$

for some positive constant C which is allowed to depend on n (for this reason the factor n in the exponent is in fact superfluous, but it simplifies the proof write-up below).

The two main results are the following:

Lemma 3.3.2. *For f as above, and B satisfying $\|f\| \leq B^{2d(n+1)}$, there exists a homogeneous polynomial g not divisible by f, vanishing at all zeroes of f of height at most B, and of degree*

$$M = O_n(1)B^{(n+1)/(nd^{1/n})}\frac{d^{4-1/n}b(f)}{\|f\|^{n^{-1}d^{-1-1/n}}} + d^{1-1/n}\log B + O_n(d^2).$$

Lemma 3.3.3. *For f as above, and B satisfying $\|f\| \geq B^{2d(n+1)}$, there exists a homogeneous polynomial g not divisible by f, vanishing at all zeroes of f of height at most B, and of degree*

$$M = O_n(d^{4-1/n}).$$

These two lemmas together clearly imply the statement of Theorem 3.1.1, at least for polynomials f satisfying the condition on leading coefficients.

We follow the exposition in [Walsh 2015, Section 4], and prove the two lemmas together. We shall need the following.

Theorem 3.3.4 [Bombieri and Vaaler 1983, Theorem 1]. *Let $\sum_{k=1}^{r} a_{mk}x_k = 0$ $(m = 1, \ldots, s)$ be a system of s linearly independent equations in $r > s$ variables $x_1, \ldots, x_r$, with coefficients $a_{mk} \in \mathbb{Z}$. Then there exists a nontrivial integer solution $(x_1, \ldots, x_r)$ satisfying*

$$\max_{1\leq i\leq r} |x_i| \leq (D^{-1}\sqrt{|\det(AA^\top)|})^{1/(r-s)}.$$

Here $A = (a_{mk})$ is the matrix of coefficients and D is the greatest common divisor of the determinants of the $s \times s$ minors of A.

Proof of Lemmas 3.3.2 and 3.3.3. Fix $B \geq 1$, and let S be the set of rational points on the hypersurface described by f of height at most B. Let $M > 0$ be such that there is no homogeneous polynomial g of degree M, not divisible by f, which vanishes on all points in S; we shall show that M is bounded in terms of n, B, d, $\|f\|$ as stated. Let us assume in the following that M is bigger than some constant (to be specified later) times d^2.

Given an integer D, write $\mathcal{B}[D]$ for the set of monomials of degree D in $n+2$ variables, so $|\mathcal{B}[D]| = \binom{D+n+1}{n+1}$. Write $\Xi \subseteq S$ for a maximal subset which is algebraically independent over monomials of degree M, in the sense that applying all monomials in $\mathcal{B}[M]$ to Ξ yields $s = |\Xi|$ linearly independent vectors. Let A be the $s \times r$ matrix whose rows are these vectors, where $r = |\mathcal{B}[M]| = \binom{M+n+1}{n+1}$; each entry of A is bounded in absolute value by B^M. Since all polynomials in $f \cdot \mathcal{B}[M-d]$ vanish on Ξ, and no polynomials of degree M not divisible by f do by assumption on M, we have $s = |\mathcal{B}[M]| - |\mathcal{B}[M-d]|$.

Now A describes a system of linear equations whose solutions correspond to (the coefficients of) homogeneous polynomials of degree M vanishing on all points in Ξ and therefore all points in S; by assumption, these polynomials are multiples of f and therefore have one coefficient of size at least $c_f \geq \|f\|C^{-nd^{1+1/n}}$ by the assumption on f. Hence Theorem 3.3.4 yields

$$\Delta \leq \sqrt{|\det(AA^\top)|}(\|f\|C^{-nd^{1+1/n}})^{s-r},$$

where we write Δ for the greatest common divisor of the determinants of the $s \times s$ minors of A. Taking logarithms, using the estimate $|\det(AA^\top)| \leq s!(rB^M)^s$ obtained by estimating the size of the coefficients of $AA^\top$, and using the estimate for Δ obtained from Proposition 3.2.6, this expands as follows:

$$\frac{n!^{1/n}}{n+1}s^{1+1/n}(\log s - O_n(1) - n(4\log d + \log b(f)))$$
$$\leq \frac{\log s!}{2} + \frac{s}{2}\log r + sM\log B - (r-s)(\log\|f\| - nd^{1+1/n}O_n(1))$$

We can use the estimates $\log s! \leq s\log s$ and $\log r \leq \log(M+1)^{n+1} \leq O_n(\log M) \leq O_n(\log s)$ to see that the first two terms on the right-hand side are both in $O_n(s^{1+1/n})$ and can hence be neglected by adjusting the constant $O_n(1)$ on the left-hand side. Dividing by Ms now yields:

$$\frac{n!^{1/n}}{n+1}\frac{s^{1/n}}{M}(\log s - O_n(1) - n(4\log d + \log b(f))) \leq \log B - \frac{r-s}{Ms}(\log\|f\| - nd^{1+1/n}O_n(1)) \quad (3\text{-}3\text{-}1)$$

The term $s = \binom{M+n+1}{n+1} - \binom{M-d+n+1}{n+1}$ is a polynomial in M and d. We can write

$$s = \frac{dM^n}{n!} + O_n(d^2M^{n-1}),$$

in particular $\log s = \log d + n\log M - O_n(1)$. By rearranging and applying the binomial series, which is legal since d^2/M is bounded above by an adjustable absolute constant, we also obtain

$$\frac{s^{1/n}}{M} = \frac{d^{1/n}}{n!^{1/n}} + O_n\left(\frac{d^2}{M}\right).$$

Thus the left-hand side of the inequality above can be replaced by

$$\frac{d^{1/n}n}{n+1}\left(\log M - O_n(1) - \left(\left(4 - \frac{1}{n}\right)\log d + \left(1 + O_n\left(\frac{d^{2-1/n}}{M}\right)\right)\log b(f)\right)\right),$$

where we have dropped terms $O_n(d^{2-1/n}\log M/M)$ and $O_n(d^{2-1/n}\log d/M)$ by adjusting the constant in $O_n(1)$.

Let us now estimate $(r-s)/(Ms)$. We have $r - s = (M^{n+1})/((n+1)!) + O_n(dM^n)$, so

$$\frac{r-s}{Ms} = \frac{1}{d(n+1)}\frac{1+O_n(d/M)}{1+O_n(d/M)} = \frac{1}{d(n+1)} + O_n\left(\frac{1}{M}\right).$$

Therefore inequality (3-3-1) becomes

$$\frac{d^{1/n}n}{n+1}\left(\log M - O_n(1) - \left(\left(4 - \frac{1}{n}\right)\log d + \left(1 + O_n\left(\frac{d^{2-1/n}}{M}\right)\right)\log b(f)\right)\right)$$
$$\leq \log B - \frac{\log\|f\|}{d(n+1)} - O_n\left(\frac{\log\|f\|}{M}\right). \quad (3\text{-}3\text{-}2)$$

Let us now assume that $\|f\| \leq B^{2d(n+1)}$ and $M \geq d^{1-1/n}\log B$. Then $\log\|f\| \leq 2d(n+1)\log B \leq O_n(d^{1/n}M)$, so we can drop the last term on the right-hand side, as well as the $O_n(\log b(f)/M)$ on the left-hand side. Rearranging yields that

$$\log M \le O_n(1) + \frac{n+1}{d^{1/n}n}\log B - \frac{\log\|f\|}{nd^{1+1/n}} + \left(4 - \frac{1}{n}\right)\log d + \log b(f),$$

so we obtain Lemma 3.3.2.

Now, on the other hand, assume that $\|f\| \ge B^{2d(n+1)}$ and $M \ge 4d(n+1)$. Rearranging inequality (3-3-2) yields

$$\begin{aligned}\log M &\le O_n(1) + \left(4 - \frac{1}{n}\right)\log d + (1 + O_n(d^{-1/n}))\log b(f) - \frac{\log\|f\|}{4nd^{1+1/n}}\\ &\le O_n(1) + \max\left\{3\log d, \left(4 - \frac{1}{n}\right)\log d\right\},\end{aligned}$$

where we have used

$$\begin{aligned}O_n(1)\log b(f) - \frac{\log\|f\|}{4nd^{1+1/n}} &\le O_n(1)\max(\log\log\|f\| - 2\log d, 0) - \frac{\log\|f\|}{4nd^{1+1/n}}\\ &\le \max(0, -2\log d + \log(O_n(1)4nd^{1+1/n}))\\ &\le O_n(1)\end{aligned}$$

by Corollary 3.2.3 and the lemma below. This establishes Lemma 3.3.3. □

Lemma 3.3.5. *Let $c > 0$. For any $x > 1$ we have* $\log\log x - \log(x)/c \le \log c + O(1)$.

Proof. Let $C = \sup_{x>1}(\log\log x - \log x)$; note that the supremum exists, since it is taken over a continuous function on $]1, \infty[$ which tends to $-\infty$ at both ends of the interval. Now $\log\log x - \log(x)/c = \log c + \log\log x^{1/c} - \log x^{1/c} \le \log c + C$. □

3.4. ***Finishing the proof.*** We use ideas from [Walsh 2015, Section 3] to finish the proof of Theorem 3.1.1.

