Algebra & Number Theory

Volume 17
2023
No. 10

msp

Algebra & Number Theory

msp.org/ant

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

The subscription price for 2023 is US $485/year for the electronic version, and $705/year (+$65, 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.

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 17:10 (2023)
https://doi.org/10.2140/ant.2023.17.1681

Special cycles on the basic locus of unitary Shimura varieties at ramified primes

Yousheng Shi

We study special cycles on the basic locus of certain unitary Shimura varieties over the ramified primes and their local analogs on the corresponding Rapoport–Zink spaces. We study the support and compute the dimension of these cycles.

1. Introduction

We study the basic locus of certain unitary Shimura varieties over ramified primes and special cycles on it. To approach this global problem we first study local special cycles on the corresponding Rapoport–Zink spaces and then apply a uniformization theorem to convert our local results on the Rapoport–Zink spaces to global ones. Our results will have applications to Kudla's program, in particular Kudla–Rapoport type of conjectures over these ramified primes; see [Kudla and Rapoport 2011; 2014; Li and Zhang 2022; Li and Liu 2022; He et al. 2023; Shi 2023].

We specialize to an integral model of Shimura varieties associated to $\mathrm{U}(1, n-1)$ which parametrize abelian schemes with certain CM action and a compatible principal polarization. This integral model and the corresponding model of Rapoport–Zink space is first proposed by Pappas [2000]; see also [Rapoport et al. 2021]. It is flat over the base, normal and Cohen–Macaulay and has isolated singularities. One can blow up these singularities to get a model which has semistable reduction and has a simple moduli interpretation; see [Krämer 2003]. We focus on the Pappas model in this paper but all results can be easily adjusted to the Krämer model case as these models are the same outside the singularities.

In the Rapoport–Zink spaces setting, we study the reduced locus of special cycles and compute their dimensions. As an intermediate step, we prove an isomorphism between two Rapoport–Zink spaces of

MSC2020: 11G15.
Keywords: special cycles, ramified primes, unitary Shimura variety.

different nature. In the Shimura variety setting, we write down the uniformization theorem of the basic locus over the ramified primes and then translate our local results to global ones. We now explain our results in more detail.

1A. *Local results.* Let $p > 2$ be a prime and fix a tower of finite extensions $\mathbb{Q}_p \subseteq H \subseteq F_0 \subset F$ where F/F_0 is quadratic and ramified. For any p-adic field R, we denote by $\mathcal{O}_R$ its ring of integers. Let $\breve{F}$ be the completion of the maximal unramified extension of F. Let $\mathrm{Nilp}\,\mathcal{O}_{\breve{F}}$ be the categories of $\mathcal{O}_{\breve{F}}$-schemes S on which p is locally nilpotent. For $S \in \mathrm{Nilp}\,\mathcal{O}_{\breve{F}}$, let $\bar{S} = S \times_{\mathrm{Spec}\,\mathcal{O}_{\breve{F}}} \mathrm{Spec}\,\bar{\mathbb{F}}_p$. The Rapoport–Zink space $\mathcal{N}^{F/H}_{(r,s)}$ is the moduli space over $\mathrm{Spf}\,\mathcal{O}_{\breve{F}}$ whose S points are objects $(X, \iota, \lambda, \rho)$ where X is a supersingular formal p-divisible group over S, $\iota : \mathcal{O}_F \to \mathrm{End}(X)$ is an $\mathcal{O}_F$-action on X whose restriction to $\mathcal{O}_H$ is strict, $\lambda : X \to X^\vee$ is a principal polarization, and $\rho : X \times_S \bar{S} \to \mathbb{X} \times_{\mathrm{Spec}\,\bar{\mathbb{F}}_p} \bar{S}$ is a map to a framing object $(\mathbb{X}, \iota_{\mathbb{X}}, \lambda_{\mathbb{X}})$ over $\mathrm{Spec}\,\bar{\mathbb{F}}_p$. We require that the Rosati involution of λ induces on $\mathcal{O}_F$ the Galois conjugation over $\mathcal{O}_{F_0}$ and the action ι satisfies the (r, s) signature condition (Definition 2.3). See Definitions 2.5 and 2.8 for the detailed definition of $\mathcal{N}^{F/H}_{(r,s)}$. We first show the following theorem (Theorem 2.10).

Theorem 1.1. *Suppose that F_0/H is unramified. Then there is an isomorphism*

$$\mathfrak{C} : \mathcal{N}^{F/H}_{(r,s)} \cong \mathcal{N}^{F/F_0}_{(r,s)}.$$

The significance of the above theorem is that $\mathcal{N}^{F/\mathbb{Q}_p}_{(r,s)}$ can be related to unitary Shimura varieties by the uniformization theorem while $\mathcal{N}^{F/F_0}_{(r,s)}$ is easier to study. From now on we mainly focus on the signature $(1, n-1)$. By [Rapoport et al. 2014] we know that $\mathcal{N}^{F/F_0}_{(1,n-1)}$ is representable by a formal scheme over $\mathrm{Spf}\,\mathcal{O}_{\breve{F}}$. Moreover there is a stratification of its reduced locus given by

$$(\mathcal{N}^{F/F_0}_{(1,n-1)})_{\mathrm{red}} = \biguplus_{\Lambda} \mathcal{N}^o_\Lambda$$

where Λ runs over the so-called vertex lattices, see Theorem 2.17.

We can define special cycles on both $\mathcal{N}^{F/H}_{(1,n-1)}$ and $\mathcal{N}^{F/F_0}_{(1,n-1)}$. The isomorphism in Theorem 1.1 maps special cycles in the first space to special cycles in the second. Without loss of generality we focus on $\mathcal{N}^{F/F_0}_{(1,n-1)}$. Let $(\mathbb{Y}, \iota_{\mathbb{Y}}, \lambda_{\mathbb{Y}})$ (resp. $(\mathbb{X}, \iota_{\mathbb{X}}, \lambda_{\mathbb{X}})$) be the framing object of $\mathcal{N}^{F/F_0}_{(0,1)}$ (resp. $\mathcal{N}^{F/F_0}_{(1,n-1)}$). Define an F vector space

$$\mathbb{V} := \mathrm{Hom}_{\mathcal{O}_F}(\mathbb{Y}, \mathbb{X}) \otimes_{\mathbb{Z}} \mathbb{Q}$$

of rank n with the Hermitian form $h(\cdot\,,\cdot)$ such that for any $x, y \in \mathbb{V}$ we have

$$h(x, y) = \lambda_{\mathbb{Y}}^{-1} \circ y^\vee \circ \lambda_{\mathbb{X}} \circ x \in \mathrm{End}_{\mathcal{O}_F}(\mathbb{Y}) \otimes \mathbb{Q} \xrightarrow{\cong} F,$$

where $y^\vee$ is the dual of y. For an $\mathcal{O}_F$-lattice $\boldsymbol{L} \subset \mathbb{V}$, the associated special cycle $\mathcal{Z}(\boldsymbol{L})$ is the subfunctor of $\mathcal{N}^{F/F_0}_{(0,1)} \times_{\mathrm{Spf}\,\mathcal{O}_{\breve{F}}} \mathcal{N}^{F/F_0}_{(1,n-1)}$ such that $\xi = (Y, \iota, \lambda_Y, \varrho_Y, X, \iota, \lambda_X, \varrho_X) \in \mathcal{Z}(\boldsymbol{L})(S)$ if for any $\boldsymbol{x} \in \boldsymbol{L}$ the quasihomomorphism

$$\varrho_X^{-1} \circ \boldsymbol{x} \circ \varrho_Y : Y \times_S \bar{S} \to X \times_S \bar{S}$$

lifts to a homomorphism from Y to X.

Any $\mathcal{O}_F$-lattice L with a Hermitian form $(\cdot\,,\cdot)$ has a Jordan splitting

$$L = \oplus_{\lambda\in\mathbb{Z}} L_\lambda \tag{1-1}$$

where $\oplus$ stands for orthogonal direct sum and L_λ is π^λ-modular (see Section 3A). We say L is integral if $(x, y) \in \mathcal{O}_F$ for any $x, y \in L$. For an integer t and a fixed Jordan decomposition as above we define

$$L_{\geq t} = \oplus_{\lambda\geq t} L_\lambda \subset L.$$

The following summarizes Theorems 3.9 and 3.10 and their corollaries.

Theorem 1.2. *Let $\boldsymbol{L} \subset \mathbb{V}$ be an $\mathcal{O}_F$-lattice of rank n:*

(i) *$\mathcal{Z}(\boldsymbol{L})$ is nonempty if and only if $\boldsymbol{L}$ is integral.*

(ii) *$\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}$ (the reduced scheme of $\mathcal{Z}(\boldsymbol{L})$) is a union of strata $\mathcal{N}^o_\Lambda$ where Λ ranges over a set of vertices which can be described in terms of $\boldsymbol{L}$.*

(iii) *Fix a Jordan decomposition of $\boldsymbol{L}$ as in (1-1). Define*

$$\mathfrak{d}(\boldsymbol{L}) := \begin{cases} \mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_{\geq 1}) - 1 & \textit{if } \mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_{\geq 1}) \textit{ is odd},\\ \mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_{\geq 1}) & \textit{if } \mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_{\geq 1}) \textit{ is even and } \boldsymbol{L}_{\geq 1}\otimes_{\mathbb{Z}}\mathbb{Q} \textit{ is split},\\ \mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_{\geq 1}) - 2 & \textit{if } \mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_{\geq 1}) \textit{ is even and } \boldsymbol{L}_{\geq 1}\otimes_{\mathbb{Z}}\mathbb{Q} \textit{ is nonsplit}.\end{cases}$$

Then $\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}$ is purely of dimension $\frac{1}{2}\mathfrak{d}(\boldsymbol{L})$, i.e., every irreducible component of $\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}$ is of dimension $\frac{1}{2}\mathfrak{d}(L)$. Here we say a Hermitian space V of dimension n is split if

$$(-1)^{n(n-1)/2}\det(V) \in \mathrm{Nm}_{F/F_0}(F^\times).$$

Otherwise we say it is nonsplit.

(iv) *Define*

$$n_{\mathrm{odd}} = \sum_{\lambda\geq 3,\ \lambda \textit{ is odd}} \mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_\lambda),$$

and

$$n_{\mathrm{even}} = \sum_{\lambda\geq 2,\ \lambda \textit{ is even}} \mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_\lambda).$$

Then $\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}$ is irreducible if and only if the following two conditions hold simultaneously:

(a) $n_{\mathrm{odd}} = 0$.

(b) $n_{\mathrm{even}} \leq 1$ *or* $n_{\mathrm{even}} = 2$ *and* $\boldsymbol{L}_{\geq 2}\otimes_{\mathbb{Z}}\mathbb{Q}$ *is nonsplit.*

1B. ***Global results.*** In the global setting, let F be a CM field with totally real subfield F_0 and $\Phi \subset \mathrm{Hom}_{\mathbb{Q}}(F, \mathbb{C})$ be a CM type of F. Denote by $x \mapsto \bar{x}$ the Galois conjugation of F/F_0 and fix a $\varphi_0 \in \Phi$. Define

$$\mathcal{V}_{\mathrm{ram}} = \{\text{finite places } v \text{ of } F_0 \mid v \text{ ramifies in } F\}. \tag{1-2}$$

We assume that $\mathcal{V}_{\mathrm{ram}}$ is nonempty and every $v \in \mathcal{V}_{\mathrm{ram}}$ is unramified over $\mathbb{Q}$ and does not divide 2.

Let V be a n dimensional F-vector space with a Hermitian form $(\cdot,\cdot)$ which has signature $(n-1,1)$ with respect to φ_0 and $(n,0)$ with respect to any other $\varphi\in\Phi\backslash\{\varphi_0\}$. The CM type Φ together with the signature of V determines a reflex field E and F embeds into E via φ_0. Define groups

$$Z^{\mathbb{Q}} := \{z\in \operatorname{Res}_{F/\mathbb{Q}}\mathbb{G}_m \mid \operatorname{Nm}_{F/F_0}(z)\in\mathbb{G}_m\},\qquad G=\operatorname{Res}_{F_0/\mathbb{Q}}\mathrm{U}(V).$$

Also define

$$\tilde{G} := Z^{\mathbb{Q}}\times G.$$

We can define a corresponding Hodge map $h_{\tilde{G}}:\mathbb{C}^\times\to\tilde{G}(\mathbb{R})$. By choosing a compact subgroup $K=K_{Z^{\mathbb{Q}}}\times K_G\subset\tilde{G}(\mathbb{A}_f)$ where $K_{Z^{\mathbb{Q}}}$ is the maximal compact subgroup of $Z^{\mathbb{Q}}(\mathbb{A}_f)$ (see (4-8)) and K_G is a compact subgroup of $G(\mathbb{A}_f)$, we get a Shimura variety $S(\tilde{G},h_{\tilde{G}})_K$ which has a canonical model over $\operatorname{Spec} E$. Further more if we assume K_G is the stabilizer of a self-dual lattice (see (4-7)), then [Rapoport et al. 2021] defined a moduli functor $\mathcal{M}$ of abelian varieties with $\mathcal{O}_F$-action and a compatible principal polarization over $\operatorname{Spec}\mathcal{O}_E$ whose complex fiber is $S(\tilde{G},h_{\tilde{G}})_K$. We review the definition in Section 4. By our assumption K is of the form $K=\prod_v K_v$ where we take the restricted product over all finite places of F_0. Throughout the paper, we use the notations

$$K_p=\prod_{v\mid p}K_v,\qquad K^p=\prod_{v\nmid p}K_v,$$

and similar notations with K replaced by K_G or $K_{Z^{\mathbb{Q}}}$.

Now assume $v_0\in\mathscr{V}_{\mathrm{ram}}$ and let w_0 be the place of F above it. Let p be the characteristic of the residue field of F_{0,v_0}. Fix a finite place ν of E above v_0 with residue field k_ν. Let $\breve{E}_\nu$ be the completion of the maximal unramified extension of E_ν. We denote by $\mathcal{M}_\nu^{ss}$ the basic locus of $\mathcal{M}$ at ν and denote by $\widehat{\mathcal{M}}_\nu^{ss}$ the completion of $\mathcal{M}\times_{\operatorname{Spec}\mathcal{O}_E}\operatorname{Spec}\mathcal{O}_{\breve{E}_\nu}$ along $\mathcal{M}_\nu^{ss}\times_{\operatorname{Spec}k_\nu}\operatorname{Spec}\bar{k}_\nu$. Then we have the following uniformization theorem which is a consequence of [Rapoport and Zink 1996, Theorem 6.30] and Theorem 1.1.

Theorem 1.3. *Assume $v_0\in\mathscr{V}_{\mathrm{ram}}$ and $\mathscr{V}_{\mathrm{ram}}$ satisfies the condition stated after (1-2). There is an isomorphism*

$$\Theta:\tilde{G}'(\mathbb{Q})\backslash\mathcal{N}'\times\tilde{G}(\mathbb{A}_f^p)/K^p\cong\widehat{M}_\nu^{ss}.$$

where $\tilde{G}'$ is an inner form of $\tilde{G}$ and

$$\mathcal{N}'=Z^{\mathbb{Q}}(\mathbb{Q}_p)/K_{Z^{\mathbb{Q}},p}\times(\mathcal{N}_{(1,n-1)}^{F_{w_0}/F_{0,v_0}}\widehat{\times}_{\operatorname{Spf}\mathcal{O}_{\breve{F}_{w_0}}}\operatorname{Spf}\mathcal{O}_{\breve{E}_\nu})\times\prod_{v\neq v_0}\mathrm{U}(V)(F_{0,v})/K_{G,v}$$

where the product in the last factor is over all places of F_0 over p not equal to v_0.

For a nondegenerate totally positive definite F/F_0-Hermitian matrix T, we define the special cycle $\mathcal{Z}(T)$ following the definition of [Kudla and Rapoport 2014] in Definition 5.2. Now assume T has rank n. Let V_T be the Hermitian F-space with Gram matrix T and define

$$\operatorname{Diff}(T,V) := \{v \text{ is a finite place of } F_0 \mid V_v \text{ is not isomorphic to } (V_T)_v\}. \tag{1-3}$$

It is well-known to experts that $\mathcal{Z}(T)$ is empty when $\mathrm{Diff}(T, V)$ contains more than one element and $\mathcal{Z}(T)$ is supported on $\mathcal{M}_\nu^{ss}$ over finite primes ν of E above v if $\mathrm{Diff}(T, V) = \{v\}$. We briefly review the proof of these results (see Proposition 5.4). Then the following theorem is a consequence of Theorems 1.2 and 1.3.

Theorem 1.4. *Assume that T is a totally positive definite F/F_0-Hermitian matrix with values in $\mathcal{O}_F$ such that* $\mathrm{Diff}(T, V) = \{v_0\}$ *where $v_0 \in \mathcal{V}_{\mathrm{ram}}$ and $\mathcal{V}_{\mathrm{ram}}$ satisfies the condition stated after (1-2). Then $\mathcal{Z}(T)$ is supported on $\mathcal{M}_\nu^{ss}$ and $\mathcal{Z}(T)_{\mathrm{red}}$ is equidimensional of dimension $\frac{1}{2}\mathfrak{d}(L_{v_0})$ where L_{v_0} is any Hermitian lattice over $\mathcal{O}_{F,v_0}$ whose gram matrix is T and $\mathfrak{d}(L_{v_0})$ is defined as in Theorem 1.2.*

The paper is organized as follows. In Section 2, we prove Theorem 1.1 (Theorem 2.10) and recall some properties of $\mathcal{N}_{(1,n-1)}^{F/F_0}$ as studied in [Rapoport et al. 2014]. In Section 3, we define our local version of special cycles on Rapoport–Zink spaces and prove Theorem 1.2 (Theorems 3.9 and 3.10). In Section 4, we recall the definition of the arithmetic model of the Shimura variety studied in [Rapoport et al. 2020]. In Section 5 we define global special cycles $\mathcal{Z}(T)$ and prove Theorems 1.3 (Theorem 5.6) and 1.4 (Theorem 5.7).

2. Relative and absolute Rapoport–Zink spaces

We use the notations as in Section 1A. In this section, we define the Rapoport–Zink space $\mathcal{N}_{(r,s)}^{F/H}$ and recall its basic properties from [Rapoport et al. 2014] when $H = F_0$ and $(r, s) = (1, n-1)$. The space $\mathcal{N}_{(1,n-1)}^{F/F_0}$ is convenient for studying special cycles. On the other hand $\mathcal{N}_{(r,s)}^{F/\mathbb{Q}_p}$ shows up naturally in the uniformization theorem (see Theorem 5.6) of the basic locus of certain unitary Shimura varieties (see Section 4). We call $\mathcal{N}_{(r,s)}^{F/F_0}$ (resp. $\mathcal{N}_{(r,s)}^{F/\mathbb{Q}_p}$) a relative (resp. absolute) Rapoport–Zink space following the terminology of [Mihatsch 2022].

In Theorem 2.10, we show that for different choices of H, $\mathcal{N}_{(r,s)}^{F/H}$ are isomorphic to each other given that F_0/H is unramified. We follow the approach of [Li and Liu 2022, Section 2.8]. Alternatively one can use the method of [Kudla et al. 2020]. The analog of Theorem 2.10 when F/F_0 is unramified was proved in [Mihatsch 2022].

2A. ***The signature condition.*** Assume F_0/H is unramified with degree f. We denote the Galois conjugation of F/F_0 by $x \mapsto \bar{x}$. Fix a uniformizer π of F such that $\pi_0 := \pi^2 \in F_0$ and is a uniformizer of F_0. Let $\boldsymbol{k}$ be the residue field of $\mathcal{O}_{F_0}$ (hence also that of $\mathcal{O}_F$) with an algebraic closure $\bar{\boldsymbol{k}}$. Let $\breve{H}$ be the completion of a maximal unramified extension of H (hence also that of F_0) in $\breve{F}$. Let $x \mapsto \sigma(x)$ denote the Frobenius of $\breve{H}/H$. Define

$$\Psi := \mathrm{Hom}_H(F_0, \breve{H}).$$

Fix a distinguished element $\psi_0 \in \Psi_0$. Define $\psi_i = \sigma^i \circ \psi_0$ for $i \in \mathbb{Z}/(f\mathbb{Z})$. Then

$$\Psi = \{\psi_i \mid i \in \mathbb{Z}/(f\mathbb{Z})\}.$$

Also define

$$\Phi := \mathrm{Hom}_H(F, \breve{F}).$$

Choose a partition of $\Phi = \Phi_+ \sqcup \Phi_-$ such that

$$\overline{\Phi}_+ = \Phi_-.$$

For $i \in \mathbb{Z}/(f\mathbb{Z})$, let φ_i be the element in Φ_+ such that its restriction to F_0 is ψ_i.

We denote by $\mathcal{O}_{\breve{H}}$ (resp. $\mathcal{O}_{\breve{F}}$) the ring of integers of $\breve{H}$ (resp. $\breve{F}$). There are decompositions by the Chinese remainder theorem

$$\mathcal{O}_{F_0} \otimes_{\mathcal{O}_H} \mathcal{O}_{\breve{H}} = \prod_{\psi \in \Psi} \mathcal{O}_{\breve{H}} \quad \text{and} \quad \mathcal{O}_F \otimes_{\mathcal{O}_H} \mathcal{O}_{\breve{H}} = \prod_{\psi \in \Psi} \mathcal{O}_F \otimes_{\mathcal{O}_{F_0},\psi} \mathcal{O}_{\breve{H}} \cong \prod_{\psi \in \Psi} \mathcal{O}_{\breve{F}}. \tag{2-1}$$

The Frobenius $1 \otimes \sigma$ is homogeneous and acts simply transitively on the index set.

Let S be an $\mathcal{O}_H$-scheme and $\mathfrak{L}$ be a locally free sheaf over S with an $\mathcal{O}_H$-action. We say the action is strict if it agrees with the structure map $\mathcal{O}_H \to \mathcal{O}_S$. A strict formal $\mathcal{O}_H$-module over S is formal p-divisible group over S with an $\mathcal{O}_H$-action $\iota : \mathcal{O}_H \to \operatorname{End}(X)$ such that its induced action on $\operatorname{Lie} X$ is strict. Denote by $X^\vee$ the dual of X in the category of strict $\mathcal{O}_H$-module; see [Mihatsch 2022, Section 11]. We say X is supersingular if its relative Dieudonné module (see [Fargues 2008, Appendix B.8]) over H at each geometric point of S has slope $\frac{1}{2}$.

Definition 2.1. For $S \in \operatorname{Nilp} \mathcal{O}_{\breve{F}}$, a hermitian $\mathcal{O}_F$-$\mathcal{O}_H$-module over S is a triple (X, ι, λ) where X is a strict formal $\mathcal{O}_H$-module together with an action $\iota : \mathcal{O}_F \to \operatorname{End}(X)$ extending the action of $\mathcal{O}_H$ and a principal polarization $X \to X^\vee$ such that

$$\lambda^{-1} \circ \iota(a)^\vee \circ \lambda = \iota(\bar{a}), \quad \forall a \in \mathcal{O}_F.$$

Two hermitian $\mathcal{O}_F$-$\mathcal{O}_H$-modules (X, ι, λ) and (X', ι', λ') are isomorphic (resp. quasiisogenic) if there is an $\mathcal{O}_F$-linear isomorphism (resp. quasiisogeny) $\varphi : X \to X'$ such that $\varphi^\vee \circ \lambda' \circ \varphi = \lambda$.

Let $r, s \in \mathbb{Z}_{\geq 0}$ and set $n := r + s$. Define the signature function $\Phi \to \mathbb{Z}_{\geq 0}$ by

$$r_\varphi = \begin{cases} r & \text{if } \varphi = \varphi_0, \\ 0 & \text{if } \varphi \in \Phi_+ \backslash \{\varphi_0\}, \\ n - r_{\bar{\varphi}} & \text{if } \varphi \in \Phi_-. \end{cases}$$

Definition 2.2. For $a \in F$, we define the following polynomial

$$P_{F/H,(r,s),\varphi_0,\Phi_+}(a; t) := \prod_{\varphi \in \Phi} (t - \varphi(a))^{r_\varphi}.$$

Let $S \in \operatorname{Nilp} \mathcal{O}_{\breve{F}}$ and $(\mathfrak{L}, \iota)$ a locally free sheaf over S together with an $\mathcal{O}_F$ action ι whose restriction to $\mathcal{O}_H$ is strict. Decomposition (2-1) induces a decomposition of $\mathfrak{L}$:

$$\mathfrak{L} = \bigoplus_{\psi \in \Psi} \mathfrak{L}_\psi. \tag{2-2}$$

Definition 2.3. We say $(\mathfrak{L}, \iota)$ satisfies the signature condition $(F/H, (r,s), \varphi_0, \Phi_+)$ if the following conditions are satisfied:

(i) $\operatorname{charpol}(\iota(a) \mid \mathfrak{L}) = P_{F/H,(r,s),\varphi_0,\Phi_+}(a;t)$ for all $a \in \mathcal{O}_F$.

(ii) $(\iota(a) - a)\,|_{\mathfrak{L}_{\psi_0}} = 0$ for all $a \in \mathcal{O}_{F_0}$.

(iii) For each $\varphi \in \Phi_+$ such that $r_\varphi \neq r_{\bar\varphi}$, the wedge condition of [Pappas 2000]:

$$\wedge^{r_{\bar\varphi}+1}((\iota(a) - \varphi(a)) \mid \mathfrak{L}_\psi) = 0, \qquad \wedge^{r_\varphi+1}((\iota(a) - \bar\varphi(a)) \mid \mathfrak{L}_\psi) = 0$$

is satisfied for all $a \in \mathcal{O}_F$ where $\psi \in \Psi$ is the restriction of φ to F_0.

Remark 2.4. When $r_\varphi = n$ or 0, the condition (iii) above is the same as the banal condition of [Li and Liu 2022, Definition 2.60] or the Eisenstein condition in [Kudla et al. 2020, Section 2.2].

Definition 2.5. Let $S \in \operatorname{Nilp} \mathcal{O}_{\breve F}$. Let

$$\mathfrak{H}_S(F/H, (r,s), \varphi_0, \Phi_+)$$

be the category of supersingular hermitian $\mathcal{O}_F$-$\mathcal{O}_H$-modules X over S such that the induced $\mathcal{O}_F$-action on $\operatorname{Lie} X$ satisfies the signature condition $(F/H, (r,s), \varphi_0, \Phi_+)$.

2B. ***Comparison theorem.*** We will prove the following theorem.

Theorem 2.6. *Assume that F_0/H is unramified. For $S \in \operatorname{Nilp} \mathcal{O}_{\breve F}$, there is an equivalence of categories*

$$\mathcal{C}_S : \mathfrak{H}_S(F/H, (r,s), \varphi_0, \Phi_+) \to \mathfrak{H}_S(F/F_0, (r,s), \varphi_0, \{\varphi_0\})$$

that is compatible with base change.

If $S = \operatorname{Spec} R$, we often write $\mathfrak{H}_R$ (resp. $\mathcal{C}_R$) instead of $\mathfrak{H}_S$ (resp. $\mathcal{C}_S$). To prove Theorem 2.6, we will use the theory of f-$\mathcal{O}$-displays developed by [Ahsendorf et al. 2016]. We recall some definitions and notations. For an $\mathcal{O}_H$-algebra R, let $W_{\mathcal{O}_H}(R)$ be the relative Witt ring with respect to a fixed uniformizer of H; see for example [Fargues and Fontaine 2018, Definition 1.2.2]. Let $x \mapsto {}^{\boldsymbol{F}}x$ be the Frobenius endomorphism and $x \mapsto {}^{\boldsymbol{V}}x$ be the Verschiebung. Let $I_{\mathcal{O}_H}(R) = {}^{\boldsymbol{V}}W_{\mathcal{O}_H}(R)$ and we can define ${}^{\boldsymbol{V}^{-1}}$ on $I_{\mathcal{O}_H}(R)$. For $a \in R$, let $[a] \in W_{\mathcal{O}_H}(R)$ be its Teichmüller representative.

Let $\hat\psi_i$ be the composition of ψ_i with the Cartier morphism $\mathcal{O}_{\breve H} \to W_{\mathcal{O}_H}(\mathcal{O}_{\breve H})$. For $i \in \mathbb{Z}/(f\mathbb{Z})$, let ϵ_i be the unique unit in $W_{\mathcal{O}_H}(\mathcal{O}_{F_0})$ such that ${}^{\boldsymbol{V}}\epsilon_i = [\psi_i(\pi_0)] - \hat\psi_i(\pi_0)$, which exists by [Ahsendorf et al. 2016, Lemma 2.24]. Following [Li and Liu 2022, (2.20)], we can define a unit $\mu_\pi \in W_{\mathcal{O}_H}(\mathcal{O}_{\breve H})$ such that

$$\frac{{}^{\boldsymbol{F}^f}\mu_\pi}{\mu_\pi} = \prod_{i=1}^{f-1} {}^{\boldsymbol{F}^{f-1-i}}\epsilon_i. \tag{2-3}$$

Definition 2.7 [Ahsendorf et al. 2016, Definition 2.1]. Assume $f \in \mathbb{Z}_{\geq 1}$. An f-$\mathcal{O}_H$-display over R is a quadruple $\mathcal{P} = (P, Q, \boldsymbol{F}, \dot{\boldsymbol{F}})$ consisting of the following data: a finitely generated projective $W_{\mathcal{O}_H}(R)$-module P, a submodule $Q \subset P$, and two ${}^{\boldsymbol{F}^f}$-linear maps

$$\boldsymbol{F} : P \to P \quad \text{and} \quad \dot{\boldsymbol{F}} : Q \to P.$$

The following conditions are required:

(i) $I_{\mathcal{O}_H}(R)P \subseteq Q$ and there is a decomposition of $W_{\mathcal{O}_H}(R)$-modules $P = L \oplus T$ such that $Q = L \oplus I_{\mathcal{O}_H}(R)T$. Such a decomposition is called a normal decomposition.

(ii) $\dot{\boldsymbol{F}}$ is an ${}^{\boldsymbol{F}^f}$-linear epimorphism.

(iii) For all $x \in P$ and $w \in W_{\mathcal{O}_H}(R)$, we have

$$\dot{\boldsymbol{F}}({}^{\boldsymbol{V}} wx) = {}^{\boldsymbol{F}^{f-1}} w\boldsymbol{F}(x).$$

We define the Lie algebra of $\mathcal{P}$ to be $\operatorname{Lie}\mathcal{P} := P/Q$. If $f = 1$, we simply call $\mathcal{P}$ an $\mathcal{O}_H$-display.

We refer to [Ahsendorf et al. 2016, Definition 2.3] for the definition of a nilpotent display and [Mihatsch 2022, Section 11] for the notion of polarizations of displays; see also [Kudla et al. 2020, Section 3]. The main result of [Ahsendorf et al. 2016] tells us that there are equivalences of categories

$$\{\text{nilpotent } f\text{-}\mathcal{O}_H\text{-displays over} R\} \to \{\text{strict formal } \mathcal{O}_{F_0}\text{-modules over } R\}$$

where $f = [F_0 : H]$, in particular

$$\{\text{nilpotent } \mathcal{O}_H\text{-displays over} R\} \to \{\text{strict formal } \mathcal{O}_H\text{-modules over } R\}.$$

Proof of Theorem 2.6. The proof is similar with that of [Li and Liu 2022, Proposition 2.62]. Assume that $S = \operatorname{Spec} R \in \operatorname{Nilp} \mathcal{O}_{\breve{F}}$. We abuse notation and denote the composition of $\hat{\psi}_i$ with $W_{\mathcal{O}_H}(\mathcal{O}_{\breve{F}_0}) \to W_{\mathcal{O}_H}(R)$ by $\hat{\psi}_i$ as well. Then (2-1) induces

$$\mathcal{O}_F \otimes_{\mathcal{O}_H} W_{\mathcal{O}_H}(R) = \prod_{\psi\in\Psi} \mathcal{O}_F \otimes_{\mathcal{O}_{F_0},\hat{\psi}_i} W_{\mathcal{O}_H}(R). \tag{2-4}$$

Assume $(X, \iota, \lambda) \in \mathfrak{H}_S(F/H, (r, s), \varphi_0, \Phi_+)$ and $\mathcal{P} = (P, Q, \boldsymbol{F}, \dot{\boldsymbol{F}})$ be its associated $\mathcal{O}_H$-display. Then $\mathcal{P}$ has an $\mathcal{O}_F$ action (still denoted by ι). Equation (2-4) induces the following decomposition

$$P = \bigoplus_{\psi\in\Psi} P_\psi, \quad Q = \bigoplus_{\psi\in\Psi} Q_\psi, \text{ with } Q_\psi = P_\psi \cap Q \tag{2-5}$$

where P_ψ has an $\mathcal{O}_F \otimes_{\mathcal{O}_{F_0},\hat{\psi}_i} W_{\mathcal{O}_H}(R)$ action. Then $\boldsymbol{F}$ and $\dot{\boldsymbol{F}}$ shift the grading on P in the following way:

$$\boldsymbol{F} : P_\psi \to P_{\sigma\circ\psi} \quad \text{and} \quad \dot{\boldsymbol{F}} : Q_\psi \to P_{\sigma\circ\psi}.$$

As in [Mihatsch 2022, Section 11.1], the principal polarization λ is equivalent to a collection of perfect $W_{\mathcal{O}_H}(R)$-bilinear skew-symmetric pairings

$$\{\langle\cdot,\cdot\rangle_\psi : P_\psi \times P_\psi \to W_{\mathcal{O}_H}(R) \mid \psi \in \Psi\}$$

such that $\langle\iota(a)x, y\rangle_\psi = \langle x, \iota(\bar{a})y\rangle_\psi$ for all $a \in \mathcal{O}_F$, $x, y \in P_\psi$ and $\langle\dot{\boldsymbol{F}}x, \dot{\boldsymbol{F}}y\rangle_{\sigma\circ\psi} = {}^{\boldsymbol{V}^{-1}}\langle x, y\rangle_\psi$ for all $x, y \in Q_\psi$.

For $\psi \neq \psi_0$, by [Li and Liu 2022, Lemma 2.60], the banal signature condition implies

$$Q_\psi = (\pi \otimes 1 + 1 \otimes [\varphi(\pi)])P_\psi + I_{\mathcal{O}_H}(R)P_\psi.$$

where φ is the element in Φ_+ above ψ. Hence for $\psi \neq \psi_0$, we can define

$$\boldsymbol{F}' : P_\psi \to P_{\sigma\circ\psi} : x \mapsto \dot{\boldsymbol{F}}((\pi \otimes 1 + 1 \otimes [\varphi(\pi)])x).$$

By [loc. cit.], $\boldsymbol{F}'$ is an ${}^{\boldsymbol{F}}$-linear isomorphism. Now define

$$P^{\mathrm{rel}} = P_{\psi_0}, \quad Q^{\mathrm{rel}} = Q_{\psi_0}, \quad \boldsymbol{F}^{\mathrm{rel}} = ((\boldsymbol{F}')^{f-1} \circ \boldsymbol{F})|_{P^{\mathrm{rel}}}, \quad \dot{\boldsymbol{F}}^{\mathrm{rel}} = ((\boldsymbol{F}')^{f-1} \circ \dot{\boldsymbol{F}})|_{Q^{\mathrm{rel}}}.$$

Then $\mathcal{P}^{\mathrm{rel}} := (P^{\mathrm{rel}}, Q^{\mathrm{rel}}, \boldsymbol{F}^{\mathrm{rel}}, \dot{\boldsymbol{F}}^{\mathrm{rel}})$ is a f-$\mathcal{O}_H$-display over R. Define

$$\iota^{\mathrm{rel}} : \mathcal{O}_F \to \mathrm{End}(\mathcal{P}^{\mathrm{rel}})$$

simply by restricting ι to P_{ψ_0}. Then the signature condition $(F/H, (r, s), \varphi_0, \Phi_+)$ restricted on P_{ψ_0} is exactly the same as the signature condition $(F/F_0, (r, s), \varphi_0, \{\varphi_0\})$. Define

$$\langle\cdot,\cdot\rangle^{\mathrm{rel}} := \mu_\pi\langle\cdot,\cdot\rangle|_{P^{\mathrm{rel}}}$$

where μ_π is as in (2-3). Then $\langle\cdot,\cdot\rangle^{\mathrm{rel}}$ is a perfect $W_{\mathcal{O}_H}(R)$-bilinear skew-symmetric pairing such that $\langle\iota(a)x, y\rangle^{\mathrm{rel}} = \langle x, \iota(\bar{a})y\rangle^{\mathrm{rel}}$ for all $a \in \mathcal{O}_F$, $x, y \in P^{\mathrm{rel}}$. By the calculation before [Li and Liu 2022, Remark 2.61], we also have

$$\langle\dot{\boldsymbol{F}}^{\mathrm{rel}}x, \dot{\boldsymbol{F}}^{\mathrm{rel}}y\rangle^{\mathrm{rel}} = {}^{\boldsymbol{F}^{f-1}\boldsymbol{V}^{-1}}\langle x, y\rangle^{\mathrm{rel}}, \quad \forall x, y \in Q^{\mathrm{rel}}.$$

The form $\langle\cdot,\cdot\rangle^{\mathrm{rel}}$ gives a principal polarization of $\mathcal{P}^{\mathrm{rel}}$. The pair $(\mathcal{P}^{\mathrm{rel}}, \iota^{\mathrm{rel}})$ together with the polarization gives an object

$$(X, \iota, \lambda)^{\mathrm{rel}} \in \mathfrak{H}_S(F/F_0, (r, s), \varphi_0, \{\varphi_0\}).$$

This is defined to be $\mathcal{C}_S((X, \iota, \lambda))$. The functor $\mathcal{C}_S$ is obviously functorial in S. The fact that $\mathcal{C}_S$ is an equivalence of categories can be proved verbatim as that of [Li and Liu 2022, Proposition 2.62]. □

2C. *Comparison of Rapoport–Zink spaces.* Fix a triple

$$(\mathbb{X}^{F/H}, \iota_{\mathbb{X}}^{F/H}, \lambda_{\mathbb{X}}^{F/H}) \in \mathfrak{H}_{\bar{k}}(F/H, (r, s), \varphi_0, \Phi_+).$$

We essentially only have one or two such choices up to isogeny according to n being odd or even, see Remark 2.14 below.

Definition 2.8. Let $\mathcal{N}_{(r,s)}^{F/H}$ be the functor which associates to $S \in \mathrm{Nilp}\,\mathcal{O}_{\breve{F}}$ the set of isomorphism classes of quadruples $(X, \iota, \lambda, \varrho)$ where

(i) $(X, \iota, \lambda) \in \mathfrak{H}_S(F/H, (r, s), \varphi_0, \Phi_+)$,

(ii) $\varrho : X \times_S \bar{S} \to \mathbb{X}^{F/H} \times_{\mathrm{Spec}\,\bar{k}} \bar{S}$ is a $\mathcal{O}_F$-linear quasiisogeny of height 0 such that λ and $\varrho^*(\lambda_{\mathbb{X}}^{F/H})$ differ locally on $\bar{S}$ by a factor in $\mathcal{O}_H^\times$.

An isomorphism between two such quadruples $(X, \iota, \lambda, \varrho)$ and $(X', \iota', \lambda', \varrho')$ is given by an $\mathcal{O}_F$-linear isomorphism $\alpha : X \to X'$ such that $\varrho' \circ (\alpha \times_S \bar{S}) = \varrho$ and $\alpha^*(\lambda')$ is an $\mathcal{O}_H^\times$ multiple of λ.

Remark 2.9. In the definition of $\mathcal{N}_{(r,s)}^{F/H}$, we can replace condition (ii) by the condition that ϱ is a $\mathcal{O}_F$-linear quasiisogeny of height 0 such that $\lambda = \varrho^*(\lambda_{\mathbb{X}})$. The resulting functor is isomorphic to the original one as $(X, \iota, \lambda, \varrho)$ and $(X, \iota, a\lambda, \varrho)$ are isomorphic in $\mathcal{N}_{(r,s)}^{F/F_0}$ for $a \in \mathcal{O}_H^\times$.

By [Rapoport and Zink 1996, Chapter 3], $\mathcal{N}_{(r,s)}^{F/H}$ is representable by a formal scheme locally of finite type over $\operatorname{Spf} \mathcal{O}_{\breve{F}}$.

Theorem 2.10. *Assume F_0/H is unramified and the framing object $(\mathbb{X}^{F/F_0}, \iota_{\mathbb{X}}^{F/F_0}, \lambda_{\mathbb{X}}^{F/F_0})$ used in the definition of $\mathcal{N}_{(r,s)}^{F/F_0}$ is isomorphic to $\mathcal{C}_{\bar{k}}((\mathbb{X}^{F/H}, \iota_{\mathbb{X}}^{F/H}, \lambda_{\mathbb{X}}^{F/H}))$. Then there is an isomorphism*

$$\mathfrak{C} : \mathcal{N}_{(r,s)}^{F/H} \cong \mathcal{N}_{(r,s)}^{F/F_0}.$$

Proof. This is a consequence of Theorem 2.6. □

2D. *The relative Rapoport–Zink space.*

In this subsection we assume $H = F_0$. We simply denote $\mathcal{N}_{(r,s)}^{F/F_0}$ by $\mathcal{N}_{(r,s)}$ and $\mathfrak{H}_S(F/F_0, (r, s), \varphi_0, \{\varphi_0\})$ by $\mathfrak{H}_S(r, s)$. We recall some background information on $\mathcal{N}_{(1,n-1)}$ from [Rapoport et al. 2014]. Although [Rapoport et al. 2014] works on the category of p-divisible groups, their arguments and results easily extend to the category of strict formal $\mathcal{O}_{F_0}$-modules using relative Dieudonné theory.

Proposition 2.11 [Rapoport et al. 2014, Proposition 2.1]. *The functor $\mathcal{N}_{(1,n-1)}$ is representable by a separated formal scheme $\mathcal{N}_{(1,n-1)}$, locally of finite type and flat over* $\operatorname{Spf} \mathcal{O}_{\breve{F}}$. *It is formally smooth over* $\operatorname{Spf} \mathcal{O}_{\breve{F}}$ *in all points of the special fiber except the superspecial points. Here a point $z \in \mathcal{N}_{(1,n-1)}(\bar{\boldsymbol{k}})$ is superspecial if* $\operatorname{Lie}(\iota(\pi)) = 0$ *where $(X, \iota, \lambda, \varrho)$ is the pullback of the universal object of $\mathcal{N}_{(1,n-1)}$ to z. The superspecial points form an isolated set of points.*

For the signature $(0, 1)$ we know that $\mathcal{N}_{(0,1)} \cong \operatorname{Spf} \mathcal{O}_{\breve{F}}$ and has a universal formal $\mathcal{O}_F$-module $\mathcal{Y}$ (the canonical lifting of $\mathbb{Y}$ in the sense of [Gross 1986]) over it.

Remark 2.12. The formal scheme $\mathcal{N}_{(1,n-1)}$ is denoted as $\mathcal{N}^0$ in [Rapoport et al. 2014]. In the rest of this section and Section 3 we often simply write $\mathcal{N}$ for $\mathcal{N}_{(1,n-1)}$ if the context is clear.

Let F^u be the unique unramified quadratic extension of F_0 in $\breve{F}_0$ where $\breve{F}_0$ is the completion of the maximal unramified extension of F_0 in $\breve{F}$. Let $\sigma \in \operatorname{Gal}(\breve{F}_0/F_0)$ be the Frobenius element. For a formal $\mathcal{O}_{F_0}$-module, we denote by $M(X)$ the relative Dieudonné module of X. When X has F_0-height n and dimension n over $\bar{\boldsymbol{k}}$, $M(X)$ is a free $\mathcal{O}_{\breve{F}_0}$-module of rank $2n$ with a σ-linear operator $\boldsymbol{F}$ and a σ^{-1}-linear operator $\boldsymbol{V}$ such that $\boldsymbol{V}\boldsymbol{F} = \boldsymbol{F}\boldsymbol{V} = \pi_0$. Denote by $\mathbb{E} = \breve{F}_0[\boldsymbol{F}, \boldsymbol{V}]$ the rational Cartier ring.

Fix a framing object $(\mathbb{X}, \iota_{\mathbb{X}}, \lambda_{\mathbb{X}}) \in \mathfrak{H}_{\bar{k}}(1, n-1)$. Let $N := M(\mathbb{X}) \otimes_{\mathbb{Z}} \mathbb{Q}$ be the rational relative Dieudonné module of $\mathbb{X}$. Then N has a skew-symmetric $\breve{F}_0$-bilinear form $\langle \cdot, \cdot \rangle$ induced by $\lambda_{\mathbb{X}}$ such that for any $x, y \in N$ we have

$$\langle \boldsymbol{F}x, y \rangle = \langle x, \boldsymbol{V}y \rangle^\sigma, \quad \langle \iota(a)x, y \rangle = \langle x, \iota(\bar{a})y \rangle, \quad a \in F.$$

We simply denote by π the induced action of $\iota_{\mathbb{X}}(\pi)$ on N. Define a σ-linear operator

$$\tau = \pi \boldsymbol{V}^{-1} = \pi^{-1} F \tag{2-6}$$

on N. Set $C = N^{\tau}$ (the set of τ-fixed points in N), then we obtain a n-dimensional F-vector space with an isomorphism

$$C \otimes_F \breve{F} \simeq N.$$

For $x, y \in C$, we have

$$\langle x, y\rangle = \langle \tau(x), \tau(y)\rangle = \langle \pi^{-1}\boldsymbol{F}x, \pi \boldsymbol{V}^{-1}y\rangle = -\langle \boldsymbol{F}x, \boldsymbol{V}^{-1}y\rangle = -\langle x, y\rangle^{\sigma}$$

Choose $\delta \in F^u \backslash F_0$ such that $\delta^2 \in \mathcal{O}_{F_0}^{\times}$. Define a form $(\cdot\,,\cdot)$ on N by

$$(x, y) = \delta(\langle \pi x, y\rangle + \pi\langle x, y\rangle) \tag{2-7}$$

for all $x, y \in C$. Then $(\cdot\,,\cdot)$ is Hermitian with values in F when restricted on C and

$$\langle x, y\rangle = \frac{1}{2\delta}\operatorname{tr}_{F/F_0}(\pi^{-1}(x, y)), \forall x, y \in C. \tag{2-8}$$

Remark 2.13. There is a unique object $(\mathbb{Y}, \iota_{\mathbb{Y}}, \lambda_{\mathbb{Y}}) \in \mathfrak{H}_{\bar{k}}(0, 1)$ up to isomorphism. We want to describe $M(\mathbb{Y})$ explicitly. As an $\mathcal{O}_{F_0}$-lattice, it is of rank 2. We can choose a basis $\{e_1, e_2\}$ such that $\boldsymbol{F}e_1 = e_2$, $\boldsymbol{F}e_2 = \pi_0 e_1$, $\boldsymbol{V}e_1 = e_2$, $\boldsymbol{V}e_2 = \pi_0 e_1$ and $\langle e_1, e_2\rangle = \delta$. With respect to this basis, $\operatorname{End}^0(\mathbb{Y}) = \operatorname{End}_{\mathbb{E}}(N)$ is of the form

$$\left\{ \begin{pmatrix} a & b\pi_0 \\ b^{\sigma} & a^{\sigma} \end{pmatrix} \,\middle|\, a, b \in F^u \right\},$$

which is the quaternion algebra $\mathbb{H}$ over F_0. By changing basis using elements in $\mathbb{H} \cap \mathrm{SL}_2(F_0)$ we can assume F, V are of the same matrix form as before and

$$\pi = \begin{pmatrix} 0 & \pi_0 \\ 1 & 0 \end{pmatrix}.$$

Thus τ is the diagonal matrix $\operatorname{diag}\{1, 1\}$ and fixes the F_0-vector space $\operatorname{span}_{F_0}\{e_1, e_2\}$. We have $(e_1, e_1) = -\delta^2$. As $\mathcal{O}_F$ is a DVR and N^{τ} is a one dimensional F-space, $\operatorname{span}_{\mathcal{O}_F}\{e_1\}$ is the unique self-dual $\mathcal{O}_F$-lattice w.r.t. $(\cdot\,,\cdot)$. Let $\varrho_{\mathbb{Y}}$ be the identity of $\mathbb{Y}$, then $(\mathbb{Y}, \iota_{\mathbb{Y}}, \lambda_{\mathbb{Y}}, \varrho_{\mathbb{Y}})$ is the unique closed point of $\mathcal{N}_{(0,1)}(\bar{\boldsymbol{k}})$.

Remark 2.14. By [Rapoport et al. 2014, Remark 4.2], when n is odd (resp. even) there is a unique (resp. exactly two) object $(\mathbb{X}, \iota_{\mathbb{X}}, \lambda_{\mathbb{X}}) \in \mathfrak{H}_{\bar{k}}(1, n-1)$ up to isogenies that preserves the $\lambda_{\mathbb{X}}$ by a factor in $\mathcal{O}_{F_0}^{\times}$. These are the framing objects in the definition of $\mathcal{N}_{(1,n-1)}$. This matches the number of similarity classes of Hermitian forms over local fields.

When n is odd, we simply take $(\mathbb{X}, \iota_{\mathbb{X}}, \lambda_{\mathbb{X}}) := (\mathbb{Y}, \iota_{\mathbb{Y}}, \lambda_{\mathbb{Y}})^n$ where $(\mathbb{Y}, \iota_{\mathbb{Y}}, \lambda_{\mathbb{Y}})$ is defined in the previous remark. When n is even, we again define $\mathbb{X} := \mathbb{Y}^n$ with the diagonal action $\iota_{\mathbb{X}}$ by $\mathcal{O}_F$. There are two choices of polarizations. The first one $\lambda_{\mathbb{X}}^{+} \in \operatorname{End}^0(\mathbb{X}) \cong M_n(\mathbb{H})$ is given by the antidiagonal matrix with 1's on the antidiagonal. The second one $\lambda_{\mathbb{X}}^{-}$ is defined by the diagonal matrix $\operatorname{diag}(1, \ldots, 1, u_1, u_2)$ where $u_1, u_2 \in \mathcal{O}_{F_0}^{\times}$ and $-u_1 u_2 \notin \operatorname{Nm}_{F/F_0}(F^{\times})$.

For two $\mathcal{O}_F$-lattices Λ, Λ' of C, we use the notation $\Lambda \subset^{\ell} \Lambda'$ to stand for the situation when $\pi\Lambda' \subseteq \Lambda \subseteq \Lambda'$ and $\dim_{\boldsymbol{k}}(\Lambda'/\Lambda) = \ell$. Define

$$\Lambda^{\sharp} := \{x \in C \mid (x, \Lambda) \subseteq \mathcal{O}_F\}, \quad \Lambda^{\vee} := \{x \in C \mid \delta\langle x, \Lambda\rangle \subseteq \mathcal{O}_{F_0}\}. \tag{2-9}$$

Similarly for an $\mathcal{O}_{\breve{F}}$-lattice $M \subset N$, define

$$M^{\sharp} := \{x \in N \mid (x, M) \subseteq \mathcal{O}_{\breve{F}}\}, \quad M^{\vee} := \{x \in N \mid \langle x, M\rangle \subseteq \mathcal{O}_{\breve{F}_0}\}. \tag{2-10}$$

Then by (2-7) and (2-8), $\Lambda^{\sharp} = \Lambda^{\vee}$. Similarly $M^{\sharp} = M^{\vee}$.

Proposition 2.15 [Rapoport et al. 2014, Proposition 2.4]. *Define the following set of $\mathcal{O}_{\breve{F}}$-lattices*

$$\mathcal{V} := \{M \subseteq N \mid M^{\sharp} = M, \pi\tau(M) \subseteq M \subseteq \pi^{-1}\tau(M), M \subset^{\leq 1} (M + \tau(M))\},$$

Then the map

$$(X, \iota, \lambda, \varrho) \mapsto \varrho(M(X)) \subset N$$

defines a bijection from $\mathcal{N}(\bar{\boldsymbol{k}})$ to $\mathcal{V}$.

A vertex lattice in C is an $\mathcal{O}_F$-lattice $\Lambda \subset C$ such that $\pi\Lambda \subseteq \Lambda^{\sharp} \subseteq \Lambda$. We denote the dimension of the $\boldsymbol{k}$-vector space $\Lambda/\Lambda^{\sharp}$ by $t(\Lambda)$, and call it the type of Λ. It is an even integer; see [Rapoport et al. 2014, Lemma 3.2].

Lemma 2.16 [Rapoport et al. 2014, Proposition 4.1]. *$\forall M \in \mathcal{V}$, there is a unique minimal vertex lattice $\Lambda(M)$ such that $M \subseteq \Lambda(M) \otimes_{\mathcal{O}_F} \mathcal{O}_{\breve{F}}$.*

Define

$$\mathcal{V}(\Lambda) := \{M \in \mathcal{V} \mid M \subseteq \Lambda \otimes_{\mathcal{O}_F} \mathcal{O}_{\breve{F}}\} \quad \text{and} \quad \mathcal{V}^{o}(\Lambda) := \{M \in \mathcal{V} \mid \Lambda(M) = \Lambda\}.$$

Then apparently $\mathcal{V}^{o}(\Lambda) \subseteq \mathcal{V}(\Lambda)$. The following theorem summarizes what we need from [Rapoport et al. 2014, Section 6], in particular [loc. cit., Theorem 6.10].

Theorem 2.17. *We have the following facts*:

(i) *For two vertex lattices Λ_1 and Λ_2*

$$\mathcal{V}(\Lambda_1) \subseteq \mathcal{V}(\Lambda_2) \Leftrightarrow \Lambda_1 \subseteq \Lambda_2.$$

If $\Lambda_1 \cap \Lambda_2$ is a vertex lattice, then

$$\mathcal{V}(\Lambda_1 \cap \Lambda_2) = \mathcal{V}(\Lambda_1) \cap \mathcal{V}(\Lambda_2),$$

otherwise $\mathcal{V}(\Lambda_1) \cap \mathcal{V}(\Lambda_2) = \varnothing$.

(ii) *For each vertex lattice Λ, there exist a reduced projective variety $\mathcal{N}_{\Lambda}^{o}$ over* Spec $\bar{\boldsymbol{k}}$ *such that*

$$\mathcal{N}_{\Lambda}^{o}(\bar{\boldsymbol{k}}) = \mathcal{V}^{o}(\Lambda).$$

The closure of any $\mathcal{N}^o_\Lambda$ *in* $\mathcal{N}_{\mathrm{red}}$ *is given by*

$$\mathcal{N}_\Lambda := \biguplus_{\Lambda' \subseteq \Lambda} \mathcal{N}^o_{\Lambda'},$$

where the union is taken over vertex lattices Λ' *included in* Λ. $\mathcal{N}_\Lambda$ *is a projective variety of dimension* $t(\Lambda)/2$. *Its set of* $\bar{\boldsymbol{k}}$ *points is* $\mathcal{V}(\Lambda)$. *The inclusion of points* $\mathcal{V}(\Lambda_1) \subseteq \mathcal{V}(\Lambda_2)$ *in* (i) *is induced by a closed embedding* $\mathcal{N}_{\Lambda_1} \to \mathcal{N}_{\Lambda_2}$.

(iii) *There is a stratification of the reduced locus of* $\mathcal{N}$ *given by*

$$\mathcal{N}_{\mathrm{red}} = \biguplus_{\Lambda} \mathcal{N}^o_\Lambda$$

where the union is over all vertex lattices. $\mathcal{N}(\bar{\boldsymbol{k}})$ *is nonempty for all* $n \geq 1$.

3. Special cycles on Rapoport–Zink spaces

In this section, we define special cycles on $\mathcal{N}^{F/H}_{(1,n-1)}$. We then state our main results on the support of these cycles. First we need some background information on Hermitian lattices.

3A. ***Hermitian lattices and Jordan splitting.*** We use $\oplus$ to denote direct sum of mutually orthogonal spaces. In particular, we use

$$(\alpha_1) \oplus \cdots \oplus (\alpha_n)$$

to denote the n-dimensional F vector space (or $\mathcal{O}_F$-lattice depending on the context) with a Hermitian form given by a diagonal matrix $\mathrm{diag}\{\alpha_1, \ldots, \alpha_n\}$ with respect to an orthogonal basis. We also use $H(i)$ to denote the hyperbolic plane which is the lattice of rank 2 with Hermitian form given by the matrix

$$\begin{pmatrix} 0 & \pi^i \\ (-\pi)^i & 0 \end{pmatrix}$$

with respect to a certain basis.

For a Hermitian lattice L with Hermitian form $(\cdot\,,\cdot)$, define sL to be $\min\{\mathrm{val}_\pi(x, y) \mid x, y \in L\}$ where val_π is normalized such that $\mathrm{val}_\pi(\pi) = 1$. We say $x \in L$ is maximal if x is not in πL. We say L is π^i-modular if $(x, L) = \pi^i \mathcal{O}_F$ for every maximal vector x in L.

Any Hermitian lattice L has a Jordan splitting

$$L = \oplus_{\lambda \in \mathbb{Z} \cup \{\infty\}} L_\lambda \tag{3-1}$$

where L_λ is π^λ-modular and L_∞ is defined to be the radical of L. Any two Jordan splitting of L have the same invariants; see [Jacobowitz 1962, Page 449].

Proposition 3.1 [Jacobowitz 1962, Proposition 8.1]. *Let* L *be a* π^i*-modular lattice of rank* n. *Then*:

(1) $L \simeq (\pi_0^i/2) \oplus (\pi_0^i/2) \oplus \cdots \oplus (\pi_0^{-(n-1)i/2} \det(L))$ *if* i *is even.*

(2) $L \simeq H(i) \oplus H(i) \oplus \cdots \oplus H(i)$ *if* i *is odd.*

In particular, when i *is odd* L *must have even rank.*

For a sub-$\mathcal{O}_F$-module L in a Hermitian F-vector space V, define

$$L_V^\sharp := \{x \in V \mid (x, y) \in \mathcal{O}_F, \forall y \in L\}. \tag{3-2}$$

When $V = L \otimes_{\mathbb{Z}} \mathbb{Q}$, we simply denote $L_V^\sharp$ by $L^\sharp$. We will use the following basic lemmas throughout the paper, sometimes without explicitly referring to them.

Lemma 3.2. *Assume L and L' are $\mathcal{O}_F$-submodules inside a Hermitian F-vector space V. Then*:

(1) $(L + L')_V^\sharp = L_V^\sharp \cap (L')_V^\sharp$.

(2) $(L_V^\sharp)_V^\sharp = L$.

Proof. (1) follows from the definition of $L_V^\sharp$. (2) can be proved by using the Jordan splitting of L. □

Lemma 3.3. *Assume L' is a sub-$\mathcal{O}_F$-module of L such that L' is π^s-modular with $s = sL$. Then $L = L' \oplus (L')^\perp$ where $(L')^\perp$ is the perpendicular complement of L' in L.*

Proof. This is a direct consequence of [Jacobowitz 1962, Proposition 4.2]. □

3B. ***Special cycles.*** For a moment, we go back to the setting of Section 2C. Let $(\mathbb{X}^{F/H}, \iota_{\mathbb{X}}^{F/H}, \lambda_{\mathbb{X}}^{F/H})$ (resp. $(\mathbb{Y}^{F/H}, \iota_{\mathbb{Y}}^{F/H}, \lambda_{\mathbb{Y}}^{F/H})$) be the framing object of $\mathcal{N}_{(1,n-1)}^{F/H}$ (resp. $\mathcal{N}_{(0,1)}^{F/H}$). Define the space of special homomorphisms to be the F-vector space

$$\mathbb{V}^{F/H} := \mathrm{Hom}_{\mathcal{O}_F}(\mathbb{Y}^{F/H}, \mathbb{X}^{F/H}) \otimes_{\mathbb{Z}} \mathbb{Q} \tag{3-3}$$

Define a Hermitian form $h^{F/H}(\cdot\,,\cdot)$ on $\mathbb{V}^{F/H}$ such that for any $x, y \in \mathbb{V}^{F/H}$ we have

$$h^{F/H}(x, y) = (\lambda_{\mathbb{Y}}^{F/H})^{-1} \circ y^\vee \circ \lambda_{\mathbb{X}}^{F/H} \circ x \in \mathrm{End}_{\mathcal{O}_F}(\mathbb{Y}^{F/H}) \otimes \mathbb{Q} \xrightarrow[\sim]{(\iota_{\mathbb{Y}}^{F/H})^{-1}} F \tag{3-4}$$

as in [Kudla and Rapoport 2011, (3.1)] where $y^\vee$ is the dual quasiisogeny of y.

Definition 3.4. For an $\mathcal{O}_F$-lattice $\boldsymbol{L} \subset \mathbb{V}^{F/H}$, the special cycle $\mathcal{Z}(\boldsymbol{L})$ is the subfunctor of $\mathcal{N}_{(0,1)}^{F/H} \times_{\mathrm{Spf}\,\mathcal{O}_{\breve{F}}} \mathcal{N}_{(1,n-1)}^{F/H}$ whose S-points is the set of isomorphism classes of tuples

$$\xi = (Y, \iota, \lambda_Y, \varrho_Y, X, \iota, \lambda_X, \varrho_X) \in \mathcal{N}_{(0,1)}^{F/H} \times_{\mathrm{Spf}\,\mathcal{O}_{\breve{F}}} \mathcal{N}_{(1,n-1)}^{F/H}(S)$$

such that for any $\boldsymbol{x} \in \boldsymbol{L}$ the quasihomomorphism

$$\varrho_X^{-1} \circ \boldsymbol{x} \circ \varrho_Y : Y \times_S \bar{S} \to X \times_S \bar{S}$$

deforms to a homomorphism from Y to X. If $\boldsymbol{L}$ is spanned by $\boldsymbol{x} \in \mathbb{V}^m$, we also denote $\mathcal{Z}(\boldsymbol{L})$ by $\mathcal{Z}(\boldsymbol{x})$.

By Grothendieck–Messing theory, $\mathcal{Z}(\boldsymbol{L})$ is a closed subformal scheme in $\mathcal{N}_{(0,1)}^{F/H} \times_{\mathrm{Spf}\,\mathcal{O}_{\breve{F}}} \mathcal{N}_{(1,n-1)}^{F/H}$.

Proposition 3.5. *Keep the same assumption as Theorem 2.10. The functor $\mathcal{C}_{\bar{k}}$ in Theorem 2.6 induces an isomorphism (denoted by the same notation) $\mathcal{C}_{\bar{k}} : \mathbb{V}^{F/H} \to \mathbb{V}^{F/F_0}$ of Hermitian vector spaces over F. Moreover for lattice $\boldsymbol{L} \in \mathbb{V}^{F/H}$, the functor $\mathfrak{C}$ in Theorem 2.10 induces an isomorphism of formal schemes*:

$$\mathcal{Z}(\boldsymbol{L}) \to \mathcal{Z}(\mathcal{C}_{\bar{k}}(\boldsymbol{L})).$$

Proof. This follows directly from Theorem 2.6. One can compare our result with [Mihatsch 2022, Remark 4.4]. □

3C. *Special cycles on relative Rapoport–Zink spaces.* By Proposition 3.5, we can without loss of generality assume that $H = F_0$. In this case we drop the superscript ${}^{F/F_0}$ over $\mathbb{X}$, $\mathbb{Y}$, $\mathbb{V}$ and h etc. For $x, y \in \mathbb{V}$ we abuse notation and denote the induced map between the corresponding relative Dieudonné modules still by x, y. As in Section 2D, we denote $\mathcal{N}_{(1,n-1)}$ simply by $\mathcal{N}$.

Lemma 3.6. *We have*

$$h(x, y)(e_1, e_1)_{\mathbb{Y}} = (x(e_1), y(e_1))_{\mathbb{X}}$$

where e_1 is as in Remark 2.13 and $(\cdot\,,\cdot)_{\mathbb{X}}$, $(\cdot\,,\cdot)_{\mathbb{Y}}$ are defined as in (2-7) for the rational relative Dieudonné module of $\mathbb{X}$ and $\mathbb{Y}$ respectively.

Proof. We claim that $\lambda_{\mathbb{Y}}^{-1} \circ y^{\vee} \circ \lambda_{\mathbb{X}}$ agrees with y^* which is the adjoint operator of y on $\mathrm{Hom}_{\mathbb{E}}(M(\mathbb{Y}) \otimes \mathbb{Q}, M(\mathbb{X}) \otimes \mathbb{Q})$ with respect to $\langle\cdot\,,\cdot\rangle_{\mathbb{X}}$ and $\langle\cdot\,,\cdot\rangle_{\mathbb{Y}}$. In fact $\langle\cdot\,,\cdot\rangle_{\mathbb{X}}$ is defined by $e\langle\cdot\,, \lambda_{\mathbb{X}} \circ \cdot\rangle_{\mathbb{X}}$ where $e\langle\cdot\,,\cdot\rangle_{\mathbb{X}}$ is the pairing between $M(\mathbb{X}) \otimes \mathbb{Q}$ and $M(\mathbb{X}^{\vee}) \otimes \mathbb{Q}$, similarly for $\langle\cdot\,,\cdot\rangle_{\mathbb{Y}}$. Hence

$$\langle y(n), m\rangle_{\mathbb{X}} = e\langle y(n), \lambda_{\mathbb{X}}(m)\rangle_{\mathbb{X}} = e\langle n, y^{\vee}\lambda_{\mathbb{X}}(m)\rangle_{\mathbb{Y}} = \langle n, \lambda_{\mathbb{Y}}^{-1} y^{\vee}\lambda_{\mathbb{X}}(m)\rangle_{\mathbb{Y}},$$

for all $n \in M(\mathbb{Y}) \otimes \mathbb{Q}$ and $m \in M(\mathbb{X}) \otimes \mathbb{Q}$. This proves the claim. Hence

$$\begin{aligned}
(x(e_1), y(e_1))_{\mathbb{X}} &= \langle \pi x(e_1), y(e_1)\rangle_{\mathbb{X}} + \pi\langle x(e_1), y(e_1)\rangle_{\mathbb{X}} \\
&= \langle y^*\pi x(e_1), e_1\rangle_{\mathbb{Y}} + \pi\langle y^* x(e_1), e_1\rangle_{\mathbb{Y}} \\
&= \langle \pi y^* x(e_1), e_1\rangle_{\mathbb{Y}} + \pi\langle y^* x(e_1), e_1\rangle_{\mathbb{Y}} \\
&= \langle \pi h(x, y)e_1, e_1\rangle_{\mathbb{Y}} + \pi\langle h(x, y)e_1, e_1\rangle_{\mathbb{Y}} \\
&= h(x, y)(e_1, e_1)_{\mathbb{Y}}.
\end{aligned}$$

This proves the lemma. □

Now assume $\boldsymbol{L} \subset \mathbb{V}$ is an $\mathcal{O}_F$-lattice and define

$$L = \{\boldsymbol{x}(e_1) \mid \boldsymbol{x} \in \boldsymbol{L}\}. \tag{3-5}$$

Then L is an $\mathcal{O}_F$-lattice in C with the same rank as $\boldsymbol{L}$ and is similar to $\boldsymbol{L}$ as a Hermitian lattice by Lemma 3.6.

Definition 3.7. Define $\mathrm{Vert}(L)$ to be the set of vertex lattices Λ such that $L \subseteq \Lambda^{\sharp}$. We also define

$$\mathcal{W}(L) := \{M \in \mathcal{V} \mid L \subseteq M\} \subset \mathcal{V} = \mathcal{N}(\bar{\boldsymbol{k}}). \tag{3-6}$$

Proposition 3.8. *For an $\mathcal{O}_F$-lattice $\boldsymbol{L} \subset \mathbb{V}$, define L as in (3-5). The set of $\bar{\boldsymbol{k}}$ points of the special cycle $\mathcal{Z}(\boldsymbol{L})$ is $\mathcal{W}(L)$. Moreover we have*

$$\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}} = \bigcup_{\Lambda \in \mathrm{Vert}(L)} \mathcal{N}_{\Lambda}. \tag{3-7}$$

Proof. Assume that $(X, \iota, \lambda, \varrho)$ is a point in $\mathcal{N}(\bar{\boldsymbol{k}})$ and $M := \varrho(M(X)) \in \mathcal{V}$ as in Proposition 2.15. By Dieudonné theory, for any $\boldsymbol{x} \in \boldsymbol{L}$, $\varrho^{-1} \circ \boldsymbol{x}$ is a homomorphism from $\mathbb{Y}$ to X if and only if $\varrho^{-1} \circ \boldsymbol{x}(M(\mathbb{Y})) \subseteq M(X)$, if and only if $\boldsymbol{x}(M(\mathbb{Y})) \subseteq M$. We know that $M(\mathbb{Y}) = \mathrm{span}_{\mathcal{O}_{\breve{F}}}\{e_1\}$. Hence the set of $\bar{\boldsymbol{k}}$ points of the special cycle $\mathcal{Z}(\boldsymbol{L})$ is $\mathcal{W}(L)$.

To prove (3-7), since both sides of the equation are reduced, it suffices to check it on the $\bar{\boldsymbol{k}}$-points, namely,

$$\mathcal{W}(L) = \bigcup_{\Lambda \in \mathrm{Vert}(L)} \mathcal{V}(\Lambda).$$

Let $M \in \mathcal{V}$ and suppose $\Lambda = \Lambda(M)$ as in Lemma 2.16. Then

$$\begin{aligned} L \subseteq M &\Leftrightarrow M \subseteq (L_C^\sharp) \otimes_{\mathcal{O}_F} \mathcal{O}_{\breve{F}} && \text{as } M = M^\sharp (\text{recall (3-2)}), \\ &\Leftrightarrow \Lambda \subseteq (L_C^\sharp) \otimes_{\mathcal{O}_F} \mathcal{O}_{\breve{F}} && \text{as } L^\sharp \text{ is } \tau\text{-invariant}, \\ &\Leftrightarrow L \subseteq \Lambda^\sharp && \text{by Lemma 3.2.} \end{aligned}$$

This in fact shows that

$$M \in \mathcal{W}(L) \Leftrightarrow \mathcal{V}^o(\Lambda) \subseteq \mathcal{W}(L).$$

Hence

$$\mathcal{W}(L) = \bigcup_{\Lambda \in \mathrm{Vert}(L)} \mathcal{V}^o(\Lambda) = \bigcup_{\Lambda \in \mathrm{Vert}(L)} \mathcal{V}(\Lambda)$$

where the last equality follows from (i) and (ii) of Theorem 2.17. This finishes the proof of the proposition. □

Corollary 3.8.1. *If $\mathcal{Z}(\boldsymbol{L})(\bar{\boldsymbol{k}})$ is nonempty, then $\boldsymbol{L}$ is integral, i.e., $h(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{O}_F$ for any $\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{L}$.*

Proof. By Proposition 3.8, there exists an $M \in \mathcal{V}$ such that $L \subseteq M$. By Lemma 3.6, we have

$$h(\boldsymbol{x}, \boldsymbol{y}) = \frac{(\boldsymbol{x}(e_1), \boldsymbol{y}(e_1))_{\mathbb{X}}}{(e_1, e_1)_{\mathbb{Y}}}.$$

Since $M = M^\sharp$, we know $(\boldsymbol{x}(e_1), \boldsymbol{y}(e_1))_{\mathbb{X}} \in (M, M)_{\mathbb{X}} = \mathcal{O}_{\breve{F}}$. Also notice that $(e_1, e_1)_{\mathbb{Y}} \in \mathcal{O}_{F_0}^\times$ by construction. The lemma follows. □

From now on we assume that L (or $\boldsymbol{L}$ equivalently) has rank n. Take a Jordan decomposition of $\boldsymbol{L}$ as in (3-1). By Corollary 3.8.1, $\lambda \geq 0$ for all λ such that $L_\lambda \neq \{0\}$. We define

$$\boldsymbol{L}_{\geq t} = \oplus_{\lambda \geq t} \boldsymbol{L}_\lambda, \tag{3-8}$$

and

$$m(\boldsymbol{L}) = \mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_{\geq 1}). \tag{3-9}$$

Also define

$$n_{\mathrm{odd}} = \sum_{\lambda \geq 3, \lambda \text{ is odd}} \mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_\lambda) \quad \text{and} \quad n_{\mathrm{even}} = \sum_{\lambda \geq 2, \lambda \text{ is even}} \mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_\lambda). \tag{3-10}$$

We say a Hermitian F-vector space V of even dimension is split if it is isomorphic to sum of copies of $H(0)\otimes_{\mathbb{Z}}\mathbb{Q}$. Equivalent it is split if and only if $(-1)^{n(n-1)/2}\det(V)\in \mathrm{Nm}_{F/F_0}F^\times$ where n is the dimension of V. The following theorem is the analog of [Kudla and Rapoport 2011, Theorem 4.2].

Theorem 3.9. *Assume that $\boldsymbol{L}\subset\mathbb{V}$ has rank n and is integral. Define L as in (3-5). Then*

$$\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}=\bigcup_{\{\Lambda\in\mathrm{Vert}(L)\mid t(\Lambda)=\mathfrak{d}(\boldsymbol{L})\}}\mathcal{N}_\Lambda$$

where

$$\mathfrak{d}(\boldsymbol{L}):=\begin{cases} m(\boldsymbol{L})-1 & \text{if } m(\boldsymbol{L}) \text{ is odd},\\ m(\boldsymbol{L}) & \text{if } m(\boldsymbol{L}) \text{ is even and } \boldsymbol{L}_{\geq 1}\otimes_{\mathbb{Z}}\mathbb{Q} \text{ is split},\\ m(\boldsymbol{L})-2 & \text{if } m(\boldsymbol{L}) \text{ is even and } \boldsymbol{L}_{\geq 1}\otimes_{\mathbb{Z}}\mathbb{Q} \text{ is nonsplit}.\end{cases}$$

We postpone the proof of Theorems 3.9 and 3.10 below to the Sections 3D and 3E respectively.

Corollary 3.9.1. *If it is nonempty, $\mathcal{Z}(\boldsymbol{L})$ is a variety of pure dimension $\frac{1}{2}\mathfrak{d}(\boldsymbol{L})$.*

Proof. The corollary follows from Theorems 3.9 and 2.17. □

The following theorem is the analog of [Kudla and Rapoport 2011, Theorem 4.5].

Theorem 3.10. *Make the same assumption as Theorem 3.9. $\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}=\mathcal{N}_\Lambda$ for a unique vertex lattice Λ if and only if the following two conditions are satisfied simultaneously*:

(1) $n_{\mathrm{odd}}=0$.

(2) $n_{\mathrm{even}}\leq 1$ *or* $n_{\mathrm{even}}=2$ *and* $\boldsymbol{L}_{\geq 2}\otimes_{\mathbb{Z}}\mathbb{Q}$ *is nonsplit.*

Corollary 3.10.1. *$\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}$ is an irreducible variety if and only if condition* (1) *and* (2) *in Theorem 3.10 are satisfied.*

Proof. By Proposition 3.8 and Theorem 2.17, $\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}$ is an irreducible variety if and only if $\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}=\mathcal{N}_\Lambda$ for a unique vertex lattice Λ. The corollary now follows from Theorem 3.10. □

Corollary 3.10.2. *The variety $\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}$ is zero dimensional if and only if the following conditions are satisfied*:

(1) $n_{\mathrm{odd}}=0$.

(2) $\mathrm{rank}_{\mathcal{O}_F}(\boldsymbol{L}_1)=0$.

(3) $n_{\mathrm{even}}\leq 1$ *or* $n_{\mathrm{even}}=2$ *and* $\boldsymbol{L}_{\geq 2}\otimes_{\mathbb{Z}}\mathbb{Q}$ *is nonsplit.*

If this is the case, then $\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}$ is in fact a single point.

Proof. The first statement of the corollary follows from Theorem 3.9 directly. If this is the case, then $\mathcal{Z}(\boldsymbol{L})_{\mathrm{red}}$ is a single point by Theorem 3.10. □

We now proceed to prove Theorems 3.9 and 3.10. Define L as in (3-5). Then we can replace all conditions on $\boldsymbol{L}$ in Theorems 3.9 and 3.10 by the same conditions on L. Moreover $\mathfrak{d}(L)=\mathfrak{d}(\boldsymbol{L})$.

3D. ***Proof of Theorem 3.9.*** It suffices to show the corresponding statements on $\bar{k}$-points, namely,

$$\mathcal{W}(L) = \bigcup_{\{\Lambda \in \mathrm{Vert}(L) | t(\Lambda) = \partial(L)\}} \mathcal{V}(\Lambda).$$

For $\boldsymbol{x} \in \mathbb{V}^n$, fix a Jordan splitting of L as in (3-1). We then have

$$L = L_0 \oplus L_{\geq 1}, \quad L^\sharp = L_0 \oplus (L_{\geq 1})^\sharp.$$

For any $\Lambda \in \mathrm{Vert}(L)$, by Proposition 3.8 we have

$$L \subseteq \Lambda^\sharp \subseteq \Lambda \subseteq L^\sharp. \tag{3-11}$$

If $L_0 \neq \{0\}$ then $s\Lambda = s\Lambda^\sharp = sL = 0$. By Lemma 3.3 we can assume

$$\Lambda = L_0 \oplus \Lambda'.$$

Then $\Lambda^\sharp = L_0 \oplus (\Lambda')^\sharp$ and we have the sequence

$$L_{\geq 1} \subseteq (\Lambda')^\sharp \subseteq \Lambda' \subseteq (L_{\geq 1})^\sharp.$$

As the map $\Lambda \mapsto \Lambda'$ above is a bijection and $\partial(L) = \partial(L_{\geq 1})$, in order to prove Theorem 3.9 we can without loss of generality assume

$$L_0 = 0 \quad \text{or equivalently} \quad \frac{1}{\pi} L \subseteq L^\sharp \tag{3-12}$$

in the rest of the subsection. Define

$$m := m(L) = \mathrm{rank}_{\mathcal{O}_F}(L_{\geq 1}),$$

which is the same as $\mathrm{rank}_{\mathcal{O}_F}(L)$ by assumption (3-12). In the rest of the section we simply write $\mathrm{rank}(\Lambda)$ instead of $\mathrm{rank}_{\mathcal{O}_F}(\Lambda)$ for an $\mathcal{O}_F$-lattice Λ.

The fact that $\partial(L)$ can be no bigger than the bounds stated in Theorem 3.9 is a restatement of [Rapoport et al. 2014, Lemma 3.3]. Our goal is to prove that it can achieve that number. To be more precise, we prove that if $\Lambda \in \mathrm{Vert}(L)$ and $t(\Lambda) < \partial(L)$, then there is a $\Lambda' \in \mathrm{Vert}(L)$ such that $\Lambda \subset \Lambda'$ (hence $\mathcal{V}(\Lambda) \subset \mathcal{V}(\Lambda')$) and $t(\Lambda') = \partial(L)$.

From now on assume $\Lambda \in \mathrm{Vert}(L)$, namely (3-11) holds. Let $t = t(\Lambda)$, then $\pi\Lambda \subset^{m-t} \Lambda^\sharp \subset^t \Lambda$. Define

$$r := \dim_k \Big(\Big(\frac{1}{\pi} \Lambda^\sharp \cap L^\sharp \Big) / \Lambda \Big).$$

Since $\Lambda^\sharp / \big(\frac{1}{\pi}\Lambda^\sharp \cap L^\sharp\big)^\sharp = \Lambda^\sharp/(\pi\Lambda + L)$, we have the following chain of inclusions

$$\pi\Lambda + L \subset^r \Lambda^\sharp \subset^t \Lambda \subset^r \frac{1}{\pi}\Lambda^\sharp \cap L^\sharp. \tag{3-13}$$

Our assumption $L = L_{\geq 1}$ implies that $L \subseteq \pi L^\sharp$. This together with (3-11) and (3-13) implies that

$$\pi\Lambda + L \subseteq \pi\Big(\frac{1}{\pi}\Lambda^\sharp \cap L^\sharp\Big) = \Lambda^\sharp \cap \pi L^\sharp. \tag{3-14}$$

Hence
$$\dim_{\boldsymbol{k}}\Big(\Big(\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp\Big)/(\pi\Lambda+L)\Big)\geq \dim_{\boldsymbol{k}}\Big(\Big(\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp\Big)/\pi\Big(\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp\Big)\Big)=m.$$
Notice that the first quotient in the above inequality is indeed a $\boldsymbol{k}$ vector space. Combine the above inequality with (3-13), we have
$$2r+t\geq m. \tag{3-15}$$

Define a $\boldsymbol{k}$-valued symmetric form $S(\cdot\,,\cdot)$ on the $\boldsymbol{k}$-vector space $\frac{1}{\pi}\Lambda^\sharp/\Lambda$ by
$$S(x,y):=\delta\pi_0\langle\pi x,y\rangle.$$

Lemma 3.11. *Suppose Λ is a vertex lattice in $\mathrm{Vert}(L)$ such that $\dim_{\boldsymbol{k}}\big(\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp/\Lambda\big)\geq 3$, then there exists a lattice $\Lambda'\in\mathrm{Vert}(L)$ with $\Lambda\subset\Lambda'$ and $t(\Lambda')>t(\Lambda)$.*

Proof. Recall that every quadratic form on a $\boldsymbol{k}$-vector ($\boldsymbol{k}$ is finite) space with dimension bigger or equal to three has an isotropic line by the Chevalley–Warning theorem. Take an isotropic line ℓ in $\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp/\Lambda$. Let $\Lambda'=:\mathrm{pr}^{-1}(\ell)$ where pr is the natural projection $\frac{1}{\pi}\Lambda^\sharp\to\frac{1}{\pi}\Lambda^\sharp/\Lambda$. The fact that ℓ is isotropic just means
$$\delta\pi_0\langle\pi\Lambda',\Lambda'\rangle\subseteq\pi_0\mathcal{O}_{F_0}.$$
This shows that $\pi\Lambda'\subseteq(\Lambda')^\sharp$. Since $\Lambda\subset^1\Lambda'$ we have
$$(\Lambda')^\sharp\subset^1\Lambda^\sharp\subseteq\Lambda\subset^1\Lambda'.$$
So Λ' is a vertex lattice and $t(\Lambda')=t(\Lambda)+2$. Since $\Lambda\subseteq L^\sharp$, by the definition of Λ', we also have $\Lambda'\subseteq L^\sharp$. In other words, $\Lambda'\in\mathrm{Vert}(L)$. The lemma is proved. $\square$

By induction using the above lemma and the fact that $\mathcal{V}(\Lambda)\subset\mathcal{V}(\Lambda')$ if $\Lambda\subset\Lambda'$ [Rapoport et al. 2014, Proposition 4.3], we reduce to the case when $r=\dim_{\boldsymbol{k}}\big(\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp/\Lambda\big)\leq 2$. Also keep in mind that (3-15) holds. There are at most four cases when $r\leq 2$ and $t(\Lambda)$ is smaller than the claimed $\mathfrak{d}(L)$ in Theorem 3.9:

(1) m is even, $t(\Lambda)=m-2$, $r=2$.

(2) m is even, $t(\Lambda)=m-2$, $r=1$.

(3) m is even, $t(\Lambda)=m-4$, $r=2$.

(4) m is odd, $t(\Lambda)=m-3$, $r=2$.

We will show that Λ can be enlarged to Λ' so that $t(\Lambda')=\mathfrak{d}(L)$ case by case.

Case (1): We have
$$\Lambda^\sharp\subset^{m-2}\Lambda\subset^2\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp\subseteq\frac{1}{\pi}\Lambda^\sharp.$$
Since $\Lambda^\sharp\subset^m\frac{1}{\pi}\Lambda^\sharp$, we actually have $\frac{1}{\pi}\Lambda^\sharp\subseteq L^\sharp$. Choose a Jordan splitting of Λ
$$\Lambda=\Lambda_0\oplus\Lambda_{-1}.$$

Then we know $\mathrm{rank}(\Lambda_0)=2$, $\Lambda_0^\sharp=\Lambda_0$, $\mathrm{rank}(\Lambda_{-1})=m-2$ and $\pi\Lambda_{-1}=\Lambda_{-1}^\sharp$. By Proposition 3.1, $\Lambda_{-1}\otimes_{\mathbb{Z}}\mathbb{Q}$ is split. If $\Lambda_0\otimes_{\mathbb{Z}}\mathbb{Q}$ is split, then there exist $e_1,e_2\in\Lambda_0$ such that $(e_1,e_1)=(e_2,e_2)=0$, $(e_1,e_2)=1$. Define

$$\Lambda'=\Lambda_{-1}\obot\mathrm{span}\{e_1,\pi^{-1}e_2\}.$$

By definition $\Lambda'\subset\frac{1}{\pi}\Lambda^\sharp$. By the fact that $\frac{1}{\pi}\Lambda^\sharp\subseteq L^\sharp$, we know that $\Lambda'\subseteq L^\sharp$. Also

$$(\Lambda')^\sharp=\Lambda_{-1}^\sharp\obot\mathrm{span}\{\pi e_1,e_2\}.$$

So $t(\Lambda')=m$. Hence $t(\Lambda')=\mathfrak{d}(L)$ as stated in Theorem 3.9. If $\Lambda_0\otimes_{\mathbb{Z}}\mathbb{Q}$ is nonsplit, then $t(\Lambda)=m-2$ already obtains the number $\mathfrak{d}(L)$ as stated in Theorem 3.9.