Lemma 3.4.1. *Let $f \in \mathbb{C}[x]$ be a polynomial of degree $\le d$, and write $\|f\|$ for the maximal absolute value among the coefficients. There exists an integer a, $0 \le a \le d$, such that $|f(a)| \ge 3^{-d}\|f\|$.*

Proof. This is a statement about the $\|\cdot\|_\infty$-operator norm of the inverse of the Vandermonde matrix with nodes $0, \dots, d$, which can be deduced from [Gautschi 1962, Theorem 1]. □

Lemma 3.4.2. *Let $f \in \mathbb{C}[x_0, \dots, x_{n+1}]$ be homogeneous of degree d. There exist integers $a_0, \dots, a_n$ with $0 \le a_i \le d$ such that $|f(a_0, \dots, a_n, 1)| \ge 3^{-(n+1)d}\|f\|$.*

Proof. Dehomogenize by setting $x_{n+1} = 1$, and then use induction with the preceding lemma. □

Proof of Theorem 3.1.1. Take a nonzero $f \in \mathbb{Z}[x_0, \dots, x_{n+1}]$ homogeneous of degree d. Consider $a_0, \dots, a_n$ as in the last lemma and let $A = I + A_0 \in \mathrm{SL}_{n+2}(\mathbb{Z})$, where I is the $(n+2) \times (n+2)$ identity matrix and A_0 has its last column equal to $(a_0, \dots, a_n, 0)$ and zero everywhere else. Note that $A^{-1} = I - A_0$.

Let $f' = f \circ A$. By construction, the x_{n+1}^d-coefficient of f' is $\geq 3^{-(n+1)d}\|f\|$. Because of the boundedness of the entries of A, we furthermore see that

$$\|f'\| \leq d^d (n+2)^d \binom{n+d+1}{n+1} \|f\| \leq \exp(O_n(d^{1+1/n}))\|f\|.$$

In particular, the x_{n+1}^d-coefficient of f' is greater than $C^{-nd^{1+1/n}}\|f'\|$ for some constant C depending only on n. The polynomial f' is primitive if and only if f is, since they are related by the matrices A, A^{-1} with integer coefficients, and $b(f) = b(f')$. Furthermore, if g' is a homogeneous polynomial in $\mathbb{Z}[x_0, \ldots, x_{n+1}]$ vanishing on all zeroes of f' up to a certain height B', then $g = g' \circ A^{-1}$ is a polynomial of the same degree vanishing on all zeroes of f up to height $B = B'/(d+1)$.

Since either Lemma 3.3.2 or Lemma 3.3.3 applies to f' and B', we obtain the desired statement for f. □

4. Proofs of Theorems 1, 2, 3, 4, 6

4.1. ***On trivial bounds.*** In this subsection, we extend our notation to varieties defined over any field K containing $\mathbb{Q}$, and we write $N(X, B)$ for the number of points in $\mathbb{P}^n(\mathbb{Q}) \cap X(K)$ of height at most B, when X is a subvariety of $\mathbb{P}_K^n$, and similarly we write $N_{\text{aff}}(Y, B)$ for the number of points in $\mathbb{Z}^n \cap Y(K) \cap [-B, B]^n$, when $Y \subseteq \mathbb{A}_K^n$.

Lemma 4.1.1. *Let $X \subseteq \mathbb{A}_{\overline{\mathbb{Q}}}^n$ be a (possibly reducible) variety of pure dimension m and degree d defined over $\overline{\mathbb{Q}}$. Then the number $N_{\text{aff}}(X, B)$ of integral points on X of height at most B is bounded by $d(2B+1)^m$.*

When X is a hypersurface, this is the well-known Schwarz–Zippel bound, and even the general case appears in many places in the literature, albeit often without making the bound completely explicit.

Proof. This is an easy inductive argument using intersections with shifts of coordinate hyperplanes. In fact, the proof of [Browning and Heath-Brown 2005, Theorem 1] automatically gives this stronger statement. □

Corollary 4.1.2. *For an irreducible affine variety X in $\mathbb{A}^n$ of degree d and dimension $< n$ there exists a tuple $(a_1, \ldots, a_n)$ of integers not on X, with $|a_i| \leq d$ for every i. For every irreducible projective variety X in $\mathbb{P}^n$ of degree d and dimension $< n$ there exists a point in $\mathbb{P}^n(\mathbb{Q})$ of height at most d not on X.*

Proof. The affine version is implied by the preceding lemma, and the projective version follows by considering the affine cone. □

Lemma 4.1.3. *Let $X \subseteq \mathbb{A}_{\overline{\mathbb{Q}}}^n$ be an absolutely irreducible variety of dimension m and degree d not defined over $\mathbb{Q}$. Then the number $N_{\text{aff}}(X, B)$ of integral points on X of height at most B is bounded by $d^2(2B+1)^{m-1}$.*

By considering the affine cone over a projective variety, this result also applies to projective varieties of dimension m, with bound $d^2(2B+1)^m$.

Proof. For every field automorphism σ of $\overline{\mathbb{Q}}$, there is a conjugate variety X^σ. Since X is not defined over $\mathbb{Q}$, there exists a σ with $X^\sigma \neq X$. All $\mathbb{Q}$-points of X necessarily also lie on X^σ. Since X^σ has degree d, it is the intersection of hypersurfaces of degree $\leq d$, see for instance [Heintz 1983, Proposition 3]. Let Y be a hypersurface of degree $\leq d$ containing X^σ and not containing X. Then $X \cap Y$ is a variety of pure dimension $m-1$ and degree at most d^2. Now Lemma 4.1.1 gives the result. □

The following allows us to reduce to the geometrically irreducible situation when counting points on varieties.

Corollary 4.1.4. *Let $X \subseteq \mathbb{A}^n$ be an irreducible variety over $\mathbb{Q}$ of dimension m and degree d which is not geometrically irreducible. Then for any $B \geq 1$ we have $N_{\text{aff}}(X, B) \leq d^2(2B+1)^{m-1}$.*

As above, this also applies to projective varieties.

Proof. Let $K/\mathbb{Q}$ be a finite Galois extension over which X splits into absolutely irreducible components, and let Y be one of the components. Since all components are Galois-conjugate, the $\mathbb{Q}$-points on X in fact also lie on Y. Now the preceding lemma applied to Y gives the result. □

Remark 4.1.5. Note that this trivially proves Theorems 1 and 3 for irreducible, but not geometrically irreducible varieties, and similarly for absolutely irreducible varieties defined over $\overline{\mathbb{Q}}$ but not over $\mathbb{Q}$. The same applies for Theorem 2 by considering a projective curve as the union of an affine curve with a finite number of points.

Thus we henceforth only need to concern ourselves with absolutely irreducible varieties defined over $\mathbb{Q}$.

4.2. ***Affine counting.*** Our results for projective hypersurfaces from the last section yield the following result for affine hypersurfaces, by refining the technique given in [Ellenberg and Venkatesh 2005, Remark 2.3].

Proposition 4.2.1. *Fix an integer $n > 0$. Then there exist c and e such that the following holds for all f, B, d. Let $f \in \mathbb{Z}[x_1, \ldots, x_{n+1}]$ be irreducible, primitive and of degree d. For each i write f_i for the degree i homogeneous part of f. Fix $B \geq 1$. Then there is a polynomial g in $\mathbb{Z}[x_1, \ldots, x_{n+1}]$ of degree at most*

$$cB^{1/d^{1/n}} d^{2-1/n} \frac{\min(\log\|f_d\| + d\log B + d^2, d^2 b(f))}{\|f_d\|^{1/n \cdot 1/d^{1+1/n}}} + cd^{1-1/n}\log B + cd^{4-1/n},$$

not divisible by f, and vanishing on all points x in $\mathbb{Z}^{n+1}$ satisfying $f(x) = 0$ and $|x_i| \leq B$.

To prove Proposition 4.2.1 we need the following lemmas:

Lemma 4.2.2 [Browning et al. 2006, Lemma 5]. *Let $f \in \mathbb{Z}[x_1, \ldots, x_{n+2}]$ be a primitive absolutely irreducible polynomial, homogeneous of degree d, defining a hypersurface Z in $\mathbb{P}^{n+1}$. Let $B \geq 1$. Then either the height of the coefficients of f is bounded by $O_n(B^{d\binom{d+n+1}{n+1}})$, or there exists a homogeneous polynomial g of degree d vanishing on all points of Z of height at most B.*

Lemma 4.2.3. *For $F \in \mathbb{Z}[x_1, \dots, x_{n+2}]$ an irreducible primitive homogeneous polynomial and $1 \le y \le \|F\|$ we have*

$$d^{4-1/n} \frac{b(F)}{\|F\|^{1/n \cdot 1/d^{1+1/n}}} \le O_n(1) d^{2-1/n} \frac{\log y + d^2}{y^{1/n \cdot 1/d^{1+1/n}}}.$$

Proof. The function

$$x \mapsto \frac{\log x}{x^{1/n \cdot 1/d^{1+1/n}}}$$

on $(1, \infty)$ is monotonically increasing up to its maximum when $x^{1/n \cdot 1/d^{1+1/n}} = e$, and monotonically decreasing thereafter.

Let us write $x = \|F\|$ and use $d^2 b(F) \le O_n(1)(\log x + d^2)$ by Corollary 3.2.3. By the monotonicity considered above, there is nothing to show when $y^{1/n \cdot 1/d^{1+1/n}} \ge e$. Otherwise,

$$2d^{2-1/n} \frac{\log y + d^2}{y^{1/n \cdot 1/d^{1+1/n}}} \ge 2d^{2-1/n} \frac{d^2}{y^{1/n \cdot 1/d^{1+1/n}}} \ge d^{4-1/n} \left(\frac{1}{e} + \frac{1}{y^{1/n \cdot 1/d^{1+1/n}}} \right),$$

and the left-hand side of the inequality in the statement is always bounded by

$$O_n(1) d^{2-1/n} \frac{\log x + d^2}{x^{1/n \cdot 1/d^{1+1/n}}} \le O_n(1) d^{2-1/n} \left(\frac{n d^{1+1/n}}{e} + \frac{d^2}{x^{1/n \cdot 1/d^{1+1/n}}} \right),$$

yielding the claim. □

As mentioned above, the following proof follows [Ellenberg and Venkatesh 2005, Remark 2.3]; but additionally we bring in the idea of forming the homogeneous polynomial F_H for primes H in the range $(B/2; B]$ to control primitivity.

Proof of Proposition 4.2.1. By applying Lemma 3.3.1 to the homogenization of f, we may assume that f is absolutely irreducible. For each natural number H, consider the polynomial $F_H \in \mathbb{Z}[x_1, \dots, x_{n+2}]$ given by $F_H(x_1, \dots, x_{n+2}) = \sum_{i=0}^{d} H^i f_i x_{n+2}^{d-i}$. Then F_H is an irreducible homogeneous polynomial of degree d. On the other hand, each integral point $(x_1, \dots, x_{n+1}) \in Z(f)(\mathbb{Z})$ gives us a rational point $(x_1, \dots, x_{n+1}, H)$ in $Z(F_H)(\mathbb{Q})$, where $Z(f)$ stands for the hypersurface in $\mathbb{A}^{n+1}$ given by f and $Z(F_H)$ stands for the hypersurface in $\mathbb{P}^{n+1}$ given by F_H.

If B is bounded by some polynomial expression in d (to be determined later), then $B^{1/(nd^{1/n})}$ is bounded by a constant depending only on n; hence we use Theorem 3.1.1 for F_1, by which there exists a number c depending only on n along with a homogeneous polynomial G_1 in $\mathbb{Z}[x_1, \dots, x_{n+2}]$ of degree at most

$$c B^{1/d^{1/n}} d^{4-1/n} \frac{b(F_1)}{\|F_1\|^{1/n \cdot 1/d^{1+1/n}}} + c d^{1-1/n} \log B + c d^{4-1/n},$$

not divisible by F_1, and vanishing at all points on $Z(F_1)(\mathbb{Q})$ of height at most B. Since $b(F_1) = b(f)$ and $\|F_1\| \ge \|f_d\|$, by Lemma 4.2.3 we obtain

$$d^{4-1/n} \frac{b(F_1)}{\|F_1\|^{1/n \cdot 1/d^{1+1/n}}} \le O_n(d^{2-1/n}) \frac{\min(d^2 b(f), \log\|f\| + d^2)}{\|f_d\|^{1/n \cdot 1/d^{1+1/n}}}.$$

Hence the polynomial $g(x_1,\dots,x_{n+1}) = G_1(x_1,\dots,x_{n+1},1)$ satisfies our proposition.

For any $B \geq 2$ Bertrand's postulate guarantees the existence of a prime B' in the interval $(B/2, B]$. Moreover, if $B' \nmid f_0$, then $F_{B'}$ is primitive. By Theorem 3.1.1 for $F_{B'}$, there exists a number c depending only on n along with a homogeneous polynomial $G_{B'}$ in $\mathbb{Z}[x_1,\dots,x_{n+2}]$ of degree at most

$$cB^{(n+1)/nd^{1/n}} d^{4-1/n} \frac{b(F_{B'})}{\|F_{B'}\|^{1/n\cdot 1/d^{1+1/n}}} + cd^{1-1/n}\log B + cd^{4-1/n},$$

not divisible by $F_{B'}$, and vanishing at all points on $Z(F_{B'})(\mathbb{Q})$ of height at most B.

It is clear that $\|F_{B'}\| \geq B'^d \|f_d\| \geq 2^{-d}B^d\|f_d\|$, so by Lemma 4.2.3 we have

$$d^{4-1/n}\frac{b(F_{B'})}{\|F_{B'}\|^{1/n\cdot 1/d^{1+1/n}}} \leq O_n(1)\left(\frac{B}{2}\right)^{-1/(nd^{1/n})} d^{2-1/n}\frac{\log\|f_d\| + d\log B + d^2}{\|f_d\|^{1/n\cdot 1/d^{1+1/n}}}.$$

Furthermore $b(F_{B'})$ agrees with $b(F_1)$ up to a factor of $\exp(\log B'/B') \leq O(1)$. Hence we in fact have

$$d^{4-1/n}\frac{b(F_{B'})}{\|F_{B'}\|^{1/n\cdot 1/d^{1+1/n}}} \leq O_n(1)B^{-1/(nd^{1/n})} d^{2-1/n}\frac{\min(\log\|f_d\| + d\log B + d^2, b(f))}{\|f_d\|^{1/n\cdot 1/d^{1+1/n}}}.$$

Thus the polynomial $g(x_1,\dots,x_{n+1}) = G_{B'}(x_1,\dots,x_{n+1},B')$ is as desired.

From now on, we suppose that $B > 2$ and $B' \mid f_0$ for all primes B' in the interval $(B/2, B]$. Then we have

$$\Bigg(\prod_{\substack{B' \text{ prime} \\ B/2<B'\leq B}} B'\Bigg) \mid f_0$$

If $f_0 \neq 0$ then we deduce that

$$\sum_{B'\text{prime}, B/2<B'\leq B} \log B' \leq \log|f_0|.$$

By Lemma 4.2.2, we are done if f_0 is large compared to $B^{d\binom{d+n+1}{n+1}}$, so in the remaining case we have

$$\sum_{B'\text{prime}, B/2<B'\leq B} \log B' \leq d\binom{d+n+1}{n+1}\log B - O_n(1)$$

Because of the well-known estimate

$$\lim_{x\mapsto+\infty}\frac{\sum_{p\leq x}\log p}{x} = 1,$$

we see that B is necessarily bounded by a certain polynomial in d in this case, so we are done by the discussion above.

If $f(0) = 0$, then by Corollary 4.1.2 there exists an integer point $A = (a_1,\dots,a_{n+1})$ with $f(a_1,\dots,a_{n+1}) \neq 0$ and $|a_i| \leq d$ for all $1 \leq i \leq n+1$. We consider the shifted polynomial $\tilde{f}(x) = f(x+A)$, for which $\tilde{f}(0) \neq 0$, $\|f_d\| = \|\tilde{f}_d\|$, and $b(\tilde{f}) = b(f)$. We apply the above discussion for $\tilde{f}$ and $\tilde{B} = B + d$ to obtain a polynomial $\tilde{g}(x)$ vanishing on all zeroes of $\tilde{f}$ of height at most $\tilde{B}$, and take $g(x) = \tilde{g}(x - A)$. This satisfies the required degree bound since $\tilde{g}$ does. □

Corollary 4.2.4. *There exists a constant c such that for all $d > 0$ and all irreducible affine curves $X \subseteq \mathbb{A}^2_{\mathbb{Q}}$ of degree d, cut out by an irreducible primitive polynomial $f \in \mathbb{Z}[x_1, x_2]$, and all $B \geq 1$ one has*

$$N_{\mathrm{aff}}(X, B) \leq cB^{1/d}\frac{\min(d^2\log\|f_d\| + d^3\log B + d^4, d^4 b(f))}{\|f_d\|^{1/d^2}} + cd\log B + cd^4.$$

Proof. Take $n = 1$ in Proposition 4.2.1 and apply Bézout's theorem. □

If the absolute irreducibility of f can be explained by the indecomposability of its Newton polytope, e.g., in the sense of [Gao 2001], then this allows for good bounds on $b(f)$ which get rid of the factor $\log B$. The following instance will be used to prove Theorem 6:

Corollary 4.2.5. *There exists a constant c such that for all affine curves $X \subseteq \mathbb{A}^2_{\mathbb{Q}}$ cut out by a polynomial $f \in \mathbb{Z}[x_1, x_2]$ of the form*

$$c_d x_1^d + c_{d'} x_2^{d'} + \sum_{\substack{i,i' \\ id'+i'd<dd'}} c_{ij} x_1^i x_2^{i'}$$

with $d > d' > 0$ coprime integers and $c_d, c_{d'} \neq 0$, and for all $B \geq 1$, one has

$$N_{\mathrm{aff}}(X, B) \leq cd^4(\log|c_d c_{d'}| + 1)B^{1/d}.$$

Proof. By dividing out by the greatest common divisor of the coefficients, we may suppose that f is primitive. The presence of the edge $(d, 0)$–$(0, d')$ in the Newton polytope of f is enough to guarantee absolute irreducibility in any characteristic [Gao 2001, Theorem 4.11]. Therefore we can bound

$$b(f) \leq \prod_{p \mid c_d c_{d'}} \exp\left(\frac{\log p}{p}\right) \leq \log|c_d c_{d'}| + 1$$

through Mertens' first theorem as in Corollary 3.2.3. □

4.3. ***Proofs of our main results.*** We can now prove our main theorems, subject to the following propositions; they allow us to reduce to the case of hypersurfaces throughout, and will be established in Section 5 by projection arguments.

Proposition 4.3.1. *Given a geometrically integral affine variety X in $\mathbb{A}^n$ of dimension m and degree d, there exists a geometrically integral affine variety X' in $\mathbb{A}^{m+1}$ birational to X, also of degree d, such that for any $B \geq 1$ we have*

$$N_{\mathrm{aff}}(X, B) \leq dN_{\mathrm{aff}}(X', c_n d^{e_n} B),$$

where c_n, e_n are constants depending only on n.

For $m = 1$, we can even achieve

$$N_{\mathrm{aff}}(X, B) \leq N_{\mathrm{aff}}(X', c_n d^{e_n} B) + d^2.$$

Proposition 4.3.2. *Given a geometrically integral projective variety X in $\mathbb{P}^n$ of dimension m and degree d, there exists a geometrically integral projective variety X' in $\mathbb{P}^{m+1}$ birational to X, also of degree d, such that for any $B \geq 1$ we have*

$$N(X, B) \leq dN(X', c_n d^{e_n} B),$$

where c_n, e_n are constants depending only on n.