Case (2): We have

$$\pi\Lambda+L\subset^1\Lambda^\sharp\subset^{m-2}\Lambda\subset^1\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp\quad\text{and}\quad\pi\Big(\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp\Big)\subset^m\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp.$$

We have already seen in (3-14) that

$$\pi\Lambda+L\subseteq\pi\Big(\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp\Big)=\Lambda^\sharp\cap\pi L^\sharp.$$

These together imply that in fact $\pi\Lambda+L=\Lambda^\sharp\cap\pi L^\sharp$. But

$$\pi\Lambda+L=\Big(\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp\Big)^\sharp.$$

So define $\Lambda'=\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp$, we have $t(\Lambda')=m$. This implies that $\Lambda'\otimes_{\mathbb{Z}}\mathbb{Q}$ is split and $t(\Lambda')=\mathfrak{d}(L)$.

Case (3): Similar to case (2).

Case (4): We have

$$\Lambda^\sharp\subset^{m-3}\Lambda\subset^2\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp\subset^1\frac{1}{\pi}\Lambda^\sharp.$$

Choose a Jordan splitting of Λ

$$\Lambda=\Lambda_0\obot\Lambda_{-1}.$$

Then we know $\mathrm{rank}(\Lambda_0)=3$, $\Lambda_0^\sharp=\Lambda_0$, $\mathrm{rank}(\Lambda_{-1})=m-3$, $\Lambda_{-1}=\frac{1}{\pi}\Lambda_{-1}^\sharp$. By assumption there is a basis $\{e_1,e_2,e_3\}$ of Λ_0 such that

$$\frac{1}{\pi}e_1,\quad\frac{1}{\pi}e_2\in\frac{1}{\pi}\Lambda^\sharp\cap L^\sharp,\quad\frac{1}{\pi}e_3\notin L^\sharp.$$

By changing $\{e_1,e_2\}$ by an $\mathcal{O}_F$ linear combination of them, we can assume $(e_i,e_i)=u_i$ $(i=1,2)$ for $u_i\in\mathcal{O}_{F_0}^\times$ and $(e_1,e_2)=0$. By modifying e_3 using linear combinations of e_1,e_2 we can in fact assume that under the basis $\{e_1,e_2,e_3\}$, the form $(\cdot,\cdot)|_{\Lambda_0}$ is represented by the diagonal matrix $\mathrm{diag}\{u_1,u_2,u_3\}$ with $u_1,u_2,u_3\in\mathcal{O}_{F_0}^\times$. This means that

$$(e_3,L^\sharp)=(e_3,e_3)\mathcal{O}_F=\mathcal{O}_F\Rightarrow e_3\in L.$$

But $\frac{1}{\pi}e_3 \notin L^\sharp$, these together contradict our assumption (3-12). In conclusion, case (4) is not possible under the assumption (3-12).

This finishes the proof of Theorem 3.9. $\square$

3E. *Proof of Theorem 3.10.* Again it suffices to show the corresponding statements on $\bar{k}$-points. By Theorem 3.9, $\mathcal{W}(L) = \mathcal{V}(\Lambda)$ is true if and only if Λ is the unique lattice in $\mathrm{Vert}(L)$ with $t(\Lambda) = \mathfrak{d}(L)$. As in the proof of Theorem 3.9, we can assume (3-12).

Lemma 3.12. *Assume that one of the following conditions holds*:

(1) $n_{\mathrm{even}} \geq 3$ *or* $n_{\mathrm{even}} = 2$ *with* $L_{\geq 2} \otimes \mathbb{Q}$ *split.*

(2) $n_{\mathrm{odd}} \geq 2$.

Then there is more than one Λ *in Vert*(L) *such that* $t(\Lambda) = \mathfrak{d}(L)$.

Proof. Fix a Jordan splitting of L as in (3-1). If $n_{\mathrm{odd}} \geq 2$ by Proposition 3.1, we can find a direct summand $H(i), i \geq 2$ of L. If $n_{\mathrm{even}} \geq 3$, scale the sub-$\mathcal{O}_F$-module $L_{\geq 2}$ to be π^2-modular to get a new lattice $L' \supseteq L$ such that L'_2 has rank bigger or equal to 3. Notice that $\mathfrak{d}(L') = \mathfrak{d}(L)$. O'Meara [2000, Proposition 63:19] showed that every quadratic space over a local field with dimension greater or equal to 5 is isotropic. We apply this to the trace form of $(\cdot\,,\cdot)|_{L'_2}$ and conclude that there is a maximal element in L'_2 that has length zero. Hence there is an $H(i), i \geq 2$ which is a direct summand of L'_2. Similarly if $n_{\mathrm{even}} = 2$ and $L_{\geq 2} \otimes \mathbb{Q}$ is split, we can find a lattice $L' \supseteq L$ such that $\mathfrak{d}(L) = \mathfrak{d}(L')$ and a direct summand $H(i)$ $(i \geq 2)$ of L'. In any case we can find a lattice $L' \supseteq L$ such that $\mathfrak{d}(L) = \mathfrak{d}(L')$ and

$$L' = L'' \obot H(a),$$

with $a \geq 2$. In particular $\mathrm{Vert}(L') \subseteq \mathrm{Vert}(L)$.

Notice that $\mathfrak{d}(L') = \mathfrak{d}(L'') + 2$. By Theorem 3.9, there is a vertex lattice $\Lambda \in \mathrm{Vert}(L'')$ such that $t(\Lambda) = \mathfrak{d}(L'')$. Let $\{e_1, e_2\}$ be a basis of $H(a)$ such that $(e_1, e_1) = (e_2, e_2) = 0$ and $(e_1, e_2) = \pi^a$. Define

$$\Lambda_1 := \Lambda \obot \mathrm{span}\{\pi^{-a}e_1, \pi^{-1}e_2\}, \quad \Lambda_2 := \Lambda \obot \mathrm{span}\{\pi^{-a}e_2, \pi^{-1}e_1\}.$$

Then

$$\Lambda_1^\sharp = \Lambda^\sharp \obot \mathrm{span}\{\pi^{-a+1}e_1, e_2\}, \quad \Lambda_2^\sharp = \Lambda^\sharp \obot \mathrm{span}\{\pi^{-a+1}e_2, e_1\}.$$

This shows that $t(\Lambda_1) = t(\Lambda_2) = \mathfrak{d}(L)$ and $\Lambda_1, \Lambda_2 \in \mathrm{Vert}(L')$, but $\Lambda_1 \neq \Lambda_2$. This proves the lemma. $\square$

This proves the "only if" part of Theorem 3.10. To prove the converse, we start with a lemma.

Lemma 3.13. *Suppose* $L = L_0 \obot L_1 \obot L_{\geq 1}$*(Jordan splitting). If* Λ *is a vertex lattice in* $\mathrm{Vert}(L)$ *such that* $t(\Lambda) = \mathfrak{d}(L)$, *then* $L_0 \obot L_1^\sharp \subset \Lambda$.

Proof. Suppose $L_0 \obot L_1^\sharp \not\subset \Lambda$. Let $\Lambda' := \Lambda + L_0 \obot L_1^\sharp$. We have $L_0^\sharp = L_0$ and $\pi L_1^\sharp = L_1$. Then $L^\sharp = L_0 \obot \frac{1}{\pi} L_1 \obot L_{\geq 1}^\sharp$ and

$$(\Lambda')^\sharp = \Lambda^\sharp \cap (L_0 \obot L_1 \obot (L_{\geq 1} \otimes \mathbb{Q})).$$

Using the above equation and the fact that $\Lambda \in \mathrm{Vert}(L)$, one checks immediately that $\pi\Lambda' \subseteq (\Lambda')^\sharp$. Since $\Lambda \subset \Lambda'$ and $\Lambda^\sharp \subseteq \Lambda$, we have $(\Lambda')^\sharp \subseteq \Lambda'$. Also $\Lambda' \subseteq L^\sharp$, so $\Lambda' \in \mathrm{Vert}(L)$. But $t(\Lambda') > t(\Lambda)$, which contradicts the maximality of $t(\Lambda)$ among vertex lattices in $\mathrm{Vert}(L)$. $\square$

Now we assume conditions (1) and (2) of Theorem 3.10 hold. By Proposition 3.1, we have the following three cases:

(1) $L \simeq L_0 \obot H(1)^\ell$.

(2) $L \simeq L_0 \obot H(1)^\ell \obot (u(-\pi_0)^a)$ with $a \geq 1$ and $u \in \mathcal{O}_{F_0}^\times$.

(3) $L \simeq L_0 \obot H(1)^\ell \obot (u_1(-\pi_0)^a) \obot (u_2(-\pi_0)^b)$, where $u_1, u_2 \in \mathcal{O}_{F_0}^\times$, $-u_1u_2 \notin \mathrm{Nm}_{F/F_0}(F/F_0)$ and a, b are integers greater or equal to 1.

We need to prove that in each case there is a unique $\Lambda \in \mathrm{Vert}(L)$ such that $t(\Lambda) = \mathfrak{d}(L)$. Cases (1) follows from Lemma 3.13 directly (in this case Λ has to be $L_0 \obot H(1)^\ell$). Case (2) follows from Lemma 3.13 and simple arguments. Now we prove (3). By Lemmas 3.13 and 3.3, it suffices to prove the statement for $L = (u_1(-\pi_0)^a) \obot (u_2(-\pi_0)^b)$.

Let $L = \mathrm{span}\{e_1, e_2\}$ and $T = \mathrm{diag}\{u_1(-\pi_0)^a, u_2(-\pi_0)^b\}$ is the gram matrix of $\{e_1, e_2\}$. Suppose $\Lambda = \mathrm{span}\{[e_1, e_2]S\} \in \mathrm{Vert}(L)$ where $S \in \mathrm{GL}_2(F)/\mathrm{GL}_2(\mathcal{O}_F)$. Since $L \otimes_{\mathbb{Z}} \mathbb{Q}$ is nonsplit, we must have $\Lambda^\sharp = \Lambda$. Then $\Lambda^\sharp = [e_1, e_2]T^{-1}\,{}^t\bar{S}^{-1}$ and

$$\Lambda^\sharp = \Lambda \Leftrightarrow S^{-1}T^{-1}\,{}^t\bar{S}^{-1} \in \mathrm{GL}_2(\mathcal{O}_F) \Leftrightarrow {}^t\bar{S}TS \in \mathrm{GL}_2(\mathcal{O}_F)$$
$$L \subseteq \Lambda^\sharp \Leftrightarrow {}^t\bar{S}T \in M_2(\mathcal{O}_F).$$

Apply Proposition 3.1 and multiply S on the right by an element in $\mathrm{GL}_2(\mathcal{O}_F)$ if necessary, we can assume

$${}^t\bar{S}TS = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix} =: T_1.$$

Assume

$$S = \begin{pmatrix} \pi^{-a} & 0 \\ 0 & \pi^{-b} \end{pmatrix} S_0,$$

then ${}^t\bar{S}_0 T_1 S_0 = T_1$. Claim: $S_0 \in \mathrm{GL}_2(\mathcal{O}_F)$. Assume $S_0 = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$, then ${}^t\bar{S}_0 T_1 S_0 = T_1$ implies that

$$u_1 x\bar{x} + u_2 z\bar{z} = u_1$$
$$u_1 \bar{y}x + u_2 \bar{w}z = 0$$
$$u_1 y\bar{y} + u_2 w\bar{w} = u_2.$$

If $z = 0$, then $y = 0$ and $x, w \in \mathcal{O}_F^\times$. If $x = 0$, then $w = 0$ and $y, z \in \mathcal{O}_F^\times$ as u_1, u_2 are units.

Now assume that $xz \neq 0$. Suppose $x = x_0\pi^e$ where $e < 0$, $x_0 \in \mathcal{O}_F^\times$, then

$$x\bar{x} - 1 = (-\pi_0)^e(x_0\bar{x}_0 - (-\pi_0)^{-e}).$$

Since F is ramified over F_0,

$$\mathrm{Nm}_{F/F_0}(\mathcal{O}_F^\times/\mathcal{O}_{F_0}^\times) = (\mathcal{O}_{F_0}^\times)^2$$

by class field theory. As $x_0\bar{x}_0 \in \mathrm{Nm}_{F/F_0}(\mathcal{O}_F^\times/\mathcal{O}_{F_0}^\times) = (\mathcal{O}_{F_0}^\times)^2$, by Hensel's lemma, $x_0\bar{x}_0 - (-\pi_0)^{-e} \in \mathrm{Nm}_{F/F_0}(\mathcal{O}_F^\times/\mathcal{O}_{F_0}^\times)$. Then

$$-\frac{u_2}{u_1} = \frac{x\bar{x}-1}{z\bar{z}} = \frac{(-\pi_0)^e(x_0\bar{x}_0 - (-\pi_0)^{-e})}{z\bar{z}} \in \mathrm{Nm}_{F/F_0}(\mathcal{O}_F^\times/\mathcal{O}_{F_0}^\times),$$

contradicts our assumption on $-u_1u_2$. This show that $e \geq 0$ and $x \in \mathcal{O}_F$, then $z \in \mathcal{O}_F$ too.

Similarly $u_1 y\bar{y} + u_2 w\bar{w} = u_2$ implies $y, w \in \mathcal{O}_F$ if $yw \neq 0$. This proves the claim that $S_0 \in \mathrm{GL}_2(\mathcal{O}_F)$. In other words

$$\Lambda = \mathrm{span}\{\pi^{-a}e_1, \pi^{-b}e_2\}.$$

This proves the uniqueness of Λ and we finish the proof of Theorem 3.10. □

4. Unitary Shimura varieties

In this section we briefly review the definition of an integral model of unitary Shimura variety following [Rapoport et al. 2021, Section 6]; see also [Rapoport et al. 2020; Cho 2018]. Let F be a CM field over $\mathbb{Q}$ with totally real subfield F_0 of index 2 in it. Let $d = [F_0 : \mathbb{Q}]$. We denote by $a \mapsto \bar{a}$ the nontrivial automorphism of F/F_0. Define

$$\mathscr{V}_{\mathrm{ram}} = \{\text{finite places } v \text{ of } F_0 \mid v \text{ ramifies in } F\}. \tag{4-1}$$

In this paper we assume that $\mathscr{V}_{\mathrm{ram}}$ is nonempty. We also make the assumption as in [Rapoport et al. 2021, Section 6] that every $v \in \mathscr{V}_{\mathrm{ram}}$ is unramified over $\mathbb{Q}$ and does not divide 2.

Fix a totally imaginary element $\sqrt{\Delta} \in F$. Denote by Φ_{F_0} (resp. Φ_F) the set of real (resp. complex) embeddings of F_0 (resp. F). Define a CM type of F by

$$\Phi = \{\varphi \in \Phi_F \mid \varphi(\sqrt{\Delta}) \in \sqrt{-1}\mathbb{R}_{>0}\}. \tag{4-2}$$

We fix a distinguished element $\varphi_0 \in \Phi$. For $\varphi \in \mathrm{Hom}_{\mathbb{Q}}(F, \mathbb{C})$, denote its complex conjugate by $\bar{\varphi}$.

4A. ***The Shimura datum.*** Define a function $r : \mathrm{Hom}_{\mathbb{Q}}(F, \mathbb{C}) \to \mathbb{Z}_{\geq 0}$ by

$$\varphi \mapsto r_\varphi := \begin{cases} 1 & \text{if } \varphi = \varphi_0; \\ 0 & \text{if } \varphi \in \Phi, \varphi \neq \varphi_0; \\ n - r_{\bar{\varphi}} & \text{if } \varphi \notin \Phi. \end{cases}$$

Assume that W is a n dimensional F-vector space with a Hermitian form $(\cdot\,,\cdot)$ such that

$$\mathrm{sig}\, W_\varphi = (r_\varphi, r_{\bar{\varphi}}), \quad \forall \varphi \in \Phi$$

where $W_\varphi := W \otimes_{F,\varphi} \mathbb{C}$ and $\mathrm{sig}\, W_\varphi$ is its signature with respect to $(\cdot\,,\cdot)$. Let $\mathrm{U}(W)$ (resp. $\mathrm{GU}(W)$) be the unitary group (resp. general unitary group) of $(W, (\cdot\,,\cdot))$. Recall that for an F_0-algebra R, we have

$$\mathrm{GU}(W)(R) = \{g \in \mathrm{GL}(W \otimes_{F_0} R) \mid (gv, gw) = c(g)(v, w), \forall v, w \in W \otimes_{F_0} R\}.$$

Define the following groups.

$$\begin{aligned} Z^{\mathbb{Q}} &:= \{z \in \operatorname{Res}_{F/\mathbb{Q}} \mathbb{G}_m \mid \operatorname{Nm}_{F/F_0}(z) \in \mathbb{G}_m\}, \\ G &= \operatorname{Res}_{F_0/\mathbb{Q}} \mathrm{U}(W), \\ G^{\mathbb{Q}} &:= \{g \in \operatorname{Res}_{F_0/\mathbb{Q}} \mathrm{GU}(W) \mid c(g) \in \mathbb{G}_m\}. \end{aligned} \tag{4-3}$$

Notice that

$$Z^{\mathbb{Q}}(\mathbb{R}) = \{(z_\varphi) \in (\mathbb{C}^\times)^\Phi \mid |z_\varphi| = |z_{\varphi_0}|, \forall \varphi \in \Phi\}.$$

Define the Hodge map

$$h_{Z^{\mathbb{Q}}} : \mathbb{C}^\times \to Z^{\mathbb{Q}}(\mathbb{R}), z \mapsto (\bar{z}, \dots, \bar{z}).$$

For each $\varphi \in \Phi$ choose a $\mathbb{C}$-basis of W_φ such that $(\cdot, \cdot)$ is given by the matrix $\operatorname{diag}(1_{r_\varphi}, -1_{r_{\bar{\varphi}}})$. Define the Hodge map

$$h_{\mathrm{GU}(W)} : \mathbb{C}^\times \to \operatorname{Res}_{F_0/\mathbb{Q}} \mathrm{GU}(W)(\mathbb{R}) \cong \prod_{\varphi \in \Phi} \mathrm{GU}(W_\varphi)$$

by sending z to $\operatorname{diag}(z \cdot 1_{r_\varphi}, \bar{z} \cdot 1_{r_{\bar{\varphi}}})$ for each φ component. Then there exists $h_{G^{\mathbb{Q}}} : \mathbb{C}^\times \to G^{\mathbb{Q}}(\mathbb{R})$ such that $h_{\mathrm{GU}(W)}$ factors as

$$h_{\mathrm{GU}(W)} = i \circ h_{G^{\mathbb{Q}}}$$

where $i : G^{\mathbb{Q}}(\mathbb{R}) \to \operatorname{Res}_{F_0/\mathbb{Q}} \mathrm{GU}(W)(\mathbb{R})$ is the natural inclusion.

Define

$$\tilde{G} := Z^{\mathbb{Q}} \times_{\mathbb{G}_m} G^{\mathbb{Q}}$$

where the maps from the factors on the right hand side to $\mathbb{G}_m$ are $\operatorname{Nm}_{F/F_0}$ and the similitude character $c(g)$ respectively. Notice that the map

$$\tilde{G} \to Z^{\mathbb{Q}} \times G, \quad (z, g) \mapsto (z, z^{-1} g) \tag{4-4}$$

is an isomorphism. We define the Hodge map $h_{\tilde{G}}$ by

$$h_{\tilde{G}} : \mathbb{C}^\times \to \tilde{G}(\mathbb{R}), z \mapsto (h_{Z^{\mathbb{Q}}}(z), h_{G^{\mathbb{Q}}}(z)).$$

Then $(\tilde{G}, h_{\tilde{G}})$ is a Shimura datum whose reflex field $E \subset \overline{\mathbb{Q}}$ is defined by

$$\operatorname{Aut}(\overline{\mathbb{Q}}/E) = \{\sigma \in \operatorname{Aut}(\overline{\mathbb{Q}}) \mid \sigma \circ \Phi = \Phi, \sigma^*(r) = r\}. \tag{4-5}$$

Remark 4.1. F always embeds into E via φ_0; [Rapoport et al. 2020, Remark 3.1]. Furthermore $E = F$ when F is Galois over $\mathbb{Q}$ or when $F = F_0 K$ where K is an imaginary quadratic field over $\mathbb{Q}$ and Φ is induced from a CM type of $K/\mathbb{Q}$. From now on we identify F_0 as a subfield of E via φ_0.

For a small enough compact group $K \in \tilde{G}(\mathbb{A}_f)$, we can define a Shimura variety $S(\tilde{G}, h_{\tilde{G}})_K$ which has a canonical model over the Spec E. We refer to [Rapoport et al. 2021, Section 3] for the moduli problem $S(\tilde{G}, h_{\tilde{G}})_K$ represents.

4B. ***Integral model.*** In this subsection, we define the integral model for $S(\tilde{G}, h_{\tilde{G}})_K$ (as a Deligne–Mumford stack) in terms of a moduli functor for a particular choice of W and K. We remark here that all the results in this section is semiglobal in natural so we could instead describe our results on semiglobal integral models defined as in [Rapoport et al. 2021, Section 4] which will allow a wider choices of W and K. It takes only slight modifications to adjust our results to the semiglobal setting so we leave it to the interested readers.

For a lattice Λ in W, we let $\Lambda^\vee$ denote its dual with respect to the symplectic form $\mathrm{tr}_{F/\mathbb{Q}}(\sqrt{\Delta}^{-1}(\cdot\,,\cdot))$ and $\Lambda^\sharp$ denote its dual with respect to the Hermitian form $(\cdot\,,\cdot)$. Then we have

$$\Lambda^\vee = \sqrt{\Delta}\partial^{-1}\Lambda^\sharp \tag{4-6}$$

where ∂ is the different ideal of $F/\mathbb{Q}$. From now on we assume that W contains a lattice Λ such that $\Lambda^\vee = \Lambda$. Define the compact subgroup $K_G \subset G(\mathbb{A}_f)$ by

$$K_G := \{g \in G(\mathbb{A}_f) \mid g(\Lambda \otimes \hat{\mathbb{Z}}) = \Lambda \otimes \hat{\mathbb{Z}}\}. \tag{4-7}$$

Also let $K_{Z^{\mathbb{Q}}}$ be the unique maximal compact subgroup of $Z^{\mathbb{Q}}(\mathbb{A}_f)$:

$$K_{Z^{\mathbb{Q}}} := \{z \in (\mathcal{O}_F \otimes \hat{\mathbb{Z}})^\times \mid \mathrm{Nm}_{F/F_0}(z) \in \hat{\mathbb{Z}}\}. \tag{4-8}$$

Define the compact subgroup

$$K := K_{Z^{\mathbb{Q}}} \times K_G \subset \tilde{G}(\mathbb{A}_f) \tag{4-9}$$

under the isomorphism (4-4).

First we define an auxiliary moduli functor $\mathcal{M}_0$ over $\operatorname{Spec}\mathcal{O}_E$. For a locally notherian $\mathcal{O}_E$-scheme S, we define $\mathcal{M}_0(S)$ to be the groupoid of triples $(A_0, \iota_0, \lambda_0)$ where:

(1) A_0 is an abelian scheme over S.

(2) $\iota_0 : \mathcal{O}_F \to \mathrm{End}(A_0)$ is an $\mathcal{O}_F$-action satisfying the Kottwitz condition of signature $((0,1)_{\varphi\in\Phi})$, namely

$$\mathrm{charpol}(\iota_0(a) \mid \mathrm{Lie}\, A_0) = \prod_{\varphi\in\Phi}(T - \bar{\varphi}(a)), \quad \forall a \in \mathcal{O}_F.$$

(3) λ_0 is a principal polarization of A_0 whose Rosati involution induces on $\mathcal{O}_F$ via ι_0 the nontrivial Galois automorphism of F/F_0.

A morphism between two objects $(A_0, \iota_0, \lambda_0)$ and $(A_0', \iota_0', \lambda_0')$ is a $\mathcal{O}_F$-linear isomorphism $A_0 \to A_0'$ that pulls λ_0' back to λ.

Since we assume $\mathcal{V}_{\mathrm{ram}}$ is nonempty, $\mathcal{M}_0$ is nonempty [Rapoport et al. 2021, Remark 3.7]. Then $\mathcal{M}_0$ is a Deligne–Mumford stack, finite and étale over $\operatorname{Spec}\mathcal{O}_E$ [Howard 2012, Proposition 3.1.2]. Moreover, we choose a 1 dimensional F vector space W_0 such that W_0 has an $\mathcal{O}_F$ lattice Λ_0 with a nondegenerate alternating form $\langle\cdot\,,\cdot\rangle_0$ satisfying:

(1) $\langle ax, y\rangle_0 = \langle x, \bar{a}y\rangle_0$ for all $a \in \mathcal{O}_F$ and $x, y \in \Lambda_0$.

(2) The quadratic form $x \mapsto \langle\sqrt{\Delta}x, x\rangle_0$ is negative definite.

(3) The dual lattice $\Lambda_0^\vee$ of Λ_0 with respect to $\langle\cdot\,,\cdot\rangle_0$ is Λ_0.

Let $(\cdot\,,\cdot)_0$ be the unique Hermitian form on W_0 such that $\mathrm{tr}_{F/\mathbb{Q}}(\sqrt{\Delta}^{-1}(\cdot,\cdot)_0)=\langle\cdot,\cdot\rangle_0$. Then $(W_0,(\cdot,\cdot)_0)$ determines a certain similarity class ξ of Hermitian forms which in turn give us an open and closed substack $\mathcal{M}_0^{\xi}$ of $\mathcal{M}_0$; see [Rapoport et al. 2020, Lemma 3.4]. Define the F-vector space

$$V = \mathrm{Hom}_F(W_0, W) \tag{4-10}$$

with the Hermitian form $(\cdot\,,\cdot)_V$ determined by $(\cdot\,,\cdot)$ and $(\cdot\,,\cdot)_0$ via

$$(x(a), y(b)) = (x, y)_V(a, b)_0, \forall x, y \in V, \forall a, b \in W_0. \tag{4-11}$$

The lattice

$$L := \mathrm{Hom}_{\mathcal{O}_F}(\Lambda_0, \Lambda) \subset V \tag{4-12}$$

is a self dual lattice with respect to the Hermitian form $(\cdot\,,\cdot)_V$.

We define the functor $\mathcal{M}$ on the category of locally notherian schemes over $\mathrm{Spec}\,\mathcal{O}_E$ as follows. For a scheme S in this category, $\mathcal{M}(S)$ is the groupoid of tuples $(A_0, \iota_0, \lambda_0, A, \iota, \lambda)$ where:

- $(A_0, \iota_0, \lambda_0)$ is an object of $\mathcal{M}_0^{\xi}(S)$.
- A is an abelian scheme over S.
- $\iota : \mathcal{O}_F \to \mathrm{End}(A)$ is an $\mathcal{O}_F$-action satisfying the Kottwitz condition of signature

  $$((1, n-1)_{\{\varphi_0\}}, (0, n)_{\Phi\setminus\{\varphi_0\}}),$$

  i.e., for all $a \in \mathcal{O}_F$

  $$\mathrm{charpol}(\iota(a) \mid \mathrm{Lie}\, A) = (T - \varphi_0(a))(T - \bar{\varphi}_0(a))^{n-1} \prod_{\varphi\in\Phi\setminus\{\varphi_0\}} (T - \bar{\varphi}(a))^n.$$

- $\lambda : A \to A^{\vee}$ is a principal polarization whose associated Rosati involution induces on $\mathcal{O}_F$ via ι the nontrivial Galois automorphism of F/F_0.

We assume further that the tuple $(A_0, \iota_0, \lambda_0, A, \iota, \lambda)$ satisfies the sign condition, the Wedge condition and the Eisenstein condition, all of which are defined with respect to the signature $((1, n-1)_{\{\varphi_0\}}, (0, n)_{\Phi\setminus\{\varphi_0\}})$.

(H1) The sign condition. Let s be a geometric point of S and $(A_{0,s}, \iota_{0,s}, \lambda_{0,s}, A_s, \iota_s, \lambda_s)$ be the pull back of $(A_0, \iota_0, \lambda_0, A, \iota, \lambda) \in \mathcal{M}(S)$ to s. For every nonsplit place v of F_0, we impose

$$\mathrm{inv}_v^r(A_{0,s}, \iota_{0,s}, \lambda_{0,s}, A_s, \iota_s, \lambda_s) = \mathrm{inv}_v(V). \tag{4-13}$$

We need to explain the two factors. We refer to [Rapoport et al. 2020, Appedix A] for the definition of $\mathrm{inv}_v^r(A_{0,s}, \iota_{0,s}, \lambda_{0,s}, A_s, \iota_s, \lambda_s)$. For $\mathrm{inv}_v(V)$, it is defined by

$$\mathrm{inv}_v(V) = (-1)^{n(n-1)/2} \det(V_v) \in F_{0,v}^{\times} / \mathrm{Nm}_{F_v/F_{0,v}} F_v^{\times},$$

where $\det(V_v)$ is the determinant of the Hermitian space $V_v := V \otimes_{F_0} F_{0,v}$. We call this the invariant of V at v. We remark that when s has characteristic zero, the sign condition is equivalent to the condition that there is an isometry

$$\mathrm{Hom}_{\mathbb{A}_{F,f}}(\hat{V}(A_{0,s}), \hat{V}(A_s)) \cong V \otimes_F \mathbb{A}_{F,f} \tag{4-14}$$

as Hermitian $\mathbb{A}_{F,f}$-vector spaces. Here $\hat{V}(A_s)$ (resp. $\hat{V}(A_{0,s})$) is the rational Tate module of A (resp. A_0). The space $\mathrm{Hom}_{\mathbb{A}_{F,f}}(\hat{V}(A_{0,s}), \hat{V}(A_s))$ is equipped with the Hermitian form [Kudla and Rapoport 2014, Section 2.3]

$$h(x, y) = \lambda_0^{-1} \circ y^\vee \circ \lambda \circ x \in \mathrm{End}_{\mathbb{A}_{F,f}}(\hat{V}(A_{0,s})) \cong \mathbb{A}_{F,f} \tag{4-15}$$

where $y^\vee$ is the dual of y with respect to the Weil pairings on $\hat{V}(A_{0,s}) \times \hat{V}(A_{0,s}^\vee)$ and $\hat{V}(A_s) \times \hat{V}(A_s^\vee)$. Hence the sign condition can be seen as a generalization of (4-14). See [Rapoport et al. 2021, Remark 6.9] for cases when the sign condition can be simplified.

The wedge condition and Eisenstein condition are only needed when S has nonempty special fibers in certain characteristics. We temporarily fix a finite prime p of $\mathbb{Q}$. Fix an embedding $\tilde{\nu} : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$. This determines a p-adic place ν of E. $\tilde{\nu}$ induces an identification

$$\mathrm{Hom}_{\mathbb{Q}}(F, \overline{\mathbb{Q}}) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Q}}(F, \overline{\mathbb{Q}}_p) : \varphi \mapsto \tilde{\nu} \circ \varphi.$$

Let $\mathscr{V}_p(F)$ be the set of places of F over p. For each $w \in \mathscr{V}_p(F)$, define

$$\mathrm{Hom}_w(F, \overline{\mathbb{Q}}) := \{\varphi \in \mathrm{Hom}_{\mathbb{Q}}(F, \overline{\mathbb{Q}}) \mid \tilde{\nu} \circ \varphi \text{ induces } w\}. \tag{4-16}$$

Let F_w^t be the maximal unramified extension of $\mathbb{Q}_p$ in F_w. For $\psi \in \mathrm{Hom}_{\mathbb{Q}_p}(F_w^t, \overline{\mathbb{Q}}_p)$, define

$$\mathrm{Hom}_{w,\psi}(F, \overline{\mathbb{Q}}) := \{\varphi \in \mathrm{Hom}_w(F, \overline{\mathbb{Q}}) \mid \tilde{\nu} \circ \varphi|_{F_w^t} = \psi\}. \tag{4-17}$$

The definitions of $\mathrm{Hom}_w(F, \overline{\mathbb{Q}})$ and $\mathrm{Hom}_{w,\psi}(F, \overline{\mathbb{Q}})$ depend on the choice of $\tilde{\nu}$ in general but the partition of $\mathrm{Hom}_{\mathbb{Q}}(F, \overline{\mathbb{Q}})$ into unions of $\mathrm{Hom}_{w,\psi}(F, \overline{\mathbb{Q}})$ does not [Rapoport et al. 2021, (5.4)].

We make a base change and assume that S is a scheme over $\mathrm{Spec}\, \mathcal{O}_{E,\nu}$ where $\mathcal{O}_{E,\nu}$ is the completion of $\mathcal{O}_E$ with respect to the ν-adic topology. Then the $\mathcal{O}_F$ action on A induces an action of

$$\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \prod_{w \in \mathscr{V}_p(F)} \mathcal{O}_{F,w}$$

on $\mathrm{Lie}\, A$. Hence we have a decomposition

$$\mathrm{Lie}\, A = \bigoplus_{w \in \mathscr{V}_p(F)} \mathrm{Lie}_w\, A. \tag{4-18}$$

For each w, the $\mathcal{O}_{F_w^t}$-action on $\mathrm{Lie}_w\, A$ induces a decomposition

$$\mathrm{Lie}_w\, A = \bigoplus_{\psi \in \mathrm{Hom}_{\mathbb{Q}_p}(F_w^t, \overline{\mathbb{Q}}_p)} \mathrm{Lie}_{w,\psi}\, A. \tag{4-19}$$

Here we make a further base change to $\mathrm{Spec}\, \mathcal{O}_{\breve{E}_\nu}$ where $\breve{E}_\nu$ is the completion of the maximal unramified extension of E_ν in $\overline{\mathbb{Q}}_p$:

(H2) The wedge condition. Assume that w is a finite place of F that is ramified over F_0. We further assume that the underlying place of w in $\mathbb{Q}$ is p and we make a base change so that S is a $\mathrm{Spec}\, \mathbb{Z}_p$-scheme. The wedge condition is only needed when S has nonempty special fiber over $\mathrm{Spec}\, \mathbb{F}_p$. By our assumption, the underlying place v of F_0 is unramified over $\mathbb{Q}$. Hence $F_w^t = F_{0,v}$ and $\mathrm{Hom}_{w,\psi}(F, \overline{\mathbb{Q}}) = \{\varphi_\psi, \bar{\varphi}_\psi\}$ for all $\psi \in \mathrm{Hom}_{\mathbb{Q}_p}(F_w^t, \overline{\mathbb{Q}}_p)$. For every ψ such that $r_{\varphi_\psi} \neq r_{\bar{\varphi}_\psi}$, decompose $\mathrm{Lie}\, A$ as in (4-18) and (4-19) and impose the wedge condition of [Pappas 2000] (compare with Definition 2.3)

$$\bigwedge^{r_{\bar{\varphi}_\psi}+1} (\iota(a) - \varphi_\psi(a) \mid \mathrm{Lie}_{w,\psi} A) = 0, \quad \bigwedge^{r_{\varphi_\psi}+1} (\iota(a) - \bar{\varphi}_\psi(a) \mid \mathrm{Lie}_{w,\psi} A) = 0 \tag{4-20}$$

for all $a \in \mathcal{O}_F$. Here since $r_{\varphi_\psi} \neq r_{\bar{\varphi}_\psi}$, φ_ψ maps F_w into E_ν, so we can view $\varphi_\psi(a)$ and $\bar{\varphi}_\psi(a)$ as sections in the structure sheaf of the base scheme S.

(H3) The Eisenstein condition. Assume that w is a finite place of F whose underlying place v in F_0 is ramified over $\mathbb{Q}$. By our assumption w is unramified over v. Again assume that the underlying place of w in $\mathbb{Q}$ is p and we make a base change so that S is a $\mathrm{Spec}\, \mathbb{Z}_p$-scheme. Decompose $\mathrm{Lie}\, A$ as in (4-18) and (4-19). The Eisenstein condition is a set of conditions on $\mathrm{Lie}_{w,\psi} A$ and is only needed when S has nonempty special fiber over $\mathrm{Spec}\, \mathbb{F}_p$. We do not describe the condition in detail but instead refer to [Rapoport et al. 2021, Section 5.2, case (1) and (2)].

Finally a morphism between two objects $(A_0, \iota_0, \lambda_0, A, \iota, \lambda)$ and $(A_0', \iota_0', \lambda_0', A', \iota', \lambda')$ is a morphism $(A_0, \iota_0, \lambda_0) \to (A_0', \iota_0', \lambda_0')$ in $\mathcal{M}_0^\xi(S)$ together with an $\mathcal{O}_F$-linear isomorphism $(A, \iota, \lambda) \to (A', \iota', \lambda')$ that pulls λ' back to λ.

The following Proposition is a partial summarize of [Rapoport et al. 2021, Theorem 3.5, 4.4 and 6.7].

Proposition 4.2. *$\mathcal{M}$ is a Deligne–Mumford stack flat over $\mathcal{O}_E$, and*

$$\mathcal{M} \times_{\mathrm{Spec}\, \mathcal{O}_E} \mathbb{C} = S(\tilde{G}, h_{\tilde{G}})_K.$$

Moreover we have:

(i) *$\mathcal{M}$ is smooth of relative dimension $n-1$ over the open subscheme of* $\mathrm{Spec}\, \mathcal{O}_E$ *obtained by removing the set $\mathcal{V}_{\mathrm{ram}}(E)$ of finite places ν of E over $\mathcal{V}_{\mathrm{ram}}$ (see* (4-1)*). If $n = 1$, then $\mathcal{M}$ is finite étale over all of* $\mathrm{Spec}\, \mathcal{O}_E$.

(ii) *If $n \geq 2$, then the fiber of $\mathcal{M}$ over a place $\nu \in \mathcal{V}_{\mathrm{ram}}(E)$ has only isolated singularities. If $n \geq 3$, then blowing up these isolated points for all $\nu \in \mathcal{V}_{\mathrm{ram}}(E)$ yields a model $\mathcal{M}^\sharp$ which has semistable reduction, hence is regular, over the open subscheme of* $\mathrm{Spec}\, \mathcal{O}_E$ *obtained by removing all places $\nu \in \mathcal{V}_{\mathrm{ram}}(E)$ that are ramified over F. This model $\mathcal{M}^\sharp$ has a moduli interpretation by* [Krämer 2003].

5. Special cycles on the basic locus of unitary Shimura varieties

5A. ***Definition of the special cycles.*** Let $\mathrm{Herm}_m(\mathcal{O}_F)$ be the set of $m \times m$ Hermitian matrices with values in $\mathcal{O}_F$. Let $\mathrm{Herm}_m(\mathcal{O}_F)_{\geq 0}$ (resp. $\mathrm{Herm}_m(\mathcal{O}_F)_{>0}$) be the subset of totally (i.e., for all archimedean places) positive semidefinite (resp. definite) matrices of $\mathrm{Herm}_m(\mathcal{O}_F)$. We define special cycles as in [Kudla and Rapoport 2014] and [Rapoport et al. 2021]. For a locally notherian scheme S over $\mathrm{Spec}\, \mathcal{O}_E$ and

$(A_0, \iota_0, \lambda_0, A, \iota, \lambda) \in \mathcal{M}(S)$, we have the finite rank locally free $\mathcal{O}_F$-module

$$\mathbb{L}(A_0, A) := \mathrm{Hom}_{\mathcal{O}_F}(A_0, A).$$

We can define a Hermitian form h' on $\mathbb{L}(A_0, A)$ by assigning for any $x, y \in \mathbb{L}(A_0, A)$

$$h'(x, y) = \iota_0^{-1}(\lambda_0^{-1} \circ y^\vee \circ \lambda \circ x) \in \mathcal{O}_F. \tag{5-1}$$

Remark 5.1. The local analog of $h'(\cdot\,,\cdot)$ is denoted by $h(\cdot\,,\cdot)$, see Section 3B. We use the notation $h'(\cdot\,,\cdot)$ here to be consistent with [Kudla and Rapoport 2014].

Definition 5.2. Let $T \in \mathrm{Herm}_m(\mathcal{O}_F)_{\geq 0}$. The special cycle $\mathcal{Z}(T)$ is the stack such that for any $\mathcal{O}_E$-scheme S, $\mathcal{Z}(T)(S)$ is the groupoid of tuples $(A_0, \iota_0, \lambda_0, A, \iota, \lambda, \boldsymbol{x})$ where $(A_0, \iota_0, \lambda_0, A, \iota, \lambda) \in \mathcal{M}(S)$ and $\boldsymbol{x} = (x_1, \dots, x_m) \in \mathbb{L}(A_0, A)^m$ such that

$$h'(\boldsymbol{x}, \boldsymbol{x}) = (h'(x_i, x_j)) = T.$$

Kudla and Rapoport [2014, Proposition 2.9] generalized to our case and shows that the natural map $\mathcal{Z}(T) \to \mathcal{M}$ is finite and unramified.

5B. *Support of the special cycles.* Let ν be a finite place of E with residue field k_ν of characteristic p. Then ν determines places w_0 of F and v_0 of F_0 respectively. For $(A_0, \iota_0, \lambda_0, A, \iota, \lambda) \in \mathcal{M}(\bar{k}_\nu)$, the $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$-action induces a decomposition of the p-divisible group $A[p^\infty]$ and its Dieudonné module

$$A[p^\infty] = \bigoplus_{w \mid p} A[w^\infty], \quad M(A[p^\infty]) = \bigoplus_{w \mid p} M_w(A) \tag{5-2}$$

where w runs over the set of places of F over p and $M_w(A) = M(A[w^\infty])$ for each w. Each $A[w^\infty]$ admits an $\mathcal{O}_{F,w}$ action. We say that $(A_0, \iota_0, \lambda_0, A, \iota, \lambda)$ is in the basic locus $\mathcal{M}_\nu^{ss}$ if each $A[w^\infty]$ is isoclinic, i.e., the rational Deudonné module $M_w(A)$ has constant slope for all w.

We assume from now on that $T \in \mathrm{Herm}_n(\mathcal{O}_F)_{>0}$. Then we have the following generalization of [Kudla and Rapoport 2014, Lemma 2.21].

Lemma 5.3. *Assume that $T \in \mathrm{Herm}_n(\mathcal{O}_F)_{>0}$. Then $\mathcal{Z}(T)$ is supported on*

$$\bigcup_\nu \mathcal{M}_\nu^{ss}$$

where ν runs over the set of finite places of E whose underlying place of F_0 does not split in F.

Proof. The proof is the same as that of [Rapoport et al. 2020, Lemma 8.7] which is a variant of the proof of [Kudla and Rapoport 2014, Lemma 2.21]. □

For $T \in \mathrm{Herm}_n(\mathcal{O}_F)_{>0}$, let V_T be the Hermitian F-vector space with gram matrix T. Recall that we define a Hermitian vector space V as in (4-10). Define $\mathrm{Diff}(T, V)$ as in (1-3) or equivalently

$$\mathrm{Diff}(T, V) := \{v \text{ is a finite place of } F_0 \mid \mathrm{inv}_v(V) \neq \mathrm{inv}_v(V_T)\}. \tag{5-3}$$

Any v in $\mathrm{Diff}(T, V)$ is automatically nonsplit in F. Since T is totally positive definite and V has signature $((n-1,1)_{\{\varphi_0\}}, (n,0)_{\Phi\setminus\{\varphi_0\}})$, by Hasse principal, $\mathrm{Diff}(T, V)$ is a finite set of odd cardinality. The following result generalizes [Kudla and Rapoport 2014, Proposition 2.22]. It should be well-known to experts; see [Li and Zhang 2022, Section 14.4].

Proposition 5.4. *Assume $T \in \mathrm{Herm}_n(\mathcal{O}_F)_{>0}$:*

(1) *If $|\mathrm{Diff}(T, V)| = \{v_0\}$ where v_0 is a finite place of F_0, then $\mathcal{Z}(T)$ is supported on*

$$\bigcup_{\nu\in\mathscr{V}(v_0)} \mathcal{M}_\nu^{ss}$$

where $\mathscr{V}(v_0)$ is the set of places of E over v_0.

(2) *$\mathcal{Z}(T)$ is empty if $|\mathrm{Diff}(T, V)| > 1$.*

Proof. We prove (1) first. By Lemma 5.3, we know that $\mathcal{Z}(T)$ is supported on the basic locus over finite places of E. Let ν be a finite place of E with residue field k_ν of characteristic p such that $\mathcal{Z}(T)(\bar{k}_\nu)$ is nonempty. Then ν determines a place v_0 of F_0 which does not split in F. Let $(A_0, \iota_0, \lambda_0, A, \iota, \lambda) \in \mathcal{Z}(T)(\bar{k}_\nu)$. By definition V_T carries the Hermitian form $h'(\cdot,\cdot)$ in (5-1).

When v does not divide p, by its definition $\mathrm{inv}_v^r(A_0, \iota_0, \lambda_0, A, \iota, \lambda)$ is the invariant at v of the Hermitian form $h(\cdot,\cdot)$ defined in (4-15) and is the same as $\mathrm{inv}_v(V)$ by the sign condition. On the other hand, the invariant at v of the Hermitian form $h(\cdot,\cdot)$ is the same as $\mathrm{inv}_v(V_T)$ by [Kudla and Rapoport 2014, Lemma 2.10].

Now assume $v \mid p$ and is nonsplit and w is the place of F above v. Since the component containing $(A_0, \iota_0, \lambda_0, A, \iota, \lambda)$ has nonempty generic fiber (this is implied for example by (5-10) below), [Rapoport et al. 2020, Proposition A1] tells us that

$$\mathrm{inv}_v^r(A_0, \iota_0, \lambda_0, A, \iota, \lambda) = \mathrm{inv}_v(V). \tag{5-4}$$

On the other hand by [Rapoport et al. 2020, (A.8)], we know that

$$\mathrm{inv}_v^r(A_0, \iota_0, \lambda_0, A, \iota, \lambda) = \mathrm{sgn}(r_{\nu,v})\,\mathrm{inv}_v(A_0, \iota_0, \lambda_0, A, \iota, \lambda)$$

where by [Rapoport et al. 2020, (A.7)]

$$\mathrm{sgn}(r_{\nu,v}) = \begin{cases} 1 & \text{if } v \mid p \text{ and } v \neq v_0, \\ -1 & \text{if } v = v_0, \end{cases}$$

and $\mathrm{inv}_v(A_0, \iota_0, \lambda_0, A, \iota, \lambda)$ is the invariant of the Hermitian form on the Dieudonné module (see (5-2))

$$\mathrm{Hom}_{F_w\otimes_{\mathbb{Z}_p} W(\bar{k}_\nu)}(M_w(A_0)\otimes\mathbb{Q}, M_w(A)\otimes\mathbb{Q}).$$

By Lemma 3.6, Proposition 3.5 and their analogs at inert primes, we know that

$$\mathrm{inv}_v(A_0, \iota_0, \lambda_0, A, \iota, \lambda) = \mathrm{inv}_v(V_T).$$

Hence we have

$$\mathrm{inv}_v(V) = \begin{cases} \mathrm{inv}_v(V_T) & \text{if } v \mid p \text{ and } v \neq v_0, \\ -\mathrm{inv}_v(V_T) & \text{if } v = v_0. \end{cases}$$

In conclusion, if $\mathcal{Z}(T)(\bar{k}_\nu)$ is nonempty we must have

$$\mathrm{Diff}(T, V) = \{v_0\}.$$

This finishes the proof of the (1).

If z is a geometric point of characteristic zero in $\mathcal{Z}(T)$, then (4-14) implies that $\mathrm{Diff}(T, V) = \varnothing$. But this is impossible by the signature assumption on V and V_T. Hence $\mathcal{Z}(T)$ has no geometric point of characteristic zero and (2) follows from (1). □

5C. *Uniformization of the basic locus and special cycles.* We now fix a place ν of E over w_0 of F and $v_0 \in \mathscr{V}_{\mathrm{ram}}$ of F_0. Let $\breve{E}_\nu$ be the completion of the maximal unramified extension of E_ν. We also denote by $\widehat{\mathcal{M}}_\nu^{ss}$ the completion of $\mathcal{M} \times_{\operatorname{Spec} \mathcal{O}_E} \operatorname{Spec} \mathcal{O}_{\breve{E}_\nu}$ along its basic locus $\mathcal{M}_\nu^{ss} \times_{\operatorname{Spec} k_\nu} \operatorname{Spec} \bar{k}_\nu$.

Lemma 5.5. *$\mathcal{M}_\nu^{ss}(\bar{k}_\nu)$ is nonempty.*

Proof. The proof is a variant of that of [Kudla and Rapoport 2014, Lemma 5.1]. Let $(A_0, \iota_0, \lambda_0) \in \mathcal{M}_0^{\xi}(\mathcal{O}_{\breve{E}_\nu})$. Also let $(A_1, \iota_1, \lambda_1)$ be defined similarly as $(A_0, \iota_0, \lambda_0)$ except that we change the signature from $(0, 1)_\Phi$ to $((1, 0)_{\{\varphi_0\}}, (0, 1)_{\Phi\backslash\{\varphi_0\}})$. Both abelian schemes have good reduction at ν by the smoothness of $\mathcal{M}_0$. Define

$$(A, \iota, \lambda') := (A_0, \iota_0, \lambda_0)^{n-1} \oplus (A_1, \iota_1, \lambda_1).$$

Then $(A_0, \iota_0, \lambda_0, A, \iota, \lambda') \in \mathcal{M}^{V'}(\mathcal{O}_{\breve{E}_\nu})$ where $\mathcal{M}^{V'}$ has the same definition as $\mathcal{M}$ except that in the sign condition we replace V by some Hermitian space V' over F with the same signature as V.

From now on we base change to $\operatorname{Spec} \bar{k}_\nu$ and for simplicity denote the base change of $(A_0, \iota_0, \lambda_0, A, \iota, \lambda')$ by the same notation. Then $(A_0, \iota_0, \lambda_0, A, \iota, \lambda') \in \mathcal{M}_\nu^{V', ss}$. Define

$$\lambda := \lambda' \circ (\iota(a/b), 1, \dots, 1) \tag{5-5}$$

where $a, b \in F_0$ represent $\det(V)$ and $\det(V')$ respectively. Since V and V' have the same the signature over the archimedean places, a/b is totally positive, hence λ is a quasipolarization. Notice that the Rosati involution induced by λ on $F \hookrightarrow \mathrm{End}^0(A)$ is the complex conjugation. By the definition of λ and the fact that $(A_0, \iota_0, \lambda_0, A, \iota, \lambda')$ satisfies the sign condition (4-13) for V' we know that $(A_0, \iota_0, \lambda_0, A, \iota, \lambda)$ satisfies the sign condition for V.

By the $\mathcal{O}_{F_0}$-action on A, we can decompose the p-divisible group $A[p^\infty]$ and the rational Dieudonné module $M(A[p^\infty])$ of $A[p^\infty]$ into

$$A[p^\infty] = \bigoplus_{v \mid p} A[v^\infty], \qquad M(A[p^\infty]) = \bigoplus_{v \mid p} M_v(A) \tag{5-6}$$

where v runs over places of F_0 over p and $M_v(A) = M(A[v^\infty])$ for each v. Let $M_{v_0}^{\mathrm{rel}}(A)$ be the relative Dieudonné module of $\mathcal{C}_{\bar{k}_\nu}(A[v_0^\infty])$ where $\mathcal{C}$ is the functor in Theorem 2.6. Choose an $\breve{\mathcal{O}}_{F, w_0}$-lattice $\Lambda_{v_0}^{\mathrm{rel}} \subset$

$M^{\mathrm{rel}}_{v_0}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ satisfying the condition in Proposition 2.15. Such choice always exists by the nonemptiness statement in Theorem 2.17 (iii). By Theorem 2.6, $\Lambda^{\mathrm{rel}}_{v_0}$ determines a self dual lattice $\Lambda_{v_0}\in M_{v_0}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$. For any other $v\neq v_0$ dividing p, we can choose a self dual lattice $\Lambda_v\subset M_v(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ with respect to the symplectic form induced by λ in a similar manner. Choose a self dual lattice $\Lambda^p\subset\hat{V}^p(A)$ with respect to the symplectic form on $\hat{V}^p(A)$ induced by λ. These lattices determines an abelian variety (B,ι_B,λ_B) isogenic to (A,ι,λ) where λ_B is a principal polarization. Then $(A_0,\iota_0,\lambda_0,B,\iota_B,\lambda_B)\in\mathcal{M}^{ss}_v(\bar{k}_v)$. □

By the lemma we can choose a framing object $(A^o_0,\iota^o_0,\lambda^o_0,A^o,\iota^o,\lambda^o)\in\mathcal{M}^{ss}_v(\bar{k}_v)$. The p-divisible group $A^o[p^\infty]$ of A^o then carries an $\mathcal{O}_F$-action $\iota^o[p^\infty]$ and a compatible polarization $\lambda^o[p^\infty]$ determined by ι^o and λ^o respectively. Decompose $A^o[p^\infty]$ as in (5-6) we get

$$(\mathbb{X},\iota_{\mathbb{X}},\lambda_{\mathbb{X}}):=(A^o[v_0^\infty],\iota^o[v_0^\infty],\lambda^o[v_0^\infty]) \tag{5-7}$$

where $\iota^o[v_0^\infty]$ is the $\mathcal{O}_{F,w_0}$-action determined by $\iota^o[p^\infty]$ and $\lambda^o[v_0^\infty]$ is the polarization of $A^o[v_0^\infty]$ determined by $\lambda^o[p^\infty]$.

Let W' be the n-dimensional Hermitian vector whose local invariants are the same as W except at v_0 and φ_0 where it has signature $(0,n)$. Associate to W' the group $G'^{\mathbb{Q}}$ as in (4-3) where we associate $G^{\mathbb{Q}}$ to W. Also define

$$V':=\mathrm{Hom}_F(W_0,W') \tag{5-8}$$

together with the naturally defined Hermitian form. Then define $\tilde{G}':=Z^{\mathbb{Q}}\times_{\mathbb{G}_m}G'^{\mathbb{Q}}$ which is an inner form of $\tilde{G}$. Let $\mathcal{N}'$ be the Rapoport–Zink space of p-divisible groups with $\mathcal{O}_F$-actions and compatible principal polarizations satisfying the Kottwitz condition, the wedge condition and the Eisenstein condition with respect to the signature $((1,n-1)_{\{\varphi_0\}},(0,n)_{\Phi\setminus\{\varphi_0\}})$, defined by the framing object $(A^o[p^\infty],\iota^o[p^\infty],\lambda^o[p^\infty])$. Then we have the following uniformization theorem.

Theorem 5.6. *We have*

$$\mathcal{N}'=Z^{\mathbb{Q}}(\mathbb{Q}_p)/K_{Z^{\mathbb{Q}},p}\times(\mathcal{N}\widehat{\times}_{\mathrm{Spf}\,\mathcal{O}_{\breve{F}_{w_0}}}\mathrm{Spf}\,\mathcal{O}_{\breve{E}_v})\times\prod_{v\neq v_0}\mathrm{U}(V)(F_{0,v})/K_{G,v} \tag{5-9}$$

where the product in the last factor is over all places of F_0 over p not equal to v_0 and $\mathcal{N}=\mathcal{N}^{F_{w_0}/\mathbb{Q}_p}_{(1,n-1)}\cong\mathcal{N}^{F_{w_0}/F_{0,v_0}}_{(1,n-1)}$. Here $\mathcal{N}^{F_{w_0}/\mathbb{Q}_p}_{(1,n-1)}$ (resp. $\mathcal{N}^{F_{w_0}/F_{0,v_0}}_{(1,n-1)}$) is defined in Definition 2.8 using the framing objects $(\mathbb{X},\iota_{\mathbb{X}},\lambda_{\mathbb{X}})$ in (5-7) (resp. $\mathcal{C}_{\bar{k}_v}((\mathbb{X},\iota_{\mathbb{X}},\lambda_{\mathbb{X}}))$). There is an isomorphism depending on the choice of base point $(A^o_0,\iota^o_0,\lambda^o_0,A^o,\iota^o,\lambda^o)\in\mathcal{M}^{ss}_v(\bar{k}_v)$,

$$\Theta:\tilde{G}'(\mathbb{Q})\backslash\mathcal{N}'\times\tilde{G}(\mathbb{A}^p_f)/K^p\cong\widehat{M}^{ss}_v. \tag{5-10}$$

Proof. Using exactly the same proof of [Rapoport et al. 2020, Lemma 8.16], we know that for $v\neq v_0$ above p, we have

$$\mathcal{N}^{F_v/\mathbb{Q}_p}_{(0,n)}\cong\mathrm{U}(V)(F_{0,v})/K_{G,v}.$$

As a corollary we know that

$$\mathcal{N}' = Z^{\mathbb{Q}}(\mathbb{Q}_p)/K_{Z^{\mathbb{Q}},p} \times (\mathcal{N}_{(1,n-1)}^{F_{w_0}/\mathbb{Q}_p} \widehat{\times}_{\operatorname{Spf} \mathcal{O}_{\breve{F}_{w_0}}} \operatorname{Spf} \mathcal{O}_{\breve{E}_\nu}) \times \prod_{v \neq v_0} \mathrm{U}(V)(F_{0,v})/K_{G,v}. \tag{5-11}$$

Then (5-10) is a special case of [Rapoport and Zink 1996, Theorem 6.30]. By Theorem 2.10, we can also replace $\mathcal{N}_{(1,n-1)}^{F_{w_0}/\mathbb{Q}_p}$ above by $\mathcal{N}_{(1,n-1)}^{F_{w_0}/F_{0,v_0}}$. □

Theorem 5.7. *Assume that $T \in \mathrm{Herm}_n(\mathcal{O}_F)_{>0}$ with $\mathrm{Diff}(T, V) = \{v_0\}$ where $v_0 \in \mathscr{V}_{\mathrm{ram}}$ (1-2). Assume that v_0 is not over 2 and is unramified over $\mathbb{Q}$. Then $\mathcal{Z}(T)_{\mathrm{red}}$ is equidimensional of dimension $\frac{1}{2}\mathfrak{d}(L_{v_0})$ where L_{v_0} is any Hermitian lattice over $\mathcal{O}_{F,v_0}$ whose gram matrix is T and $\mathfrak{d}(L_{v_0})$ is defined as in Theorem 3.9.*

Proof. The proof resembles that of [Kudla and Rapoport 2014, Proposition 11.2]. By Proposition 5.4, $\mathcal{Z}(T)$ is supported on the basic locus over ν for those finite places ν of E that induces v_0. Fix such a ν and let w_0 be the place of F above v_0. Choose a framing object $(A_0^o, \iota_0^o, \lambda_0^o, A^o, \iota^o, \lambda^o) \in \mathcal{M}_\nu^{ss}(\bar{k}_\nu)$ which determines a supersingular formal $\mathcal{O}_{F,w_0}$-module $(\mathbb{X}, \iota_{\mathbb{X}}, \lambda_{\mathbb{X}})$ as in (5-7).

Define V' as in (5-8) and $G' := \mathrm{U}(V')$. By Proposition 5.4, we know that

$$V' \cong V_T$$

as Hermitian spaces. In particular, $V'_v \cong V_v$ as a Hermitian space for all finite places $v \neq v_0$ of F_0. We can thus think of

$$L^{v_0} := L \otimes_{\mathcal{O}_{F_0}} \hat{\mathcal{O}}_{F_0}^{v_0}$$

(see (4-12) for the definition of L) as a lattice in $V'(\mathbb{A}_{F_0,f}^{v_0})$. Its stabilizer in $G'(\mathbb{A}_{F_0,f}^{v_0})$ is $K_G^{v_0}$. On the other hand, by Proposition 3.5 we have the following identification.

$$V'_{v_0} \cong \mathrm{Hom}_{\mathcal{O}_{F,w_0}}(\mathbb{Y}, \mathbb{X}) \otimes \mathbb{Q} \cong \mathrm{Hom}_{\mathcal{O}_{F,w_0}}(\mathcal{C}_{\bar{k}_\nu}(\mathbb{Y}), \mathcal{C}_{\bar{k}_\nu}(\mathbb{X})) \otimes \mathbb{Q} = \mathbb{V}.$$

Let $\widehat{\mathcal{Z}(T)}_\nu$ be the closure of $\mathcal{Z}(T) \times_{\operatorname{Spec} \mathcal{O}_E} \operatorname{Spec} \mathcal{O}_{\breve{E}_\nu}$ in $\widehat{\mathcal{M}}_\nu^{ss}$. Then by Theorem 5.6 and the fact that $\tilde{G}' = Z^{\mathbb{Q}} \times \mathrm{Res}_{F_0/\mathbb{Q}} G'$, we have (see [Kudla and Rapoport 2014, Proposition 6.3])

$$\widehat{\mathcal{Z}(T)}_\nu \cong (Z^{\mathbb{Q}}(\mathbb{Q}) \backslash Z^{\mathbb{Q}}(\mathbb{A}_f)/K_{Z^{\mathbb{Q}}}) \times \coprod_{g \in G'(F_0) \backslash G'(\mathbb{A}_{F_0,f}^{v_0})/K_G^{v_0}} \coprod_{\substack{\boldsymbol{x} \in \Omega(T) \\ g^{-1}\boldsymbol{x} \in (L^{v_0})^n}} \mathcal{Z}(\boldsymbol{x}),$$

where $\mathcal{Z}(\boldsymbol{x})$ is the special cycle of $\mathcal{N}_{(1,n-1)}^{F_{w_0}/F_{0,v_0}}$ defined in Definition 3.4 and

$$\Omega(T) := \{\boldsymbol{x} \in (V')^n \mid (\boldsymbol{x}, \boldsymbol{x}) = T\}.$$

Here we think of V' as a subset of both $\mathbb{V}$ and $V'(\mathbb{A}_{F_0,f}^{v_0})$. The theorem is now a consequence of Theorem 3.9. □

Acknowledgement

The author would like to thank Michael Rapoport for suggesting the problem and reading through early versions of the paper. We would also like to thank Patrick Daniels, Qiao He and Tonghai Yang for helpful discussions.

References

[Ahsendorf et al. 2016] T. Ahsendorf, C. Cheng, and T. Zink, "$\mathcal{O}$-displays and π-divisible formal $\mathcal{O}$-modules", *J. Algebra* **457** (2016), 129–193. MR Zbl

[Cho 2018] S. Cho, "The basic locus of the unitary Shimura variety with parahoric level structure, and special cycles", preprint, 2018. arXiv 1807.09997

[Fargues 2008] L. Fargues, "L'isomorphisme entre les tours de Lubin–Tate et de Drinfeld et applications cohomologiques", pp. 1–325 in *L'isomorphisme entre les tours de Lubin–Tate et de Drinfeld*, Progr. Math. **262**, Birkhäuser, Basel, 2008. MR Zbl

[Fargues and Fontaine 2018] L. Fargues and J.-M. Fontaine, *Courbes et fibrés vectoriels en théorie de Hodge p-adique*, Astérisque **406**, Soc. Math. France, Paris, 2018. MR Zbl

[Gross 1986] B. H. Gross, "On canonical and quasicanonical liftings", *Invent. Math.* **84**:2 (1986), 321–326. MR

[He et al. 2023] Q. He, Y. Shi, and T. Yang, "The Kudla–Rapoport conjecture at a ramified prime for $U(1, 1)$", *Trans. Amer. Math. Soc.* **376**:4 (2023), 2257–2291. MR Zbl

[Howard 2012] B. Howard, "Complex multiplication cycles and Kudla–Rapoport divisors", *Ann. of Math.* (2) **176**:2 (2012), 1097–1171. MR Zbl

[Jacobowitz 1962] R. Jacobowitz, "Hermitian forms over local fields", *Amer. J. Math.* **84** (1962), 441–465. MR Zbl

[Krämer 2003] N. Krämer, "Local models for ramified unitary groups", *Abh. Math. Sem. Univ. Hamburg* **73** (2003), 67–80. MR Zbl

[Kudla and Rapoport 2011] S. Kudla and M. Rapoport, "Special cycles on unitary Shimura varieties, I: Unramified local theory", *Invent. Math.* **184**:3 (2011), 629–682. MR Zbl

[Kudla and Rapoport 2014] S. Kudla and M. Rapoport, "Special cycles on unitary Shimura varieties II: Global theory", *J. Reine Angew. Math.* **697** (2014), 91–157. MR Zbl

[Kudla et al. 2020] S. Kudla, M. Rapoport, and T. Zink, "On the p-adic uniformization of unitary Shimura curves", preprint, 2020. arXiv 2007.05211

[Li and Liu 2022] C. Li and Y. Liu, "Chow groups and L-derivatives of automorphic motives for unitary groups, II", *Forum Math. Pi* **10** (2022), Paper No. e5, 71. MR Zbl

[Li and Zhang 2022] C. Li and W. Zhang, "Kudla–Rapoport cycles and derivatives of local densities", *J. Amer. Math. Soc.* **35**:3 (2022), 705–797. MR Zbl

[Mihatsch 2022] A. Mihatsch, "Relative unitary RZ-spaces and the arithmetic fundamental lemma", *J. Inst. Math. Jussieu* **21**:1 (2022), 241–301. MR Zbl

[O'Meara 2000] O. T. O'Meara, *Introduction to quadratic forms*, Springer, 2000. MR Zbl

[Pappas 2000] G. Pappas, "On the arithmetic moduli schemes of PEL Shimura varieties", *J. Algebraic Geom.* **9**:3 (2000), 577–605. MR Zbl

[Rapoport and Zink 1996] M. Rapoport and T. Zink, *Period spaces for p-divisible groups*, Annals of Mathematics Studies **141**, Princeton University Press, Princeton, NJ, 1996. MR Zbl

[Rapoport et al. 2014] M. Rapoport, U. Terstiege, and S. Wilson, "The supersingular locus of the Shimura variety for $\mathrm{GU}(1, n-1)$ over a ramified prime", *Math. Z.* **276**:3-4 (2014), 1165–1188. MR Zbl

[Rapoport et al. 2020] M. Rapoport, B. Smithling, and W. Zhang, "Arithmetic diagonal cycles on unitary Shimura varieties", *Compos. Math.* **156**:9 (2020), 1745–1824. MR Zbl

[Rapoport et al. 2021] M. Rapoport, B. Smithling, and W. Zhang, "On Shimura varieties for unitary groups", *Pure Appl. Math. Q.* **17**:2 (2021), 773–837. MR Zbl

[Shi 2023] Y. Shi, "Special cycles on unitary Shimura curves at ramified primes", *Manuscripta Math.* **172**:1-2 (2023), 221–290. MR

Communicated by Shou-Wu Zhang
Received 2021-04-02 Revised 2022-09-07 Accepted 2022-12-08

0023140@zju.edu.cn Zhejiang University, Zhejiang, China

ALGEBRA AND NUMBER THEORY 17:10 (2023)
https://doi.org/10.2140/ant.2023.17.1715

Hybrid subconvexity bounds for twists of GL(3) × GL(2) L-functions.

Bingrong Huang and Zhao Xu

We prove hybrid subconvexity bounds for $\mathrm{GL}(3) \times \mathrm{GL}(2)$ L-functions twisted by a primitive Dirichlet character modulo M (prime) in the M- and t-aspects. We also improve hybrid subconvexity bounds for twists of $\mathrm{GL}(3)$ L-functions in the M- and t-aspects.

1. Introduction

The subconvexity problem of automorphic L-functions on the critical line is one of the central problems in number theory. In general, let $\mathcal{C}$ denote the analytic conductor of the relevant L-function; see, e.g., Iwaniec and Kowalski [2004, Section 5.1]), then one hopes to obtain a subconvexity bound $\mathcal{C}^{1/4-\delta}$ for some $\delta > 0$ on the critical line. Subconvexity bounds have many very important applications such as the equidistribution problems; see, e.g., Michel and Venkatesh [2010].

For the $\mathrm{GL}(1)$ case, i.e., the Riemann zeta function and Dirichlet L-functions, subconvexity bounds have been known for a long time thanks to Weyl [1921] and Burgess [1963]. In the last decades, many cases of $\mathrm{GL}(2)$ L-functions have been treated; see Michel and Venkatesh [2010]. In the last ten years, people have made progress on $\mathrm{GL}(3)$ L-functions; see [Blomer 2012; Li 2011; Munshi 2015a; 2015b; 2022; Sharma 2022]. In this paper, we extend the techniques in [Lin and Sun 2021; Munshi 2022; Sharma 2022] to prove, for the first time, hybrid subconvexity bounds for $\mathrm{GL}(3) \times \mathrm{GL}(2)$ L-functions twisted by a primitive Dirichlet character modulo M (prime), which reach the best known bounds in the M- and t-aspects simultaneously. Our method also improves hybrid subconvexity bounds for twists of $\mathrm{GL}(3)$ L-functions due to Huang [2021a] and Lin [2021].

Let π be a Hecke–Maass cusp form of type (ν_1, ν_2) for $\mathrm{SL}(3, \mathbb{Z})$ with the normalized Fourier coefficients $A(m, n)$. The L-function of π is defined as

$$L(s, \pi) = \sum_{n \geq 1} \frac{A(1, n)}{n^s}, \quad \mathrm{Re}(s) > 1.$$

This work was in part supported by the National Key R&D Program of China 2021YFA1000700 and NSFC 12031008. B.H. was also supported by NSFC 12001314 and the Young Taishan Scholars Program. Z.X. was also supported by Natural Science Foundation of Shandong Province ZR2019MA011.
MSC2020: primary 11F66; secondary 11F67.
Keywords: hybrid subconvexity, twists, GL(3) × GL(2) L-functions, delta method.

Let f be a Hecke–Maass cusp form with the spectral parameter t_f for $\mathrm{SL}(2,\mathbb{Z})$, with the normalized Fourier coefficients $\lambda_f(n)$. The L-function of f is defined by

$$L(s, f) = \sum_{n\geq 1} \frac{\lambda_f(n)}{n^s}, \quad \mathrm{Re}(s) > 1.$$

Let χ be a primitive Dirichlet character modulo M. The $\mathrm{GL}(3) \times \mathrm{GL}(2) \times \mathrm{GL}(1)$ Rankin–Selberg L-function is defined as

$$L(s, \pi \times f \times \chi) = \sum_{m\geq 1}\sum_{n\geq 1} \frac{A(m,n)\lambda_f(n)\chi(m^2 n)}{(m^2 n)^s}, \quad \mathrm{Re}(s) > 1.$$

These L-functions have analytic continuation to the whole complex plane. In this paper, we consider the L-values at the point $\frac{1}{2}+it$ with $t \in \mathbb{R}$. The Phragmén–Lindelöf principle and the functional equation imply the convexity bounds

$$L\big(\tfrac{1}{2}+it, \pi \times f \times \chi\big) \ll_{\pi,f,\varepsilon} (M(1+|t|))^{3/2+\varepsilon},$$

for any $\varepsilon > 0$. It is known that the Riemann hypothesis for $L(s,\pi \times f \times \chi)$ implies the Lindelöf hypothesis, i.e., $L\big(\frac{1}{2}+it, \pi \times f \times \chi\big) \ll_{\pi,f,\varepsilon} (M(1+|t|))^{\varepsilon}$. For $M = 1$, the first subconvex exponent in t-aspect was obtained by Munshi [2022]. Recently, Lin and Sun [2021] proved that

$$L\big(\tfrac{1}{2}+it, \pi \times f\big) \ll_{\pi,f,\varepsilon} (1+|t|)^{3/2-3/20+\varepsilon}.$$

For $t = 0$ and prime M, Sharma [2022] proved that

$$L\big(\tfrac{1}{2}, \pi \times f \times \chi\big) \ll_{\pi,f,\varepsilon} M^{3/2-1/16+\varepsilon}.$$

In the context of L-functions, obtaining hybrid bounds that perfectly combine the two aspects is a difficult problem; see [Blomer and Harcos 2008; Fan and Sun 2022; Heath-Brown 1978; Lin 2021; Huang 2021c; Petrow and Young 2020; 2023]. Our main result in this paper is the following hybrid subconvexity bounds.

Theorem 1.1. *With the notation as above. Let $t \in \mathbb{R}$ and M be prime. Then we have*

$$L\big(\tfrac{1}{2}+it, \pi \times f \times \chi\big) \ll_{\pi,f,\varepsilon} M^{3/2-1/16+\varepsilon}(1+|t|)^{3/2-3/20+\varepsilon}.$$

Remark 1.2. Below we will carry out the proof under the assumption $t \geq M^{\varepsilon}$ for some small $\varepsilon > 0$. For the case $t \ll M^{\varepsilon}$, one can extend the method of Sharma [2022] to prove $L\big(\frac{1}{2}+it, \pi \times f \times \chi\big) \ll_{t,\pi,f,\varepsilon} M^{3/2-1/16+\varepsilon}$ with polynomial dependence on t. For the case $t \leq -M^{\varepsilon}$, the same result follows from the case $t \geq M^{\varepsilon}$ by the functional equation.

Remark 1.3. Let π, χ and t be the same as above and f be a weight k Hecke modular form for $\mathrm{SL}(2,\mathbb{Z})$. The same hybrid subconvexity bounds for $L\big(\frac{1}{2}+it, \pi \times f \times \chi\big)$ can be proved by our method. The only thing need to be changed is the $\mathrm{GL}(2)$ Voronoi summation formula.

Note that by the Hecke relation of the Fourier coefficients (see [Goldfeld 2006, Theorem 6.4.11]), we have

$$A(1,m)A(1,n)=\sum_{d\,|\,(m,n)} A\Big(d,\frac{mn}{d^2}\Big).$$

Hence we have

$$L(s,\pi\times\chi)^2=\sum_{m\geq 1}\sum_{n\geq 1}\frac{A(m,n)\tau(n)\chi(m^2n)}{(m^2n)^s},\qquad \mathrm{Re}(s)>1,$$

where $\tau(n)=\sum_{d\,|\,n}1$ is the divisor function which is the coefficient of the Eisenstein series for $\mathrm{SL}(2,\mathbb{Z})$. The subconvexity bounds for $L\big(\frac{1}{2}+it,\pi\times\chi\big)$ follow from bounds for $L\big(\frac{1}{2}+it,\pi\times f\times\chi\big)$ with f being a GL(2) Eisenstein series.

Theorem 1.4. *With the notation as above. Let $t\in\mathbb{R}$ and M be prime. Then we have*

$$L\big(1/2+it,\pi\times\chi\big)\ll_{\pi,\varepsilon} M^{3/4-1/32+\varepsilon}(1+|t|)^{3/4-3/40+\varepsilon}.$$

Remark 1.5. The only difference in the proofs of Theorem 1.4 and Theorem 1.1 is that we need to use the Voronoi summation formula for $\tau(n)$ instead of those for Fourier coefficients of a GL(2) cusp form. This will give us another zero frequency contribution in the dual sum. This contribution will not have any effect on the final result. Indeed, in the generic case, the weight function for the sum of $\tau(n)$ is oscillating. By integration by parts, we can show its contribution is negligibly small.

Theorem 1.4 improves the hybrid subconvexity bounds for twists of GL(3) L-functions due to Huang [2021a] and Lin [2021], and also reaches the best known bounds in the M- and t-aspects simultaneously; see Sharma [2022] and Aggarwal [2021]. Recall that under the same assumptions Lin [2021] proved that

$$L\big(\tfrac{1}{2}+it,\pi\times\chi\big)\ll_{\pi,\varepsilon}(M(1+|t|))^{3/4-1/36+\varepsilon}.$$

One may give a quick comparison with Lin's work [2021]. Actually, we have a different structure from Lin's paper. Theorem 1.4 can be viewed as a subconvexity result for GL(3) × GL(2) × GL(1) L-functions, where the GL(2)-item is the Eisenstein series. Lin's work is to consider the $L\big(\frac{1}{2}+it,\pi\times\chi\big)$ directly.[1]

Heath-Brown [1978] proved the first hybrid subconvexity bounds for Dirichlet L-functions by extending the Burgess method and van der Corput method to give good estimates for hybrid sums $\sum\chi(n)n^{it}$. Recently, Petrow and Young [2020; 2023] proved the Weyl bound in both aspects by estimating moments of L-functions. For the GL(2) case, Blomer and Harcos [2008] proved the first hybrid subconvexity bounds in the M- and t-aspects by using moments of L-functions. Recently, Fan and Sun [2022] improved the bounds by using a delta method. Our method can also provide hybrid subconvexity bounds in the GL(1) and GL(2) settings, but are weaker than the best known results.

The basic observation is that the subconvexity bounds for GL(3) × GL(2) × GL(1) L-functions in individual M-aspect or t-aspect were proved by applying the Duke–Friedlander–Iwaniec delta method

[1] Kıral, Kuan and Lesesvre [Kıral et al. 2022] further improved subconvexity bounds for twisted GL(3) L-functions under the restriction $M<t^{8/7}$.

to separate oscillatory factors. This suggests to us that in order to prove a hybrid subconvexity bound one may use the same method as the starting point. This philosophy may allow us to make progress in other hybrid settings; see [Huang 2021c]. However, technically speaking, to estimate the complicated sums (e.g., (3-1) below) is much more difficult. We have to take care of both aspects carefully. It is worth mentioning that, as in [Aggarwal 2021; Huang 2021b; Lin and Sun 2021], we drop the conductor-lowering trick which was used in Munshi [2015a] for the t-aspect, but we still use the conductor-lowering trick for the M-aspect as in Munshi [2015b] and Sharma [2022].

1A. ***Sketch of the proof.*** We give a brief sketch of the proof. By the approximate functional equation and some standard analysis, we need to get

$$\sum_{n\sim N} A(r,n)\lambda_f(n)\chi(n)n^{-it} \ll N^{1/2+\varepsilon}M^{3/2-1/16}t^{3/2-3/20},$$

where $N \ll (Mt)^{3+\varepsilon}/r^2$, $r \ll M^{1/8}t^{3/10}$ and $(r, M) = 1$ (see Proposition 3.1). We will apply the Duke–Friedlander–Iwaniec delta method with moduli $q \le Q$ (see Lemma 2.6). For simplicity let us focus on the generic case, i.e., $N = M^3t^3$, $r = 1$ and $q \sim Q = (LN/MK)^{1/2}$ for some parameters L and $K \ll t^{1-\varepsilon}$ which will be chosen later. After applying the Duke–Friedlander–Iwaniec delta method and the conductor-lowering trick for the M-aspect by Munshi (see Sharma [2022]), the main object of study is given by

$$\frac{1}{L}\sum_{\ell\sim L}\overline{A(1,\ell)}\int_{x\sim 1}\frac{1}{M}\sideset{}{^\star}\sum_{b \bmod M}\frac{1}{Q}\sum_{\substack{q\sim Q\\(q,\ell M)=1}}\frac{1}{q}\sideset{}{^\star}\sum_{a \bmod q}\sum_{n\sim LN}A(1,n)e\biggl(\frac{n(aM+bq)}{qM}\biggr)e\biggl(\frac{nx}{MqQ}\biggr)$$
$$\cdot\sum_{m\sim N}\lambda_f(m)\chi(m)e\biggl(\frac{-m\ell(aM+bq)}{qM}\biggr)m^{-it}e\biggl(\frac{-m\ell x}{MqQ}\biggr)\,\mathrm{d}x.$$

By using the Ramanujan conjecture on average, trivially estimating at this stage gives $O(LN^2)$. So we want to save LN plus a "little more" in the above sum. Note that here we don't need the conductor-lowing trick for the t-aspect as observed in [Aggarwal 2021; Huang 2021b; Lin and Sun 2021]. In fact, the x-integral above plays the same role as the v-integral in Munshi [2015a].

We apply the Voronoi summation formulas to both n and m sums. For the n sum, by the GL(3) Voronoi, we get essentially

$$qM\sum_{n_2=1}^{\infty}\frac{A(1,n_2)}{n_2}S(\overline{(aM+bq)},n_2;qM)\Psi_x\biggl(\frac{n_2}{q^3M^3}\biggr),$$

for certain weight function Ψ_x depending on x. The conductor in the above n_2-sum is $K^3M^3Q^3$, and the length is about LN. Hence the dual length becomes $n_2 \asymp K^3M^3Q^3/(LN) = L^2N^2/Q^3$. By Lemma 4.1, the current bound for this dual sum is $QM\cdot(QM)^{1/2}\cdot(LN/(MQ^2))^{3/2}$. So we save $(LN)^{1/4}/(MK)^{3/4}$.

In the GL(2) Voronoi, the dual sum becomes essentially

$$\frac{N}{Mq\tau(\overline{\chi})}\sum_{\substack{u \bmod M\\ u\not\equiv b \bmod M}}\overline{\chi}(u\ell)\sum_{m\geq 1}\lambda_f(m)e\biggl(\pm\frac{m\overline{\ell(aM+(b-u)q)}}{Mq}\biggr)H^{\pm}\biggl(\frac{mN}{M^2q^2}\biggr)$$

for certain weight function $H^{\pm}$. The conductor in the m-sum is $t^2Q^2M^2$, so the dual length becomes $m\asymp t^2Q^2M^2/N = LMt^2/K$. By Lemma 2.4 and the square root cancellation in the u sum, the trivial bound for this dual sum is $(N/QM)\cdot(M^{1/2}Q^{1/2}/N^{1/4})\cdot(t^2Q^2M^2/N)^{3/4}\cdot(1/t^{1/2})$. Hence we save $N^{1/2}K^{1/2}/(L^{1/2}M^{1/2}t)$. By the stationary phase method, we save $K^{1/2}$ from the x-integral. We also save $Q^{1/2}$ in the a sum and $M^{1/2}$ in the b sum. Hence in total we have saved

$$\frac{(LN)^{1/4}}{(MK)^{3/4}}\cdot\frac{N^{1/2}K^{1/2}}{L^{1/2}M^{1/2}t}\cdot K^{1/2}Q^{1/2}M^{1/2}=\frac{N}{Mt}.$$

Hence we still need to save LMt plus a “little more”. Generally we arrive at

$$\frac{N^{13/12}}{M^2LQ}\sum_{\ell\in\mathcal{L}}\overline{A(1,\ell)\chi(\ell)}\ell^{1/3}\sum_{q\sim Q}\frac{1}{q^{3/2}}\sum_{n_2\asymp L^2N^2/Q^3}\frac{A(1,n_2)}{n_2^{2/3}}\sum_{m\asymp M^2Q^2t^2/N}\frac{\lambda_f(m)}{m^{1/4}}\mathcal{C}\mathcal{J},$$

for certain character sum $\mathcal{C}$ and integral transform $\mathcal{J}$ (see (4-11)).

Next applying the Cauchy inequality we arrive at

$$\biggl(\sum_{n_2\asymp L^2N^2/Q^3}\biggl|\sum_{\ell\in\mathcal{L}}\overline{A(1,\ell)\chi(\ell)}\ell^{1/3}\sum_{q\sim Q}\frac{1}{q^{3/2}}\sum_{m\asymp M^2Q^2t^2/N}\frac{\lambda_f(m)}{m^{1/4}}\mathcal{C}\mathcal{J}\biggr|^2\biggr)^{1/2},$$

where we seek to save LMt plus extra. Opening the absolute value square we apply the Poisson summation formula on the sum over n_2. For the zero frequency we save $(LQM^2Q^2t^2/N)^{1/2}$. This gives a bound of size $N^{3/4}M^{3/4}K^{3/4}/L^{1/4}$. We save enough in the zero frequency if $K<t$ and $L>1$.

For the non-zero frequencies, the conductor is of size Q^2MK, hence the length of the dual sum is $O((Q^2MK/(L^2N^2/Q^3))^{1/2}) = O(L^{1/4}N^{1/4}/(M^{3/4}K^{3/4}))$. In the integral transform we save $K^{1/4}$ and the character sums save $(Q^2M^{1/2})^{1/2}=QM^{1/4}$. Hence in total in the non-zero frequencies we save $(M^{3/4}K^{3/4}/L^{1/4}N^{1/4})K^{1/4}QM^{1/4}$. This gives a bound of size $N^{1/4}QL^{1/4}Mt = N^{3/4}L^{3/4}M^{1/2}t/K^{1/2}$. We save enough in the non-zero frequencies if $L<M^{1/3}$ and $K>t^{1/2}$. We also have different bounds from other cases. In fact, the best choice is $L=M^{1/4}$ and $K=t^{4/5}$ which gives $O(N^{1/2+\varepsilon}M^{3/2-1/16}t^{3/2-3/20})$ as claimed.

1B. *Plan for this paper.* The rest of this paper is organized as follows. In Section 2, we introduce some notation and present some lemmas that we will need later. The approximate functional equation allows us to reduce the subconvexity problem to estimating certain convolution sums. In Section 3, we apply the delta method to the convolution sums. In Section 4, we apply the Voronoi summation formulas and estimate the integral transforms by the stationary phase method. In Section 5, we apply the Cauchy–Schwarz inequality and Poisson summation formula, and then analyze the integrals. Then we deal with character sums and the zero frequency contribution in Section 6. In Section 7, we give the contribution from non zero frequencies. Finally, in Section 8, we balance parameters optimally and prove Proposition 3.1 which leads to Theorem 1.1.

Notation. Throughout the paper, ε is an arbitrarily small positive number; all of them may be different at each occurrence. By a smooth dyadic subdivision of a sum $\sum_{n\geq 1} A(n)$, we will mean

$$\sum_{(V,N)} \sum_{n\geq 1} A(n) V\left(\frac{n}{N}\right),$$

where

$$\sum_{(V,N)} V\left(\frac{n}{N}\right) = 1$$

with V being a smooth function supported on $[1, 2]$ and satisfying $V^{(j)}(x) \ll_j 1$. The weight functions U, V, W may also change at each occurrence. As usual, $e(x) = e^{2\pi i x}$ and $n \sim N$ means $N \leq n < 2N$.