For $m = 1$, we can even achieve

$$N(X, B) \leq N(X', c_n d^{e_n} B) + d^2.$$

Proof of Theorem 2. In the case of a planar curve, i.e., for $n = 2$, Corollary 3.1.2 gives the claim. For the general case, we may assume that the given curve is geometrically integral by Remark 4.1.5, and then reduce to $n = 2$ by applying Proposition 4.3.2 (where $m = 1$). □

Proof of Theorem 3. We may assume that the curve X is geometrically integral by Remark 4.1.5. In the case of a planar curve, i.e., for $n = 2$, Corollary 4.2.4 yields that

$$N(X, B) \leq O_n((d^3 \log B + d^4) B^{1/d}),$$

by observing that

$$\frac{d^2 \log\| f_d \| + d^3 \log B + d^4}{\| f_d \|^{1/d^2}} \leq d^3 \log B + 2d^4.$$

We can reduce the general case to $n = 2$ by applying Proposition 4.3.1 (where $m = 1$), yielding the same estimate. □

Proof of Theorem 6. In the penultimate step of their proof of Theorem 1.1, Bhargava et al. [2020] establish the bound

$$h_2(K) \leq O_{d,\varepsilon}(|\Delta_K|^{1/4+\varepsilon}) + \sum_{\beta \in \mathcal{B}} N_{\mathrm{aff}}(f_\beta, |\Delta_K|^{1/2})$$

where $\mathcal{B} \subseteq \mathcal{O}_K$ is a set of size $O_d(|\Delta_K|^{1/2-1/d})$ and

$$f_\beta = y^2 - N_{K/\mathbb{Q}}(x - \beta) = y^2 - x^d - \text{lower order terms in } x.$$

Theorem 3 implies that

$$N_{\mathrm{aff}}(f_\beta, |\Delta_K|^{1/2}) \leq O_d(|\Delta_K|^{1/(2d)} \log|\Delta_K|),$$

yielding the desired result when d is even. If d is odd then instead of Theorem 3 we apply Corollary 4.2.5 with $d' = 2$, $c_d = -1$, $c_{d'} = 1$ to get rid of the factor $\log|\Delta_K|$. □

For the proof of Theorem 4, we need the following explicit form of Proposition 1 of [Browning et al. 2006] with $D = 1$.

Proposition 4.3.3. *There exists a constant c such that for all $d \geq 3$ and all polynomials $f \in \mathbb{Z}[x_1, x_2, x_3]$ of degree d such that the highest degree part $h(f) = f_d$ of f is irreducible, all finite sets I of curves C of $\mathbb{A}^3_{\mathbb{Q}}$ of degree* 1 *and lying on the hypersurface defined by f, and all $B \geq 1$ one has*

$$N_{\text{aff}}\biggl(X \cap \biggl(\bigcup_{C\in I} C\biggr), B\biggr) \leq cd^6 B + \#I.$$

Proof. We write $I = I_1 \cup I_2$ where $I_1 = \{L \in I \mid N_{\text{aff}}(L, B) \leq 1\}$ and $I_2 = \{L \in I \mid N_{\text{aff}}(L, B) > 1\}$. It is clear that $N_{\text{aff}}\bigl(X \cap \bigcup_{L\in I_1} L\bigr) \leq \#I_1$. If $L \in I_2$, then there exist $a = (a_1, a_2, a_3)$, $v = (v_1, v_2, v_3) \in \mathbb{Z}^3$ such that $H(a) \leq B$, v is primitive and $L(\mathbb{Q}) = \{a + \lambda v \mid \lambda \in \mathbb{Q}\}$. Since v is primitive we deduce that

$$L(\mathbb{Z}) \cap [-B, B]^3 = \{a + \lambda v \mid \lambda \in \mathbb{Z}, H(a + \lambda v) \leq B\}.$$

So

$$\#(L(\mathbb{Z}) \cap [-B, B]^3) \leq 1 + \frac{2B}{H(v)}.$$

Since $L \in I_2$ we have $H(v) \leq 2B$ and $f_d(v) = 0$. On the other hand, for each point v with $f_d(v) = 0$, there are at most $d(d-1)$ lines $L \in I_2$ in the direction of v, since each such line intersects a generic hyperplane in $\mathbb{A}^3$ in a point which is simultaneously a zero of f and of the directional derivative of f in the direction of v. Put $A_i = \{v \in \mathbb{P}^2(\mathbb{Q}) \mid f_d(v) = 0, H(v) = i\}$ and $n_i = \#A_i$. Then, by Corollary 3.1.2, there exists a constant c independent of f such that $\sum_{1\leq i\leq k} n_i \leq cd^4 k^{2/d}$. By our discussion,

$$N_{\text{aff}}\biggl(X \cap \biggl(\bigcup_{C\in I} C\biggr), B\biggr) \leq \#I_1 + (d-1)d \sum_{i=1}^{2B} n_i \biggl(1 + \frac{2B}{i}\biggr).$$

On the other hand, summation by parts gives the following:

$$\begin{aligned}\sum_{i=1}^{2B} n_i \biggl(1 + \frac{2B}{i}\biggr) &= \sum_{k=1}^{2B-1} \biggl(\sum_{i=1}^{k} n_i\biggr)\biggl(\frac{2B}{k} - \frac{2B}{k+1}\biggr) + \biggl(\sum_{i=1}^{2B} n_i\biggr)\biggl(1 + \frac{2B}{2B}\biggr)\\ &\leq cd^4 \biggl(\sum_{k=1}^{2B-1} k^{2/d} \frac{2B}{k(k+1)} + 2(2B)^{2/d}\biggr).\end{aligned}$$

Since $d \geq 3$, one has $\sum_{k\geq 1} k^{2/d} \cdot 1/(k(k+1)) < +\infty$ and $B^{2/d} \leq B$. Thus, by enlarging c, we have

$$N_{\text{aff}}\biggl(X \cap \biggl(\bigcup_{C\in I} C\biggr), B\biggr) \leq cd^6 B + \#I$$

as desired. □

In order to prove Theorem 4, we now first consider the case of a surface in $\mathbb{P}^3$, with proof inspired by the proof of Corollary 7.3 of [Salberger 2013] in combination with the improvements developed above.

Proposition 4.3.4. *There exists a constant c such that for all polynomials f in $\mathbb{Z}[y_1, y_2, y_3]$ whose homogeneous part of highest degree f_d is irreducible over $\overline{\mathbb{Q}}$ and whose degree d is least* 5, *one has $N_{\text{aff}}(f, B) \leq cd^{14} B$.*

Proof of Proposition 4.3.4 for $d \geq 16$. For any prime modulo which f_d is absolutely irreducible, the reduction of f is likewise absolutely irreducible, so $b(f) \leq b(f_d)$. Applying the usual estimate from Corollary 3.2.3, Proposition 4.2.1 yields for each $B \geq 1$ a polynomial g of degree at most

$$cd^{7/2}B^{1/\sqrt{d}}, \tag{4-3-1}$$

not divisible by f and vanishing on all points x in $\mathbb{Z}^n$ satisfying $f(x) = 0$ and $|x_i| \leq B$, with c an absolute constant. Let C be an irreducible component of the (reduced) intersection of $f = 0$ with $g = 0$. Call this intersection $\mathcal{C}$. If C is of degree $\delta > 1$, then

$$N_{\text{aff}}(C, B) \leq c'\delta^3 B^{1/\delta}(\log B + \delta) \tag{4-3-2}$$

by Theorem 3, for some absolute constant c'.

By Proposition 4.3.3, the total contribution of integral curves D of $\mathcal{C}$ of degree 1 is at most

$$c''d^6 B \tag{4-3-3}$$

for some absolute constant c''.

Suppose that $C_1, \dots, C_k$ are irreducible components of the intersection of $f = 0$ and $g = 0$ and $\deg(C_i) > 1$ for all i. Furthermore, we assume that $\deg(C_i) \leq \log B$ for all $1 \leq i \leq m$ and $\deg(C_i) > \log B$ for all $i > m$. Since the function $\delta \mapsto 4\log_B(\delta) + 1/\delta$ is decreasing in $(0, \log B/4)$ and increasing in $(\log B/4, +\infty)$, by enlarging c', for all $1 \leq i \leq m$ we have

$$N_{\text{aff}}(C_i, B) \leq c' B^{1/2}(\log B + 1). \tag{4-3-4}$$

On the other hand, if $\delta > \log B$ then $B^{1/\delta}$ is bounded, so (4-3-1) and (4-3-2) imply

$$\sum_{m+1 \leq i \leq k} N_{\text{aff}}(C_i, B) \leq c'''d^{14}B^{4/\sqrt{d}} \tag{4-3-5}$$

for some c''' independent of d and B.

Putting the estimates (4-3-1), (4-3-3), (4-3-4), (4-3-5) together proves the proposition when d is at least 16. □

To give a proof of Proposition 4.3.4 for lower values of d than 16, one could try to get a form of Theorem 3 with a lower exponent of the degree and repeat the above proof. We proceed differently: we treat the values for d going from 6 up to 15 by inspecting the proof of [Browning et al. 2006, Theorem 2] in combination with some of the above refinements, and the case of $d = 5$ by using [Salberger 2013, Theorem 7.2] (at the cost of being less self-contained).

Proof of Proposition 4.3.4 with $6 \leq d \leq 15$. Fix $6 \leq d \leq 15$, let $f \in \mathbb{Z}[y_1, y_2, y_3]$ be of degree d with absolutely irreducible homogeneous part of highest degree, and let X be the surface described by f.

In [Browning et al. 2006, Theorem 2], the estimate $N_{\text{aff}}(f, B) \leq O_{d,\varepsilon}(B^{1+\varepsilon})$ is established for every $\varepsilon > 0$. However, using our Theorem 2 and Proposition 4.3.3, we shall show that their proof [Browning et al. 2006, pages 568–570] in fact gives the bound $N_{\mathrm{aff}}(f, B) \le O_d(B)$, without any ε, which is sufficient for our purposes.

Specifically, they first consider the case in which Lemma 4.2.2 applies, so all the rational points on X of height up to B lie on a union of irreducible curves with sum of degrees at most d^2. Applying Theorem 2 to those curves of degree ≥ 2 and Proposition 4.3.3 for the contribution of curves of degree 1 yields the claim in this case.

In the remaining case, it is argued that there is an open subset $U \subseteq X$ (specifically consisting of those nonsingular points on X which have multiplicity at most 2 on the tangent plane section at the point) whose complement consists of $O_d(1)$ integral components of degree $O_d(1)$; by the same argument as in the preceding paragraph, the contribution of this complement is $O_d(B)$, so it suffices to estimate $N_{\mathrm{aff}}(U, B)$.