2. Preliminaries

2A. ***Automorphic forms.*** Let f be a Hecke–Maass cusp form with the spectral parameter t_f for $\mathrm{SL}(2, \mathbb{Z})$, with the normalized Fourier coefficients $\lambda_f(n)$. Let θ_2 be the bound toward to the Ramanujan conjecture and we have $\theta_2 \leq \frac{7}{64}$ due to Kim and Sarnak [2003]. It is well known that, by the Rankin–Selberg theory, one has

$$\sum_{n\leq N} |\lambda_f(n)|^2 \ll_f N. \tag{2-1}$$

Let π be a Hecke–Maass cusp form of type (ν_1, ν_2) for $\mathrm{SL}(3, \mathbb{Z})$ with the normalized Fourier coefficients $A(r, n)$. Similarly, Rankin–Selberg theory gives

$$\sum_{r^2 n\leq N} |A(r, n)|^2 \ll_\pi N. \tag{2-2}$$

We record the Hecke relation

$$A(r, n) = \sum_{d\,|\,(r,n)} \mu(d) A\left(\frac{r}{d}, 1\right) A\left(1, \frac{n}{d}\right)$$

which follows from the Möbius inversion and [Goldfeld 2006, Theorem 6.4.11]. Hence we have the individual bounds

$$A(r, n) \ll (rn)^{\theta_3+\varepsilon}, \tag{2-3}$$

where $\theta_3 \leq \frac{5}{14}$ is the bound toward to the Ramanujan conjecture on GL(3); see [Kim 2003]. So we have

$$\sum_{n\sim N} |A(r, n)| \ll \sum_{n_1\,|\,r^\infty} \sum_{\substack{n\sim N/n_1 \\ (n,r)=1}} |A(r, nn_1)| \leq \sum_{n_1\,|\,r^\infty} |A(r, n_1)| \sum_{\substack{n\sim N/n_1 \\ (n,r)=1}} |A(1, n)| \ll r^{\theta_3+\varepsilon} N \tag{2-4}$$

and

$$\sum_{n\sim N}|A(r,n)|^2 \ll \sum_{n_1\mid r^\infty}\sum_{\substack{n\sim N/n_1\\(n,r)=1}}|A(r,nn_1)|^2 \le \sum_{n_1\mid r^\infty}|A(r,n_1)|^2\sum_{\substack{n\sim N/n_1\\(n,r)=1}}|A(1,n)|^2 \ll r^{2\theta_3+\varepsilon}N. \tag{2-5}$$

Here we have used (2-2) and the fact $\sum_{d\mid r^\infty} d^{-\sigma}\ll r^{\varepsilon}$, for $\sigma>0$.

2B. *L-functions.* The Rankin–Selberg L-function $L(s,\pi\times f\times\chi)$ has the following functional equation

$$\Lambda(s,\pi\times f\times\chi)=\epsilon_{\pi\times f\times\chi}\Lambda(1-s,\tilde{\pi}\times f\times\bar{\chi}),$$

where

$$\Lambda(s,\pi\times f\times\chi)=M^{3s}\pi^{-3s}\prod_{j=1}^{3}\prod_{\pm}\Gamma\Big(\frac{s-\alpha_j\pm it_f}{2}\Big)L(s,\pi\times f\times\chi)$$

is the completed L-function and $\epsilon_{\pi\times f\times\chi}$ is the root number. Here α_j are the Langlands parameters of π, and $\tilde{\pi}$ is the contragredient representation of π. By [Iwaniec and Kowalski 2004, Section 5.2], we can obtain the approximate functional equation which leads us to the following result.

Lemma 2.1. *We have*

$$L\big(\tfrac12+it,\pi\times f\times\chi\big)\ll (M(|t|+1))^{\varepsilon}\sup_{N\ll(M(|t|+1))^{3+\varepsilon}}\frac{|S(N)|}{\sqrt{N}}+(M(|t|+1))^{-A},$$

where

$$S(N)=\sum_{r\ge1}\sum_{n\ge1}A(r,n)\lambda_f(n)\chi(r^2n)(r^2n)^{-it}V\Big(\frac{r^2n}{N}\Big),$$

with some compactly supported smooth function V such that $\operatorname{supp} V\subset[1,2]$ *and* $V^{(j)}\ll_j 1$.

We first estimate the contribution from large values of r. By (2-1) and (2-5) we have

$$\begin{aligned}
&\sum_{r\ge M^{1/8}(|t|+1)^{3/10}}\Big|\sum_{n\ge1}A(r,n)\lambda_f(n)\chi(n)(r^2n)^{-it}V\Big(\frac{r^2n}{N}\Big)\Big|\\
&\qquad\ll \sum_{M^{1/8}(|t|+1)^{3/10}\le r\ll\sqrt{N}}\Big(\sum_{n\asymp N/r^2}|A(r,n)|^2\Big)^{1/2}\Big(\sum_{n\asymp N/r^2}|\lambda_f(n)|^2\Big)^{1/2}\\
&\qquad\ll \sum_{M^{1/8}(|t|+1)^{3/10}\le r\ll\sqrt{N}} r^{\theta_3+\varepsilon}\frac{N}{r^2}\\
&\qquad\ll N\sum_{M^{1/8}(|t|+1)^{3/10}\le r\ll\sqrt{N}} r^{-3/2-\varepsilon}\\
&\qquad\ll N^{1/2}M^{3/2-1/16}(|t|+1)^{3/2-3/20+\varepsilon},
\end{aligned}\tag{2-6}$$

for $N\ll(M(|t|+1))^{3+\varepsilon}$. The contribution from those terms to $L\big(\frac12+it,\pi\times f\times\chi\big)$ is bounded by $M^{3/2-1/16+\varepsilon}(|t|+1)^{3/2-3/20+\varepsilon}$.

Therefore, combining this together with Lemma 2.1, we prove the following lemma.

Lemma 2.2. *We have*

$$L\big(\tfrac{1}{2}+it,\pi\times f\times\chi\big)\ll t^{\varepsilon}\sum_{\substack{r\le M^{1/8}t^{3/10}\\(r,M)=1}}\frac{1}{r}\sup_{N\ll(Mt)^{3+\varepsilon}/r^2}\frac{|S(r,N)|}{\sqrt{N}}+M^{3/2-1/16}t^{3/2-3/20+\varepsilon},$$

where

$$S(r,N):=\sum_{n\ge 1}A(r,n)\lambda_f(n)\chi(n)n^{-it}V\left(\frac{n}{N}\right).$$

2C. *Summation formulas.* We first recall the Poisson summation formula over an arithmetic progression.

Lemma 2.3. *Let $\beta\in\mathbb{Z}$ and $c\in\mathbb{Z}_{\ge 1}$. For a Schwartz function $f:\mathbb{R}\to\mathbb{C}$, we have*

$$\sum_{\substack{n\in\mathbb{Z}\\ n\equiv\beta \bmod c}}f(n)=\frac{1}{c}\sum_{n\in\mathbb{Z}}\hat{f}\left(\frac{n}{c}\right)e\left(\frac{n\beta}{c}\right),$$

where $\hat{f}(y)=\int_{\mathbb{R}}f(x)e(-xy)\,\mathrm{d}x$ is the Fourier transform of f.

Proof. See, e.g., [Iwaniec and Kowalski 2004, (4.24)]. □

We recall the Voronoi summation formula for $\mathrm{SL}(2,\mathbb{Z})$. Let g be a smooth compactly supported function on $(0,\infty)$.

Lemma 2.4. *With the notation as above. Then we have*

$$\sum_{n\ge 1}\lambda_f(n)e\left(\frac{an}{q}\right)g\left(\frac{n}{N}\right)=\frac{N}{q}\sum_{\pm}\sum_{n\ge 1}\lambda_f(n)e\left(\mp\frac{\bar{a}n}{q}\right)H^{\pm}\left(\frac{nN}{q^2}\right)\tag{2-7}$$

where

$$H^{+}(y)=\frac{-\pi}{\sin(\pi i t_f)}\int_0^{\infty}g(\xi)\big(J_{2it_f}(4\pi\sqrt{y\xi})-J_{-2it_f}(4\pi\sqrt{y\xi})\big)\,\mathrm{d}\xi,\tag{2-8}$$

and

$$H^{-}(y)=4\epsilon_f\cosh(\pi t_f)\int_0^{\infty}g(\xi)K_{2it_f}(4\pi\sqrt{y\xi})\,\mathrm{d}\xi.\tag{2-9}$$

For $y\gg T^{\varepsilon}$, we have

$$H^{+}(y)=y^{-1/4}\int_0^{\infty}g(\xi)\xi^{-1/4}\sum_{j=0}^{J}\frac{c_je(2\sqrt{y\xi})+d_je(-2\sqrt{y\xi})}{(y\xi)^{j/2}}\,\mathrm{d}\xi+O(T^{-A})\tag{2-10}$$

for some constant $J=J(A)$ and

$$H^{-}(y)\ll_{t_f,A}y^{-A}.\tag{2-11}$$

Proof. See, e.g., [Lin and Sun 2021, Section 3.1]. □

Notice that (2-10) and (2-11) are only valid for $y \gg T^{\varepsilon}$. So we also need the facts which state that, for $y > 0$, $k \geq 0$ and $\operatorname{Re} \nu = 0$, one has (see [Kowalski et al. 2002, Lemma C.2])

$$\begin{aligned} y^k J_\nu^{(k)}(y) &\ll_{k,\nu} \frac{1}{(1+y)^{1/2}}, \\ y^k K_\nu^{(k)}(y) &\ll_{k,\nu} \frac{e^{-y}(1+|\log y|)}{(1+y)^{1/2}}. \end{aligned} \tag{2-12}$$

We now recall the Voronoi summation formula for $\mathrm{SL}(3,\mathbb{Z})$. Let ψ be a smooth compactly supported function on $(0,\infty)$, and let $\tilde{\psi}(s) := \int_0^\infty \psi(x) x^s \,\mathrm{d}x/x$ be its Mellin transform. For $\sigma > \frac{5}{14}$, we define

$$\Psi^{\pm}(z) := z \frac{1}{2\pi i} \int_{(\sigma)} (\pi^3 z)^{-s} \gamma_3^{\pm}(s) \tilde{\psi}(1-s) \,\mathrm{d}s, \tag{2-13}$$

with

$$\gamma_3^{\pm}(s) := \prod_{j=1}^{3} \frac{\Gamma((s+\alpha_j)/2)}{\Gamma((1-s-\alpha_j)/2)} \pm \frac{1}{i} \prod_{j=1}^{3} \frac{\Gamma((1+s+\alpha_j)/2)}{\Gamma((2-s-\alpha_j)/2)}, \tag{2-14}$$

where α_j are the Langlands parameters of π as above. Note that changing $\psi(y)$ to $\psi(y/N)$ for a positive real number N has the effect of changing $\Psi^{\pm}(z)$ to $\Psi^{\pm}(zN)$. The Voronoi formula on GL(3) was first proved by Miller and Schmid [2006]. The present version is due to Goldfeld and Li [2006] with slightly renormalized variables; see Blomer [2012, Lemma 3].

Lemma 2.5. *Let $c, d, \bar{d} \in \mathbb{Z}$ with $c \neq 0$, $(c,d) = 1$, and $d\bar{d} \equiv 1 \pmod{c}$. Then we have*

$$\sum_{n=1}^{\infty} A(m,n) e\left(\frac{n\bar{d}}{c}\right) \psi(n) = \frac{c\pi^{3/2}}{2} \sum_{\pm} \sum_{n_1 \mid cm} \sum_{n_2=1}^{\infty} \frac{A(n_2,n_1)}{n_1 n_2} S\left(md, \pm n_2; \frac{mc}{n_1}\right) \Psi^{\pm}\left(\frac{n_1^2 n_2}{c^3 m}\right),$$

where $S(a,b;c) := \sum^{*}_{d(c)} e((ad+b\bar{d})/c)$ is the classical Kloosterman sum.

2D. *The delta method.* There are several oscillatory factors contributing to the convolution sums. Our method is based on separating these oscillations using the circle method. In the present situation we will use a version of the delta method of Duke, Friedlander and Iwaniec. More specifically we will use the expansion (20.157) given in [Iwaniec and Kowalski 2004, Section 20.5]. Let $\delta : \mathbb{Z} \to \{0,1\}$ be defined by

$$\delta(n) = \begin{cases} 1 & \text{if } n = 0; \\ 0 & \text{otherwise.} \end{cases}$$

We seek a Fourier expansion which matches with $\delta(n)$.

Lemma 2.6. *Let Q be a large positive number. Then we have*

$$\delta(n) = \frac{1}{Q} \sum_{1 \leq q \leq Q} \frac{1}{q} \sideset{}{^\star}\sum_{a \bmod q} e\left(\frac{na}{q}\right) \int_{\mathbb{R}} g(q,x) e\left(\frac{nx}{qQ}\right) \mathrm{d}x, \tag{2-15}$$

where $g(q,x)$ is a weight function satisfying that

$$g(q,x) = 1 + O\left(\frac{Q}{q}\left(\frac{q}{Q} + |x|\right)^{A}\right), \qquad g(q,x) \ll |x|^{-A}, \text{ for any } A > 1, \tag{2-16}$$

and

$$\frac{\partial^j}{\partial x^j} g(q,x) \ll |x|^{-j} \min(|x|^{-1}, Q/q) \log Q, \qquad j \geq 1. \tag{2-17}$$

Here the $\star$ *on the sum indicates that the sum over* a *is restricted by the condition* $(a,q)=1$.

Proof. See [Huang 2021b, Lemma 15] and [Iwaniec and Kowalski 2004, Section 20.5]. □

In applications of (2-15), we can first restrict to $|x| \ll Q^{\varepsilon}$. If $q \gg Q^{1-\varepsilon}$, then by (2-17) we get $\frac{\partial^j}{\partial x^j} g(q,x) \ll Q^{\varepsilon}|x|^{-j}$, for any $j \geq 1$. If $q \ll Q^{1-\varepsilon}$ and $Q^{-\varepsilon} \ll |x| \ll Q^{\varepsilon}$, then by (2-17) we also have $\frac{\partial^j}{\partial x^j} g(q,x) \ll Q^{\varepsilon}|x|^{-j}$, for any $j \geq 1$. Finally, if $q \ll Q^{1-\varepsilon}$ and $|x| \ll Q^{-\varepsilon}$, then by (2-16), we can replace $g(q,x)$ by 1 with a negligible error term. So in all cases, we can view $g(q,x)$ as a nice weight function.

We remark that there is no restrictions on Q, so we can choose Q to be any large positive number. Recall that in Sharma [2022] and Lin and Sun [2021], the authors took Q to be $(NL/M)^{1/2}$ and $(N/t^{4/5})^{1/2}$, respectively. This motivates us to choose $Q=(NL/MK)^{1/2}$. As we will see, after balancing finally, we can take $L=M^{1/4}$ and $K=t^{4/5}$ optimally, which coincides with Sharma [2022] and Lin and Sun [2021].

2E. *Oscillatory integrals.* Let $\mathcal{F}$ be an index set and $X = X_T : \mathcal{F} \to \mathbb{R}_{\geq 1}$ be a function of $T \in \mathcal{F}$. A family of $\{w_T\}_{T\in\mathcal{F}}$ of smooth functions supported on a product of dyadic intervals in $\mathbb{R}^d_{>0}$ is called X-inert if for each $j=(j_1,\dots,j_d) \in \mathbb{Z}^d_{\geq 0}$ we have

$$\sup_{T\in\mathcal{F}} \sup_{(x_1,\dots,x_d)\in\mathbb{R}^d_{>0}} X_T^{-j_1-\cdots-j_d} |x_1^{j_1}\cdots x_d^{j_d} w_T^{(j_1,\dots,j_d)}(x_1,\dots,x_d)| \ll_{j_1,\dots,j_d} 1.$$

We will use the following stationary phase lemma several times.

Lemma 2.7. *Suppose* $w=w_T(t)$ *is a family of* X*-inert functions, with compact support on* $[Z,2Z]$, *so that* $w^{(j)}(t) \ll (Z/X)^{-j}$. *Also suppose that* ϕ *is smooth and satisfies* $\phi^{(j)} \ll Y/Z^j$ *for some* $Y/X^2 \geq R \geq 1$ *and all* t *in the support of* w. *Let*

$$I = \int_{-\infty}^{\infty} w(t) e^{i\phi(t)}\, \mathrm{d}t.$$

(i) *If* $|\phi'(t)| \gg Y/Z$ *for all* t *in the support of* w, *then* $I \ll_A ZR^{-A}$ *for* A *arbitrarily large.*

(ii) *If* $|\phi''(t)| \gg Y/Z^2$ *for all* t *in the support of* w, *and there exists* $t_0 \in \mathbb{R}$ *such that* $\phi'(t_0)=0$ (*note that* t_0 *is necessarily unique*), *then*

$$I = \frac{e^{i\phi(t_0)}}{\sqrt{\phi''(t_0)}} F_T(t_0) + O_A(ZR^{-A}),$$

where F_T *is a family of* X*-inert functions* (*depending on* A) *supported on* $t_0 \asymp Z$.

Proof. See [Blomer et al. 2013, Section 8] and [Kıral et al. 2019, Lemma 3.1]. □

3. Reduction

Now we start to prove Theorem 1.1. We assume $t \geq M^{\varepsilon}$. Recall that, Lemma 2.2, we are considering $S(r, N)$ with $N \ll (Mt)^{3+\varepsilon}/r^2$, $r \ll M^{1/8}t^{3/10}$, and $(r, M) = 1$. We will prove the following proposition.

Proposition 3.1. *We have*

$$S(r, N) \ll N^{1/2+\varepsilon} M^{3/2-1/16} t^{3/2-3/20},$$

for $N \ll (Mt)^{3+\varepsilon}/r^2$, $r \ll M^{1/8}t^{3/10}$ *and* $(r, M) = 1$.

Let $\mathcal{L}$ be the set of primes in $[L, 2L]$. Assume $M \notin [L, 2L]$. For $\ell \in \mathcal{L}$ and $n \geq 1$, by the Hecke relation, we have

$$A(1, \ell)A(r, n) = A(r, \ell n) + \delta_{\ell \mid r} A(r/\ell, n) + \delta_{\ell \mid n} A(r\ell, n/\ell).$$

By the prime number theorem for $L(s, \pi \times \tilde{\pi})$ we have

$$L^* := \sum_{\ell \in \mathcal{L}} |A(1, \ell)|^2 \gg L^{1-\varepsilon}.$$

We have

$$\begin{aligned} S(r, N) &= \frac{1}{L^*} \sum_{\ell \in \mathcal{L}} \overline{A(1, \ell)} \sum_{n \geq 1} A(r, n)A(1, \ell)\lambda_f(n)\chi(n)n^{-it} V\left(\frac{n}{N}\right) \\ &= S_1(N) + S_2(N) + S_3(N), \end{aligned}$$

where

$$S_1(N) = \frac{1}{L^*} \sum_{\ell \in \mathcal{L}} \overline{A(1, \ell)} \sum_{n \geq 1} A(r, n\ell)\lambda_f(n)\chi(n)n^{-it} V\left(\frac{n}{N}\right),$$

$$S_2(N) = \frac{1}{L^*} \sum_{\ell \in \mathcal{L}} \overline{A(1, \ell)} \sum_{n \geq 1} \delta_{\ell \mid r} A(r/\ell, n)\lambda_f(n)\chi(n)n^{-it} V\left(\frac{n}{N}\right),$$

and

$$S_3(N) = \frac{1}{L^*} \sum_{\ell \in \mathcal{L}} \overline{A(1, \ell)} \sum_{n \geq 1} \delta_{\ell \mid n} A(r\ell, n/\ell)\lambda_f(n)\chi(n)n^{-it} V\left(\frac{n}{N}\right).$$

We only consider $S_1(N)$, since the same method works for the other two sums and will give better bounds as the lengths of those sums are smaller. Actually, in S_2, since $\ell \mid r$, only $\tau(r)$ ℓ's contribute; in S_3, since $\ell \mid n$, the length of the n-sum is of size N/L. As the structures of sums in S_2 and S_3 are the same as in S_1, we can get better bounds than S_1.

Now we apply $(1/M)\sum_{b \bmod M} e((n - m\ell)b/M)$ to detect the condition $M \mid (n - m\ell)$, and then use the delta method, obtaining

$$\begin{aligned} S_1(N) = \frac{1}{L^*} \sum_{\ell \in \mathcal{L}} \overline{A(1, \ell)} \frac{1}{M} \sum_{b \bmod M} \sum_{n \geq 1} A(r, n) W\left(\frac{n}{\ell N}\right) \cdot \sum_{m \geq 1} \lambda_f(m)\chi(m)m^{-it} V\left(\frac{m}{N}\right) e\left(\frac{(n-m\ell)b}{M}\right) \\ \cdot \frac{1}{Q} \sum_{1 \leq q \leq Q} \frac{1}{q} \sideset{}{^\star}\sum_{a \bmod q} e\left(\frac{(n-m\ell)a}{Mq}\right) \int_{\mathbb{R}} g(q, x) e\left(\frac{(n-m\ell)x}{MqQ}\right) \mathrm{d}x. \end{aligned}$$

Rearranging the order of the sums and integrals we get

$$S_1(N) = \frac{1}{L^*}\sum_{\ell\in\mathcal{L}} \overline{A(1,\ell)}\frac{1}{M}\sum_{b \bmod M}\frac{1}{Q}\sum_{1\le q\le Q}\int_{\mathbb{R}} g(q,x)\frac{1}{q}\sideset{}{^\star}\sum_{a \bmod q} \cdot \sum_{n\ge 1} A(r,n) e\Big(\frac{n(bq+a)}{Mq}\Big) W\Big(\frac{n}{\ell N}\Big) e\Big(\frac{nx}{pqQ}\Big) \cdot \sum_{m\ge 1}\lambda_f(m)\chi(m)m^{-it} e\Big(\frac{-m\ell(bq+a)}{Mq}\Big) V\Big(\frac{m}{N}\Big) e\Big(\frac{-m\ell x}{MqQ}\Big)\,\mathrm{d}x.$$

Inserting a smooth partition of unity for the x-integral and a dyadic partition for the q-sum, we get

$$S_1(N) \ll N^{\varepsilon} \sup_{t^{-B}\ll X\ll t^{\varepsilon}} \sup_{1\ll R\ll Q} \sum_{1\le j\le 3} |S_{1j}^{\pm}(N,X,R)| + O(t^{-A}),$$

for any large constant $A > 0$ and some large constant $B > 0$ depending on A, where $S_{11}^{\pm}(N,X,R)$, $S_{12}^{\pm}(N,X,R)$ and $S_{13}^{\pm}(N,X,R)$ denote the terms with $(b,M) = 1$, $M \mid b$ and $(q,\ell M) > 1$, respectively. More precisely, we have

$$S_{11}^{\pm}(N,X,R)j = \frac{1}{L^*}\sum_{\ell\in\mathcal{L}} \overline{A(1,\ell)}\int_{\mathbb{R}}\frac{1}{M}\sideset{}{^\star}\sum_{b \bmod M}\frac{1}{Q}\sum_{\substack{q\sim R\\(q,\ell M)=1}}\frac{1}{q}\sideset{}{^\star}\sum_{a \bmod q} g(q,x)U\Big(\frac{\pm x}{X}\Big) \cdot \sum_{n\ge 1} A(r,n) e\Big(\frac{n(aM+bq)}{qM}\Big) W\Big(\frac{n}{\ell N}\Big) e\Big(\frac{nx}{MqQ}\Big) \cdot \sum_{m\ge 1}\lambda_f(m)\chi(m) e\Big(\frac{-m\ell(aM+bq)}{qM}\Big) m^{-it} V\Big(\frac{m}{N}\Big) e\Big(\frac{-m\ell x}{MqQ}\Big)\,\mathrm{d}x, \tag{3-1}$$

$$S_{12}^{\pm}(N,X,R) = \frac{1}{L^*}\sum_{\ell\in\mathcal{L}} \overline{A(1,\ell)}\int_{\mathbb{R}}\frac{1}{M}\frac{1}{Q}\sum_{\substack{q\sim R\\(q,\ell M)=1}}\frac{1}{q}\sideset{}{^\star}\sum_{a \bmod q} g(q,x)U\Big(\frac{\pm x}{X}\Big) \cdot \sum_{n\ge 1} A(r,n) e\Big(\frac{na}{q}\Big) W\Big(\frac{n}{\ell N}\Big) e\Big(\frac{nx}{MqQ}\Big) \cdot \sum_{m\ge 1}\lambda_f(m)\chi(m) e\Big(\frac{-m\ell a}{q}\Big) m^{-it} V\Big(\frac{m}{N}\Big) e\Big(\frac{-m\ell x}{MqQ}\Big)\,\mathrm{d}x,$$

and

$$S_{13}^{\pm}(N,X,R) = \frac{1}{L^*}\sum_{\ell\in\mathcal{L}} \overline{A(1,\ell)}\int_{\mathbb{R}}\frac{1}{M}\sum_{b \bmod M}\frac{1}{Q}\sum_{\substack{q\sim R\\(q,\ell M)>1}}\frac{1}{q}\sideset{}{^\star}\sum_{a \bmod q} g(q,x)U\Big(\frac{\pm x}{X}\Big) \cdot \sum_{n\ge 1} A(r,n) e\Big(\frac{n(a+bq)}{qM}\Big) W\Big(\frac{n}{\ell N}\Big) e\Big(\frac{nx}{MqQ}\Big) \cdot \sum_{m\ge 1}\lambda_f(m)\chi(m) e\Big(\frac{-m\ell(a+bq)}{qM}\Big) m^{-it} V\Big(\frac{m}{N}\Big) e\Big(\frac{-m\ell x}{MqQ}\Big)\,\mathrm{d}x.$$

Note that in $S_{11}^{\pm}(N,X,R)$ and $S_{12}^{\pm}(N,X,R)$, we have made a change of variable $a \to aM$. Here U is a fixed compactly supported 1-inert function with $\operatorname{supp} U \subset (0,\infty)$. We will only give details for the treatment of $S_{11}^{\pm}(N,X,R)$, since the same method works for $S_{12}^{\pm}(N,X,R)$ and $S_{13}^{\pm}(N,X,R)$ and will give a better upper bound. More precisely, in $S_{12}^{\pm}(N,X,R)$, we do not have the b-sum. In $S_{13}^{\pm}(N,X,R)$, we have the condition $(q,\ell M)>1$. In fact, we should have the following cases:

(i) $b \equiv 0 \bmod M$ and $q=\ell^j q'$ with $j \geq 1$ and $(q',\ell M)=1$.

(ii) $b \equiv 0 \bmod M$ and $q=M^k q'$ with $k \geq 1$ and $(q',\ell M)=1$.

(iii) $b \equiv 0 \bmod M$ and $q=\ell^j M^k q'$ with $j,k \geq 1$ and $(q',\ell M)=1$.

(iv) $(b,M)=1$ and $q=\ell^j q'$ with $j \geq 1$ and $(q',\ell M)=1$.

(v) $(b,M)=1$ and $q=M^k q'$ with $k \geq 1$ and $(q',\ell M)=1$.

(vi) $(b,M)=1$ and $q=\ell^j M^k q'$ with $j,k \geq 1$ and $(q',\ell M)=1$.

4. Applying Voronoi

We first apply the Voronoi summation formula (see Lemma 2.5) to the sum over n in $S_{11}^{\pm}(N,X,R)$, getting

$$\sum_{n\geq 1} A(r,n) e\left(\frac{n(bq+aM)}{qM}\right) W\left(\frac{n}{\ell N}\right) e\left(\frac{nx}{MqQ}\right)$$
$$= qM \sum_{\eta_1=\pm 1} \sum_{n_1 \mid qMr} \sum_{n_2=1}^{\infty} \frac{A(n_1,n_2)}{n_1 n_2} S(r\overline{(aM+bq)}, \eta_1 n_2; qMr/n_1) \Psi_x^{\operatorname{sgn}(\eta_1)}\left(\frac{n_1^2 n_2}{q^3 M^3 r}\right), \tag{4-1}$$

where $\Psi_x^{\operatorname{sgn}(\eta_1)}(z)$ is defined as in Lemma 2.5 with $\psi(y)$ replaced by $W(y/\ell N)e(xy/MqQ)$.

Lemma 4.1. (i) *If $zNL \gg t^{\varepsilon}$, then $\Psi_x^{\eta_1}(z)$ is negligibly small unless $\operatorname{sgn}(x) = -\operatorname{sgn}(\eta_1)$ and $N\ell(-\eta_1 x)/(MqQ) \asymp (zN\ell)^{1/3}$, in which case we have*

$$\Psi_x^{\operatorname{sgn}(\eta_1)}(z) = (zN\ell)^{1/2} e\left(\eta_1 \frac{2(zMqQ)^{1/2}}{(-\eta_1 x)^{1/2}}\right) \mathcal{W}\left(\frac{z^{1/2}(MqQ)^{3/2}}{N\ell(-\eta_1 x)^{3/2}}\right) + O(t^{-A}),$$

where $\mathcal{W}$ is a certain compactly supported 1-inert function depending on A.

(ii) *If $zNL \ll t^{\varepsilon}$ and $(NLX)/(MRQ) \gg t^{\varepsilon}$, then $\Psi_x^{\operatorname{sgn}(\eta_1)}(z) \ll t^{-A}$.*

(iii) *If $zNL \ll t^{\varepsilon}$ and $(NLX)/(MRQ) \ll t^{\varepsilon}$, then $\Psi_x^{\operatorname{sgn}(\eta_1)}(z) \ll t^{\varepsilon}$.*

Proof. See [Huang 2021b, 5.3]. □

In the last case, by taking $\sigma = \frac{1}{2}$ and making a change of variable, we get

$$\Psi_x^{\pm}(z) = (z\ell N)^{1/2} \frac{1}{2\pi^{5/2}} \int_{\mathbb{R}} (\pi^3 z\ell N)^{-i\tau} \gamma_3^{\pm}(1/2+i\tau) \int_0^{\infty} W(\xi) e\left(\frac{x\ell N\xi}{MqQ}\right) \xi^{-1/2-i\tau}\, d\xi\, d\tau.$$

We can truncate τ at $\tau \ll t^{\varepsilon}$ with a negligibly small error by repeated integration by parts for the ξ-integral above. That is, we have

$$\Psi_x^{\pm}(z) = (z\ell N)^{1/2} W_{x,\ell}^{\pm}(z) + O(t^{-A}), \tag{4-2}$$

where

$$W_{x,\ell}^{\pm}(z) = \frac{1}{2\pi^{5/2}} \int_{|\tau|\le t^{\varepsilon}} (\pi^3 z\ell N)^{-i\tau} \gamma_3^{\pm}(1/2+i\tau) \int_0^{\infty} W(\xi) e\Big(\frac{x\ell N\xi}{MqQ}\Big) \xi^{-1/2-i\tau}\, \mathrm{d}\xi\, \mathrm{d}\tau.$$

The contribution from the error to $S_{11}^{\pm}(N, X, R)$ is also negligibly small. Note that the function $W_{x,\ell}^{\pm}(z)$ satisfies that

$$\frac{\partial^j}{\partial z^j} W_{x,\ell}^{\pm}(z) \ll_j t^{\varepsilon} z^{-j}. \tag{4-3}$$

Now we consider the m-sum. By

$$\chi(m) = \bar{\chi}(\ell)\chi(m\ell) = \frac{\bar{\chi}(\ell)}{\tau(\bar{\chi})} \sum_{u \bmod M} \bar{\chi}(u) e\Big(\frac{um\ell}{M}\Big),$$

one has

$$\begin{aligned}\sum_{m\ge 1} \lambda_f(m)\chi(m) m^{-it} e\Big(\frac{-m\ell(bq+aM)}{Mq}\Big) V\Big(\frac{m}{N}\Big) e\Big(\frac{-m\ell x}{MqQ}\Big) \\ = \frac{1}{\tau(\bar{\chi})} \sum_{m\ge 1} \lambda_f(m) m^{-it} V\Big(\frac{m}{N}\Big) e\Big(-\frac{m\ell x}{MqQ}\Big) \\ \cdot \Bigg(\sum_{\substack{u \bmod M\\ u\not\equiv b \bmod M}} \bar{\chi}(u\ell) \Big(e\Big(-\frac{m\ell(aM+(b-u)q)}{Mq}\Big) + e\Big(-\frac{m\ell a}{q}\Big)\Big)\Bigg) \\ =: \Sigma_1 + \Sigma_2,\end{aligned}$$

say. From now on, we only deal with the terms involving Σ_1, since the treatment of Σ_2 is similar and in fact simpler. With the help of Lemma 2.4, we obtain

$$\Sigma_1 = \frac{N^{1-it}}{Mq\tau(\bar{\chi})} \sum_{\substack{u \bmod M\\ u\not\equiv b \bmod M}} \bar{\chi}(u\ell) \sum_{\pm} \sum_{m\ge 1} \lambda_f(m) e\Big(\pm \frac{m\overline{\ell(aM+(b-u)q)}}{Mq}\Big) H^{\pm}\Big(\frac{mN}{M^2q^2}\Big), \tag{4-4}$$

where $H^{\pm}$ is defined as in Lemma 2.4 with $g(\xi)$ replaced by $V(\xi)\xi^{-it} e(-N\ell x\xi/MqQ)$.

Lemma 4.2. *If $z \ll t^{\varepsilon}$, then $H^{\pm}(z)$ is negligible unless $t \asymp (N\ell X)/(MqQ)$ and $x < 0$.*

Proof. If $z \ll t^{\varepsilon}$, then, in view of (2-8) and (2-9), we may regard $H^{\pm}(z)$ as

$$\mathcal{I}(z) := \int_0^{\infty} V(\xi) e\Big(-\frac{t\log\xi}{2\pi} - \frac{N\ell x\xi}{MqQ}\Big) J_f(z\xi)\, \mathrm{d}\xi, \tag{4-5}$$

where $J_f(z) = (-\pi/\sin(\pi i t_f))(J_{2it_f}(4\pi\sqrt{z}) - J_{-2it_f}(4\pi\sqrt{z}))$ or $J_f(z) = 4\epsilon_f \cosh(\pi t_f) K_{2it_f}(4\pi\sqrt{z})$. Then, by partial integration together with (2-12), $\mathcal{I}_1(z)$ is negligible unless $x < 0$ and $(NLX)/(MRQ) \asymp t$. $\square$

If $mN/M^2q^2 \gg t^\varepsilon$, then, in view of (2-11), $H^-(mN/M^2q^2)$ is negligible. For the term in (4-4) involving H^+, with the help of (2-10), we may replace it by

$$\frac{N^{3/4-it}}{M^{1/2}q^{1/2}\tau(\overline{\chi})}\sum_{\substack{u \bmod M\\ u\neq b}}\overline{\chi}(u\ell)\sum_{\eta_2=\pm1}\sum_{m\geq1}\frac{\lambda_f(m)}{m^{1/4}}e\biggl(\frac{m\overline{\ell(aM+(b-u)q)}}{Mq}\biggr)$$
$$\cdot\int_{\mathbb{R}}\xi^{-1/4}V(\xi)e\biggl(-\frac{t\log\xi}{2\pi}+\eta_2\frac{2\sqrt{mN\xi}}{Mq}-\frac{N\ell x\xi}{MqQ}\biggr)\,d\xi. \tag{4-6}$$

Note that we have $\ell \asymp L$, $|x| \asymp X$ and $q \asymp R$. By Lemma 4.1 and Lemma 4.2 and according to the size of $(N\ell x)/(MqQ)$, $(n_1^2n_2N\ell)/(q^3M^3r)$ and $(mN)/(M^2q^2)$, we can reduce $S_1^\pm(N,X,R)$ to the following three cases:

Case a.
$$\frac{NLX}{MRQ} \asymp \biggl(\frac{n_1^2n_2NL}{R^3M^3r}\biggr)^{1/3} \gg t^\varepsilon, \qquad \frac{mN}{M^2R^2} \gg t^\varepsilon.$$

In this case, we insert (4-1) and (4-4) into (3-1) and use Lemma 4.1(i) and (4-6), so that it is sufficient to estimate

$$\frac{N^{5/4-it}}{\tau(\overline{\chi})M^2LQr^{1/2}}\sum_{\ell\in\mathcal{L}}\overline{A(1,\ell)\chi(\ell)}\ell^{1/2}\sideset{}{^\star}\sum_{b \bmod M}\sum_{\substack{q\sim R\\(q,\ell M)=1}}\frac{1}{q^2}\sideset{}{^\star}\sum_{a \bmod q}\sum_{\substack{u \bmod M\\u\neq b}}\overline{\chi}(u)$$
$$\cdot\sum_{m\geq1}\frac{\lambda_f(m)}{m^{1/4}}e\biggl(\frac{m\overline{\ell(aM+(b-u)q)}}{Mq}\biggr)\sum_{\eta_1,\eta_2=\pm1}\sum_{n_1\mid qMr}\sum_{n_2\asymp\frac{N_0}{n_1^2}}\frac{A(n_1,n_2)}{n_2^{1/2}}$$
$$\cdot S(r\overline{(aM+bq)},\eta_1n_2;qMr/n_1)\int_{\mathbb{R}}\xi^{-1/4}V(\xi)e\biggl(-\frac{it\log\xi}{2\pi}+\eta_2\frac{2\sqrt{mN\xi}}{Mq}\biggr)$$
$$\cdot\int_{\mathbb{R}}g(q,x)e\biggl(-\frac{N\ell x\xi}{MqQ}+\eta_1\frac{2(n_1^2n_2Q)^{1/2}}{Mq((-\eta_1rx))^{1/2}}\biggr)\mathcal{W}\biggl(\frac{Q^{3/2}(n_1^2n_2)^{1/2}}{r^{1/2}(-\eta_1x)^{3/2}N\ell}\biggr)U\biggl(\frac{-\eta_1x}{X}\biggr)\,dx\,d\xi, \tag{4-7}$$

where $N_0 = N^2L^2X^3r/Q^3$. Let $x = -\eta_1Xv$. Then the resulting x-integral becomes

$$-\eta_1X\int_{\mathbb{R}}e\biggl(\eta_1\frac{N\ell X\xi v}{MqQ}+\eta_1\frac{2(n_1^2n_2Q)^{1/2}}{Mq(rXv)^{1/2}}\biggr)g(q,-\eta_1Xv)U(v)W\biggl(\frac{Q^{3/2}(n_1^2n_2)^{1/2}}{r^{1/2}(Xv)^{3/2}N\ell}\biggr)\,dv. \tag{4-8}$$

Let

$$h(v) = \eta_1\frac{N\ell X\xi v}{MqQ}+\eta_1\frac{2(n_1^2n_2Q)^{1/2}}{Mq(rXv)^{1/2}}.$$

Then

$$h'(v) = \eta_1\frac{N\ell X\xi}{MqQ}-\eta_1\frac{(n_1^2n_2Q)^{1/2}}{Mq(rX)^{1/2}}v^{-3/2}, \qquad h''(v) = \eta_1\frac{3(n_1^2n_2Q)^{1/2}}{2Mq(rX)^{1/2}}v^{-5/2}. \tag{4-9}$$

Note that the solution of $h'(v_0)=0$ is $v_0 = (n_1^2n_2)^{1/3}Q/(r^{1/3}(N\ell\xi)^{2/3}X) \asymp 1$, and

$$h(v_0) = \eta_1\frac{3(n_1^2n_2N\ell\xi)^{1/3}}{r^{1/3}Mq}, \qquad h''(v_0) = \frac{3\eta_1}{2v_0^2}\cdot\frac{(n_1^2n_2Q)^{1/2}}{Mq(rXv_0)^{1/2}} = \frac{3\eta_1}{2v_0^2}\cdot\frac{(n_1^2n_2N\ell\xi)^{1/3}}{r^{1/3}Mq}.$$

By the argument below Lemma 2.6, we can think $g(q,x)$ as a nice function which satisfies

$$\frac{\partial^j}{\partial x^j} g(q,x) \ll Q^{\varepsilon_1}|x|^{-j}, \tag{4-10}$$

up to a negligible error. Here ε_1 is a small positive number such that $t^{\varepsilon}/Q^{2\varepsilon_1} \gg t^{\varepsilon/2}$. Then, by applying Lemma 2.7, we have (4-8) is equal to

$$\frac{r^{1/6}(qM)^{1/2}X}{(n_1^2 n_2 N\ell\xi)^{1/6}} e\left(\eta_1 \frac{3(n_1^2 n_2 N\ell\xi)^{1/3}}{r^{1/3}Mq}\right) g(q,-\eta_1 X v_0)\mathcal{U}(v_0) W\left(\frac{Q^{3/2}(n_1^2 n_2)^{1/2}}{r^{1/2}(Xv_0)^{3/2}N\ell}\right) + O(t^{-A}),$$

where $\mathcal{U}$ is a certain compactly supported 1-inert function depending on A. We may assume $(n_1, M)=1$, since otherwise we have $M \mid n_1$ which leads to a simpler case. Hence, by letting

$$\mathcal{V}(\xi) = \xi^{-5/12} V(\xi) g(q,-\eta_1 X v_0)\mathcal{U}(v_0) W\left(\frac{Q^{3/2}(n_1^2 n_2)^{1/2}}{r^{1/2}(Xv_0)^{3/2}N\ell}\right),$$

at the cost of a negligible error, we can rewrite (4-7) as

$$\frac{N^{13/12-it}X}{\tau(\bar{\chi})M^{3/2}LQr^{1/3}} \sum_{\ell\in\mathcal{L}} \overline{A(1,\ell)\chi(\ell)}\ell^{1/3} \sum_{\substack{q\sim R\\(q,\ell M)=1}} \frac{1}{q^{3/2}}$$
$$\cdot \sum_{\eta_1,\eta_2=\pm1} \sum_{n_1\mid qr} \frac{1}{n_1^{1/3}} \sum_{n_2 \asymp \frac{N_0}{n_1^2}} \frac{A(n_1,n_2)}{n_2^{2/3}} \sum_{m\geq 1} \frac{\lambda_f(m)}{m^{1/4}} \mathcal{C}(m,n_1,n_2,\ell,q)\mathcal{J}_{\boldsymbol{a}}(m,n_1,n_2,\ell,q), \tag{4-11}$$

where

$$\mathcal{J}_{\boldsymbol{a}}(m,n_1,n_2,\ell,q) = \int_{\mathbb{R}} \mathcal{V}(\xi) e\left(-\frac{t}{2\pi}\log\xi + \eta_1 \frac{3(n_1^2 n_2 N\ell\xi)^{1/3}}{r^{1/3}Mq} + \eta_2 \frac{2\sqrt{mN\xi}}{Mq}\right) \mathrm{d}\xi,$$

and

$$\mathcal{C}(m,n_1,n_2,\ell,q) = \sideset{}{^\star}\sum_{b \bmod M} \sideset{}{^\star}\sum_{a \bmod q} S(r\overline{(aM+bq)}, \eta_1 n_2, qMr/n_1)$$
$$\cdot \sum_{\substack{u \bmod M\\ u\neq b}} \bar{\chi}(u) e\left(\frac{m\overline{\ell(aM+(b-u)q)}}{Mq}\right). \tag{4-12}$$

By partial integration, one can truncate the m-sum at

$$m \ll \max\{t^2R^2M^2/N, NL^2X^2/Q^2\}.$$

We have

$$\mathcal{C}(m,n_1,n_2,\ell,q) = \sideset{}{^\star}\sum_{\alpha \bmod qMr/n_1} f(\alpha, m\bar{\ell}, q)\tilde{S}(\alpha, m\bar{\ell}, q) e\left(\eta_1 \frac{\bar{\alpha} n_1 n_2}{qMr}\right), \tag{4-13}$$

where

$$\tilde{S}(\alpha,m,q) = \sideset{}{^\star}\sum_{b \bmod M} \sum_{\substack{u \bmod M\\ u\neq b}} \bar{\chi}(u) e\left(\frac{\bar{q}^2(n_1\alpha\bar{b} + m\overline{(b-u)})}{M}\right),$$

and

$$f(\alpha, m, q) = \sum_{\substack{d \mid q \\ n_1\alpha \equiv -m \pmod d}} d\mu(q/d).$$

Case b. $$\frac{NLX}{MRQ} \asymp \left(\frac{n_1^2 n_2 NL}{R^3 M^3 r}\right)^{1/3} \asymp t, \qquad \frac{mN}{M^2R^2} \ll t^{\varepsilon}.$$

In this case, we replace $H^{\pm}(z)$ by $\mathcal{I}(z)$ as defined in (4-5). Hence, we are led to estimate

$$\begin{aligned}
&\frac{N^{3/2-it}}{\tau(\overline{\chi}) M^{5/2} L Q r^{1/2}} \sum_{\ell \in \mathcal{L}} \overline{A(1,\ell)\chi(\ell)} \ell^{1/2} \sideset{}{^\star}\sum_{b \bmod M} \sum_{\substack{q \sim R \\ (q,\ell M)=1}} \frac{1}{q^{5/2}} \sideset{}{^\star}\sum_{a \bmod q} \sum_{\substack{u \bmod M \\ u \neq b}} \overline{\chi}(u) \\
&\quad \cdot \sum_{m \geq 1} \frac{\lambda_f(m)}{m^{1/4}} e\left(\frac{m\overline{\ell(aM+(b-u)q)}}{Mq}\right) \sum_{\eta_1 = \pm 1} \sum_{n_1 \mid qMr} \sum_{n_2 \asymp N_0/n_1^2} \frac{A(n_1,n_2)}{n_2^{1/2}} \\
&\quad \cdot S(r\overline{(aM+bq)}, \eta_1 n_2; qMr/n_1) \int_{\mathbb{R}} \xi^{-1/4} V(\xi) J_f\left(\frac{mN\xi}{M^2q^2}\right) e\left(-\frac{it\log\xi}{2\pi} Mq\right) \\
&\quad \cdot \int_{\mathbb{R}} g(q,x) e\left(-\frac{N\ell x\xi}{MqQ} + \eta_1 \frac{2(n_1^2 n_2 Q)^{1/2}}{Mq((-\eta_1 r x))^{1/2}}\right) \mathcal{W}\left(\frac{Q^{3/2}(n_1^2 n_2)^{1/2}}{r^{1/2}(-\eta_1 x)^{3/2} N\ell}\right) U\left(\frac{-\eta_1 x}{X}\right) \mathrm{d}x\, \mathrm{d}\xi.
\end{aligned}$$

By doing a similar treatment as in Case a, one can equate the above with (up to a negligible error and another term with $M \mid n_1$)

$$\begin{aligned}
&\frac{N^{4/3-it} X}{\tau(\overline{\chi}) M^2 L Q r^{1/3}} \sum_{\ell \in \mathcal{L}} \overline{A(1,\ell)\chi(\ell)} \ell^{1/3} \sum_{\substack{q \sim R \\ (q,\ell M)=1}} \frac{1}{q^2} \\
&\quad \cdot \sum_{\eta_1,\eta_2 = \pm 1} \sum_{n_1 \mid qr} \frac{1}{n_1^{1/3}} \sum_{n_2 \asymp N_0/n_1^2} \frac{A(n_1,n_2)}{n_2^{2/3}} \sum_{m \geq 1} \frac{\lambda_f(m)}{m^{1/4}} \mathcal{C}(m,n_1,n_2,\ell,q) \mathcal{J}_{\boldsymbol{b}}(m,n_1,n_2,\ell,q),
\end{aligned} \tag{4-14}$$

where $\mathcal{C}$ is defined as in (4-12) and

$$\mathcal{J}_{\boldsymbol{b}}(m,n_1,n_2,\ell,q) = \int_{\mathbb{R}} \xi^{-1/4} V(\xi) J_f\left(\frac{mN\xi}{M^2q^2}\right) e\left(-\frac{t}{2\pi}\log\xi + \eta_1 \frac{3(n_1^2 n_2 N\ell\xi)^{1/3}}{r^{1/3} Mq}\right) \mathrm{d}\xi. \tag{4-15}$$

Case c. $$\frac{n_1^2 n_2}{R^3 M^3 r} LN \ll t^{\varepsilon}, \qquad \frac{NLX}{MRQ} \ll t^{\varepsilon}, \qquad \frac{mN}{M^2R^2} \gg t^{\varepsilon}.$$

Since $(NLX)/(MRQ) \ll t^{\varepsilon}$, we first deal with the ξ-integral in (4-6). Making a change of variable $\xi \rightsquigarrow \xi^2$, we have

$$\mathcal{J}_{\boldsymbol{c}}(m,\ell,q) = 2\int_{\mathbb{R}} \xi^{-1/2} V(\xi^2) e\left(-\frac{N\ell x\xi^2}{MqQ}\right) e\left(-\frac{t\log\xi}{\pi} + \eta_2 \frac{2\sqrt{mN}}{Mq}\xi\right) \mathrm{d}\xi.$$

Let

$$h(\xi) = -\frac{t\log\xi}{\pi} + \eta_2 \frac{2\sqrt{mN}}{Mq}\xi.$$

Then we have

$$h'(\xi)=-\frac{t}{\pi\xi}+\eta_2\frac{2\sqrt{mN}}{Mq},\quad h''(\xi)=\frac{t}{\pi\xi^2},\quad h^{(j)}(\xi)\asymp_j t,\quad j\geq 2.$$

Note that

$$\frac{t}{1+(NLX/MRQ)^2}\gg t^{1-\varepsilon}.$$

Hence, by Lemma 2.7, the integral is negligibly small unless $mN/(M^2R^2)\asymp t$ and $\eta_2=1$, in which case we have the stationary phase point $\xi_0=tMq/(2\pi\sqrt{mN})$ and

$$\mathcal{J}_{\mathfrak{c}}(m,\ell,q)=\frac{1}{t^{1/2}}e\left(-\frac{t}{\pi}\log\frac{tMq}{2\pi e\sqrt{mN}}\right)V_{x,\ell}\left(\frac{tMq}{\sqrt{mN}}\right)+O(t^{-A}),$$

where $V_{x,\ell}$ is a t^{ε}-inert function.

Together with (4-1) and (4-6), we have $S_{11}^{\pm}(N,X,R)$ is equal to (up to a negligibly small error term and another term with $u=b$)

$$\begin{aligned}\frac{1}{L^*}\sum_{\ell\in\mathcal{L}}\overline{A(1,\ell)}\int_{\mathbb{R}}\frac{1}{M}\sideset{}{^\star}\sum_{b \bmod M}\frac{1}{Q}\sum_{\substack{q\sim R\\(q,\ell M)=1}}\frac{1}{q}\sideset{}{^\star}\sum_{a \bmod q}g(q,x)U\left(\frac{\pm x}{X}\right)qM\sum_{\eta_1=\pm1}\sum_{n_1\mid qMr}\\
\cdot\sum_{n_2=1}^{\infty}\frac{A(n_1,n_2)}{n_1n_2}S(r\overline{(aM+bq)},\eta_1n_2;qMr/n_1)\left(\frac{n_1^2n_2\ell N}{q^3M^3r}\right)^{1/2}W_{x,\ell}^{\operatorname{sgn}(\eta_1)}\left(\frac{n_1^2n_2}{q^3M^3r}\right)\\
\cdot\frac{N^{3/4-it}}{M^{1/2}q^{1/2}\tau(\overline{\chi})}\sum_{\substack{u \bmod M\\u\neq b}}\overline{\chi}(u\ell)\sum_{m\geq1}\frac{\lambda_f(m)}{m^{1/4}}e\left(\frac{m\overline{\ell(aM+(b-u)q)}}{Mq}\right)\\
\cdot\frac{1}{t^{1/2}}e\left(-\frac{t}{\pi}\log\frac{tMq}{2\pi e\sqrt{mN}}\right)V_{x,\ell}\left(\frac{tMq}{\sqrt{mN}}\right)\mathrm{d}x.\end{aligned}$$

We assume $(n_1,M)=1$, since otherwise we have $M\mid n_1$ which leads to a simpler case. Rearranging the sums, inserting a dyadic partition for the n_2-sum, and estimating the x-integral trivially, the above is bounded by

$$N^{\varepsilon}\sup_{1\ll N_0\ll(R^3M^3r/LN)t^{\varepsilon}}\sup_{x\asymp X}|S_{11}^{\pm}(N,X,R,N_0)|,$$

where

$$\begin{aligned}S_{11}^{\pm}(N,X,R,N_0)=\frac{N^{5/4}X}{M^{5/2}LQr^{1/2}}\frac{1}{t^{1/2}}\sum_{\eta_1=\pm1}\sum_{n_1\leq Rr}\sum_{n_2\asymp N_0/n_1^2}\frac{A(n_1,n_2)}{n_2^{1/2}}\sum_{\ell\in\mathcal{L}}\overline{A(1,\ell)\chi(\ell)}\ell^{1/2}\\
\cdot\sum_{\substack{q\sim R\\n_1\mid qr\\(q,\ell M)=1}}\frac{1}{q^{2+2it}}\sum_{m\asymp R^2M^2t^2/N}\frac{\lambda_f(m)}{m^{1/4-it}}\mathcal{C}(m,n_1,n_2,\ell,q)W_{x,\ell}^{\operatorname{sgn}(\eta_1)}\left(\frac{n_1^2n_2}{q^3M^3r}\right)V_{x,\ell}\left(\frac{tMq}{\sqrt{mN}}\right),\end{aligned}$$

and $\mathcal{C}$ is defined as in (4-12).

5. Applying Cauchy and Poisson

5A. *Case a.* In this subsection, we assume Case a. Write

$$q = q_1 q_2 \qquad \text{with } q_1 \mid (rn_1)^\infty \text{ and } (q_2, rn_1) = 1,$$

then we have

$$\begin{aligned}(4\text{-}11) \ll \frac{N^{13/12+\varepsilon}X}{M^2LQr^{1/3}} \sum_{\eta_1,\eta_2=\pm 1} \sum_{n_1 \ll Rr} \frac{1}{n_1^{1/3}} \sum_{(n_1/(n_1,r)) \mid q_1 \mid (rn_1)^\infty} \frac{1}{q_1^{3/2}} \sum_{n_2 \asymp N_0/n_1^2} \frac{|A(n_1,n_2)|}{n_2^{2/3}} \\ \cdot \Bigg| \sum_{\substack{\ell \in \mathcal{L} \\ (\ell,q_1)=1}} \overline{A(1,\ell)\chi(\ell)} \ell^{1/3} \sum_{\substack{q_2 \sim R/q_1 \\ (q_2, rn_1\ell M)=1}} \frac{1}{q_2^{3/2}} \sum_{m \ll \max\{t^2R^2M^2/N, NL^2X^2/Q^2\}} \frac{\lambda_f(m)}{m^{1/4}} \\ \cdot \mathcal{C}(m,n_1,n_2,\ell,q_1q_2)\mathcal{J}_{\boldsymbol{a}}(m,n_1,n_2,\ell,q_1q_2)\Bigg|.\end{aligned}$$

Now we use the Cauchy–Schwarz inequality and (2-5) to get

$$\ll \frac{N^{3/4+\varepsilon}X^{1/2}}{M^2L^{4/3}Q^{1/2}r^{1/2}} \sum_{\eta_1,\eta_2=\pm 1} \sup_{M_1 \ll \max\{t^2R^2M^2/N, NL^2X^2/Q^2\}} \sum_{n_1 \ll Rr} n_1^{\theta_3} \sum_{(n_1/(n_1,r)) \mid q_1 \mid n_1^\infty} \frac{1}{q_1^{3/2}} \Omega_{\boldsymbol{a}}^{1/2}, \tag{5-1}$$

where

$$\Omega_{\boldsymbol{a}} = \sum_{n_2 \asymp N_0/n_1^2} \Bigg| \sum_{\substack{\ell \in \mathcal{L} \\ (\ell,q_1)=1}} \overline{A(1,\ell)\chi(\ell)} \ell^{1/3} \sum_{\substack{q_2 \sim R/q_1 \\ (q_2, rn_1\ell M)=1}} \frac{1}{q_2^{3/2}} \sum_{m \sim M_1} \frac{\lambda_f(m)}{m^{1/4}} \mathcal{C}(m,n_1,n_2,\ell,q_1q_2)\mathcal{J}_{\boldsymbol{a}}(m,n_1,n_2,\ell,q_1q_2)\Bigg|^2.$$

Opening the absolute square, we get

$$\begin{aligned}\Omega_{\boldsymbol{a}} \ll \sum_{n_2 \geq 1} W\left(\frac{n_1^2 n_2}{N_0}\right) \sum_{\substack{\ell \in \mathcal{L} \\ (\ell\ell',q_1)=1}} \sum_{\ell' \in \mathcal{L}} \overline{A(1,\ell)\chi(\ell)} A(1,\ell')\chi(\ell')(\ell\ell')^{1/3} \\ \cdot \sum_{m \sim M_1} \frac{\lambda_f(m)}{m^{1/4}} \sum_{m' \sim M_1} \frac{\lambda_f(m')}{m'^{1/4}} \sum_{\substack{q_2 \sim R/q_1 \\ (q_2,\ell)=1 \\ (q_2q_2', rn_1M)=1}} \sum_{\substack{q_2' \sim R/q_1 \\ (q_2',\ell')=1}} \frac{1}{(q_2q_2')^{3/2}} \\ \cdot \mathcal{C}(m,n_1,n_2,\ell,q_1q_2)\mathcal{J}_{\boldsymbol{a}}(m,n_1,n_2,\ell,q_1q_2)\overline{\mathcal{C}(m',n_1,n_2,\ell',q_1q_2')}\,\overline{\mathcal{J}_{\boldsymbol{a}}(m',n_1,n_2,\ell',q_1q_2')},\end{aligned}$$

where W is supported on $[1,2]$ and satisfies $W^{(j)}(x) \ll 1$. We apply the Poisson summation formula on n_2, getting

$$\Omega_{\boldsymbol{a}} \ll \frac{N_0 q_1^3 L^{2/3}}{n_1^2 M_1^{1/2} R^3} \sum_{\substack{\ell\in\mathcal{L} \\ (\ell\ell', q_1)=1}} \sum_{\ell'\in\mathcal{L}} |A(1,\ell)A(1,\ell')| \sum_{m\sim M_1} \sum_{m'\sim M_1} |\lambda_f(m)||\lambda_f(m')| \cdot \sum_{\substack{q_2\sim R/q_1 \\ (q_2,\ell)=1}} \sum_{\substack{q_2'\sim R/q_1 \\ (q_2',\ell')=1 \\ (q_2q_2', rn_1M)=1}} \sum_{n_2\geq 1} |\mathfrak{C}(n_2)||\mathfrak{J}_{\boldsymbol{a}}(n_2)|,$$

where

$$\mathfrak{C}(n_2) = \sideset{}{^\star}\sum_{b \bmod Mb'} \sideset{}{^\star}\sum_{\bmod M} \Bigg(\sum_{\substack{u \bmod M \\ u\neq b}} \overline{\chi}(u) e\bigg(\frac{m\overline{q_1^2 q_2^2 \ell(b-u)}}{M}\bigg)\Bigg) \cdot \Bigg(\sum_{\substack{u' \bmod M \\ u'\neq b'}} \chi(u') e\bigg(\frac{-m'\overline{q_1^2 q_2'^2 \ell'(b'-u')}}{M}\bigg)\Bigg)\Bigg(\sum_{d\,|\,q_1q_2} \sum_{d'\,|\,q_1q_2'} dd'\mu(q_1q_2/d)\mu(q_1q_2'/d') \cdot \sideset{}{^\star}\sum_{\alpha \pmod{Mrq_1q_2/n_1}} \sideset{}{^\star}\sum_{\substack{\alpha' \pmod{Mrq_1q_2'/n_1} \\ q_2'\bar{\alpha}-q_2\overline{\alpha'}\equiv -\eta_1 n_2 (Mrq_1q_2q_2'/n_1) \\ n_1\alpha\equiv -m\bar{\ell}(d) \\ n_1\alpha'\equiv -m'\overline{\ell'}(d')}} e\bigg(\frac{n_1\alpha\overline{bq_1^2q_2^2} - n_1\alpha'\overline{b'q_1^2q_2'^2}}{M}\bigg)\Bigg), \tag{5-2}$$

and

$$\mathfrak{J}_{\boldsymbol{a}}(n_2) = \int_{\mathbb{R}} W(w)\mathcal{I}_{\boldsymbol{a}}(N_0w, m, q_2)\overline{\mathcal{I}_{\boldsymbol{a}}(N_0w, m', q_2')} e\bigg(-\frac{N_0 n_2 w}{q_1q_2q_2'Mn_1r}\bigg)\,\mathrm{d}w$$

with

$$\mathcal{I}_{\boldsymbol{a}}(w,n,q_2) = \int_{\mathbb{R}} \mathcal{V}(\xi) e\bigg(-\frac{t}{2\pi}\log\xi + \eta_1\frac{3(wN\ell\xi)^{1/3}}{r^{1/3}Mq_1q_2} + \eta_2\frac{2\sqrt{mN\xi}}{Mq_1q_2}\bigg)\,\mathrm{d}\xi.$$

5A1. $(NLX)/(MRQ) \ll t^{1-\varepsilon}$. We first consider $\mathcal{I}(N_0w, m, q_2)$. Let

$$g(\xi) = -\frac{t}{2\pi}\log\xi + \eta_1\frac{3(N_0wN\ell\xi)^{1/3}}{r^{1/3}Mq_1q_2} + \eta_2\frac{2\sqrt{mN\xi}}{Mq_1q_2}. \tag{5-3}$$

There exists a stationary phase point ξ_* if and only if $m \asymp t^2M^2R^2/N$ and $\eta_2 = 1$, in which case ξ_* can be written as $\xi_0 + \xi_1 + \xi_2 + \cdots$ with

$$\begin{aligned}\xi_0 &= \frac{t^2M^2q_1^2q_2^2}{4\pi^2 mN} = \left(\frac{t}{\pi C}\right)^2 \asymp 1,\\ \xi_1 &= -\eta_1\frac{4\pi B w^{1/3}}{3t}\xi_0^{4/3} \asymp \frac{B}{t},\\ \xi_2 &= \frac{28\pi^2B^2w^{2/3}}{27t^2}\xi_0^{5/3} \asymp \frac{B^2}{t^2},\\ \xi_i &= f_i(t,C)\left(\eta_1\frac{Bw^{1/3}}{t}\right)^i \ll \left(\frac{B}{t}\right)^i, \quad i \geq 3,\end{aligned}$$

where $B = 3(N_0N\ell)^{1/3}/(r^{1/3}Mq_1q_2) \asymp NLX/(MRQ)$, $C = 2\sqrt{mN}/(Mq_1q_2)$ and $f_i(t,C) \asymp 1$ is a function. Recall that $\mathcal{V}(\xi) = \xi^{-5/12}V(\xi)g(q, -\eta_1 Xv_0)\mathcal{U}(v_0)W(Q^{3/2}(n_1^2n_2)^{1/2}/(r^{1/2}(Xv_0)^{3/2}N\ell))$, $v_0 = (n_1^2n_2)^{1/3}Q/(r^{1/3}(N\ell\xi)^{2/3}X) \asymp 1$ and (4-10). So it is easy to check the conditions in Lemma 2.7. By using this lemma together with the Taylor expansion, $\mathcal{I}_{\boldsymbol{a}}(N_0w, m, q_2)$ is essentially reduced to

$$\frac{1}{t^{1/2}}\xi_0^{-it}e\left(Bw^{1/3}g_1(C) + B^2w^{2/3}g_2(C) + O\left(\frac{|B|^3}{t^2}\right)\right), \tag{5-4}$$

where $g_1(C) = \eta_1\xi_0^{1/3} = \eta_1 t^{2/3}/(\pi C)^{2/3} \asymp 1$ and $g_2(C) = -4\pi/(9t)\xi_0^{2/3} \ll 1/t$. To estimate $\mathfrak{J}_a(n_2)$, we use the strategy in [Lin and Sun 2021, Lemma 4.3] and [Munshi 2022, Lemma 5] to get the following result.

Lemma 5.1. *Let $N_2 = Q^2Rn_1/(NLX^2q_1)t^\varepsilon$ and $N_2' = t^\varepsilon(NLn_1/(M^2Rt^2q_1) + R^2Q^3Mn_1/(N^2L^2X^3q_1))$. Assume $(NLX)/(MRQ) \ll t^{1-\varepsilon}$:*

(i) *We have $\mathfrak{J}_{\boldsymbol{a}}(n_2) \ll t^{-A}$ unless $n_2 \ll N_2$, in which case one has*

$$\mathfrak{J}_a(n_2) \ll \frac{1}{t^{1-\varepsilon}}. \tag{5-5}$$

(ii) *If $N_2' \ll n_2 \ll N_2$, we have*

$$\mathfrak{J}_{\boldsymbol{a}}(n_2) \ll \frac{RQ^{3/2}M^{1/2}n_1^{1/2}}{t^{1-\varepsilon}NLX^{3/2}q_1^{1/2}n_2^{1/2}}. \tag{5-6}$$

(iii) *If $q_2 = q_2'$, we have $\mathfrak{J}_{\boldsymbol{a}}(0) \ll t^{-A}$ unless $\ell m' - \ell' m \ll t^\varepsilon(M_1N^2L^3X^2/(M^2R^2Q^2t^2) + M_1MRQ/(NX))$.*

Proof. Let $w = u^3$. Then we may equate the w-integral in $\mathfrak{J}_{\boldsymbol{a}}$ with

$$\int_{\mathbb{R}} W(u^3)u^2 e\left(-\frac{N_0n_2u^3}{q_1q_2q_2'Mn_1r} + (Bg_1(C) - B'g_1(C'))u + (B^2g_2(C) - B'^2g_2(C'))u^2 + O\left(\frac{B^3}{t^2}\right)\right)\mathrm{d}u,$$

where $B' = 3(N_0N\ell')^{1/3}/(r^{1/3}Mq_1q_2')$, $C' = 2\sqrt{m'N}/(Mq_1q_2')$. Applying integration by parts, the above integral is $\ll t^{-A}$ if $n_2 \gg N_2$, which gives the first result in (i). The second result in (i) is obvious, since we may save $t^{1/2}$ in both $\mathcal{I}_{\boldsymbol{a}}(N_0w, m, q_2)$ and $\overline{\mathcal{I}_{\boldsymbol{a}}(N_0w, m', q_2')}$ according to (5-4).

It is easy to see that

$$B^2 g_2(C) - B'^2 g_2(C') \ll \frac{B\xi_0^{1/3} + B'\xi_0'^{1/3}}{t} |B\xi_0^{1/3} - B'\xi_0'^{1/3}| \ll |Bg_1(C) - B'g_1(C')| t^{-\varepsilon}, \tag{5-7}$$

where we have used $\xi_0' = (t/(\pi C'))^2 \asymp 1$ and $B,\ B' \asymp (NLX)/(MRQ) \ll t^{1-\varepsilon}$. Therefore, if $N_2' \ll n_2 \ll N_2$, the u-integral is $O(t^{-A})$ unless $|Bg_1(C) - B'g_1(C')| \asymp N_0 n_2/(q_1 q_2 q_2' M n_1 r)$. By the second derivative test and (5-4), we get (5-6).

For $n_2 = 0$ and $q_2 = q_2'$, we may rewrite the above u-integral as

$$\int_{\mathbb{R}} W(u^3) u^2 e\left((Bg_1(C) - B'g_1(C'))u + (B^2 g_2(C) - B'^2 g_2(C'))u^2 + O\left(\frac{B^3}{t^2}\right)\right) \mathrm{d}u.$$

Notice that

$$\frac{Bg_1(C)}{(m'\ell)^{1/3}} = \frac{B'g_1(C')}{(m\ell')^{1/3}} \quad \text{and} \quad Bg_1(C) - B'g_1(C') = \frac{Bg_1(C)}{(m'\ell)^{1/3}}((m'\ell)^{1/3} - (m\ell')^{1/3}).$$

So by partial integration and (5-7), the u-integral is $O(t^{-A})$ unless

$$(m'\ell)^{1/3} - (m\ell')^{1/3} \ll \left(\frac{B^3}{t^2} + 1\right) \frac{(M_1 L)^{1/3} t^{\varepsilon}}{B}.$$

This actually proves the result in (iii). □

5A2. $(NLX)/(MRQ) \gg t^{1-\varepsilon}$. It is easy to see that $R \ll N^{1+\varepsilon} LX/(MtQ)$. We have the following Lemma 5.2.

Lemma 5.2. *Let N_2 be defined as in Lemma 5.1. Then, if $(NLX)/(MRQ) \gg t^{1-\varepsilon}$, one has the following estimates*:

(1) *If $n_2 \gg N_2$, we have $\mathfrak{J}_{\boldsymbol{a}}(n_2) \ll N^{-A}$.*

(2) *If $n_2 \ll N_2$, we have*

$$\mathfrak{J}_{\boldsymbol{a}}(n_2) \ll \frac{MRQ}{N^{1-\varepsilon} LX}.$$

Proof. The first result can be done by applying integration by parts with respect to the w-integral. For $n_2 \ll N_2$, we can use the arguments as in [Munshi 2022, Lemma 1] to see

$$\int_{\mathbb{R}} W(w) |\mathcal{I}_{\boldsymbol{a}}(N_0 w, n, \ell, q_2)|^2 \,\mathrm{d}w \ll \frac{MRQ}{N^{1-\varepsilon} LX},$$

which implies (ii). □

Remark 5.3. In the case of $(NLX)/(MRQ) \gg t^{1+\varepsilon}$, we remark that one may replace it by a more explicit version like Lemma 5.1. However, the present result is enough for our purpose.

5B. ***Case b.*** After a similar treatment, and noting that $m \ll M^2R^2t^\varepsilon/N$, we have

$$(4\text{-}14) \ll \frac{N^{1+\varepsilon}X^{1/2}}{M^{5/2}L^{4/3}Q^{1/2}r^{1/2}} \sum_{\eta_1=\pm 1} \sup_{M_1 \ll (M^2R^2t^\varepsilon/N)} \sum_{n_1 \ll Rr} n_1^{\theta_3} \sum_{(n_1/(n_1,r))|q_1|n_1^\infty} \frac{1}{q_1^2}\Omega_{\boldsymbol{b}}^{1/2}, \tag{5-8}$$

where

$$\Omega_{\boldsymbol{b}} \ll \frac{N_0q_1^4L^{2/3}}{n_1^2M_1^{1/2}R^4} \sum_{\substack{\ell\in\mathcal{L} \\ (\ell\ell',q_1)=1}} \sum_{\ell'\in\mathcal{L}} |A(1,\ell)A(1,\ell')| \sum_{m\sim M_1} \sum_{m'\sim M_1} |\lambda_f(m)||\lambda_f(m')| \sum_{\substack{q_2\sim R/q_1 \\ (q_2,\ell)=1}} \sum_{\substack{q_2'\sim R/q_1 \\ (q_2',\ell')=1 \\ (q_2q_2',n_1M)=1}} \sum_{n_2\geq 1} |\mathfrak{C}(n_2)||\mathfrak{J}_{\boldsymbol{b}}(n_2)|,$$

with $\mathfrak{C}(n_2)$ defined as in (5-2) and

$$\mathfrak{J}_{\boldsymbol{b}}(n_2) = \int_{\mathbb{R}} W(w)\mathcal{I}_{\boldsymbol{b}}(N_0w,m,q_2)\overline{\mathcal{I}_{\boldsymbol{b}}(N_0w,m',q_2')}e\left(-\frac{N_0n_2w}{q_1q_2q_2'Mn_1r}\right)\mathrm{d}w,$$
$$\mathcal{I}_{\boldsymbol{b}}(w,n,q_2) = \int_{\mathbb{R}} \xi^{-1/4}V(\xi)J_f\left(\frac{mN\xi}{M^2q^2}\right)e\left(-\frac{t}{2\pi}\log\xi + \eta_1\frac{3(wN\ell\xi)^{1/3}}{r^{1/3}Mq_1q_2}\right)\mathrm{d}\xi.$$

By the exactly treatment, we have the following lemma.

Lemma 5.4. *The results in Lemma 5.2 hold when replacing $\mathfrak{J}_{\boldsymbol{a}}$ by $\mathfrak{J}_{\boldsymbol{b}}$.*

5C. ***Case c.*** After a similar treatment, we have

$$S_{11}^{\pm}(N,X,R,N_0) \leq \frac{N^{5/4}X}{M^{5/2}LQr^{1/2}} \frac{1}{t^{1/2}} \sum_{\eta_1=\pm 1} \sum_{n_1\leq Rr} \sum_{(n_1/(n_1,r))\,|\,q_1\,|\,(rn_1)^\infty} \frac{1}{q_1^2} \sum_{n_2\asymp N_0/n_1^2} \frac{|A(n_1,n_2)|}{n_2^{1/2}}$$
$$\cdot\left|\sum_{\ell\in\mathcal{L}} \overline{A(1,\ell)\chi(\ell)}\ell^{1/2} \sum_{\substack{q_2\sim R/q_1 \\ (q_2,\ell Mrn_1)=1}} \frac{1}{q_2^{2+2it}}\right.$$
$$\left.\cdot \sum_{m\asymp R^2M^2t^2/N} \frac{\lambda_f(m)}{m^{1/4-it}} \mathcal{C}(m,n_1,n_2,\ell,q) W_{x,\ell}^{\mathrm{sgn}(\eta_1)}\left(\frac{n_1^2n_2}{q^3M^3r}\right)V_{x,\ell}\left(\frac{tMq}{\sqrt{mN}}\right)\right|.$$

By the Cauchy–Schwarz inequality and (2-5) we have

$$S_{11}^{\pm}(N,X,R,N_0) \ll \frac{N^{5/4+\varepsilon}X}{M^{5/2}LQr^{1/2}} \frac{1}{t^{1/2}} \sum_{\eta_1=\pm 1} \sum_{n_1\leq Rr} n_1^{\theta_3} \sum_{(n_1/(n_1,r))|q_1|(rn_1)^\infty} \frac{1}{q_1^2}\Omega_{\boldsymbol{c}}^{1/2}, \tag{5-9}$$

where

$$\Omega_{\boldsymbol{c}} = \sum_{n_2\asymp N_0/n_1^2} \left|\sum_{\ell\in\mathcal{L}} \overline{A(1,\ell)\chi(\ell)}\ell^{1/2} \sum_{\substack{q_2\sim R/q_1 \\ (q_2,\ell Mrn_1)=1}} \frac{1}{q_2^{2+2it}} \sum_{m\asymp R^2M^2t^2/N} \frac{\lambda_f(m)}{m^{1/4-it}}\right.$$
$$\left.\cdot\,\mathcal{C}(m,n_1,n_2,\ell,q)W_{x,\ell}^{\mathrm{sgn}(\eta_1)}\left(\frac{n_1^2n_2}{q^3M^3r}\right)V_{x,\ell}\left(\frac{tMq}{\sqrt{mN}}\right)\right|^2.$$

Opening the square we get

$$\Omega_{\boldsymbol{c}} \ll L \sum_{\ell\in\mathcal{L}} |A(1,\ell)| \sum_{\substack{q_2\sim R/q_1\\ (q_2,\ell M r n_1)=1}} \frac{1}{q_2^2} \sum_{m\asymp R^2M^2t^2/N} \frac{|\lambda_f(m)|}{m^{1/4}} \cdot \sum_{\ell'\in\mathcal{L}} |A(1,\ell')| \sum_{\substack{q_2'\sim R/q_1\\ (q_2',\ell' M r n_1)=1}} \frac{1}{q_2'^2} \sum_{m'\asymp R^2M^2t^2/N} \frac{|\lambda_f(m')|}{m'^{1/4}} \cdot \biggl|\sum_{n_2\geq 1} W\Bigl(\frac{n_1^2n_2}{N_0}\Bigr)\mathcal{C}(m,n_1,n_2,\ell,q)\overline{\mathcal{C}(m',n_1,n_2,\ell',q')}\biggr|,$$

where $W(n_1^2n_2/N_0)$ is a smooth compactly supported function which contains the weight function $W_{x,\ell}^{\operatorname{sgn}(\eta_1)}(n_1^2n_2/(q^3M^3r))\overline{W_{x,\ell}^{\operatorname{sgn}(\eta_1)}(n_1^2n_2/(q^3M^3r))}$. Note that by (4-3) we have

$$\frac{\partial^j}{\partial n_2^j} W\Bigl(\frac{n_1^2n_2}{N_0}\Bigr) \ll_j t^\varepsilon n_2^{-j}, \quad j\geq 0.$$

By the Poisson summation formula modulo $Mrq_1q_2q_2'/n_1$ we get

$$\Omega_{\boldsymbol{c}} \ll \frac{N_0}{n_1^2}\frac{Lq_1^4}{R^4}\frac{N^{1/2}}{RMt} \sum_{\ell\in\mathcal{L}} |A(1,\ell)| \sum_{\substack{q_2\sim R/q_1\\ (q_2,\ell M r n_1)=1}} \sum_{m\asymp R^2M^2t^2/N} \cdot \sum_{\ell'\in\mathcal{L}} |A(1,\ell')| \sum_{\substack{q_2'\sim R/q_1\\ (q_2',\ell' M r n_1)=1}} \sum_{m'\asymp R^2M^2t^2/N} |\lambda_f(m')|^2 \sum_{n_2\in\mathbb{Z}} |\mathfrak{C}(n_2)||\mathfrak{I}_{\boldsymbol{c}}(n_2)|,$$

where $\mathfrak{C}(n_2)$ is defined as in (5-2) and

$$\mathfrak{I}_{\boldsymbol{c}}(n_2) = \frac{n_1^2}{N_0}\int_{\mathbb{R}} W\Bigl(\frac{n_1^2u}{N_0}\Bigr) e\Bigl(-\frac{un_2}{Mrq_1q_2q_2'/n_1}\Bigr)\,\mathrm{d}u = \int_{\mathbb{R}} W(\xi) e\Bigl(-\frac{N_0n_2\xi}{Mrq_1q_2q_2'n_1}\Bigr)\,\mathrm{d}\xi.$$

By repeated integration by parts we have

$$\mathfrak{I}_{\boldsymbol{c}}(n_2) \ll \begin{cases} t^{-A} & \text{if } n_2 \gg (MrR^2n_1)/(q_1N_0)t^\varepsilon, \\ t^\varepsilon & \text{if } n_2 \ll (MrR^2n_1)/(q_1N_0)t^\varepsilon. \end{cases} \tag{5-10}$$

6. The zero frequency

In this section we estimate the contribution from the terms with $n_2=0$. Denote the contribution of this part to Ω_* by Ω_0, where $*\in\{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\}$. Note that $q_2'\bar{\alpha}-q_2\overline{\alpha'}\equiv 0 \pmod{Mq_2q_2'}$. So we have

$q_2' = (q_2'\bar{\alpha}, Mq_2q_2') = (q_2\overline{\alpha'}, Mq_2q_2') = q_2$, and hence $\alpha = \alpha'$. We have

$$\mathfrak{C}(0) = \delta_{q=q'} \sideset{}{^\star}\sum_{b \pmod M} \sideset{}{^\star}\sum_{b' \pmod M} \Bigg(\sum_{\substack{u \pmod M \\ u \neq b}} \bar{\chi}(u) e\bigg(\frac{m\overline{q^2\ell(b-u)}}{M}\bigg)\Bigg)\Bigg(\sum_{\substack{u' \pmod M \\ u' \neq b'}} \chi(u') e\bigg(\frac{-m'\overline{q^2\ell'(b'-u')}}{M}\bigg)\Bigg)$$

$$\cdot \sum_{d \mid q} \sum_{d' \mid q} dd' \mu(q/d)\mu(q/d') \sideset{}{^\star}\sum_{\substack{\alpha \pmod{Mrq/n_1} \\ n_1\alpha \equiv -m\bar{\ell}(d) \\ n_1\alpha \equiv -m'\bar{\ell}'(d')}} e\bigg(\frac{n_1\alpha\overline{bq^2} - n_1\alpha\overline{b'q^2}}{M}\bigg).$$

6A. ***Case a:*** $t^{\varepsilon} \ll (LNX)/(MRQ) \ll t^{1-\varepsilon}$**.**

6A1. $M \mid (m\bar{\ell} - m'\bar{\ell}')$. Denote the contribution of this part to Ω_0 by Ω_{01}. Moreover, the α-sum depends on either $b \equiv b' \pmod M$ or $b \not\equiv b' \pmod M$. The character sum becomes

$$\begin{aligned} \mathfrak{C}(0) &\ll M|\mathfrak{C}_1'| \sum_{d \mid q} \sum_{d' \mid q} dd' \sum_{\substack{\alpha \pmod{rq/n_1} \\ n_1\alpha \equiv -m\bar{\ell} \pmod d \\ n_1\alpha \equiv -m'\bar{\ell}' \pmod d}} 1 + |\mathfrak{C}_1''| \sum_{d \mid q} \sum_{d' \mid q} dd' \sum_{\substack{\alpha \pmod{rq/n_1} \\ n_1\alpha \equiv -m\bar{\ell} \pmod d \\ n_1\alpha \equiv -m'\bar{\ell}' \pmod d}} 1 \\ &\ll (M|\mathfrak{C}_1'| + |\mathfrak{C}_1''|) \sum_{d \mid q} \sum_{d' \mid q} (d, d') rq \delta_{(d,d') \mid (m\ell' - m'\ell)}, \end{aligned} \tag{6-1}$$

where

$$\mathfrak{C}_1' = \sideset{}{^\star}\sum_{b \pmod M} \sum_{\substack{u \pmod M \\ u \neq b}} \sum_{\substack{u' \pmod M \\ u' \neq b}} \bar{\chi}(u)\chi(u') e\bigg(\frac{m\overline{q^2\ell(b-u)}}{M}\bigg) e\bigg(-\frac{m'\overline{q^2\ell'(b-u')}}{M}\bigg),$$

and

$$\mathfrak{C}_1'' = \sideset{}{^\star}\sum_{b \pmod M} \sideset{}{^\star}\sum_{\substack{b' \pmod M \\ b' \not\equiv b \pmod M}} \sum_{\substack{u \pmod M \\ u \neq b}} \sum_{\substack{u' \pmod M \\ u' \neq b'}} \bar{\chi}(u)\chi(u') e\bigg(\frac{m\overline{q^2\ell(b-u)}}{M}\bigg) e\bigg(-\frac{m'\overline{q^2\ell'(b'-u')}}{M}\bigg).$$

Since $M \mid (m\bar{\ell} - m'\bar{\ell}')$, similar to [Sharma 2022, (6.3)], we have square root cancellation in the sum over u and u', and hence we obtain

$$\mathfrak{C}_1' \ll M^2 \quad \text{and} \quad \mathfrak{C}_1'' \ll M^3.$$

Hence

$$\mathfrak{C}(0) \ll M^3 \sum_{d \mid q} \sum_{d' \mid q} (d, d') rq \delta_{(d,d') \mid (m\ell' - m'\ell)}.$$

Note that $(M, (d, d')) = 1$ and

$$|A(1, \ell)A(1, \ell')\lambda_f(m)\lambda_f(m')| \ll |A(1, \ell)\lambda_f(m')|^2 + |A(1, \ell')\lambda_f(m)|^2.$$

By Lemma 5.1, we have

$$\sum_{\ell}\sum_{\ell'}\sum_{m}\sum_{m'}|\mathfrak{J}(0)| \ll \sum_{\ell}|A(1,\ell)|^2\sum_{m'}|\lambda_f(m')|^2 \sum_{\substack{\ell'\quad m \\ M(d,d')\,|\,(m\ell'-m'\ell)}}\sum |\mathfrak{J}(0)| \\ + \sum_{\ell'}|A(1,\ell')|^2\sum_{m}|\lambda_f(m)|^2 \sum_{\substack{\ell\quad m' \\ M(d,d')\,|\,(m\ell'-m'\ell)}}\sum |\mathfrak{J}(0)| \\ \ll N^{\varepsilon}LM_1\biggl(\frac{LM_1((LNX)/(MRQt))^2+LM_1(MRQ)/(LNX)}{M(d,d')}+1\biggr)\frac{1}{t}. \tag{6-2}$$

Hence we have

$$\Omega_{01} \ll N^{\varepsilon}\frac{N_0M^3}{n_1^2M_1^{1/2}}\frac{L^{2/3}q_1^3}{R^3}\biggl(\sum_{\substack{q_2\sim R/q_1\\(q_2,rn_1)=1}}\sum_{\substack{d\,|\,q\\d'\,|\,q}}rqLM_1\biggl(\frac{LM_1(LNX/MRQt)^2+LM_1(MRQ/LNX)}{M}+q\biggr)\frac{1}{t}\biggr) \\ \ll N^{\varepsilon}\frac{N_0M^3}{n_1^2M_1^{1/2}}\frac{L^{2/3}q_1^2}{R^2}rRLM_1\biggl(\frac{LM_1(LNX/MRQt)^2+LM_1(MRQ/LNX)}{Mt}+\frac{R}{t}\biggr).$$

By using $N_0=N^2L^2X^3r/Q^3$ and $M_1\ll t^2R^2M^2/N$, we get

$$\Omega_{01} \ll N^{\varepsilon}\frac{r^2N^{3/2}L^{11/3}Rq_1^2M^4X^3}{n_1^2Q^3}\biggl(\frac{L^3NX^2}{MRQ^2}+\frac{M^2R^2Qt^2}{N^2X}+1\biggr).$$

Hence, the contribution from Ω_{01} to (5-1) is

$$\ll \frac{N^{3/4+\varepsilon}X^{1/2}}{M^2L^{4/3}Q^{1/2}r^{1/2}}\sum_{n_1\ll RMr}n_1^{\theta_3}\sum_{(n_1/(n_1,r))|q_1|(rn_1)^{\infty}}\frac{1}{n_1q_1^{1/2}}\biggl(\frac{r^2N^{3/2}L^{11/3}RM^4X^3}{Q^3}\biggr)^{1/2} \\ \cdot\biggl(\frac{L^3NX^2}{MRQ^2}+\frac{M^2R^2Qt^2}{N^2X}+1\biggr)^{1/2} \\ \ll N^{\varepsilon}r^{1/2}\frac{N^{3/2}L^{1/2}R^{1/2}X^2}{Q^2}\biggl(\frac{L^{3/2}N^{1/2}X}{M^{1/2}R^{1/2}Q}+\frac{MRQ^{1/2}t}{NX^{1/2}}+1\biggr).$$

Recall $Q=(NL/MK)^{1/2}$. Thus, by $X\ll t^{\varepsilon}$ and $R\le Q$, we arrive at

$$\ll N^{\varepsilon}r^{1/2}\frac{N^2L^2}{M^{1/2}Q^3}+N^{\varepsilon}r^{1/2}N^{1/2}L^{1/2}Mt+N^{\varepsilon}r^{1/2}\frac{N^{3/2}L^{1/2}}{Q^{3/2}} \\ \ll N^{\varepsilon}r^{1/2}N^{1/2}L^{1/2}MK^{3/2}+N^{\varepsilon}r^{1/2}N^{1/2}L^{1/2}Mt+N^{\varepsilon}r^{1/2}\frac{N^{3/4}M^{3/4}K^{3/4}}{L^{1/4}}. \tag{6-3}$$

6A2. $M\nmid(m\bar{\ell}-m'\bar{\ell}')$. Denote the contribution of this part to Ω_0 by Ω_{02}. In this case, we also have $q_2=q_2'$ and $\alpha=\alpha'$. So we can estimate the character as in (6-1). Since $M\nmid(m\bar{\ell}-m'\bar{\ell}')$, the nondegeneracy holds for the variables b, u, u' in $\mathfrak{C}_1'$ and $\mathfrak{C}_1''$ and hence we have

$$\mathfrak{C}_1'\ll M^{3/2} \quad\text{and}\quad \mathfrak{C}_1''\ll M^{5/2}.$$

Thus we get

$$\mathfrak{C}(0) \ll M^{5/2} \sum_{d \mid q_1q_2} \sum_{d' \mid q_1q_2} dd' \frac{rq_1q_2}{[d,d']} \delta_{(d,d') \mid (m\ell'-m'\ell)}. \tag{6-4}$$

As in (6-2), by Lemma 5.1, we have

$$\sum_{\ell} \sum_{\ell'} \sum_{m} \sum_{\substack{m' \\ (d,d') \mid (m\ell'-m'\ell)}} |\mathfrak{J}(0)| \ll N^{\varepsilon} LM_1 \left(\frac{LM_1(LNX/MRQt)^2 + LM_1MRQ/LNX}{(d,d')} + 1 \right) \frac{1}{t}.$$

Hence, similar to the estimate for Ω_{01}, we have

$$\Omega_{02} \ll N^{\varepsilon} \frac{r^2N^{3/2}L^{11/3}Rq_1^2M^{7/2}X^3}{n_1^2Q^3} \left(\frac{L^3NX^2}{RQ^2} + \frac{M^3R^2Qt^2}{N^2X} + 1 \right).$$

Hence, similar to the estimate for (6-3), the contribution from Ω_{02} to (5-1) is

$$\ll N^{\varepsilon} r^{1/2} N^{1/2} L^{1/2} M^{5/4} K^{3/2} + N^{\varepsilon} r^{1/2} N^{1/2} L^{1/2} M^{5/4} t + N^{\varepsilon} r^{1/2} \frac{N^{3/4}M^{1/2}K^{3/4}}{L^{1/4}}. \tag{6-5}$$

6B. ***Case a:* $(LNX)/(MRQ) \gg t^{1-\varepsilon}$.** By the same argument as in the Section 6A and Lemma 5.2 we have

$$\begin{aligned}
\Omega_0 \ll N^{\varepsilon} \frac{N_0M^3}{n_1^2M_1^{1/2}} \frac{L^{2/3}q_1^3}{R^3} \sum_{\substack{q_2 \sim R/q_1 \\ (q_2,rn_1)=1}} \sum_{\substack{d \mid q \\ d' \mid q}} rqLM_1 \left(\frac{LM_1}{M} + q \right) \frac{MRQ}{NLX} \\
+ N^{\varepsilon} \frac{N_0M^{5/2}}{n_1^2M_1^{1/2}} \frac{L^{2/3}q_1^3}{R^3} \sum_{\substack{q_2 \sim R/q_1 \\ (q_2,rn_1)=1}} \sum_{\substack{d \mid q \\ d' \mid q}} rqLM_1(LM_1+q) \frac{MRQ}{NLX} \\
\ll N^{\varepsilon} \frac{N_0}{n_1^2M_1^{1/2}} \frac{L^{2/3}q_1^3}{R^3} \sum_{\substack{q_2 \sim R/q_1 \\ (q_2,rn_1)=1}} rqLM_1(LM_1M^{5/2} + qM^3) \frac{MRQ}{NLX} \\
\ll N^{\varepsilon} \frac{r^2N^{3/2}Mq_1^2L^{11/3}X^3}{n_1^2Q^3} \left(\frac{NL^3M^{5/2}X^2}{Q^2} + RM^3 \right).
\end{aligned}$$

Here we have used $N_0 = N^2L^2X^3r/Q^3$ and $M_1 \ll (NL^2X^2/Q^2)N^{\varepsilon}$. Therefore, the contribution from Ω_0 to (5-1) is

$$\begin{aligned}
\ll \frac{N^{3/4+\varepsilon}X^{1/2}}{M^2L^{4/3}Q^{1/2}r^{1/2}} \sum_{n_1 \ll RMr} n_1^{\theta_3} \sum_{(n_1/(n_1,r)) \mid q_1 \mid (rn_1)^\infty} \frac{1}{n_1q_1^{1/2}} \left(\frac{r^2N^{3/2}ML^{11/3}X^3}{Q^3} \left(\frac{NL^3M^{5/2}X^2}{Q^2} + RM^3 \right) \right)^{1/2} \\
\ll N^{\varepsilon} r^{1/2} \frac{N^{3/2}L^{1/2}X^2}{M^{3/2}Q^2} \left(\frac{N^{1/2}L^{3/2}M^{5/4}X}{Q} + R^{1/2}M^{3/2} \right).
\end{aligned}$$

Note that we have $R \ll NLX/(MQt^{1-\varepsilon})$ now. By this and inserting $Q=(NL/MK)^{1/2}$, one can bound the above by

$$\ll N^{\varepsilon} r^{1/2} N^{1/2} L^{1/2} M^{5/4} K^{3/2} + N^{\varepsilon} r^{1/2} \frac{N^{3/4} M^{3/4} K^{5/4}}{L^{1/4} t^{1/2}}. \tag{6-6}$$

6C. *Case b:* $(LNX)/(MRQ) \asymp t$. By the same argument as in the Section 6A and Lemma 5.4 we have

$$\begin{aligned}\Omega_0 \ll N^{\varepsilon} \frac{N_0 M^3}{n_1^2 M_1^{1/2}} \frac{L^{2/3} q_1^4}{R^4} \sum_{\substack{q_2 \sim R/q_1 \\ (q_2, rn_1)=1}} \sum_{\substack{d \mid q \\ d' \mid q}} rqLM_1 \left(\frac{LM_1}{M} + q \right) \frac{MRQ}{NLX} \\ + N^{\varepsilon} \frac{N_0 M^{5/2}}{n_1^2 M_1^{1/2}} \frac{L^{2/3} q_1^4}{R^4} \sum_{\substack{q_2 \sim R/q_1 \\ (q_2, rn_1)=1}} \sum_{\substack{d \mid q \\ d' \mid q}} rqLM_1 (LM_1 + q) \frac{MRQ}{NLX} \\ \ll N^{\varepsilon} \frac{N_0}{n_1^2} \frac{L^{2/3} q_1^3}{R^3} rRLM_1^{1/2} (LM_1 M^{5/2} + RM^3) \frac{MRQ}{NLX}.\end{aligned}$$

By $N_0 = N^2 L^2 X^3 r/Q^3$ and $M_1 \ll (M^2 R^2/N) t^{\varepsilon}$ we obtain

$$\begin{aligned}\Omega_0 &\ll N^{\varepsilon} \frac{1}{n_1^2} \frac{N^2 L^2 X^3 r}{Q^3} \frac{MRQ}{NLX} \frac{L^{2/3} q_1^3}{R^3} rRL \frac{MR}{N^{1/2}} \left(LM^{5/2} \frac{M^2 R^2}{N} + RM^3 \right) \\ &\ll N^{\varepsilon} \frac{r^2 N^{1/2} M^2 q_1^3 L^{8/3} X^2}{n_1^2 Q^2} \left(\frac{LM^{9/2} R^2}{N} + RM^3 \right).\end{aligned}$$

Thus, the contribution from Ω_0 to (5-8) is

$$\begin{aligned}&\ll \frac{N^{1+\varepsilon} X^{1/2}}{M^{5/2} L^{4/3} Q^{1/2} r^{1/2}} \sum_{n_1 \ll RMr} n_1^{\theta_3} \sum_{(n_1/(n_1,r)) \mid q_1 \mid (rn_1)^{\infty}} \frac{1}{n_1 q_1^{1/2}} \left(\frac{r^2 N^{1/2} M^2 L^{8/3} X^2}{Q^2} \left(\frac{LM^{9/2} R^2}{N} + RM^3 \right) \right)^{1/2} \\ &\ll N^{\varepsilon} r^{1/2} \frac{N^{3/4} L^{1/2} M^{3/4} R X^{3/2}}{Q^{3/2}} + N^{\varepsilon} r^{1/2} \frac{N^{5/4} R^{1/2} X^{3/2}}{Q^{3/2}}.\end{aligned}$$

By $Q=(NL/MK)^{1/2}$ again and noting that $R \asymp (NLX)/(MQt)$, we deduce that the above is dominated by

$$\ll N^{\varepsilon} r^{1/2} N^{1/2} L^{1/4} M \frac{K^{5/4}}{t} + N^{\varepsilon} r^{1/2} \frac{N^{3/4} M^{1/2} K}{L^{1/2} t^{1/2}}. \tag{6-7}$$

6D. *Case c:* $(LNX)/(MRQ) \ll t^{\varepsilon}$. By the same argument as in the Section 6A and (5-10) we have (taking $M_1 \asymp R^2 M^2 t^2/N$)

$$\begin{aligned}\Omega_0 &\ll N^{\varepsilon} \frac{N_0 M^3}{n_1^2 M_1^{1/2}} \frac{L q_1^4}{R^4} \sum_{\substack{q_2 \sim R/q_1 \\ (q_2, rn_1)=1}} \sum_{\substack{d \mid q \\ d' \mid q}} rqLM_1 \left(\frac{LM_1}{M} + q \right) + N^{\varepsilon} \frac{N_0 M^{5/2}}{n_1^2 M_1^{1/2}} \frac{L q_1^4}{R^4} \sum_{\substack{q_2 \sim R/q_1 \\ (q_2, rn_1)=1}} \sum_{\substack{d \mid q \\ d' \mid q}} rqLM_1 (LM_1 + q) \\ &\ll N^{\varepsilon} \frac{N_0}{n_1^2} \frac{L q_1^3}{R^3} rRLM_1^{1/2} (LM_1 M^{5/2} + RM^3).\end{aligned}$$

By $N_0 \ll (R^3M^3r/LN)t^\varepsilon$ and $M_1 \asymp R^2M^2t^2/N$, one has

$$\Omega_0 \ll N^\varepsilon \frac{1}{n_1^2}\frac{R^3M^3r}{LN}\frac{Lq_1^3}{R^3}rRL\frac{RMt}{N^{1/2}}\left(LM^{5/2}\frac{R^2M^2t^2}{N}+RM^3\right)$$
$$\ll N^\varepsilon \frac{r^2q_1^3R^2LM^4t}{n_1^2N^{3/2}}\left(\frac{LM^{9/2}R^2t^2}{N}+RM^3\right).$$

So the contribution from Ω_0 to (5-9) is

$$\ll \frac{N^{5/4+\varepsilon}X}{M^{5/2}LQr^{1/2}t^{1/2}}\left(\frac{r^2R^2LM^4t}{N^{3/2}}\left(\frac{LM^{9/2}R^2t^2}{N}+RM^3\right)\right)^{1/2}$$
$$\ll N^\varepsilon r^{1/2}\frac{M^{7/4}R^2tX}{Q}+N^\varepsilon r^{1/2}\frac{N^{1/2}MR^{3/2}X}{L^{1/2}Q}.$$

Now we have the condition $X \ll (MRQ/LN)t^\varepsilon$, so one computes the above as

$$\ll N^\varepsilon r^{1/2}N^{1/2}L^{1/2}M^{5/4}\frac{t}{K^{3/2}}+N^\varepsilon r^{1/2}\frac{N^{3/4}M^{3/4}}{L^{1/4}K^{5/4}}. \tag{6-8}$$

Combining (6-3), (6-5), (6-6), (6-7) and (6-8), we see that the contribution of the zero frequency is dominated by

$$\ll N^\varepsilon r^{1/2}N^{1/2}L^{1/2}M^{5/4}K^{3/2}+N^\varepsilon r^{1/2}N^{1/2}L^{1/2}M^{5/4}t$$
$$+N^\varepsilon r^{1/2}\frac{N^{3/4}M^{3/4}K^{3/4}}{L^{1/4}}+N^\varepsilon r^{1/2}\frac{N^{3/4}M^{3/4}K^{5/4}}{L^{1/4}t^{1/2}}. \tag{6-9}$$

7. The nonzero frequencies

7A. $n_2 \not\equiv 0 \pmod M$. Denote the contribution from $n_2 \not\equiv 0 \pmod M$ in Ω_* by $\Omega_{*,1}$, where $* \in \{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}$. We have

$$\mathfrak{C}(n_2) \ll |\mathfrak{C}_1(n_2)\mathfrak{C}_2(n_2)\mathfrak{C}_3(n_2)|,$$

where

$$\mathfrak{C}_1(n_2)=\sideset{}{^\star}\sum_{b \bmod M}\sideset{}{^\star}\sum_{b' \bmod M}\Bigg(\sum_{\substack{u \bmod M\\ u\neq b}}\bar{\chi}(u)e\left(\frac{m\overline{q_2^2\ell(b-u)}}{M}\right)\Bigg)$$
$$\cdot\Bigg(\sum_{\substack{u' \bmod M\\ u'\neq b'}}\chi(u')e\left(-\frac{m'\overline{q_2'^2\ell(b'-u')}}{M}\right)\Bigg)\Bigg(\sideset{}{^\star}\sum_{\substack{\alpha,\alpha' \bmod M\\ q_2'\bar{\alpha}-q_2\overline{\alpha'}\equiv -\eta_1 n_2 (M)}} e\left(\frac{\alpha b\overline{q_2^2}-\alpha' b'\overline{q_2'^2}}{M}\right)\Bigg),$$

$$\mathfrak{C}_2(n_2)=\sum_{d_1\mid q_1}\sum_{d_1'\mid q_1} d_1d_1' \sideset{}{^\star}\sum_{\substack{\alpha_1 \bmod rq_1/n_1\\ n_1\alpha_1\equiv -m\bar{\ell} \bmod d_1 \\ q_2'\alpha_1-q_2\overline{\alpha_1'}\equiv -\eta_1 n_2 \pmod{rq_1/n_1}}}\ \sideset{}{^\star}\sum_{\substack{\alpha_1' \bmod rq_1/n_1\\ n_1\alpha_1'\equiv -m'\overline{\ell'} \bmod d_1'}} 1,$$

and

$$\mathfrak{C}_3(n_2) = \sum_{d_2 \mid q_2} \sum_{d_2' \mid q_2'} d_2 d_2' \sideset{}{^\star}\sum_{\substack{\alpha_2(q_2),\alpha_2'(q_2') \\ q_2'\overline{\alpha_2} - q_2\overline{\alpha_2'} \equiv -\eta_1 n_2 \bmod q_2 q_2' \\ n_1\alpha_2 \equiv -m\bar{\ell} \bmod d_2 \\ n_1\alpha_2' \equiv -m'\bar{\ell'} \bmod d_2'}} 1.$$

For $\mathfrak{C}_2(n_2)$, the congruence condition determines at most one solution of α_1' in terms of α_1, and hence we have

$$\mathfrak{C}_2(n_2) \le \sum_{d_1 \mid q_1} d_1 \sum_{d_1' \mid q_1} d_1' \sideset{}{^\star}\sum_{\substack{\alpha_1 \bmod rq_1/n_1 \\ -m\bar{\ell} \equiv n_1\alpha_1 \bmod d_1}} 1.$$

Note that α_1 is uniquely determined modulo $d_1/(d_1, n_1)$. Since $(d_1/(d_1, n_1), n_1/(d_1, n_1)) = 1$, $(d_1/(d_1, n_1)) \mid (q_1/(d_1, n_1))$ and $n_1/(d_1, n_1) \mid rq_1/(d_1, n_1)$, we have $d_1/(d_1, n_1) \mid rq_1/n_1$. Hence we have

$$\mathfrak{C}_2(n_2) \ll \frac{rq_1}{n_1} \sum_{d_1 \mid q_1} \sum_{d_1' \mid q_1} d_1'(d_1, n_1)\delta_{(d_1,n_1) \mid m}.$$

Similarly by considering α_1-sum first we have

$$\mathfrak{C}_2(n_2) \ll \frac{rq_1}{n_1} \sum_{d_1 \mid q_1} \sum_{d_1' \mid q_1} d_1(d_1', n_1)\delta_{(d_1',n_1) \mid m'}.$$

For $\mathfrak{C}_3(n_2)$, from the congruence $q_2'\bar{\alpha} - q_2\overline{\alpha'} \equiv -\eta_1 n_2 \bmod q_2 q_2'$ we have $(q_2, q_2') \mid n$. Since $(n_1, q_2) = 1$, we have $\alpha \equiv -m\bar{\ell}\bar{n}_1 \bmod d_2$ and hence $q_2'\bar{\alpha} \equiv -\eta_1 n_2 \bmod d_2$. Therefore we get $n_1 q_2' \equiv \eta_1 m n_2 \bar{\ell} \bmod d_2$. Similarly we have $-n_1 q_2 \equiv \eta_1 m' n_2 \bar{\ell'} \bmod d_2'$. Note that the congruence determines $\alpha_2 \bmod [q_2/(q_2, q_2'), d_2]$ and for each given α_2 we have at most one solution of $\alpha_2' \bmod q_2'$. Hence we have

$$\mathfrak{C}_3(n) \ll \sum\sum_{\substack{d_2 \mid (q_2, -q_2' n_1 \ell + \eta_1 m n_2) \\ d_2' \mid (q_2', q_2 n_1 \ell' + \eta_1 m' n_2)}} d_2 d_2' \frac{q_2}{[q_2/(q_2, q_2'), d_2]} \delta_{(q_2,q_2') \mid n}.$$

Similarly we have

$$\mathfrak{C}_3(n_2) \ll \sum\sum_{\substack{d_2 \mid (q_2, -q_2' n_1 \ell + \eta_1 m n_2) \\ d_2' \mid (q_2', q_2 n_1 \ell' + \eta_1 m' n_2)}} d_2 d_2' \frac{q_2'}{[q_2'/(q_2, q_2'), d_2']} \delta_{(q_2,q_2') \mid n_2}.$$

Together with [Sharma 2022, (5.6)] and [Lin et al. 2023, Proposition 4.4], we have

$$\begin{aligned}
&\mathfrak{C}_1(n_2) \ll M^{5/2}, \\
&\mathfrak{C}_2(n_2) \ll \frac{q_1 r}{n_1} \sum_{d_1 \mid q_1} \sum_{d_1' \mid q_1} \min\{d_1'(d_1, n_1)\delta_{(d_1,n_1) \mid m}, d_1(d_1', n_1)\delta_{(d_1',n_1) \mid m'}\}, \\
&\mathfrak{C}_3(n_2) \ll \sum\sum_{\substack{d_2 \mid (q_2, -q_2' n_1 \ell + \eta_1 m n_2) \\ d_2' \mid (q_2', q_2 n_1 \ell' + \eta_1 m' n_2)}} d_2 d_2' \min\left\{\frac{q_2}{[q_2/(q_2, q_2'), d_2]}, \frac{q_2'}{[q_2'/(q_2, q_2'), d_2']}\right\} \delta_{(q_2,q_2') \mid n_2}.
\end{aligned}$$

Now, we need some careful counting to estimate $\Omega_{*,1}$; see [Munshi 2022, Section 6; Sharma 2022, Section 5; Lin et al. 2023, Section 6; Lin and Sun 2021, Section 4.5].

7A1. *Case a.* It is obvious that, for fixed tuple (n_1, α, n_2), the congruence

$$-q_2' n_1 \ell + \eta_1 m n_2 \equiv 0 \bmod d_2$$

has a solution if and only if $(d_2, n_2) \mid q_2'\ell$, in which case m is uniquely determined modulo $d_2/(d_2, n_2)$. Combining this together with the condition $\delta_{(d_1,n_1)\mid m}$ in $\mathfrak{C}_2(n_2)$, the number of m $(\sim M_1)$ is dominated by $\delta_{(d_2,n_2)\mid q_2'} O(1 + M_1(d_2, n_2)/((d_1, n_1)d_2))$. Then, we get

$$\begin{aligned}\Omega_{\boldsymbol{a},1} \ll \frac{q_1^4 r N_0 L^{2/3} M^{5/2}}{n_1^3 M_1^{1/2} R^3} &\sum_{d_1 \mid q_1} \sum_{d_1' \mid q_1} d_1'(d_1, n_1) \sum_{\substack{\ell \in \mathcal{L} \\ (\ell\ell', q_1)=1}} \sum_{\ell' \in \mathcal{L}} |A_\pi(1, \ell) A_\pi(1, \ell')| \\ &\cdot \sum_{\substack{q_2 \sim R/q_1 \\ (q_2, \ell)=1}} \sum_{\substack{q_2' \sim R/q_1 \\ (q_2', \ell')=1 \\ (q_2 q_2', n_1 M)=1}} \sum_{d_2 \mid q_2} \sum_{d_2' \mid q_2'} \sum_{\substack{1 \le n_2 \le N_2 \\ (d_2, n_2) \mid q_2'\ell \\ (q_2, q_2') \mid n_2}} d_2 d_2' \left(1 + \frac{M_1(d_2, n_2)}{(d_1, n_1)d_2}\right) \\ &\cdot \min\left\{\frac{q_2}{[q_2/(q_2, q_2'), d_2]}, \frac{q_2'}{[q_2'/(q_2, q_2'), d_2']}\right\} \sum_{\substack{m' \sim M_1 \\ q_2 n_1 \ell' + \eta_1 m' n_2 \equiv 0 \pmod{d_2'}}} |\lambda_f(m')|^2 |\mathfrak{J}_{\boldsymbol{a}}(n_2)|.\end{aligned}$$

Let us make the following notation:

$$\begin{gathered}(q_2, q_2') = q_3, \quad q_2 = q_3 q_4, \quad q_2' = q_3 q_4' \\ d_2 = d_0 d_3 d_4, \quad d_0 \mid (q_3, q_4), \quad d_3 \mid q_3, \quad (d_3, q_4) = 1, \quad (d_4, q_3) = 1, \quad d_4 \mid q_4, \\ d_2' = d_3' d_4', \quad d_3' \mid q_3, \quad d_4' \mid q_4.\end{gathered}$$

It is easy to see that

$$\begin{aligned}(d_2, n_2) &\le (d_0 d_3, n_2)(d_4, n_2) \\ &\le d_0 d_3 (d_4, n_2) \\ &= d_0 d_3 (d_4, n_2/q_3), q_2/[q_2/(q_2, q_2'), d_2] \\ &= q_3 q_4/[q_4, d_2] \\ &\le q_3/d_3,\end{aligned}$$

and

$$q_2'/[q_2'/(q_2, q_2'), d_2'] = q_3 q_4'/[q_4', d_2'] \le q_3 q_4'/d_2'.$$

Then, breaking the n_2-sum into dyadic segments $n_2 \sim \tilde{N}_2$ with $\tilde{N}_2 \ll N_2$ and using Lemmas 5.1 and 5.2, one has

$$\begin{aligned}\Omega_{\boldsymbol{a},1} \ll \sup_{\substack{1\ll \tilde{N}_2 \ll N_2\\ \text{dyadic}}} \frac{N^{\varepsilon} q_1^4 r N_0 L^{2/3} M^{5/2}}{n_1^3 M_1^{1/2} R^3} & \sum_{d_1 \mid q_1} \sum_{d_1' \mid q_1} (d_1, n_1) d_1' \sum_{\substack{\ell \in \mathcal{L}\\ (\ell\ell', q_1)=1}} \sum_{\ell' \in \mathcal{L}} |A_\pi(1,\ell) A_\pi(1,\ell')| \\ & \cdot \sum_{\substack{q_3 \le R/q_1\\ (q_3, n_1 \ell\ell' M)=1}} \sum_{\substack{q_4 \sim R/q_3 q_1\\ (q_4,\ell)=1}} \sum_{\substack{q_4' \sim R/q_3 q_1\\ (q_4',\ell')=1\\ (q_4 q_4', n_1 M)=1}} \sum_{d_0 \mid (q_3,q_4)} \sum_{\substack{d_3 \mid q_3\\ (d_3,q_4)=1}} \sum_{\substack{d_4 \mid q_4\\ (d_4,q_3)=1}} d_0 d_3 d_4 \\ & \cdot \sum_{d_3' \mid q_3} \sum_{d_4' \mid q_4'} d_3' d_4' \sum_{\substack{n_2 \sim \tilde{N}_2\\ (d_2,n_2) \mid q_3 q_4' \ell\\ q_3 \mid n_2}} \left(1 + \frac{M_1 (d_4, n_2/q_3)}{(d_1,n_1) d_4}\right) C(\tilde{N}_2) \\ & \cdot \min\left\{\frac{q_3}{d_3}, \frac{q_3 q_4'}{d_3' d_4'}\right\} \sum_{\substack{m' \sim M_1\\ q_3 q_4 n_1 \ell' + \eta_2 m' n_2 \equiv 0 \pmod{d_3' d_4'}}} |\lambda_f(m')|^2,\end{aligned}$$

where

$$C(\tilde{N}_2) = \begin{cases} (RQ^{3/2} M^{1/2} n_1^{1/2})/(tNLX^{3/2} q_1^{1/2} \tilde{N}_2^{1/2}) & N_2' \ll \tilde{N}_2 \ll N_2 \text{ and } NLX/MRQ \ll t^{1-\varepsilon}, \\ 1/t & \tilde{N}_2 \ll N_2' \text{ and } NLX/MRQ \ll t^{1-\varepsilon}, \\ MRQ/NLX & \tilde{N}_2 \ll N_2 \text{ and } NLX/MRQ \gg t^{1-\varepsilon}. \end{cases} \tag{7-1}$$

Case (i): $q_3 q_4 n_1 \ell' + \eta_2 m' n_2 \neq 0$. Denote the contribution from this part in $\Omega_{\boldsymbol{a},1}$ by $\Omega_{\boldsymbol{a},11}$. Write

$$q_3 = d_3' q_5, \quad q_4 = d_0 q_6 \quad \text{and} \quad q_4' = d_4' q_6',$$

then we have

$$\begin{aligned}\Omega_{\boldsymbol{a},11} \ll \sup_{\substack{1\ll \tilde{N}_2 \ll N_2\\ \text{dyadic}}} \frac{N^{\varepsilon} q_1^5 r N_0 L^{2/3} M^{5/2}}{n_1^3 M_1^{1/2} R^3} & \sum_{d_1 \mid q_1} (d_1, n_1) \sum_{\ell \in \mathcal{L}} \sum_{\ell' \in \mathcal{L}} |A_\pi(1,\ell) A_\pi(1,\ell')| \\ & \cdot \sum_{d_3' \le R/q_1} d_3' \sum_{q_5 \le R/q_1 d_3'} \sum_{\substack{d_0 \le R/q_1 d_3' q_5\\ d_0 \mid d_3' q_5}} d_0 \sum_{\substack{d_3 \mid d_3' q_5\\ (d_3,q_4)=1}} \sum_{q_6 \sim R/q_1 d_3' d_0 q_5} \sum_{\substack{d_4 \mid d_0 q_6\\ (d_4, d_3' q_5)=1}} \\ & \cdot \sum_{\substack{n_2 \sim \tilde{N}_2\\ d_3' q_5 \mid n_2}} d_3' q_5 \left(d_4 + \frac{M_1 (d_4, n_2/d_3' q_5)}{(d_1,n_1)}\right) C(\tilde{N}_2) \sum_{m' \sim M_1} |\lambda_f(m')|^2 \\ & \cdot \sum_{\substack{d_4' \le R/q_1 d_3' q_5\\ 0 \neq d_3' d_4 q_5 q_6 n_1 \ell' + \eta_1 m' n_2 \equiv 0 \pmod{d_3' d_4'}}} d_4' \sum_{q_6' \sim R/q_1 d_3' q_5 d_4'} 1,\end{aligned}$$

By the well known bound of the divisor function, the number of the tuple (d_0, d_3, d_4, d_4') is bounded by $O(N^\varepsilon)$. Combining this together with (2-1) and (2-2), we get

$$\Omega_{\boldsymbol{a},11} \ll \sup_{\substack{1\ll\tilde{N}_2\ll N_2\\ \text{dyadic}}} \frac{N^\varepsilon q_1^3 r N_0 M^{5/2} M_1^{1/2} L^{8/3} \tilde{N}_2 C(\tilde{N}_2)}{n_1^3 R}(R+M_1) \tag{7-2}$$

Case (ii): $q_3q_4n_1\ell' + \eta_2 m' n_2 = 0$. Denote the contribution from this part in $\Omega_{\boldsymbol{a},1}$ by $\Omega_{\boldsymbol{a},12}$. In this subsection, we use $(d_2, n_2) \le (q_2'\ell, q_2) = q_3$. Therefore we have

$$\begin{aligned}
\Omega_{\boldsymbol{a},12} \ll \sup_{\substack{1\ll\tilde{N}_2\ll N_2\\ \text{dyadic}}} & \frac{N^\varepsilon q_1^4 r N_0 L^{2/3} M^{5/2}}{n_1^3 M_1^{1/2} R^3} \sum_{d_1\,|\,q_1}\sum_{d_1'\,|\,q_1} d_1'(d_1,n_1) \\
&\cdot \sum_{\ell\in\mathcal{L}}\sum_{\ell'\in\mathcal{L}} |A_\pi(1,\ell)A_\pi(1,\ell')| \sum_{q_3\le R/q_1}\sum_{q_4,q_4'\sim R/q_1q_3}\sum_{d_0\,|\,(q_3,q_4)}\sum_{\substack{d_3\,|\,q_3\\(d_3,q_4)=1}}\sum_{\substack{d_4\,|\,q_4\\(d_4,q_3)=1}} d_0d_3d_4 \\
&\cdot \sum_{d_3'\,|\,q_3}\sum_{d_4'\,|\,q_4'} d_3'd_4' \sum_{\substack{n_2\sim\tilde{N}_2\\ q_3\,|\,n_2}} \left(1+\frac{M_1q_3}{(d_1,n_1)d_0d_3d_4}\right) C(\tilde{N}_2) \\
&\cdot \min\left\{\frac{q_3}{d_3}, \frac{q_3q_4'}{d_3'd_4'}\right\} \sum_{\substack{m'\sim M_1\\ q_3q_4n_1\ell'+\eta_1m'n_2=0}} |\lambda_f(m')|^2 \\
\ll \sup_{\substack{1\ll\tilde{N}_2\ll N_2\\ \text{dyadic}}} & \frac{N^\varepsilon q_1^5 r N_0 L^{2/3} M^{5/2}}{n_1^3 M_1^{1/2} R^3} \sum_{d_1\,|\,q_1}(d_1,n_1)\sum_{m'\sim M_1}|\lambda_f(m')|^2 \sum_{q_3\le R/q_1} q_3 \sum_{\substack{n_2\sim\tilde{N}_2\\ q_3\,|\,n_2}} C(\tilde{N}_2) \\
&\cdot \sum_{q_4\sim R/q_1q_3}\sum_{\ell\in\mathcal{L}} |A_\pi(1,\ell)| \left(\frac{R}{q_1}+\frac{M_1q_3}{(d_1,n_1)}\right) \\
&\cdot \sum_{d_0\,|\,(q_3,q_4)}\sum_{\substack{d_3\,|\,q_3\\(d_3,q_4)=1}}\sum_{\substack{d_4\,|\,q_4\\(d_4,q_3)=1}}\sum_{d_3'\,|\,q_3}\sum_{\ell'\in\mathcal{L}} |A_\pi(1,\ell')|\delta_{q_3q_4\ell'\,|\,m'n_2} \sum_{q_4'\sim R/q_1q_3}\sum_{d_4'\,|\,q_4'} q_4'.
\end{aligned}$$

Now, we estimate the last two sums trivially, and then use the condition $\delta_{q_3q_4\ell'\,|\,m'n_2}$ together with (2-2) and (2-3), obtaining

$$\begin{aligned}
&\sum_{q_4\sim R/q_1q_3}\sum_{\ell\in\mathcal{L}} |A_\pi(1,\ell)| \left(\frac{R}{q_1}+\frac{M_1q_3}{(d_1,n_1)}\right) \\
&\quad\cdot \sum_{d_0\,|\,(q_3,q_4)}\sum_{\substack{d_3\,|\,q_3\\(d_3,q_4)=1}}\sum_{\substack{d_4\,|\,q_4\\(d_4,q_3)=1}}\sum_{d_3'\,|\,q_3}\sum_{\ell'\in\mathcal{L}} |A_\pi(1,\ell')|\delta_{q_3q_4\ell'\,|\,m'n_2} \sum_{q_4'\sim R/q_1q_3}\sum_{d_4'\,|\,q_4'} q_4' \\
&\qquad\ll \frac{R^2L^{1+\theta_3}}{q_1^2q_3^2}\left(\frac{R}{q_1}+\frac{M_1q_3}{(d_1,n_1)}\right),
\end{aligned}$$

where $\theta_3 \le \frac{5}{14}$. Therefore, it follows that

$$\Omega_{\boldsymbol{a},12} \ll \sup_{\substack{1\ll \tilde{N}_2 \ll N_2 \\ \text{dyadic}}} \frac{N^{\varepsilon} q_1^4 r N_0 L^{2/3} M^{5/2}}{n_1^3 M_1^{1/2} R^3} \sum_{d_1 \mid q_1} (d_1, n_1) \sum_{m \sim M_1} |\lambda_f(m')|^2 \sum_{q_3 \le R/q_1} q_3 \sum_{\substack{n_2 \sim \tilde{N}_2 \\ q_3 \mid n_2}} C(\tilde{N}_2) \cdot \frac{R^2 L^{1+\theta_3}}{q_1^2 q_3^2} \left(\frac{R}{q_1} + \frac{M_1 q_3}{(d_1, n_1)} \right)$$

$$\ll \sup_{\substack{1\ll \tilde{N}_2 \ll N_2 \\ \text{dyadic}}} \frac{q_1^3 r N^{\varepsilon} N_0 M^{5/2} M_1^{1/2} L^{5/3+\theta_3} \tilde{N}_2 C_1(\tilde{N}_2)}{n_1^3 R} (R + M_1). \tag{7-3}$$

Recall

$$\begin{aligned} Q &= \left(\frac{NL}{MK} \right)^{1/2}, \quad N_0 = \frac{N^2 L^2 X^3 r}{Q^3}, \quad N_2 = \frac{Q^2 R n_1}{NLX^2 q_1} t^{\varepsilon}, \\ N_2' &= t^{\varepsilon} \left(\frac{NLn_1}{M^2 R t^2 q_1} + \frac{R^2 Q^3 M n_1}{N^2 L^2 X^3 q_1} \right), \quad N \ll \frac{(Mt)^{3+\varepsilon}}{r^2}. \end{aligned} \tag{7-4}$$

For $NLX/(MRQ) \ll t^{1-\varepsilon}$, we have $M_1 \ll t^2 R^2 M^2 / N$. By taking $L = M^{1/4}$ and $K = t^{4/5}$, one has $R + M_1 \ll t^2 M^2 R Q / N$. Hence, by applying these bounds into (7-2) and (7-3), we derive that

$$\Omega_{\boldsymbol{a},1} \ll \sup_{\substack{1\ll \tilde{N}_2 \ll N_2 \\ \text{dyadic}}} \frac{N^{\varepsilon} q_1^3 r N_0 M^{11/2} R Q t^3 L^{8/3} \tilde{N}_2 C(\tilde{N}_2)}{n_1^3 N^{3/2}}.$$

Combining this together with (7-1) and (7-4), we get

$$\Omega_{\boldsymbol{a},1} \ll \frac{N^{\varepsilon} q_1^2 r^2}{n_1^2} \left(\frac{Q^3 L^{19/6} M^6 t^2}{N} + \frac{N^{3/2} L^{17/3} M^{7/2}}{Q^2} + \frac{Q^4 L^{8/3} M^{13/2} t^2}{N^{3/2}} \right).$$

For $NLX/(MRQ) \gg t^{1-\varepsilon}$, we have $M_1 \ll NL^2 X^2 / Q^2$ and $R \ll NLX/(MQt^{1-\varepsilon})$. Thus, in this case, we arrive at

$$\Omega_{\boldsymbol{a},1} \ll \frac{N^{\varepsilon} q_1^2 r^2}{n_1^2} \left(\frac{N^{5/2} L^{17/3} M^{3/2}}{Q^3 t^2} + \frac{N^{5/2} L^{20/3} M^{5/2}}{Q^4 t} \right).$$

Therefore, the contribution from $\Omega_{\boldsymbol{a},1}$ to (5-1) is

$$\begin{aligned} &\ll \frac{N^{3/4+\varepsilon} X^{1/2}}{M^2 L^{4/3} Q^{1/2} r^{1/2}} \sum_{n_1 \ll RMr} n_1^{\theta_3} \sum_{(n_1/(n_1,r)) \mid q_1 \mid (rn_1)^{\infty}} \frac{r}{n_1 q_1^{1/2}} \\ &\qquad \cdot \left(\frac{Q^3 L^{19/6} M^6 t^2}{N} + \frac{N^{3/2} L^{17/3} M^{7/2}}{Q^2} + \frac{Q^4 L^{8/3} M^{13/2} t^2}{N^{3/2}} + \frac{N^{5/2} L^{17/3} M^{3/2}}{Q^3 t^2} + \frac{N^{5/2} L^{20/3} M^{5/2}}{Q^4 t} \right)^{1/2} \\ &\ll r^{1/2} N^{3/4+\varepsilon} M^{1/2} L^{3/4} \left(\frac{t}{K^{1/2}} + K^{3/4} + \frac{K^{5/4}}{t^{1/2}} \right) + r^{1/2} N^{1+\varepsilon} \frac{L^{1/2} K}{M^{1/4} t}. \end{aligned} \tag{7-5}$$

7A2. *Case b.* By the same arguments, we obtain

$$\Omega_{\boldsymbol{b},1} \ll \sup_{\substack{1\ll \tilde{N}_2 \ll N_2 \\ \text{dyadic}}} \frac{N^{\varepsilon} q_1^4 r N_0 M^{5/2} M_1^{1/2} L^{8/3} \tilde{N}_2 C(\tilde{N}_2)}{n_1^3 R^2}(R+M_1),$$

where $M_1 \ll M^2R^2t^{\varepsilon}/N$ and $R \asymp (NLX)/(MQt)$. So we see that

$$\Omega_{\boldsymbol{b},1} \ll \frac{N^{\varepsilon} q_1^3 r^2}{n_1^2}\left(\frac{N^{3/2}L^{14/3}M^{5/2}}{Q^2t^2} + \frac{N^{3/2}L^{17/3}M^{7/2}}{Q^3t^3}\right),$$

which contributes (5-8) at most

$$\ll \frac{N^{1+\varepsilon}X^{1/2}r^{1/2}}{M^{5/2}L^{4/3}Q^{1/2}} \sum_{n_1 \ll RMr} \frac{1}{n_1^{1-\theta_3}} \sum_{(n_1/(n_1,r))|q_1|n_1^{\infty}} \frac{1}{q_1^{1/2}}\left(\frac{N^{3/2}L^{14/3}M^{5/2}}{Q^2t^2} + \frac{N^{3/2}L^{17/3}M^{7/2}}{Q^3t^3}\right)^{1/2}$$
$$\ll \frac{N^{1+\varepsilon}r^{1/2}L^{1/4}K^{3/4}}{M^{1/2}t} + \frac{N^{3/4+\varepsilon}r^{1/2}L^{1/2}M^{1/4}K}{t^{3/2}}. \tag{7-6}$$

7A3. *Case c.* Similarly, by the same treatment and the results in Section 5C, we have

$$\Omega_{\boldsymbol{c},1} \ll \frac{N^{\varepsilon} q_1^4 r N_0 M^{5/2} M_1^{1/2} L^3 \tilde{N}_2}{n_1^3 R^2}(R+M_1),$$

where $N_0 \ll (R^3M^3r/LN)t^{\varepsilon}$, $\tilde{N}_2 = (MrR^2n_1/q_1N_0)$ and $M_1 = R^2M^2t^2/N$. It is easy to see that

$$\Omega_{\boldsymbol{c},1} \ll \frac{q_1^3r^2}{n_1^2}\left(\frac{R^3M^{13/2}t^3L^3}{N^{3/2}} + \frac{R^2M^{9/2}tL^3}{N^{1/2}}\right).$$

Notice that $X \ll (MRQ/NL)t^{\varepsilon}$ now. Hence, the contribution from $\Omega_{\boldsymbol{c},1}$ to (5-9) is

$$\ll \frac{N^{5/4+\varepsilon}Xr^{1/2}}{M^{5/2}LQ}\frac{1}{t^{1/2}} \sum_{\eta_1=\pm 1}\sum_{n_1\le Rr} \frac{1}{n_1^{1-\theta_3}} \sum_{(n_1/(n_1,r))\,|\,q_1\,|\,(rn_1)^{\infty}} \frac{1}{q_1^{1/2}}\left(\frac{R^3M^{13/2}t^3L^3}{N^{3/2}} + \frac{R^2M^{9/2}tL^3}{N^{1/2}}\right)^{1/2}$$
$$\ll \frac{r^{1/2}N^{3/4}M^{1/2}L^{3/4}t}{K^{5/4}} + \frac{r^{1/2}NL^{1/2}}{M^{1/4}K}. \tag{7-7}$$

7B. $\boldsymbol{n_2 \equiv 0 \pmod{M}, n_2 \neq 0}$**.** Denote the contribution of this part to Ω by Ω_2. By the congruence condition $q_2'\bar{\alpha} - q_2\overline{\alpha'} \equiv -n_2 \pmod{M}$, we have $\alpha' \equiv \overline{q_2'}q_2\alpha \pmod{M}$. Hence,

$$\mathfrak{C}(n_2) \ll |\mathfrak{C}_1(n_2)||\mathfrak{C}_2(n_2)||\mathfrak{C}_3(n_2)|,$$

where $\mathfrak{C}_2(n_2)$ and $\mathfrak{C}_3(n_2)$ are defined as in Section 7A, and

$$\mathfrak{C}_1(n_2) = \sideset{}{^\star}\sum_{b \bmod M}\ \sideset{}{^\star}\sum_{b' \bmod M}\left(\sum_{\substack{u \bmod M\\ u\neq b}} \bar{\chi}(u)e\left(\frac{m\overline{q_2^2\ell(b-u)}}{M}\right)\right)$$
$$\cdot\left(\sum_{\substack{u' \bmod M\\ u'\neq b'}} \chi(u')e\left(-\frac{m'\overline{q_2'^2\ell'(b'-u')}}{M}\right)\right)\left(\sideset{}{^\star}\sum_{\alpha \bmod M} e\left(\frac{\alpha\overline{b q_2^2} - \alpha q_2\overline{b' q_2'^3}}{M}\right)\right)$$

Note that the innermost α-sum is a Ramanujan sum. We get

$$\mathfrak{C}_1(n_2) \ll M \Bigg| \sideset{}{^\star}\sum_{b \bmod M} \Bigg(\sum_{\substack{u \bmod M \\ u \neq b}} \bar{\chi}(u) e\Big(\frac{n q_2^2 \overline{\ell(b-u)}}{M}\Big)\Bigg)\Bigg(\sum_{\substack{u' \bmod M \\ u' \neq b q_2^3 \overline{q_2'}^3}} \chi(u') e\Big(\frac{n' q_2'^2 \overline{\ell'(b q_2^3 \overline{q_2'}^3 - u')}}{M}\Big)\Bigg)\Bigg|$$
$$+ \Bigg| \sideset{}{^\star}\sum_{b \bmod M} \sideset{}{^\star}\sum_{\substack{b' \bmod M \\ b' \not\equiv b q_2^3 \overline{q_2'}^3 \bmod M}} \Bigg(\sum_{\substack{u \bmod M \\ u \neq b}} \bar{\chi}(u) e\Big(\frac{n q_2^2 \overline{\ell(b-u)}}{M}\Big)\Bigg)$$
$$\cdot \Bigg(\sum_{\substack{u' \bmod M \\ u' \neq b'}} \chi(u') e\Big(\frac{n' q_2'^2 \overline{\ell'(b'-u')}}{M}\Big)\Bigg)\Bigg|.$$

As in [Sharma 2022, Section 6.2], there is a square root cancellation in the sum over u and u', so we arrive at

$$\mathfrak{C}_1(n_2) \ll M^3.$$

Therefore, by the same treatment as in Section 7A together with the condition $n_2 \equiv 0 \pmod M$, we can get a better result than that in Section 7A.

Combining the above argument together with (7-5), (7-6) and (7-7), the contribution of the non-zero frequencies can be dominated by

$$\ll r^{1/2} N^{3/4+\varepsilon} M^{1/2} L^{3/4} \Big(\frac{t}{K^{1/2}} + K^{3/4} + \frac{K^{5/4}}{t^{1/2}} \Big) + \frac{r^{1/2} N^{1+\varepsilon} L^{1/2}}{M^{1/4}} \Big(\frac{K}{t} + \frac{1}{K} \Big). \tag{7-8}$$

8. Proof of Proposition 3.1

Now we are ready to give an upper bound for $S_{11}^{\pm}(N, X, R)$ when $(r, M) = 1$. By (6-9) and (7-8), we get

$$S_{11}^{\pm}(N, X, R) \ll r^{1/2} N^{1/2+\varepsilon} L^{1/2} M^{5/4} (K^{3/2} + t) + \frac{r^{1/2} N^{3/4+\varepsilon} M^{3/4}}{L^{1/4}} \Big(K^{3/4} + \frac{K^{5/4}}{t^{1/2}} \Big)$$
$$+ r^{1/2} N^{3/4+\varepsilon} M^{1/2} L^{3/4} \Big(\frac{t}{K^{1/2}} + K^{3/4} + \frac{K^{5/4}}{t^{1/2}} \Big) + \frac{r^{1/2} N^{1+\varepsilon} L^{1/2}}{M^{1/4}} \Big(\frac{K}{t} + \frac{1}{K} \Big).$$

Noting that $N \ll (Mt)^{3+\varepsilon}/r^2$ and $r \ll M^{1/8} t^{3/10}$, and assuming $K < t$, we obtain

$$S_{11}^{\pm}(N, X, R) \ll N^{1/2+\varepsilon} \Bigg(M^{1/16} t^{3/20} L^{1/2} M^{5/4} (K^{3/2} + t) + \frac{L^{1/2}}{M^{7/4}} \Big(K t^{1/2} + \frac{t^{3/2}}{K} \Big)$$
$$+ \frac{M^{3/2}}{L^{1/4}} t^{3/4} K^{3/4} + M^{5/4} L^{3/4} t^{3/4} \Big(\frac{t}{K^{1/2}} + K^{3/4} \Big) \Bigg).$$

To balance the terms in the second line, the best choice of K is to satisfy $t/K^{1/2} = K^{3/4}$ and the best choice of L is to satisfy $M^{3/2}/L^{1/4} = M^{5/4} L^{3/4}$. Hence we should take

$$L = M^{1/4}, \quad K = t^{4/5},$$

from which we deduce that

$$S_{11}^{\pm}(N, X, R) \ll N^{1/2+\varepsilon} M^{3/2-1/16} t^{3/2-3/20}.$$

As we point out in Section 3, all the other cases (such as $S_{12}^{\pm}(N, X, R)$, $S_{13}^{\pm}(N, X, R)$, $S_2(N)$, $S_3(N)$) are similar and in fact easier. Hence, we finally prove Proposition 3.1.

Acknowledgements

We would like to thank Yongxiao Lin and Qingfeng Sun for helpful discussions and comments. We are grateful to the referee for his/her very helpful comments and suggestions.

References

[Aggarwal 2021] K. Aggarwal, "A new subconvex bound for GL(3) L-functions in the t-aspect", *Int. J. Number Theory* **17**:5 (2021), 1111–1138. MR Zbl

[Blomer 2012] V. Blomer, "Subconvexity for twisted L-functions on GL(3)", *Amer. J. Math.* **134**:5 (2012), 1385–1421. MR Zbl

[Blomer and Harcos 2008] V. Blomer and G. Harcos, "Hybrid bounds for twisted L-functions", *J. Reine Angew. Math.* **621** (2008), 53–79. MR Zbl

[Blomer et al. 2013] V. Blomer, R. Khan, and M. Young, "Distribution of mass of holomorphic cusp forms", *Duke Math. J.* **162**:14 (2013), 2609–2644. MR Zbl

[Burgess 1963] D. A. Burgess, "On character sums and L-series, II", *Proc. Lond. Math. Soc.* (3) **13** (1963), 524–536. MR Zbl

[Fan and Sun 2022] Y. Fan and Q. Sun, "A Bessel δ-method and hybrid bounds for GL_2", *Q. J. Math.* **73**:2 (2022), 617–656. MR Zbl

[Goldfeld 2006] D. Goldfeld, *Automorphic forms and L-functions for the group* $\mathrm{GL}(n, \mathbb{R})$, Cambridge Stud. Adv. Math. **99**, Cambridge Univ. Press, 2006. MR Zbl

[Goldfeld and Li 2006] D. Goldfeld and X. Li, "Voronoi formulas on GL(n)", *Int. Math. Res. Not.* **2006** (2006), art. id. 86295. MR Zbl

[Heath-Brown 1978] D. R. Heath-Brown, "Hybrid bounds for Dirichlet L-functions", *Invent. Math.* **47**:2 (1978), 149–170. MR Zbl

[Huang 2021a] B. Huang, "Hybrid subconvexity bounds for twisted L-functions on GL(3)", *Sci. China Math.* **64**:3 (2021), 443–478. MR Zbl

[Huang 2021b] B. Huang, "On the Rankin–Selberg problem", *Math. Ann.* **381**:3-4 (2021), 1217–1251. MR Zbl

[Huang 2021c] B. Huang, "Uniform bounds for GL(3) × GL(2) L-functions", preprint, 2021. arXiv 2104.13025

[Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc. Colloq. Publ. **53**, Amer. Math. Soc., Providence, RI, 2004. MR Zbl

[Kim 2003] H. H. Kim, "Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2", *J. Amer. Math. Soc.* **16**:1 (2003), 139–183. MR Zbl

[Kıral et al. 2019] E. M. Kıral, I. Petrow, and M. P. Young, "Oscillatory integrals with uniformity in parameters", *J. Théor. Nombres Bordeaux* **31**:1 (2019), 145–159. MR Zbl

[Kıral et al. 2022] E. M. Kıral, C. I. Kuan, and D. Lesesvre, "Subconvexity for twisted GL_3 L-functions", *Acta Arith.* **202**:3 (2022), 281–302. MR Zbl

[Kowalski et al. 2002] E. Kowalski, P. Michel, and J. VanderKam, "Rankin–Selberg L-functions in the level aspect", *Duke Math. J.* **114**:1 (2002), 123–191. MR Zbl

[Li 2011] X. Li, "Bounds for GL(3) × GL(2) L-functions and GL(3) L-functions", *Ann. of Math.* (2) **173**:1 (2011), 301–336. MR Zbl

[Lin 2021] Y. Lin, "Bounds for twists of GL(3) L-functions", *J. Eur. Math. Soc.* **23**:6 (2021), 1899–1924. MR Zbl

[Lin and Sun 2021] Y. Lin and Q. Sun, "Analytic twists of $\mathrm{GL}_3 \times \mathrm{GL}_2$ automorphic forms", *Int. Math. Res. Not.* **2021**:19 (2021), 15143–15208. MR Zbl

[Lin et al. 2023] Y. Lin, P. Michel, and W. Sawin, "Algebraic twists of $\mathrm{GL}_3 \times \mathrm{GL}_2$ L-functions", *Amer. J. Math.* **145**:2 (2023), 585–645. MR Zbl

[Michel and Venkatesh 2010] P. Michel and A. Venkatesh, "The subconvexity problem for GL_2", *Publ. Math. Inst. Hautes Études Sci.* **111** (2010), 171–271. MR Zbl

[Miller and Schmid 2006] S. D. Miller and W. Schmid, "Automorphic distributions, L-functions, and Voronoi summation for GL(3)", *Ann. of Math.* (2) **164**:2 (2006), 423–488. MR Zbl

[Munshi 2015a] R. Munshi, "The circle method and bounds for L-functions, III: t-aspect subconvexity for GL(3) L-functions", *J. Amer. Math. Soc.* **28**:4 (2015), 913–938. MR Zbl

[Munshi 2015b] R. Munshi, "The circle method and bounds for L-functions, IV: Subconvexity for twists of GL(3) L-functions", *Ann. of Math.* (2) **182**:2 (2015), 617–672. MR Zbl

[Munshi 2022] R. Munshi, "Subconvexity for $\mathrm{GL}(3)\times\mathrm{GL}(2)$ L-functions in t-aspect", *J. Eur. Math. Soc.* **24**:5 (2022), 1543–1566. MR Zbl

[Petrow and Young 2020] I. Petrow and M. P. Young, "The Weyl bound for Dirichlet L-functions of cube-free conductor", *Ann. of Math.* (2) **192**:2 (2020), 437–486. MR Zbl

[Petrow and Young 2023] I. Petrow and M. P. Young, "The fourth moment of Dirichlet L-functions along a coset and the Weyl bound", *Duke Math. J.* **172**:10 (2023), 1879–1960. MR

[Sharma 2022] P. Sharma, "Subconvexity for $\mathrm{GL}(3) \times \mathrm{GL}(2)$ twists", *Adv. Math.* **404**:B (2022), art. id. 108420. MR Zbl

[Weyl 1921] H. Weyl, "Zur Abschätzung von $\zeta(1+ti)$", *Math. Z.* **10** (1921), 88–101. Zbl

Communicated by Philippe Michel
Received 2021-04-21 Revised 2022-03-20 Accepted 2022-10-17

brhuang@sdu.edu.cn *Data Science Institute and School of Mathematics, Shandong University, Jinan, China*

zxu@sdu.edu.cn *School of Mathematics, Shandong University, Jinan, China*

ALGEBRA AND NUMBER THEORY 17:10 (2023)
https://doi.org/10.2140/ant.2023.17.1753

Separation of periods of quartic surfaces

Pierre Lairez and Emre Can Sertöz

We give a computable lower bound for the distance between two distinct periods of a given quartic surface defined over the algebraic numbers. The main ingredient is the determination of height bounds on components of the Noether–Lefschetz loci. This makes it possible to study the Diophantine properties of periods of quartic surfaces and to certify a part of the numerical computation of their Picard groups.

1. Introduction

Periods are a countable set of complex numbers containing all the algebraic numbers, as well as many of the transcendental constants of nature. In light of the ubiquity of periods in mathematics and the sciences, Kontsevich and Zagier [2001] asked for the development of an algorithm to check for the equality of two given periods. We solve this problem for periods coming from quartic surfaces by giving a computable separation bound, that is, a lower bound on the minimum distance between distinct periods.

Let $f \in \mathbb{C}[w, x, y, z]_4$ be a homogeneous quartic polynomial defining a smooth quartic X_f in $\mathbb{P}^3(\mathbb{C})$. The periods of X_f are the integrals of a nowhere vanishing holomorphic 2-form on X_f over integral 2-cycles in X_f. The periods can also be given in the form of integrals of a rational function

$$\frac{1}{2\pi i}\oint_\gamma \frac{\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z}{f(1,x,y,z)}, \tag{1}$$

where γ is a 3-cycle in $\mathbb{C}^3 \setminus X_f$. The integral (1) depends only on the homology class of γ. These periods form a group under addition. The geometry of quartic surfaces dictates that there are only 21 independent 3-cycles in $\mathbb{C}^3 \setminus X_f$. These give 21 periods $\alpha_1, \dots, \alpha_{21} \in \mathbb{C}$ such that the integral over any other 3-cycle is an integer linear combination of these periods.

It is possible to compute the periods to high precision [Sertöz 2019], typically to thousands of decimal digits, and to deduce from them interesting algebraic invariants such as the Picard group of X_f [Lairez and Sertöz 2019]. This point of view has been fruitful for computing algebraic invariants for algebraic curves from their periods [van Wamelen 1999; Costa et al. 2019; Bruin et al. 2019; Booker et al. 2016].

For quartic surfaces, the computation of the Picard group reduces to computing the lattice in $\mathbb{Z}^{21}$ of integer relations $x_1\alpha_1 + \cdots + x_{21}\alpha_{21} = 0$, where $x_i \in \mathbb{Z}$. A basis for this lattice can be guessed from approximate α_i's using lattice reduction algorithms. But is it possible to *prove* that all guessed relations are true relations? Previous work related to this question [Simpson 2008] required explicit construction of

MSC2020: primary 14Q10, 14J28, 32G20; secondary 11Y16, 14Q20, 11J99.
Keywords: K3 surfaces, periods, Diophantine approximation, Hodge loci, effective mathematics.

algebraic curves on X_f, which becomes challenging very quickly. Instead, we give a method of proving relations by checking them at a predetermined finite precision. At the moment, this is equally challenging, but we conjecture that the numerical approach can be made asymptotically faster, see Section 4.4 for details.

The Lefschetz theorem on (1, 1)-classes (Section 2.2) associates a divisor on X_f to any integer relation between the periods of X_f. In turn, the presence of a divisor imposes algebraic conditions on the coefficients of f. Such algebraic conditions define the *Noether–Lefschetz loci* on the space of quartic polynomials (Section 3). In addition to the degree computations of Maulik and Pandharipande [2013], we give height bounds on the polynomial equations defining the Noether–Lefschetz loci (Theorem 14). These lead to our main result (Theorem 17): Assume f has algebraic coefficients, then for $x_i \in \mathbb{Z}$,

$$x_1\alpha_1 + \cdots + x_{21}\alpha_{21} = 0 \quad \text{or} \quad |x_1\alpha_1 + \cdots + x_{21}\alpha_{21}| > 2^{-c^{\max_i |x_i|^9}} \tag{2}$$

for some constant $c > 0$ depending only on f and the choice of the 21 independent 3-cycles (see Theorem 17 for a coordinate-free formulation). The constant c is computable in rather simple terms and without prior knowledge of the Picard group of X_f. We use the term "computable" in the sense of "computable with a Turing machine", not "primitive recursive", as our suggested algorithm to compute c depends, through Lemma 1, on the numerical computation of a nonzero constant (depending on f), whose magnitude is not known *a priori*, only the fact that it is nonzero.

The expression (2) is essentially a lower bound for the linear independence measure [Shidlovskii 1989, Chapter 11] for the periods of X_f. Our construction of this bound bears a loose resemblance to the ideas involved in the statement of the analytic subgroup theorem [Wüstholz 1989], and in particular, to the Masser–Wüstholz period theorem [1993]. We briefly comment on this analogy in Section 5.4.

As a consequence of the separation bound (2), we apply a construction in the manner of Liouville [1851] and prove, for instance, that the number

$$\sum_{n\geq 0} (2\upuparrows 3n)^{-1} \tag{3}$$

is not a quotient of two periods of a single quartic surface that is defined over $\bar{\mathbb{Q}}$, where $2\upuparrows 3n$ denotes an exponentiation tower with $3n$ twos (Theorem 19, with $\theta_{i+1} = 2^{2^{2^{\theta_i}}}$).

The methods we employed to attain the period separation bound (2) can, in principle, be generalized to separate the periods of some other algebraic varieties, e.g., of cubic fourfolds. We discuss these and other generalizations in Section 5.

2. Periods and deformations

2.1. ***Construction of the period map.*** For any nonzero homogeneous polynomial f in $\mathbb{C}[w, x, y, z]$, let X_f denote the surface in $\mathbb{P}^3$ defined as the zero locus of f. Let $R \doteq \mathbb{C}[w, x, y, z]$, and let $R_4 \subset R$ be the subspace of degree 4 homogeneous polynomials. Let $U_4 \subset R_4$ denote the dense open subset of all homogeneous polynomials f of degree 4 such that X_f is smooth. For our purposes, it will be useful to consider not only the periods of a single quartic surface X_f, but also the *period map*, to study the dependence of periods on f.

The topology of X_f does not depend on f as long as X_f is smooth: given two polynomials $f, g \in U_4$, we can connect them by a continuous path in U_4, and the surface X_f deforms continuously along this path, giving a homeomorphism $X_f \simeq X_g$, which is uniquely defined up to isotopy. In particular, if we fix a base point $b \in U_4$, then for every $f \in \widetilde{U}_4$, where $\widetilde{U}_4$ is a universal covering of U_4, we have a uniquely determined isomorphism of cohomology groups $H^2(X_b, \mathbb{Z}) \simeq H^2(X_f, \mathbb{Z})$. Let $H_{\mathbb{Z}}$ denote the second cohomology group of X_b, which is isomorphic to $\mathbb{Z}^{22}$, e.g., [Huybrechts 2016, §1.3.3].

The hyperplane class and its multiples are redundant for the problem we are interested in, as their periods are 0. In practice, therefore, we work with a rank 21 quotient lattice. The map (7) below identifies this quotient with the cohomology of the complement of the quartic.

An element of $\widetilde{U}_4$ determines a polynomial $f \in U_4$ together with an identification of $H^2(X_f, \mathbb{Z})$ with $H_{\mathbb{Z}}$. We often work locally around a given polynomial f and, in that case, we do not actively distinguish between U_4 and its universal covering.

The group $H_{\mathbb{Z}}$ is endowed with an even unimodular pairing

$$(x, y) \in H_{\mathbb{Z}} \times H_{\mathbb{Z}} \to x \cdot y \in \mathbb{Z}, \tag{4}$$

given by the intersection form on cohomology. Through this pairing, the second homology and cohomology groups are canonically identified with one another. For K3 surfaces, such as smooth quartic surfaces in $\mathbb{P}^3$, the structure of the lattice $H_{\mathbb{Z}}$ with its intersection form is explicitly known [Huybrechts 2016, Proposition 1.3.5]. The fundamental class of a generic hyperplane section of X_f gives an element of $H_{\mathbb{Z}}$ denoted by h.

Further, the complex cohomology group $H^2(X_f, \mathbb{C})$, which is just $H_{\mathbb{C}} \doteq H_{\mathbb{Z}} \otimes \mathbb{C}$, is isomorphic to the corresponding de Rham cohomology $H^2_{\mathrm{dR}}(X_f, \mathbb{C})$ group as follows: Elements of $H^2_{\mathrm{dR}}(X_f, \mathbb{C})$ are represented by differential 2-forms. To a form Ω, one associates the element $\Theta(\Omega)$ of $H^2(X_f, \mathbb{C})$ given by the map

$$\Theta(\Omega)\colon [\gamma] \in H_2(X_f, \mathbb{C}) \mapsto \int_\gamma \Omega \in \mathbb{C}. \tag{5}$$

The group $H^2_{\mathrm{dR}}(X_f, \mathbb{C})$ has a distinguished element Ω_f, a nowhere vanishing holomorphic 2-form, described below. Every other holomorphic 2-form on X_f is a scalar multiple of Ω_f [Huybrechts 2016, Example 1.1.3]. Mapping Ω_f to $H_{\mathbb{C}}$ gives rise to the *period map*

$$\mathcal{P}\colon f \in \widetilde{U}_4 \mapsto \omega_f \doteq \Theta(\Omega_f) \in H_{\mathbb{C}}. \tag{6}$$

The coordinates of the *period vector* ω_f, in some fixed basis of $H_{\mathbb{Z}}$, generates the group of periods of X_f.

There is a standard Thom–Gysin type map in homology

$$T\colon H_2(X_f, \mathbb{Z}) \to H_3(\mathbb{P}^3 \setminus X_f, \mathbb{Z}), \tag{7}$$

see [Voisin 2003, p. 159] for a modern description. Roughly speaking, T takes the class of a 2-cycle in X_f and returns the class of a narrow S^1-bundle around the cycle lying entirely in $\mathbb{P}^3 \setminus X_f$. See [Griffiths 1969a, §3] for this classical interpretation. The map T is a surjective morphism, and its kernel is generated by the class of a hyperplane section of X_f.

We choose Ω_f so that the following identity holds:

$$\int_\gamma \Omega_f = \frac{1}{2\pi i} \int_{T(\gamma)} \frac{\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z}{f(1,x,y,z)}. \tag{8}$$

Therefore, in view of (5), the coefficients of ω_f in a basis of $H_{\mathbb{Z}}$ coincides with periods as defined in (1).

The image $\mathcal{D}$ of the period map $\mathcal{P}$ is called the *period domain*. It admits a simple description

$$\mathcal{D} \doteq \mathcal{P}(\widetilde{U}_4) = \left\{ w \in H_{\mathbb{C}} \setminus \{0\} \mid w \cdot h = 0,\ w \cdot w = 0,\ w \cdot \overline{w} > 0 \right\}, \tag{9}$$

where "$\cdot$" denotes the intersection form on $H_{\mathbb{Z}}$, extended to $H_{\mathbb{C}}$ by $\mathbb{C}$-linearity, and h denotes the fundamental class of a hyperplane section, as introduced above [Huybrechts 2016, Chapter 6]. Moreover, by the local Torelli theorem for K3 surfaces [Huybrechts 2016, Proposition 6.2.8], the map $\mathcal{P}$ is a submersion: its derivative at any point of $\widetilde{U}_4$ is surjective.

2.2. ***The Lefschetz (1,1)-theorem.*** Lefschetz proved that the linear integer relations between the periods of a quartic surface X_f are in correspondence with homology classes coming from algebraic curves in X_f. We now explain this statement in more detail. Let $C \subset X_f$ be an algebraic curve. Its fundamental class is the element $[C]$ of $H_{\mathbb{Z}}$ obtained as the Poincaré dual of the homology class of C. Here, we identify $H_{\mathbb{Z}}$ with $H^2(X_f, \mathbb{Z})$ by fixing a preimage of f in $\widetilde{U}_4$. The Picard group $\operatorname{Pic}(X_f)$ of X_f is the sublattice of $H_{\mathbb{Z}}$ spanned by the fundamental classes of algebraic curves.

It follows from the definition that for any class $[\Omega] \in H^2_{\mathrm{dR}}(X_f)$ of a differential 2-form on X_f,

$$[C] \cdot \Theta(\Omega) = \int_C \Omega. \tag{10}$$

Moreover, if Ω is a holomorphic 2-form, then $\int_C \Omega = 0$, because the restriction of Ω to the complex 1-dimensional subvariety C vanishes. In particular $[C] \cdot \omega_f = 0$. It turns out that this condition characterizes the elements of $\operatorname{Pic}(X_f)$.

More precisely, let $H^{1,1}(X_f) \subset H_{\mathbb{C}}$ denote the space orthogonal to ω_f and $\bar{\omega}_f$, the conjugate of ω_f, with respect to the intersection form. This space is a direct summand in the Hodge decomposition of $H^2(X_f, \mathbb{C})$.

The Lefschetz (1,1)-theorem [Griffiths and Harris 1978, p. 163] asserts that the lattice of integer relations coincide with the Picard group

$$\operatorname{Pic}(X_f) = H_{\mathbb{Z}} \cap H^{1,1}(X_f). \tag{11}$$

Noting that for any $\gamma \in H_{\mathbb{Z}}$, we have $\bar{\gamma} = \gamma$, where $\bar{\gamma}$ denotes the complex conjugate, it follows that $\overline{\omega_f \cdot \gamma} = \bar{\omega}_f \cdot \gamma$, so that (11) becomes

$$\operatorname{Pic}(X_f) = \{\gamma \in H_{\mathbb{Z}} \mid \gamma \cdot \omega_f = 0\}. \tag{12}$$

2.3. ***A deformation argument.*** Let $\gamma_1, \dots, \gamma_{22}$ be a basis of $H_{\mathbb{Z}}$. The space $H_{\mathbb{R}}$ (respectively, $H_{\mathbb{C}}$) is endowed with the coefficientwise Euclidean (respectively, Hermitian) norm

$$\left\| \sum_{i=1}^{22} x_i \gamma_i \right\|^2 \doteq \sum_{i=1}^{22} |x_i|^2. \tag{13}$$

For $\gamma \in H_{\mathbb{Z}}$, if $|\gamma \cdot \omega_f|$ is small enough, then γ is close to being an integer relation between the periods of X_f. We want to argue that, in this case, γ is a genuine integer relation between the periods of X_g for some polynomial $g \in U_4$ close to f.

Recall $f, g \in \widetilde{U}_4$ means f and g are smooth quartics with second cohomology identified with $H_{\mathbb{Z}}$. The space $\widetilde{U}_4$ inherits a metric from U_4, so that $\widetilde{U}_4 \to U_4$ is locally isometric. The metric on $U_4 \subset R_4 \simeq \mathbb{C}^{35}$ is induced by an inner product. The choice of an inner product will change the distances, but this is absorbed into the constants in the statements below.

Let $f \in \widetilde{U}_4$ be fixed. For any $g \in R_4$ and $t \in \mathbb{C}$ small enough, the polynomials $f + tg \in R_4$ lift canonically to $\widetilde{U}_4$. For any $\gamma \in H_{\mathbb{C}}$, we consider the map

$$\phi_{\gamma,g}(t) \doteq \gamma \cdot \mathcal{P}(f + tg), \tag{14}$$

which is well defined and analytic in a neighborhood of 0 in $\mathbb{C}$.

Lemma 1. *There is a constant $C > 0$, depending only on f, such that for any $\gamma \in H_{\mathbb{C}}$ satisfying $\gamma \cdot h = 0$ and $|\gamma \cdot \bar{\omega}_f| \|\omega_f\| \le \frac{1}{2} \|\gamma\| (\omega_f \cdot \bar{\omega}_f)$, there is a monomial $m \in R_4$ for which $|\phi'_{\gamma,m}(0)| \ge C \|\gamma\|$.*

Proof. Observe that for any monomial $m \in R_4$, we have $\phi'_{\gamma,m}(0) = \gamma \cdot \mathrm{d}_f \mathcal{P}(m)$, where $\mathrm{d}_f \mathcal{P}$ is the derivative at f of $\mathcal{P}$. Let Q be the positive semidefinite Hermitian form defined on $H_{\mathbb{C}}$ by

$$Q(\gamma) \doteq \sum_m |\gamma \cdot \mathrm{d}_f \mathcal{P}(m)|^2, \tag{15}$$

where the sum is taken over the monomials in m. Since $\max_m |\phi'_{\gamma,m}(0)|^2 \ge (1/\dim R_4) Q(\gamma)$, it is enough to prove that $Q(\gamma) \ge C\|\gamma\|$ for some constant $C > 0$, when $\gamma \cdot h = 0$ and $|\gamma \cdot \bar{\omega}_f| \|\omega_f\| \le \frac{1}{2} \|\gamma\| (\omega_f \cdot \bar{\omega}_f)$.

The form Q vanishes exactly on the orthogonal complement (for the intersection product) of the tangent space $T_{\omega_f}\mathcal{D}$ of $\mathcal{D}$ at ω_f. By (9),

$$T_{\omega_f}\mathcal{D} = \{w \in H_{\mathbb{C}} \mid w \cdot h = w \cdot \omega_f = 0\}. \tag{16}$$

So the kernel of Q is $K \doteq \mathbb{C}h + \mathbb{C}\omega_f$. Moreover, let E be the orthogonal complement of $\mathbb{C}h + \mathbb{C}\bar{\omega}_f$ (still for the intersection product). Since $h \cdot \omega_f = h \cdot \bar{\omega}_f = 0$, $h \cdot h = 4$ and $\omega_f \cdot \bar{\omega}_f > 0$, we check that $E \cap K = 0$. In particular, the form Q is positive definite on E, so there is a constant $C > 0$ such that $Q(\eta) \ge C\|\eta\|$ for any $\eta \in E$. This constant is easily computable as the smallest eigenvalue of the matrix of the restriction of Q on that space, in a unitary basis, for the Hermitian norm $\|-\|$.

Now, let γ such that $\gamma \cdot h = 0$ and

$$|\gamma \cdot \bar{\omega}_f| \|\omega_f\| \leq \tfrac{1}{2} \|\gamma\| (\omega_f \cdot \bar{\omega}_f). \tag{17}$$

Let $a \doteq (\gamma \cdot \bar{\omega}_f)/(\omega_f \cdot \bar{\omega}_f)$ and $\eta \doteq \gamma - a\omega_f$, so that $\eta \cdot \bar{\omega}_f = 0$ and $\eta \cdot h = 0$, that is, $\eta \in E$. Since ω_f is in the kernel of Q, we have $Q(\eta) = Q(\gamma)$, and thus $Q(\gamma) \geq C\|\eta\|$. Lastly, we compute that

$$\|\eta\| \geq \|\gamma\| - |a| \|\omega_f\| = \|\gamma\| - \left| \frac{\gamma \cdot \overline{\omega_f}}{\omega_f \cdot \bar{\omega}_f} \right| \|\omega_f\| \geq \frac{1}{2} \|\gamma\|, \tag{18}$$

using (17). So $Q(\gamma) \geq \frac{1}{2} C \|\gamma\|$. □

The next statement is proved using the following result of [Smale 1986]. Let ϕ be an analytic function on a maximal open disc around 0 in $\mathbb{C}$ with $\phi'(0) \neq 0$. We define

$$\gamma_{\text{Smale}}(\phi) \doteq \sup_{k \geq 2} \left| \frac{1}{k!} \frac{\phi^{(k)}(0)}{\phi'(0)} \right|^{1/(k-1)} \quad \text{and} \quad \beta_{\text{Smale}}(\phi) \doteq \left| \frac{\phi(0)}{\phi'(0)} \right|. \tag{19}$$

If $\beta_{\text{Smale}}(\phi)\gamma_{\text{Smale}}(\phi) \leq \frac{1}{34}$, then there is a $t \in \mathbb{C}$ such that $|t| \leq 2\beta_{\text{Smale}}(\phi)$ and $\phi(t) = 0$ [Smale 1986], see also [Blum et al. 1998, Chapter 8, Theorem 2].

Proposition 2. *For any $f \in \widetilde{U}_4$, there exists C_f and $\varepsilon_f > 0$ such that for all $\varepsilon < \varepsilon_f$ the following holds: For any $\gamma \in H_{\mathbb{R}}$, if $\gamma \cdot h = 0$ and $|\gamma \cdot \omega_f| \leq \varepsilon \|\gamma\|$, then there is a monomial $m \in R_4$ and $t \in \mathbb{C}$ such that $|t| \leq C_f \varepsilon$ and $\gamma \cdot \omega_{f+tm} = 0$.*

Proof. Let $\gamma \in H_{\mathbb{R}}$ such that $\gamma \cdot h = 0$ and

$$|\gamma \cdot \omega_f| \leq \left(\frac{\omega_f \cdot \bar{\omega}_f}{2\|\omega_f\|} \right) \|\gamma\|. \tag{20}$$

Since γ has real coefficients, we have $|\gamma \cdot \omega_f| = |\gamma \cdot \bar{\omega}_f|$ and we may apply Lemma 1 to obtain a monomial m and a constant C such that

$$|\phi'_{\gamma,m}(0)| \geq C\|\gamma\|. \tag{21}$$

It follows, in particular, that

$$\beta_{\text{Smale}}(\phi_{\gamma,m}) \leq \frac{|\gamma \cdot \omega_f|}{C\|\gamma\|}. \tag{22}$$

Moreover, for any $k \geq 2$, and using $C \leq 1$,

$$\begin{aligned}
\left| \frac{1}{k!} \frac{\phi^{(k)}_{\gamma,m}(0)}{\phi'_{\gamma,m}(0)} \right|^{1/(k-1)} &\leq C^{-1} \left| \frac{\phi^{(k)}_{\gamma,m}(0)}{k!\|\gamma\|} \right|^{1/(k-1)} \\
&= C^{-1} \left| \frac{\gamma}{\|\gamma\|} \cdot \frac{1}{k!} \mathrm{d}^k_f \mathcal{P}(m, \dots, m) \right|^{1/(k-1)} &(23)\\
&\leq C^{-1} \left\| \frac{1}{k!} \mathrm{d}^k_f \mathcal{P} \right\|^{1/(k-1)}, &(24)
\end{aligned}$$

where $\mathrm{d}_f^k\mathcal{P} : R_4^k \to H_{\mathbb{C}}$ is the k-th higher derivative of $\mathcal{P}$ at f and where $|||\cdot|||$ is the operator norm defined as

$$\left\|\left\| \frac{1}{k!}\mathrm{d}_f^k\mathcal{P} \right\|\right\| \doteq \sup_{\gamma\in H_{\mathbb{C}}} \sup_{h_1,\dots,h_k} \frac{\left|\gamma\cdot(1/k!)\mathrm{d}_f^k\mathcal{P}(h_1,\dots,h_n)\right|}{\|\gamma\|\|h_1\|\cdots\|h_n\|}, \tag{25}$$

with supremum taken over $h_1,\dots,h_n \in \mathbb{C}[w,x,y,z]_4$. It follows that

$$\gamma_{\mathrm{Smale}}(\phi_{\gamma,m}) \le C^{-1}\sup_{k\ge 2}\left\|\left\| \frac{1}{k!}\mathrm{d}_f^k\mathcal{P} \right\|\right\|^{1/(k-1)}. \tag{26}$$

Let Γ denote the supremum on the right-hand side of (26). By Smale's theorem, together with (22) and (26), if $|\gamma\cdot\omega_f| \le \frac{1}{34}C^2\Gamma^{-1}\|\gamma\|$, then there is a $t\in\mathbb{C}$ such that $|t| \le 2C^{-1}|\gamma\cdot\omega_f|\|\gamma\|^{-1}$ and $\gamma\cdot\mathcal{P}(f+tm)=0$. The claim follows with $C_f \doteq 2C^{-1}$ and

$$\varepsilon_f \doteq \min\left(\frac{1}{34}C^2\Gamma^{-1}, \frac{\omega_f\cdot\bar{\omega}_f}{2\|\omega_f\|}\right). \tag{27}$$

This concludes the proof. □

The constants C_f and ε_f are actually computable with simple algorithms. The constant from Lemma 1 is not hard to get with elementary linear algebra. It only remains to compute an upper bound for Γ. We address this issue in Section 2.4.

Corollary 3. *For any $f \in \widetilde{U}_4$, any $\varepsilon < \varepsilon_f$ and any $\gamma \in H_{\mathbb{Z}}$, if $|\gamma\cdot\omega_f| \le \frac{1}{4}\varepsilon$, then there exists a monomial $m\in R_4$ and $t\in\mathbb{C}$ such that $|t|\le C_f\varepsilon$ and $\gamma\in\mathrm{Pic}(X_{f+tm})$.*

Proof. We may assume that $\gamma\cdot\omega_f \ne 0$ (otherwise, choose any m and $t=0$). Let $\gamma' = \gamma - \frac{1}{4}(\gamma\cdot h)h$. Since $h\cdot h = 4$, we have $\gamma'\cdot h = 0$. Moreover, we have $\gamma'\cdot\omega_f = \gamma\cdot\omega_f \ne 0$. In particular, $\gamma'\ne 0$, and since $\gamma'\in\frac{1}{4}H_{\mathbb{Z}}$, we have $\|\gamma'\|\ge\frac{1}{4}$. Then

$$|\gamma'\cdot\omega_f| \le 4\|\gamma'\||\gamma\cdot\omega_f| \le \varepsilon\|\gamma'\|, \tag{28}$$

and Proposition 2 applies. □

2.4. ***Effective bounds for the higher derivatives of the period map.*** In the proof of Proposition 2, only the quantity Γ is not clearly computable. We show in this section how to compute an upper bound for Γ using the Griffiths–Dwork reduction. We follow here [Griffiths 1969a; Griffiths 1969b].

Firstly, as a variant of (8) avoiding dehomogeneization, we write

$$\mathcal{P}(f) = \left(\frac{1}{2\pi i}\int_{T(\gamma_i)}\frac{\mathrm{Vol}}{f}\right)_{1\le i\le 22}, \tag{29}$$

where Vol is the projective volume form

$$\mathrm{Vol} \doteq w\,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z - x\,\mathrm{d}w\,\mathrm{d}y\,\mathrm{d}z + y\,\mathrm{d}w\,\mathrm{d}x\,\mathrm{d}z - z\,\mathrm{d}w\,\mathrm{d}x\,\mathrm{d}y. \tag{30}$$

For any $k>0$ and $a\in R_{4k-4}$, we denote

$$\int\frac{a\,\mathrm{Vol}}{f^k} \doteq \left(\frac{1}{2\pi i}\int_{T(\gamma_i)}\frac{a\,\mathrm{Vol}}{f^k}\right)_{1\le i\le 22} \in H_{\mathbb{C}}. \tag{31}$$

For any $h \in R_4$ close enough to 0, we have the power series expansion

$$\int \frac{\mathrm{Vol}}{f+h} = \sum_{k\geq 1} (-1)^{k-1} \int \frac{h^{k-1}\,\mathrm{Vol}}{f^k}. \tag{32}$$

Proposition 4. *For any $k \geq 3$, there is a linear map $G_k \colon R_{4k-4} \to R_8$ such that*

$$\int \frac{a}{f^k}\,\mathrm{Vol} = \int \frac{G_k(a)}{f^3}\,\mathrm{Vol}\,.$$

Moreover, there is a computable constant C, which depends only on f, such that for any $k \geq 3$, we have $|||G_k||| \leq C^{k-3}$, where R is endowed with the 1-norm (57).

Before we begin the proof of proposition, let us show that this is enough to bound Γ. Let

$$A\colon a \in R_8 \mapsto \int (a/f^3)\,\mathrm{Vol} \in H_{\mathbb{C}},$$

then, using (32), we obtain

$$\int \frac{\mathrm{Vol}}{f+h} = \sum_{k\geq 1} (-1)^{k-1} A(G_k(h^{k-1})), \tag{33}$$

and it follows that

$$\frac{1}{k!}\mathrm{d}^k_f \mathcal{P}(h_1, \ldots, h_k) = (-1)^k A(G_{k+1}(h_1 \cdots h_k)). \tag{34}$$

In particular,

$$\left\| \frac{1}{k!}\mathrm{d}^k_f \mathcal{P}(h_1, \ldots, h_k) \right\| \leq |||A|||\,|||G_{k+1}|||\, \|h_1 \cdots h_n\|_1 \tag{35}$$

$$\leq |||A|||\,|||G_{k+1}|||\, \|h_1\|_1 \cdots \|h_n\|_1, \tag{36}$$

and therefore, $|||(1/k!)\mathrm{d}^k_f \mathcal{P}||| \leq |||A|||C^{k+1}$, from which we get

$$\Gamma \leq C \max\bigl(|||A|||C^2, 1\bigr). \tag{37}$$

Let us remark on how to bound the operator norm of A in practice. The period integrals can be approximated to arbitrary precision and with rigorous error bounds as in [Sertöz 2019]. This construction gives a small neighborhood of A in the matrix space. In practice, we represent this neighborhood as a matrix A' of complex balls and compute the operator norm of A' as usual but using complex ball arithmetic. This will return a real open interval containing $|||A||| \neq 0$. If the precision is high enough, 0 will not be contained in the closure of this interval, and we can take the lower bound of the interval.

2.4.1. *Proof of Proposition 4.* Let $R = \mathbb{C}[w, x, y, z]$. We define two families of maps for this proof. First, for $d \geq 12$, a multivariate division map $Q_d \colon R_d \to R^4_{d-3}$, such that for any $a \in R_d$,

$$a = \sum_{i=0}^{3} Q_d(a)_i\, \partial_i f. \tag{38}$$

Note that such a map exists as soon as $d \geq 12$ by a theorem due to Macaulay, see [Lazard 1977, Corollaire, p. 169]. The choice of Q_d is not unique. We fix Q_{12} arbitrarily and define $Q_d(a)$, for $d > 12$ and $a \in R_{12}$, as follows: Write $a = \sum_{i=0}^{3} x_i a_i$, in such a way that the terms of the sum have disjoint monomial support, and define

$$Q_d(a) = \sum_{i=0}^{3} x_i Q_{d-1}(a_i). \tag{39}$$

It is easy to check that this definition satisfies (38).