Further, it is argued that the points on U of height at most B are covered by a certain collection of irreducible curves. The subcollection I consisting of those curves of degree at most 2 satisfies $|I| \le O_{d,\varepsilon}(B^{2/\sqrt{d}+2\varepsilon})$, so our Proposition 4.3.3 and [Browning et al. 2006, Proposition 1] gives a contribution $O_{d,\varepsilon}(B + B^{2/\sqrt{d}+3\varepsilon}) \le O_d(B)$.

The remaining curves, of which there are no more than $O_{d,\varepsilon}(B^{2/\sqrt{d}})$, all contribute at most $B^{1/3-1/(2\sqrt{d})}$ [Browning et al. 2006, Proposition 2], so their total contribution is

$$O_{d,\varepsilon}(B^{3/(2\sqrt{d})+1/3+\varepsilon}) \le O_d(B). \qquad \square$$

Theorem 4.3.5 [Salberger 2013, Theorem 7.2]. *Let X be a geometrically integral surface in $\mathbb{P}^3_{\mathbb{Q}}$ of degree d and X_{ns} its nonsingular locus. Suppose that the hyperplane defined by $x_0 = 0$ intersects X properly, and identify $\mathbb{A}^3$ with the open subset of $\mathbb{P}^3$ given by $x_0 \ne 0$. There exists a positive constant c bounded solely in terms of d such that the following holds: for every $B \ge 1$ there exists a set of $O_d(B^{1/\sqrt{d}} \log B + 1)$ geometrically integral curves D_λ on X of degree $O_d(1)$ such that*

$$N_{\mathrm{aff}}\Bigl(X_{\mathrm{ns}} \setminus \bigcup_{\lambda} D_\lambda, B\Bigr) \le O_d(B^{2/\sqrt{d}+c/\log(1+\log B)}).$$

Proof of Proposition 4.3.4 for $d = 5$. Suppose that the degree d of f is exactly 5, and let X be the surface in $\mathbb{A}^3_{\mathbb{Q}}$ given by f. We may assume that $B \ge 2$. By Theorem 4.3.5, there is $c > 0$ such that for each $B \ge 2$ there is a set $\mathcal{C}$ of at most

$$cB^{1/\sqrt{d}} \log B$$

geometrically integral curves $C \subseteq \mathbb{A}^3_{\mathbb{Q}}$ of degree at most c and lying on X such that

$$N_{\mathrm{aff}}\Bigl(X_{\mathrm{ns}} \setminus \bigcup_{C\in\mathcal{C}} C, B\Bigr) \le O(B^{2/\sqrt{d}+c/\log(\log B)}) \le O(B),$$

where X_{ns} is the open subvariety of nonsingular points.

The complement of X_{ns} in X is a union of irreducible curves the sum of whose degrees is bounded by a constant. Applying Theorem 2 to those curves of degree ≥ 2 and Proposition 4.3.3 for the contribution of curves of degree 1 yields that the complement of X_{ns} contributes at most $O(B)$ points, which is satisfactory for our purposes.

Similarly, the curves in $\mathcal{C}$ of degree 1 contribute at most $O(cB^{1/\sqrt{d}}\log B + B) \leq O(B)$ points by Proposition 4.3.3, and the curves in $\mathcal{C}$ of degree ≥ 2 each contribute at most $O(B^{1/2+\varepsilon})$ by Theorem 3, again giving a contribution of size $O(B)$. This proves the claim. □

Remark 4.3.6. We see that Proposition 4.3.4 for fixed $d \geq 6$, and therefore also Theorems 1 and 4 for fixed degree, already follow from combining [Browning et al. 2006] with the results of [Walsh 2015] and Proposition 4.3.3. Similarly, for fixed degree $d \geq 5$ one can use the results of [Salberger 2013]. However, keeping track of the dependence on d in Section 3 permits us to use a considerably simpler argument for fixed $d \geq 16$ than in the works cited, and to furthermore obtain polynomial dependence on d.

It remains to prove Theorems 1 and 4. This closely follows [Browning et al. 2006, Lemma 8, Theorem 3]. The proofs are based on Proposition 4.3.4 and the following lemma.

Lemma 4.3.7. *Let $n \geq 3$ and $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$ be a geometrically integral hypersurface of degree d. Then there exists a nonzero form $F \in \mathbb{Z}[y_0, \dots, y_n]$ of degree at most $(n+1)(d^2-1)$ such that $F(A) = 0$ whenever the hyperplane section $H_A \cap X$ is not geometrically integral, where $A \in (\mathbb{P}^n)^*$ and $H_A \subseteq \mathbb{P}^n$ denotes the hyperplane cut out by the linear form associated with A.*

Proof. Suppose that X is given by f, a geometrically irreducible form of degree d. For $A \in (\mathbb{P}^n)^*$ write $A = (a_0 : a_1 : \cdots : a_n) \in (\mathbb{P}^n)^*$. Assuming $a_0 \neq 0$, one has that $H_A \cap X$ is not geometrically integral if and only if

$$f\left(-\frac{a_1}{a_0}x_1 - \cdots - \frac{a_n}{a_0}x_n, x_1, \dots, x_n\right)$$

is reducible. Since $n \geq 3$ and since X is geometrically integral, we have for a generic choice of $B \in (\mathbb{P}^n)^*$ that $H_B \cap X$ is also geometrically integral. Hence Theorem 3.2.2 implies that there exists a nonzero form F_0 in $\mathbb{Z}[y_1, \dots, y_n]$ of degree at most $d^2 - 1$ such that $F_0(a_1, \dots, a_n) = 0$. Similarly, if $a_i \neq 0$, we produce a nonzero form F_i in $\mathbb{Z}[y_0, \dots, y_{i-1}, y_{i+1}, \dots, y_n]$ such that $F_i(a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_n) = 0$. So $F = \prod_{i=0}^n F_i$ is as we want. □

Proof of Theorem 4. Let $n \geq 3$ and $X \subseteq \mathbb{A}^n_{\mathbb{Q}}$ be a geometrically integral hypersurface of degree $d \geq 5$ described by a polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$ with absolutely irreducible highest degree part. We proceed by induction on n, where the base case $n = 3$ is Proposition 4.3.4.

Now assume that $n > 3$ and the theorem holds for all lower n. Let $f_d = h(f)$ be the homogeneous part of highest degree, which describes a hypersurface in $\mathbb{P}^{n-1}$. By Lemma 4.3.7 and Corollary 4.1.2, there exists $A = (a_1, \dots, a_n)$ such that the hyperplane section $\{f_d = 0\} \cap \{\sum a_i x_i = 0\}$ is geometrically integral of degree d, with all a_i having absolute value at most $n(d^2-1)$.

Now

$$N_{\mathrm{aff}}(f, B) \leq \sum_{|k| \leq n^2(d^2-1)B} N_{\mathrm{aff}}\left(\{f = 0\} \cap \left\{\sum a_i x_i = k\right\}, B\right).$$

For each k, the variety $\{f=0\}\cap\left\{\sum a_i x_i=k\right\}$ is a hypersurface in the affine plane $\left\{\sum a_i x_i=k\right\}$, which after a change of variables is described by a polynomial $g\in\mathbb{Z}[x_1,\ldots,x_{n-1}]$ whose homogeneous part of highest degree is absolutely irreducible by the construction of A. Now the induction hypothesis finishes the proof. □

Proof of Theorem 1. We may assume that the variety in question is geometrically irreducible by Remark 4.1.5, and can reduce to consideration of a hypersurface by Proposition 4.3.2. Hence let $n\geq 3$ and consider an absolutely irreducible polynomial $f\in\mathbb{Z}[x_0,\ldots,x_n]$ homogeneous of degree $d\geq 5$.

Then f defines not only a projective hypersurface X in $\mathbb{P}^n$, but also an affine hypersurface in $\mathbb{A}^{n+1}$, the cone of X. We now trivially have

$$N(f,B)\leq N_{\mathrm{aff}}(f,B),$$

so Theorem 4 finishes the proof. □

Remark 4.3.8. Using the explicit exponents obtained in Proposition 4.3.4 and in the proof of Proposition 4.3.2 in Section 5, we can conservatively estimate $e(n)\leq 2n+8$ for the exponent in Theorem 4, and $e(n)\leq 2n^3$ for the exponent in Theorem 1.

5. Reduction to hypersurfaces via projection

In this section we prove Propositions 4.3.1 and 4.3.2, which allowed us to reduce to the case of hypersurfaces in the proofs of our main theorems. This is an elaboration of familiar projection arguments, which classically show that every variety is birational to a hypersurface, and which are used in the proofs of [Browning et al. 2006, Theorem 1] and [Pila 1995, Theorem A]. The additional difficulty for us is that we have to keep track of the dependence on the degree of the variety throughout. Our main auxiliary result is:

Lemma 5.1. *Given a geometrically irreducible subvariety $X\subseteq\mathbb{P}^n$ of dimension $m<n-1$ and degree d, one can find an $(n-m-2)$-plane Λ disjoint from X and an $(m+1)$-plane Γ, both defined over $\mathbb{Q}$, such that $\Lambda\cap\Gamma=\varnothing$, such that the corresponding projection map $p_{\Lambda,\Gamma}:\mathbb{P}^n\setminus\Lambda\to\Gamma$ satisfies*

$$H(p_{\Lambda,\Gamma}(P))\leq c_n d^{2(n-m-1)^2}H(P) \tag{5-1}$$

for all $P\in\mathbb{P}^n(\mathbb{Q})\setminus\Lambda$, and such that $p_{\Lambda,\Gamma}|_X$ is birational onto its image. Here c_n is an explicit constant depending only on n.

Because Λ is disjoint from X, the statement that $p_{\Lambda,\Gamma}|_X$ is birational onto its image is equivalent to saying that $p_{\Lambda,\Gamma}(X)$ is again a variety of degree d; see [Harris 1992, Example 18.16].