Second, for $k \geq 3$, we define $G_k \colon R_{4k-4} \to R_8$ as follows: Begin with $G_3 = \mathrm{id}$, and then define G_k for $k \geq 4$ inductively. For $a \in R_{4k-4}$, we write $(b_0, \ldots, b_3) = Q_{4k-4}(a)$ and define

$$G_k(a) \doteq G_{k-1}\Big(\frac{1}{k-1}(\partial_0 b_0 + \cdots + \partial_3 b_3)\Big). \tag{40}$$

This map is the Griffiths–Dwork reduction, and it satisfies

$$\int_\gamma \frac{a\Omega}{f^k} = \int_\gamma \frac{G_k(a)\Omega}{f^3}. \tag{41}$$

Lemma 5. *For any $d \geq 12$, we have $|||Q_d||| \leq |||Q_{12}|||$, where R is endowed with the 1-norm and R^4 with the norm $\|(f_0, \ldots, f_3)\|_1 \doteq \|f_0\|_1 + \cdots + \|f_3\|_1$.*

Proof. For any $a \in R_d$,

$$\|Q_d(a)\|_1 = \sum_{i=0}^{3} \|Q_d(a)_i\|_1 \leq \sum_{i=0}^{3}\sum_{j=0}^{3} \|x_j Q_{d-1}(a_j)_i\|_1 \tag{42}$$

$$= \sum_{i=0}^{3}\sum_{j=0}^{3} \|Q_{d-1}(a_j)_i\|_1 = \sum_j \|Q_{d-1}(a_j)\|_1 \tag{43}$$

$$\leq |||Q_{d-1}||| \sum_j \|a_j\|_1 = |||Q_{d-1}|||\, \|a\|_1, \tag{44}$$

using, for the last equality, that the terms a_j have disjoint monomial support. □

Lemma 6. *For any $k \geq 3$, we have $|||G_k||| \leq (4|||Q_{12}|||)^{k-3}$, where R is endowed with the 1-norm.*

Proof. We proceed by induction on k (the base case $k = 3$ is trivial since $G_3 = \mathrm{id}$). Let $a \in R_{4k-4}$ and $(b_0, \ldots, b_3) = Q_{4k-4}(a)$. By (40), we have

$$\|G_k(a)\|_1 \leq \frac{|||G_{k-1}|||}{k-1}\big(\|\partial_0 b_0\|_1 + \cdots + \|\partial_3 b_3\|_1\big). \tag{45}$$

By the induction hypothesis, $|||G_{k-1}||| \leq (4|||Q_{12}|||)^{k-4}$, and moreover, since each b_i has degree $4k-7$, we have $\|\partial_i b_i\|_1 \leq (4k-7)\|b_i\|_1$. If follows that

$$\|G_k(a)\|_1 \leq \big(4|||Q_{12}|||\big)^{k-4} \frac{4k-7}{k-1}\big(\|b_0\|_1 + \cdots + \|b_3\|_1\big). \tag{46}$$

Next, we note that $\|b_0\|_1 + \cdots + \|b_3\|_1 = \|Q_{4k-4}(a)\|_1$ and, by Lemma 5, we have $|||Q_{4k-4}(a)||| \leq |||Q_{12}|||$. Therefore,

$$\|G_k(a)\|_1 \leq \big(4|||Q_{12}|||\big)^{k-3} \|a\|_1, \tag{47}$$

and the claim follows. □

3. The Noether–Lefschetz locus

3.1. ***Basic properties.*** We define the Noether–Lefschetz locus for quartic surfaces and review a few classical properties, especially algebraicity, with a view towards Theorem 14 about the degree and the height of the equations defining the components of the Noether–Lefschetz locus.

3.1.1. *Definition.* The Noether–Lefschetz locus of quartics $\mathcal{NL}$ is the set of all $f \in U_4$ such that the rank of $\operatorname{Pic}(X_f)$ is at least 2. Equivalently, in view of (12), $\mathcal{NL}$ is the set of quartic polynomials f whose primitive periods (1) are $\mathbb{Z}$-linearly dependent.

The set $\mathcal{NL}$ is locally the union of smooth analytic hypersurfaces in U_4. To see this, let $\widetilde{\mathcal{NL}}$ be the lift of $\mathcal{NL}$ in the universal covering $\widetilde{U}_4$ of U_4. Recall that $\mathcal{P}\colon \widetilde{U}_4 \to \mathcal{D}$ is the period map. The Lefschetz (1,1)-theorem implies

$$\widetilde{\mathcal{NL}} = \bigcup_{\gamma \in H_{\mathbb{Z}} \setminus \mathbb{Z}h} \mathcal{P}^{-1}\{w \in \mathcal{D} \mid w \cdot \gamma = 0\}. \tag{48}$$

That is, $\widetilde{\mathcal{NL}}$ is the pullback of smooth hyperplane sections of $\mathcal{D}$. Since $\mathcal{P}$ is a submersion, $\widetilde{\mathcal{NL}}$ is the union of smooth analytic hypersurfaces. It follows that $\mathcal{NL}$ is locally the union of smooth analytic hypersurfaces.

We break $\mathcal{NL}$ into algebraic pieces as follows: For any integers d and g, let $\mathcal{NL}_{d,g}$ be the set

$$\mathcal{NL}_{d,g} = \bigl\{ f \in U_4 \mid \exists \gamma \in \operatorname{Pic}(X_f) \setminus \mathbb{Z}h : \gamma \cdot h = d \text{ and } \gamma \cdot \gamma = 2g-2 \bigr\}. \tag{49}$$

By replacing γ by $\gamma + h$ or $-\gamma$, we observe that

$$\mathcal{NL}_{d,g} = \mathcal{NL}_{d+4,g+d+2} = \mathcal{NL}_{-d,g}. \tag{50}$$

In particular, $\mathcal{NL}_{d,g}$ is equal to some $\mathcal{NL}_{d',g'}$ with $d' > 0$ and $g' \geq 0$, so that

$$\mathcal{NL} = \bigcup_{d>0} \bigcup_{g \geq 0} \mathcal{NL}_{d,g}. \tag{51}$$

For $\gamma \in H_{\mathbb{Z}}$, let $\Delta(\gamma) = (h \cdot \gamma)^2 - 4\gamma \cdot \gamma$. It is the negative of the discriminant of the lattice generated by h and γ in $H_{\mathbb{Z}}$, with respect to the intersection product (and it is zero if $\gamma \in \mathbb{Z}h$). It follows from the Hodge index theorem, see [Hartshorne 1977, Theorem V.1.9] that for any $f \in U_4$ and any $\gamma \in \operatorname{Pic}(X_f)$, where $\Delta(\gamma) \geq 0$, with equality if and only if $\gamma \in \mathbb{Z}h$. If $\gamma \cdot h = d$ and $\gamma \cdot \gamma = 2g-2$, then $\Delta(\gamma) = d^2 - 8g + 8$. We obtain, therefore, that for any $d > 0$ and $g \geq 0$,

$$\mathcal{NL}_{d,g} = \begin{cases} \{f \in U_4 \mid \exists \gamma \in \operatorname{Pic}(X_f) : \gamma \cdot h = d, \\ \qquad\qquad\qquad\qquad \gamma \cdot \gamma = 2g-2\}, & \text{if } d^2 > 8g-8, \\ \varnothing, & \text{otherwise.} \end{cases} \tag{52}$$

It is, in fact, more natural to introduce, for $\Delta > 0$, the locus

$$\mathcal{NL}_{\Delta} \doteq \{f \in U_4 \mid \exists \gamma \in \operatorname{Pic}(X_f) : \Delta(\gamma) = \Delta\} \tag{53}$$

$$= \bigcup_{\substack{d>0, \\ d^2 \equiv \Delta \bmod 8}} \mathcal{NL}_{d,(d^2-\Delta)/8+1}. \tag{54}$$

Due to (50), $\mathcal{NL}_\Delta$ reduces to a single $\mathcal{NL}_{d,g}$. Namely,

$$\mathcal{NL}_\Delta = \begin{cases} \mathcal{NL}_{4t,2t^2+(8-\Delta)/8}, & \text{if } \Delta \equiv 0 \mod 8, \\ \mathcal{NL}_{4t+1,2t^2+t+(9-\Delta)/8}, & \text{if } \Delta \equiv 1 \mod 8, \\ \mathcal{NL}_{4t+2,2t^2+2t+(12-\Delta)/8}, & \text{if } \Delta \equiv 4 \mod 8, \\ \varnothing, & \text{otherwise,} \end{cases} \tag{55}$$

where $t = \lceil \frac{1}{4}\sqrt{\Delta}\, \rceil$. Conversely, each $\mathcal{NL}_{d,g} = \mathcal{NL}_{d^2-8g+8}$.

3.1.2. *Algebraicity.* For any $d > 0$ and $g \geq 0$, the set $\mathcal{NL}_{d,g}$ is either empty or an algebraic hypersurface in U_4. This is a classical result, e.g., [Voisin 2003, Theorem 3.32], which we recall here to obtain an explicit algebraic description of $\mathcal{NL}_{d,g}$.

Lemma 7. *For any $f \in U_4$, $d > 0$ and $g \geq 0$, we have: $f \in \mathcal{NL}_{d,g}$ if and only if X_f contains an effective divisor with Hilbert polynomial $t \mapsto dt + 1 - g$.*

Proof. Assume that X_f contains an effective divisor C with Hilbert polynomial $t \mapsto td + 1 - g$. Since X_f is smooth, C is a locally principal divisor and gives an element γ of $\operatorname{Pic} X_f$. The integer d is the degree of C, so it is the number of points in the intersection with a generic hyperplane, that is, $d = \gamma \cdot h$. Moreover, g is the arithmetic genus of C, which is determined by $2g - 2 = \gamma \cdot \gamma$ [Hartshorne 1977, Exercises III.5.3(b) and V.1.3(a)]. So, $f \in \mathcal{NL}_{d,g}$.

Conversely, let $f \in \mathcal{NL}_{d,g}$. By definition, there is a divisor C on X_f such that its class γ in $\operatorname{Pic} X_f$ satisfies $\gamma \cdot h = d$ and $\gamma \cdot \gamma = 2g - 2$. From the Riemann–Roch theorem for surfaces [Hartshorne 1977, Theorem V.1.6], we get

$$\dim H^0(X, \mathcal{O}_X(C)) + \dim H^0(X, \mathcal{O}_X(-C)) \geq \tfrac{1}{2}\gamma \cdot \gamma + 2 = g + 1 > 0,$$

so that either C or $-C$ must be linearly equivalent to an effective divisor. Since $\gamma \cdot h > 0$, it follows that $-C$ cannot be effective, and therefore, C must be. As above, the Hilbert polynomial of C is given by $t \mapsto dt + 1 - g$. $\square$

In light of Lemma 7, the algebraicity of $\mathcal{NL}_{d,g}$ is proved by using the Hilbert scheme $\mathcal{H}_{d,g}$. The Hilbert scheme $\mathcal{H}_{d,g}$ of degree d and genus g curves in $\mathbb{P}^3$ is a projective scheme that parametrizes all the subschemes of $\mathbb{P}^3$ whose Hilbert polynomial is $t \mapsto dt + 1 - g$.

The Hilbert scheme $\mathcal{H}_{d,g}$ may contain components that are not desirable for our purposes. For example, $\mathcal{H}_{3,0}$, which contains twisted cubics in $\mathbb{P}^3$, contains two irreducible components [Piene and Schlessinger 1985]: a 12-dimensional component that is the closure of the space of all smooth cubic rational curves in $\mathbb{P}^3$ and a 15-dimensional component parametrizing the union of a plane cubic curve with a point in $\mathbb{P}^3$. We would be only interested in the first, not in the second component. So we introduce $\mathcal{H}'_{d,g}$, the union of components of $\mathcal{H}_{d,g}$ obtained by removing the components that do not correspond to locally complete-intersection pure-dimensional subschemes of $\mathbb{P}^3$.

When $d^2 > 8g - 8$, Lemma 7 can be rephrased as

$$\mathcal{NL}_{d,g} = \operatorname{proj}_1 \left\{ (f, C) \in U_4 \times \mathcal{H}'_{d,g} \mid C \subset X_f \right\}, \tag{56}$$

where proj_1 denotes the projection $U_4 \times \mathcal{H}'_{d,g} \to U_4$. Since $\mathcal{H}'_{d,g}$ is a projective variety, and the condition $C \subset X_f$ is algebraic, this shows that $\mathcal{NL}_{d,g}$ is a closed subvariety of U_4 (for more details about this construction, see [Voisin 2003, §3.3]).

We note, furthermore, that $\mathcal{NL}_{d,g}$ is clearly invariant under the action of the Galois group of algebraic numbers. Therefore, it can be defined over the rational numbers.

As a consequence, for any nonnegative integers d and g, there is a squarefree primitive homogeneous polynomial $\mathrm{NL}_{d,g} \in \mathbb{Z}[u_1, \dots, u_{35}]$ in the 35 coefficients of the general quartic polynomial that is unique up to sign and whose zero locus is $\mathcal{NL}_{d,g}$ in U_4. Similarly, we define NL_Δ up to sign as the unique squarefree primitive polynomial vanishing exactly on $\mathcal{NL}_\Delta$.

3.2. *Height of multiprojective varieties.* The mainstay of our results is a bound on the degree and size of the coefficients of the polynomials $\mathrm{NL}_{d,g}$. The determination of these bounds is based on (56) and involves the theory of heights of multiprojective varieties as developed by D'Andrea et al. [2013], and, before them, [Bost et al. 1991; Philippon 1995; Krick et al. 2001; Rémond 2001a; 2001b], among others. We recall here the results that we need, following [D'Andrea et al. 2013].

3.2.1. *Heights of polynomials.* Let $f = \sum_\alpha c_\alpha \boldsymbol{x}^\alpha \in \mathbb{C}[x_1, \dots, x_n]$. We recall the following different measures of height of f:

$$\|f\|_1 \doteq \sum_\alpha |c_\alpha|, \tag{57}$$

$$\|f\|_{\sup} \doteq \sup_{|x_1|=\cdots=|x_n|=1} |f(\boldsymbol{x})|, \tag{58}$$

$$m(f) \doteq \int_{[0,1]^n} \log|f(e^{2\pi i t_1}, \dots, e^{2\pi i t_n})|\,\mathrm{d}t_1 \cdots \mathrm{d}t_n. \tag{59}$$

Lemma 8 [D'Andrea et al. 2013, Lemma 2.30]. *For any homogeneous polynomial $f \in \mathbb{C}[x_1, \dots, x_n]$,*

$$\exp(m(f)) \le \|f\|_{\sup} \le \|f\|_1 \le \exp(m(f))(n+1)^{\deg f}.$$

3.2.2. *Extended Chow ring.* The extended Chow ring [D'Andrea et al. 2013, Definition 2.50] is a tool to track a measure of height of multiprojective varieties when performing intersections and projections. We present here a very brief summary. Bold letters refer to multiindices, and all varieties are considered over $\mathbb{Q}$. Let $\boldsymbol{n} \in \mathbb{N}^r$, and let $\mathbb{P}^{\boldsymbol{n}}$ be the multiprojective space $\mathbb{P}^{\boldsymbol{n}} = \mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_m}$.

An *algebraic cycle* is a finite $\mathbb{Z}$-linear combination $\sum_V n_V V$ of irreducible subvarieties of $\mathbb{P}^{\boldsymbol{n}}$. The *irreducible components* of an algebraic cycle, as above, are the irreducible varieties V such that $n_V \neq 0$. An algebraic cycle is *equidimensional* if all its irreducible components have the same dimension. An algebraic cycle is *effective* if $n_V \ge 0$ for all V. The *support* of X, denoted by $\operatorname{supp} X$, is the union of the irreducible components of X.

Let $A^*(\mathbb{P}^{\boldsymbol{n}}; \mathbb{Z})$ be the extended Chow ring, namely

$$A^*(\mathbb{P}^{\boldsymbol{n}}; \mathbb{Z}) \doteq \mathbb{R}[\eta, \theta_1, \dots, \theta_m]/(\eta^2, \theta_1^{n_1+1}, \dots, \theta_m^{n_m+1}), \tag{60}$$

where θ_i is the class of the pullback of a hyperplane from $\mathbb{P}^{n_i}$ and η is used to keep track of heights of varieties. For two elements a and b of this ring, we write $a \le b$ when the coefficients of $b-a$ in the monomial basis are nonnegative.

To an algebraic cycle X of $\mathbb{P}^{\boldsymbol{n}}$, we associate an element $[X]_{\mathbb{Z}}$ of $A^*(\mathbb{P}^{\boldsymbol{n}};\mathbb{Z})$ [D'Andrea et al. 2013, Definition 2.50]. If X is effective, then $[X]_{\mathbb{Z}} \ge 0$. The coefficients of the terms in $[X]_{\mathbb{Z}}$ for monomials not involving η record the usual multidegrees of X. The terms involving η record mixed canonical heights of X. The definition of these heights is based on the heights of various Chow forms associated to X [D'Andrea et al. 2013, §2.3]. For the computations in this paper, we only need the following results:

Let $f \in \mathbb{Z}[\boldsymbol{x}_{\boldsymbol{\Delta}},\dots,\boldsymbol{x}_{\boldsymbol{r}}]$ be a nonzero multihomogeneous polynomial with respect to the group of variables $\boldsymbol{x}_1,\dots,\boldsymbol{x}_n$. We assume that f is *primitive*, that is, the gcd of the coefficients of f is 1. The element associated in $A^*(\mathbb{P}^{\boldsymbol{n}};\mathbb{Z})$ to the hypersurface $V(f) \subset \mathbb{P}^{\boldsymbol{n}}$ is [D'Andrea et al. 2013, Proposition 2.53 (2)]

$$[V(f)]_{\mathbb{Z}} = m(f)\eta + \deg_{\boldsymbol{x}_1}(f)\theta_1 + \cdots + \deg_{\boldsymbol{x}_r}(f)\theta_r. \tag{61}$$

To such a polynomial f, we also associate [D'Andrea et al. 2013, Equation (2.57)]

$$[f]_{\sup} \doteq \log(\|f\|_{\sup})\eta + \deg_{\boldsymbol{x}_1}(f)\theta_1 + \cdots + \deg_{\boldsymbol{x}_r}(f)\theta_r. \tag{62}$$

3.2.3. *Arithmetic Bézout theorem.* Let X be an effective cycle and H a hypersurface in $\mathbb{P}^{\boldsymbol{n}}$. They *intersect properly* if no irreducible component of X is in H. When X and H intersect properly, one defines an intersection product $X \cdot H$, that is an effective cycle supported on $X \cap H$. If X is equidimensional of dimension r, then $X \cdot H$ is equidimensional of dimension $r-1$.

The following statement is an arithmetic Bézout bound that not only bounds the degree, as with the classical Bézout bound, but also the height of an intersection:

Theorem 9 [D'Andrea et al. 2013, Theorem 2.58]. *Let X be an effective equidimensional cycle on $\mathbb{P}^{\boldsymbol{n}}$ and $f \in \mathbb{Z}[\boldsymbol{x}_1,\dots,\boldsymbol{x}_m]$. If X and $V(f)$ intersect properly, then $[X\cdot V(f)]_{\mathbb{Z}} \le [X]_{\mathbb{Z}} \cdot [f]_{\sup}$.*

This theorem can be applied (as in [D'Andrea et al. 2013, Corollary 2.61]) to bound the height of the irreducible components of a variety in terms of its defining equations.

Proposition 10. *Let $Z \subset \mathbb{P}^{\boldsymbol{n}}$ be an equidimensional variety, and let X be $V(f_1,\dots,f_s)\cap Z$, where f_i is a multihomogeneous polynomial of multidegree at most $\boldsymbol{d}$ and sup-norm at most L. Let X_r be the union of all the irreducible components of X of codimension r in Z. Then*

$$[X_r]_{\mathbb{Z}} \le [Z]_{\mathbb{Z}}\left(\log(sL)\eta + \sum_{i=1}^{m} d_i\theta_i\right)^r.$$

Proof. Let (y_{ij}) be a new group of variables, with $1 \le i \le r$ and $1 \le j \le s$. Let $g_i \doteq \sum_{j=1}^{s} y_{ij} f_j$ and $X' \doteq V(g_1,\dots,g_r)$ in $\mathbb{P}^k \times Z$, with $k = rs-1$ We first claim that $\mathbb{P}^k \times X_r$ is a union of components of X'. Indeed, let ξ_0 be the generic point of $\mathbb{P}^k$ and ξ_1 be the generic point of a component Y of X_r, so that $\xi = (\xi_0,\xi_1)$ is the generic point of the component $\mathbb{P}^k \times Y$ of $\mathbb{P}^k \times X_r$. Since X has codimension r at ξ_1, the generic linear combinations $g_1,\dots,g_r$ form a regular sequence at ξ (in other words, they form a regular sequence at ξ_1 for generic values of the v_{ij}). Therefore, X' has codimension r at ξ. Since $\mathbb{P}^k \times Y \subseteq X'$, it follows that $\mathbb{P}^k \times Y$ is a component of X'.

Let X'_r be the union of the components of codimension r of X'. The argument above shows that $[\mathbb{P}^k \times X_r]_{\mathbb{Z}} \le [X'_r]_{\mathbb{Z}}$. Besides, by repeated application of [D'Andrea et al. 2013, Corollary 2.61],

$$[X'_r]_{\mathbb{Z}} \le [\mathbb{P}^k \times Z]_{\mathbb{Z}} \prod_{i=1}^{r} [g_i]_{\sup}, \tag{63}$$

where θ_0 is the variable attached to $\mathbb{P}^k$ in the extended Chow ring of $\mathbb{P}^k \times \mathbb{P}^{\boldsymbol{n}}$. We compute, using (61), that

$$[g_i]_{\sup} \le \log(sL)\eta + \theta_0 + \sum_{i=1}^{s} d_i \theta_i. \tag{64}$$

Finally, we note that $[\mathbb{P}^k \times X_r]_{\mathbb{Z}} = [X_r]_{\mathbb{Z}}$ and $[\mathbb{P}^k \times Z]_{\mathbb{Z}} = [Z]_{\mathbb{Z}}$ by [D'Andrea et al. 2013, Propositions 2.51.3 and 2.66]. □

Proposition 11. *Let X be an equidimensional closed subvariety of $\mathbb{P}^k \times \mathbb{P}^{\boldsymbol{n}}$, and let $Y \subset \mathbb{P}^{\boldsymbol{n}}$ be the projection of X. If Y is equidimensional, then*

$$\theta_0^k [Y]_{\mathbb{Z}} \le \theta_0^{\dim X - \dim Y} [X]_{\mathbb{Z}} \in A^*(\mathbb{P}^k \times \mathbb{P}^{\boldsymbol{n}}; \mathbb{Z}),$$

where θ_0 is the variable attached to $\mathbb{P}^k$ in the extended Chow ring of $\mathbb{P}^k \times \mathbb{P}^{\boldsymbol{n}}$.

Proof. We will argue by induction on $r \doteq \dim X - \dim Y$. When $r = 0$, this is [D'Andrea et al. 2013, Proposition 2.64].

Suppose now that $r > 0$ and X is irreducible. Let $\mathbb{Q}[\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{\boldsymbol{m}}]$ denote the multihomogeneous coordinate ring of $\mathbb{P}^k \times \mathbb{P}^{\boldsymbol{n}}$. There is an i, with $0 \le i \le k$, such that $H \doteq V(y_i) \subset \mathbb{P}^k \times \mathbb{P}^{\boldsymbol{n}}$ intersects X properly (otherwise, X would be included in all $V(y_i)$ and would be empty). Since the fibers of $X \to Y$ are positive dimensional, H intersects each fiber. In particular, the set-theoretical projections of X and $X \cap H$ coincide. As X is irreducible, so is Y. In particular, there is an irreducible component $X' \subset X \cap H$ that maps to Y. By the induction hypothesis applied to X', we have $\theta_0^k [Y]_{\mathbb{Z}} \le \theta_0^{\dim X' - \dim Y} [X']_{\mathbb{Z}}$. Moreover, $[X']_{\mathbb{Z}} \le [X]_{\mathbb{Z}} [y_i]_{\sup}$, and, in view of (62), $[y_i]_{\sup} = \theta_0$. The claim follows.

If X is reducible, then we apply the inequality above to each of the irreducible components of Y together with an irreducible component of X mapping onto that component. □

3.3. *Explicit equations for the Noether–Lefschetz loci.*

Following Gotzmann [1978], Bayer [1982] and the exposition of Lella [2012], we describe the equations defining the Hilbert schemes of curves in $\mathbb{P}^3$. An explicit description of the Noether–Lefschetz loci $\mathcal{NL}_{d,g}$ follows.

3.3.1. *Hilbert schemes of curves.* For $d > 0$ and $g \ge 0$, let $\mathcal{H}_{d,g}$ be the Hilbert scheme of curves of degree d and genus g in $\mathbb{P}^3$. It parametrizes subschemes of $\mathbb{P}^3$ with Hilbert polynomial $p(m) \doteq dm + 1 - g$. Smooth curves in $\mathbb{P}^3$ of degree d and genus g, in particular, have Hilbert polynomial $p(m)$. Let $R = \mathbb{C}[w, x, y, z]$ be the homogeneous coordinate ring of $\mathbb{P}^3$. For $m \ge 0$, let R_m denote the m-th homogeneous part of R, and let $q(m) = \dim R_m - p(m)$.

The Hilbert scheme $\mathcal{H}_{d,g}$ can be realized in a Grassmannian variety as follows: A subscheme X of $\mathbb{P}^3$ is uniquely defined by a saturated homogeneous ideal I of R. If the Hilbert polynomial of X is p, then I is the saturation of the ideal generated by the degree r slice $I_r \doteq I \cap R_r$ [Gotzmann 1978] and [Bayer 1982, §II.10], where

$$r = \binom{d}{2} + 1 - g \tag{65}$$

is the Gotzmann number of p [Bayer 1982, §II.1.17]. For practical reasons, we need $r \geq 4$, so we define instead

$$r = \max\left(\binom{d}{2} + 1 - g, 4\right). \tag{66}$$

So X is entirely determined by I_r, which is a $q(r)$-dimensional subspace of R_r.

Let $\mathbb{G}$ be the Grassmannian variety of $q(r)$-dimensional subspaces of R_r. As a set, one can construct $\mathcal{H}_{d,g}$ as the subset of all $\Xi \in \mathbb{G}$ such that the ideal generated by Ξ in R defines a subscheme of $\mathbb{P}^3$ with Hilbert polynomial p. In fact, $\mathcal{H}_{d,g}$ is a subvariety that is defined by the following condition [Bayer 1982, §VI.1]:

$$\mathcal{H}_{d,g} = \left\{ \Xi \in \mathbb{G} \mid \dim(R_1 \Xi) \leq q(r+1) \right\}, \tag{67}$$

where R_1 is the space of linear forms in w, x, y, z, so that $R_1 \Xi$ is a subspace of R_{r+1}.

Several authors gave explicit equations for $\mathcal{H}_{d,g}$ in the Plücker coordinates [Bayer 1982; Grothendieck 1966; Gotzmann 1978; Brachat et al. 2016]. We will prefer here a more direct path that avoids the Plücker embedding.

3.4. ***Equations for the relative Hilbert scheme.*** Define the relative Hilbert scheme of curves inside quartic surfaces

$$\mathcal{H}_{d,g}(4) \doteq \left\{ (f, C) \in \mathbb{P}(R_4) \times \mathcal{H}_{d,g} \mid C \subset V(f) \right\}, \tag{68}$$

for each $d > 0$ and $g \geq 0$.

We define the following auxiliary spaces to better describe (68): First, define the ambient space

$$\mathcal{A} \doteq \mathbb{P}(R_4) \times \mathbb{P}\left(\operatorname{End}(\mathbb{C}^{q(r)-N_{r-4}}, R_r)\right) \times \mathbb{P}\left(\operatorname{End}(R_{r+1}, \mathbb{C}^{p(r+1)})\right). \tag{69}$$

Second, let $\mathcal{B} = \{(f, \phi, \psi) \in \mathcal{A}\}$ be the set of all triples satisfying the conditions

(i) $R_{r-3} f \subseteq \ker \psi$,

(ii) $R_1 \operatorname{im}(\phi) \subseteq \ker \psi$,

(iii) $\operatorname{im} \phi \cap R_{r-4} f = 0$,

(iv) ϕ and ψ are full rank.

Finally, we denote by $\overline{\mathcal{B}}$ the Zariski closure of $\mathcal{B}$.

Lemma 12. *The map $\mathcal{B} \to \mathcal{H}_{d,g}(4)$ defined by $(f, \phi, \psi) \mapsto (f, R_{r-4} f + \operatorname{im} \phi)$ is well defined and surjective.*

Proof. Let $(f, \phi, \psi) \in \mathcal{B}$, and let $\Xi = R_{r-4} f + \operatorname{im} \phi$. Constraint (iv) implies that $\operatorname{im} \phi$ has dimension $q(r) - N_{r-4}$. Together with Constraint (iii), we have $\dim \Xi = q(r)$. Moreover, Constraint (iv) implies that $\ker \psi$ has dimension $q(r+1)$. In particular, since $R_1 \Xi = R_{r-3} f + R_1 \operatorname{im} \phi$, Constraints (i) and (ii) imply that $R_1 \Xi$ has dimension at most $q(r+1)$. So, $\Xi \in \mathcal{H}_{d,g}(4)$. Since $R_{r-4} f \subseteq \Xi$, the polynomial f is in the saturation of the ideal generated by Ξ. Hence, $(f, \Xi) \in \mathcal{H}_{d,g}(4)$.

Conversely, let $(f, \Xi) \in \mathcal{H}_{d,g}(4)$, then $R_{r-4} f \subset \Xi$ and there is a full rank map $\phi \colon \mathbb{C}^{q(r) - N_{r-4}} \to R_r$ such that $\operatorname{im} \phi$ complements $R_{r-4} f$ in Ξ. Furthermore, $\dim R_1 \Xi \le q(r+1)$, because $\Xi \in \mathcal{H}_{d,g}$, so there is a full rank map $\psi : R_{r+1} \to \mathbb{C}^{p(r+1)}$ such that $R_1 \Xi \subseteq \ker \psi$. So, (f, Ξ) is the image of $(f, \phi, \psi) \in \mathcal{B}$. □

Lemma 13. *For any $a \ge 0$, let $\overline{\mathcal{B}}_a$ be the union of the codimension a components of $\overline{\mathcal{B}}$. Then*

$$[\overline{\mathcal{B}}_a]_{\mathbb{Z}} \le \big(15 \log(d+2) \eta + \theta_1 + \theta_2 + \theta_3\big)^a$$

Proof. Let $\mathcal{B}'$ be the closed set defined by Constraints (i) and (ii). Constraints (iii) and (iv) are open, so any component of $\overline{\mathcal{B}}$ is a component of $\mathcal{B}'$. In particular, $[\overline{\mathcal{B}}_a]_{\mathbb{Z}} \le [\mathcal{B}'_a]_{\mathbb{Z}}$.

Constraint (i) is expressed with $p(r+1) N_{r-3}$ polynomial equations of multidegree $(1, 0, 1)$ (with respect to f, ϕ and ψ, respectively). Namely, $\psi(mf) = 0$ for every monomial m in R_{r-3}. Each $p(r+1)$ components of the equation $\psi(mf) = 0$ involves a sum of 35 terms (since f, as a quartic polynomial, contains only 35 terms) with coefficients 1. So the 1-norm of these constraints is at most 35 (which is also at most N_r, since $r \ge 4$).

Constraint (ii) is expressed with $4p(r+1)(q(r) - N_{r-4})$ polynomial equations of multidegree $(0, 1, 1)$. Namely, $\psi(v\phi(e)) = 0$ for any basis vector e and any variable $v \in \{w, x, y, z\}$. Each $p(r+1)$ component of the equation $\psi(v\phi(e)) = 0$ involves a sum of N_r terms with coefficients 1. So the 1-norm of these constraints is at most N_r.

The claim is then a consequence of Proposition 10, with

$$s = p(r+1) N_{r-3} + 4p(r+1)(q(r) - N_{r-4}) \quad \text{and} \quad L = N_r.$$

We check routinely, with Mathematica, that $sL \le (d+2)^{15}$. □

Theorem 14. *There is an absolute constant $A > 0$ such that for any $d > 0$ and $g \ge 0$, we have*

$$\deg(\mathrm{NL}_{d,g}) \le A^{d^9} \quad \textit{and} \quad \|\mathrm{NL}_{d,g}\|_1 \le 2^{A^{d^9}}.$$

Proof. We assume $\mathcal{NL}_{d,g}$ is nonempty, since these inequalities are trivially satisfied if $\mathcal{NL}_{d,g} = \varnothing$ with $\mathrm{NL}_{d,g} = 1$. Let $P_2 \doteq \mathbb{P}\big(\operatorname{End}(\mathbb{C}^{q(r) - N_{r-4}}, R_r)\big)$ and $P_3 \doteq \mathbb{P}\big(\operatorname{End}(R_{r+1}, \mathbb{C}^{p(r+1)})\big)$ denote the second and third factors of $\mathcal{A}$, respectively. Let $\alpha \doteq (q(r) - N_{r-4}) N_r - 1$ and $\beta \doteq p(r+1) N_{r+1} - 1$ denote the dimensions of P_2 and P_3, respectively. Let $\mathcal{E}$ be the projection of $\overline{\mathcal{B}}$ on $\mathbb{P}(R_4) \times P_2$. The fibers of the map $\overline{\mathcal{B}} \to \mathcal{E}$ are projective subspaces of P_3 since Constraints (i) and (ii) are linear in ψ. The dimension of these fibers are $\beta' \doteq p(r+1)^2 - 1$. So, by Proposition 11,

$$\theta_3^{\beta} [\mathcal{E}]_{\mathbb{Z}} \le \theta_3^{\beta'} [\overline{\mathcal{B}}]_{\mathbb{Z}}. \tag{70}$$

Next, the map $\mathcal{B} \to \mathcal{H}_{d,g}(4)$ factors through $\mathcal{E}$, and the fibers of the corresponding map $\mathcal{E} \to \mathcal{H}_{d,g}(4)$ have dimension $\alpha' \doteq (q(r) - N_{r-4})q(r) - 1$. Finally, let e be the dimension of the fibers of the map $\mathcal{H}_{d,g}(4) \to \mathcal{NL}_{d,g}$. (If this dimension is not generically constant, we work one component at a time.) Once again, by Proposition 11, we obtain

$$\theta_2^{\alpha}[\mathcal{NL}_{d,g}]_{\mathbb{Z}} \le \theta_2^{\alpha'+e}[\mathcal{E}]_{\mathbb{Z}}. \tag{71}$$

Since $[\mathcal{NL}_{d,g}]_{\mathbb{Z}} = m(\mathrm{NL}_{d,g})\eta + \deg(\mathrm{NL}_{d,g})\theta_1$, taking $L = 15\log(d+2)$, we get

$$\begin{aligned} \deg \mathrm{NL}_{d,g} &\le \text{coeff. of } \theta_1\theta_2^{\alpha-\alpha'-e}\theta_3^{\beta-\beta'} \text{ in } (L\eta+\theta_1+\theta_2+\theta_3)^{\alpha+\beta-\alpha'-\beta'-e+1} && (72)\\ &\le 3^{\alpha+\beta-\alpha'-\beta'-e+1}. && (73)\end{aligned}$$

The exponent is a polynomial in d and g. Unless $d^2 \ge 8g-8$, we have that $\mathcal{NL}_{d,g}$ is empty. So, we may bound the exponent with a polynomial only in d, which turns out to be of degree 9. Therefore, $\deg \mathrm{NL}_{d,g} \le A^{d^9}$ for some constant $A > 0$.

Similarly,

$$\begin{aligned} m(\mathrm{NL}_{d,g}) &\le \text{coeff. of } \eta\theta_2^{\alpha-\alpha'-e}\theta_3^{\beta-\beta'} \text{ in } (L\eta+\theta_1+\theta_2+\theta_3)^{\alpha+\beta-\alpha'-\beta'-e+1} && (74)\\ &\le (\alpha+\beta-\alpha'-\beta'-e+1)L3^{\alpha+\beta-\alpha'-\beta'-e} && (75)\\ &\le 2^{O(d^9)}. && (76)\end{aligned}$$

By [D'Andrea et al. 2013, Lemma 2.30.3],

$$\|\mathrm{NL}_{d,g}\|_1 \le \exp(m(\mathrm{NL}_{d,g}))36^{\deg \mathrm{NL}_{\Delta}}, \tag{77}$$

and this implies the claim, for some other constant $A > 0$. □

For the following, we write $a{\uparrow}b$ for a^b. This is a right-associative operation.

Corollary 15. *There is an absolute constant $A > 0$ such that for any $\Delta > 0$,*

$$\deg(\mathrm{NL}_{\Delta}) \le A{\uparrow}\Delta{\uparrow}\tfrac{9}{2} \quad \textit{and} \quad \|\mathrm{NL}_{\Delta}\|_1 \le 2{\uparrow}A{\uparrow}\Delta{\uparrow}\tfrac{9}{2}.$$

In fact, one can obtain the following explicit bounds:

$$\deg(\mathrm{NL}_{\Delta}) \le 3^{(\Delta+20)^{9/2}} \quad \textit{and} \quad \log_2\|\mathrm{NL}_{\Delta}\|_1 \le (\Delta+60)^5 3^{(\Delta+20)^{9/2}}.$$

Proof. The first statement follows directly from (55) and Theorem 14 using a different A. The second statement is found by carrying out the arguments in the proof of Theorem 14 with the help of a computer algebra system. □

3.5. ***How good are these bounds?*** We can compare our degree bounds for NL_{Δ} to the exact degrees computed by Maulik and Pandharipande [2013], from which it actually follows that

$$\deg \mathrm{NL}_{\Delta} = O(\Delta^{19/2}). \tag{78}$$

This sharper bound does not directly imply a sharper bound on the height of NL_Δ, but it suggests the following conjecture. This would improve subsequently Theorems 17 and 19. In particular, (2) would be exponential in the size of the coefficients, as opposed to being doubly exponential.

Conjecture 16. *As Δ goes to ∞, we have*

$$\log \|\mathrm{NL}_\Delta\|_1 \leq \Delta^{19/2+o(1)}.$$

Now we turn to the details of (78). Following Maulik and Pandharipande [2013] (but replacing q by q^8), consider the power series

$$A \doteq \sum_{n\in\mathbb{Z}} q^{n^2}, \quad B \doteq \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2}, \quad \Psi = 108 \sum_{n>0} q^{8n^2}, \tag{79}$$

and Θ defined by

$$\begin{aligned}2^{22}\Theta \doteq{} & 3A^{21}-81A^{19}B^2-627A^{18}B^3-14436A^{17}B^4-20007A^{16}B^5\\ & -169092A^{15}B^6-120636A^{14}B^7-621558A^{13}B^8\\ & -292796A^{12}B^9-1038366A^{11}B^{10}-346122A^{10}B^{11}\\ & -878388A^9B^{12}-207186A^8B^{13}-361908A^7B^{14}-56364A^6B^{15}\\ & -60021A^5B^{16}-4812A^4B^{17}-1881A^3B^{18}-27A^2B^{19}+B^{21}.\end{aligned} \tag{80}$$

From [Maulik and Pandharipande 2013, Corollary 2], we have, for any $\Delta > 0$,

$$\deg \mathrm{NL}_\Delta \leq \text{coeff. of } q^\Delta \text{ in } \Theta - \Psi. \tag{81}$$

In fact, this is an equality when the components of $\mathcal{NL}_\Delta$ are given appropriate multiplicities. Let $\Theta[k]$ denote the coefficient of q^k in Θ. By (81), we only need to bound $\Theta[\Delta]$ in order to bound $\deg \mathrm{NL}_\Delta$. To do so, replace every negative sign in the definition of Θ by a positive sign, including those in B, to obtain the *coefficientwise* inequality

$$\Theta \leq 6\left(\sum_{n\in\mathbb{Z}} q^{n^2}\right)^{21}. \tag{82}$$

The coefficient of q^k in $\left(\sum_{n\in\mathbb{Z}} q^{n^2}\right)^{21}$ is

$$r_{21}(k) \doteq \#\left\{(a_1,\dots,a_{21}) \in \mathbb{Z}^{21} \;\middle|\; \sum_i a_i^2 = k\right\}. \tag{83}$$

The asymptotic bound $r_d(k) = O(k^{d/2-1})$, for $d > 4$, is well known, e.g., [Krätzel 2000, Satz 5.8].

4. Separation bound

We now state and prove the main results. Recall that $a\uparrow b = a^b$ is right associative, and for $\gamma \in H_\mathbb{Z}$, we defined the discriminant $\Delta(\gamma)$ as $(\gamma\cdot h)^2 - 4\gamma\cdot\gamma$.

Theorem 17. *For any $f \in U_4$ with algebraic coefficients, there is a computable constant $c > 1$ such that for any $\gamma \in H^2(X_f, \mathbb{Z})$, if $\gamma \cdot \omega_f \neq 0$, then*

$$|\gamma \cdot \omega_f| > \left(2\uparrow c\uparrow \Delta(\gamma)\uparrow \tfrac{9}{2}\right)^{-1}.$$

To make the connection with (1), recall the map T introduced in (7). We choose a basis $\gamma_1, \ldots, \gamma_{21}$ of $H_3(\mathbb{P}^3 \setminus X_f, \mathbb{Z}) \simeq H_{\mathbb{Z}}/\mathbb{Z}h$, write $T(\gamma) = \sum_i x_i \gamma_i$ and observe that $\Delta(\gamma)$ is a quadratic function of the coordinates x_i, so that $\Delta(\gamma)^{1/2} \leq C \max_i |x_i|$ for some constant C depending on the choice of basis.

4.1. ***Multiplicity of Noether–Lefschetz loci.*** The multiplicity at a point $p \in \mathbb{C}^s$ of some nonzero polynomial $F \in \mathbb{C}[x_1, \ldots, x_s]$ is the unique integer k such that all partial derivatives of F of order $< k$ vanish at p and some partial derivative of order k does not. It is denoted by $\operatorname{mult}_p F$.

The multiplicity of NL_Δ at some $f \in U_4$ is related to the elements of $\operatorname{Pic}(X_f)$ with discriminant Δ. For $\Delta > 0$, let E_Δ be a set of representatives for elements of discriminant Δ modulo the equivalence relation $\sim$ on $H_{\mathbb{Z}}$ defined by

$$\gamma \sim \gamma', \quad \text{if } \exists a \in \mathbb{Q}^*,\ b \in \mathbb{Q} : \gamma' = a\gamma + bh. \tag{84}$$

Lemma 18. *For any $f \in U_4$ and any $\Delta > 0$,*

$$\operatorname{mult}_f \mathrm{NL}_\Delta = \#(\operatorname{Pic} X_f \cap E_\Delta).$$

Proof. Let $\widetilde{\mathcal{NL}}_\Delta$ be the lift of $\mathcal{NL}_\Delta$ in $\widetilde{U}_4$. Arguing as in Section 3.1.1, $\widetilde{\mathcal{NL}}_\Delta$ is the union of smooth analytic hypersurfaces

$$\widetilde{\mathcal{NL}}_\Delta = \bigcup_{\eta \in E_\Delta} \mathcal{P}^{-1}\{w \in \mathcal{D} \mid w \cdot \eta = 0\}. \tag{85}$$

Then the same holds locally for $\mathcal{NL}_\Delta$.

For any $f \in U_4$, it follows from the smoothness of branches of $\mathcal{NL}_\Delta$ that $\operatorname{mult}_f \mathrm{NL}_\Delta$ is exactly the number of branches meeting at f. The branches meeting at f are described by the elements of $\operatorname{Pic} X_f$ with discriminant Δ. Two elements γ and γ' describe the same branch (that is, the same hyperplane section of $\mathcal{D}$) if and only if $\gamma' \sim \gamma$. So $\operatorname{mult}_f \mathrm{NL}_\Delta$ is exactly the number of equivalence classes in $\{\gamma \in \operatorname{Pic} X_f \mid \Delta(\gamma) = \Delta\}$ for this relation. ☐

4.2. ***Proof of Theorem 17.*** We first apply Corollary 3. Let $\varepsilon = 4|\gamma \cdot \omega_f|$. The corollary gives constants $C_f > 0$ and $\varepsilon_f > 0$ (depending only on f) such that if $\varepsilon < \varepsilon_f$, then there exists a monomial $m \in R_4$ and $t \in \mathbb{C}$ such that

$$|t| \leq C_f \varepsilon \tag{86}$$

and

$$\gamma \in \operatorname{Pic} X_{f+tm}. \tag{87}$$

Assume $\varepsilon < \varepsilon_f$. As u varies, the number $\#\big(\operatorname{Pic}(X_{f+um}) \cap E_\Delta\big)$ has a strict local maximum at $u = t$, where t and m are as above. By Lemma 18, so does $\operatorname{mult}_{f+um} \mathrm{NL}_{\Delta(\gamma)}$. In particular, there is some higher-order partial derivative of NL_Δ which vanishes at $f+tm$ but not at $f+um$, for u close to but not equal to t. Let $\alpha \in \mathbb{N}^{35}$ be the multiindex for which

$$P \doteq \frac{1}{\alpha_1! \cdots \alpha_{35}!} \frac{\partial^{|\alpha|} \mathrm{NL}_\Delta}{\partial u^\alpha} \in \mathbb{Z}[u_1, \dots, u_{35}] \tag{88}$$

is this derivative. For a monomial $u^\beta \doteq u_1^{\beta_1} \cdots u_{35}^{\beta_{35}}$, we have

$$\frac{1}{\alpha_1! \cdots \alpha_{35}!} \frac{\partial^{|\alpha|} u^\beta}{\partial u^\alpha} = \prod_{i=1}^{35} \binom{\beta_i}{\alpha_i} u^{\beta-\alpha}. \tag{89}$$

Since $\binom{\beta_i}{\alpha_i} \le 2^{\beta_i}$, it follows that

$$\left\| \frac{1}{\alpha_1! \cdots \alpha_{35}!} \frac{\partial^{|\alpha|} \mathrm{NL}_\Delta}{\partial u^\alpha} \right\|_1 \le 2^{\deg \mathrm{NL}_\Delta} \|\mathrm{NL}_\Delta\|_1. \tag{90}$$

Let $Q \in \bar{\mathbb{Q}}[s]$ be the polynomial $Q(s) \doteq P(f+sm)$. By construction, $Q \neq 0$ and $Q(t) = 0$. Clearly $\deg Q \le \deg \mathrm{NL}_\Delta$, and we check that

$$\|Q\|_1 \le \|P\|_1 \big(\|f\|_1 + 1\big)^{\deg P}. \tag{91}$$

Then

$$\|Q\|_1 \le 2^{\deg \mathrm{NL}_\Delta} \|\mathrm{NL}_\Delta\|_1 \big(\|f\|_1 + 1\big)^{\deg \mathrm{NL}_\Delta}. \tag{92}$$

From Corollary 15, we find a constant c depending only on f such that

$$\deg Q \le c \uparrow \Delta \uparrow \tfrac{9}{2} \quad \text{and} \quad \|Q\|_1 \le 2 \uparrow c \uparrow \Delta \uparrow \tfrac{9}{2}. \tag{93}$$

We write $Q = \sum_{i=0}^{\deg Q} q_i s^i$. Let k be the smallest integer such that $q_k \neq 0$. Since $Q(t) = 0$, it follows that

$$|q_k t^k| \le \sum_{i=k+1}^{\deg Q} |q_i t^i|. \tag{94}$$

If $\varepsilon < C_f^{-1}$, we have $|t| < 1$, by (86), and it follows that

$$|t| \ge \frac{|q_k|}{\|Q\|_1}. \tag{95}$$

Let $D \ge 1$ be the degree of the number field generated by the coefficients of f. Let $H > 0$ be an upper bound for the absolute logarithmic Weil height for the coefficient vector of f [Waldschmidt 2000, p. 77]. Then q_k is an algebraic number defined by a polynomial expression $\tilde{q}_k(f)$ in the coefficients of f, with $\tilde{q}_k$ having integer coefficients. Liouville's inequality [Waldschmidt 2000, Proposition 3.14] gives

$$|q_k| \ge \|\tilde{q}_k\|_1^{-D+1} e^{-DH \deg \tilde{q}_k}. \tag{96}$$

It is easy to see that $\deg \tilde{q}_k \le \deg \mathrm{NL}_\Delta$ and $\|\tilde{q}_k\|_1 \le 2^{\deg \mathrm{NL}_\Delta} \|\mathrm{NL}_\Delta\|_1$, the latter can be bounded by $\|Q\|_1$.

By (86), this leads to

$$\varepsilon \geq \left(2\uparrow c\uparrow\Delta\uparrow\tfrac{9}{2}\right)^{-D(1+H)}, \tag{97}$$

for some other constant c depending only on f. Recall that (97) holds with the assumptions that $\varepsilon \leq \varepsilon_f$ and $\varepsilon < C_f^{-1}$. However, we can choose c large enough so that the right-hand side of (97) is smaller than ε_f and C_f^{-1}. Then (97) holds unconditionally. Absorb the outer exponent of (97) into c to conclude the proof of Theorem 17. □

4.3. ***Numbers à la Liouville.*** Let $(\theta_i)_{i\geq 0}$ be a sequence of positive integers such that θ_i is a strict divisor of θ_{i+1} for all $i \geq 0$ (in particular, $\theta_i \geq 2^i$.) Consider the number

$$L_\theta \doteq \sum_{i=0}^{\infty} \theta_i^{-1}.$$

As a corollary to the separation bound obtained in Theorem 17, the following result states that L_θ is not a ratio of periods of quartic surfaces when θ grows fast enough:

Theorem 19. *If $\theta_{i+1} \geq 2\uparrow 2\uparrow\theta_i\uparrow 10$, for all i large enough, then L_θ is not equal to $(\gamma_1\cdot\omega_f)/(\gamma_2\cdot\omega_f)$ for any $\gamma_1, \gamma_2 \in H_{\mathbb{Z}}$ and any $f \in U_4$ with algebraic coefficients.*

Proof. Let $l_k = \sum_{i=0}^{k} \theta_i^{-1}$. Since θ_i divides θ_{i+1}, we can write $l_k = u_k/\theta_k$ for some integer u_k. And since the divisibility is strict, $\theta_i \geq 2^i$ and $u_k \leq 2\theta_k$. Moreover,

$$0 < L_\theta - l_k \leq 2\theta_{k+1}^{-1}, \tag{98}$$

using $\theta_{k+i+1} \geq 2^i\theta_{k+1}$, for any $i \geq 0$. Assume now that $L_\theta = (\gamma_1\cdot\omega_f)/(\gamma_2\cdot\omega_f)$ for some $\gamma_1, \gamma_2 \in H_{\mathbb{Z}}$ and some $f \in U_4$ with rational coefficients. Then, with

$$\gamma_k \doteq \theta_k\gamma_1 - u_k\gamma_2, \tag{99}$$

we check that $\Delta(\gamma_k) = O(\theta_k^2)$ and that

$$0 < |\theta_k||\gamma_2\cdot\omega_f|(L_\theta - l_k) = |\gamma_k\cdot\omega_f| \leq C\frac{\theta_k}{\theta_{k+1}}, \tag{100}$$

for some constant C. By Theorem 17, we obtain

$$(2\uparrow c\uparrow\theta_k\uparrow 9)^{-1} \leq C\frac{\theta_k}{\theta_{k+1}}, \tag{101}$$

for some constant $c > 0$ which depends only on f. This contradicts the assumption on the growth of θ. □

4.4. ***Computational complexity.*** Given a polynomial $f \in \bar{\mathbb{Q}}[w, x, y, z] \cap U_4$ and a cohomology class $\gamma \in H^2(X_f, \mathbb{Z})$, we can decide if $\gamma \in \mathrm{Pic}(X_f)$ (that is, $\gamma\cdot\omega_f = 0$) as follows:

(a) Compute the constant c in Theorem 17.

(b) Let $\varepsilon = \left(2\uparrow c\uparrow\Delta(\gamma)\uparrow\tfrac{9}{2}\right)^{-1}$ and compute an approximation $s \in \mathbb{C}$ of the period $\gamma\cdot\omega_f$ such that $|s - \gamma\cdot\omega_f| < \tfrac{1}{2}\varepsilon$.

Then γ is in $\mathrm{Pic}(X_f)$ if and only if $|s| < \tfrac{1}{2}\varepsilon$.

Computing the Picard group itself is an interesting application of this procedure. Algorithms for computing the Picard group of X_f, or even just the rank of it, break the problem into two: a part gives larger and larger lattices inside $\mathrm{Pic}(X_f)$ while the other part gets finer and finer upper bounds on the rank of $\mathrm{Pic}(X_f)$ [Charles 2014; Hassett et al. 2013; Poonen et al. 2015]. The computation stops when the two parts meet. Approximations from the inside are based on finding sufficiently many elements of $\mathrm{Pic}(X_f)$. So while deciding the membership of γ in $\mathrm{Pic}(X_f)$ can be solved by computing $\mathrm{Pic}(X_f)$ first, it makes sense not to assume prior knowledge of the Picard group and to study the complexity of deciding membership as $\Delta(\gamma) \to \infty$, with f fixed.

Step (a) does not depend on γ, so only the complexity of Step (b) matters, that is, the numerical approximation of $\gamma \cdot \omega_f$. This approximation amounts to numerically solving a Picard–Fuchs differential equation [Sertöz 2019] and the complexity is $(\log(1/\varepsilon))^{1+o(1)}$ [Beeler et al. 1972; van der Hoeven 2001; Mezzarobba 2010; 2016]. With the value of ε in Step (b), we have a complexity bound of $\exp(\Delta(\gamma)^{O(1)})$ for deciding membership.

For the sake of comparison, we may speculate about an approach that would decide the membership of γ in $\mathrm{Pic}(X_f)$ by trying to construct an explicit algebraic divisor on X_f whose cohomology class is equal to γ. It would certainly need to decide the existence of a point satisfying some algebraic conditions in some Hilbert scheme $\mathcal{H}_{d,g}$, with $d = O(\Delta^{\frac{1}{2}})$ and $g = O(\Delta)$ (see Section 3.1.1). Embedding $\mathcal{H}_{d,g}$ (or some fibration over it, as we did in Section 3.4) in some affine chart of a projective space of dimension $d^{O(1)}$ will lead to a complexity of $\exp(\Delta(\gamma)^{O(1)})$ for deciding membership in this way.

However, if Conjecture 16 holds true, then the complexity of the numerical approach for deciding membership would reduce to $\Delta(\gamma)^{O(1)}$.

5. Concluding remarks

5.1. ***Going beyond quartic surfaces.*** There are two directions in which the main result, Theorem 17, can, in principle, be generalized beyond quartic surfaces.

In the first direction, our effective methods naturally extend to complete intersections in complete simplicial toric varieties, provided the complete intersection has a K3 type middle cohomology satisfying the integral Hodge conjecture. By this last condition, we mean that a single period should govern if a homology cycle is algebraic. For instance, cubic fourfolds satisfy all of these conditions [Voisin 2013]. Of course, polarized K3 surfaces of degrees 2, 6 and 8 also work, in addition to the degree 4 case covered here.

To generalize the result to this context, one needs to compute two ingredients. The height and degree bounds for the image of a Hilbert schemes, and the "spread" of the period map (as in Section 2.4). Our use of effective Nullstellensatz to compute heights clearly extends. To compute the spread, we used the Griffiths–Dwork reduction, which continues to work for complete intersections in compact simplicial toric varieties [Batyrev and Cox 1994; Dimca 1995; Mavlyutov 1999].

The second direction one could generalize the result is to stick with surfaces in $\mathbb{P}^3$ but to increase the degree. In this case, we do not know how to control the vanishing of individual period integrals. However, the Lefschetz (1, 1)-theorem can be used to relate algebraic cycles to the simultaneous vanishing of a vector of periods coming from all holomorphic forms. For instance, on quintic surfaces one can separate 4-dimensional (holomorphic) period vectors from one another. The deduction of the separation bounds would be possible from a parallel discussion to the one provided here. This application would make it possible to prove our heuristic Picard group computations of surfaces [Lairez and Sertöz 2019].

It would also be highly desirable to be able to numerically verify arbitrary, nonlinear, relations between periods of quartics. However, in order to generalize our approach to this setup, one would need the integral Hodge conjecture on products of quartic surfaces.

5.2. ***Closed formulae for the bounds.*** It is possible to determine a closed formula, involving the height of f, that bounds the constant c in Theorem 17. We removed the deduction of such a formula due to the excessive technical complexity it presents. In addition, the pursuit of a human readable bound gets us further and further from the optimal bounds. We envisioned using the constant c on computer calculations where an algorithmic deduction of c is possible and preferable. We designed our proofs so that such an algorithm is explicit in the proofs. An implementation of this algorithm would be beneficial after the bounds for the heights of the Noether–Lefschetz loci are brought down significantly.

5.3. ***Optimal bounds.*** We conjectured by analogy (Conjecture 16) that our bounds for the height of the Noether–Lefschetz locus can be lowered by one level of exponentiation. One can be more optimistic based on the following observation: For many example quartics X_f, we determined the equations for the Hilbert scheme of lines over each pencil X_{f+tm} for monomials m. Then, going through the algorithm in the proofs, we computed sharper separation bounds on these example quartics. On these examples, the separation bound was around 10^{-60}. In other words, it was sufficient to deduce whether a homology cycle was the class of a line using only 60 digits of precision. This suggests that for homology cycles of small discriminant, optimal separation bounds may be small enough to be used in practice. It would be interesting to see if generalizing the work of Maulik and Pandharipande from degrees to heights by using the modularity of arithmetic Chow rings [Kudla 2003] would give close to optimal bounds.

5.4. ***Analogies with related work.*** Our construction bears a remote resemblance to the analytic subgroup theorem of Wüstholz [1989] and the period theorem of Masser and Wüstholz [1993]. The analytic subgroup theorem and its applications work with the exponential map $\exp_A : T_0 A \to A$ of a (principally polarized) abelian variety A over $\bar{\mathbb{Q}} \subset \mathbb{C}$. The periods of A form a lattice $\Lambda \doteq \ker \exp A$. Let $P = \exp_A^{-1} A(\bar{\mathbb{Q}})$ be the periods of all algebraic points on A.

The analytic subgroup theorem implies that $\bar{\mathbb{Q}}$-linear relations between any set of elements $S \subset P$ are determined by abelian subvarieties of B: there is an abelian subvariety such that $T_0 B$ coincides with the span of S. Observe that the linear relations live on the domain of the transcendental map $\exp_A$ and are converted to an algebraic subvariety on the codomain. When $S = \{\gamma\} \subset \Lambda$, the Masser–Wüstholz period theorem bounds the degree of smallest B whose tangent space contains γ using the height of A and the norm of γ.

In our work, we consider the space U_4 of smooth homogeneous quartic polynomials of degree 4 and its universal cover $\widetilde{U}_4 \to U_4$. We then take the (transcendental) period map $\mathcal{P}\colon \widetilde{U}_4 \to H_{\mathbb{C}}$. Note that the $\mathbb{Z}$-relations between periods are realized as linear subspaces of the period domain, whereas the preimage of these linear spaces are the Noether–Lefschetz loci. These Noether–Lefschetz loci map to algebraic hypersurfaces on the space U_4.

Superficially, the main difference between the two approaches is the direction of the naturally appearing transcendental maps that linearize relations between periods. However, the nature of the two transcendental maps appearing in both constructions also differs substantially.

Acknowledgements

We thank Bjorn Poonen for suggesting the use of heights of Noether–Lefschetz loci and Gavril Farkas for suggesting the paper by Maulik and Pandharipande. We also thank Alin Bostan and Matthias Schütt for numerous helpful comments. We thank the referee for a careful reading of the paper.

Sertöz was supported by the Max Planck Institute for Mathematics in the Sciences, Leibniz University Hannover, and the Max Planck Institute for Mathematics. Lairez was supported by the project *De Rerum Natura* ANR-19-CE40-0018 of the French National Research Agency (ANR).

References

[Batyrev and Cox 1994] V. V. Batyrev and D. A. Cox, "On the Hodge structure of projective hypersurfaces in toric varieties", *Duke Math. J.* **75**:2 (1994), 293–338. MR Zbl

[Bayer 1982] D. A. Bayer, *The division algorithm and the Hilbert scheme*, Ph.D. thesis, Harvard University, 1982, available at https://www.proquest.com/docview/303209159.

[Beeler et al. 1972] M. Beeler, R. W. Gosper, and R. Schroeppel, "HAKMEM", AI memo 239, MIT AI Lab., 1972, available at https://tinyurl.com/hakmem239.

[Blum et al. 1998] L. Blum, F. Cucker, M. Shub, and S. Smale, *Complexity and real computation*, Springer, 1998. MR Zbl

[Booker et al. 2016] A. R. Booker, J. Sijsling, A. V. Sutherland, J. Voight, and D. Yasaki, "A database of genus-2 curves over the rational numbers", *LMS J. Comput. Math.* **19**:suppl. A (2016), 235–254. MR Zbl

[Bost et al. 1991] J.-B. Bost, H. Gillet, and C. Soulé, "Un analogue arithmétique du théorème de Bézout", *C. R. Acad. Sci. Paris Sér. I Math.* **312**:11 (1991), 845–848. MR Zbl

[Brachat et al. 2016] J. Brachat, P. Lella, B. Mourrain, and M. Roggero, "Extensors and the Hilbert scheme", *Ann. Sc. Norm. Super. Pisa Cl. Sci.* (5) **16**:1 (2016), 65–96. MR Zbl

[Bruin et al. 2019] N. Bruin, J. Sijsling, and A. Zotine, "Numerical computation of endomorphism rings of Jacobians", pp. 155–171 in *Proceedings of the Thirteenth Algorithmic Number Theory Symposium* (Madison, WI, 2018), edited by R. Scheidler and J. Sorenson, Open Book Ser. **2**, Math. Sci. Publ., Berkeley, CA, 2019. MR

[Charles 2014] F. Charles, "On the Picard number of K3 surfaces over number fields", *Algebra Number Theory* **8**:1 (2014), 1–17. MR Zbl

[Costa et al. 2019] E. Costa, N. Mascot, J. Sijsling, and J. Voight, "Rigorous computation of the endomorphism ring of a Jacobian", *Math. Comp.* **88**:317 (2019), 1303–1339. MR Zbl

[D'Andrea et al. 2013] C. D'Andrea, T. Krick, and M. Sombra, "Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze", *Ann. Sci. École Norm. Sup.* (4) **46**:4 (2013), 549–627. MR Zbl

[Dimca 1995] A. Dimca, "Residues and cohomology of complete intersections", *Duke Math. J.* **78**:1 (1995), 89–100. MR Zbl

[Gotzmann 1978] G. Gotzmann, "Eine Bedingung für die Flachheit und das Hilbertpolynom eines graduierten Ringes", *Math. Z.* **158**:1 (1978), 61–70. MR Zbl

[Griffiths 1969a] P. A. Griffiths, "On the periods of certain rational integrals, I", *Ann. of Math.* (2) **90**:3 (1969), 460–495. MR Zbl

[Griffiths 1969b] P. A. Griffiths, "On the periods of certain rational integrals, II", *Ann. of Math.* (2) **90**:3 (1969), 496–541. MR Zbl

[Griffiths and Harris 1978] P. Griffiths and J. Harris, *Principles of algebraic geometry*, Wiley, New York, 1978. MR Zbl

[Grothendieck 1966] A. Grothendieck, "Techniques de construction et théorèmes d'existence en géométrie algébrique, IV: Les schémas de Hilbert", exposé 221 in *Séminaire Bourbaki*: 1960/1961, W. A. Benjamin, New York, 1966. Reprinted as pp. 249–276 in *Séminaire Bourbaki* **6**, Soc. Math. France, Paris, 1995. MR

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, 1977. MR Zbl

[Hassett et al. 2013] B. Hassett, A. Kresch, and Y. Tschinkel, "Effective computation of Picard groups and Brauer–Manin obstructions of degree two $K3$ surfaces over number fields", *Rend. Circ. Mat. Palermo* (2) **62**:1 (2013), 137–151. MR Zbl

[van der Hoeven 2001] J. van der Hoeven, "Fast evaluation of holonomic functions near and in regular singularities", *J. Symbolic Comput.* **31**:6 (2001), 717–743. MR Zbl

[Huybrechts 2016] D. Huybrechts, *Lectures on K3 surfaces*, Cambridge Stud. Adv. Math. **158**, Cambridge Univ. Press, 2016. MR Zbl

[Kontsevich and Zagier 2001] M. Kontsevich and D. Zagier, "Periods", pp. 771–808 in *Mathematics unlimited*: 2001 *and beyond*, edited by B. Engquist and W. Schmid, Springer, 2001. MR Zbl

[Krätzel 2000] E. Krätzel, *Analytische Funktionen in der Zahlentheorie*, Teubner-Texte Math. **139**, Teubner, Stuttgart, 2000. MR Zbl

[Krick et al. 2001] T. Krick, L. M. Pardo, and M. Sombra, "Sharp estimates for the arithmetic Nullstellensatz", *Duke Math. J.* **109**:3 (2001), 521–598. MR Zbl

[Kudla 2003] S. S. Kudla, "Modular forms and arithmetic geometry", pp. 135–179 in *Current developments in mathematics* (Cambridge, 2002), edited by D. Jerison et al., Int. Press, Somerville, MA, 2003. MR Zbl

[Lairez and Sertöz 2019] P. Lairez and E. C. Sertöz, "A numerical transcendental method in algebraic geometry: computation of Picard groups and related invariants", *SIAM J. Appl. Algebra Geom.* **3**:4 (2019), 559–584. MR Zbl

[Lazard 1977] D. Lazard, "Algèbre linéaire sur $K[X_1, \dots, X_n]$, et élimination", *Bull. Soc. Math. France* **105**:2 (1977), 165–190. MR Zbl

[Lella 2012] P. Lella, *Computable Hilbert schemes*, Ph.D. thesis, Università degli Studi di Torino, 2012. arXiv 1202.4384

[Liouville 1851] J. Liouville, "Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques", *J. Math. Pures Appl.* **16** (1851), 133–142.

[Masser and Wüstholz 1993] D. Masser and G. Wüstholz, "Periods and minimal abelian subvarieties", *Ann. of Math.* (2) **137**:2 (1993), 407–458. MR Zbl

[Maulik and Pandharipande 2013] D. Maulik and R. Pandharipande, "Gromov–Witten theory and Noether–Lefschetz theory", pp. 469–507 in *A celebration of algebraic geometry* (Cambridge, 2011), edited by B. Hassett et al., Clay Math. Proc. **18**, Amer. Math. Soc., Providence, RI, 2013. MR Zbl

[Mavlyutov 1999] A. R. Mavlyutov, "Cohomology of complete intersections in toric varieties", *Pacific J. Math.* **191**:1 (1999), 133–144. MR Zbl

[Mezzarobba 2010] M. Mezzarobba, "NumGfun: a package for numerical and analytic computation with D-finite functions", pp. 139–146 in *ISSAC* 2010: *Proceedings of the* 2010 *International Symposium on Symbolic and Algebraic Computation* (Munich, 2010), edited by S. M. Watt, ACM, New York, 2010. MR Zbl

[Mezzarobba 2016] M. Mezzarobba, "Rigorous multiple-precision evaluation of D-finite functions in SageMath", lecture notes, 2016. arXiv 1607.01967

[Philippon 1995] P. Philippon, "Sur des hauteurs alternatives, III", *J. Math. Pures Appl.* (9) **74**:4 (1995), 345–365. MR Zbl

[Piene and Schlessinger 1985] R. Piene and M. Schlessinger, "On the Hilbert scheme compactification of the space of twisted cubics", *Amer. J. Math.* **107**:4 (1985), 761–774. MR Zbl

[Poonen et al. 2015] B. Poonen, D. Testa, and R. van Luijk, "Computing Néron–Severi groups and cycle class groups", *Compos. Math.* **151**:4 (2015), 713–734. MR Zbl

[Rémond 2001a] G. Rémond, "Élimination multihomogène", pp. 53–81 in *Introduction to algebraic independence theory*, edited by Y. V. Nesterenko and P. Philippon, Lecture Notes in Math. **1752**, Springer, 2001. MR

[Rémond 2001b] G. Rémond, "Géométrie diophantienne multiprojective", pp. 95–131 in *Introduction to algebraic independence theory*, edited by Y. V. Nesterenko and P. Philippon, Lecture Notes in Math. **1752**, Springer, 2001. MR

[Sertöz 2019] E. C. Sertöz, "Computing periods of hypersurfaces", *Math. Comp.* **88**:320 (2019), 2987–3022. MR Zbl

[Shidlovskii 1989] A. B. Shidlovskii, *Transcendental numbers*, de Gruyter Stud. Math. **12**, de Gruyter, Berlin, 1989. MR Zbl

[Simpson 2008] C. Simpson, "Algebraic cycles from a computational point of view", *Theoret. Comput. Sci.* **392**:1-3 (2008), 128–140. MR Zbl

[Smale 1986] S. Smale, "Newton's method estimates from data at one point", pp. 185–196 in *The merging of disciplines: new directions in pure, applied, and computational mathematics* (Laramie, WY, 1985), edited by R. E. Ewing et al., Springer, 1986. MR Zbl

[Voisin 2003] C. Voisin, *Hodge theory and complex algebraic geometry, II*, Cambridge Stud. Adv. Math. **77**, Cambridge Univ. Press, 2003. MR Zbl

[Voisin 2013] C. Voisin, "Abel–Jacobi map, integral Hodge classes and decomposition of the diagonal", *J. Algebraic Geom.* **22**:1 (2013), 141–174. MR Zbl

[Waldschmidt 2000] M. Waldschmidt, *Diophantine approximation on linear algebraic groups*, Grundlehren der Math. Wissenschaften **326**, Springer, 2000. MR Zbl

[van Wamelen 1999] P. van Wamelen, "Examples of genus two CM curves defined over the rationals", *Math. Comp.* **68**:225 (1999), 307–320. MR Zbl

[Wüstholz 1989] G. Wüstholz, "Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen", *Ann. of Math.* (2) **129**:3 (1989), 501–517. MR Zbl

Communicated by Antoine Chambert-Loir
Received 2021-06-18 Revised 2022-05-19 Accepted 2022-09-21

pierre.lairez@inria.fr *INRIA Saclay, Palaiseau, France*

emre@sertoz.com *Faculty of Mathematics and Physics, Leibniz Universität Hannover, Hannover, Germany*

ALGEBRA AND NUMBER THEORY 17:10 (2023)
https://doi.org/10.2140/ant.2023.17.1779

Global dimension of real-exponent polynomial rings

Nathan Geist and Ezra Miller

The ring R of real-exponent polynomials in n variables over any field has global dimension $n+1$ and flat dimension n. In particular, the residue field $\Bbbk = R/\mathfrak{m}$ of R modulo its maximal graded ideal $\mathfrak{m}$ has flat dimension n via a Koszul-like resolution. Projective and flat resolutions of all R-modules are constructed from this resolution of $\Bbbk$. The same results hold when R is replaced by the monoid algebra for the positive cone of any subgroup of $\mathbb{R}^n$ satisfying a mild density condition.

1. Introduction

Overview. The aim of this note is to prove that the commutative ring R of real-exponent polynomials in n variables over any field $\Bbbk$ has global dimension $n+1$ and flat dimension n (Theorem 3.6 and Corollary 2.10). It might be unexpected that R has finite global dimension at all, but it should be more expected that the flat dimension is achieved by the residue field $\Bbbk = R/\mathfrak{m}$ of R modulo its maximal graded ideal $\mathfrak{m}$; a Koszul-like construction shows that it is (Proposition 2.4 along with Example 2.5). In one real-exponent variable the residue field $\Bbbk$ also achieves the global dimension bound of 2 (Lemma 3.2), and this calculation lifts to n variables by tensoring with an ordinary Koszul complex (Proposition 3.4), demonstrating global dimension at least $n+1$. Projective and flat resolutions of all R-modules are constructed from resolutions of the residue field in the proofs of Theorems 3.6 and 2.9 to yield the respective upper bounds of $n+1$ and n. The results extend to the monoid algebra for the positive cone of any subgroup of $\mathbb{R}^n$ satisfying a mild density condition (Definition 4.1 and Theorem 4.3).

Background. Global dimension measures how long projective resolutions of modules can get, or how high the homological degree of a nonvanishing Ext module can be [20, Theorem 4.1.2]. Finding rings of finite global dimension is of particular value, since they are considered to be smooth, generalizing the best-known case of local noetherian commutative rings [2; 19], which correspond to germs of functions on nonsingular algebraic varieties.

The related notion of flat dimension (also called Tor dimension or weak global dimension) measures how long flat resolutions of modules can get, or how high the homological degree of a nonvanishing Tor module can be. Flat dimension is bounded by global dimension because projective modules are flat. These two dimensions agree for noetherian commutative rings [20, Proposition 4.1.5]. Without the

MSC2020: primary 05E40, 06F05, 13D02, 13D05, 13F20; secondary 13P25, 14A22, 55N31, 62R40.
Keywords: global dimension, homological dimension, flat dimension, polynomial ring, real-exponent polynomial, commutative ring, monoid algebra, real cone, quantum noncommutative toric variety, persistent homology.

noetherian condition equality can fail; commutative examples include von Neumann regular rings that are infinite products of fields (see [20, page 98]), but domains are harder to come by.

The cardinality of a real-exponent polynomial ring a priori indicates a difference between flat and projective dimension that could be as high as 1 plus the index on $\aleph$ in the cardinality of the real numbers [17, page 14]. In certain situations, such as in valuation rings, ideals generated by $\aleph_n$ and no fewer elements are known to cause global dimension at least $n+2$ [16]; see also [17, page 14]. But despite R having an ideal minimally generated by all monomials with total degree 1, of which there are $2^{\aleph_0}$, the dimension of the positive cone of exponents is more pertinent than its cardinality. This remains the case when the exponent set is intersected with a suitably dense subgroup of $\mathbb{R}^n$: the rank of the subgroup is irrelevant (Section 4).

Methods. The increase from global dimension n to $n+1$ in the presence of n variables is powered by the violation of condition 5 from [3, Theorem P]: a monomial ideal with an "open orthant" of exponents, such as the maximal ideal $\mathfrak{m}_1$ in one indeterminate, is a direct limit of principal monomial ideals (Lemma 3.1) but is not projective (Lemma 3.2). This phenomenon occurs already for Laurent polynomials L_1 in one integer-exponent variable. But although $\mathfrak{m}_1$ and L_1 both have projective dimension 1, the real-exponent maximal ideal $\mathfrak{m}_1$ is a submodule of a projective (actually, free) module; the inclusion has a cokernel, and its projective dimension is greater by 1.

The most nontrivial point is how to produce a projective resolution of length at most $n+1$ for any module over the real-exponent polynomial ring R in n variables. Our approach takes two steps. The first is a length n Koszul-like complex (Definition 2.7) in $2n$ variables that resolves the residue field and can be massaged into a flat resolution of any module (Theorem 2.9). This "total Koszul" construction was applied to combinatorially resolve monomial ideals in ordinary (that is, integer-exponent) polynomial rings [7, Section 6]. The integer grading in the noetherian case makes this construction produce a Koszul double complex, which is key for the combinatorial purpose of minimalizing the resulting free resolution by splitting an associated spectral sequence. It is not obvious whether the double complex survives to the real-exponent setting, but the total complex does (Definition 2.7; see [20, Application 4.5.6]), and that suffices here because minimality is much more subtle — if it is even possible — in the presence of real exponents [13].

Motivations. Beyond basic algebra, there has been increased focus on nonnoetherian settings in, for example, noncommutative geometry and topological data analysis.

Quantum noncommutative toric geometry [9] is based on dense finitely generated additive subgroups of $\mathbb{R}^n$ instead of the discrete sublattices that the noetherian commutative setting requires. The situations treated by our main theorems, including especially Section 4, correspond to "smooth" affine quantum toric varieties and could have consequences for sheaf theory in that setting.

The question of finite global dimension over real-exponent polynomial rings has surfaced in topological data analysis (TDA), where modules graded by $\mathbb{R}^n$ are known as real multiparameter persistent homology; see [6; 12; 13], for example, or [18] for a perspective from quiver theory. The question of global dimension arises because defining metrics for statistical analysis requires distances between persistence modules, many of which use derived categorical constructions [4; 8; 15]; see [6, Section 7.1] for an explicit mention of the finite global dimension problem.

Real-exponent modules that are graded by $\mathbb{R}^n$ and satisfy a suitable finiteness condition ("tameness") to replace the too-easily violated noetherian or finitely presented conditions admit finite multigraded resolutions by monomial ideals [14, Theorem 6.12], which are useful for TDA. But even in the tame setting no universal bound is known for the finite lengths of such resolutions [13, Remark 13.15]. The global dimension calculations here suggest but do not immediately imply a universal bound of $n+1$.

Notation. The ordered additive group $\mathbb{R}$ of real numbers has its monoid $\mathbb{R}_+$ of nonnegative elements. The n-fold product $\mathbb{R}^n = \prod_{i=1}^n \mathbb{R}$ has nonnegative cone $\mathbb{R}^n_+ = \prod_{i=1}^n \mathbb{R}_+$. The monoid algebra $R = R_n = \Bbbk[\mathbb{R}^n_+]$ over an arbitrary field $\Bbbk$ is the ring of real-exponent polynomials in n variables: finite sums $\sum_{\boldsymbol{a}\in\mathbb{R}^n_+} c_{\boldsymbol{a}}\boldsymbol{x}^{\boldsymbol{a}}$, where $\boldsymbol{x}^{\boldsymbol{a}} = x_1^{a_1}\cdots x_n^{a_n}$. Its unique monoid-graded maximal ideal $\mathfrak{m}$ is spanned over $\Bbbk$ by all nonunit monomials.

Unadorned tensor products are over $\Bbbk$. For example, $R \cong R_1 \otimes \cdots \otimes R_1$ is an n-fold tensor product over $\Bbbk$, where $R_1 = \Bbbk[\mathbb{R}_+]$ is the real-exponent polynomial ring in one variable with graded maximal ideal $\mathfrak{m}_1$.

2. Flat dimension n

Lemma 2.1. *The filtered colimit $\varinjlim_{\varepsilon>0}(R_1 \hookleftarrow \langle x^\varepsilon\rangle)$ of the inclusions of the principal ideals generated by x^ε for positive $\varepsilon \in \mathbb{R}$ is a flat resolution $\mathring{\mathbb{K}}^1_\bullet : R_1 \hookleftarrow \mathfrak{m}_1$ of $\Bbbk$ over R_1.*

Proof. Colimits commute with homology so the colimit is a resolution. Filtered colimits of free modules are flat by Lazard's criterion [11], so the resolution is flat. □

Definition 2.2. The *open Koszul complex* is the tensor product $\mathring{\mathbb{K}}^{\boldsymbol{x}}_\bullet = \bigotimes_{i=1}^n \mathring{\mathbb{K}}^1_\bullet$ over the field $\Bbbk$ of n copies of the flat resolution in Lemma 2.1. The 2^n summands of $\mathring{\mathbb{K}}^{\boldsymbol{x}}_\bullet$, each a tensor product of j copies of R_1 and $n-j$ copies of $\mathfrak{m}_1$, are *orthant ideals*.

Example 2.3. The open Koszul complex in two real-exponent variables is depicted in Figure 2. From a geometric perspective, take the ordinary Koszul complex from Figure 1, replace the free modules with their continuous versions, and push the generators as close to the origin as possible without meeting it. The four possible orthant ideals are rendered in Figure 2. From left to right, viewing them as tensor products, they correspond to the product of two closed rays $\Bbbk[\mathbb{R}_+]$, the product (in both orders) of a closed ray with an open ray $\mathfrak{m}$, and the product of two open rays. In n real-exponent variables the 2^n orthant ideals arise from all n-fold tensor products of closed and open rays.

Proposition 2.4. *The open Koszul complex $\mathring{\mathbb{K}}^{\boldsymbol{x}}_\bullet$ is a flat resolution of $\Bbbk$ over R.*

Proof. Lemma 2.1 and the Künneth theorem [20, Theorem 3.6.3]. □

Limit-Koszul complexes similar to $\mathring{\mathbb{K}}^{\boldsymbol{x}}_\bullet$ have previously been used to compute flat dimensions of absolute integral closures [1] in the context of tight closure.

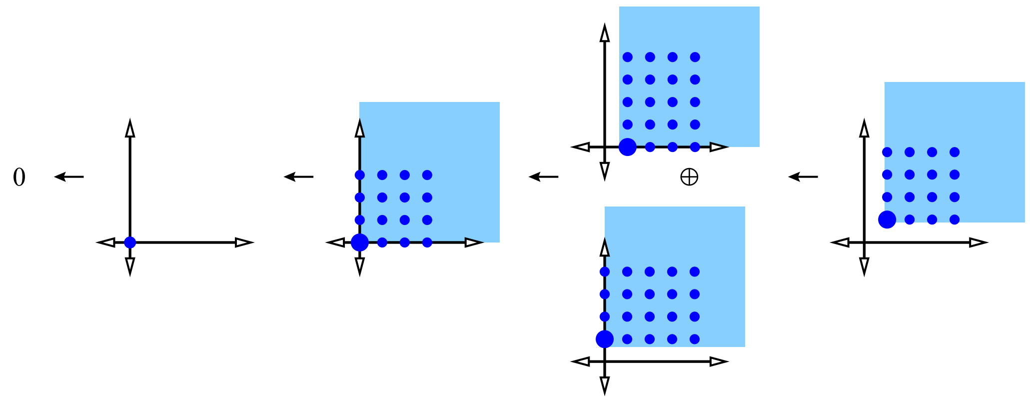

Figure 1. Ordinary Koszul complex in two variables.

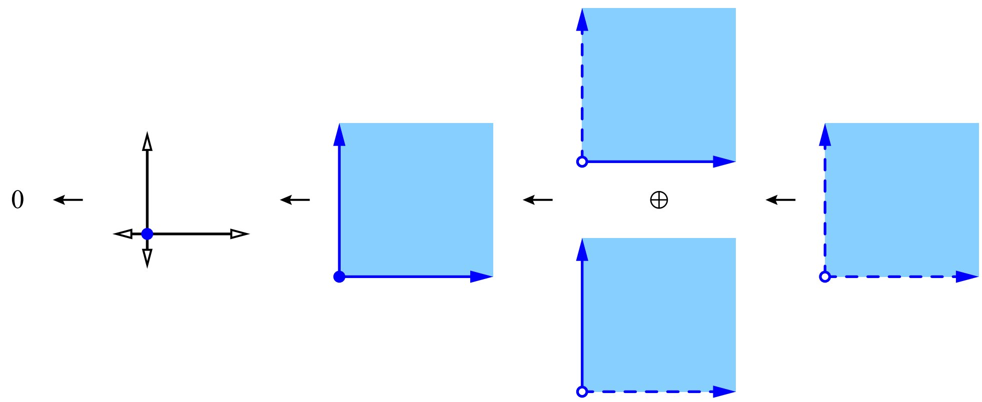

Figure 2. Open Koszul complex in two real-exponent variables.

Example 2.5. The sequence $\boldsymbol{x}^{[\varepsilon]} = x_1^\varepsilon, \dots, x_n^\varepsilon$ is regular in R [5, Chapter 1], so the usual Koszul complex $\mathbb{K}_\bullet(\boldsymbol{x}^{[\varepsilon]})$ is a length n free resolution of $B_n^\varepsilon = R/\langle \boldsymbol{x}^{[\varepsilon]}\rangle$ over R. Using this resolution, $\mathrm{Tor}_n^R(\Bbbk, B_n^\varepsilon) = \Bbbk$ because $\Bbbk \otimes_R \mathbb{K}_\bullet(\boldsymbol{x}^{[\varepsilon]})$ has vanishing differentials.

Lemma 2.6. *The real-exponent polynomial ring $R^{\otimes 2} = R \otimes R$ has $2n$ variables*

$$\boldsymbol{x} = x_1, \dots, x_n = x_1 \otimes 1, \dots, x_n \otimes 1 \quad \textit{and} \quad \boldsymbol{y} = y_1, \dots, y_n = 1 \otimes x_1, \dots, 1 \otimes x_n.$$

Over $R^{\otimes 2}$ is a directed system of Koszul complexes $\mathbb{K}_\bullet(\boldsymbol{x}^{[\varepsilon]} - \boldsymbol{y}^{[\varepsilon]})$ on the sequences

$$\boldsymbol{x}^{[\varepsilon]} - \boldsymbol{y}^{[\varepsilon]} = x_1^\varepsilon - y_1^\varepsilon, \dots, x_n^\varepsilon - y_n^\varepsilon$$

with $\varepsilon > 0$. The colimit $\mathring{\mathbb{K}}_\bullet^{\boldsymbol{x}-\boldsymbol{y}} = \varinjlim_{\varepsilon>0} \mathbb{K}_\bullet(\boldsymbol{x}^{[\varepsilon]} - \boldsymbol{y}^{[\varepsilon]})$ is an $R^{\otimes 2}$-flat resolution of R.

Proof. The general case is the tensor product over $\Bbbk$ of n copies of the case $n = 1$, which in turn reduces to the calculation $R^{\otimes 2}/\langle x^\varepsilon - y^\varepsilon \mid \varepsilon > 0\rangle \cong R$. $\square$

Definition 2.7. Denote by $R^{\boldsymbol{x}}$ and $R^{\boldsymbol{y}}$ the copies of R embedded in $R^{\otimes 2}$ as $R \otimes 1$ and $1 \otimes R$. Fix an $R^{\boldsymbol{x}}$-module M:

(1) Write $M^{\boldsymbol{y}}$ for the corresponding $R^{\boldsymbol{y}}$-module, with the $\boldsymbol{x}$ variables renamed to $\boldsymbol{y}$.

(2) The *open total Koszul complex* of an $R^{\boldsymbol{x}}$-module M is $\mathring{\mathbb{K}}_{\bullet}^{\boldsymbol{x}-\boldsymbol{y}}(M) = \mathring{\mathbb{K}}_{\bullet}^{\boldsymbol{x}-\boldsymbol{y}} \otimes_{R^{\boldsymbol{y}}} M^{\boldsymbol{y}}$.

Remark 2.8. By Definition 2.2, each of the 4^n summands of $\mathring{\mathbb{K}}_{\bullet}^{\boldsymbol{x}-\boldsymbol{y}}$ in Lemma 2.6 is the tensor product over $\Bbbk$ of an orthant $R^{\boldsymbol{x}}$-ideal and an orthant $R^{\boldsymbol{y}}$-ideal.

Theorem 2.9. *The open total Koszul complex $\mathring{\mathbb{K}}_{\bullet}^{\boldsymbol{x}-\boldsymbol{y}}(M)$ is a length n resolution of M over $R^{\otimes 2}$ for any $R^{\boldsymbol{x}}$-module M. This resolution is flat over $R^{\boldsymbol{x}}$; more precisely, as an $R^{\boldsymbol{x}}$-module $\mathring{\mathbb{K}}_{\bullet}^{\boldsymbol{x}-\boldsymbol{y}}(M)$ is a direct sum of orthant $R^{\boldsymbol{x}}$-ideals.*

Proof. The tensor product $\mathring{\mathbb{K}}_{\bullet}^{\boldsymbol{x}-\boldsymbol{y}} \otimes_{R^{\boldsymbol{y}}} M^{\boldsymbol{y}}$ is over $R^{\boldsymbol{y}}$ and hence converts the orthant $R^{\boldsymbol{x}}$-ideal decomposition for $\mathring{\mathbb{K}}^{\boldsymbol{x}-\boldsymbol{y}}$ afforded by Remark 2.8 into one for $\mathring{\mathbb{K}}_{\bullet}^{\boldsymbol{x}-\boldsymbol{y}}(M)$.

Since tensor products commute with colimits, $\mathring{\mathbb{K}}_{\bullet}^{\boldsymbol{x}-\boldsymbol{y}}(M) = \varinjlim_{\varepsilon>0} \mathbb{K}_{\bullet}^{\varepsilon}(M)$, where $\mathbb{K}_{\bullet}^{\varepsilon}(M) = \mathbb{K}_{\bullet}(\boldsymbol{x}^{[\varepsilon]} - \boldsymbol{y}^{[\varepsilon]}) \otimes_{R^{\boldsymbol{y}}} M^{\boldsymbol{y}}$. Each complex $\mathbb{K}_{\bullet}^{\varepsilon}(M)$ is the ordinary Koszul complex of the sequence $\boldsymbol{x}^{[\varepsilon]} - \boldsymbol{y}^{[\varepsilon]}$ on the $R^{\otimes 2}$-module $R^{\otimes 2} \otimes_{R^{\boldsymbol{y}}} M^{\boldsymbol{y}}$. But $\boldsymbol{x}^{[\varepsilon]} - \boldsymbol{y}^{[\varepsilon]}$ is a regular sequence on this module because the $\boldsymbol{x}$ variables are algebraically independent from the $\boldsymbol{y}$ variables. Thus $\mathbb{K}_{\bullet}^{\varepsilon}(M)$ is acyclic by exactness of colimits. Moreover, again by algebraic independence, the nonzero homology of $\mathbb{K}_{\bullet}^{\varepsilon}(M)$ is naturally the $R^{\boldsymbol{y}}$-module $M^{\boldsymbol{y}}$, with an action of $\Bbbk[\boldsymbol{x}^{[\varepsilon]}]$ where x_i^{ε} acts the same way as y_i^{ε} due to the relation $x_i^{\varepsilon} - y_i^{\varepsilon}$. □

Corollary 2.10. *The n-variable real-exponent polynomial ring has flat dimension n.*

Proof. Example 2.5 implies that $\operatorname{fl.dim} R \geq n$, and $\operatorname{fl.dim} R \leq n$ by Theorem 2.9. □

3. Global dimension $n+1$

Lemma 3.1. *Fix an orthant ideal $\mathcal{O} \neq R$. Choose a sequence $\{\boldsymbol{\varepsilon}_k\}_{k\in\mathbb{N}}$ such that $\boldsymbol{\varepsilon}_k = (\varepsilon_{1k}, \dots, \varepsilon_{nk}) \in \mathbb{R}_+^n$ has*

- *$\varepsilon_{ik} = 0$ for all k if the i-th factor of $\mathcal{O}$ is R_1 and*
- *$\{\varepsilon_{ik}\}_{k\in\mathbb{N}}$ strictly decreases with limit 0 if the i-th factor of $\mathcal{O}$ is $\mathfrak{m}_1$.*

Let $F = \bigoplus_k \langle \boldsymbol{x}^{\boldsymbol{\varepsilon}_k} \rangle$ be the direct sum of the principal ideals in R generated by the monomials with degrees $\boldsymbol{\varepsilon}_k$. Each summand $\langle \boldsymbol{x}^{\boldsymbol{\varepsilon}_k} \rangle$ is free with basis vector 1_k, and $\mathcal{O}$ has a free resolution $0 \leftarrow F \leftarrow F \leftarrow 0$ whose differential sends $1_k \in \langle \boldsymbol{x}^{\boldsymbol{\varepsilon}_k} \rangle$ to $1_k - \boldsymbol{x}^{\boldsymbol{\varepsilon}_k - \boldsymbol{\varepsilon}_{k+1}} 1_{k+1}$.

Proof. The augmentation map $\mathcal{O} \xleftarrow{\alpha} F$ sends 1_k to $\boldsymbol{x}^{\boldsymbol{\varepsilon}_k}$. It is surjective by definition of $\mathcal{O}$. Since α is graded by the monoid $\mathbb{R}_+^n$, its kernel can be calculated degree by degree. In degree $\boldsymbol{a} \in \mathbb{R}_+$ the kernel is spanned by all differences $\boldsymbol{x}^{\boldsymbol{a}-\boldsymbol{\varepsilon}_k} 1_k - \boldsymbol{x}^{\boldsymbol{a}-\boldsymbol{\varepsilon}_\ell} 1_\ell$ such that $\boldsymbol{\varepsilon}_k$ and $\boldsymbol{\varepsilon}_\ell$ both weakly precede $\boldsymbol{a}$; indeed, this subspace of the $\boldsymbol{a}$-graded component $F_{\boldsymbol{a}}$ has codimension 1, and it is contained in the kernel because $\boldsymbol{x}^{\boldsymbol{a}-\boldsymbol{\varepsilon}_k} \boldsymbol{x}^{\boldsymbol{\varepsilon}_k} = \boldsymbol{x}^{\boldsymbol{a}-\boldsymbol{\varepsilon}_\ell} \boldsymbol{x}^{\boldsymbol{\varepsilon}_\ell}$. The differential is injective because each element $f \in F$ has nonzero coefficient on a basis vector 1_k with k maximal, and the image of f has nonzero coefficient on 1_{k+1}. □

Lemma 3.2. *$\Bbbk = R_1/\mathfrak{m}_1$ has a free resolution of length* 2, *and* $\operatorname{Ext}^2_{R_1}(\Bbbk, F) \neq 0$.

Proof. The resolution of $\mathfrak{m}_1$ over R_1 in Lemma 3.1 (with $n = 1$) can be augmented and composed with the inclusion $R_1 \hookleftarrow \mathfrak{m}_1$ to yield a free resolution of $\Bbbk$ over R_1. The long exact sequence from $0 \leftarrow \Bbbk \leftarrow R_1 \leftarrow \mathfrak{m}_1 \leftarrow 0$ implies that $\operatorname{Ext}^{i+1}_{R_1}(\Bbbk, -) \cong \operatorname{Ext}^i_{R_1}(\mathfrak{m}_1, -)$ for $i \geq 1$. Now apply $\operatorname{Hom}(\mathfrak{m}_1, -)$ to the exact sequence $0 \to F \to F \to \mathfrak{m}_1 \to 0$. The first few terms are $0 \to \operatorname{Hom}(\mathfrak{m}_1, F) \to \operatorname{Hom}(\mathfrak{m}_1, F) \to R_1 \to \operatorname{Ext}^1(\mathfrak{m}_1, F)$. The image of $\operatorname{Hom}(\mathfrak{m}_1, F) \to R_1$ is $\mathfrak{m}_1$, so $\Bbbk \hookrightarrow \operatorname{Ext}^1(\mathfrak{m}_1, F) \cong \operatorname{Ext}^2(\Bbbk, F)$ is nonzero. □

Remark 3.3. Any ideal that is a countable (but not finite) union of a chain of principal ideals has projective dimension 1 [17, page 14]. But it is convenient to have an explicit free resolution of $\mathfrak{m}_1$ over R_1, and it is no extra work to resolve all orthant ideals.

Proposition 3.4. *Set $\mathfrak{m}_1 = \langle x_n^\varepsilon \mid \varepsilon > 0\rangle$ and $J = \langle x_1, \ldots, x_{n-1}\rangle \subseteq R$. Using $x = x_n$ for R_1, consider the R_1-module F in Lemma 3.2 with $n = 1$ as an R-module via $R \twoheadrightarrow R_1$, where $x_i^\varepsilon \mapsto 0$ for all $\varepsilon > 0$ and $i \leq n-1$. Then $\operatorname{Ext}^{n+1}_R(R/I, F) \neq 0$ when $I = J + \mathfrak{m}_1$.*

Proof. Let $\mathbb{F}_\bullet : 0 \leftarrow R_1 \leftarrow F \leftarrow F \leftarrow 0$ be the R_1-free resolution of $\Bbbk$ obtained by augmenting the resolution of $\mathfrak{m}_1$ in Lemma 3.1 with $n = 1$. Let $\mathbb{K}_\bullet = \mathbb{K}_\bullet^{R_{n-1}}(\boldsymbol{x}_{n-1})$ be the ordinary Koszul complex over R_{n-1} on the sequence $\boldsymbol{x}_{n-1} = x_1, \ldots, x_{n-1}$, which is a free resolution of $R_{n-1}/\boldsymbol{x}_{n-1}R_{n-1}$ over R_{n-1}. Then $\operatorname{Tot}(\mathbb{F}_\bullet \otimes_\Bbbk \mathbb{K}_\bullet)$ is a free resolution of R/I over R. On the other hand,

$$\begin{aligned}
\mathbb{F}_\bullet \otimes_\Bbbk \mathbb{K}_\bullet &\cong \mathbb{F}_\bullet \otimes_{R_1} R_1 \otimes_\Bbbk R_{n-1} \otimes_{R_{n-1}} \mathbb{K}_\bullet \\
&\cong \mathbb{F}_\bullet \otimes_{R_1} R \otimes_{R_{n-1}} \mathbb{K}_\bullet \\
&\cong \mathbb{F}_\bullet \otimes_{R_1} R \otimes_R R \otimes_{R_{n-1}} \mathbb{K}_\bullet \\
&= \mathbb{F}_\bullet^R \otimes_R \mathbb{K}_\bullet^R,
\end{aligned}$$

where $\mathbb{F}_\bullet^R = \mathbb{F}_\bullet \otimes_{R_1} R$ is an R-free resolution of $R/\mathfrak{m}_1 R$ and the ordinary Koszul complex $\mathbb{K}_\bullet^R = R \otimes_{R_{n-1}} \mathbb{K}_\bullet = \mathbb{K}_\bullet^R(\boldsymbol{x}_{n-1})$ of the sequence $\boldsymbol{x}_{n-1}$ in R is an R-free resolution of R/J.

Using $(-)^*$ to denote the free dual $\operatorname{Hom}_R(-, R)$, compute

$$\begin{aligned}
\operatorname{Hom}_R(\mathbb{F}_\bullet^R \otimes_R \mathbb{K}_\bullet^R, F) &\cong \operatorname{Hom}_R(\mathbb{F}_\bullet^R, \operatorname{Hom}_R(\mathbb{K}_\bullet^R, F)) \\
&\cong \operatorname{Hom}_R(\mathbb{F}_\bullet^R, (\mathbb{K}_\bullet^R)^* \otimes_R F) \\
&\cong \operatorname{Hom}_R(\mathbb{F}_\bullet^R, (\mathbb{K}_\bullet^R)^* \otimes_R R_1 \otimes_{R_1} F),
\end{aligned} \tag{3-1}$$

where the bottom isomorphism is because the R-action on F factors through R_1. The differentials of the complex $(\mathbb{K}_\bullet^R)^* \otimes_R R_1 \cong (\mathbb{K}_\bullet^R)^* \otimes_{R_{n-1}} \Bbbk$ all vanish, and this complex has cohomology $R_1^{\binom{n-1}{q}}$ in degree q.

Hence the total complex of Equation (3-1) has homology

$$\begin{aligned}\operatorname{Ext}^i_R(R/I, F) &\cong \bigoplus_{p+q=i} H_p \operatorname{Hom}_R(\mathbb{F}^R_\bullet, F^{\binom{n-1}{q}}) \\ &\cong \bigoplus_{p+q=i} H_p \operatorname{Hom}_{R_1}(\mathbb{F}_\bullet, F^{\binom{n-1}{q}}) \\ &\cong \bigoplus_{p+q=i} \operatorname{Ext}^p_{R_1}(\Bbbk, F^{\binom{n-1}{q}}),\end{aligned}$$

where the middle isomorphism is again because the R-action on F factors through R_1. Taking $p = 2$ and $q = n-1$ yields the nonvanishing by Lemma 3.2. □

Remark 3.5. The proof of Proposition 3.4 is essentially a Grothendieck spectral sequence for the derived functors of the composite $\operatorname{Hom}_{R_1}(\Bbbk, -) \circ \operatorname{Hom}_{R_{n-1}}(R_{n-1}/\boldsymbol{x}_{n-1}, -)$, but the elementary Koszul argument isn't more lengthy than verifying the hypotheses.

Theorem 3.6. *The n-variable real-exponent polynomial ring has global dimension $n+1$.*

Proof. Proposition 3.4 yields the lower bound $\operatorname{gl.dim} R \geq n+1$. For the opposite bound, given any R-module M, each module in the length n flat resolution from Theorem 2.9 has a free resolution of length at most 1 by Lemma 3.1. By the comparison theorem for projective resolutions [20, Theorem 2.2.6], the differentials of the flat resolution lift to chain maps of these free resolutions. The total complex of the resulting double complex has length at most $n+1$. □

Remark 3.7. As an $\mathbb{R}^n$-graded module, the quotient R/I in Proposition 3.4 is nonzero only in degrees from $\mathbb{R}^{n-1} \subseteq \mathbb{R}^n$. Hence R/I is ephemeral [4], meaning, more or less, that its set of nonzero degrees has measure 0. The projective dimension exceeding n is not due solely to this ephemerality. Indeed, multiplication by x_n^1 induces an inclusion of R/I into R/I' for $I' = \langle x_1, \dots, x_{n-1}\rangle + \langle x_n^\varepsilon \mid \varepsilon > 1\rangle$, which is supported on a unit cube in $\mathbb{R}^n_+$ that is neither open nor closed. Theorem 3.6 implies that $\operatorname{Ext}^{n+1}_R(R/I', N) \twoheadrightarrow \operatorname{Ext}^{n+1}_R(x_n R/I, N)$ is surjective for all modules N, so R/I' has projective dimension $n+1$. On the other hand, it could be the closed right endpoints [10] — that is, closed socle elements [13, Section 4.1] — that cause the problem. Thus it could be that sheaves in the conic topology ("γ-topology"; see [4; 8; 15]) have consistently lower projective dimensions.

4. Dense exponent sets

The results in Sections 2 and 3 extend to monoid algebras for positive cones of subgroups of $\mathbb{R}^n$ satisfying a mild density condition. Applications to noncommutative toric geometry should require restriction to subgroups of this sort.

Definition 4.1. Let $G \subseteq \mathbb{R}^n$ be a subgroup whose intersection with each coordinate ray ρ of $\mathbb{R}^n$ is dense. Write $G_+ = G \cap \mathbb{R}^n_+$ for the positive cone in G, set $\mathring{\rho} = \rho \cap \mathbb{R}^n_+ \smallsetminus \{\mathbf{0}\}$, and let $\mathring{G}_+ = \prod_\rho G \cap \mathring{\rho}_+$ be the set of points in G whose projections to all coordinate rays are strictly positive and still lie in G. Set

$R_G = \Bbbk[G_+]$, the monoid algebra of G_+ over $\Bbbk$. Let $R_G^{\boldsymbol{x}}$ and $R_G^{\boldsymbol{y}}$ be the copies of R_G embedded in $R_G^{\otimes 2}$ as $R_G \otimes 1$ and $1 \otimes R_G$. For $\boldsymbol{\varepsilon} \in \mathring{G}_+$ let $\boldsymbol{x}^{[\boldsymbol{\varepsilon}]} = x_1^{\varepsilon_1}, \ldots, x_n^{\varepsilon_n}$ be the corresponding sequence of elements in R_G.

(1) The *open Koszul complex* over R_G is the colimit $\mathring{\mathbb{K}}_\bullet^{\boldsymbol{x}} = \varinjlim_{\boldsymbol{\varepsilon} \in \mathring{G}_+} \mathbb{K}_\bullet(\boldsymbol{x}^{[\boldsymbol{\varepsilon}]})$.

(2) Fix an $R_G^{\boldsymbol{x}}$-module M. Write $M^{\boldsymbol{y}}$ for the corresponding $R_G^{\boldsymbol{y}}$-module, with the $\boldsymbol{x}$ variables renamed to $\boldsymbol{y}$. With notation for variables as in Lemma 2.6, the *open total Koszul complex* of M is the colimit $\mathring{\mathbb{K}}_\bullet^{\boldsymbol{x}-\boldsymbol{y}}(M) = \varinjlim_{\boldsymbol{\varepsilon} \in \mathring{G}_+} \mathbb{K}_\bullet(\boldsymbol{x}^{[\boldsymbol{\varepsilon}]} - \boldsymbol{y}^{[\boldsymbol{\varepsilon}]}) \otimes_{R^{\boldsymbol{y}}} M^{\boldsymbol{y}}$.

(3) Given a subset $\sigma \subseteq \{1, \ldots, n\}$, the *orthant ideal* $I_\sigma \subseteq R_G$ is generated by all monomials $\boldsymbol{x}^{\boldsymbol{\varepsilon}}$ for $\boldsymbol{\varepsilon} \in G_+$ such that $\varepsilon_i > 0$ for all $i \in \sigma$.

Example 4.2. Let G be generated by $\left[\begin{smallmatrix}2\\0\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}\pi\\0\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}0\\e\end{smallmatrix}\right]$ as a subgroup of $\mathbb{R}^2$, so G consists of the integer linear combinations of these four vectors. The intersection $G \cap \rho^y$ with the y-axis ρ^y arises from integer coefficients α, β, γ, and δ such that

$$\begin{bmatrix}0\\y\end{bmatrix} = \alpha\begin{bmatrix}2\\0\end{bmatrix} + \beta\begin{bmatrix}\pi\\0\end{bmatrix} + \gamma\begin{bmatrix}1\\1\end{bmatrix} + \delta\begin{bmatrix}0\\e\end{bmatrix}.$$

This occurs precisely when $2\alpha + \pi\beta + \gamma = 0$, and in that case $y = \gamma + \delta e$. Since π is irrational it is linearly independent from 1 over the integers, so $\beta = 0$ and hence $\gamma = -2\alpha$ is always an even integer. Since e is irrational, the only integer points in $G \cap \rho^y$ have even y-coordinate:

$$G \cap \rho^y = \left\langle \begin{bmatrix}0\\2\end{bmatrix}, \begin{bmatrix}0\\e\end{bmatrix} \right\rangle.$$

The point $\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right] \in G$ has strictly positive projection to ρ^y, but that projection lands outside of G. Hence $\mathring{G}_+ = G \cap \mathring{\rho}_+^x \times G \cap \mathring{\rho}_+^y$ is a proper subgroup of G, given the strictly positive point $\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right] \in G_+ \smallsetminus \mathring{G}_+$. Nonetheless, $\mathring{G}_+$ contains positive real multiples of $\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$ approaching the origin, which is all the colimit in the proof of Theorem 4.3 requires.

Theorem 4.3. *If a subgroup $G \subseteq \mathbb{R}^n$ is dense in every coordinate subspace of $\mathbb{R}^n$ as in Definition 4.1, then Theorem 2.9 holds verbatim with $R_G = \Bbbk[G \cap \mathbb{R}_+^n]$ in place of R. Consequently, the ring R_G has flat dimension n and global dimension $n + 1$.*

Proof. For $\sigma \subseteq \{1, \ldots, n\}$ and $\boldsymbol{\varepsilon} \in \mathbb{R}^n$ let $\boldsymbol{\varepsilon}_\sigma \in \mathbb{R}^n$ be the restriction of $\boldsymbol{\varepsilon}$ to σ, so $\boldsymbol{\varepsilon}_\sigma$ has entry 0 in the coordinate indexed by every $j \notin \sigma$. The 2^n summands of $\mathring{\mathbb{K}}_\bullet^{\boldsymbol{x}}$ are orthant ideals because $\mathbb{K}_i(\boldsymbol{x}^{[\boldsymbol{\varepsilon}]}) \cong \bigoplus_{|\sigma|=i} \langle \boldsymbol{x}^{\boldsymbol{\varepsilon}_\sigma} \rangle$ naturally with respect to the inclusions induced by the colimit defining $\mathring{\mathbb{K}}_\bullet^{\boldsymbol{x}}$. Each orthant ideal is flat because this colimit is filtered: given two vectors $\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2 \in \mathring{G}_+$, the coordinatewise minimum $\boldsymbol{\varepsilon}_1 \wedge \boldsymbol{\varepsilon}_2 \in \mathbb{R}_+^n$ lies in $\mathring{G}_+$ because its projection to each ray lies in G. Proposition 2.4 therefore generalizes to R_G by the exactness of colimits and the cokernel calculation $\Bbbk = R_G/\mathfrak{m}$ for the G-graded maximal ideal $\mathfrak{m} = \langle \boldsymbol{x}^{\boldsymbol{\varepsilon}} \mid \mathbf{0} \neq \boldsymbol{\varepsilon} \in G_+ \rangle$. Example 2.5 generalizes with no additional work. Lemma 2.6 generalizes by exactness of colimits and the cokernel calculation $R_G \cong R_G^{\otimes 2}/\langle \boldsymbol{x}^{[\boldsymbol{\varepsilon}]} - \boldsymbol{y}^{[\boldsymbol{\varepsilon}]} \mid \mathbf{0} \neq \boldsymbol{\varepsilon} \in G_+ \rangle$. The conclusion of Remark 2.8 generalizes, but the reason is direct calculation of $\mathring{\mathbb{K}}_\bullet(\boldsymbol{x}^{[\boldsymbol{\varepsilon}]} - \boldsymbol{y}^{[\boldsymbol{\varepsilon}]})$ as was done for $\mathring{\mathbb{K}}_i^{\boldsymbol{x}}$.

The original proof of Theorem 2.9 uses that tensor products commute with colimits, but the generalized proof avoids that argument by simply defining $\mathring{\mathbb{K}}_{\bullet}^{x-y}$ as the relevant colimit. The rest of the proof and the generalization of the flat dimension claim in Corollary 2.10 work mutatis mutandis, given the strengthened versions of the results they cite.

The orthant ideal resolution in Lemma 3.1 generalizes to R_G by the density hypothesis, including specifically the part about intersecting with coordinate subspaces. The Ext calculation in Lemma 3.2 works again by density of the exponent set of $\mathfrak{m}_1$ in $\mathbb{R}_+$. The statement and proof of Proposition 3.4 work mutatis mutandis for R_G in place of R as long as the power of x_i generating J lies in the intersection of G with the corresponding coordinate ray of $\mathbb{R}^n$. The proof of Theorem 3.6 then works verbatim, given the strengthened versions of the results it cites. □

References

[1] I. M. Aberbach and M. Hochster, "Finite Tor dimension and failure of coherence in absolute integral closures", *J. Pure Appl. Algebra* **122**:3 (1997), 171–184. MR Zbl

[2] M. Auslander and D. A. Buchsbaum, "Homological dimension in local rings", *Trans. Amer. Math. Soc.* **85** (1957), 390–405. MR Zbl

[3] H. Bass, "Finitistic dimension and a homological generalization of semi-primary rings", *Trans. Amer. Math. Soc.* **95** (1960), 466–488. MR Zbl

[4] N. Berkouk and F. Petit, "Ephemeral persistence modules and distance comparison", *Algebr. Geom. Topol.* **21**:1 (2021), 247–277. MR Zbl

[5] W. Bruns and J. Herzog, *Cohen–Macaulay rings*, Cambridge Stud. Adv. Math. **39**, Cambridge Univ. Press, 1993. MR Zbl

[6] P. Bubenik and N. Milićević, "Homological algebra for persistence modules", *Found. Comput. Math.* **21**:5 (2021), 1233–1278. MR Zbl

[7] J. Eagon, E. Miller, and E. Ordog, "Minimal resolutions of monomial ideals", preprint, 2019. arXiv 1906.08837

[8] M. Kashiwara and P. Schapira, "Persistent homology and microlocal sheaf theory", *J. Appl. Comput. Topol.* **2**:1-2 (2018), 83–113. MR Zbl

[9] L. Katzarkov, E. Lupercio, L. Meersseman, and A. Verjovsky, "Quantum (non-commutative) toric geometry: foundations", *Adv. Math.* **391** (2021), art. id. 107945. MR Zbl

[10] W. Kim, E. Miller, S. Moore, and M. Regan, "Functorial endpoints for multiparameter persistence", in progress.

[11] D. Lazard, "Sur les modules plats", *C. R. Acad. Sci. Paris* **258** (1964), 6313–6316. MR Zbl

[12] M. Lesnick, "The theory of the interleaving distance on multidimensional persistence modules", *Found. Comput. Math.* **15**:3 (2015), 613–650. MR Zbl

[13] E. Miller, "Essential graded algebra over polynomial rings with real exponents", preprint, 2020. arXiv 2008.03819

[14] E. Miller, "Homological algebra of modules over posets", preprint, 2020. arXiv 2008.00063

[15] E. Miller, "Stratifications of real vector spaces from constructible sheaves with conical microsupport", *J. Appl. Comput. Topol.* **7**:3 (2023), 473–489. MR

[16] B. L. Osofsky, "Global dimension of valuation rings", *Trans. Amer. Math. Soc.* **127** (1967), 136–149. MR Zbl

[17] B. L. Osofsky, "The subscript of $\aleph_n$, projective dimension, and the vanishing of $\varprojlim^{(n)}$", *Bull. Amer. Math. Soc.* **80** (1974), 8–26. MR Zbl

[18] S. Y. Oudot, *Persistence theory: from quiver representations to data analysis*, Math. Surv. Monogr. **209**, Amer. Math. Soc., Providence, RI, 2015. MR Zbl

[19] J.-P. Serre, "Sur la dimension homologique des anneaux et des modules noethériens", pp. 175–189 in *Proceedings of the International Symposium on Algebraic Number Theory* (Tokyo/Nikko, 1955), Sci. Council Japan, Tokyo, 1956. MR Zbl

[20] C. A. Weibel, *An introduction to homological algebra*, Cambridge Stud. Adv. Math. **38**, Cambridge Univ. Press, 1994. MR Zbl

Communicated by Antoine Chambert-Loir
Received 2021-09-25 Revised 2022-05-16 Accepted 2022-10-17

geistn@bc.edu Mathematics Department, Duke University, Durham, NC, United States

ezra@math.duke.edu Mathematics Department, Duke University, Durham, NC, United States

ALGEBRA AND NUMBER THEORY 17:10 (2023)
https://doi.org/10.2140/ant.2023.17.1789

Differences between perfect powers: prime power gaps

Michael A. Bennett and Samir Siksek

We develop machinery to explicitly determine, in many instances, when the difference $x^2 - y^n$ is divisible only by powers of a given fixed prime. This combines a wide variety of techniques from Diophantine approximation (bounds for linear forms in logarithms, both archimedean and nonarchimedean, lattice basis reduction, methods for solving Thue–Mahler and S-unit equations, and the primitive divisor theorem of Bilu, Hanrot and Voutier) and classical algebraic number theory, with results derived from the modularity of Galois representations attached to Frey–Hellegoarch elliptic curves. By way of example, we completely solve the equation

$$x^2 + q^\alpha = y^n,$$

where $2 \le q < 100$ is prime, and x, y, α and n are integers with $n \ge 3$ and $\gcd(x, y) = 1$.

Bennett is supported by NSERC. Siksek is supported by an EPSRC Grant EP/S031537/1 “Moduli of elliptic curves and classical Diophantine problems”.
MSC2020: primary 11D61; secondary 11D41, 11F80.
Keywords: exponential equation, Lucas sequence, shifted power, Galois representation, Frey curve, modularity, level lowering, Baker’s bounds, Hilbert modular forms, Thue–Mahler equations.

1. Introduction

The *Lebesgue–Nagell* equation

$$x^2 + D = y^n \tag{1}$$

has a very extensive literature, motivated, at least in part, by attempts to extend Mihăilescu's theorem [2004] (Catalan's conjecture) to larger gaps in the sequence of perfect powers, in an attempt to attack Pillai's conjecture [1936]. In (1), we will suppose that x and y are coprime nonzero integers, and that the prime divisors of D belong to a fixed, finite set of primes S. Under these assumptions, bounds for linear forms in logarithms, p-adic and complex, imply that the set of integer solutions (x, y, n) to (1), with $|y| > 1$ and $n \geq 3$, is finite and effectively determinable. If, in addition, we suppose that D is positive and that y is odd, then these solutions may be explicitly determined, provided $|S|$ is not too large, through appeal to the primitive divisor theorem of Bilu, Hanrot and Voutier [Bilu et al. 2001], in conjunction with techniques from Diophantine approximation.

If either $D > 0$ and y is even, or if $D < 0$, the primitive divisor theorem cannot be applied to solve (1) and we must work rather harder, appealing to either bounds for linear forms in logarithms or to results based upon the modularity of Galois representations associated to certain Frey–Hellegouarch elliptic curves. In a companion paper [Bennett and Siksek 2023], we develop machinery for handling (1) in the first difficult case where $D > 0$ and y is even. Though the techniques we discuss in the present paper are more widely applicable, we will, for simplicity, restrict attention to the case where D in (1) is divisible by a single prime q, whilst treating both the cases $D < 0$ and $D > 0$. That is, we will concern ourselves primarily with the equation

$$x^2 + (-1)^\delta q^\alpha = y^n, \quad q \nmid x, \tag{2}$$

where $\delta \in \{0, 1\}$ and α is a nonnegative integer. In the case $\delta = 0$, our main result is the following.

Theorem 1. *If x, y, q, α and n are positive integers with q prime, $2 \leq q < 100$, $q \nmid x$, $n \geq 3$ and*

$$x^2 + q^\alpha = y^n, \tag{3}$$

then (q, α, y, n) is one of

$$(2,1,3,3),\ (2,2,5,3),\ (2,5,3,4),\ (3,5,7,3),\ (3,4,13,3),\ (7,1,2,3),\ (7,3,8,3),\ (7,1,32,3),$$
$$(7,2,65,3),\ (7,1,2,4),\ (7,2,5,4),\ (7,1,2,5),\ (7,1,8,5),\ (7,1,2,7),\ (7,3,2,9),\ (7,1,2,15),$$
$$(11,1,3,3),\ (11,1,15,3),\ (11,2,5,3),\ (11,3,443,3),\ (13,1,17,3),\ (17,1,3,4),\ (19,1,7,3),$$
$$(19,1,55,5),\ (23,1,3,3),\ (23,3,71,3),\ (23,3,78,4),\ (23,1,2,5),\ (23,1,2,11),\ (29,2,5,7),$$
$$(31,1,4,4),\ (31,1,2,5),\ (31,1,2,8),\ (41,2,29,4),\ (41,2,5,5),\ (47,1,6,3),\ (47,1,12,3),$$
$$(47,1,63,3),\ (47,2,17,3),\ (47,3,74,3),\ (47,1,3,5),\ (47,1,2,7),\ (53,1,9,3),\ (53,1,29,3),$$
$$(53,1,3,6),\ (61,1,5,3),\ (67,1,23,3),\ (71,1,8,3),\ (71,1,6,4),\ (71,1,3,7),\ (71,1,2,9),$$
$$(79,1,20,3),\ (79,1,2,7),\ (83,1,27,3),\ (83,1,3,9),\ (89,1,5,3),\ (97,2,12545,3),\ (97,1,7,4).$$

One might note that the restriction $q \nmid x$ can be removed, with a modicum of effort, at least for certain values of q. The cases where primitive divisor arguments are inapplicable correspond to $q \in \{7, 23, 31, 47, 71, 79\}$ and y even (and this is where the great majority of work lies in proving Theorem 1). If $q = 7$, Theorem 1 generalizes recent work of Koutsianas [2020], who established a similar result under certain conditions upon α and q, and, in particular, showed that (3) has no solutions with $q = 7$ and prime $n \equiv 13, 23 \pmod{24}$. We note that the solution(s) with $q = 83$ were omitted in the statement of Theorem 1 of Berczes and Pink [2012].

Our results for (2) with $\delta = 1$ are less complete, at least when α is odd.

Theorem 2. *Suppose that*

$$q \in \{7, 11, 13, 19, 23, 29, 31, 43, 47, 53, 59, 61, 67, 71, 79, 83\}. \tag{4}$$

If x and n are positive integers, $q \nmid x$, $n \geq 3$ and

$$x^2 - q^{2k+1} = y^n, \tag{5}$$

where y and k are integers, then (q, k, y, n) is one of

$$(7, 2, 393, 3), \quad (7, 1, -3, 5), \quad (11, 1, 37, 3) \quad (11, 0, 5, 5), \quad (11, 1, 37, 3), \quad (13, 0, 3, 5),$$
$$(19, 0, 5, 3), \quad (19, 2, -127, 3), \quad (19, 0, -3, 4), \quad (19, 0, 3, 4), \quad (23, 1, 1177, 3),$$
$$(31, 0, -3, 3), \quad (43, 0, -3, 3), \quad (71, 0, 5, 3), \quad (71, 1, -23, 3), \quad (79, 0, 45, 3).$$

To the best of our knowledge, these are the first examples of primes q for which (5) has been completely solved (though the cases with $k = 0$ are treated in the thesis of Barros [2010]). There are eight other primes in the range $3 \leq q < 100$ for which we are unable to give a similarly satisfactory statement. For four of these, namely $q = 3, 5, 17$ and 37, the equation (5) has a solution with $y = \pm 1$. For such primes we are unaware of any results that would enable us to completely treat fixed exponents n of moderate size; this difficulty is well known for the $D = -2$ case of (1). One should note that it is relatively easy to solve (5) for $q \in \{3, 5, 37\}$, under the additional assumption that y is even (and somewhat harder if $q = 17$ and y is even). For the other four primes, namely $q = 41, 73, 89$ and 97, we give a method which appears theoretically capable of success, but is alas prohibitively expensive, computationally speaking. We content ourselves by proving the following modest result for these primes.

Theorem 3. *Let $q \in \{41, 73, 89, 97\}$. The only solutions to (5) with $q \nmid x$ and $3 \leq n \leq 1000$ are with (q, k, y, n) equal to one of*

$$(41, 0, -2, 5), \quad (41, 0, 2, 3), \quad (41, 0, 2, 7), \quad (41, 1, 10, 5), \quad (73, 0, -6, 4),$$
$$(73, 0, -4, 3), \quad (73, 0, 2, 3), \quad (73, 0, 3, 3), \quad (73, 0, 6, 3), \quad (73, 0, 6, 4), \quad (73, 0, 72, 3),$$
$$(89, 0, -4, 3), \quad (89, 0, -2, 3), \quad (89, 0, 2, 5), \quad (89, 0, 2, 13), \quad (97, 0, 2, 7).$$

There are no solutions to (5) with $n > 1000$, $q \nmid x$ and either $q = 73$ and $y \equiv 0 \pmod 2$, or with $q = 97$ and $y \equiv 1 \pmod 2$.

The additional assumption that the exponent of our prime q is even simplifies matters considerably. In the case of (3), Berczes and Pink [2008] deduced Theorem 1 for even values of α (whence primitive divisor technology works efficiently). For completeness, we extend this to $q < 1000$; the results for $q < 100$ are, of course, just a special case of Theorem 1.

Theorem 4. *If x, y, q, k and n are positive integers with q prime, $2 \le q < 1000$, $q \nmid x$, $n \ge 3$ and*

$$x^2 + q^{2k} = y^n, \tag{6}$$

then (q, k, y, n) is one of

$$(2, 1, 5, 3), \quad (3, 2, 13, 3), \quad (7, 1, 65, 3), \quad (7, 1, 5, 4), \quad (11, 1, 5, 3), \quad (29, 1, 5, 7),$$
$$(41, 1, 29, 4), \quad (41, 1, 5, 5), \quad (47, 1, 17, 3), \quad (97, 1, 12545, 3), \quad (107, 1, 37, 3), \quad (191, 1, 65, 3),$$
$$(239, 1, 169, 4), \quad (239, 1, 13, 8), \quad (431, 1, 145, 3), \quad (587, 1, 197, 3), \quad (971, 1, 325, 3).$$

More interesting for us is the case where the difference $x^2 - y^n$ is positive (so that primitive divisor arguments are inapplicable and there are no prior results available in the literature). We prove the following.

Theorem 5. *If x, q, k and n are positive integers with q prime, $2 \le q < 1000$, $q \nmid x$, $n \ge 3$ and*

$$x^2 - q^{2k} = y^n, \tag{7}$$

where y is an integer, then (q, k, y, n) is one of

$$(3, 1, -2, 3), \ (3, 1, 40, 3), \ (3, 1, \pm 2, 4), \ (3, 2, -2, 5), \ (5, 2, 6, 3), \ (7, 2, 15, 3), \ (7, 1, 2, 5), \ (11, 1, 12, 3),$$
$$(11, 2, 3, 5), \ (13, 1, 3, 3), \ (13, 1, 12, 5), \ (17, 1, -4, 3), \ (17, 1, \pm 12, 4), \ (17, 2, 42, 3), \ (29, 1, -6, 3),$$
$$(31, 1, 2, 7), \ (43, 1, -12, 3), \ (43, 1, 126, 3), \ (43, 4, 96222, 3), \ (47, 1, 6300, 3), \ (53, 1, 6, 3),$$
$$(71, 1, 30, 3), \ (71, 2, -136, 3), \ (89, 1, 84, 3), \ (97, 2, 3135, 3), \ (101, 1, 24, 3), \ (109, 1, 20, 3),$$
$$(109, 1, 35, 3), \ (109, 1, 570, 3), \ (127, 1, -10, 3), \ (127, 1, 8, 3), \ (127, 1, 198, 3), \ (127, 1, 2, 9),$$
$$(179, 1, -30, 3), \ (193, 1, 63, 3), \ (197, 1, 260, 3), \ (223, 1, 30, 3), \ (251, 1, -10, 3), \ (251, 1, -6, 5),$$
$$(257, 1, -4, 5), \ (263, 1, 2418, 3), \ (277, 1, -30, 3), \ (307, 1, 60, 3), \ (307, 1, 176, 3), \ (307, 2, 2262, 3),$$
$$(359, 1, -28, 3), \ (383, 2, 25800, 3), \ (397, 1, -42, 3), \ (431, 1, 12, 3), \ (433, 1, -12, 3), \ (433, 1, 143, 3),$$
$$(433, 2, 26462, 3), \ (479, 1, 90, 3), \ (499, 1, -12, 5), \ (503, 1, 828, 3), \ (557, 1, -60, 3), \ (577, 1, \pm 408, 4),$$
$$(593, 1, -70, 3), \ (601, 1, 72, 3), \ (659, 1, 42, 3), \ (683, 1, 193346, 3), \ (701, 1, 4452, 3), \ (727, 1, 18, 3),$$
$$(739, 1, 234, 3), (769, 1, 255, 3), (811, 1, -70, 3), (857, 1, -72, 3), \ (997, 1, 48, 3).$$

We note that, with sufficient computational power, there is no obstruction to extending the results of Theorems 4 and 5 to larger prime values q. Without fundamentally new ideas, it is not clear that the same may be said of, for example, Theorem 1. In this case, the bounds we obtain upon the exponent n via linear forms in logarithms, even for relatively small q, leave us with a computation which, while finite, is barely tractable.

Equation (8) has been completely resolved [Ivorra 2003; Siksek 2003] for $q = 2$, except for the case $(\alpha, \delta) = (1, 1)$ which corresponds to $D = -2$ in (1). The solutions for $q = 2$ in our theorems are included for completeness. For the remainder of the paper, we suppose that q is an odd prime. In particular, we are concerned with the equation

$$x^2 + (-1)^\delta q^\alpha = y^n, \quad \gcd(x, y) = 1, \ \alpha > 0, \tag{8}$$

where q is a fixed odd prime, $n \geq 3$, and $\delta \in \{0, 1\}$.

Our proofs will use a broad combination of techniques, which include

- lower bounds for linear forms in complex and p-adic logarithms which yield bounds for the exponent n in (8);
- Frey–Hellegouarch curves and their Galois representations which provide a wealth of local information regarding solutions to (8);
- the celebrated primitive divisor theorem of Bilu, Hanrot and Voutier, that can be used to treat most cases of (8) when y is odd and $\delta = 0$;
- elementary descent arguments that reduce (8) for a fixed exponent n to Thue–Mahler equations, which are possible to resolve thanks to the Thue–Mahler solver associated to [Gherga and Siksek 2022].

The outline of this paper is as follows. In Section 2, we solve the equation $x^2 + (-1)^\delta q^\alpha = y^n$ for $n \in \{3, 4\}$ and $3 \leq q < 100$ by reducing the problem to the determination of S-integral points on elliptic curves. In Section 3, we solve the equation $x^2 - q^{2k} = y^n$, for q in the range $3 \leq q < 1000$, with y odd, using an elementary sieving argument; this completes the proof of Theorem 5 in the case y is odd. Next, Section 4 provides a short overview of Lucas sequences, their ranks of apparition, and the primitive divisor theorem of Bilu, Hanrot and Voutier. We make use of this machinery in Section 5 to solve the equation $x^2 + q^{2k} = y^n$ for q in the range $3 \leq q < 1000$, thereby proving Theorem 4. Section 6 reduces the equation $x^2 - q^{2k} = y^n$, for even values of y, to Thue–Mahler equations of the form

$$y_1^n - 2^{n-2} y_2^n = q^k. \tag{9}$$

In Section 7, we give a brief outline of the modular approach to Diophantine equations. Section 8 applies this modular approach, particularly the (n, n, n) Frey–Hellegouarch elliptic curves of Kraus [1997], to (9); this allows us to deduce that there are no solutions for $3 \leq q < 1000$ except for possibly $q \in \{31, 127, 257\}$, where the mod n representation of the Frey–Hellegouarch curve arises from that of an elliptic curve with full 2-torsion and conductor $2q$. Before we can complete the proof of Theorem 5, we need an upper bound for the exponent n. We give a sharpening of Bugeaud's bound [1997] for the equation $x^2 - q^{2k} = y^n$, which uses (9) and the theory of linear forms in real and p-adic logarithms. In Section 10, we complete the proof of Theorem 5; our approach makes use of a sieving technique that builds on the information obtained from the modular approach in Section 8 and the upper bound for n established in Section 9. The remainder of the paper is concerned with (8) where $\alpha = 2k + 1$, and for $3 \leq q < 100$. In Section 11, we solve $x^2+q^{2k+1}=y^n$ with y odd with the help of the primitive divisor theorem, and in Section 12 we solve $x^2-q^{2k+1}=y^5$ by reducing to Thue–Mahler equations.

It remains, then, to handle the equations $x^2-q^{2k+1}=y^n$ and $x^2+q^{2k+1}=y^n$ where, in the latter case, we may additionally assume that y is even. In Section 13, we study the more general equation

$$y^n+q^\alpha z^n=x^2, \quad \gcd(x,y)=1, \tag{10}$$

where q is prime, using Galois representations of Frey–Hellegouarch curves. Our approach builds on previous work of Bennett and Skinner [2004], and also on the work of Ivorra and Kraus [2006]. We then restrict ourselves in Section 14 to the case $z=\pm 1$ and α odd in (10). In this section, we develop a variety of sieves based upon local information coming from the Frey–Hellegouarch curves that allows us, in many situations, to eliminate values of q from consideration completely and, in the more difficult cases, to solve (8) for a fixed pair (q,n). In particular, we employ this strategy to complete the proofs of Theorems 2 and 3. Finally, in Section 15, we return to bounds for linear forms in p-adic and complex logarithms to derive explicit upper bounds upon n in (8), and then report upon a (somewhat substantial) computation to use the arguments of Section 14 to solve (8) for all remaining pairs (q,n) required to finish the proof of Theorem 1.

2. Reduction to S-integral points on elliptic curves for $n \in \{3, 4\}$

In the following sections, it will be of value to us to assume that the exponent n in (8) is not too small. This is primarily to ensure that the Frey–Hellegouarch curve we attach to a putative solution has a corresponding mod n Galois representation that is irreducible. For suitably large prime values of n (typically, $n\geq 7$), the desired irreducibility follows from Mazur's isogeny theorem. In Section 4, such an assumption allows us to (mostly) ignore so-called *defective* Lucas sequences.

In this section, we treat separately the cases $n=3$ and $n=4$ for $q<100$, where the problem of solving (8) reduces immediately to one of determining S-integral points on specific models of genus one curves; here $S=\{q\}$. This approach falters for many values of q in the range $100<q<1000$ as we are often unable to compute the Mordell–Weil groups of the relevant elliptic curves. Thus for the proofs of Theorems 4 and 5 for exponents $n=3$, $n=4$, where we treat values of q less than 1000, we shall employ different techniques including sieving arguments and reduction to Thue–Mahler equations.

The case n = 3. Supposing that we have a coprime solution to (8) with $n=3$, we can write $\alpha=6b+c$, where $0\leq c\leq 5$. Taking $X=y/q^{2b}$ and $Y=x/q^{3b}$, it follows that (X,Y) is an S-integral point on the elliptic curve

$$Y^2=X^3+(-1)^{\delta+1}q^c, \tag{11}$$

where $S=\{q\}$. Here, for a particular choice of $\delta\in\{0,1\}$ and prime q we may use the standard method for computing S-integral points on elliptic curves based on lower bounds for linear forms in elliptic logarithms (e.g., [Pethő et al. 1999]). We made use of the built-in `Magma` [Bosma et al. 1997] implementation of this

q	δ	α	x	y
2	0	1	5	3
2	0	2	11	5
2	1	1	1	−1
2	1	7	71	17
2	1	9	13	−7
2	1	3	3	1
3	0	4	46	13
3	0	5	10	7
3	1	1	2	1
3	1	2	1	−2
3	1	2	253	40
5	1	1	2	−1
5	1	4	29	6
7	0	1	1	2
7	0	1	181	32
7	0	2	524	65
7	0	3	13	8
7	1	4	76	15
7	1	5	7792	393
11	0	1	4	3
11	0	1	58	15
11	0	2	2	5
11	0	3	9324	443
11	1	2	43	12
11	1	3	228	37
13	0	1	70	17
13	1	2	14	3
17	1	1	3	−2
17	1	1	4	−1
17	1	1	5	2
17	1	1	9	4
17	1	1	23	8
17	1	1	282	43
17	1	1	375	52
17	1	7	21063928	76271
17	1	1	378661	5234
17	1	2	15	−4
17	1	4	397	42
19	0	1	18	7
19	1	1	12	5
19	1	5	654	−127
23	0	1	2	3
23	0	3	588	71
23	1	3	40380	1177
29	1	2	25	−6
31	1	1	2	−3
37	1	1	6	−1
37	1	1	8	3
37	1	1	3788	243
37	1	3	228	11
41	1	1	7	2
43	1	1	4	−3
43	1	2	11	−12
43	1	8	30042907	96222
43	1	2	1415	126
47	0	1	13	6
47	0	1	41	12
47	0	1	500	63
47	0	2	52	17
47	0	3	549	74
47	1	2	500047	6300
53	0	1	26	9
53	0	1	156	29
53	1	2	55	6
61	0	1	8	5
67	0	1	110	23
71	0	1	21	8
71	1	1	14	5
71	1	2	179	30
71	1	3	588	−23
71	1	4	4785	−136
73	1	1	3	−4
73	1	1	9	2
73	1	1	10	3
73	1	1	17	6
73	1	1	611	72
73	1	1	6717	356
79	0	1	89	20
79	1	1	302	45
83	0	1	140	27
89	0	1	6	5
89	1	1	5	−4
89	1	1	9	−2
89	1	1	33	10
89	1	1	408	55
89	1	2	775	84
97	0	2	1405096	12545
97	1	1	77	18
97	1	4	175784	3135

Table 1. Solutions to the equation $x^2 + (-1)^\delta q^\alpha = y^3$ for primes $2 \le q < 100$, $\delta \in \{0, 1\}$ and x, y, α integers satisfying $\alpha > 0$, $x > 0$, $y \neq 0$, and $\gcd(x, y) = 1$.

method to compute these S-integral points on (11) for $\delta \in \{0, 1\}$ and $2 \le q < 100$. We obtained a total of 83 solutions to (8) for these values of q with $\alpha > 0$, $x > 0$, $y \neq 0$ and $\gcd(x, y) = 1$. These are given in Table 1.

The case $n = 4$. Next we consider the case $n = 4$ separately. Write $\alpha = 4b + c$ where $0 \le c \le 3$. Let $X = (y/q^b)^2$, $Y = xy/q^{3b}$. Then (X, Y) is an S-integral point on the elliptic curve

$$Y^2 = X(X^2 + (-1)^{\delta+1} q^c), \tag{12}$$

q	δ	α	x	y
2	0	5	7	3
2	1	3	3	1
3	1	1	2	1
3	1	5	122	11
3	1	2	5	2

q	δ	α	x	y
7	0	1	3	2
7	0	2	24	5
17	0	1	8	3
17	1	2	145	12
19	1	1	10	3

q	δ	α	x	y
23	0	3	6083	78
31	0	1	15	4
41	0	2	840	29
71	0	1	35	6
73	1	1	37	6
97	0	1	48	7

Table 2. Solutions to the equation $x^2 + (-1)^\delta q^\alpha = y^4$ for primes $2 \le q < 100$, $\delta \in \{0, 1\}$ and x, y, α integers satisfying $\alpha > 0$, $x > 0$, $y > 0$, and $\gcd(x, y) = 1$.

where $S = \{q\}$. We again appealed to the built-in Magma [Bosma et al. 1997] implementation of this method to compute these S-integral points on (12) for $\delta \in \{0, 1\}$ and $2 \le q < 100$. We obtained a total of 16 solutions to (8) for these values of q with $\alpha > 0$, $x > 0$, $y > 0$ and $\gcd(x, y) = 1$. These are given in Table 2.

3. An elementary approach to $x^2 - q^{2k} = y^n$ with y odd

In this section, we apply an elementary factorization argument to prove Theorem 5 for y odd. In other words, we consider the equation

$$x^2 - q^{2k} = y^n, \quad x, k, n \text{ positive integers, } n \ge 3,\ \gcd(x, y) = 1,\ y \text{ an odd integer.} \tag{13}$$

Here $q \ge 3$ is a prime. From this, we immediately see that

$$x + q^k = y_1^n \quad \text{and} \quad x - q^k = y_2^n, \tag{14}$$

with $y = y_1 y_2$, so that we have

$$y_1^n - y_2^n = 2q^k. \tag{15}$$

If $2 \mid n$, then $y_1^n \equiv y_2^n \equiv 1 \pmod 4$, a contradiction. We may suppose henceforth, without loss of generality, that n is an odd prime. Observe that

$$(y_1 - y_2)(y_1^{n-1} + y_1^{n-2} y_2 + \cdots + y_2^{n-1}) = y_1^n - y_2^n = 2q^k. \tag{16}$$

Clearly $y_1 > y_2$ and, as they are both odd, $y_1 - y_2 \ge 2$ and $2 \mid (y_1 - y_2)$. Write

$$d = \gcd(y_1 - y_2, y_1^{n-1} + y_1^{n-2} y_2 + \cdots + y_2^{n-1})$$

so that $y_2 \equiv y_1 \pmod d$ and

$$0 \equiv y_1^{n-1} + y_1^{n-2} y_2 + \cdots + y_2^{n-1} \equiv n y_1^{n-1} \pmod d.$$

Similarly, we have $n y_2^{n-1} \equiv 0 \pmod d$ and so $d \in \{1, n\}$.

We first deal with the case $d = n$, whereby, from (16), $q = n$. Let $r = \mathrm{ord}_n(y_1 - y_2) \geq 1$ and write $y_1 = y_2 + n^r\kappa$ where $n \nmid \kappa$. Then

$$\mathrm{ord}_n(y_1^{n-1} + y_1^{n-2}y_2 + \cdots + y_2^{n-1}) = \mathrm{ord}_n\left(\frac{(y_2 + n^r\kappa)^n - y_2^n}{n^r\kappa}\right) = 1.$$

Hence

$$y_1 - y_2 = 2n^{k-1} \quad \text{and} \quad y_1^{n-1} + y_1^{n-2}y_2 + \cdots + y_2^{n-1} = n, \tag{17}$$

and so

$$n = \prod_{i=1}^{n-1} |y_1 - \zeta_n^i y_2| \geq \big||y_1| - |y_2|\big|^{n-1}.$$

Recall that y_1 and y_2 are both odd. If $y_2 \neq \pm y_1$, then the right-hand side of this last inequality is at least 2^{n-1}, which is impossible. Thus $y_2 = \pm y_1$, so that, from (17), $y_1^{n-1} \mid n$. It follows that $|y_1| = |y_2| = 1$, contradicting (14).

Thus $d = 1$, whence

$$y_1 - y_2 = 2 \quad \text{and} \quad y_1^{n-1} + y_1^{n-2}y_2 + \cdots + y_2^{n-1} = q^k. \tag{18}$$

Since the polynomial $X^{n-1} + X^{n-2} + \cdots + 1$ has a root modulo q, the Dedekind–Kummer theorem tells us that q splits in $\mathbb{Z}[\zeta_n]$ and so $q \equiv 1 \pmod{n}$. We therefore have the following.

Proposition 3.1. *If x, y, q, k and n are positive integers satisfying (13) with n and q prime, then $n \mid (q-1)$ and there exists an odd positive integer X such that $y = X(X+2)$ and*

$$(X+2)^n - X^n = 2q^k. \tag{19}$$

This last result makes it an extremely straightforward matter to solve (7) in the case y is odd.

Lemma 3.2. *The only solutions to (13) with $3 \leq q < 1000$ prime correspond to the identities*

$$76^2 - 7^4 = 15^3, \quad 122^2 - 11^4 = 3^5. \quad 14^2 - 13^2 = 3^3, \quad 175784^2 - 97^4 = 3135^3,$$
$$234^2 - 109^2 = 35^3, \quad 536^2 - 193^2 = 63^3, \quad 1764^2 - 433^2 = 143^3, \quad 4144^2 - 769^2 = 255^3.$$

Proof. Suppose first that $n = 3$, where (19) becomes

$$3(X+1)^2 + 1 = q^k. \tag{20}$$

From [Cohn 1997; 2003], we know that the equation $3u^2 + 1 = y^m$ has no solutions with $m \geq 3$. We conclude that $k = 1$ or 2. Solving (20) with $k = 1$ or 2 and $3 \leq q < 1000$ leads to the seven solutions with $n = 3$.

We now suppose that $n \geq 5$ is prime. By a theorem of Bennett and Skinner [2004, Theorem 2], the only solutions to the equation $X^n + Y^n = 2Z^2$ with $n \geq 5$ prime and $\gcd(X, Y) = 1$ are with either $|XY| = 1$ or $(n, X, Y, Z) = (5, 3, -1, \pm 11)$. We note that if k is even then (19) can be rewritten as $(X+2)^n - X^n = 2(q^{k/2})^2$, and therefore $n = 5$, $X = 1$ and $q^{k/2} = 11$. This yields the solution $122^2 - 11^4 = 3^5$.

We may therefore suppose that k is odd. Recalling that $n \mid (q-1)$ leaves us with precisely 191 pairs (q, n) to consider, ranging from $(11, 5)$ to $(997, 83)$. Fix one of these pairs (q, n) and let $\ell \nmid nq$ be an odd prime. Let $\mathcal{Z}_\ell$ be the set of $\beta \in \mathbb{Z}/(\ell-1)\mathbb{Z}$ such that β is odd and the polynomial

$$(X+2)^n - X^n - 2q^\beta$$

has a root in $\mathbb{F}_\ell$. We note that the value of q^k modulo ℓ depends only on the residue class of k modulo $\ell - 1$. From (19), we deduce that $(k \bmod \ell) \in \mathcal{Z}_\ell$. Now let $\ell_1, \ell_2, \ldots, \ell_m$ be a collection of odd primes with $\ell_i \nmid nq$ for $1 \le i \le m$. Let

$$M = \operatorname{lcm}(\ell_1 - 1, \ell_2 - 1, \ldots, \ell_m - 1) \tag{21}$$

and set

$$\mathcal{Z}_{\ell_1,\ldots,\ell_m} = \{\beta \in \mathbb{Z}/M\mathbb{Z} : (\beta \bmod \ell_i) \in \mathcal{Z}_{\ell_i} \text{ for } i = 1, \ldots, m\}. \tag{22}$$

It is clear that $(k \bmod M) \in \mathcal{Z}_{\ell_1,\ldots,\ell_m}$. We wrote a short `Magma` script which, for each pair (q, n), computed $\mathcal{Z}_{\ell_1,\ldots,\ell_m}$ where $\ell_1, \ell_2, \ldots, \ell_m$ are the odd primes ≤ 101 distinct from n and q. In all 191 cases we found that $\mathcal{Z}_{\ell_1,\ldots,\ell_m} = \varnothing$, completing the desired contradiction. □

4. Lucas sequences and the primitive divisor theorem

The primitive divisor theorem of Bilu, Hanrot and Voutier [Bilu et al. 2001] shall be our main tool for treating (8) when $\delta = 0$ and y is odd. In this section, we state this result and a related theorem of Carmichael that shall be useful later. A pair of algebraic integers (γ, δ) is called a *Lucas pair* if $\gamma + \delta$ and $\gamma\delta$ are nonzero coprime rational integers, and γ/δ is not a root of unity. We say that two Lucas pairs (γ_1, δ_1) and (γ_2, δ_2) are *equivalent* if $\gamma_1/\gamma_2 = \pm 1$ and $\delta_1/\delta_2 = \pm 1$. Given a Lucas pair (γ, δ) we define the corresponding *Lucas sequence* by

$$L_m = \frac{\gamma^m - \delta^m}{\gamma - \delta}, \qquad m = 0, 1, 2, \ldots .$$

A prime ℓ is said to be a *primitive divisor* of the m-th term if ℓ divides L_m but ℓ does not divide $(\gamma - \delta)^2 \cdot L_1 L_2 \cdots L_{m-1}$.

Theorem 6 [Bilu et al. 2001]. *Let (γ, δ) be a Lucas pair and write $\{L_m\}$ for the corresponding Lucas sequence.*

(i) *If $m \ge 30$, then L_m has a primitive divisor.*

(ii) *If $m \ge 11$ is prime, then L_m has a primitive divisor.*

(iii) *L_7 has a primitive divisor unless (γ, δ) is equivalent to $((a - \sqrt{b})/2, (a + \sqrt{b})/2)$ where*

$$(a, b) \in \{(1, -7), (1, -19)\}. \tag{23}$$

(iv) *L_5 has a primitive divisor unless (γ, δ) is equivalent to $((a - \sqrt{b})/2, (a + \sqrt{b})/2)$ where*

$$(a, b) \in \{(1, 5), (1, -7), (2, -40), (1, -11), (1, -15), (12, -76), (12, -1364)\}. \tag{24}$$

Let ℓ be a prime. We define the *rank of apparition of* ℓ in the Lucas sequence $\{L_m\}$ to be the smallest positive integer m such that $\ell \mid L_m$. We denote the rank of apparition of ℓ by m_ℓ. The following theorem will be useful for us; a concise proof may be found in [Bennett et al. 2022, Theorem 8].

Theorem 7 [Carmichael 1913]. *Let (γ, δ) be a Lucas pair, and $\{L_m\}$ the corresponding Lucas sequence. Let ℓ be a prime.*

(i) *If $\ell \mid \gamma\delta$ then $\ell \nmid L_m$ for all positive integers m.*

(ii) *Suppose $\ell \nmid \gamma\delta$. Write $D = (\gamma - \delta)^2 \in \mathbb{Z}$.*

  (a) *If $\ell \neq 2$ and $\ell \mid D$, then $m_\ell = \ell$.*
  (b) *If $\ell \neq 2$ and $\left(\frac{D}{\ell}\right) = 1$, then $m_\ell \mid (\ell - 1)$.*
  (c) *If $\ell \neq 2$ and $\left(\frac{D}{\ell}\right) = -1$, then $m_\ell \mid (\ell + 1)$.*
  (d) *If $\ell = 2$, then $m_\ell = 2$ or 3.*

(iii) *If $\ell \nmid \gamma\delta$ then*

$$\ell \mid L_m \iff m_\ell \mid m.$$

5. The equation $x^2 + q^{2k} = y^n$: the proof of Theorem 4

In this section, we prove Theorem 4 with the help of the primitive divisor theorem. We are concerned with the equation

$$x^2 + q^{2k} = y^n, \quad x, k, n \text{ positive integers}, \ n \geq 3, \ \gcd(x, y) = 1. \tag{25}$$

Here $q \geq 3$ is a prime. Considering this equation modulo 8 immediately tells us that y is odd and x is even. Without loss of generality, we may suppose that $4 \mid n$ or that n is divisible by an odd prime.

Lemma 5.1. *Solutions to (25) with $4 \mid n$ and odd prime q satisfy $k = 1$, $q^2 = 2y^{n/2} - 1$ and $x = (q^2 - 1)/2$. In particular, the only solutions to (25) with $4 \mid n$ and prime $3 \leq q < 1000$ correspond to the identities*

$$24^2 + 7^2 = 5^4, \quad 840^2 + 41^2 = 29^4 \quad \textit{and} \quad 28560^2 + 239^2 = 13^8 = 169^4.$$

Proof. Suppose that $4 \mid n$. Then $(y^{n/2} + x)(y^{n/2} - x) = q^{2k}$, and so

$$y^{n/2} + x = q^{2k} \quad \text{and} \quad y^{n/2} - x = 1.$$

Thus $2y^{n/2} = q^{2k} + 1$. By Theorem 1 of [Bennett and Skinner 2004], the only solutions to the equation $A^r + B^r = 2C^2$ with $r \geq 4$, $ABC \neq 0$ and $\gcd(A, B) = 1$ are with $|AB| = 1$ or $(r, A, B, C) = (5, 3, -1, \pm 11)$. It follows that the equation $2y^{n/2} = q^{2k} + 1$ has no solutions with $k \geq 2$ and $4 \mid n$. Therefore $k = 1$, and hence $q^2 = 2y^{n/2} - 1$. The only primes in the range $3 \leq q < 1000$, such that $q^2 = 2y^{n/2} - 1$ with $4 \mid n$, are $q = 7$, 41 and 239, which lead to the solutions stated in the lemma. $\square$

Henceforth, we will suppose that n is an odd prime. Thus $x+q^k i=\alpha^n$, where we can write $\alpha=a+bi$, for a and b coprime integers with $y=a^2+b^2$. Subtracting this equation from its conjugate yields

$$q^k=b\cdot\frac{\alpha^n-\bar{\alpha}^n}{\alpha-\bar{\alpha}}. \tag{26}$$

Lemma 5.2. *Solutions to (25) with $n=3$ and odd prime q must satisfy*

(i) *either $q=3$ and $(k,x,y)=(2,46,13)$;*

(ii) *or $q=3a^2-1$ for some positive integer a and $(k,x,y)=(1,a^3-3a,a^2+1)$;*

(iii) *or $q^2=3a^2+1$ for some positive integer a and $(k,x,y)=(1,8a^3+3a,4a^2+1)$.*

In particular, the only solutions to (25) with $n=3$ and prime $3\le q<1000$ correspond to the identities

$$46^2+3^4=13^3,\quad 524^2+7^2=65^3,\quad 2^2+11^2=5^3,\quad 52^2+47^2=17^3,$$
$$1405096^2+97^2=12545^3,\quad 198^2+107^2=37^3,\quad 488^2+191^2=65^3,$$
$$1692^2+431^2=145^3,\quad 2702^2+587^2=197^3,\quad 5778^2+971^2=325^3.$$

Proof. Let $n=3$. Thanks to Table 1, we know that the only solution with $q=3$ is the one given in (i). We may thus suppose that $q\ge 5$. Equation (26) gives

$$q^k=b(3a^2-b^2).$$

By the coprimality of a and b, we have $b=\pm 1$ or $b=\pm q^k$. We note that $b=-1$ gives $q^k=1-3a^2$ which is impossible. Also if $b=q^k$ then $3a^2-q^{2k}=1$ which is impossible modulo 3. Thus either $b=1$ or $b=-q^k$. If $b=1$, then

$$q^k=3a^2-1,$$

and if $b=-q^k$ then

$$q^{2k}=3a^2+1.$$

From Theorem 1.1 of [Bennett and Skinner 2004], these equations have no solutions in positive integers if $k\ge 4$ or $k\ge 2$, respectively. If $k=3$, the elliptic curve corresponding to the first equation has Mordell–Weil rank 0 over $\mathbb{Q}$ and it is straightforward to show that the equation has no integer solutions. We therefore have that $k=1$ in either case. Thus $q=3a^2-1$ or $q^2=3a^2+1$, and these yield the parametric solutions in (ii) and (iii). For $5\le q<1000$, the primes q of the form $3a^2-1$ are

$$11, 47, 107, 191, 431, 587, 971.$$

For $5\le q<1000$, the primes q satisfying $q^2=3a^2+1$ are $q=7$ and 97. These yield the solutions given in the statement of the lemma. $\square$

We expect that there are infinitely many primes q of the form $3a^2-1$, but are very unsure about the number of primes q satisfying $q^2=3a^2+1$ (the only ones known are 7, 97 and 708158977). Quantifying such results, in any case, is well beyond current technology.

In view of Lemma 5.2, we henceforth suppose that n is ≥ 5 and prime. The following lemma now completes the proof of Theorem 4.

Lemma 5.3. *Let (k, x, y, n) be a solution to (25) with prime $n \geq 5$ and odd prime q. Then k is odd,*

$$\begin{cases} n \mid (q-1) & \text{if } q \equiv 1 \pmod 4, \\ n \mid (q+1) & \text{if } q \equiv 3 \pmod 4, \end{cases} \tag{27}$$

and there is an integer a such that

$$y = a^2 + 1, \quad x = \frac{(a+i)^n + (a-i)^2}{2}, \quad \frac{(a+i)^n - (a-i)^n}{2i} = \pm q^k.$$

In particular, the only solutions to (25) with prime $3 \leq q < 1000$ and prime $n \geq 5$ correspond to the identities

$$38^2 + 41^2 = 5^5, \quad 278^2 + 29^2 = 5^7.$$

Proof. Suppose n is ≥ 5 and prime in (25). By Theorem 1 of [Bennett et al. 2010], the equation $A^4 + B^2 = C^m$ has no solutions satisfying $\gcd(A, B) = 1$, $AB \neq 0$ and $m \geq 4$. We conclude that k is odd. We note that $(\alpha, \overline{\alpha})$ is a Lucas pair and write $\{L_m\}$ for the corresponding Lucas sequence. By Theorem 6, L_n must have a primitive divisor, and from (26) this primitive divisor is q. In particular, q does not divide $D = (\alpha - \overline{\alpha})^2 = -4b^2$. Thus by (26) we have $b = \pm 1$ and $D = -4$. Moreover, the rank of apparition of q in the sequence is n. By Theorem 7, we have $n \mid (q-1)$ if $q \equiv 1 \pmod 4$ and $n \mid (q+1)$ if $q \equiv 3 \pmod 4$.

We now let q be a prime in the range $3 \leq q < 1000$. There are 168 pairs (q, n) with q in this range and n a prime ≥ 5 satisfying (27), ranging from $(19, 5)$ to $(997, 83)$. For each of these pairs (q, n), and each sign $\eta = \pm 1$, we need to consider the equation

$$\frac{(a+i)^n - (a-i)^n}{2i} = \eta \cdot q^k, \tag{28}$$

where k is an odd integer. We shall follow the sieving approach of Lemma 3.2 to eliminate all but two of the possible $2 \times 168 = 336$ triples (q, n, η). Fix such a triple (q, n, η). Let $f_n \in \mathbb{Z}[X]$ be the polynomial

$$f_n(X) = \frac{(X+i)^n - (X-i)^n}{2i}.$$

Let $\ell \nmid nq$ be an odd prime, and let $\mathcal{Z}_\ell$ be the set $\beta \in \mathbb{Z}/(\ell-1)\mathbb{Z}$ such that β is odd and $f_n(X) - \eta \cdot q^\beta$ has a root in $\mathbb{F}_\ell$. It follows that $(k \pmod{\ell}) \in \mathcal{Z}_\ell$. Now let $\ell_1, \ell_2, \ldots, \ell_m$ be a collection of odd primes $\nmid qn$. Define M and $\mathcal{Z}_{\ell_1,\ldots,\ell_m}$ by (21) and (22), respectively. It is clear that $(k \pmod M) \in \mathcal{Z}_{\ell_1,\ldots,\ell_m}$. We wrote a short `Magma` script which, for each triple (q, n, η), computed $\mathcal{Z}_{\ell_1,\ldots,\ell_m}$ where $\ell_1 \ldots, \ell_m$ are the odd primes < 150 distinct from n and q. In all but two of the 336 cases we found that $\mathcal{Z}_{\ell_1,\ldots,\ell_m} = \varnothing$. The two exceptions are $(q, n, \eta) = (41, 5, 1)$ and $(29, 7, -1)$, and so these are the only two cases we need to consider. Let

$$F_n(X, Y) = \frac{(X+iY)^n - (X-iY)^n}{2iY}.$$

This is a homogeneous degree $n-1$ polynomial belonging to $\mathbb{Z}[X,Y]$. Now (28) can be written as $F_n(a,1)=\eta\cdot q^k$. Thus it is sufficient to solve the Thue–Mahler equations $F_n(X,Y)=\eta\cdot q^k$ for $(q,n,\eta)=(41,5,1)$ and $(29,7,-1)$. Explicitly these equations are

$$5X^4-10X^2Y^2+Y^4=41^k \tag{29}$$

and

$$7X^6-35X^4Y^2+21X^2Y^4-Y^6=-29^k. \tag{30}$$

Using the `Magma` implementation of the Thue–Mahler solver described in [Gherga and Siksek 2022], we find that the solutions to (29) are $(X,Y,k)=(\pm2,\pm1,1)$ and $(0,\pm1,0)$, and that the solutions to (30) are also $(X,Y,k)=(\pm2,\pm1,1)$ and $(0,\pm1,0)$. These lead to the two solutions stated in the lemma. □

6. The equation $x^2-q^{2k}=y^n$ with y even: reduction to Thue–Mahler equations

Section 3 dealt with (7) in the case that y is odd, using purely elementary means. We now turn our attention to (7) with y even, and consider the equation

$$x^2-q^{2k}=y^n,\quad x,k,n \text{ positive integers},\ n\ge3,\ \gcd(x,y)=1,\ y \text{ an even integer}. \tag{31}$$

Here $q\ge3$ is a prime and, without loss of generality, $n=4$ or n is an odd prime.

Lemma 6.1. *Write $\gamma=1+\sqrt2$. Any solution to (31) with $n=4$ and q an odd prime must satisfy $k=1$,*

$$q=\frac{\gamma^{2m}+\gamma^{-2m}}{2},\quad x=\frac{\gamma^{4m}+6+\gamma^{-4m}}{8}\quad\text{and}\quad y=\frac{\gamma^{2m}-\gamma^{-2m}}{2\sqrt2}, \tag{32}$$

for some integer m. In particular, the only solutions with $3\le q<1000$ correspond to the identities

$$5^2-3^2=(\pm2)^4,\quad 145^2-17^2=(\pm12)^4\quad\text{and}\quad 166465^2-577^2=(\pm408)^4.$$

Proof. Suppose $n=4$. Then $(x+y^2)(x-y^2)=q^{2k}$, and so, by the coprimality of x and y,

$$x+y^2=q^{2k}\quad\text{and}\quad x-y^2=1,$$

or equivalently

$$x=\frac{q^{2k}+1}{2}\quad\text{and}\quad q^{2k}-2y^2=1. \tag{33}$$

First we show that $k=1$. From the second equation, we have $(q^k+1)(q^k-1)=2y^2$. Since the greatest common divisor of the two factors on the left is 2 we see that one of the two factors must be a perfect square, i.e., $q^k+1=z^2$ or $q^k-1=z^2$ for some nonzero integer z, and it is easy to see that k must be odd. The impossibility of these cases for $k\ge3$ follows from Mihăilescu's theorem [2004] (Catalan's conjecture). Hence $k=1$.

The second equation in (33) implies that $q+y\sqrt2$ is a totally positive unit in $\mathbb{Z}[\sqrt2]$. Thus

$$q+y\sqrt2=\gamma^{2m}\quad\text{and}\quad q-y\sqrt2=\gamma^{-2m}, \tag{34}$$

for some integer m. The formulae for q and y in (32) follow from this, and the formula for x follows from the first relation in (33).

We focus on primes $3 \le q < 1000$. From the first relation in (34),

$$|m| < \frac{\log(2q)}{2\log\gamma} < \frac{\log 2000}{2\log(1+\sqrt{2})} < 5.$$

Thus $-4 \le m \le 4$. The values $m = \pm 1, \pm 2, \pm 4$, respectively, give the three solutions in the statement of the lemma. If $m = 0$ or ± 3, then we obtain $q = 1$ or 99 which are not prime. □

In view of Lemma 6.1, we may henceforth suppose that $n \ge 3$ is odd. Let x' be either x or $-x$, chosen so that $x' \equiv q^k \pmod 4$. From (31), we deduce the existence of relatively prime integers y_1 and y_2 for which

$$x' + q^k = 2y_1^n \quad \text{and} \quad x' - q^k = 2^{n-1}y_2^n, \tag{35}$$

with $y = 2y_1y_2$, so that we have

$$y_1^n - 2^{n-2}y_2^n = q^k. \tag{36}$$

We have thus reduced the resolution of (31) for particular q and n to solving a degree n Thue–Mahler equation.

Lemma 6.2. *The only solutions to* (31) *with* $n \in \{3, 5\}$ *and* $3 \le q < 1000$ *an odd prime correspond to the identities*

$$53^2 - 3^2 = 40^3,\ \ 1^2 - 3^2 = (-2)^3,\ \ 7^2 - 3^4 = (-2)^5,\ \ 29^2 - 5^4 = 6^3,\ \ 9^2 - 7^2 = 2^5,\ \ 43^2 - 11^2 = 12^3,$$
$$499^2 - 13^2 = 12^5,\ \ 15^2 - 17^2 = -4^3,\ \ 397^2 - 17^4 = 42^3,\ \ 25^2 - 29^2 = (-6)^3,\ \ 11^2 - 43^2 = (-12)^3,$$
$$1415^2 - 43^2 = 126^3,\ \ 30042907^2 - 43^8 = 96222^3,\ \ 500047^2 - 47^2 = 6300^3,\ \ 55^2 - 53^2 = 6^3,$$
$$179^2 - 71^2 = 30^3,\ \ 4785^2 - 71^4 = (-136)^3,\ \ 775^2 - 89^2 = 84^3,\ \ 155^2 - 101^2 = 24^3,$$
$$13609^2 - 109^2 = 570^3,\ \ 141^2 - 109^2 = 20^3,\ \ 129^2 - 127^2 = 8^3,\ \ 123^2 - 127^2 = (-10)^3,$$
$$2789^2 - 127^2 = 198^3,\ \ 71^2 - 179^2 = (-30)^3,\ \ 4197^2 - 197^2 = 260^3,\ \ 277^2 - 223^2 = 30^3,$$
$$249^2 - 251^2 = (-10)^3,\ \ 235^2 - 251^2 = (-6)^5,\ \ 255^2 - 257^2 = -4^5,\ \ 118901^2 - 263^2 = 2418^3,$$
$$223^2 - 277^2 = (-30)^3,\ \ 2355^2 - 307^2 = 176^3,\ \ 143027^2 - 307^4 = 2262^3,\ \ 557^2 - 307^2 = 60^3,$$
$$327^2 - 359^2 = (-28)^3,\ \ 4146689^2 - 383^4 = 25800^3,\ \ 289^2 - 397^2 = (-42)^3,\ \ 433^2 - 431^2 = 12^3,$$
$$431^2 - 433^2 = (-12)^3,\ \ 4308693^2 - 433^4 = 26462^3,\ \ 979^2 - 479^2 = 90^3,\ \ 13^2 - 499^2 = (-12)^5,$$
$$23831^2 - 503^2 = 828^3,\ \ 307^2 - 557^2 = (-60)^3,\ \ 93^2 - 593^2 = (-70)^3,\ \ 857^2 - 601^2 = 72^3,$$
$$713^2 - 659^2 = 42^3,\ \ 85016415^2 - 683^2 = 193346^3,\ \ 297053^2 - 701^2 = 4452^3,\ \ 731^2 - 727^2 = 18^3,$$
$$3655^2 - 739^2 = 234^3,\ \ 561^2 - 811^2 = (-70)^3,\ \ 601^2 - 857^2 = (-72)^3,\ \ 1051^2 - 997^2 = 48^3.$$

Proof. For $n \in \{3, 5\}$ and primes $3 \le q < 1000$, we solved the Thue–Mahler equation (36) using the `Magma` implementation of the Thue–Mahler solver described in [Gherga and Siksek 2022]. The computation resulted in the solutions given in the statement of the lemma. □

7. The modular approach to Diophantine equations: some background

Let $F/\mathbb{Q}$ be an elliptic curve over the rationals of conductor N_F and minimal discriminant Δ_F. Let $p \geq 5$ be a prime. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion $F[p]$ gives rise to a 2-dimensional mod p representation

$$\bar{\rho}_{F,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p).$$

Suppose $\bar{\rho}_{F,p}$ is irreducible (that is, F does not have an p-isogeny); this can often be established by appealing to Mazur's isogeny theorem [1978]. A standard consequence of Ribet's lowering theorem [1990], building on the modularity of elliptic curves over $\mathbb{Q}$ due to Wiles and others [Wiles 1995; Breuil et al. 2001], is that $\bar{\rho}_{F,p}$ arises from a weight-2 newform of level

$$N = N_F \Big/ \prod_{\substack{\ell \,\|\, N_F \\ p \mid \mathrm{ord}_\ell(\Delta_F)}} \ell.$$

More precisely, there is a newform f of weight 2 and level N with normalized $\mathfrak{q}$-expansion

$$f = \mathfrak{q} + \sum_{m=2}^{\infty} c_m \mathfrak{q}^m \tag{37}$$

such that

$$\bar{\rho}_{F,p} \sim \bar{\rho}_{f,\mathfrak{p}}, \tag{38}$$

where $\mathfrak{p}$ is a prime ideal above p of the ring of integers $\mathcal{O}_f$ of the Hecke eigenfield $K_f = \mathbb{Q}(c_1, c_2, \dots)$.

The original motivation for the great theorems of Ribet and Wiles included Fermat's last theorem. To motivate what is to come in later sections, we quickly sketch the deduction of FLT from the above. Let x, y and z be nonzero coprime rational integers satisfying $x^p + y^p + z^p = 0$ where $p \geq 5$ is prime. After appropriately permuting x, y and z, we may suppose that $2 \mid y$ and that $x^n \equiv -1 \pmod 4$. Let F be the Frey–Hellegouarch curve

$$Y^2 = X(X - x^p)(X + y^p).$$

It follows from Mazur's isogeny theorem and related results that $\bar{\rho}_{E,p}$ is irreducible. A short computation reveals that

$$\Delta_F = 2^{-8}(xyz)^{2p} \quad \text{and} \quad N_F = 2\,\mathrm{Rad}(xyz),$$

where $\mathrm{Rad}(m)$ denotes the product of the prime divisors of m. We find that $N = 2$. Thus $\bar{\rho}_{F,p}$ arises from a newform f of weight 2 and level 2; the nonexistence of such newforms provides the desired contradiction.

It is possible to use a similar strategy to treat various Diophantine problems including generalized Fermat equations $Ax^p + By^q = Cz^r$, for certain signatures (p, q, r). This is done by Kraus [1997] for signature (p, p, p) and by Bennett and Skinner [2004] for signature $(p, p, 2)$. Fortunately, these papers provide recipes for the Frey–Hellegouarch curves F and for the levels N, and establish the required irreducibility of $\bar{\rho}_{F,n}$. We shall make frequent use of these recipes in later sections. It is known (and easily checked using standard dimension formulae) that there are no weight-2 newforms at levels

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60, \tag{39}$$

but there are newforms at all other levels. Thus, if the level N predicted by the recipes is not in the list (39) then we do not immediately obtain a contradiction. Instead, we may compute the possible newforms using implementations (for example, in Magma or SAGE) of modular symbols algorithms due to Cremona [1997] and Stein [2007]. We then use the relation (38) to help us extract information about the solutions to our Diophantine equation. In doing this, we shall often make use of the following standard result; see, for example, [Kraus and Oesterlé 1992; Siksek 2012, Section 5].

Lemma 7.1. *Let $F/\mathbb{Q}$ be an elliptic curve of conductor N_F. Let f be a weight-2 newform of level N having $\mathfrak{q}$-expansion as in (37). Suppose (38) holds for some prime $p \geq 5$. Let $\ell \neq p$ be a rational prime.*

(i) *If $\ell \nmid N_F N$ then $a_\ell(F) \equiv c_\ell \pmod{\mathfrak{p}}$.*

(ii) *If $\ell \nmid N$ but $\ell \,||\, N_F$ then $\ell + 1 \equiv \pm c_\ell \pmod{\mathfrak{p}}$.*

If f is a rational newform (i.e., $K_f = \mathbb{Q}$) then (i), (ii) also hold for $\ell = p$.

We will also make frequent use of the following theorem.

Theorem 8 [Kraus 1997, Proposition 2]. *Let f be a newform of weight 2 and level N with $\mathfrak{q}$-expansion as in (37), and Hecke eigenfield K_f with ring of integers $\mathcal{O}_f$. Write*

$$M = \operatorname{lcm}(4, N) \quad \text{and} \quad \mu(M) = M \cdot \prod_{\substack{r \mid M \\ r \text{ prime}}} \left(1 + \frac{1}{r}\right).$$

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_f$ and suppose the following two conditions hold.

(i) *For all primes $\ell \leq \mu(M)/6$, $\ell \nmid 2N$, we have*

$$\ell + 1 \equiv c_\ell \pmod{\mathfrak{p}}.$$

(ii) *For all primes $\ell \leq \mu(M)/6$, $\ell \mid 2N$, $\ell^2 \nmid 4N$, we have*

$$(\ell + 1)(c_\ell - 1) \equiv 0 \pmod{\mathfrak{p}}.$$

Then $\ell + 1 \equiv c_\ell \pmod{\mathfrak{p}}$ for all primes $\ell \nmid 2N$.

8. The equation $x^2 - q^{2k} = y^n$ with y even: an approach via Frey curves

We are still concerned with (31). In view of the results of Section 6, we may suppose that $n \geq 7$ is prime. To show that (31) has no solutions for a particular pair (q, n), it is enough to show the same for (36). We shall think of (36) as a Fermat equation of signature (n, n, n) by writing it as $y_1^n - 2^{n-2} y_2^n = q^k \cdot 1^n$. This enables us to apply recipes of Kraus [1997] for Frey–Hellegouarch curves and level lowering. The following lemma will eliminate some cases when applying those recipes.

Lemma 8.1. *Suppose $n \geq 7$ is prime. Then* $\gcd(k, 2n) = 1$.

Proof. Theorem 1.2 of [Bennett and Skinner 2004] asserts that the equation $A^p + 2^\alpha B^p = C^2$ with prime $p \geq 7$ has no solutions in nonzero integers with $\gcd(A, B, C) = 1$ and $\alpha \geq 2$. It immediately follows from (36) that k is odd. Moreover, Theorem 3 of [Ribet 1997] asserts that the equation $A^p + 2^\alpha B^p + C^p = 0$ has no solutions with $ABC \neq 0$ for prime $p \geq 7$ and $2 \leq \alpha \leq p-1$. It follows that $n \nmid k$. □

Following Kraus, we attach to a solution of (36) a Frey–Hellegouarch curve F, where

$$F : Y^2 = X(X + y_1^n)(X + 2^{n-2} y_2^n) \tag{40}$$

if $q \equiv 1 \pmod 4$, and

$$F : Y^2 = X(X - q^k)(X + 2^{n-2} y_2^n), \tag{41}$$

if $q \equiv 3 \pmod 4$. The Frey–Hellegouarch curve F is semistable, and has minimal discriminant and conductor, respectively, given by

$$\Delta_F = 2^{2n-12} q^{2k} (y_1 y_2)^n \quad \text{and} \quad N_F = 2q \cdot \mathrm{Rad}_2(y_1 y_2), \tag{42}$$

where $\mathrm{Rad}_2(m)$ denotes the product of the odd primes dividing m. From Kraus [1997], the mod n representation of F arises from a newform f of weight 2 and level $N = 2q$.