In order to prove Lemma 5.1, we first concentrate on finding an appropriate Λ, which we think of as living in the Grassmannian $\mathbb{G}(n-m-2,n)$ consisting of all $(n-m-2)$-planes in $\mathbb{P}^n$. It is well-known that the latter has the structure of an $(m+2)(n-m-1)$-dimensional irreducible projective variety through the Plücker embedding

$$P_{n-m-2,n}:\mathbb{G}(n-m-2,n)\hookrightarrow\mathbb{P}^{\nu}:\Lambda\mapsto\det(P_1,\ldots,P_{n-m-1}),$$

where $\nu = \binom{n+1}{n-m-1} - 1$ and $(P_1, \dots, P_{n-m-1})$ is the $(n-m-1) \times (n+1)$ matrix whose rows are coordinates for $n-m-1$ independent points $P_i \in \Lambda$. Here and throughout this section, for a matrix M whose number of rows does not exceed its number of columns, we write $\det(M)$ to denote the tuple consisting of its maximal minors, with respect to some fixed ordering.

Fixing such a $\Lambda \in \mathbb{G}(n-m-2)$ and independent points $P_1, \dots, P_{n-m-1} \in \Lambda$, we can also consider the map

$$\pi_\Lambda : \mathbb{P}^n \setminus \Lambda \to \mathbb{P}^\mu : P \mapsto \det(P, P_1, \dots, P_{n-m-1}),$$

where $\mu = \binom{n+1}{n-m} - 1$. Writing $\pi_\Lambda = (\pi_{\Lambda,0}, \dots, \pi_{\Lambda,\mu})$ we see that the nonzero $\pi_{\Lambda,j}$ can be viewed as linear forms whose coefficients are coordinates of $P_{n-m-2,n}(\Lambda)$, modulo sign flips. Note that $\pi_{\Lambda,j}(P) = 0$ for all j if and only if $P \in \Lambda$. In particular π_Λ is well-defined and easily seen to factor as

$$\mathbb{P}^n \setminus \Lambda \xrightarrow{p_{\Lambda,\Gamma}} \Gamma \hookrightarrow \mathbb{P}^\mu \tag{5-2}$$

for all $(m+1)$-planes Γ such that $\Gamma \cap \Lambda = \varnothing$.

Another theoretical ingredient we need is the Chow point F_X associated with an irreducible m-dimensional degree d variety $X \subseteq \mathbb{P}^n$. This is an irreducible multihomogeneous polynomial of multidegree $(d, d, \dots, d)$ in $m+1$ sets of $n+1$ variables such that for all tuples $(H_1, H_2, \dots, H_{m+1})$ of $m+1$ hyperplanes in $\mathbb{P}^n$ one has $F_X(H_1, \dots, H_{m+1}) = 0$ if and only if $H_1 \cap H_2 \cap \dots \cap H_{m+1} \cap X \neq \varnothing$. See e.g., [Gelfand et al. 1994, Chapter 4].

Lemma 5.2. *Let X be a geometrically irreducible degree d subvariety of $\mathbb{P}^n$ having dimension $m < n-1$ and consider*

$$G_X = \{\Lambda \in \mathbb{G}(n-m-2, n) \mid \Lambda \cap X = \varnothing \textit{ and } \pi_\Lambda|_X \textit{ is birational onto its image}\}$$

with π_Λ as above. This is a dense open subset of $\mathbb{G}(n-m-2, n)$ whose complement, when viewed under the Plücker embedding, is cut out by hypersurfaces of degree less than $(m+1)^2 d^2$.

Proof. Given a hyperplane $H \subseteq \mathbb{P}^\mu$ we abusively write $H \circ \pi_\Lambda$ for $\pi_\Lambda^{-1}(H) \cup \Lambda$, since this is the hyperplane in $\mathbb{P}^n$ cut out by the precomposition of π_Λ with the linear form associated with H. Define a multihomogeneous degree $(d, d, \dots, d)$ polynomial $R_{X,\Lambda}$ in $m+1$ sets of $\mu+1$ variables by letting

$$R_{X,\Lambda}(H_1, H_2, \dots, H_{m+1}) = F_X(H_1 \circ \pi_\Lambda, H_2 \circ \pi_\Lambda, \dots, H_{m+1} \circ \pi_\Lambda).$$

Note that its coefficients are degree $(m+1)d$ polynomial expressions in the coordinates of $P_{n-m-2,n}(\Lambda)$. We will show that

$$G_X = \{\Lambda \in \mathbb{G}(n-m-2, n) \mid R_{X,\Lambda} \text{ is absolutely irreducible}\}, \tag{5-3}$$

which implies that the complement of G_X is precisely the vanishing locus of the Noether irreducibility polynomials from Theorem 3.2.2 evaluated in these coefficients. This indeed yields expressions in the coordinates of $P_{n-m-2,n}(\Lambda)$ of degree less than $(m+1)^2 d^2$, where we note that not all these expressions can vanish identically, since generic Λ's do not meet X and generic projections are known to be birational [Harris 1992, page 224].

We now prove (5-3). First note that $\Lambda \cap X \neq \varnothing$ implies that $R_{X,\Lambda}$ vanishes identically. Indeed, if $P \in \Lambda$ then all hyperplanes of the form $H \circ \pi_\Lambda$ pass through P, so if moreover $P \in X$ we see that $R_{X,\Lambda}$ is identically zero. We can therefore assume that $\Lambda \cap X = \varnothing$. This ensures that $\pi_\Lambda(X)$ is an irreducible projective variety of dimension m; see [Harris 1992, page 134], so we can consider its Chow point $F_{\pi_\Lambda(X)}$, which is an irreducible multihomogeneous polynomial of multidegree

$$(\deg(\pi_\Lambda(X)), \deg(\pi_\Lambda(X)), \dots, \deg(\pi_\Lambda(X)))$$

in the same $m+1$ sets of $\mu+1$ variables as in the case of $R_{X,\Lambda}$. It has the property that for all tuples $(H_1, \dots, H_{m+1})$ of hyperplanes in $\mathbb{P}^\mu$ we have $F_{\pi_\Lambda(X)}(H_1, \dots, H_{m+1}) = 0$ if and only if $H_1 \cap \cdots \cap H_{m+1} \cap \pi_\Lambda(X) \neq \varnothing$. But in this case $\pi_\Lambda^{-1}(H_1) \cap \cdots \cap \pi_\Lambda^{-1}(H_{m+1}) \cap X \neq \varnothing$ so that $R_{X,\Lambda}(H_1, \dots, H_{m+1}) = 0$. Conversely, if $R_{X,\Lambda}(H_1, \dots, H_{m+1}) = 0$ then there exists a point $P \in H_1 \circ \pi_\Lambda \cap \cdots \cap H_{m+1} \circ \pi_\Lambda \cap X$, which since $\Lambda \cap X = \varnothing$ implies that $\pi_\Lambda(P) \in H_1 \cap \cdots \cap H_{m+1} \cap \pi_\Lambda(X)$ and hence that $F_{\pi_\Lambda(X)}(H_1, \dots, H_{m+1}) = 0$. We conclude that $F_{\pi_\Lambda(X)}$ and $R_{X,\Lambda}$ have the same vanishing locus and because the former polynomial is irreducible there must exist some $r \geq 1$ such that

$$R_{X,\Lambda} = F^r_{\pi_\Lambda(X)}.$$

In particular $R_{X,\Lambda}$ is irreducible if and only if $r = 1$. But this is true if and only if $\pi_\Lambda(X)$ has degree d, which as we know holds if and only if $\pi_\Lambda|_X$ is birational onto its image. □

Lemma 5.3. *Using the assumptions and notation from Lemma 5.2, there exists an* $(n-m-2)$*-plane* $\Lambda \in G_X(\mathbb{Q})$ *such that*

$$H(\Lambda) \leq ((m+1)^2 d^2)^{n-m-1}(n-m-1)!$$

when considered under the Plücker embedding.

Proof. Consider the rational map

$$\pi : (\mathbb{P}^n)^{n-m-1} \dashrightarrow \mathbb{P}^\nu : (P_1, \dots, P_{n-m-1}) \mapsto \det(P_1, \dots, P_{n-m-1})$$

which is well-defined on the open U consisting of tuples of independent points. Observe that $\pi(U) = \mathbb{G}(n-m-2, n)$. By Lemma 5.2 there exists a polynomial F of degree less than $(m+1)^2 d^2$ which vanishes on the complement of G_X but which does not vanish identically on $\mathbb{G}(n-m-2, n)$. The polynomial

$$Q := F\left(\det\begin{pmatrix} x_{10} & x_{11} & \dots & x_{1n} \\ x_{20} & x_{21} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-m-1,0} & x_{n-m-1,1} & \dots & x_{n-m-1,n} \end{pmatrix}\right)$$

is multihomogeneous of multidegree $(\deg(F), \dots, \deg(F))$ in the $n-m-1$ blocks of $n+1$ variables corresponding to the rows of the displayed matrix. Clearly Q vanishes on the complement of U, while it is not identically zero because $Q(P_1, \dots, P_{n-m-1}) = F(\pi(P_1, \dots, P_{n-m-1}))$ for any tuple of independent points P_i.

Write

$$Q = \sum_j Q_j(x_{10}, \dots, x_{1n}) R_j(x_{20}, \dots, x_{n-m-1,n})$$

for nonzero Q_j and linearly independent polynomials R_j. Lemma 4.1.1 helps us to find a point $P_1 \in \mathbb{P}^n(\mathbb{Q})$ of height at most $\deg(F)$ such that $Q_1(P_1) \neq 0$. By the linear independence of the R_j one sees that $Q(P_1, x_{20}, \dots, x_{n-m-1,n})$ is not identically zero. Repeating the argument eventually yields a tuple of points $P_1, P_2, \dots, P_{n-m-1}$ of height at most $\deg(F)$ such that $Q(P_1, \dots, P_{n-m-1}) \neq 0$. In particular this tuple of points belongs to U, i.e., they are independent, and $\pi(P_1, P_2, \dots, P_{n-m-1}) \in G_X(\mathbb{Q})$. From this the lemma follows easily. □

Proof of Lemma 5.1. Let Λ be the $\mathbb{Q}$-rational $(n-m-2)$-plane produced by the proof of Lemma 5.3. In particular $\Lambda \cap X = \varnothing$ and $\pi_\Lambda|_X$ is birational onto its image. Then for all $(m+1)$-planes Γ such that $\Gamma \cap \Lambda = \varnothing$ the projection map $p_{\Lambda,\Gamma}|_X$ is also birational onto its image, thanks to the factorization from (5-2).