Let $\ell \nmid 2q$ be a prime. Write

$$T \;=\; \{a \in \mathbb{Z} \cap [-2\sqrt{\ell}, 2\sqrt{\ell}] : a \equiv \ell + 1 \pmod 4\}.$$

Let

$$\mathcal{D}'_{f,\ell} = ((\ell+1)^2 - c_\ell^2) \cdot \prod_{a \in T} (a - c_\ell),$$

and

$$\mathcal{D}_{f,\ell} = \begin{cases} \ell \cdot \mathcal{D}'_{f,\ell} & \text{if } K_f \neq \mathbb{Q}, \\ \mathcal{D}'_{f,\ell} & \text{if } K_f = \mathbb{Q}, \end{cases}$$

Lemma 8.2. *Let f be a newform of weight 2 and level $2q$, and suppose that (38) holds. Let $\ell \nmid 2q$ be a prime. Then $\mathfrak{n} \mid \mathcal{D}_{f,\ell}$.*

Proof. If $\ell \nmid y_1 y_2$, then $\ell \nmid N_F$ and so is a prime of good reduction for F. As F has full 2-torsion we deduce that $4 \mid (\ell + 1 - a_\ell(F))$. By the Hasse–Weil bounds, $a_\ell(F)$ belongs to the set T. If $\ell \mid y_1 y_2$, then $\ell \mid\mid N_F$. The lemma now follows from Lemma 7.1. □

It is straightforward from Lemma 8.2 and the fact that $\mathfrak{n} \mid n$ that $n \mid \mathrm{Norm}(\mathcal{D}_{f,\ell})$. Thus if $\mathcal{D}_{f,\ell} \neq 0$, we immediately obtain an upper bound upon the exponent n. This approach will result in a bound on the exponent n in (31) unless f corresponds to an elliptic curve over $\mathbb{Q}$ with full 2-torsion and conductor $N = 2q$; for this see [Siksek 2012, Section 9]. Mazur showed that such an elliptic curve exists if and only if $q \geq 31$ is a Fermat or a Mersenne prime; see, for example, [Siksek 2012, Theorem 8]. We note that 31, 127 and 257 are the only such primes in our range $3 \leq q < 1000$. We shall exploit this approach to prove the following.

Proposition 8.3. *Let $n \geq 7$ and $3 \leq q < 1000$ be primes.*

(i) *If $q \notin \{31, 127, 257\}$, then (31) has no solutions.*

(ii) *Suppose $q \in \{31, 127, 257\}$, write $q = 2^m + \eta$ where $\eta = \pm 1$, and let*

$$E_q : Y^2 = X(X + 1)(X - \eta \cdot 2^m). \tag{43}$$

Suppose (k, x, y) is a solution to (31) and let F be as above. Then

$$\bar{\rho}_{F,n} \sim \bar{\rho}_{E_q,n}.$$

In Cremona's notation, these E_q are the elliptic curves `62a2`, `254d2` and `514a2`, for $q = 31$, 127 and 257, respectively.

Proof. There are no newforms of weight 2 and levels 6, 10 and 22. Therefore the proof is complete in the cases where $q \in \{3, 5, 11\}$. We may thus suppose that $7 \leq q < 1000$ is prime and that $q \neq 11$.

For a newform f of weight 2 and level $2q$, and a collection of primes $\ell_1, \ldots, \ell_m$ (all coprime to $2q$), we write $\mathcal{D}_{f,\ell_1,\ldots,\ell_m}$ for the ideal of $\mathcal{O}_f$ generated by $\mathcal{D}_{f,\ell_1}, \ldots, \mathcal{D}_{f,\ell_m}$. Let $\mathcal{B}_{f,\ell_1,\ldots,\ell_m} \in \mathbb{Z}$ be the norm of the ideal $\mathcal{D}_{f,\ell_1,\ldots,\ell_m}$. If $\bar{\rho}_{F,n} \sim \bar{\rho}_{f,\mathfrak{n}}$, then $\mathfrak{n} \mid \mathcal{D}_{f,\ell_1,\ldots,\ell_m}$ by Lemma 8.2. As $\mathfrak{n} \mid n$, we deduce that $n \mid \mathcal{B}_{f,\ell_1,\ldots,\ell_m}$. In our computations we will take $\ell_1, \ldots, \ell_m$ to be all the primes < 200 distinct from 2 and q, and write $\mathcal{B}_f$ for $\mathcal{B}_{f,\ell_1,\ldots,\ell_m}$.

We wrote a short `Magma` script which computed, for all newforms f at all levels $2q$ under consideration, the integer $\mathcal{B}_f$. We found that $\mathcal{B}_f \neq 0$ for all newforms f except for three rational newforms of levels 62, 254 and 514 (corresponding to $q = 31$, 127 and 257, respectively). Thus, for all other newforms, we at least obtain a bound on n. In many cases this bound is already sharp enough to contradict our assumption that $n \geq 7$. We give a few examples.

Let $q = 13$. Then there are two eigenforms f_1, f_2 of level $2q = 26$, and

$$\mathcal{B}_{f_1} = 3 \times 5, \quad \mathcal{B}_{f_2} = 3 \times 7.$$

Thus we eliminate f_1 from consideration, and also conclude that $n = 7$. It is natural to wonder if $n = 7$ can be eliminated by increasing the size of our set of primes $\ell_1, \ldots, \ell_m$, but this is not the case. The newform f_2 is rational and corresponds to the elliptic curve `26b1` with Weierstrass model

$$E' : Y^2 + XY + Y = X^3 - X^2 - 3X + 3.$$

The torsion subgroup of $E'(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/7\mathbb{Z}$, generated by the point $(1, 0)$. In particular, for any prime $\ell \nmid 26$, we have $7 \mid (\ell + 1 - a_\ell(E'))$. Since $a_\ell(E') = c_\ell(f_2)$, we have $7 \mid \mathcal{B}_{f_2,\ell}$. Thus $7 \mid \mathcal{B}_{f,\ell_1,\ldots,\ell_n}$ regardless of the set of primes $\ell_1, \ldots, \ell_m$ that we choose. However we can still obtain a contradiction for $n = 7$ in this case. Indeed, we have $\bar{\rho}_{F,7} \sim \bar{\rho}_{f_2,7} \sim \bar{\rho}_{E',7}$. Since E' has nontrivial 7-torsion, the representation $\bar{\rho}_{E',7}$ is reducible. However, the representation of the Frey curve $\bar{\rho}_{F,7}$ is irreducible as shown by Kraus [1997, Lemme 4], contradicting the fact that F has full rational 2-torsion.

For $q = 31$, there are two newforms, g_1 and g_2. We find that $\mathcal{B}_{g_1} = 0$ and $\mathcal{B}_{g_2} = 2^3 \times 3^2$; thus we may eliminate g_2 for consideration. The eigenform g_1 is rational and corresponds to the elliptic curve E_{31} with Cremona label 62a2. Hence $\bar{\rho}_{F,p} \sim \bar{\rho}_{g_1,p} \sim \bar{\rho}_{E_{31},p}$, whence the proof is complete for $q = 31$.

For $q = 37$, there are two newforms, h_1 and h_2. We find that $\mathcal{B}_{h_1} = 3^3$ and $\mathcal{B}_{h_2} = 19$. Thus $n = 19$ and

$$\bar{\rho}_{F,19} \sim \bar{\rho}_{h_2,19}. \tag{44}$$

The newform h_2 has $\mathfrak{q}$-expansion

$$h_2 = \mathfrak{q} + \mathfrak{q}^2 + \alpha\mathfrak{q}^3 + \mathfrak{q}^4 + (-3\alpha - 1)\mathfrak{q}^5 + \alpha\mathfrak{q}^6 + 2\alpha\mathfrak{q}^7 + \cdots, \quad \text{where } \alpha = \frac{-1+\sqrt{5}}{2},$$

and Hecke eigenfield $K = \mathbb{Q}(\sqrt{5})$. Let $\mathfrak{n}$ be the prime ideal $\mathfrak{n} = (4 - \alpha) \cdot \mathcal{O}_K$ having norm 19. We checked, using Theorem 8, that $\ell + 1 \equiv c_\ell \pmod{\mathfrak{n}}$ for all primes $\ell \nmid 2 \cdot 37$, where c_ℓ is the ℓ-th coefficient of h_2. From relation (44), we know that

$$a_\ell(F) \equiv c_\ell \pmod{\mathfrak{n}}$$

for all primes ℓ of good reduction for $F_{3,1}$. Thus $19 \mid (\ell + 1 - a_\ell(F_{3,1}))$ for all primes ℓ of good reduction. As before, this now implies that $\bar{\rho}_{F,19}$ is reducible [Serre 1975, IV-6], giving a contradiction. The proof is thus complete for $q = 37$.

The above arguments allow us to prove (ii) in the statement of the proposition, and to obtain a contradiction for all $3 \le q < 1000$, $q \notin \{31, 127, 257\}$, except when $n = 7$ and q belongs to the list

$$43, 101, 103, 139, 163, 379, 467, 509, 557, 569, 839, 937, 947, 977.$$

For $n = 7$ and these values of q, we checked using the aforementioned Thue–Mahler solver that the only solutions to (36) are $(y_1, y_2, k) = (1, 0, 0)$. Since $k \neq 0$ in (31), the proof is complete. $\square$

Symplectic criteria. When $q \ge 31$ is a Fermat or Mersenne prime, it does not seem to be possible, working purely with Galois representations of elliptic curves, to eliminate the possibility that $\bar{\rho}_{F,n} \sim \bar{\rho}_{E_q,n}$. However, the so-called 'symplectic method' of Halberstadt and Kraus [2002] allows us to derive an additional restriction on the solutions to (31).

Lemma 8.4. *Let $q = 2^m + \eta$ be a Fermat or Mersenne prime. Let $n \ge 7$ be a prime $\neq q$. Suppose (x, y, k) is a solution to (31), and let F be the Frey–Hellegouarch curve constructed above, and E_q be given by (43). Suppose $\bar{\rho}_{F,n} \sim \bar{\rho}_{E_q,n}$. Then either $n \mid (m - 4)$ or*

$$\left(\frac{(24 - 6m)k}{n}\right) = 1. \tag{45}$$

Proof. We note that the curves F and E_q have multiplicative reduction at both 2 and q. Write Δ_1 and Δ_2 for the minimal discriminants of F and E_q, respectively. By [Halberstadt and Kraus 2002, Lemme 1.6], the ratio

$$\frac{\mathrm{ord}_2(\Delta_1) \cdot \mathrm{ord}_q(\Delta_1)}{\mathrm{ord}_2(\Delta_2) \cdot \mathrm{ord}_q(\Delta_2)}$$

is a square modulo n, provided $n \nmid \mathrm{ord}_2(\Delta_i)$, $n \nmid \mathrm{ord}_q(\Delta_i)$. It is in invoking this result of Halberstadt and Kraus that we require the assumption that $n \neq q$. We find that

$$\Delta_1 = 2^{2n-12} q^{2k} (y_1 y_2)^{2n} \quad \text{and} \quad \Delta_2 = 2^{2m-8} q^2.$$

We have previously noted that $n \nmid k$ by appealing to a result of Ribet. Suppose $n \nmid (m-4)$. Then the valuations $\mathrm{ord}_2(\Delta_i)$ and $\mathrm{ord}_q(\Delta_i)$ are all indivisible by n. The result follows. □

9. The equation $x^2 - q^{2k} = y^n$: an upper bound for the exponent n

To help us complete the proof of Theorem 5, we begin by deriving an upper bound for n. Our approach is essentially a minor sharpening of Theorem 3 of [Bugeaud 1997] in a slightly special case. Since this result is valid for an arbitrary prime q, it may be of independent interest.

Theorem 9. *Let $x, y, q, k \geq 1$ and $n \geq 3$ be integers satisfying (7), with n and q prime, and $q \nmid x$. Then*

$$n < 1000\, q \log q.$$

Proof. If $q = 2$, then we have that $n \leq 5$ from Theorem 1.2 of [Bennett and Skinner 2004]. We may thus suppose that q is odd and, additionally, that y is even, or, via Proposition 3.1, we immediately obtain the much stronger result that $n \mid (q-1)$. We are therefore in case (35). By Proposition 8.3, we may suppose that $q = 31$ or that $q \geq 127$. Set $Y = \max\{|y_1|, |2y_2|\}$ and suppose first that

$$q^k \geq Y^{n/2}, \tag{46}$$

or equivalently

$$2k \log q \geq n \log Y. \tag{47}$$

We set

$$\Lambda = \frac{q^k}{(2y_2)^n} = \left(\frac{y_1}{2y_2}\right)^n - \frac{1}{4};$$

we wish to apply an upper bound for linear forms in q-adic logarithms to Λ, in order to bound k. To do this, we must first treat the case where $y_1/2y_2$ and $\frac{1}{4}$ are multiplicatively dependent, i.e., where $y_1 y_2$ has no odd prime divisors. Under this assumption, since y_1 is odd, we find from (36) that

$$2^j \pm 1 = q^k,$$

for an integer j with $j \equiv -2 \pmod{n}$. Via Mihăilescu's theorem [2004], if $n \geq 7$, necessarily $k = 1$, $y_1 = \pm 1$, $y_2 = -2^\kappa$ for some integer κ and

$$q = 2^{(\kappa+1)n-2} \pm 1.$$

In this case, we find a solution to (7) corresponding to the identity

$$(-q \pm 2)^2 - q^2 = 4 \mp 4q = (\mp 2^{\kappa+1})^n,$$

whereby, certainly $n < 1000\, q \log q$.

Otherwise, we may suppose that $y_1/2y_2$ and $\frac{1}{4}$ are multiplicatively independent and that $Y \geq 3$. We will appeal to Théorème 4 of Bugeaud and Laurent [1996], with, in the notation of that result, $(\mu, \nu) = (10, 5)$ (see also Proposition 1 of Bugeaud [1997]). Before we state this result, we require some notation. Let $\overline{\mathbb{Q}_q}$ denote an algebraic closure of the q-adic field $\mathbb{Q}_q$, and define ν_q to be the unique extension to $\overline{\mathbb{Q}_q}$ of the standard q-adic valuation over $\mathbb{Q}_q$, normalized so that $\nu_q(q) = 1$. For any algebraic number α of degree d over $\mathbb{Q}$, define the *absolute logarithmic height* of α via the formula

$$h(\alpha) = \frac{1}{d}\left(\log|a_0| + \sum_{i=1}^{d} \log \max(1, |\alpha^{(i)}|)\right), \tag{48}$$

where a_0 is the leading coefficient of the minimal polynomial of α over $\mathbb{Z}$ and the $\alpha^{(i)}$ are the conjugates of α in $\mathbb{C}$.

Theorem 10 (Bugeaud–Laurent). *Let q be a prime number and let α_1, α_2 denote algebraic numbers which are q-adic units. Let f be the residual degree of the extension $\mathbb{Q}_q(\alpha_1, \alpha_2)/\mathbb{Q}_q$ and put*

$$D = \frac{[\mathbb{Q}_q(\alpha_1, \alpha_2) : \mathbb{Q}_q]}{f}.$$

Let b_1 and b_2 be positive integers and put

$$\Lambda_1 = \alpha_1^{b_1} - \alpha_2^{b_2}.$$

Denote by $A_1 > 1$ and $A_2 > 1$ real numbers such that

$$\log A_i \geq \max\left\{h(\alpha_i), \frac{\log q}{D}\right\}, \quad i \in \{1, 2\},$$

and put

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

If α_1 and α_2 are multiplicatively independent, then we have the bound

$$\nu_q(\Lambda_1) \leq \frac{24q(q^f - 1)}{(q-1)\log^4 q} D^4 \left(\max\left\{\log b' + \log\log q + 0.4, \frac{10 \log q}{D}, 5\right\}\right)^2 \cdot \log A_1 \cdot \log A_2.$$

We apply this with

$$f = 1, \quad D = 1, \quad \alpha_1 = \frac{y_1}{2y_2}, \quad \alpha_2 = \frac{1}{4}, \quad b_1 = n, \quad b_2 = 1,$$

so that we may choose

$$\log A_1 = \max\{\log Y, \log q\}, \quad \log A_2 = \max\{2 \log 2, \log q\},$$

and

$$b' = \frac{n}{\log A_2} + \frac{1}{\log A_1}.$$

Let us assume now that

$$n \geq 1000\, q \log q, \tag{49}$$

whilst recalling that either $q = 31$ or $q \geq 127$. We therefore have

$$b' < 1.001 \frac{n}{\log q}$$

and hence find that

$$k \leq 24 \frac{q}{\log^3 q} (\max\{\log n + 0.401, 10 \log q\})^2 \log A_1, \tag{50}$$

whence, from (47),

$$n \log Y \leq 48 \frac{q}{\log^2 q} (\max\{\log n + 0.401, 10 \log q\})^2 \log A_1. \tag{51}$$

Let us suppose first that

$$\log n + 0.401 \geq 10 \log q.$$

If $q \geq Y$, we have that $\log A_1 = \log q$ and hence

$$\frac{n \log Y}{(\log n + 0.401)^2} \leq 48 \frac{q}{\log q}.$$

From (49), we thus have

$$\frac{\log^2 q}{(\log(1000\, q \log q) + 0.401)^2} \leq \frac{0.048}{\log Y} \leq \frac{0.048}{\log 3},$$

contradicting $q \geq 31$. If, on the other hand, $q < Y$, then $\log A_1 = \log Y$ and so

$$\frac{n}{(\log n + 0.401)^2} \leq 48 \frac{q}{\log^2 q}. \tag{52}$$

With (49), this implies that

$$\log^3 q < 0.048(\log(1000\, q \log q) + 0.401)^2,$$

again contradicting $q \geq 31$.

We may therefore assume that

$$\log n + 0.401 < 10 \log q,$$

so that

$$n \log Y \leq 4800\, q \log A_1.$$

If $q \geq Y$, then, from (49),

$$\log Y < 4.8,$$

whereby $3 \leq Y \leq 121$. If $|y_1| \geq 2|y_2|$, it follows from (36) that

$$q^k \geq |y_1|^n - \tfrac{1}{4}|y_1|^n = \tfrac{3}{4} Y^n. \tag{53}$$

Suppose, conversely, that $|y_1| \leq 2|y_2| - 1$ (so that $1 \leq |y_2| \leq 60$). If $y_1 > 0$ and $y_2 < 0$, it follows from (36) that

$$q^k > \tfrac{1}{4} Y^n. \tag{54}$$

We may thus suppose that y_1 and y_2 have the same sign, whence, from (36), (49) and $|y_2| \leq 60$,

$$q^k = 2^{n-2}|y_2|^n - |y_1|^n > 0.24 \cdot |2y_2|^n = 0.24 \cdot Y^n. \tag{55}$$

Combining (53), (54) and (55), we thus have from (50) that

$$n \log Y + \log 0.24 < k \log q \leq 2400\, q \log q,$$

contradicting (49) and $q \geq 31$. If $q < Y$, then, via (49),

$$1000\, q \log q \leq n \leq 4800\, q, \tag{56}$$

a contradiction for $q \geq 127$. We may thus suppose that $q = 31$, $Y > 31$ and, from (52), $n \leq 12119$, which contradicts (49).

Next suppose that inequality (46) (and hence also inequality (47)) fails to hold. In this case, we will apply lower bounds for linear forms in two complex logarithms. Following Bugeaud, we take

$$\Lambda_1 = 4\Lambda = \frac{4q^k}{(2y_2)^n} = 4\left(\frac{y_1}{2y_2}\right)^n - 1,$$

so that

$$\log|\Lambda_1| = 2\log 2 + k \log q - n \log|2y_2|. \tag{57}$$

If $Y = \max\{|y_1|, |2y_2|\} = |y_1|$, then, from (35), it follows that

$$q^k \geq \tfrac{3}{4}|y_1|^n = \tfrac{3}{4}Y^n,$$

contradicting $q^k < Y^{n/2}$. It follows that $Y = |2y_2|$ and so, from (57),

$$\log|\Lambda_1| = 2\log 2 + k\log q - n \log Y \leq 2 \log 2 - \frac{n}{2}\log Y. \tag{58}$$

From (49), we have that $|\Lambda_1| \leq \frac{1}{2000}$, so that

$$\left| n \log\left|\frac{2y_2}{y_1}\right| - 2\log 2\right| \leq |\log(1-\Lambda_1)| \leq 1.001\,|\Lambda_1|. \tag{59}$$

We will appeal to the following.

Theorem 11 [Laurent 2008, Corollary 1]. *Consider the linear form*

$$\Lambda = c_2 \log \beta_2 - c_1 \log \beta_1,$$

where c_1 and c_2 are positive integers, and β_1 and β_2 are multiplicatively independent algebraic numbers. Define $D = [\mathbb{Q}(\beta_1, \beta_2) : \mathbb{Q}]/[\mathbb{R}(\beta_1, \beta_2) : \mathbb{R}]$ and set

$$b' = \frac{c_1}{D \log B_2} + \frac{c_2}{D \log B_1},$$

where $B_1, B_2 > 1$ are real numbers such that

$$\log B_i \geq \max\left\{h(\beta_i), \frac{|\log \beta_i|}{D}, \frac{1}{D}\right\}, \quad i \in \{1, 2\}.$$

Then

$$\log|\Lambda| \geq -CD^4\left(\max\left\{\log b' + 0.21, \frac{m}{D}, 1\right\}\right)^2 \log B_1 \log B_2,$$

for each pair (m, C) *in the following set*

$$\big\{(10, 32.3), (12, 29.9), (14, 28.2), (16, 26.9), (18, 26.0), (20, 25.2), (22, 24.5), (24, 24.0), (26, 23.5), (28, 23.1), (30, 22.8)\big\}.$$

Applying this result to the left-hand side of (59), with $(m, C) = (10, 32.3)$,

$$\beta_2 = \left|\frac{2y_2}{y_1}\right|, \quad \beta_1 = 4, \quad c_2 = n, \quad c_1 = 1, \quad D = 1,$$

$$\log B_2 = \log Y, \quad \log B_1 = 2\log 2 \quad \text{and} \quad b' = \frac{n}{2\log 2} + \frac{1}{\log Y} < \frac{1.001n}{2\log 2},$$

we may conclude that

$$\log|\Lambda_1| \geq -0.001 - 44.8(\max\{\log n - 0.11, 10\})^2 \log Y.$$

Combining this with (58), we thus have

$$n \leq 89.6(\max\{\log n - 0.11, 10\})^2 + \frac{1.4}{\log Y}.$$

After a little work we find that

$$n \leq 8961,$$

contradicting (49) and $q \geq 31$. □

10. The equation $x^2 - q^{2k} = y^n$: proof of Theorem 5

In this section, we complete the proof of Theorem 5. Let $3 \leq q < 1000$ be a prime and let (k, x, y, n) be a solution to (7) where $x, k \geq 1$ and $n \geq 3$ are positive integers satisfying $q \nmid x$. Thanks to Lemmata 3.2, 6.1 and 6.2, we may suppose that y is even and that $n \geq 7$ is prime. It follows from Proposition 8.3 that $q = 31$, 127 or 257 and $\bar{\rho}_{F,n} \sim \bar{\rho}_{E_q,n}$, where E_q is given in (43), and F is the Frey–Hellegouarch curve given in (40) or (41) according to whether $q \equiv 1$ or 3 (mod 4). From Theorem 9, we have

$$n < 1000 \times 257 \times \log 257 < 1.5 \times 10^6.$$

We now give a method, which for a given exponent n and prime $q \in \{31, 127, 257\}$, is capable of showing that (36) has no solutions. This is an adaptation of the method called 'predicting the exponents of constants' in [Siksek 2012, Section 13]. Let $n \geq 7$ be prime and choose $\ell \neq q$ to be a prime satisfying

(i) $\ell = tn + 1$ for some positive integer t;

(ii) $n \nmid ((\ell + 1)^2 - a_\ell(E_q)^2)$.

For $\kappa \in \mathbb{F}_\ell$, $\kappa \notin \{0, 1\}$, set

$$E(\kappa) : Y^2 = X(X-1)(X-\kappa).$$

Let g be a primitive root for ℓ (that is, a generator for $\mathbb{F}_\ell^*$) and let $h = g^n$. Define $\mathcal{X}_\ell \subset \mathbb{F}_\ell^*$ via

$$\mathcal{X}_\ell = \left\{\tfrac{1}{4}h^r : 0 \le r \le t-1 \text{ and } h^r \not\equiv 4 \pmod{\ell}\right\}$$

and

$$\mathcal{Y}_\ell = \{(\kappa - 1)\cdot(\mathbb{F}_\ell^*)^n : \kappa \in \mathcal{X}_\ell \text{ and } a_\ell(E(\kappa))^2 \equiv a_\ell(E_q)^2 \pmod{n}\} \subset \mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^n.$$

Define further

$$\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^n \quad \text{via } \phi(s) = q^s \cdot (\mathbb{F}_\ell^*)^n.$$

Finally, let

$$\mathcal{Z}_\ell = \left\{ s \in \phi^{-1}(\mathcal{Y}_\ell) : \left(\frac{(24-6m)s}{n}\right) = 1 \right\},$$

where $q = 2^m \pm 1$; thus $m = 5$, 7 and 8 for $q = 31$, 127 and 257, respectively. We note that $n \nmid (m-4)$ in all cases, so that (45) holds.

Lemma 10.1. *Let $q \in \{31, 127, 257\}$ and $n \ge 7$, $n \ne q$ be prime. Let $\ell_1, \dots, \ell_t$ be primes $\ne q$ satisfying* (*i*) *and* (*ii*) *above, and also*

$$\bigcap_{i=1}^{t} \mathcal{Z}_{\ell_i} = \varnothing. \tag{60}$$

Then (7) has no solutions with $k \ge 1$ and $q \nmid x$.

Proof. From Proposition 8.3, $\bar{\rho}_{F,n} \sim \bar{\rho}_{E_q,n}$. The minimal discriminant and conductor of F are given in (42). Thus a prime $\ell \nmid 2q$ satisfies $\ell \,||\, N_F$ if and only if $\ell \mid y_1 y_2$, otherwise $\ell \nmid N_F$. Let $\ell \ne q$ be a prime satisfying (i) and (ii). By (ii) we know, thanks to Lemma 7.1, that $\ell \nmid y_1 y_2$, and so $a_\ell(F) \equiv a_\ell(E_q) \pmod{n}$. Let $\kappa \in \mathbb{F}_\ell$ satisfy

$$\kappa \equiv \frac{2^{n-2} y_2^n}{y_1^n} \pmod{\ell}.$$

Then $E(\kappa)/\mathbb{F}_\ell$ is a quadratic twist of $F/\mathbb{F}_\ell$ and so $a_\ell(E(\kappa)) = \pm a_\ell(F)$. We conclude that $a_\ell(E(\kappa))^2 \equiv a_\ell(E_q)^2 \pmod{n}$.

Recall that $\ell = tn + 1$ and $h = g^n$, where g is a primitive root of $\mathbb{F}_\ell$. Observe that

$$4\kappa \equiv \frac{2^n y_2^n}{y_1^n} \equiv h^r \pmod{\ell},$$

for some $0 \le r \le t-1$. Moreover,

$$\kappa - 1 \equiv \frac{2^{n-2} y_2^n}{y_1^n} - 1 \equiv -\frac{q^k}{y_1^n} \not\equiv 0 \pmod{\ell}.$$

In particular, $\kappa \neq 1$ and so $\kappa \in \mathcal{X}_\ell$ and $q^k \cdot (\mathbb{F}_\ell^*)^n = (\kappa - 1) \cdot (\mathbb{F}_\ell^*)^n \in \mathcal{Y}_\ell$. Hence $s \in \phi^{-1}(\mathcal{Y}_\ell)$, where $s = \bar{k} \in \mathbb{Z}/n\mathbb{Z}$. Since k also satisfies (45), we conclude that $s \in \mathcal{Z}_\ell$. As this is true for $\ell = \ell_1, \ldots, \ell_t$, the element s belongs to the intersection (60) giving a contradiction. □

Corollary 10.2. *For $q \in \{31, 127, 257\}$ and prime n with $7 \leq n < 1.5 \times 10^6$, equation (7) has no solutions with $k \geq 1$ and $q \nmid x$.*

Proof. For $n \neq q$, we ran a short `Magma` script that searches for suitable primes ℓ_i and verifies the criterion of Lemma 10.1. This succeeded for all the primes $7 \leq n < 1.5 \times 10^6$ in a few minutes, except for $(q, n) = (31, 7)$. In this case, we found that $\bigcap \mathcal{Z}_{\ell_i} = \{\bar{1}\}$ no matter how many primes ℓ_i we chose. The reason for this is that there is a solution to (36) with $n = 7$ and $k = 1$, namely $(-1)^7 - 2^5 \cdot (-1)^7 = 31^1$.

In the case $n = q$, we are unable to appeal directly to Lemma 10.1 as we no longer necessarily have (45). We can, however, still derive a slightly weaker analogue of Lemma 10.1 with the $\mathcal{Z}_\ell$ replaced by the (typically) larger sets

$$\mathcal{Z}'_\ell = \phi^{-1}(\mathcal{Y}_\ell).$$

For $n = q$, we find that

$$\mathcal{Z}'_{311} \cap \mathcal{Z}'_{373} = \varnothing, \quad \mathcal{Z}'_{509} \cap \mathcal{Z}'_{2287} = \varnothing \quad \text{and} \quad \mathcal{Z}'_{1543} = \varnothing,$$

for $q = 31$, 127 and 257, respectively. □

To complete the proof of Theorem 5, it remains only to solve the Thue–Mahler equation

$$y_1^7 - 32 y_2^7 = 31^k.$$

Using the Magma implementation of [Gherga and Siksek 2022], we find that the only solution with k positive is with $k = 1$ and $y_1 = y_2 = -1$, corresponding to the solution $(q, k, y, n) = (31, 1, 2, 7)$ to (7).

11. The equation $x^2 + q^{2k+1} = y^n$ with y odd

In previous sections, we have completed the proofs of Theorems 4 and 5, therefore solving (8) with $3 \leq q < 1000$ prime, for even exponents α. The remainder of the paper is devoted to solving (8) for odd exponents α, and for the more modest range $3 \leq q < 100$. In this section, we focus on the equation

$$x^2 + q^{2k+1} = y^n, \quad x, y, k \text{ integers}, \ k \geq 0, \ \gcd(x, y) = 1, \ y \text{ odd}, \tag{61}$$

with exponent $n \geq 5$ prime; here $q \geq 3$ is prime.

Theorem 12 (Arif and Abu Muriefah). *Suppose $q \geq 3$ and $n \geq 5$ are prime, and that n does not divide the class number of $\mathbb{Q}(\sqrt{-q})$. Then the only solution to (61) corresponds to the identity*

$$22434^2 + 19 = 55^5. \tag{62}$$

Proof. The proof given by Arif and Abu Muriefah [2002] is somewhat lengthy and slightly incorrect. For the convenience of the reader we give a corrected and simplified proof. Let $M = \mathbb{Q}(\sqrt{-q})$ and suppose that n does not divide the class number of M. This and the assumptions in (61) quickly lead us to conclude that

$$x+q^k\sqrt{-q}=\alpha^n$$

for some $\alpha \in \mathcal{O}_M$ with $\mathrm{Norm}(\alpha)=y$. Thus

$$\alpha^n-\bar{\alpha}^n=2q^k\sqrt{-q}. \tag{63}$$

If $\alpha/\bar{\alpha}$ is a root of unity, then by the coprimality of α and $\bar{\alpha}$, we can conclude that α is a unit and so $y=1$ giving a contradiction. Thus $\alpha/\bar{\alpha}$ is not a root of unity. Therefore

$$u_m=\frac{\alpha^m-\bar{\alpha}^m}{\alpha-\bar{\alpha}}$$

is a Lucas sequence. Since $\alpha\bar{\alpha}=y$, we note that $\alpha\bar{\alpha}$ is coprime to $2q$. Suppose that the term u_n has a primitive divisor ℓ. By definition, this is a prime ℓ dividing u_n that does not divide $(\alpha-\bar{\alpha})^2\cdot u_1u_2\cdots u_{n-1}$. However $\alpha=u+v\sqrt{-q}$ or $\alpha=(u+v\sqrt{-q})/2$ where $u, v\in\mathbb{Z}$. Thus $(\alpha-\bar{\alpha})^2=-4q$ or $-q$, respectively. In particular $\ell\neq q$. It follows from (26) that $\ell=2$. By Theorem 7 and the primality of n, we have $n=m_2$, the rank of apparition of $\ell=2$ in the sequence u_n. Again by Theorem 7, $n=m_2=2$ or 3 contradicting our assumption that $n\geq 5$. It follows that u_n does not have a primitive divisor.

We now invoke the primitive divisor theorem (Theorem 6) to conclude that $n=5$ or 7 and that $(\alpha,\bar{\alpha})$ is equivalent to $((a-\sqrt{b})/2, (a+\sqrt{b})/2)$ where possibilities for (a,b) are given by (24) if $n=5$, and by (23) if $n=7$. For illustration, we take $n=5$ and $(a,b)=(12,-76)$. Thus $\alpha=(\pm 12\pm\sqrt{-76})/2=\pm 6\pm\sqrt{-19}$, whence $q=19$ and $y=\mathrm{Norm}(\alpha)=55$, quickly giving the solution in (62). The other possibilities for (a,b) in (23) and (24) do not yield solutions to (61). □

Corollary 11.1. *The only solutions to (61) with $3\leq q<100$ and $n\geq 5$ prime correspond to the identities*

$$22434^2+19=55^5, \quad 14^2+47=3^5 \quad \text{and} \quad 46^2+71=3^7.$$

Proof. Write h_q for the class number of $M=\mathbb{Q}(\sqrt{-q})$. Thanks to Theorem 12, if $n\nmid h_q$ then the only corresponding solution is $22434^2+19=55^5$. Thus we may suppose that $n\mid h_q$. The only values of q in our range with h_q divisible by a prime ≥ 5 are $q=47$, 71 and 79, where $h_q=5$, 7 and 5, respectively. We therefore reduce to considering the three cases $(q,n)=(47,5)$, $(71,7)$ and $(79,5)$, with $h_q=n$ in all three cases. From (61), we have

$$(x+q^k\sqrt{q})\cdot\mathcal{O}_M=\mathfrak{A}^n.$$

If $\mathfrak{A}$ is principal, then we are in the situation of the proof of Theorem 12 and we obtain a contradiction. Thus $\mathcal{A}$ is not principal. Now for the three quadratic fields under consideration the class group is generated by the class $[\mathfrak{P}]$ where

$$\mathfrak{P}=2\cdot\mathcal{O}_M+\frac{(1+\sqrt{-q})}{2}\cdot\mathcal{O}_M$$

is one of the two prime ideals dividing 2. We conclude that $[\mathfrak{A}] = [\mathfrak{P}]^{-r}$ for some $1 \le r \le n-1$. Observe that $\mathfrak{C}\overline{\mathfrak{C}}$ is principal for any ideal $\mathfrak{C}$ of $\mathcal{O}_M$, so $[\overline{\mathfrak{C}}] = [\mathfrak{C}]^{-1}$. We choose $\mathfrak{B} = \mathfrak{A}$ or $\overline{\mathfrak{A}}$ so that $[\mathfrak{B}] = [\mathfrak{P}]^{-r}$ where $1 \le r \le (n-1)/2$. We note that

$$(x \pm q^k \sqrt{-q}) \cdot \mathcal{O}_M = \mathfrak{B}^n = (\mathfrak{P}^{-n})^r \cdot (\mathfrak{P}^r \mathfrak{B})^n,$$

where the $\pm$ sign is $+$ if $\mathfrak{B} = \mathfrak{A}$ and $-$ if $\mathfrak{B} = \overline{\mathfrak{A}}$. We note that both $\mathfrak{P}^{-n}$ and $\mathfrak{P}^r\mathfrak{B}$ are principal. We find that $\mathfrak{P}^{-n} = 2^{-n-1}(u + v\sqrt{-q}) \cdot \mathcal{O}_M$ where u, v are given by

$$(u, v) = \begin{cases} (-9, 1) & \text{if } q = 47, \\ (-21, 1) & \text{if } q = 71, \\ (7, 1) & \text{if } q = 79. \end{cases}$$

The ideal $\mathfrak{P}^r\mathfrak{B}$ is integral as well as principal, and so has the form $(X' + Y'\sqrt{-q}) \cdot \mathcal{O}_M$ where X' and Y' are either both integers, or both halves of odd integers. We conclude that

$$2^{s+rn+r}(x \pm q^k \sqrt{-q}) = (u + v\sqrt{-q})^r \cdot (X + Y\sqrt{-q})^n,$$

where $X, Y \in \mathbb{Z}$ and $s = 0$ or n. Equating imaginary parts gives

$$G_r(X, Y) = \pm 2^{s+rn+r} q^k,$$

where $G_r \in \mathbb{Z}[X, Y]$ is a homogeneous polynomial of degree n. We solved this Thue–Mahler equation using the Thue–Mahler solver associated to the paper [Gherga and Siksek 2022], for each of our three pairs (q, n) and each $0 \le r \le (n-1)/2$. For illustration, we consider the case $q = 47$, $n = 5$, $r = 2$. Thus $(u, v) = (-9, 1)$. We find

$$G_2(X, Y) = 2(-9X^5 + 85X^4Y + 4230X^3Y^2 - 7990X^2Y^3 - 99405XY^4 + 37553Y^5)$$

and are therefore led to solve the Thue–Mahler equation

$$-9X^5 + 85X^4Y + 4230X^3Y^2 - 7990X^2Y^3 - 99405XY^4 + 37553Y^5 = \pm 2^j q^k.$$

We find that the solutions are

$$(X, Y, j, k) = (1, 1, 16, 0) \quad \text{and} \quad (-1, -1, 16, 0),$$

and compute $G_2(1, 1) = -2^{17}$, $G_2(-1, -1) = 2^{17}$. We note that $17 = n + rn + r$; therefore $s = n = 5$. We deduce that

$$x \pm 47^k \sqrt{-47} = \pm(-9 + \sqrt{-47})^2 \cdot (1 + \sqrt{-47})^5 = \pm(14 - \sqrt{-47}).$$

Thus $x = \pm 14$ and $k = 0$, giving the solution $14^2 + 47 = 3^5$. The other cases are similar. $\square$

12. The equation $x^2 + (-1)^\delta q^{2k+1} = y^5$

We will soon apply Frey–Hellegouarch curves to study the equation $x^2 + (-1)^\delta q^{2k+1} = y^n$ for prime exponents $n \geq 7$, and for q a prime in the range $3 \leq q < 100$. In Section 2, we have solved this equation for $n \in \{3, 4\}$. This leaves only the exponent $n = 5$ which we now treat through reduction to Thue–Mahler equations.

Lemma 12.1. *Let $3 \leq q < 100$ be a prime. The only solutions to the equation*

$$x^2 - q^{2k+1} = y^5, \quad x,\ y,\ k \text{ integers},\ k \geq 0,\ \gcd(x, y) = 1,$$

correspond to the identities

$$2^2 - 3 = 1^5, \quad 2^2 - 5 = (-1)^5, \quad 10^2 - 7^3 = (-3)^5, \quad 56^2 - 11 = 5^5, \quad 16^2 - 13 = 3^5,$$
$$4^2 - 17 = (-1)^5, \quad 7^2 - 17 = 2^5, \quad 6^2 - 37 = (-1)^5, \quad 3788^2 - 37 = 27^5,$$
$$3^2 - 41 = (-2)^5, \quad 411^2 - 41^3 = 10^5, \quad 11^2 - 89 = 2^5.$$

Proof. Let $M = \mathbb{Q}(\sqrt{q})$. For q in our range, the class number of M is 1, unless $q = 79$ in which case the class number is 3. Suppose first that y is odd. Then

$$(x + q^k\sqrt{q})\mathcal{O}_M = \mathfrak{A}^5,$$

where $\mathfrak{A}$ is an ideal of $\mathcal{O}_M$. Since the class number is not divisible by 5, we see that $\mathfrak{A}$ is principal and conclude that

$$x + q^k\sqrt{q} = \epsilon^r \cdot \alpha^5, \tag{64}$$

where ϵ is some fixed choice of a fundamental unit for M, $-2 \leq r \leq 2$, and $\alpha \in \mathcal{O}_M$. Note that

$$-x + q^k\sqrt{q} = \epsilon^{-r} \cdot \beta^5,$$

where β is one of $\pm\bar{\alpha}$. Thus we may, without loss of generality, suppose that $0 \leq r \leq 2$. The case $r = 0$ is easily shown not to lead to any solutions by following the approach in the proof of Theorem 12. Thus we suppose $r = 1$ or 2.

Let

$$\theta = \begin{cases} \sqrt{q} & \text{if } q \equiv 3 \pmod 4, \\ (1 + \sqrt{q})/2 & \text{if } q \equiv 1 \pmod 4. \end{cases}$$

Then $\{1, \theta\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_M$ and so we may write $\alpha = X + Y\theta$ where $X, Y \in \mathbb{Z}$. It follows that

$$\epsilon^r \cdot \alpha^5 = F_r(X, Y) + G_r(X, Y)\theta,$$

where F_r, G_r are homogeneous degree-5 polynomials in $\mathbb{Z}[X, Y]$. Equating the coefficients of θ in (64) yields the Thue–Mahler equations

$$G_r(X, Y) = \begin{cases} q^k & \text{if } q \equiv 3 \pmod 4, \\ 2q^k & \text{if } q \equiv 1 \pmod 4. \end{cases}$$

Solving these equations for prime $3 \le q < 100$ and for $r \in \{1, 2\}$ leads to the solutions given in the statement of the theorem with y odd.

Next we consider the case when y is even, so that $q \equiv 1 \pmod 8$. The possible values of q in our range are 17, 41, 73, 89 and 97 (where, in each case, M has class number 1). We can rewrite the equation $x^2 - q^{2k+1} = y^5$ as

$$\left(\frac{x + q^k\sqrt{q}}{2}\right)\left(\frac{x - q^k\sqrt{q}}{2}\right) = 2^3 y_1^5,$$

where $y_1 = y/2$. The two factors on the left-hand side are coprime. Let β be a generator of

$$\mathfrak{P} = 2\mathcal{O}_M + \left(\frac{1+\sqrt{q}}{2}\right) \cdot \mathcal{O}_M$$

which is one of the two prime ideals above 2. After possibly replacing x by $-x$ we obtain

$$\frac{x - q^k}{2} + q^k\theta = \frac{x + q^k\sqrt{q}}{2} = \epsilon^r \beta\alpha^5,$$

where $-2 \le r \le 2$. Writing $\alpha = X + Y\theta$ and equating the coefficients of θ on both sides gives, for each choice of q and r, a Thue–Mahler equation. Solving these leads to the solutions in the statement of the theorem with y even. □

Lemma 12.2. *Let $3 \le q < 100$ be a prime. The only solutions to the equation*

$$x^2 + q^{2k+1} = y^5, \quad x, y, k \textit{ integers}, \ k \ge 0, \ \gcd(x, y) = 1,$$

correspond to the identities

$$5^2+7=2^5, \quad 181^2+7=8^5, \quad 22434^2+19=55^5, \quad 3^2+23=2^5, \quad 1^2+31=2^5 \quad \textit{and} \quad 14^2+47=3^5.$$

Proof. By Corollary 11.1 we know that the only solutions when y is odd correspond to the identities $22434^2 + 19 = 55^5$ and $14^2 + 47 = 3^5$. Thus we may suppose y is even, and write $y = 2y_1$. It follows that $q = 7, 23, 31, 47, 71, 79$. Let $M = \mathbb{Q}(\sqrt{-q})$. Let $\theta = (1 + \sqrt{-q})/2$, so that $1, \theta$ is a $\mathbb{Z}$-basis for $\mathcal{O}_M$. Observe that

$$\left(\frac{x + q^k\sqrt{-q}}{2}\right)\left(\frac{x - q^k\sqrt{-q}}{2}\right) = 2^3 y_1^5,$$

where the two factors on the left-hand side generate coprime ideals. Let

$$\mathfrak{P} = 2\mathcal{O}_M + \theta \cdot \mathcal{O}_M;$$

this is one of the two primes above 2. Thus, after possibly changing the sign of x,

$$\left(\frac{x + q^k\sqrt{-q}}{2}\right) \cdot \mathcal{O}_M = \mathfrak{P}^3 \cdot \mathfrak{A}^5$$

for some ideal $\mathfrak{A}$ of $\mathcal{O}_M$. The class number of $\mathcal{O}_M$ is 1, 3, 3, 5, 7, 5 according to whether $q = 7, 23, 31, 47, 71, 79$. In all cases the class group is cyclic and generated by $[\mathfrak{P}]$. If $q = 47$ or 79 then the class number is 5, and so $\mathfrak{A}^5$ is principal. Hence $\mathfrak{P}^3$ is principal which is a contradiction. Thus there are no solutions for $q = 47$ or 79. Let

$$\mathfrak{C} = \begin{cases} 1 \cdot \mathcal{O}_M, & q = 7, 23, 31, \\ \mathfrak{P}^2, & q = 71. \end{cases}$$

Note that $\mathfrak{P}^3\mathfrak{C}^{-5}$ is principal and we write $\mathfrak{P}^3\mathfrak{C}^{-5} = (u + v\theta) \cdot \mathcal{O}_M$. Thus

$$\left(\frac{x + q^k\sqrt{-q}}{2}\right) \cdot \mathcal{O}_M = (u + v\theta) \cdot (\mathfrak{C}\mathfrak{A})^5.$$

As the class number is coprime to 5, we see that $\mathfrak{C}\mathfrak{A}$ is principal. Write $\mathfrak{C}\mathfrak{A} = (X + Y\theta) \cdot \mathcal{O}_K$. After possibly changing the signs of X, Y, we have

$$\frac{x - q^k}{2} + q^k\theta = \frac{x + q^k\sqrt{-q}}{2} = (u + v\theta)(X + Y\theta)^5.$$

Comparing the coefficients of θ yields a degree-5 Thue–Mahler equation. Solving these Thue–Mahler equations as before gives the claimed solutions with y even. □

13. Frey–Hellegouarch curves for a ternary equation of signature $(n, n, 2)$

In studying (7), we employed a factorization argument which reduced to (36) (which in turn we treated as a special case of a Fermat equation having signature (n, n, n)). In the remainder of the paper, we are primarily interested in the equation $x^2 + (-1)^\delta q^{2k+1} = y^n$, where q is a prime. We shall treat this, for prime $n \geq 7$, as a Fermat equation of signature $(n, n, 2)$ by rewriting this as $y^n + q^{2k+1}(-1)^{(\delta+1)n} = x^2$, a special case of

$$y^n + q^\alpha z^n = x^2, \quad \gcd(x, y) = 1. \tag{65}$$

Equation (65) has previously been studied by Ivorra and Kraus [2006], and by Bennett and Skinner [2004]. In this section, we recall some of these results and strengthen them slightly before specialising them to the case $z = \pm 1$ in forthcoming sections.

Theorem 13 (Ivorra and Kraus). *Suppose that q is a prime with the property that q cannot be written in the form*

$$q = |t^2 \pm 2^k|,$$

where t and k are integers, with $k = 0$, $k = 3$ or $k \geq 7$. Then there are no solutions to the Diophantine equation (65) in integers x, y, z, n and α with n prime satisfying

$$n > (\sqrt{8(q+1)} + 1)^{2(q-1)}. \tag{66}$$

To verify whether or not a given prime q can be written as $|t^2 - 2^k|$, an old result of Bauer and Bennett [2002] can be helpful. We have, from Corollary 1.7 of [Bauer and Bennett 2002], if t and k are positive integers with $k \geq 3$ odd,

$$|t^2 - 2^k| > 2^{13k/50},$$

unless

$$(t, k) \in \{(3, 3), (181, 15)\}.$$

In particular, a short computation reveals that Theorem 13 is applicable to the following primes $q < 100$:

$$q \in \{11, 13, 19, 29, 43, 53, 59, 61, 67, 83\}. \tag{67}$$

We shall make Theorem 13 more precise for these particular values of q. To this end we attach to a solution of (65) a certain Frey–Hellegouarch curve, following the recipes of Bennett and Skinner. If yz is even in (65), then we define, assuming, without loss of generality, that $x \equiv 1 \pmod 4$,

$$F : Y^2 + XY = X^3 + \left(\frac{x-1}{4}\right)X^2 + \frac{y^n}{64}X, \quad \text{if } y \text{ is even}, \tag{68}$$

and

$$F : Y^2 + XY = X^3 + \left(\frac{x-1}{4}\right)X^2 + \frac{q^\alpha z^n}{64}X, \quad \text{if } z \text{ is even}.$$

If, on the other hand, yz is odd, we define

$$F : Y^2 = X^3 + 2xX^2 + q^\alpha z^n X \tag{69}$$

or

$$F : Y^2 = X^3 + 2xX^2 + y^n X, \tag{70}$$

depending on whether $y \equiv 1 \pmod 4$ or $y \equiv -1 \pmod 4$, respectively. Let

$$\kappa = \begin{cases} 1 & \text{if } yz \text{ is even}, \\ 5 & \text{if } yz \text{ is odd}. \end{cases} \tag{71}$$

By the results of [Bennett and Skinner 2004], in each case, we may suppose that $n \nmid \alpha$ and that the mod n representation of F arises from a newform f of weight 2 and level $N = 2^\kappa \cdot q$. Let the q-expansion of f be given by (37). As before, we denote the Hecke eigenfield by $K_f = \mathbb{Q}(c_1, c_2, \dots)$ and its ring of integers by $\mathcal{O}_f$. In particular, there is a prime ideal $\mathfrak{n}$ of $\mathcal{O}_f$ such that (38) holds. Let $\ell \nmid 2q$ be prime and

$$T = \{a \in \mathbb{Z} \cap [-2\sqrt{\ell}, 2\sqrt{\ell}] : a \equiv 0 \pmod 2\}.$$

We write

$$\mathcal{D}'_{f,\ell} = ((\ell+1)^2 - c_\ell^2) \cdot \prod_{a \in T} (a - c_\ell),$$

and

$$\mathcal{D}_{f,\ell} = \begin{cases} \ell \cdot \mathcal{D}'_{f,\ell} & \text{if } K_f \neq \mathbb{Q}, \\ \mathcal{D}'_{f,\ell} & \text{if } K_f = \mathbb{Q}. \end{cases}$$

Lemma 13.1. *Let f be a newform of weight 2 and level $N = 2^\kappa \cdot q$. Let $\ell \nmid 2q$ be a prime. If $\bar{\rho}_{F,n} \sim \bar{\rho}_{f,\mathfrak{n}}$ then $\mathfrak{n} \mid \mathcal{D}_{f,\ell}$.*

Proof. The proof is almost identical to the proof of Lemma 8.2. The only difference is the definition of T which takes into account the fact F has a single rational point of order 2 instead of full 2-torsion. $\square$

The following is a slight refinement of Theorem 1.3 of [Bennett and Skinner 2004].

Proposition 13.2. *Suppose that q belongs to (67). Then there are no solutions to (65) in integers x, y, z, n and α with $\gcd(x, y) = 1$ and $n \geq 7$ prime, except, possibly, $n = 7$ and $q \in \{29, 43, 53, 59, 61\}$, or one of the following holds*:

- $q = 11,\ n = 7$ *and* $yz \equiv 1 \pmod 2$, *or*
- $q = 19,\ n = 7$ *and* $yz \equiv 1 \pmod 2$, *or*
- $q = 43,\ n = 11$ *and* $yz \equiv 1 \pmod 2$, *or*
- $q = 53,\ n = 17$ *and* $yz \equiv 1 \pmod 2$, *or*
- $q = 59,\ n = 11$ *and* $yz \equiv 0 \pmod 2$, *or*
- $q = 61,\ n = 13$ *and* $yz \equiv 1 \pmod 2$, *or*
- $q = 67,\ n \in \{7, 11, 13, 17\}$ *and* $yz \equiv 1 \pmod 2$, *or*
- $q = 83,\ n = 7$ *and* $yz \equiv 1 \pmod 2$.

Proof. For a weight-2 newform f of level N and primes $\ell_1, \dots, \ell_m$ (all coprime to $2q$), write $\mathcal{D}_{f,\ell_1,\dots,\ell_m}$ for the ideal of $\mathcal{O}_f$ generated by $\mathcal{D}_{f,\ell_1}, \dots, \mathcal{D}_{f,\ell_m}$. Let $\mathcal{B}_{f,\ell_1,\dots,\ell_m} \in \mathbb{Z}$ be the norm of the ideal $\mathcal{D}_{f,\ell_1,\dots,\ell_m}$. If $\bar{\rho}_{F,n} \sim \bar{\rho}_{f,\mathfrak{n}}$ then $\mathfrak{n} \mid \mathcal{D}_{f,\ell_1,\dots,\ell_m}$ by Lemma 13.1. Write $\mathcal{B}_{f,\ell_1,\dots,\ell_m} = \mathrm{Norm}(\mathcal{D}_{f,\ell_1,\dots,\ell_m})$. Thus $n \mid \mathcal{B}_{f,\ell_1,\dots,\ell_m}$. In our computations, we take $\ell_1, \dots, \ell_m$ to be the primes < 100 coprime to $2q$, and we let $\mathcal{B}_f = \mathcal{B}_{f,\ell_1,\dots,\ell_m}$. If $\mathcal{B}_f \neq 0$, then we certainly have a bound on n. If $\mathcal{B}_f$ is divisible only by primes ≤ 5, then we know that (38) does not hold for that particular f, and we can eliminate it from further consideration.

For primes q in (67), we apply this with newforms f of levels $N = 2^\kappa q$, $\kappa \in \{1, 5\}$. We obtain the desired conclusion that (65) has no solutions provided $n \geq 7$ is prime, unless $q \in \{29, 43, 53, 59, 61\}$ and $n = 7$, or (q, n, κ) is one of

$$(11, 7, 5),\quad (13, 7, 1),\quad (19, 7, 5),\quad (43, 11, 1),\quad (43, 11, 5),\quad (53, 17, 5),\quad (59, 11, 1),\quad (61, 31, 1),$$
$$(61, 13, 5),\quad (67, 17, 1),\quad (67, 7, 5),\quad (67, 11, 5),\quad (67, 13, 5),\quad (67, 17, 5),\quad (83, 7, 1),\quad (83, 7, 5).$$

We show that the triples $(13, 7, 1)$, $(43, 11, 1)$, $(61, 31, 1)$, $(67, 17, 1)$ and $(83, 7, 1)$ do not have corresponding solutions; the remaining triples lead to the noted possible exceptions. For illustration, take $q = 83$ and $\kappa = 1$, so that $N = 2 \times 83 = 166$. There are three conjugacy classes of weight-2 newforms of level N, which we denote by f_1, f_2, f_3, which respectively have Hecke eigenfields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\theta)$ where $\theta^3 - \theta^2 - 6\theta + 4 = 0$. We find

$$\mathcal{B}_{f_1} = 3^2 \times 5, \quad \mathcal{B}_{f_2} = 5, \quad \mathcal{B}_{f_3} = 7.$$

We therefore deduce that $f = f_3$ and $n = 7$. In fact, $\mathcal{D}_f = (7, 3 + \theta)$ is a prime ideal above 7, so we take $\mathfrak{n} = (7, 3 + \theta)$. A short calculation verifies the congruences in hypotheses (i) and (ii) of Theorem 8, whence $\ell + 1 \equiv c_\ell \pmod{\mathfrak{n}}$ for all ℓ with $\ell \nmid 2 \cdot 83$. It follows from Lemma 7.1 that

$$a_\ell(F) \equiv c_\ell \pmod{\mathfrak{n}}$$

for all primes ℓ of good reduction for F and hence $7 \mid (\ell + 1 - a_\ell(F))$ for all such primes ℓ of good reduction. This now implies that $\bar{\rho}_{F,7}$ is reducible [Serre 1975, IV-6], giving a contradiction.

We argue similarly for

$$(q, n, \kappa) = (13, 7, 1),\ (43, 11, 1),\ (61, 31, 1),\ (67, 17, 1).$$

In each case, Lemma 13.1 eliminates all but one class of newforms which are then treated via Theorem 8. □

For other odd primes $q < 100$, outside the set (67), we can, in certain cases, still show that (65) has no nontrivial solutions for suitably large n, under the additional assumption that $yz \equiv 0 \pmod 2$ or, for other q, under the assumption that $yz \equiv 1 \pmod 2$. To be precise, we have the following two propositions.

Proposition 13.3. *Suppose that $q \in \{3, 5, 37, 73\}$. Then there are no solutions to (65) in integers x, y, z, n and α with $yz \equiv 0 \pmod 2$, $\gcd(x, y) = 1$ and $n \geq 7$ prime, except, possibly, $(q, n) = (73, 7)$.*

Proposition 13.4. *Suppose that $q \in \{23, 31, 47, 71, 79, 97\}$. Then there are no solutions to (65) in integers x, y, z, n and α with $yz \equiv 1 \pmod 2$, $\gcd(x, y) = 1$ and $n \geq 7$ prime, except, possibly, $n = 7$ and $q \in \{23, 31, 47, 71, 97\}$, or $(q, n) = (79, 11)$, or $(q, n) = (97, 29)$.*

As in the case of Proposition 13.2, these results follow after a small amount of computation, by applying Lemma 13.1 and Theorem 8.

14. The equation $x^2 \pm q^{2k+1} = y^n$ and proofs of Theorems 2 and 3

We now specialize and improve on the results of Section 13, proving the following.

Proposition 14.1. *Let (x, y, k) be a solution to the equation*

$$x^2 + (-1)^\delta q^{2k+1} = y^n, \quad \delta \in \{0, 1\},\ k \geq 0,\ \gcd(x, y) = 1, \tag{72}$$

where q is a prime in the range $3 \leq q < 100$, and $n \geq 7$ is prime. Suppose, in addition, that

(a) *if y is odd then $\delta = 1$;*

(b) *if $\delta = 1$ then $q \notin \{3, 5, 17, 37\}$.*

If y is even, suppose, without loss of generality, that $x \equiv 1 \pmod 4$. Write

$$\kappa = \begin{cases} 1 & \text{if } y \text{ is even,} \\ 5 & \text{if } y \text{ is odd.} \end{cases} \tag{73}$$

Let $\upsilon \in \{0, 1\}$ satisfy $k \equiv \upsilon \pmod 2$. Attach to the solution (x, y, k) the Frey–Hellegouarch curve

$$G = G_{x,k} : \begin{cases} Y^2 = X^3 + 4xX^2 + 4(x^2 + (-1)^\delta q^{2k+1})X & \text{if } \kappa = 1, \\ Y^2 = X^3 - 4xX^2 + 4(x^2 + (-1)^\delta q^{2k+1})X & \text{if } \kappa = 5 \text{ and } q \equiv (-1)^\delta \bmod 4, \\ Y^2 = X^3 + 2xX^2 + (x^2 + (-1)^\delta q^{2k+1})X & \text{if } \kappa = 5 \text{ and } q \equiv (-1)^{\delta+1} \bmod 4. \end{cases}$$

q	δ	κ	v	E
7	0	1	0	14a1
7	0	1	1	14a1
23	0	1	0	46a1
31	0	1	0	62a1
31	0	1	1	62a1
41	1	1	0	82a1
41	1	5	0	1312a1, 1312b1
41	1	5	1	1312a1, 1312b1

q	δ	κ	v	E
47	0	1	0	94a1
71	0	1	0	142c1
71	0	1	1	142c1
73	1	5	0	2336a1, 2336b1
73	1	5	1	2336a1, 2336b1
79	0	1	0	158e1
89	1	1	0	178b1
97	1	1	0	194a1

Table 3. Data for Proposition 14.1. Here the elliptic curves E are given by their Cremona labels.

Then either $n > 1000$ and $\bar{\rho}_{G,n} \sim \bar{\rho}_{E,n}$ where $E/\mathbb{Q}$ is an elliptic curve of conductor $2^\kappa q$ given in Table 3 or the solution (x, y, k) corresponds to one of the identities

$$11^2 + 7 = 2^7, \quad 45^2 + 23 = 2^{11}, \quad 13^2 - 41 = 2^7, \quad 9^2 + 47 = 2^7,$$
$$7^2 + 79 = 2^7, \quad 91^2 - 89 = 2^{13}, \quad 15^2 - 97 = 2^7.$$

Before proving this result, we make a few remarks on the assumptions in Proposition 14.1. Our eventual goal is to prove Theorems 1, 2 and 3, and thus we are interested in the equation $x^2 + (-1)^\delta q^\alpha = y^n$ where $3 \le q < 100$. Theorems 4 and 5 (proved in Sections 5 and 10, respectively) treat the case where α is even, so we are reduced to $\alpha = 2k + 1$. The results of Section 2, Corollary 11.1 and Lemmas 12.1, 12.2 allow us to restrict the exponent n to be a prime ≥ 7. Thanks to Theorem 12, we need not consider the case where $\delta = 0$ and y is odd, which explains the reason for assumption (a). With a view to proving the proposition, we will soon provide a method which is usually capable, for a fixed q, δ and n, of showing that (72) does not have a solution. If $\delta = 1$, and q is one of the values 3, 5, 17 or 37, then there is a solution to (72) for all odd values of the exponent n:

$$2^2 - 3 = 1^n, \quad 2^2 - 5 = (-1)^n, \quad 4^2 - 17 = (-1)^n, \quad 6^2 - 37 = (-1)^n;$$

and so our method fails if $\delta = 1$ and q is one of these four values. This explains assumption (b) in the statement of the proposition.

We note that (72) is a special case of (65) with z specialised to the value $(-1)^{\delta+1}$, and with $\alpha = 2k+1$. The value κ in the statement of the proposition agrees with value for κ in (71) given in the previous section. We note that if y is odd, then $y \equiv (-1)^\delta \cdot q \pmod 4$. The Frey–Hellegouarch curve G is, up to isogeny, the same as the Frey–Hellegouarch curve F in the previous section, but is more convenient for our purposes. More precisely, the model G is isomorphic to F given in (68) if y even (i.e., $\kappa = 1$), and to F given in (70) if $y \equiv 3 \pmod 4$ (i.e., $\kappa = 5$ and $q \equiv (-1)^{\delta+1} \bmod 4$). It is 2-isogenous to F in (69) if $y \equiv 1 \pmod 4$ (i.e., $\kappa = 5$ and $q \equiv (-1)^\delta \bmod 4$). Thus $\bar{\rho}_{F,n} \sim \bar{\rho}_{G,n}$ in all three cases. We conclude from the previous section that $\bar{\rho}_{G,n} \sim \bar{\rho}_{f,\mathfrak{n}}$ where f is a weight-2 newform of level $N = 2^\kappa q$.

Note that if $\kappa = 1$ (that is, y is even) then $1 + (-1)^\delta q \equiv 0 \pmod 8$. This together with the assumptions of Proposition 14.1 shows that we are concerned with 30 possibilities for the triple (q, δ, κ), namely

$$\begin{gathered}(7,0,1),\ (7,1,5),\ (11,1,5),\ (13,1,5),\ (19,1,5),\ (23,0,1),\ (23,1,5),\ (29,1,5),\\ (31,0,1),\ (31,1,5),\ (41,1,1),\ (41,1,5),\ (43,1,5),\ (47,0,1),\ (47,1,5),\ (53,1,5),\\ (59,1,5),\ (61,1,5),\ (67,1,5),\ (71,0,1),\ (71,1,5),\ (73,1,1),\ (73,1,5),\ (79,0,1),\\ (79,1,5),\ (83,1,5),\ (89,1,1),\ (89,1,5),\ (97,1,1),\ (97,1,5).\end{gathered} \tag{74}$$

Bounding the exponent n. In the previous section we defined an ideal $\mathcal{D}_{f,\ell_1,\ldots,\ell_r}$ which if nonzero allows us to bound the exponent n in (65). That bound will also be valid for (72) since it is a special case of (65). We now offer a refinement that is often capable of yielding a better bound for (72).

Fix a triple (q, δ, κ) from the above list. We also fix $v \in \{0, 1\}$ and suppose that $k \equiv v \pmod 2$. Let f be a weight-2 newform of level $N = 2^\kappa q$ with q-expansion as in (37). Write K_f for the Hecke eigenfield of f, and $\mathcal{O}_f$ for the ring of integers of K_f. For a prime $\ell \neq 2, q$, define

$$\mathcal{S}_\ell = \{a_\ell(G_{w,v}) : w \in \mathbb{F}_\ell,\ w^2 + (-1)^\delta q^{2v+1} \not\equiv 0 \pmod \ell\}.$$

Let

$$\mathcal{T} = \mathcal{T}_\ell = \begin{cases} \mathcal{S}_\ell \cup \{\ell+1, -\ell-1\} & \text{if } (-1)^{\delta+1} q \text{ is a square modulo } \ell,\\ \mathcal{S}_\ell & \text{otherwise.}\end{cases}$$

Let

$$\mathcal{E}'_\ell = \prod_{a \in \mathcal{T}} (a - c_\ell) \quad \text{and} \quad \mathcal{E}_\ell = \begin{cases} \ell \cdot \mathcal{E}'_\ell & \text{if } K_f \neq \mathbb{Q},\\ \mathcal{E}'_\ell & \text{if } K_f = \mathbb{Q},\end{cases}$$

where, as before, c_ℓ is the ℓ-th coefficient in the q-expansion of f.

Lemma 14.2. *Let $\mathfrak{n}$ be a prime ideal of $\mathcal{O}_f$ above n. If $\bar\rho_{G,n} \sim \bar\rho_{f,\mathfrak{n}}$ then $\mathfrak{n} \mid \mathcal{E}_\ell$.*

Proof. Write $k = 2u + v$ with $u \in \mathbb{Z}$. Let $w \in \mathbb{F}_\ell$ satisfy $w \equiv x/q^{2u} \pmod \ell$. Hence

$$y^n = x^2 + (-1)^\delta q^{2k+1} \equiv q^{4u} \cdot (w^2 + (-1)^\delta q^{2v+1}) \pmod \ell.$$

It follows that $\ell \mid y$ if and only if $w^2 + (-1)^\delta q^{2v+1} \pmod \ell$. Suppose first that $\ell \nmid y$. The elliptic curves $G_{x,k}/\mathbb{F}_\ell$ and $G_{w,v}/\mathbb{F}_\ell$ are isomorphic, and so $a_\ell(G_{x,k}) = a_\ell(G_{w,v})$. In particular, $a_\ell(G_{x,k}) \in \mathcal{T}_\ell$ and so $a_\ell(G_{x,k}) - c_\ell$ divides $\mathcal{E}_\ell$. Likewise, if $\ell \mid y$ (which can only happen if $(-1)^{\delta+1} q$ is a square modulo ℓ) then $(\ell+1)^2 - c_\ell^2$ divides $\mathcal{E}_\ell$. The lemma follows from Lemma 7.1. □

A sieve. Lemma 14.2 will soon allow us to eliminate most possibilities for the newform f in a manner similar to Propositions 13.2, 13.3 and 13.4. We will still need to treat some cases for fixed exponent n. To this end, we will employ a sieving technique similar to the one in Section 10.

Fix a prime $n \geq 7$, and let $\mathfrak{n}$ be a prime ideal of $\mathcal{O}_f$ above n. Let $\ell \neq q$ be a prime. Suppose

(i) $\ell = tn + 1$ for some positive integer t;

(ii) either $\mathfrak{n} \nmid (4 - c_\ell^2)$, or $(-1)^{\delta+1} q$ is not a square modulo ℓ.

Let

$$\begin{aligned} A &= \{m \in \{0, 1, \ldots, 2n-1\} : m \equiv v \pmod 2,\ n \nmid (2m+1)\},\\ \mathcal{X}_\ell &= \{(z, m) \in \mathbb{F}_\ell \times A : (z^2 + (-1)^\delta q^{2m+1})^t \equiv 1 \pmod \ell\},\\ \mathcal{Y}_\ell &= \{(z, m) \in \mathcal{X}_\ell : a_\ell(G_{z,m}) \equiv c_\ell \pmod{\mathfrak{n}}\},\\ \mathcal{Z}_\ell &= \{m : \text{there exists } z \text{ such that } (z, m) \in \mathcal{Y}_\ell\}. \end{aligned}$$

Lemma 14.3. *Let $\ell_1, \ldots, \ell_r$ be primes $\neq q$ satisfying (i), (ii). Let*

$$\mathcal{Z}_{\ell_1,\ldots,\ell_r} = \bigcap_{i=1}^{r} \mathcal{Z}_{\ell_i}.$$

If $\bar\rho_{G,n} \sim \bar\rho_{f,\mathfrak{n}}$ then

$$(k \bmod 2n) \in \mathcal{Z}_{\ell_1,\ldots,\ell_r}.$$

Proof. Let m be the unique element of $\{0, 1, \ldots, 2n-1\}$ satisfying $k \equiv m \pmod{2n}$. Let $\ell \neq q$ be a prime satisfying (i) and (ii). It is sufficient to show that $m \in \mathcal{Z}_\ell$. First we will demonstrate that $\ell \nmid y$. If $(-1)^{\delta+1}q$ is not a square modulo ℓ then $\ell \nmid y$ from (72). Otherwise, by (ii), $\mathfrak{n} \nmid (4 - c_\ell^2)$. However, from (i) and the fact that $\mathfrak{n} \mid n$ we have $\ell + 1 \equiv 2 \pmod{\mathfrak{n}}$ and so $\mathfrak{n} \nmid ((\ell+1)^2 - c_\ell^2)$. It follows from Lemma 7.1 that ℓ is a prime of good reduction for $G_{x,k}$ and so $\ell \nmid y$. We deduce from Lemma 7.1 that $a_\ell(G_{x,k}) \equiv c_\ell \pmod{\mathfrak{n}}$.

In the previous section, we observed that $n \nmid \alpha$ in (65) thanks to the results of [Bennett and Skinner 2004], whence $n \nmid (2k+1)$. Since $k \equiv v \pmod 2$, we know that $m \in A$. Write $k = 2nb + m$ with b a nonnegative integer and let $z \in \mathbb{F}_\ell$ satisfy $z \equiv x/q^{2nb} \pmod \ell$. Then

$$z^2 + (-1)^\delta q^{2m+1} \equiv \frac{1}{q^{4nb}}(x^2 + (-1)^\delta q^{2k+1}) \equiv \left(\frac{y}{q^{4b}}\right)^n \pmod \ell.$$

From (i), we deduce that

$$(z^2 + (-1)^\delta q^{2m+1})^t \equiv \left(\frac{y}{q^{4b}}\right)^{\ell-1} \equiv 1 \pmod \ell.$$

Thus $(z, m) \in \mathcal{X}_\ell$. Moreover, we have that $G_{x,k}/\mathbb{F}_\ell$ and $G_{z,m}/\mathbb{F}_\ell$ are isomorphic elliptic curves, whence $a_\ell(G_{z,m}) = a_\ell(G_{x,k}) \equiv c_\ell \pmod{\mathfrak{n}}$. Thus $(z, m) \in \mathcal{Y}_\ell$ and so $m \in \mathcal{Z}_\ell$ as required. □

Remarks. We would like to explain how to compute $\mathcal{Z}_\ell$ efficiently, given n and ℓ.

(1) In our computations, the value t will be relatively small compared to n and to $\ell = tn + 1$. Let g be a primitive root modulo ℓ (that is, a cyclic generator for $\mathbb{F}_\ell^\times$), and let $h = g^n$. The set $\mathcal{X}_\ell$ consists of pairs $(z, m) \in \mathbb{F}_\ell \times A$ such that $(z^2 + (-1)^\delta q^m)^t \equiv 1 \pmod \ell$. Hence $z^2 + (-1)^\delta q^m$ is one of the values $1, h, h^2, \ldots, h^{t-1}$. Thus, to compute $\mathcal{X}_\ell$, we run through $i = 0, 1, \ldots, t-1$ and $m \in A$ and solve $z^2 = h^i - (-1)^\delta q^m$. We note that the expected cardinality of $\mathcal{X}_\ell$ should be roughly $t \times \#A \approx t \times n \approx \ell$.

(2) It seems at first that, in order to compute $\mathcal{Y}_\ell$ and $\mathcal{Z}_\ell$, we need to compute $a_\ell(G_{z,m})$ for all $(z, m) \in \mathcal{X}_\ell$, and this might be an issue for large ℓ. There is in fact a shortcut that often means that we only need to

perform a few of these computations. In fact we will need to compute $\mathcal{Z}_\ell$ for large values of ℓ only for rational newforms f that correspond to elliptic curves $E/\mathbb{Q}$ with nontrivial 2-torsion. In this case, we note that $a_\ell(G_{z,m}) \equiv a_\ell(E) \pmod 2$, as both elliptic curves have nontrivial 2-torsion. If $(z, m) \in \mathcal{Y}_\ell$, then $a_\ell(G_{z,m}) \equiv a_\ell(E) \pmod{2n}$. However, by the Hasse–Weil bounds,

$$|a_\ell(G_{z,m}) - a_\ell(E)| \le 4\sqrt{\ell}.$$

Suppose, in addition, that $n^2 > 4\ell$ (which will be usually satisfied as t is typically small). Then, the congruence $a_\ell(G_{z,m}) \equiv c_\ell = a_\ell(E) \pmod{2n}$ is equivalent to the equality $a_\ell(G_{z,m}) = a_\ell(E)$, and so to $\#G_{z,m}(\mathbb{F}_\ell) = \#E(\mathbb{F}_\ell)$. To check whether the equality $\#G_{z,m}(\mathbb{F}_\ell) = \#E(\mathbb{F}_\ell)$ holds for a particular pair $(z, m) \in \mathcal{X}_\ell$, we first choose a random point $Q \in G_{z,m}(\mathbb{F}_\ell)$ and check whether $\#E(\mathbb{F}_\ell) \cdot Q = 0$. Only for pairs $(z, m) \in \mathcal{X}_\ell$ that pass this test do we need to compute $a_\ell(G_{z,m})$ and check the congruence $a_\ell(G_{z,m}) \equiv a_\ell(E) \pmod n$.

A refined sieve. We note that if $\mathcal{Z}_{\ell_1,\dots,\ell_r} = \varnothing$ then $\bar{\rho}_{G,n} \not\sim \bar{\rho}_{f,\mathfrak{n}}$. In our computations, described later, we are always able to find suitable primes $\ell_1, \dots, \ell_r$ satisfying (i), (ii), so that $\mathcal{Z}_{\ell_1,\dots,\ell_r} = \varnothing$, at least for n suitably large. For smaller values of n (say less than 50), we occasionally failed. We now describe a refined sieving method that, whilst being somewhat slow, has a better chance of succeeding for those smaller values of the exponent n.

Let (q, δ, κ) be one of our 30 triples given in (74), and let $n \ge 7$ be a prime. Suppose that (x, y, k) is a solution to (72) where y is even if and only if $\kappa = 1$. Let $\phi = \sqrt{(-1)^{\delta+1} q}$ and set $M = \mathbb{Q}(\phi)$. Let $\mathfrak{P}$ be one of the prime ideals of $\mathcal{O}_M$ above 2.

Our first goal is to produce a finite set $\mathcal{S} \subset M^*$, such that

$$x + q^k \phi = \gamma \cdot \alpha^n \tag{75}$$

for some $\gamma \in \mathcal{S}$ and $\alpha \in \mathcal{O}_M$. This is the objective of Lemmata 14.4 and 14.5. Both of these make an additional assumption on the class group, but this assumption will in fact be satisfied in all cases where we need to apply our refined sieve.

Lemma 14.4. *Let $\kappa = 5$. Suppose that the class group $\mathrm{Cl}(\mathcal{O}_M)$ of $\mathcal{O}_M$ is cyclic and generated by the class $[\mathfrak{P}]$. Let $h = \#\mathrm{Cl}(\mathcal{O}_M)$ and set*

$$\mathcal{I} = \{0 \le i \le h-1 : \mathfrak{P}^{-ni} \text{ is principal}\}.$$

Choose for each $i \in \mathcal{I}$ a generator β_i for $\mathfrak{P}^{-ni}$. Let ϵ be a fundamental unit for M (recall that if $\kappa = 5$ then $\delta = 1$ and so M is real). Let

$$\mathcal{S} = \left\{ \epsilon^j \beta_i : -\frac{n-1}{2} \le j \le \frac{n-1}{2},\, i \in \mathcal{I} \right\}.$$

Then there is some $\gamma \in \mathcal{S}$ and $\alpha \in \mathcal{O}_M$ such that (75) holds. Also, $\mathrm{Norm}(\alpha) = 2^\mu y$ *for some $\mu \ge 0$.*

Proof. As $\kappa = 5$, we have that y is odd. Then

$$(x + q^k \phi)\mathcal{O}_M = \mathfrak{A}^n,$$

where $\mathfrak{A}$ is an ideal of $\mathcal{O}_M$ with norm y. Since $[\mathfrak{P}]$ generates the class group, the same is true of $[\mathfrak{P}]^{-1}$. Hence $[\mathfrak{A}] = [\mathfrak{P}]^{-i}$ for some $i \in \{0, 1, \dots, h-1\}$. Now

$$(x + q^k\theta)\mathcal{O}_M = \mathfrak{P}^{-ni} \cdot (\mathfrak{P}^i \cdot \mathfrak{A})^n.$$

Since $\mathfrak{P}^i \cdot \mathfrak{A}$ is principal, it follows that $\mathfrak{P}^{-ni}$ is also principal. The lemma follows. □

Lemma 14.5. *Let $\kappa = 1$. Suppose that the class group $\mathrm{Cl}(\mathcal{O}_M)$ of $\mathcal{O}_M$ is cyclic and generated by the class $[\mathfrak{P}]$. Let $h = \#\mathrm{Cl}(\mathcal{O}_M)$ and set*

$$\mathcal{I} = \{0 \le i \le h-1 : \mathfrak{P}^{n(1-i)-2} \text{ is principal}\}.$$

Choose for each $i \in \mathcal{I}$ a generator β_i for $\mathfrak{P}^{n(1-i)-2}$. Let

$$\mathcal{S}' = \{\beta_i : i \in \mathcal{I}\} \cup \{\overline{\beta_i} : i \in \mathcal{I}\},$$

where $\overline{\beta_i}$ denotes the Galois conjugate of β_i. Let

$$\mathcal{S} = \begin{cases} \{2 \cdot \beta : \beta \in \mathcal{S}'\} & \text{if } \delta = 0, \\ \{2 \cdot \epsilon^j \cdot \beta : -(n-1)/2 \le j \le (n-1)/2,\ \beta \in \mathcal{S}'\} & \text{if } \delta = 1, \end{cases}$$

where ϵ is a fundamental unit for M. Then there is some $\gamma \in \mathcal{S}$ and $\alpha \in \mathcal{O}_M$ such that (75) holds. Also, $\mathrm{Norm}(\alpha) = 2^\mu y$ for some $\mu \in \mathbb{Z}$.

Proof. As $\kappa = 1$, we have that y is even. Then

$$\left(\frac{x + q^k\phi}{2}\right)\mathcal{O}_M = \mathfrak{C}^{n-2}\mathfrak{A}^n,$$

where $\mathfrak{A}$ is an ideal of $\mathcal{O}_M$ with norm $y/2$ and $\mathfrak{C}$ is one of $\mathfrak{P}$, $\overline{\mathfrak{P}}$. Since $[\mathfrak{P}]$ generates the class group so does $[\mathfrak{C}]^{-1}$. Hence $[\mathfrak{A}] = [\mathfrak{C}]^{-i}$ for some $i \in \{0, 1, \dots, h-1\}$. Now

$$\left(\frac{x + q^k\phi}{2}\right)\mathcal{O}_M = \mathfrak{C}^{n(1-i)-2} \cdot (\mathfrak{C}^i\mathfrak{A})^n.$$

But $\mathfrak{C}^i \cdot \mathfrak{A}$ is principal, whence $\mathfrak{C}^{n(1-i)-2}$ is principal, and so $i \in \mathcal{I}$ and $\mathfrak{C}^{n(1-i)-2}$ is generated by either β_i or $\overline{\beta_i}$. The lemma follows. □

We will now describe our refined sieve. Fix $m \in \{0, 1, \dots, 2n\}$ and suppose $k \equiv m \pmod{2n}$. Let $\mathfrak{n}$ be a prime ideal of $\mathcal{O}_f$ above n. Let $\ell \ne q$ be a prime. Suppose

(a) $\ell = tn + 1$ for some positive integer t;

(b) $\mathfrak{n} \nmid (4 - c_\ell^2)$;

(c) $(-1)^{\delta+1}q$ is a square modulo ℓ.

We choose an integer s such that $s^2 \equiv (-1)^{\delta+1}q \pmod{\ell}$. Let

$$\mathfrak{L} = \ell\mathcal{O}_M + (s - \phi)\mathcal{O}_M.$$

By the Dedekind–Kummer theorem ℓ splits in $\mathcal{O}_M$ and $\mathfrak{L}$ is one of the two prime ideals above ℓ. In particular, $\mathcal{O}_M/\mathfrak{L} \cong \mathbb{F}_\ell$ and $\phi \equiv s \pmod{\mathfrak{L}}$. Let

$$\begin{aligned}
\mathcal{X}_{\ell,m} &= \{z \in \mathbb{F}_\ell : (z^2+(-1)^\delta q^{2m+1})^t \equiv 1 \pmod{\ell}\},\\
\mathcal{Y}_{\ell,m} &= \{z \in \mathcal{X}_{\ell,m} : a_\ell(G_{z,m}) \equiv c_\ell \pmod{\mathfrak{n}}\},\\
\mathcal{U}_{\ell,m} &= \{(z,\gamma) : z \in \mathcal{Y}_{\ell,m},\, \gamma \in \mathcal{S},\, (z+q^m\phi)^t \equiv \gamma^t \pmod{\mathfrak{L}}\},\\
\mathcal{W}_{\ell,m} &= \{\gamma : \text{there exists } z \text{ such that } (z,\gamma) \in \mathcal{U}_{\ell,m}\}.
\end{aligned}$$

Lemma 14.6. *Let $\ell_1, \dots, \ell_r$ be primes $\neq q$ satisfying (a), (b) and (c) above. Let*

$$\mathcal{W} = \mathcal{W}_{\ell_1,\dots,\ell_r} = \bigcap_{i=1}^{r} \mathcal{W}_{\ell_i}.$$

If $\bar{\rho}_{G,n} \sim \bar{\rho}_{f,\mathfrak{n}}$, then there is some $\gamma \in \mathcal{W}$ and some $\alpha \in \mathcal{O}_M$ such that (75) holds.

Proof. Suppose ℓ satisfies conditions (a), (b) and (c). As ℓ satisfies (a) and (b), it also satisfies hypotheses (i) and (ii) preceding the statement of Lemma 14.3. Write $k = 2nb + m$ where b is a nonnegative integer, and let $z \equiv x/q^{2nb} \pmod{\ell}$. It follows from the proof of Lemma 14.3 that $\ell \nmid y$ and that $z \in \mathcal{Y}_{\ell,m}$. We know from Lemmata 14.4 and 14.5 that there is some $\gamma \in \mathcal{S}$ such that $x + q^k\phi = \gamma\alpha^n$ where $\alpha \in \mathcal{O}_M$ satisfies $\mathrm{Norm}(\alpha) = 2^\mu y$ for some $\mu \in \mathbb{Z}$. Note that γ is supported only on the prime ideals above 2. Since $\mathfrak{L} \mid \ell$, we have $\mathrm{ord}_{\mathfrak{L}}(\alpha) = \mathrm{ord}_{\mathfrak{L}}(\gamma) = 0$. Hence

$$z + q^m\phi \equiv \frac{1}{q^{2nb}}(x + q^k\phi) \equiv \gamma \cdot \left(\frac{\alpha}{q^{2b}}\right)^n \pmod{\mathcal{L}}.$$

Since $(\mathcal{O}_M/\mathcal{L})^* \cong \mathbb{F}_\ell^*$ is cyclic of order $\ell - 1 = tn$, we have

$$(z + q^m\phi)^t \equiv \gamma^t \pmod{\mathcal{L}}.$$

Thus $(z,\gamma) \in \mathcal{U}_{\ell,m}$ and hence $\gamma \in \mathcal{W}_{\ell,m}$. The lemma follows. ☐

Proof of Proposition 14.1. Our proof of Proposition 14.1 is the result of applying `Magma` scripts based on Lemmata 14.2, 14.3 and 14.6, as well as solving a few Thue–Mahler equations. Our approach subdivides the proof into 60 cases corresponding to 60 quadruples $(q, \delta, \kappa, \upsilon)$: here (q, δ, κ) is one of the 30 triples in (74), and $\upsilon \in \{0, 1\}$. Let (x, y, k) be a solution to (72) with prime exponent $n \geq 7$. Suppose that y is even if $\kappa = 1$ and y is odd if $\kappa = 5$. Suppose, in addition, that $k \equiv \upsilon \pmod 2$. Our first step is to compute the newforms f of weight 2 and level $N = 2^\kappa q$. We know that for one these newforms f, we have $\bar{\rho}_{G,n} \sim \bar{\rho}_{f,\mathfrak{n}}$ where $G = G_{x,k}$ is the Frey–Hellegouarch curve given in Proposition 14.1, and $\mathfrak{n} \mid n$ is a prime ideal of $\mathcal{O}_f$, the ring of integers of the Hecke eigenfield K_f. Let $p_1, \dots, p_s$ be the primes ≤ 200 distinct from 2 and q, and let

$$\mathcal{E}_f = \sum_{i=1}^{s} \mathcal{E}_{p_i},$$

where $\mathcal{E}_{p_i}$ is as in Lemma 14.2. It follows from Lemma 14.2 that if $\bar{\rho}_{G,n} \sim \bar{\rho}_{f,\mathfrak{n}}$ then $\mathfrak{n} \mid \mathcal{E}_f$, and so $n \mid \mathrm{Norm}(\mathcal{E}_f)$.