The proof of Lemma 5.3 moreover shows that Λ can be assumed to be the linear span of rational points $P_1, \dots, P_{n-m-1} \in \mathbb{P}^n$ satisfying $H(P_i) \le (m+1)^2 d^2 =: B_1$. By Lemma 5.4 below we can find linear forms $L_1, L_2, \dots, L_{n-m-1}$ with integral coefficients whose absolute value is bounded by

$$B_2 := \sqrt{(n-m-2)!(n+1)}\, B_1^{n-m-2}$$

such that L_i vanishes on $P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_{n-m-1}$ but not on P_i. Together these linear forms cut out an $(m+1)$-plane Γ such that $\Gamma \cap \Lambda = \varnothing$. Furthermore

$$p_{\Lambda,\Gamma}(P) = P - \frac{L_1(P)}{L_1(P_1)} P_1 - \dots - \frac{L_{n-m-1}(P)}{L_{n-m-1}(P_{n-m-1})} P_{n-m-1} \tag{5-4}$$

for all $P \in \mathbb{P}^n \setminus \Lambda$. So we have

$$H(p_{\Lambda,\Gamma}(P)) \le (n-m)((n+1)B_1 B_2)^{n-m-1} H(P) = c d^{2(n-m-1)^2} H(P) \tag{5-5}$$

for some constant c that is easily bounded by an expression purely in n. □

Lemma 5.4. *Let $B, r, s \in \mathbb{Z}_{\ge 1}$ be integers such that $s < r$. Consider a linear system of linearly independent equations $\sum_{k=1}^r a_{ik} x_k = 0$ for $i = 1, \dots, s$, where all a_{ij} are integers satisfying $|a_{ij}| \le B$. There exists a nonzero tuple of integers $(x_1, x_2, \dots, x_r)$ violating the first equation but satisfying all other equations such that*

$$|x_i| \le \sqrt{(s-1)!r}\, B^{s-1} \tag{5-6}$$

for all i.

Proof. This follows from [Bombieri and Vaaler 1983, Theorem 2], which strengthens Theorem 3.3.4. It ensures the existence of $r-s+1$ linearly independent tuples of integers $(x_1, x_2, \dots, x_r)$ satisfying the last $s-1$ equations and meeting the bound (5-6). Since the space of solutions to the full linear system of s equations has dimension $r-s$, at least one of these tuples must violate the first equation. □

We can now prove Propositions 4.3.1 and 4.3.2, reducing the situation of a general variety to a hypersurface.

Proof of Proposition 4.3.2. Let X be a geometrically integral projective variety in $\mathbb{P}^n$ of dimension m and degree d, where we may assume that $n > m+1$. We consider a projection $p_{\Lambda,\Gamma}$ as in Lemma 5.1. By dropping appropriately chosen coordinates, its image X' can be viewed as a hypersurface in $\mathbb{P}^{m+1}$, birational to X and hence also of degree d. In each fiber of $p_{\Lambda,\Gamma}$ there are at most d points. The height relation from Lemma 5.1 now immediately implies

$$N(X, B) \leq dN(X', c_n d^{2(n-m-1)^2} B)$$

for all $B \geq 1$. This proves the claim for $m > 1$. For $m = 1$, consider the normalization $\tilde{X} \to X$ and compose it with the morphism $X \to X'$ induced by $p_{\Lambda,\Gamma}$ to find a resolution of singularities $\tilde{X} \to X'$. The latter map is one-to-one away from the singular points of X', which together have no more than $(d-1)(d-2)$ preimages by [Kunz 2005, Theorem 17.7(b)]. But then the same claims must apply to $X \to X'$, yielding the stronger bound

$$N(X, B) \leq N(X', c_n d^{2(n-2)^2} B) + d^2,$$

as wanted. □

Proof of Proposition 4.3.1. Let X be a geometrically integral affine variety in $\mathbb{A}^n$ of dimension m and degree d, where we may assume that $m < n-1$. Let Z be the projective closure of X in $\mathbb{P}^n$; we apply Lemma 5.1 and shall argue later that we can take the $(n-m-2)$-plane Λ to be contained in the hyperplane $\mathbb{P}^{n-1}$ at infinity. Let $Z' \subseteq \Gamma$ be the image of Z under the projection $p_{\Lambda,\Gamma}$. As above, by dropping some coordinates we can view Γ as $\mathbb{P}^{m+1} = \mathbb{A}^{m+1} \sqcup \mathbb{P}^m$ where $p_{\Lambda,\Gamma}(\mathbb{P}^{n-1} \setminus \Lambda)$ corresponds to $\mathbb{P}^m$. In particular $p_{\Lambda,\Gamma}$ maps X to the affine part $X'_0 = Z' \cap \mathbb{A}^{m+1}$ of Z'.

Consider $P_1, P_2, \ldots, P_{n-m-1}$ and $L_1, L_2, \ldots, L_{n-m-1}$ as in the proof of Lemma 5.1. Let $P \in X$ be a point having integer coordinates; when considered as a projective point of Z its coordinate at infinity is 1. Since the coordinates at infinity of the P_i are 0, the projection formula (5-4) shows that $p_{\Lambda,\Gamma}(P) \in Z'$ admits integer coordinates such that the coordinate at infinity is

$$L_1(P_1)L_2(P_2)\cdots L_{n-m-1}(P_{n-m-1}),$$

regardless of the choice of P. As a consequence, this is a multiple of the denominators appearing among the coordinates of $p_{\Lambda,\Gamma}(P)$ when viewed as an affine rational point of X'_0. Therefore, postcomposing with a coordinate scaling map $\mathbb{A}^{m+1} \to \mathbb{A}^{m+1}$, we obtain another variety X' in $\mathbb{A}^{m+1}$ such that every integral point P of X is mapped to an integral point of X' whose height satisfies the same upper bound as in (5-5). All fibers of this map $X \to X'$ have at most d points, and in the case of curves the map is even one-to-one away from the singular points on X'. So we can conclude as in the proof of Proposition 4.3.2.

It remains to argue why we can take Λ in the hyperplane at infinity. We first claim that the "good set" G_Z from Lemma 5.2 has a nonempty intersection with the Grassmannian parametrizing $(n-m-2)$-planes Λ contained in $\mathbb{P}^{n-1}$. Indeed, it is apparent that the generic such Λ does not intersect the $(m-1)$-dimensional set $Z \cap \mathbb{P}^{n-1}$ and hence satisfies $\Lambda \cap Z = \varnothing$. Furthermore, the argument from [Harris 1992, page 224] showing that generic projections are birational leaves enough freedom to draw the same conclusion when restricting to projections from planes at infinity. More precisely, if $m = n-2$ then it suffices to project from a point outside the cone spanned by Z and some random point $q \in Z$. Since this cone is irreducible of dimension at most $m+1 = n-1$ and since $Z \not\subseteq \mathbb{P}^{n-1}$, the generic point at infinity indeed meets this requirement. If $m < n-2$ then the desired conclusion follows by applying the foregoing argument to $n-m-1$ successive projections from points.

So we can redo the proof of Lemma 5.3 starting from a polynomial F of degree less than $(m+1)^2d^2$ which vanishes on the complement of G_X but which does not vanish identically on the Grassmannian of $(n-m-2)$-planes that are contained in the hyperplane at infinity; we just argued that such an F exists. Then one can proceed with the same polynomial Q as before, but with zeroes substituted for the variables $x_{10}, x_{20}, \dots, x_{n-m-1,0}$. □

6. Lower bounds

We conclude with some lower bounds showing that one cannot make the dependence on d subpolynomial. Our main auxiliary tool is the following lemma.

Lemma 6.1. *For each pair of integers $d \geq 1$, $n \geq 2$ there exists an absolutely irreducible degree d polynomial $f \in \mathbb{Q}[x_1, x_2, \dots, x_n]$ which vanishes at all integral points $(r_1, r_2, \dots, r_n)$ for which $|r_i| \leq \lfloor (d-1)/2n \rfloor$ for all i.*

Proof. The lemma is immediate if $d = 1$, so we can assume that $d \geq 2$. We claim that there exists a polynomial

$$x_1^d + x_2^d + \cdots + x_{n-1}^d + x_n^{d-1} + \sum_{0 \leq i_1, \dots, i_n \leq \lfloor (d-1)/n \rfloor} a_{i_1,\dots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

which vanishes simultaneously at the integral points $(r_1, r_2, \dots, r_n)$ satisfying

$$\left\lfloor \frac{d-1}{2n} \right\rfloor - \left\lfloor \frac{d-1}{n} \right\rfloor \leq r_i \leq \left\lfloor \frac{d-1}{2n} \right\rfloor$$

for all i. From this the lemma follows, because indeed $\lfloor (d-1)/2n \rfloor - \lfloor (d-1)/n \rfloor \leq -\lfloor (d-1)/2n \rfloor$ and because the polynomial is absolutely irreducible, as its Newton polytope is indecomposable; see e.g., [Gao 2001, Theorem 4.11]. To verify the claim, note that every point $(r_1, r_2, \dots, r_n)$ imposes a linear condition on the coefficients $a_{i_1,\dots,i_n}$, together resulting in a linear system of $(\lfloor (d-1)/n \rfloor + 1)^n$ equations in the same number of unknowns. It suffices to see that the matrix corresponding to its linear part is nonsingular. But this matrix is the n-th Kronecker power of the Vandermonde matrix $(r^i)_{r,i}$ where r and

i range over

$$\left\{\left\lfloor\frac{d-1}{2n}\right\rfloor-\left\lfloor\frac{d-1}{n}\right\rfloor,\dots,\left\lfloor\frac{d-1}{2n}\right\rfloor\right\} \quad\text{and}\quad \left\{0,\dots,\left\lfloor\frac{d-1}{n}\right\rfloor\right\},$$

respectively. Therefore its determinant is a power of the determinant of this Vandermonde matrix, from which the desired conclusion follows. □

Proof of Proposition 5. If $d = 1, 2$ then we let X be a line or conic through a coordinate point, respectively, so that we can take $B = 1$. If $d \geq 3$ then we consider the affine curve defined by the polynomial f from the proof of the foregoing lemma for $n = 2$. Let X be its projective closure, which has an extra height 1 point at infinity. With $B = \lfloor (d-1)/2\rfloor - \lfloor (d-1)/4\rfloor$ one observes that

$$N(X, B) \geq \left(\left\lfloor\frac{d-1}{2}\right\rfloor+1\right)^2+1 \geq \frac{d^2}{4} = \frac{d^2}{5}\cdot\frac{5}{4} \geq \frac{d^2}{5}\cdot B^{2/d}.$$ □

Note that using the same f and B one also finds that

$$N_{\text{aff}}(f, B) \geq \left(\left\lfloor\frac{d-1}{2}\right\rfloor+1\right)^2 \geq \frac{d^2}{4\log d}B^{1/d}\log B$$

for all $d \geq 3$, confirming our claim that, in the statement of Theorem 3, it is impossible to replace the quartic dependence on d by any expression which is $o(d^2/\log d)$. In arbitrary dimension, the same reasoning shows that there exists a positive constant $c = c(n)$ such that for all integers $d > 0$ we can find an absolutely irreducible degree d polynomial $f \in \mathbb{Q}[x_1, x_2, \dots, x_n]$ along with an integer $B \geq 1$ such that

$$N_{\text{aff}}(f, B) \geq cd^2B^{n-2} \quad\text{and}\quad N(X, B) \geq cdB^{\dim X},$$

where $X \subseteq \mathbb{P}^n_{\mathbb{Q}}$ denotes the integral degree d hypersurface defined by the homogenization of f. This shows that Theorems 1 and 4 cannot hold with $e < 1$ or $e < 2$, respectively.

References

[Bhargava et al. 2020] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao, "Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves", *J. Amer. Math. Soc.* (online publication August 2020).

[Binyamini and Novikov 2019] G. Binyamini and D. Novikov, "Complex cellular structures", *Ann. of Math.* (2) **190**:1 (2019), 145–248. MR Zbl

[Bombieri and Pila 1989] E. Bombieri and J. Pila, "The number of integral points on arcs and ovals", *Duke Math. J.* **59**:2 (1989), 337–357. MR Zbl

[Bombieri and Vaaler 1983] E. Bombieri and J. Vaaler, "On Siegel's lemma", *Invent. Math.* **73**:1 (1983), 11–32. MR Zbl

[Browning 2009] T. D. Browning, *Quantitative arithmetic of projective varieties*, Progr. Math. **277**, Birkhäuser, Basel, 2009. MR Zbl

[Browning and Heath-Brown 2005] T. D. Browning and D. R. Heath-Brown, "Counting rational points on hypersurfaces", *J. Reine Angew. Math.* **584** (2005), 83–115. MR Zbl

[Browning et al. 2006] T. D. Browning, D. R. Heath-Brown, and P. Salberger, "Counting rational points on algebraic varieties", *Duke Math. J.* **132**:3 (2006), 545–578. MR Zbl

[Burguet et al. 2015] D. Burguet, G. Liao, and J. Yang, "Asymptotic h-expansiveness rate of C^∞ maps", *Proc. Lond. Math. Soc.* (3) **111**:2 (2015), 381–419. MR Zbl

[Cafure and Matera 2006] A. Cafure and G. Matera, "Improved explicit estimates on the number of solutions of equations over a finite field", *Finite Fields Appl.* **12**:2 (2006), 155–185. MR Zbl

[Cluckers et al. 2020a] R. Cluckers, A. Forey, and F. Loeser, "Uniform Yomdin–Gromov parametrizations and points of bounded height in valued fields", *Algebra Number Theory* **14**:6 (2020), 1423–1456. MR

[Cluckers et al. 2020b] R. Cluckers, J. Pila, and A. Wilkie, "Uniform parameterization of subanalytic sets and Diophantine applications", *Ann. Sci. École Norm. Sup.* (4) **53**:1 (2020), 1–42.

[Dèbes and Walkowiak 2008] P. Dèbes and Y. Walkowiak, "Bounds for Hilbert's irreducibility theorem", *Pure Appl. Math. Q.* **4**:4 (2008), 1059–1083. MR Zbl

[Ellenberg and Venkatesh 2005] J. Ellenberg and A. Venkatesh, "On uniform bounds for rational points on nonrational curves", *Int. Math. Res. Not.* **2005**:35 (2005), 2163–2181. MR Zbl

[Gao 2001] S. Gao, "Absolute irreducibility of polynomials via Newton polytopes", *J. Algebra* **237**:2 (2001), 501–520. MR Zbl

[Gautschi 1962] W. Gautschi, "On inverses of Vandermonde and confluent Vandermonde matrices", *Numer. Math.* **4** (1962), 117–123. MR Zbl

[Gelfand et al. 1994] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants, resultants, and multidimensional determinants*, Birkhäuser, Boston, 1994. MR Zbl

[Harris 1992] J. Harris, *Algebraic geometry: a first course*, Grad. Texts in Math. **133**, Springer, 1992. MR Zbl

[Heath-Brown 1983] D. R. Heath-Brown, "Cubic forms in ten variables", *Proc. Lond. Math. Soc.* (3) **47**:2 (1983), 225–257. MR

[Heath-Brown 2002] D. R. Heath-Brown, "The density of rational points on curves and surfaces", *Ann. of Math.* (2) **155**:2 (2002), 553–595. MR Zbl

[Heintz 1983] J. Heintz, "Definability and fast quantifier elimination in algebraically closed fields", *Theoret. Comput. Sci.* **24**:3 (1983), 239–277. MR Zbl

[Kunz 2005] E. Kunz, *Introduction to plane algebraic curves*, Birkhäuser, Boston, 2005. MR Zbl

[Motte 2018] F. Motte, "On the Malle conjecture and the Grunwald problem", preprint, 2018. arXiv

[Pila 1995] J. Pila, "Density of integral and rational points on varieties", pp. 183–187 in *Columbia University Number Theory Seminar* (New York, 1992), Astérisque **228**, Soc. Math. France, Paris, 1995. MR Zbl

[Pila 1996] J. Pila, "Density of integer points on plane algebraic curves", *Int. Math. Res. Not.* **1996**:18 (1996), 903–912. MR Zbl

[Pila 2010] J. Pila, "Counting rational points on a certain exponential-algebraic surface", *Ann. Inst. Fourier* (*Grenoble*) **60**:2 (2010), 489–514. MR Zbl

[Ruppert 1986] W. Ruppert, "Reduzibilität ebener Kurven", *J. Reine Angew. Math.* **369** (1986), 167–191. MR Zbl

[Salberger 2007] P. Salberger, "On the density of rational and integral points on algebraic varieties", *J. Reine Angew. Math.* **606** (2007), 123–147. MR Zbl

[Salberger 2013] P. Salberger, "Counting rational points on projective varieties", submitted, 2013.

[Salberger 2015] P. Salberger, "Uniform bounds for rational points on cubic hypersurfaces", pp. 401–421 in *Arithmetic and geometry* (Bonn, Germany, 2013), edited by L. Dieulefait et al., Lond. Math. Soc. Lect. Note Ser. **420**, Cambridge Univ. Press, 2015. MR Zbl

[Sedunova 2017] A. Sedunova, "On the Bombieri–Pila method over function fields", *Acta Arith.* **181**:4 (2017), 321–331. MR Zbl

[Serre 1989] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, Aspects Math. **E15**, Vieweg & Sohn, Braunschweig, Germany, 1989. MR Zbl

[Serre 1992] J.-P. Serre, *Topics in Galois theory*, Res. Notes in Math. **1**, Jones and Bartlett, Boston, 1992. MR Zbl

[Vermeulen 2020] F. Vermeulen, "Points of bounded height on curves and the dimension growth conjecture over $\mathbb{F}_q[t]$", preprint, 2020. arXiv

[Walkowiak 2005] Y. Walkowiak, "Théorème d'irréductibilité de Hilbert effectif", *Acta Arith.* **116**:4 (2005), 343–362. MR Zbl

[Walsh 2015] M. N. Walsh, "Bounded rational points on curves", *Int. Math. Res. Not.* **2015**:14 (2015), 5644–5658. MR Zbl

Communicated by Jonathan Pila
Received 2020-02-04 Accepted 2020-04-23

wouter.castryck@kuleuven.be *KU Leuven, imec-COSIC, Leuven, Belgium*

Ghent University, Department of Mathematics: Algebra and Geometry, Ghent, Belgium

raf.cluckers@univ-lille.fr *University of Lille, CNRS, UMR 8524 – Laboratoire Painlevé, Lille, France*

KU Leuven, Department of Mathematics, Leuven, Belgium

philip.dittmann@tu-dresden.de *Technische Universität Dresden, Institut für Algebra, Dresden, Germany*

kien.nguyenhuu@kuleuven.be *KU Leuven, Department of Mathematics, Leuven, Belgium*

Thang Long Institute of Mathematics and Applied Sciences, Hanoi, Vietnam

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in *ANT* are usually in English, but articles written in other languages are welcome.

Length There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@msp.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 14 No. 8 2020

1937-0652(2020)14:8;1-U