We illustrate this by taking $(q, \delta, \kappa, v) = (31, 1, 5, 0)$. There are 8 newforms $f_1, \ldots, f_8$ of weight 2 and level $2^\kappa q = 992$, which all happen to be irrational. We find that

$$\mathrm{Norm}(\mathcal{E}_{f_j}) = 7,\ 7,\ 2^{10},\ 2^{10},\ 2^3,\ 2^3,\ 2^6 \times 3^2,\ 2^6 \times 3^2,$$

respectively for $j = 1, 2, \ldots, 8$. Thus $n = 7$ and $f = f_1$ or f_2. We consider first

$$f = f_1 = \mathfrak{q} + \sqrt{2}\mathfrak{q}^3 - \mathfrak{q}^5 - (1+\sqrt{2})\mathfrak{q}^7 - \mathfrak{q}^9 + 2(1-\sqrt{2})\mathfrak{q}^{11} + \cdots,$$

with Hecke eigenfield $K_f = \mathbb{Q}(\sqrt{2})$ having ring of integers $\mathcal{O}_f = \mathbb{Z}[\sqrt{2}]$. We found that $\mathcal{E}_f = (1+2\sqrt{2})$ which is one of the two prime ideals above 7. Hence $\mathfrak{n} = (1+2\sqrt{2})$. Next we compute $\mathcal{Z} = \mathcal{Z}_{\ell_1,\ldots,\ell_{30}}$ as in Lemma 14.3 where $\ell_1, \ldots, \ell_{30} \neq 31$ are the 30 primes satisfying (i) and (ii) with $t \leq 200$. We find that $\mathcal{Z} = \{0, 8\}$. Thus, by Lemma 14.3, we have $k \equiv 0$ or $8 \pmod{14}$. Now for $m = 0$ and $m = 8$, we compute $\mathcal{W} = \mathcal{W}_{\ell_1,\ldots,\ell_{36}}$ as in Lemma 14.6, where $\ell_1, \ldots, \ell_{36} \neq 31$ are the 36 primes satisfying (a), (b) and (c) with $t \leq 800$. We found that $\mathcal{W} = \varnothing$ for $m = 0$ and that $\mathcal{W} = \{\epsilon^3\}$ for $m = 8$ where $\epsilon = 1520 + 273\sqrt{31}$ is the fundamental unit of $M = \mathbb{Q}(\sqrt{31})$. Hence we conclude, by Lemma 14.6, that $k \equiv 8 \pmod{14}$ and that

$$x + 31^k\sqrt{31} = (1520 + 273\sqrt{31})^3 (X + Y\sqrt{31})^7,$$

for some integers X, Y. Equating the coefficients of $\sqrt{31}$ on both sides results in a degree-7 Thue–Mahler equation with huge coefficients. However, using an algorithm of Stoll and Cremona [2003] for reducing binary forms we discover that this Thue–Mahler equation can be rewritten as

$$31^k = -56U^7 + 112U^6V - 84U^5V^2 + 140U^4V^3 + 490U^3V^4 + 1596U^2V^5 + 2807UV^6 + 2119V^7,$$

where $U, V \in \mathbb{Z}$ are related to X, Y via the unimodular substitution

$$U = 2X + 11Y \quad \text{and} \quad V = 7X + 39Y.$$

We applied the Thue–Mahler solver to this and found that it has no solutions. Next we take $f = f_2$ which also has Hecke eigenfield $K_f = \mathbb{Q}(\sqrt{2})$. We apply Lemmata 14.2, 14.3 and 14.6 using the same sets of primes p_j and ℓ_i as for f_1. We find $\mathcal{E}_f = (1-2\sqrt{2})$, and so $\mathfrak{n} = (1-2\sqrt{2})$ and $n = 7$. Again we obtain $\mathcal{Z} = \{0, 8\}$ on applying Lemma 14.3. We find that $\mathcal{W} = \varnothing$ for $m = 0$ and $\mathcal{W} = \{\bar{\epsilon}^3\}$ for $m = 8$. Again the corresponding Thue–Mahler equation has no solutions. Thus (72) has no solutions with $n \geq 7$ prime for $q = 31$, $\delta = 1$ and with y odd (i.e., $\kappa = 5$) and $k \equiv 0 \pmod 2$. We used the above approach to deal with all the cases where $\mathcal{E}_f$ is nonzero. In all the cases where $\mathcal{E}_f = 0$, the newform f is rational, and in fact corresponds to an elliptic curve $E/\mathbb{Q}$ with nontrivial 2-torsion. These elliptic curves are listed in Table 3. Thus $\bar{\rho}_{G,n} \sim \bar{\rho}_{E,n}$. What is required for Proposition 14.1 is to show in these cases that there are no solutions with prime $7 \leq n < 1000$ apart from the ones listed in the statement of the proposition. We illustrate how this works by taking $(q, \delta, \kappa, v) = (7, 0, 1, 0)$. There is a unique newform f of weight 2

n	$\mathcal{Z}$
7	$\{0, 8, 12\}$
11	$\{8\}$
13	$\{4\}$
41	$\{44\}$
other values	$\varnothing$

Table 4. For the quadruple $(q, \delta, \kappa, v) = (7, 0, 1, 0)$ and for prime $7 \le n < 1000$ we computed $\mathcal{Z} = \mathcal{Z}_{\ell_1,\dots,\ell_r}$ as given by Lemma 14.3. Here we chose $\ell_1, \dots, \ell_r$ to be the primes $\neq q$ satisfying (i) and (ii) with $t \le 200$.

and level $N = 2^\kappa q = 14$ which corresponds to the elliptic curve

$$Y^2 + XY + Y = X^3 + 4X - 6$$

with Cremona label `14a1`. For each prime $7 \le n < 1000$ we computed $\mathcal{Z} = \mathcal{Z}_{\ell_1,\dots,\ell_r}$ with $\ell_1, \dots, \ell_r$ being the primes $\neq 7$ satisfying conditions (i), (ii) with $t \le 200$. The results of this computation are summarized in Table 4. Note that by Lemma 14.3, $(k \pmod{2n}) \in \mathcal{Z}$. We deduce that there are no solutions for prime n satisfying $17 \le n < 1000$, $n \neq 41$. For $n = 7$, 11, 13 and 41, and for each m in the corresponding $\mathcal{Z}$, we compute $\mathcal{W} = \mathcal{W}_{\ell_1,\dots,\ell_r}$ as in Lemma 14.6 where $\ell_1, \dots, \ell_r$ are now the primes $\neq q$ satisfying (a), (b) and (c) with $t \le 800$. We found that $\mathcal{W} = \varnothing$ in all cases except for $n = 7$, $m = 0$, when $\mathcal{W} = 11 - \sqrt{-7}$. It follows from Lemma 14.6 that $x + 7^k\sqrt{-7} = (11 - \sqrt{-7}) \cdot \alpha^7$ where $\alpha \in \mathbb{Z}[\theta]$ where $\theta = (1 + \sqrt{-7})/2$. Write $\alpha = (X + Y\theta)$ with $X, Y \in \mathbb{Z}$. Thus

$$\frac{x - 7^k}{2} + 7^k \cdot \theta = (6 - \theta) \cdot (X + Y\theta)^7.$$

Equating the coefficients of θ on either side yields the Thue–Mahler equation

$$-X^7 + 35X^6Y + 147X^5Y^2 - 105X^4Y^3 - 595X^3Y^4 - 231X^2Y^5 + 161XY^6 + 45Y^7 = 7^k.$$

We find that the only solution is $(X, Y, k) = (-1, 0, 0)$. Hence $x = -11$, and the corresponding solution to (72) is $11^2 + 7 = 2^7$. We observe that $-11 \equiv 1 \pmod 4$ which is consistent with our assumption $x \equiv 1 \pmod 4$ if $\kappa = 1$, made in the statement of Proposition 14.1. The other cases are similar.

Proofs of Theorems 2 and 3. We now deduce Theorems 2 and 3 from Proposition 14.1. These two theorems concern the equation $x^2 - q^{2k+1} = y^n$ with $n \ge 3$ and $q \nmid x$. Thus we are in the $\delta = 1$ case of the proposition. By the remarks following the statement of the proposition we are reduced to the case $n \ge 7$ is prime. Theorem 2 is concerned with the primes q appearing in (4), whilst Theorem 3 deals with $q = 41$, 73, 89 and 97. A glance at Table 3 reveals that all the elliptic curves E appearing in Proposition 14.1 for the case $\delta = 1$ in fact correspond to the values $q = 41$, 73, 89 and 97. Theorems 2 and 3 now follow immediately from the proposition.

n	$\{\ell_1, \dots, \ell_r\}$	time (seconds)
$2^{10} + 7 = 1031$	{2063, 12373, 30931}	0.18
$2^{11} + 5 = 2053$	{94439, 110863, 143711, 168347, 197089}	7.75
$2^{12} + 3 = 4099$	{73783, 98377, 114773}	4.39
$2^{13} + 17 = 8209$	{246271, 525377, 574631}	15.50
$2^{14} + 27 = 16411$	{98467, 459509, 590797}	6.19
$2^{15} + 3 = 32771$	{65543, 983131, 1179757}	3.91
$2^{16} + 1 = 65537$	{917519, 1310741, 1703963, 2359333}	57.51
$2^{17} + 29 = 131101$	{2097617, 9439273, 11799091, 12585697}	142.59
$2^{18} + 3 = 262147$	{1048589, 4194353, 6291529}	65.89
$2^{19} + 21 = 524309$	{6291709, 10486181, 23069597}	402.12
$2^{20} + 7 = 1048583$	{20971661, 25165993, 44040487}	1319.57
$2^{21} + 17 = 2097169$	{37749043, 176162197, 188745211}	2468.46
$2^{22} + 15 = 4194319$	{75497743, 92275019, 100663657}	4983.07

Table 5. Write n_u for the smallest prime $> 2^u$. For $10 \le u \le 22$ the prime $n = n_u$ belongs to the range $1000 < n < 6 \times 10^6$. The table lists the primes $n = n_u$ in this range and, for each, a set of primes $\ell_1, \dots, \ell_r$ satisfying conditions (i), (ii) such that $\mathscr{Z}_{\ell_1,\dots,\ell_r} = \varnothing$. It also records the time the computation took for each of these values of n, on a single processor.

Remark. It is well-known that the exponent n can be explicitly bounded in (72) in terms of the prime q. For example, if $\delta = 1$ and $\kappa = 5$ (i.e., y is odd) then Bugeaud [1997] showed that

$$n \le 4.5 \times 10^6 q^2 \log^2 q. \tag{76}$$

Let $(q, \delta, \kappa, v) = (73, 1, 5, 1)$ and E be the elliptic curve with Cremona label `2336a1`; this is one of the two outstanding cases from Table 3 for which the bound (76) is applicable. We are in fact able to substantially improve this bound for the case in consideration through a specialization and minor refinement (we omit the details) of Bugeaud's approach and deduce that

$$n < 6 \times 10^6.$$

Theorem 3 only resolves $x^2 - 73^{2k+1} = y^n$ for $3 \le n \le 1000$. It is natural to ask whether we can apply the same technique, namely Lemma 14.3, to show that there are no solutions for prime exponents n in the range $1000 < n < 6 \times 10^6$. Write n_u for the smallest prime $> 2^u$. For $10 \le u \le 22$ the prime $n = n_u$ belongs to the range $1000 < n < 6 \times 10^6$. For each of these 13 primes we computed primes $\ell_1, \dots, \ell_r$ satisfying conditions (i) and (ii) such that $\mathscr{Z}_{\ell_1,\dots,\ell_r} = \varnothing$, whence by Lemma 14.3 there are no solutions for that particular exponent n. Table 5 records the values of $\ell_1, \dots, \ell_r$ as well as the time taken to perform the corresponding computation in `Magma` on a single processor. There are 412681 primes in the range $1000 < n < 6 \times 10^6$. On the basis of the timing in the table we crudely estimate that it would take around 60 years to carry out the computation (on a single processor) for all 412681 primes.

q	Cremona label for E	minimal model for E
7	14a1	$Y^2+XY+Y=X^3+4X-6$
23	46a1	$Y^2+XY=X^3-X^2-10X-12$
31	62a1	$Y^2+XY+Y=X^3-X^2-X+1$
47	94a1	$Y^2+XY+Y=X^3-X^2-1$
71	142c1	$Y^2+XY=X^3-X^2-X-3$
79	158e1	$Y^2+XY+Y=X^3+X^2+X+1$

Table 6. Elliptic curve E of conductor $2q$ and nontrivial 2-torsion.

We shall shortly give a substantially faster method for treating the case $\delta=0$. Alas this method is not available for $\delta=1$, as we explain in due course.

15. The proof of Theorem 1: large exponents

We now complete the proof of Theorem 1 which is concerned, for prime $3\le q<100$, with the equation

$$x^2+q^\alpha=y^n,$$

subject to the assumptions that $q\nmid x$ and $n\ge 3$. The exponents $n=3$ and $n=4$ were treated in Section 2, so we may suppose that $n\ge 5$ is prime. The case $\alpha=2k$ was handled in Section 5, so we suppose further that $\alpha=2k+1$. The case with y odd was the topic of Section 11, so we may assume that y is even. Finally, the case with exponent $n=5$ was resolved in Section 12, whence we may suppose that $n\ge 7$ is prime. To summarize, we are reduced to treating the equation

$$x^2+q^{2k+1}=y^n, \quad k\ge 0,\ q\nmid x,\ y \text{ even},\ n\ge 7 \text{ prime}. \tag{77}$$

By Proposition 14.1, we may in fact suppose that $n>1000$ and that

$$q\in\{7,\ 23,\ 31,\ 47,\ 71,\ 79\}. \tag{78}$$

For convenience, we restate Proposition 14.1 specialized to our current situation.

Lemma 15.1. *Let q be one of the values in (78). Let (x,y,k) satisfy (77), where $n>1000$ is prime. Suppose, without loss of generality, that $x\equiv 1 \pmod 4$. Attach to this solution the Frey–Hellegouarch elliptic curve*

$$G=G_{x,k}:Y^2=X^3+4xX^2+4(x^2+q^{2k+1})X.$$

Then $\bar\rho_{G,n}\sim\bar\rho_{E,n}$ where E is an elliptic curve of conductor $2q$ and nontrivial 2-torsion given in Table 6.

Upper bounds for n: linear forms in logarithms, complex and q-adic. We will appeal to bounds for linear forms in logarithms to deduce an upper bound for the prime exponent n in (77) where q belongs to (78).

Proposition 15.2. *Let q belong to the list (78). Let (x, y, k) satisfy (77) with prime exponent $n > 1000$. Then $n < U_q$ where*

$$U_q = \begin{cases} 2.8 \times 10^8 & \text{if } q = 7, \\ 1.1 \times 10^9 & \text{if } q = 23, \\ 5.0 \times 10^8 & \text{if } q = 31, \\ 2.2 \times 10^9 & \text{if } q = 47, \\ 2.3 \times 10^9 & \text{if } q = 71, \\ 2.2 \times 10^9 & \text{if } q = 79. \end{cases} \tag{79}$$

To obtain this result, our first order of business will be to produce a lower bound upon y.

Lemma 15.3. *If there exists a solution to (77), then $y > 4n - 4\sqrt{2n} + 2$.*

Proof. We suppose without loss of generality that $x \equiv 1 \pmod 4$, so that we can apply Lemma 15.1. We first show that y is divisible by an odd prime. Suppose otherwise and write $y = 2^\mu$ with $\mu \geq 1$. Then the Frey–Hellegouarch curve $G_{x,k}$ has conductor $2q$ and minimal discriminant $-2^{2n\mu-12}q^{2k+1}$. A short search of Cremona's tables [1997] reveals that there are no such elliptic curves for the values q in (78) (recall that $n > 1000$). Thus, there necessarily exists an odd prime $p \mid y$; since $q \nmid y$, we observe that $q \neq p$. By Lemma 7.1,

$$a_p(E) \equiv \pm(p+1) \pmod n,$$

where E is given by Table 6. As E has nontrivial 2-torsion, we conclude that $2n \mid (p + 1 \mp a_p(E))$. However, from the Hasse–Weil bounds,

$$0 < p + 1 \mp a_p(E) < (\sqrt{p} + 1)^2 \leq (\sqrt{y/2} + 1)^2,$$

and therefore $2n < (\sqrt{y/2} + 1)^2$. The desired inequality follows. □

Now let q be any of the values in (78), write $M = \mathbb{Q}(\sqrt{-q})$, and let $\mathcal{O}_M$ be its ring of integers. Note that the units of $\mathcal{O}_M$ are ± 1. Fix $\mathfrak{P}$ to be one of the two prime ideals of $\mathcal{O}_M$ above 2. After possibly replacing x by $-x$ we have

$$\frac{x + q^k\sqrt{-q}}{2} \cdot \mathcal{O}_M = \mathfrak{P}^{n-2} \cdot \mathfrak{A}^n, \tag{80}$$

where $\mathfrak{A}$ is an ideal of $\mathcal{O}_M$ with norm $y/2$. Hence

$$\frac{x - q^k\sqrt{-q}}{x + q^k\sqrt{-q}} = \left(\frac{\mathfrak{P}}{\overline{\mathfrak{P}}}\right)^2 \cdot \left(\frac{\overline{\mathfrak{P}} \cdot \overline{\mathfrak{A}}}{\mathfrak{P} \cdot \mathfrak{A}}\right)^n.$$

For all six values of q under consideration, the class group is cyclic and generated by the class $[\mathfrak{P}]$. Let h_q be the class number of M; this value is respectively 1, 3, 3, 5, 7 and 5 for q in (78) (see Table 7). As $n > 1000$ is prime, $\gcd(n, h_q) = 1$. Since $\mathcal{O}_M$ has class number h_q, it follows that $\mathfrak{P}^{h_q}$ is principal, say $\mathfrak{P}^{h_q} = (\alpha_q) \cdot \mathcal{O}_M$. We fix our choice of $\mathfrak{P}$ so that α_q is given by Table 7. Write $\beta_q = \alpha_q / \overline{\alpha_q}$. Thus

$$\left(\frac{x - q^k\sqrt{-q}}{x + q^k\sqrt{-q}}\right)^{h_q} = \beta_q^2 \gamma^n, \tag{81}$$

q	7	23	31	47	71	79
h_q	1	3	3	5	7	5
α_q	$\frac{1+\sqrt{-7}}{2}$	$\frac{3+\sqrt{-23}}{2}$	$\frac{1+\sqrt{-31}}{2}$	$\frac{9+\sqrt{-47}}{2}$	$\frac{21+\sqrt{-71}}{2}$	$\frac{7+\sqrt{-79}}{2}$

Table 7. Here, h_q denotes the class number of $M=\mathbb{Q}(\sqrt{-q})$, and α_q is a generator for the principal ideal $\mathfrak{P}^{h_q}$, where $\mathfrak{P}$ is one of the two prime ideals of $\mathcal{O}_M$ above 2.

where $\gamma\in M$ is some generator for the principal ideal $((\overline{\mathfrak{P}}\cdot\overline{\mathfrak{A}})/(\mathfrak{P}\cdot\mathfrak{A}))^{h_q}$.

To derive an upper bound on n, we begin by using (81) to find a "small" linear form in logarithms.Write

$$\Lambda=\log\left(\frac{x-q^k\sqrt{-q}}{x+q^k\sqrt{-q}}\right).$$

Lemma 15.4. *If there exists a solution to (77) with $y^n>100\,q^{2k+1}$, then*

$$\log|\Lambda|<0.75+\left(k+\frac{1}{2}\right)\log q-\frac{n}{2}\log y.$$

Proof. The assumption that $y^n>100q^{2k+1}$, together with, say, Lemma B.2 of [Smart 1998], implies that

$$|\Lambda|\le-10\log\left(\frac{9}{10}\right)\left|\frac{x-q^k\sqrt{-q}}{x+q^k\sqrt{-q}}-1\right|=-20\log\left(\frac{9}{10}\right)\frac{q^k\sqrt{q}}{y^{n/2}},$$

whence the lemma follows. □

To show that $\log|\Lambda|$ here is indeed small, we first require an upper bound upon k. From (81), we have

$$\left(\frac{x-q^k\sqrt{-q}}{x+q^k\sqrt{-q}}\right)^{h_q}-1=\beta_q^2\gamma^n-1$$

and so

$$\frac{-2q^k\sqrt{-q}}{x+q^k\sqrt{-q}}\sum_{i=0}^{h_q-1}\left(\frac{x-q^k\sqrt{-q}}{x+q^k\sqrt{-q}}\right)^i=\beta_q^2\gamma^n-1. \tag{82}$$

Since $\gcd(x,q)=1$, it follows from (82) that, if we set

$$\Lambda_1=\gamma^n-\overline{\beta_q}^2,$$

then $\nu_q(\Lambda_1)\ge k$. To complement this with an upper bound for linear forms in q-adic logarithms, we appeal to Theorem 10, with

$$q\in\{7,23,31,47,79\},\quad f=1,\quad D=2,\quad \alpha_1=\gamma,\quad \alpha_2=\overline{\beta_q},\quad b_1=n,\quad b_2=2,$$
$$\log A_1=\frac{h_q}{2}\log y,\quad \log A_2=\frac{1}{2}\log q\quad\text{and}\quad b'=\frac{n}{\log q}+\frac{2}{h_q\log y}.$$

Here, we use Lemma 13.2 of Bugeaud, Mignotte and Siksek [Bugeaud et al. 2006] which implies that

$$h(\alpha_1)=\frac{h_q}{2}\log y\quad\text{and}\quad h(\alpha_2)=\frac{h_q}{2}\log 2.$$

In the case $q = 71$, we make identical choices except to take $\log A_2 = \frac{7}{2}\log 2$, whence

$$b' = \frac{n}{7\log 2} + \frac{2}{7\log y}.$$

Theorem 10 thus yields the inequality

$$\nu_q(\Lambda_1) \le \frac{96\,q\,h_q}{\log^3 q}\cdot(\max\{\log b' + \log\log q + 0.4, 5\log q\})^2 \log y,$$

for $q \in \{7, 23, 31, 47, 79\}$, and

$$\nu_{71}(\Lambda_1) \le 701.2\cdot(\max\{\log b' + \log\log 71 + 0.4, 5\log 71\})^2 \log y,$$

if $q = 71$.

Let us now suppose that

$$n > 10^8, \tag{83}$$

which will certainly be the case if $n \ge U_q$, for U_q as defined in (79). Then, from Lemma 15.3, in all cases we have that

$$b' < 1.001\frac{n}{\log q}$$

and hence obtain the inequalities

$$k < \frac{96\,q\,h_q}{\log^3 q}\cdot(\max\{\log n + 0.4001, 5\log q\})^2 \log y, \quad \text{if } q \in \{7, 23, 31, 47, 79\} \tag{84}$$

and

$$k < 701.2\cdot(\max\{\log n + 0.4001, 5\log 71\})^2 \log y, \quad \text{if } q = 71. \tag{85}$$

Now consider

$$\Lambda_2 = h_q \log\frac{x - q^k\sqrt{-q}}{x + q^k\sqrt{-q}} = n\log(\epsilon_1\gamma) + 2\log(\epsilon_2\beta_q) + j\pi i, \tag{86}$$

where we take the principal branches of the logarithms and the integers $\epsilon_i \in \{-1, 1\}$ and j are chosen so that $\mathrm{Im}(\log(\epsilon_1\gamma))$ and $\mathrm{Im}(\log(\epsilon_2\beta_q))$ have opposite signs, and we have both

$$|\log(\epsilon_2\beta_q)| < \frac{\pi}{2}$$

and $|\Lambda_2|$ minimal. Explicitly,

q	7	23	31	47	71	79
ϵ_2	-1	-1	-1	1	1	-1
$\lvert\log(\epsilon_2\beta_q)\rvert$	$\arccos\frac{3}{4}$	$\arccos\frac{7}{16}$	$\arccos\frac{15}{16}$	$\arccos\frac{17}{64}$	$\arccos\frac{185}{256}$	$\arccos\frac{15}{64}$

Assume first that

$$y^n \le 100q^{2k+1}.$$

If $q \in \{7, 23, 31, 47, 79\}$, it follows from (84) that

$$n < \frac{2\log 10}{\log y} + \frac{\log q}{\log y} + \frac{192\, q\, h_q}{\log^2 q} \cdot (\max\{\log n + 0.4001, 5\log q\})^2,$$

in each case contradicting Lemma 15.3 and (83). We obtain a similar contradiction in case the $q = 71$ upon considering (85).

It follows, then, that we may assume $y^n > 100q^{2k+1}$ and hence conclude, from Lemma 15.4, that

$$\log|\Lambda_2| < \log h_q + 0.75 + \left(k + \frac{1}{2}\right)\log q - \frac{n}{2}\log y.$$

If $q \in \{7, 23, 31, 47, 79\}$, (84) thus implies that

$$\log|\Lambda_2| < \log h_q + 0.75 + \frac{1}{2}\log q + \frac{96\, q\, h_q}{\log^2 q} \cdot (\max\{\log n + 0.4001, 5\log q\})^2 \log y - \frac{n}{2}\log y.$$

An analogous inequality holds for $q = 71$, upon appealing to (85). From Lemma 15.3 and (83), we find that

$$\log|\Lambda_2| < -\kappa_q\, n \log y, \tag{87}$$

where

$$\kappa_q = \begin{cases} 0.499 & \text{if } q = 7, \\ 0.497 & \text{if } q \in \{23, 31\}, \\ 0.494 & \text{if } q = 47, \\ 0.486 & \text{if } q = 71, \\ 0.490 & \text{if } q = 79. \end{cases} \tag{88}$$

It therefore follows from the definition of Λ_2 that

$$|j|\,\pi < \pi n + 2\arccos\tfrac{15}{64} + y^{-0.486n} < \pi n + \pi,$$

and so

$$|j| \le n. \tag{89}$$

Linear forms in three logarithms. To deduce an initial lower bound upon the linear form in logarithms $|\Lambda_2|$, we will use the following.

Theorem 14 [Matveev 2000, Theorem 2.1]. *Let $\mathbb{K}$ be an algebraic number field of degree D over $\mathbb{Q}$ and put $\chi = 1$ if $\mathbb{K}$ is real, $\chi = 2$ otherwise. Suppose that $\alpha_1, \alpha_2, \dots, \alpha_{n_0} \in \mathbb{K}^*$ with absolute logarithmic heights $h(\alpha_i)$ for $1 \le i \le n_0$, and suppose that*

$$A_i \ge \max\{D\,h(\alpha_i), |\log\alpha_i|\}, \quad 1 \le i \le n_0,$$

for some fixed choice of the logarithm. Define

$$\Lambda = b_1\log\alpha_1 + \cdots + b_{n_0}\log\alpha_{n_0},$$

where the b_i are integers and set

$$B = \max\left\{1, \max\left\{|b_i|\frac{A_i}{A_{n_0}} : 1 \le i \le n_0\right\}\right\}.$$

Define, with $e := \exp(1)$,

$$\Omega = A_1 \cdots A_{n_0}, \quad C(n_0) = C(n_0, \chi) = \frac{16}{n_0! \chi} e^{n_0}(2n_0 + 1 + 2\chi)(n_0 + 2)(4n_0 + 4)^{n_0+1}\left(\frac{en_0}{2}\right)^{\chi},$$
$$C_0 = \log(e^{4.4n_0+7} n_0^{5.5} D^2 \log(eD)) \quad \textit{and} \quad W_0 = \log(1.5eBD \log(eD)).$$

Then, if $\log \alpha_1, \ldots, \log \alpha_{n_0}$ *are linearly independent over* $\mathbb{Z}$ *and* $b_{n_0} \neq 0$, *we have*

$$\log |\Lambda| > -C(n_0)\, C_0\, W_0\, D^2\, \Omega.$$

We apply Theorem 14 to $\Lambda = \Lambda_2$ with

$$D = 2, \quad \chi = 2, \quad n_0 = 3, \quad b_3 = n, \quad \alpha_3 = \epsilon_1 \gamma, \quad b_2 = -2, \quad \alpha_2 = \epsilon_2 \beta_q, \quad b_1 = j \quad \text{and} \quad \alpha_1 = -1.$$

We may thus take

$$A_3 = \log y, \quad A_2 = \max\{h_q \log 2, |\log(\epsilon_2 \beta_q)|\}, \quad A_1 = \pi \quad \text{and} \quad B = n.$$

Since

$$4\, C(3)\, C_0 = 2^{18} \cdot 3 \cdot 5 \cdot 11 \cdot e^5 \cdot \log(e^{20.2} \cdot 3^{5.5} \cdot 4 \log(2e)) < 1.80741 \times 10^{11},$$

and

$$W_0 = \log(3en \log(2e)) < 2.63 + \log n,$$

we may therefore conclude that

$$\log |\Lambda_2| > -5.68 \times 10^{11} \max\bigl\{h_q \log 2, |\log(\epsilon_2 \beta_q)|\bigr\}(2.63 + \log n) \log y.$$

It thus follows from (87) that

$$n < \kappa_q^{-1}\, 5.68 \times 10^{11} \max\bigl\{h_q \log 2, |\log(\epsilon_2 \beta_q)|\bigr\}(2.63 + \log n)$$

and hence

$$n < \begin{cases} 2.77 \times 10^{13} & \text{if } q = 7, \\ 8.24 \times 10^{13} & \text{if } q \in \{23, 31\}, \\ 1.42 \times 10^{14} & \text{if } q \in \{47, 79\}, \\ 2.02 \times 10^{14} & \text{if } q = 71. \end{cases} \tag{90}$$

To improve these inequalities, we appeal to a sharper, rather complicated, lower bound for linear forms in three complex logarithms, due to Mignotte [2008, Theorem 2]. Our argument is very similar to that employed in a recent paper of the authors [Bennett and Siksek 2023]. We note that recent work of Mignotte and Voutier [2022] would substantially improve our bounds (and reduce our subsequent computations considerably).

Theorem 15 (Mignotte). *Consider three nonzero algebraic numbers* α_1, α_2 *and* α_3, *which are either all real and* > 1, *or all complex of modulus one and all* $\neq 1$. *In addition, assume that the three numbers* α_1, α_2 *and* α_3 *are either all multiplicatively independent, or that two of the numbers are multiplicatively* *independent and the third is a root of unity. We also consider three positive rational integers* b_1, b_2, b_3 *with* $\gcd(b_1, b_2, b_3) = 1$, *and the linear form*

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1 - b_3 \log \alpha_3,$$

where the logarithms of the α_i *are arbitrary determinations of the logarithm, but which are all real or all purely imaginary. We assume that*

$$0 < |\Lambda| < \frac{2\pi}{w},$$

where w *is the maximal order of a root of unity in* $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. *Suppose further that*

$$b_2 |\log \alpha_2| = b_1 \, |\log \alpha_1| + b_3 \, |\log \alpha_3| \pm |\Lambda| \tag{91}$$

and put

$$d_1 = \gcd(b_1, b_2), \quad d_3 = \gcd(b_3, b_2) \quad \textit{and} \quad b_2 = d_1 b_2' = d_3 b_2''$$

Let $K, L, R, R_1, R_2, R_3, S, S_1, S_2, S_3, T, T_1, T_2, T_3$ *be positive rational integers with*

$$K \geq 3, \quad L \geq 5, \quad R > R_1 + R_2 + R_3, \quad S > S_1 + S_2 + S_3 \quad \textit{and} \quad T > T_1 + T_2 + T_3.$$

Let $\rho \geq 2$ *be a real number. Let* a_1, a_2 *and* a_3 *be real numbers such that*

$$a_i \geq \rho |\log \alpha_i| - \log |\alpha_i| + 2D\, h(\alpha_i), \quad i \in \{1, 2, 3\},$$

where $D = [\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{Q}]/[\mathbb{R}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{R}]$, *and set*

$$U = \left(\frac{KL}{2} + \frac{L}{4} - 1 - \frac{2K}{3L} \right) \log \rho.$$

Assume further that

$$U \geq (D+1) \log(K^2 L) + gL(a_1 R + a_2 S + a_3 T) + D(K-1) \log b - 2 \log \frac{e}{2}, \tag{92}$$

where

$$g = \frac{1}{4} - \frac{K^2 L}{12RST} \quad \textit{and} \quad b = (b_2' \eta_0)(b_2'' \zeta_0) \left(\prod_{k=1}^{K-1} k! \right)^{-4/(K(K-1))},$$

with

$$\eta_0 = \frac{R-1}{2} + \frac{(S-1)b_1}{2b_2} \quad \textit{and} \quad \zeta_0 = \frac{T-1}{2} + \frac{(S-1)b_3}{2b_2}.$$

Put

$$\mathcal{V} = \sqrt{(R_1+1)(S_1+1)(T_1+1)}.$$

If, for some positive real number χ, *we have*

(i) $(R_1+1)(S_1+1)(T_1+1) > K\mathcal{M}$,

(ii) $\operatorname{Card}\{\alpha_1^r \alpha_2^s \alpha_3^t : 0 \leq r \leq R_1, 0 \leq s \leq S_1, 0 \leq t \leq T_1\} > L$,

(iii) $(R_2+1)(S_2+1)(T_2+1) > 2K^2$,

(iv) $\operatorname{Card}\{\alpha_1^r \alpha_2^s \alpha_3^t : 0 \leq r \leq R_2, 0 \leq s \leq S_2, 0 \leq t \leq T_2\} > 2KL$, *and*

(v) $(R_3+1)(S_3+1)(T_3+1) > 6K^2L$,

where

$$\mathcal{M} = \max\{R_1+S_1+1,\, S_1+T_1+1,\, R_1+T_1+1,\, \chi\mathcal{V}\},$$

then either

$$|\Lambda| \cdot \frac{LSe^{LS|\Lambda|/(2b_2)}}{2|b_2|} > \rho^{-KL}, \tag{93}$$

or at least one of the following conditions holds:

(C1) $|b_1| \le R_1$ *and* $|b_2| \le S_1$ *and* $|b_3| \le T_1$.

(C2) $|b_1| \le R_2$ *and* $|b_2| \le S_2$ *and* $|b_3| \le T_2$.

(C3) ***Either*** *there exist nonzero rational integers* r_0 *and* s_0 *such that*

$$r_0 b_2 = s_0 b_1 \tag{94}$$

with

$$|r_0| \le \frac{(R_1+1)(T_1+1)}{\mathcal{M}-T_1} \quad \textit{and} \quad |s_0| \le \frac{(S_1+1)(T_1+1)}{\mathcal{M}-T_1}, \tag{95}$$

or *there exist rational integers* r_1, s_1, t_1 *and* t_2, *with* $r_1 s_1 \ne 0$, *such that*

$$(t_1 b_1 + r_1 b_3)s_1 = r_1 b_2 t_2, \quad \gcd(r_1, t_1) = \gcd(s_1, t_2) = 1, \tag{96}$$

which also satisfy

$$|r_1 s_1| \le \gcd(r_1, s_1) \cdot \frac{(R_1+1)(S_1+1)}{\mathcal{M}-\max\{R_1, S_1\}},$$
$$|s_1 t_1| \le \gcd(r_1, s_1) \cdot \frac{(S_1+1)(T_1+1)}{\mathcal{M}-\max\{S_1, T_1\}}$$

and

$$|r_1 t_2| \le \gcd(r_1, s_1) \cdot \frac{(R_1+1)(T_1+1)}{\mathcal{M}-\max\{R_1, T_1\}}.$$

Also, *when* $t_1 = 0$ *we can take* $r_1 = 1$, *and when* $t_2 = 0$ *we can take* $s_1 = 1$.

We will apply this result to $\Lambda = \Lambda_2$. For simplicity, we will provide full details for the case $q = 7$; the arguments for the other values of q under consideration are similar and follow closely their analogues in [Bennett and Siksek 2023]. If $j = 0$, then Λ_2 immediately reduces to a linear form in two logarithms and we may appeal to Theorem 11, with (in the notation of that result)

$$c_2 = n, \quad \beta_2 = \epsilon_1\gamma, \quad c_1 = 2, \quad \beta_1 = \frac{1}{\epsilon_2\beta_q}, \quad D = 1,$$

whence we may choose

$$\log B_2 = \tfrac{1}{2}\log y \quad \text{and} \quad \log B_1 = 1.$$

We thus have, from (83) and Lemma 15.3,

$$b' = \frac{4}{\log y} + n < 1.001n.$$

From Theorem 11 with $(m, C) = (10, 32.3)$, it follows, again from (83), that

$$\log|\Lambda_2| \geq -64.6(\log n + 0.211)^2 \log y.$$

Combining this with inequality (87) contradicts (83). We argue similarly if $j = \pm n$, again reaching a contradiction via bounds for linear forms in two complex logarithms.

We may thus suppose that $j \neq 0$ and $|j| < n$ (so that, in particular, $\gcd(j, n) = 1$), and hence choose

$$b_1 = 2, \quad \alpha_1 = \frac{1}{\epsilon_2 \beta_q}, \quad b_2 = n, \quad \alpha_2 = \epsilon_1 \gamma, \quad b_3 = -j \quad \text{and} \quad \alpha_3 = -1. \tag{97}$$

From the fact that $\operatorname{Im}(\log(\epsilon_1\gamma))$ and $\operatorname{Im}(\log(\epsilon_2\beta_q))$ have opposite signs, (91) is satisfied and we have

$$d_1 = d_3 = 1 \quad \text{and} \quad b_2' = b_2'' = n.$$

It follows that

$$h(\alpha_1) = \tfrac{1}{2}\log(2), \quad h(\alpha_2) = \tfrac{1}{2}\log(y) \quad \text{and} \quad h(\alpha_3) = 0,$$

and hence we can take

$$a_1 = \rho \arccos \tfrac{3}{4} + \log 2, \quad a_2 = \rho\pi + \log y \quad \text{and} \quad a_3 = \rho\pi.$$

As noted in [Bugeaud et al. 2006], if we suppose that $m \geq 1$ and define

$$\begin{aligned} &K = [mLa_1a_2a_3], \quad R_1 = [c_1a_2a_3], \quad S_1 = [c_1a_1a_3], \quad T_1 = [c_1a_1a_2], \quad R_2 = [c_2a_2a_3], \\ &S_2 = [c_2a_1a_3], \quad T_2 = [c_2a_1a_2], \quad R_3 = [c_3a_2a_3], \quad S_3 = [c_3a_1a_3], \quad T_3 = [c_3a_1a_2], \end{aligned} \tag{98}$$

where

$$c_1 = \max\left\{(\chi mL)^{2/3}, \left(\frac{2mL}{a_1}\right)^{1/2}\right\}, \quad c_2 = \max\left\{2^{1/3}(mL)^{2/3}, \left(\frac{m}{a_1}\right)^{1/2} L\right\} \quad \text{and} \quad c_3 = (6m^2)^{1/3}L, \tag{99}$$

then conditions (i)–(v) are automatically satisfied. It remains to verify inequality (92).

To carry this out, we optimize numerically over values of ρ, L, m and χ as in [Bennett and Siksek 2023] (full details are available there, by way of example, in the case $q = 7$). Pari/GP code for carrying this out is due to Voutier [2023]. In each case, we obtain a sharpened upper bound upon the exponent n, provided inequality (93) holds. If, on the other hand, inequality (93) fails to be satisfied, from inequality (83) and our choices of S_1 and S_2, necessarily (C3) holds and we may rewrite Λ_2 as a linear form in two complex logarithms to which we can apply Theorem 11. In this case, we once again obtain a sharpened upper bound for n. Iterating this process leads to the upper bounds U_q given in (79). We observe that direct application of the new bounds from [Mignotte and Voutier 2022], with the corresponding Pari/GP code, substantially sharpens these bounds, though this is not especially important for our purposes. This completes the proof of Proposition 15.2.

Proof of Theorem 1. We now finish the proof of Theorem 1. By the remarks at the beginning of the current section, we are reduced to considering solutions (x, y, k) to (77), where q belongs to (78). Thanks to Propositions 14.1 and 15.2, we may suppose that the prime exponent n belongs to the range $1000 < n < U_q$ where U_q is given by (79).

Lemma 15.5. *Let (x, y, k) be a solution to (77) where q belongs to (78) and the exponent n is a prime belonging to the range $1000 < n < U_q$. Let $M = \mathbb{Q}(\sqrt{-q})$. Let h_q and α_q be as in Table 7, and choose i to be the unique integer $0 \le i \le h_q - 1$ satisfying $ni \equiv -2 \pmod{h_q}$. Write $n^* = (-ni-2)/h_q$. Then, after possibly changing the sign of x,*

$$\frac{x + q^k\sqrt{-q}}{2} = \alpha_q^{n^*} \cdot \gamma^n, \tag{100}$$

where $\gamma \in \mathcal{O}_M$. Additionally, $\mathrm{Norm}(\gamma) = 2^{i-1}y$.

Proof. Recall that h_q is the class number of M, and that $\mathfrak{P}^{h_q} = \alpha_q \mathcal{O}_M$, where $\mathfrak{P}$ is one of the two prime ideals of $\mathcal{O}_M$ above 2. From (78), after possibly replacing x by $-x$,

$$\left(\frac{x + q^k\sqrt{-q}}{2}\right) \cdot \mathcal{O}_M = \mathfrak{P}^{-2} \cdot \mathfrak{A}^n,$$

where $\mathfrak{A}$ is an ideal of $\mathcal{O}_M$ of norm $y/2$. Now, for the values of q we are considering, the class group is cyclic and generated by $[\mathfrak{P}]$. Thus there is some $0 \le i \le h_q - 1$ such that $\mathfrak{P}^i\mathfrak{A}$ is principal. However,

$$\left(\frac{x + q^k\sqrt{-q}}{2}\right) \cdot \mathcal{O}_M = \mathfrak{P}^{-ni-2} \cdot (\mathfrak{P}^i \cdot \mathfrak{A})^n.$$

We deduce that $\mathfrak{P}^{-ni-2}$ is principal. As the class $[\mathfrak{P}]$ generates the class group, we infer that i is the unique integer $0 \le i \le h_q - 1$ satisfying $ni \equiv -2 \pmod{h_q}$. Write $n^* = (-ni-2)/h_q$. As $\mathfrak{P}^{h_q} = \alpha_q$, we have $\mathfrak{P}^{-ni-2} = \alpha_q^{n^*} \cdot \mathcal{O}_M$. Hence

$$\frac{x + q^k\sqrt{-q}}{2} = \alpha_q^{n^*} \cdot \gamma^n,$$

where $\gamma \in \mathcal{O}_M$ is a generator for the principal ideal $\mathfrak{P}^i\mathfrak{A}$. We note that $\mathrm{Norm}(\gamma) = 2^{i-1}y$. □

The following lemma, inspired by ideas of Kraus [1998], provides a computational framework for showing that (77) has no solutions for a particular exponent n.

Lemma 15.6. *Let q belong to the list (78) and let $\beta_q = \overline{\alpha_q}/\alpha_q$. Let n be a prime belonging to the range $1000 < n < U_q$. Let E be the elliptic curve given in Table 6. Let $\ell \ne q$ be a prime satisfying the three conditions*

(I) *$-q$ is a square modulo ℓ;*

(II) *$\ell = tn + 1$ for some positive integer t;*

(III) $a_\ell(E)^2 \not\equiv 4 \pmod{n}$.

Let $\mathfrak{L}$ be one of the two prime ideals of $\mathcal{O}_M$ above ℓ, and write $\mathbb{F}_{\mathfrak{L}} = \mathcal{O}_M/\mathfrak{L} \cong \mathbb{F}_\ell$. Let $\beta \in \mathbb{F}_{\mathfrak{L}}$ satisfy $\beta \equiv \overline{\alpha_q}/\alpha_q \pmod{\mathfrak{L}}$. Choose g to be a cyclic generator for $\mathbb{F}_{\mathfrak{L}}^*$, set $h = g^n$, and define

$$\mathfrak{X}_{\ell,n} = \{\beta^{n^*} \cdot h^j : j = 0, 1, \ldots, t-1\} \subset \mathbb{F}_{\mathfrak{L}}.$$

For $\mathfrak{x} \in \mathfrak{X}_{\ell,n}$ let

$$E_{\mathfrak{x}} : Y^2 = X(X+1)(X+\mathfrak{x}).$$

Finally, define

$$\mathfrak{Y}_{\ell,n} = \{\mathfrak{x} \in \mathfrak{X} : a_{\mathfrak{L}}(E_{\mathfrak{x}})^2 \equiv a_\ell(E)^2 \pmod{n}\}.$$

If $\mathfrak{Y}_{\ell,n} = \varnothing$, then (77) has no solutions.

Proof. Suppose that (x, y, k) is a solution to (77) for our particular pair (q, n). We change the sign of x if necessary so that (100) holds and let $x' = \pm x$ so that $x' \equiv 1 \pmod 4$. By Lemma 15.1, we know that $\bar{\rho}_{G_{x',k},n} \sim \bar{\rho}_{E,n}$. Observe that $G_{x',k}$ is either the same elliptic curve as $G_{x,k}$ if $x' = x$, or it is a quadratic twist by -1 if $x' = -x$. Hence $a_\ell(G_{x,k}) = \pm a_\ell(G_{x',k})$ for any odd prime ℓ of good reduction for either (and hence both) elliptic curves. We let ℓ be a prime satisfying conditions (I), (II) and (III). From (III) and (II), we note that $a_\ell(E) \not\equiv \pm(\ell+1) \pmod{n}$. It follows from Lemma 7.1 that $\ell \nmid y$, and that $a_\ell(G_{x',k}) \equiv a_\ell(E) \pmod{n}$. Thus $a_\ell(G_{x,k})^2 \equiv a_\ell(E)^2 \pmod{n}$. By Lemma 15.5, identity (100) holds where $\mathrm{Norm}(\gamma) = 2^{i-1}y$. In particular, $\mathfrak{L}$ is disjoint from the support of γ and α_q. It follows from (100) that

$$\frac{x - q^k\sqrt{-q}}{x + q^k\sqrt{-q}} = \left(\frac{\overline{\alpha_q}}{\alpha_q}\right)^{n^*} \cdot \left(\frac{\overline{\gamma}}{\gamma}\right)^{n}.$$

As g is a generator of $\mathbb{F}_{\mathfrak{L}}^*$ which is cyclic of order $\ell - 1 = tn$, and as $h = g^n$, there is some $0 \le j \le t-1$ such that $(\overline{\gamma}/\gamma)^n \equiv h^j \pmod{\mathfrak{L}}$. Hence

$$\frac{x - q^k\sqrt{-q}}{x + q^k\sqrt{-q}} \equiv \mathfrak{x} \pmod{\mathfrak{L}},$$

for some $\mathfrak{x} \in \mathfrak{X}_{\ell,n}$. The Frey–Hellegouarch curve $G_{x,k}$ defined in Lemma 15.1 can be rewritten as

$$Y^2 = X(X + 2(x - q^k\sqrt{-q}))(X + 2(x + q^k\sqrt{-q}))$$

and hence modulo $\mathfrak{L}$ is a quadratic twist of $E_{\mathfrak{x}}$. We deduce that $a_{\mathfrak{L}}(E_{\mathfrak{x}})^2 = a_\ell(G_{x,k})^2 \equiv a_\ell(E)^2 \pmod{n}$, whence $\mathfrak{x} \in \mathfrak{Y}_{\ell,n}$. This completes the proof. □

To finish the proof of Theorem 1, we wrote a `Magma` script which, for each q in (78) and each prime n in the interval $1000 < n < U_q$, found a prime ℓ satisfying conditions (I), (II) and (III), with $\mathfrak{Y}_{\ell,n} = \varnothing$. The following table gives the approximate time taken for this computation, on a single processor:

q	7	23	31	47	71	79
time (hours)	115	450	226	988	1058	1019

As one may observe from our proofs, for a given q, the upper bound U_q upon n in (77), coming from bounds for linear forms in logarithms, depends strongly upon the class number of $\mathbb{Q}(\sqrt{-q})$. It is this dependence which makes extending Theorem 1 to larger values of q an expensive proposition, computationally.

16. Concluding remarks

There are quite a few additional Frey–Hellegouarch curves at our disposal, that might prove helpful in completing the solution of (5), for some of our problematical values of q. A number of these arise from considering (5) as a special case of

$$x^2 - q^\delta z^\kappa = y^n,$$

where, say, $\kappa \in \{3, 4, 6\}$ and $0 \le \delta < \kappa$. In each case, the dimensions of the spaces of modular forms under consideration grow quickly, complicating matters. This is particularly true if $\kappa \in \{4, 6\}$, where our Frey–Hellegouarch curve will a priori be defined over $\mathbb{Q}(\sqrt{q})$, and so the relevant modular forms are Hilbert modular forms which are more challenging to compute than classical modular forms.

In the case y is even in (5) (whence we are in the situation where our bounds coming from linear forms in logarithms are weaker), we can attach a Frey–Hellegouarch $\mathbb{Q}$-curve to a potential solution (which at least corresponds to a classical modular form). To do this, write $M = \mathbb{Q}(\sqrt{q})$ and $\mathcal{O}_M$ for the ring of integers of M. Assuming that M has class number one (which is the case for, say, the remaining values $q \in \{41, 89, 97\}$), we have

$$\frac{x + q^k \sqrt{q}}{2} = \delta^r \gamma^{n-2} \alpha^n$$

for some $r \in \mathbb{Z}$ and $\alpha \in \mathcal{O}_M$. Here, δ is a fundamental unit for $\mathcal{O}_M$ and γ is a suitably chosen generator for one of the two prime ideals above 2 in M. From this equation,

$$q^k \sqrt{q} = \delta^r \gamma^{n-2} \alpha^n - \bar{\delta}^r \bar{\gamma}^{n-2} \bar{\alpha}^n.$$

Treating this as a ternary equation of signature $(n, n, 2)$, we can attach to such a solution a Frey–Hellegouarch $\mathbb{Q}$-curve; see, for example, [van Langen 2021, Section 6]. We will not pursue this here.

Acknowledgments

The authors are grateful to the anonymous referee for numerous insightful comments, and to Pedro-José Carzola Garcia, Ritesh Goenka and Vandita Patel for finding errors in earlier drafts of this paper.

References

[Arif and Abu Muriefah 2002] S. A. Arif and F. S. Abu Muriefah, "On the Diophantine equation $x^2 + q^{2k+1} = y^n$", *J. Number Theory* **95**:1 (2002), 95–100. MR Zbl

[Barros 2010] C. F. Barros, *On the Lebesgue–Nagell equation and related subjects*, Ph.D. thesis, University of Warwick, 2010.

[Bauer and Bennett 2002] M. Bauer and M. A. Bennett, "Applications of the hypergeometric method to the generalized Ramanujan–Nagell equation", *Ramanujan J.* **6**:2 (2002), 209–270. MR Zbl

[Bennett and Siksek 2023] M. A. Bennett and S. Siksek, "Differences between perfect powers: the Lebesgue–Nagell equation", *Trans. Amer. Math. Soc.* **376**:1 (2023), 335–370. MR Zbl

[Bennett and Skinner 2004] M. A. Bennett and C. M. Skinner, "Ternary Diophantine equations via Galois representations and modular forms", *Canad. J. Math.* **56**:1 (2004), 23–54. MR Zbl

[Bennett et al. 2010] M. A. Bennett, J. S. Ellenberg, and N. C. Ng, "The Diophantine equation $A^4+2^\delta B^2=C^n$", *Int. J. Number Theory* **6**:2 (2010), 311–338. MR Zbl

[Bennett et al. 2022] M. A. Bennett, A. Gherga, V. Patel, and S. Siksek, "Odd values of the Ramanujan tau function", *Math. Ann.* **382**:1-2 (2022), 203–238. MR Zbl

[Bérczes and Pink 2008] A. Bérczes and I. Pink, "On the Diophantine equation $x^2+p^{2k}=y^n$", *Arch. Math.* (*Basel*) **91**:6 (2008), 505–517. MR Zbl

[Bérczes and Pink 2012] A. Bérczes and I. Pink, "On the Diophantine equation $x^2+d^{2l+1}=y^n$", *Glasg. Math. J.* **54**:2 (2012), 415–428. MR Zbl

[Bilu et al. 2001] Y. Bilu, G. Hanrot, and P. M. Voutier, "Existence of primitive divisors of Lucas and Lehmer numbers", *J. Reine Angew. Math.* **539** (2001), 75–122. MR Zbl

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Breuil et al. 2001] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises", *J. Amer. Math. Soc.* **14**:4 (2001), 843–939. MR Zbl

[Bugeaud 1997] Y. Bugeaud, "On the Diophantine equation $x^2-p^m=\pm y^n$", *Acta Arith.* **80**:3 (1997), 213–223. MR Zbl

[Bugeaud and Laurent 1996] Y. Bugeaud and M. Laurent, "Minoration effective de la distance p-adique entre puissances de nombres algébriques", *J. Number Theory* **61**:2 (1996), 311–342. MR Zbl

[Bugeaud et al. 2006] Y. Bugeaud, M. Mignotte, and S. Siksek, "Classical and modular approaches to exponential Diophantine equations, II: The Lebesgue–Nagell equation", *Compos. Math.* **142**:1 (2006), 31–62. MR Zbl

[Carmichael 1913] R. D. Carmichael, "On the numerical factors of the arithmetic forms $\alpha^n\pm\beta^n$", *Ann. of Math.* (2) **15**:1-4 (1913), 49–70. MR Zbl

[Cohn 1997] J. H. E. Cohn, "The Diophantine equation $x^4-Dy^2=1$, II", *Acta Arith.* **78**:4 (1997), 401–403. MR Zbl

[Cohn 2003] J. H. E. Cohn, "The Diophantine equation $x^n=Dy^2+1$", *Acta Arith.* **106**:1 (2003), 73–83. MR Zbl

[Cremona 1997] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge Univ. Press, 1997. MR Zbl

[Gherga and Siksek 2022] A. Gherga and S. Siksek, "Efficient resolution of Thue–Mahler equations", preprint, 2022. arXiv 2207.14492

[Halberstadt and Kraus 2002] E. Halberstadt and A. Kraus, "Courbes de Fermat: résultats et problèmes", *J. Reine Angew. Math.* **548** (2002), 167–234. MR Zbl

[Ivorra 2003] W. Ivorra, "Sur les équations $x^p+2^\beta y^p=z^2$ et $x^p+2^\beta y^p=2z^2$", *Acta Arith.* **108**:4 (2003), 327–338. MR Zbl

[Ivorra and Kraus 2006] W. Ivorra and A. Kraus, "Quelques résultats sur les équations $ax^p+by^p=cz^2$", *Canad. J. Math.* **58**:1 (2006), 115–153. MR Zbl

[Koutsianas 2020] A. Koutsianas, "An application of the modular method and the symplectic argument to a Lebesgue–Nagell equation", *Mathematika* **66**:1 (2020), 230–244. MR Zbl

[Kraus 1997] A. Kraus, "Majorations effectives pour l'équation de Fermat généralisée", *Canad. J. Math.* **49**:6 (1997), 1139–1161. MR Zbl

[Kraus 1998] A. Kraus, "Sur l'équation $a^3+b^3=c^p$", *Exp. Math.* **7**:1 (1998), 1–13. MR Zbl

[Kraus and Oesterlé 1992] A. Kraus and J. Oesterlé, "Sur une question de B. Mazur", *Math. Ann.* **293**:2 (1992), 259–275. MR Zbl

[van Langen 2021] J. M. van Langen, "On the sum of fourth powers in arithmetic progression", *Int. J. Number Theory* **17**:1 (2021), 191–221. MR Zbl

[Laurent 2008] M. Laurent, "Linear forms in two logarithms and interpolation determinants, II", *Acta Arith.* **133**:4 (2008), 325–348. MR Zbl

[Matveev 2000] E. M. Matveev, "An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, II", *Izv. Ross. Akad. Nauk Ser. Mat.* **64**:6 (2000), 125–180. In Russian; translated in *Izv. Math.* **64**:6 (2000), 1217–1269. MR Zbl

[Mazur 1978] B. Mazur, "Rational isogenies of prime degree", *Invent. Math.* **44**:2 (1978), 129–162. MR Zbl

[Mignotte 2008] M. Mignotte, "A kit on linear forms in three logarithms", preprint, 2008, available at https://irma.math.unistra.fr/~bugeaud/travaux/kit.pdf.

[Mignotte and Voutier 2022] M. Mignotte and P. Voutier, "A kit for linear forms in three logarithms", preprint, 2022. arXiv 2205.08899

[Mihăilescu 2004] P. Mihăilescu, "Primary cyclotomic units and a proof of Catalan's conjecture", *J. Reine Angew. Math.* **572** (2004), 167–195. MR Zbl

[Pethő et al. 1999] A. Pethő, H. G. Zimmer, J. Gebel, and E. Herrmann, "Computing all S-integral points on elliptic curves", *Math. Proc. Cambridge Philos. Soc.* **127**:3 (1999), 383–402. MR Zbl

[Pillai 1936] S. S. Pillai, "On $a^x - b^y = c$", *J. Indian Math. Soc.* **2** (1936), 119–122. Correction in **2** (1937), 215. 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

[Ribet 1997] K. A. Ribet, "On the equation $a^p + 2^\alpha b^p + c^p = 0$", *Acta Arith.* **79**:1 (1997), 7–16. MR Zbl

[Serre 1975] J.-P. Serre, "Divisibilité de certaines fonctions arithmétiques", exposé 20 in *Séminaire Delange–Pisot–Poitou: théorie des nombres*, 1974/1975, *I*, Secrétariat Math., Paris, 1975. MR Zbl

[Siksek 2003] S. Siksek, "On the Diophantine equation $x^2 = y^p + 2^k z^p$", *J. Théor. Nombres Bordeaux* **15**:3 (2003), 839–846. MR Zbl

[Siksek 2012] S. Siksek, "The modular approach to Diophantine equations", pp. 151–179 in *Explicit methods in number theory* (Paris, 2004), Panor. Synthèses **36**, Soc. Math. France, Paris, 2012. MR Zbl

[Smart 1998] N. P. Smart, *The algorithmic resolution of Diophantine equations*, Lond. Math. Soc. Stud. Texts **41**, Cambridge Univ. Press, 1998. MR Zbl

[Stein 2007] W. Stein, *Modular forms: a computational approach*, Grad. Stud. in Math. **79**, Amer. Math. Soc., Providence, RI, 2007. MR Zbl

[Stoll and Cremona 2003] M. Stoll and J. E. Cremona, "On the reduction theory of binary forms", *J. Reine Angew. Math.* **565** (2003), 79–99. MR Zbl

[Voutier 2023] P. Voutier, "lfl3-kit", 2023, available at https://github.com/PV-314/lfl3-kit. PARI/GP code.

[Wiles 1995] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. of Math.* (2) **141**:3 (1995), 443–551. MR Zbl

Communicated by Frank Calegari
Received 2021-10-11 Revised 2022-09-22 Accepted 2022-11-28

bennett@math.ubc.ca Department of Mathematics, University of British Columbia, Vancouver, Canada

s.siksek@warwick.ac.uk Mathematics Institute, University of Warwick, Coventry, United Kingdom

ALGEBRA AND NUMBER THEORY 17:10 (2023)
https://doi.org/10.2140/ant.2023.17.1847

On fake linear cycles inside Fermat varieties

Jorge Duque Franco and Roberto Villaflor Loyola

We introduce a new class of Hodge cycles with nonreduced associated Hodge loci; we call them fake linear cycles. We characterize them for all Fermat varieties and show that they exist only for degrees $d = 3, 4, 6$, where there are infinitely many in the space of Hodge cycles. These cycles are pathological in the sense that the Zariski tangent space of their associated Hodge locus is of maximal dimension, contrary to a conjecture of Movasati. They provide examples of algebraic cycles not generated by their periods in the sense of Movasati and Sertöz (2021). To study them we compute their Galois action in cohomology and their second-order invariant of the IVHS. We conclude that for any degree $d \geq 2 + \frac{6}{n}$, the minimal codimension component of the Hodge locus passing through the Fermat variety is the one parametrizing hypersurfaces containing linear subvarieties of dimension $\frac{n}{2}$, extending results of Green, Voisin, Otwinowska and Villaflor Loyola.

1. Introduction

The classical Noether–Lefschetz locus NL_d is the space of degree $d \geq 4$ surfaces in $\mathbb{P}^3$ with Picard rank bigger than 1. This space is known to have countably many components given by algebraic subvarieties of the space of smooth degree d surfaces in $\mathbb{P}^3$. A classical result due to Green [1988] and Voisin [1988] states that for $d \geq 5$ it has only one minimal codimension component, which parametrizes surfaces containing lines (for $d = 4$ all components have the same codimension). The higher dimension analogue of the Noether–Lefschetz locus is the so-called Hodge locus $\mathrm{HL}_{n,d}$ which is the locus of degree d hypersurfaces $X \subseteq \mathbb{P}^{n+1}$ for n even, with lattice of Hodge cycles $H^{n/2,n/2}(X) \cap H^n(X, \mathbb{Z})$ of rank bigger than 1. This space is nontrivial for $d \geq 2 + \frac{4}{n}$, and it is known to have countably many components which are algebraic subvarieties of $T \subseteq H^0(\mathbb{P}^{n+1}, \mathcal{O}(d))$ the space of smooth degree d hypersurfaces of $\mathbb{P}^{n+1}$. A natural question is to ask whether the analogue of the Green–Voisin theorem still holds for higher dimensions, i.e., if for $d \geq 2 + \frac{6}{n}$ the only minimal codimension component of the Hodge locus is $\Sigma_{(1,\dots,1)}$, that is, the one parametrizing hypersurfaces containing linear subvarieties of dimension $\frac{n}{2}$. The first result in this direction was obtained by Otwinowska [2002, Theorem 3] who answered positively the question for $d \gg n$. The conjecture for smaller degrees remains open, and even to establish that the codimension of $\Sigma_{(1,\dots,1)}$ — which is equal to $\binom{n/2+d}{d} - \left(\frac{n}{2}+1\right)^2$ — is a lower bound for the codimension of all components is also a conjecture. A partial result on the lower bound conjecture was obtained by Movasati [2017, Theorem 2], who proved it for all components passing through the Fermat point. The characterization of $\Sigma_{(1,\dots,1)}$ as

MSC2020: 14C25, 14C30, 14D07.
Keywords: fake linear cycles, algebraic cycles, Hodge locus, Noether–Lefschetz locus, Galois cohomology, second-order invariant IVHS.

the only component passing through the Fermat point attaining this bound was recently established in Theorem 1.1 of [Villaflor Loyola 2022b] for $d \neq 3, 4, 6$. In this article we treat the remaining cases.

The previously mentioned results rely on the description of the Zariski tangent space of the local Hodge loci $V_\lambda \subseteq (T, t)$, associated to some Hodge cycle $\lambda \in H^{n/2,n/2}(X_t) \cap H^n(X_t, \mathbb{Z})$ for $X_t = \mathrm{Supp}(t) \subseteq \mathbb{P}^{n+1}$ and $t \in T$, in terms of the infinitesimal variation of Hodge structure. In practice, instead of bounding the codimension of the components of the Hodge locus, one bounds the codimension of the Zariski tangent space of all V_λ. This is the case for all the previous results of Green, Voisin, Otwinowska and Movasati. In particular, Movasati proved that if $0 \in T$ corresponds to the Fermat point then the codimension of $T_0 V_\lambda$ is greater than or equal to $\binom{n/2+d}{d} - \left(\frac{n}{2}+1\right)^2$ for all nontrivial Hodge cycles $\lambda \in H^{n/2,n/2}(X_0) \cap H^n(X_0, \mathbb{Z})$ of the Fermat variety. This naturally led Movasati [2021, Conjecture 18.8] to conjecture that this bound is attained if and only if λ is the class of a linear algebraic cycle $\mathbb{P}^{n/2} \subseteq X_0$ of the Fermat variety. Our main result disproves this conjecture for $d = 3, 4, 6$ in all dimensions, providing a complete answer to Movasati's question for the cases not covered by [Villaflor Loyola 2022b].

Theorem 1.1. *For $d = 3, 4, 6 \geq 2 + \frac{6}{n}$ and n even, there are infinitely many scheme-theoretically different Hodge loci V_λ associated to nontrivial Hodge cycles of the Fermat variety $\lambda \in H^{n/2,n/2}(X_0) \cap H^n(X_0, \mathbb{Z})$ such that*

$$\operatorname{codim} T_0 V_\lambda = \binom{n/2+d}{d} - \left(\frac{n}{2}+1\right)^2.$$

In particular, infinitely many of these Hodge cycles are not linear cycles. We call them fake linear cycles. All fake linear cycles are of the form

$$\lambda_{\mathrm{prim}} = \mathrm{res}\left(\frac{P_\lambda \Omega}{F^{n/2+1}}\right),$$

where P_λ is given (up to some relabeling of the coordinates) by

$$P_\lambda = c_\lambda \prod_{j=1}^{n/2+1} \frac{x_{2j-2}^{d-1} - (c_{2j-2}x_{2j-1})^{d-1}}{x_{2j-2} - c_{2j-2}x_{2j-1}}, \tag{1}$$

where $c_0, c_2, \ldots, c_n \in \zeta_{2d}^{-3} \cdot \mathbb{S}^1_{\mathbb{Q}(\zeta_d)} = \{\zeta_{2d}^{-3} \cdot z \in \mathbb{Q}(\zeta_{2d}) : z \in \mathbb{Q}(\zeta_d) \text{ and } |z| = 1\}$ but not all being d-th roots of -1 simultaneously, and $c_\lambda \in \mathbb{Q}(\zeta_{2d})^\times$. For any such choice of c_i's, there exists some $c_\lambda \in \mathbb{Q}(\zeta_{2d})^\times$ such that the class λ_{prim}, given by P_λ as in (1), is the class of a fake linear cycle.

We point out that the condition on the c_i's not all being d-th roots of -1 simultaneously is to avoid that λ_{prim} becomes the class of a true linear cycle. Since the Hodge conjecture is known for these Fermat varieties [Shioda 1979] we know that fake linear cycles are rational combinations of linear cycles. The proof of the above result follows after a first-order analysis of the Hodge loci.

Curiously Fermat varieties of degrees $d = 3, 4, 6$ correspond exactly to those where the group $H^n(X_d^n, \mathbb{Z})_{\mathrm{alg}}$ of algebraic cycles has maximal rank $h^{n/2,n/2}$ (see Proposition 2.6 and [Beauville 2014] for a survey on these rare-to-find varieties). The subtle part of the above result is showing the existence of c_λ in such a way that the corresponding class is a Hodge class. For this is necessary to describe the Galois action of $\mathbb{Q}(\zeta_{2d})/\mathbb{Q}$ on the space of totally decomposable Hodge monomials in the sense of [Shioda 1979]. An immediate consequence of Theorem 1.1 is that the Artinian Gorenstein ideal associated to each fake linear cycle is of the form

$$J^F = \langle x_0 - c_0 x_1, x_2 - c_2 x_3, \ldots, x_n - c_n x_{n+1}, x_0^{d-1}, \ldots, x_{n+1}^{d-1} \rangle. \tag{2}$$

The name fake linear cycle is inspired from this fact and the principle introduced in [Movasati and Sertöz 2021] which predicts that for "good enough" algebraic cycles, one should obtain the supporting equations of a representative of the cycle as generators of $J^{F,\lambda}$ for small degrees. It was proved by Cifani, Pirola and Schlesinger [Cifani et al. 2023] that all arithmetically Cohen–Macaulay curves inside a smooth surface in $\mathbb{P}^3$ satisfy this principle, which says that the curve can be *reconstructed from its periods*. It was also shown by them that not all curves can be reconstructed from their periods (for example, a rational degree 4 curve inside a quartic). After (2) we see that fake linear cycles provide more examples (of any dimension) of algebraic cycles which cannot be reconstructed from their periods. In fact, otherwise the supporting equations of the cycle should be the $\frac{n}{2}+1$ equations of degree 1 which define a $\frac{n}{2}$-dimensional linear subvariety inside $\mathbb{P}^{n+1}$, but this linear variety is never contained in X_d^n.

Beside the above anomalous properties of fake linear cycles, we show that their associated Hodge loci are nonreduced, completing thus the proof of following result.

Theorem 1.2. *For n even and $d \geq 2 + \frac{6}{n}$ the unique component of minimal codimension of the Hodge locus* $\mathrm{HL}_{n,d}$ *passing through the Fermat variety is* $\Sigma_{(1,\ldots,1)}$, *that is, the one parametrizing hypersurfaces containing linear subvarieties of dimension* $\frac{n}{2}$.

For the proof of Theorem 1.2 it is necessary to compute the quadratic fundamental form of the Hodge loci associated to fake linear cycles. For this we rely on the description of this second-order invariant of the IVHS introduced in Theorem 7 of [Maclean 2005].

The text is organized as follows. In Section 2 we recall the cohomology and homology of Fermat varieties. Section 3 is devoted to the computation of the field of definition of totally decomposable Hodge monomials, together with the explicit description of the Galois action on them (see Proposition 3.7). In Section 4 we recall the basic results and notation about the Artinian Gorenstein ideal associated to a Hodge cycle based on [Villaflor Loyola 2022b]. The proof of Theorem 1.1 is given in Section 5. Section 6 is devoted to the computation of the quadratic fundamental form associated to each fake linear cycle and the proof of Theorem 1.2.

2. Topology of Fermat varieties

In this section we describe the homology and cohomology groups of Fermat varieties. For this we start by recalling the notation and main results of [Shioda 1979]. Let

$$X_d^n := \{F := x_0^d + \cdots + x_{n+1}^d = 0\}$$

be the n-dimensional Fermat variety of degree d. Shioda described the cohomology groups $H^n_{\mathrm{dR}}(X^n_d)$ in terms of a spectral decomposition compatible with the Hodge decomposition. This decomposition goes as follows. Let

$$G^n_d := (\mu_d)^{n+2}/\Delta(\mu_d),$$

where $\mu_d := \langle \zeta_d \rangle \simeq \mathbb{Z}/d\mathbb{Z}$ is the group of d-th roots of unity. The above group acts on X^n_d by coordinate-wise multiplication:

$$g = (g_0, \dots, g_{n+1}), \quad g \cdot x = (g_0 \cdot x_0 : \dots : g_{n+1} \cdot x_{n+1}). \tag{3}$$

The dual group $\hat{G}^n_d$ corresponds to the group of characters

$$\hat{G}^n_d := \{\alpha = (a_0, \dots, a_{n+1}) \in (\mathbb{Z}/d\mathbb{Z})^{n+2} : a_0 + \dots + a_{n+1} = 0\}$$

whose pairing with G^n_d is

$$\alpha(g) := g_0^{a_0} \cdots g_{n+1}^{a_{n+1}}.$$

The action of G^n_d on X^n_d induces an action of G^n_d on $H^n(X^n_d, \mathbb{Z})$ and $H^n(X^n_d, \mathbb{Z})_{\mathrm{prim}}$, which naturally extends to $H^n(X^n_d, \mathbb{Z})_{\mathrm{prim}} \otimes \mathbb{C} \simeq H^n_{\mathrm{dR}}(X^n_d)_{\mathrm{prim}}$. We have the decomposition

$$H^n_{\mathrm{dR}}(X^n_d)_{\mathrm{prim}} = \bigoplus_{\alpha \in \hat{G}^n_d} V(\alpha), \tag{4}$$

which is finer than the Hodge decomposition, and where

$$V(\alpha) := \{\omega \in H^n_{\mathrm{dR}}(X^n_d)_{\mathrm{prim}} : g^*\omega = \alpha(g)\omega, \forall g \in G^n_d\}.$$

The following is the main result of [Shioda 1979].

Theorem 2.1 (Shioda). (i) $\dim V(\alpha) = 1$ *if* $a_0 \cdots a_{n+1} \neq 0$, *and* $V(\alpha) = 0$ *otherwise.*

(ii) *Each piece of the Hodge decomposition corresponds to*

$$H^{p,q}(X^n_d)_{\mathrm{prim}} = \bigoplus_{|\alpha| = q+1} V(\alpha),$$

where $|\alpha| := \frac{1}{d} \sum_{i=0}^{n+1} \bar{a}_i$, *and* $\bar{a}_i \in \{0, \dots, d-1\}$ *is the residue of* a_i *modulo* d.

(iii) *If* n *is even, then*

$$(H^{n/2,n/2}(X^n_d)_{\mathrm{prim}} \cap H^n(X^n_d, \mathbb{Z})) \otimes \mathbb{C} = \bigoplus_{\alpha \in \mathcal{B}^n_d} V(\alpha)$$

with

$$\mathcal{B}^n_d := \left\{\alpha \in \hat{G}^n_d : |t \cdot \alpha| = \frac{n}{2} + 1, \forall t \in (\mathbb{Z}/d\mathbb{Z})^\times\right\}.$$

The previous result can be complemented with Griffiths' basis theorem [1969a; 1969b]. This theorem describes the primitive cohomology classes of any smooth hypersurface $X = \{F = 0\} \subseteq \mathbb{P}^{n+1}$ in terms of the Jacobian ring $R^F := \mathbb{C}[x_0, \dots, x_{n+1}]/J^F$, where $J^F := \langle \partial F/\partial x_0, \dots, \partial F/\partial x_{n+1}\rangle$ is the Jacobian ideal. This description is compatible with the Hodge filtration and is done via the residue map as follows:

$$R^F_{d(q+1)-n-2} \xrightarrow{\sim} F^p H^n_{\mathrm{dR}}(X)_{\mathrm{prim}}/F^{p+1}H^n_{\mathrm{dR}}(X)_{\mathrm{prim}}, \qquad P \mapsto \omega_P := \mathrm{res}\left(\frac{P\Omega}{F^{q+1}}\right).$$

In the particular case of the Fermat variety one has

$$H^n_{\mathrm{dR}}(X^n_d)_{\mathrm{prim}} = \bigoplus_{\beta} \mathbb{C}\cdot\omega_\beta, \tag{5}$$

where

$$\omega_\beta = \mathrm{res}\left(\frac{x^\beta\Omega}{F^{n/2+1}}\right)$$

and $\beta = (\beta_0, \dots, \beta_{n+1})$ with $\beta_i \in \{0, \dots, d-2\}$ such that $\frac{1}{d}(\deg(x^\beta)+n+2) \in \mathbb{Z}$. The relation between Griffiths' decomposition (5) and Shioda's decomposition (4) is clarified by the following proposition.

Proposition 2.2. *Let $\alpha = (a_0, \dots, a_{n+1}) \in \hat{G}^n_d$ be such that $a_0 \cdots a_{n+1} \neq 0$. Then*

$$V(\alpha) = \mathbb{C}\cdot\omega_\beta,$$

where $\beta_i = \overline{a_i} - 1$ for all $i = 0, \dots, n+1$. In particular for any polynomial $P \in R^F_{(d-2)(n/2+1)}$

$$\omega_P \in (H^{n/2,n/2}(X^n_d)_{\mathrm{prim}} \cap H^n(X^n_d, \mathbb{Z})) \otimes \mathbb{C} \quad \text{if and only if} \quad P \in \bigoplus_{\substack{\alpha\in\mathcal{B}^n_d \\ V(\alpha)=\mathbb{C}\cdot\omega_\beta}} \mathbb{C}\cdot x^\beta.$$

Proof. By item (i) of Theorem 2.1 it is enough to show that $\omega_\beta \in V(\alpha)$ for $\alpha = (a_0, \dots, a_{n+1})$ with $a_0 \cdots a_{n+1} \neq 0$ and $\beta_i = \overline{a_i} - 1$. Let $g = (\zeta_d^{c_0}, \dots, \zeta_d^{c_{n+1}}) \in G^n_d$. Then

$$g^*\omega_\beta = \zeta_d^{\sum_{j=0}^{n+1}(\beta_j+1)c_j}\omega_\beta = \zeta_d^{\sum_{j=0}^{n+1}a_jc_j}\omega_\beta = \alpha(g)\omega_\beta. \qquad \square$$

Remark 2.3. Note that the forms $\omega_\beta \in V(\alpha)$ for $\alpha \in \mathcal{B}^n_d$ are not Hodge cycles. In general one can show that $\omega_\beta \in H^{n/2,n/2}(X^n_d)_{\mathrm{prim}} \cap H^n(X^n_d, \overline{\mathbb{Q}})$ assuming the Hodge conjecture.

Remark 2.4. As a consequence of Theorem 2.1, one can show the Hodge conjecture for several Fermat varieties [Shioda 1979] including those of degree $d = 3, 4, 6$. By an elementary argument one can characterize these Fermat varieties as those where the group $H^n(X^n_d, \mathbb{Z})_{\mathrm{alg}}$ of algebraic cycles has maximal rank $h^{n/2,n/2}$. Part of this was already noted in Proposition 11 of [Beauville 2014] and in Corollary 15.1 of [Movasati 2021]. For the sake of completeness we will provide the argument here, starting with an elementary number theory fact which will be also used later in Proposition 5.8.

Lemma 2.5. *Let $d \geq 5$ and $d \neq 6$ be a integer. Consider $q := \min\{p \text{ prime} : p \nmid 2d\}$. Then $q < \frac{d}{2}$ or $q = \frac{d+1}{2}$. The second case only holds for $d = 5, 9$.*

Proof. If $d = 4k$, then $\gcd\big(2d, \frac{d}{2}-1\big) = 1$, and therefore every prime $p|\big(\frac{d}{2}-1\big)$ satisfies that $p \nmid 2d$ and $p < \frac{d}{2}$. Similarly, if $d = 4k+2$, then $\gcd\big(2d, \frac{d}{2}-2\big) = 1$ and we can take $p|\big(\frac{d}{2}-2\big)$. If $d = 4k+3$, then $\gcd\big(2d, \frac{d-1}{2}\big) = 1$ and we can take $p|\frac{d-1}{2}$. If $d = 4k+1$, then $\gcd\big(2d, \frac{d+1}{2}\big) = 1$ and so taking $p|\frac{d+1}{2}$ we conclude that $q \le \frac{d+1}{2}$, i.e., $q \le \frac{d+1}{2} - 1 < \frac{d}{2}$ unless $q = \frac{d+1}{2}$. To see that this only happens for $d = 5, 9$ note that if $q = p_n$ is the n-th prime number, then $p_2 \cdots p_{n-1} \mid d = 2p_n - 1$. One sees that $p_2 \cdots p_{n-1}$ quickly becomes bigger than $2p_n - 1$ for $n \ge 4$. □

Proposition 2.6. *For even-dimensional Fermat varieties X^n_d one has*

$$\operatorname{rank} H^n(X^n_d, \mathbb{Z})_{\mathrm{alg}} = h^{n/2,n/2} \quad \textit{if and only if} \quad \varphi(d) \le 2 \ (d = 1, 2, 3, 4, 6).$$

Proof. Let us note first that if $\varphi(d) \le 2$, we know the Hodge conjecture by [Shioda 1979] and so it is enough to show, by Theorem 2.1(iii), that for all $\alpha \in \hat{G}^n_d$ with $|\alpha| = \frac{n}{2} + 1$ one has

$$|t \cdot \alpha| = \frac{n}{2} + 1 \quad \forall t \in (\mathbb{Z}/d\mathbb{Z})^\times. \tag{6}$$

This is trivial if $\varphi(d) = 1$, and for $\varphi(d) = 2$ we have $(\mathbb{Z}/d\mathbb{Z})^\times = \{1, d-1\}$ where the result is also clear. Conversely, if $\varphi(d) > 2$ let us construct some $\alpha \in \hat{G}^n_d$ with $|\alpha| = \frac{n}{2} + 1$ not satisfying (6). Note that if we find such an α for $n = 2$, then to construct one for any $n \ge 4$ is easy by just adding pairs of entries of the form $(1, d-1)$. Thus we are reduced to the case $n = 2$. Let us consider first the case $d \ne 5, 9$. By Lemma 2.5 there exists some $k \in \{2, 3, \ldots, d-1\}$ such that

$$\frac{d}{k+1} < q < \frac{d}{k}, \quad \text{where } q := \min\{p \text{ prime} : p \nmid 2d\}.$$

We claim the desired character is any

$$\alpha = (aq, bq, cq, 2d - (k+1)q)$$

such that $a + b + c = k + 1$ with $a, b, c \in \{1, 2, \ldots, k\}$. In fact, $|\alpha| = 2$ but if $t = q^{-1} \in (\mathbb{Z}/d\mathbb{Z})^\times$ then

$$|t \cdot \alpha| = |(a, b, c, r)| = \frac{k+1+r}{d} < 2.$$

Finally for the cases $d = 5, 9$ consider the characters $\alpha = (2, 2, 2, 4), (5, 5, 5, 3)$, respectively, and $t = 2$. □

Let us turn now to the homology groups of Fermat varieties. For this let us denote by

$$U^n_d := \{(x_1, \ldots, x_{n+1}) \in \mathbb{C}^{n+1} : 1 + x_1^d + \cdots + x_{n+1}^d = 0\} = X^n_d \cap \mathbb{C}^{n+1}$$

the affine Fermat variety. A basis for $H_n(U^n_d, \mathbb{Z})$ is given by the so-called *vanishing cycles*.

Definition 2.7. For every $\beta \in \{0, \ldots, d-2\}^{n+1}$ consider the homological cycle

$$\delta_\beta := \sum_{a \in \{0,1\}^{n+1}} (-1)^{\sum_{i=1}^{n+1}(1-a_i)} \Delta_{\beta+a},$$

where $\Delta_{\beta+a} : \Delta^n := \left\{(t_1, \ldots, t_{n+1}) \in \mathbb{R}^{n+1} : t_i \ge 0, \ \sum_{i=1}^{n+1} t_i = 1\right\} \to U^n_d$ is given by

$$\Delta_{\beta+a}(t) := (\zeta_{2d}^{2(\beta_1+a_1)-1} t_1^{1/d}, \zeta_{2d}^{2(\beta_2+a_2)-1} t_2^{1/d}, \ldots, \zeta_{2d}^{2(\beta_{n+1}+a_{n+1})-1} t_{n+1}^{1/d}).$$

Proposition 2.8. *The set $\{\delta_\beta\}_{\beta \in \{0,\ldots,d-2\}^{n+1}}$ is a basis of $H_n(U^n_d, \mathbb{Z})$.*

Proof. This is a well-known fact. For a proof see for instance [Movasati 2021, Remark 7.1]. □

Using the Leray–Thom–Gysin sequence in homology [Movasati 2021, §4.6], it is easy to see that

$$H_n(X_d^n,\mathbb{Q}) = \mathrm{Im}(H_n(U_d^n,\mathbb{Q}) \to H_n(X_d^n,\mathbb{Q})) \oplus \mathbb{Q}\cdot[\mathbb{P}^{n/2+1}\cap X_d^n]. \tag{7}$$

Hence every $\omega \in H^n_{\mathrm{dR}}(X_d^n)$ is determined by its periods over the vanishing cycles and $[\mathbb{P}^{n/2+1}\cap X_d^n]$. Since this last period is zero when $\omega \in H^n_{\mathrm{dR}}(X_d^n)_{\mathrm{prim}}$, we see that every primitive class is determined by its periods over all vanishing cycles. These periods can be explicitly computed following [Deligne 1982] (see Proposition 3.3).

3. Galois action in cohomology

Let $X \subseteq \mathbb{P}^{n+1}$ be a smooth hypersurface of the projective space.

Definition 3.1. For every $\omega \in H^n_{\mathrm{dR}}(X)$, the *field of definition* of ω is

$$\mathbb{Q}_\omega := \mathbb{Q}\biggl(\frac{1}{(2\pi i)^{n/2}}\int_\delta \omega : \delta \in H_n(X,\mathbb{Z})\biggr).$$

Since $H_n(X,\mathbb{Z})$ is finitely generated, $\mathbb{Q}_\omega$ is also finitely generated. This is the field of definition of ω in the following sense:

$$\omega \in H^n(X,\mathbb{Q}_\omega).$$

Definition 3.2. For every $t \in \mathrm{Gal}(\mathbb{Q}_\omega/\mathbb{Q})$ we define the *Galois action in cohomology* as $t(\omega) \in H^n(X,\mathbb{Q}_\omega)$ such that

$$t\biggl(\frac{1}{(2\pi i)^{n/2}}\int_\delta \omega\biggr) = \frac{1}{(2\pi i)^{n/2}}\int_\delta t(\omega), \quad \forall \delta \in H_n(X,\mathbb{Z}).$$

In order to describe the Galois action in the cohomology of Fermat varieties we will use the following elementary result about periods, whose proof can be found in [Deligne 1982, Lemma 7.12; Movasati 2021, Proposition 15.1].

Proposition 3.3. *For a Fermat variety of degree d and even dimension n, let $\omega_\beta \in H^{n/2,n/2}(X_d^n)_{\mathrm{prim}}$ and $\beta' \in \{0,\dots,d-2\}^{n+1}$. Then*

$$\int_{\delta_{\beta'}} \omega_\beta = \frac{1}{d^{n+1}\frac{n}{2}!(2\pi i)} \prod_{i=0}^{n+1} (\zeta_d^{(\beta_i+1)(\beta_i'+1)} - \zeta_d^{(\beta_i+1)\beta_i'})\Gamma\biggl(\frac{\beta_i+1}{d}\biggr),$$

where $\beta_0' := 0$ and Γ is the classical Gamma function.

Using the above formula one can obtain the following elementary result which can also be found as part of [Deligne 1982, Theorem 7.15].

Proposition 3.4. *For every character $\alpha = (a_0,\dots,a_{n+1})$ with $a_0\cdots a_{n+1} \neq 0$,*

$$V(\alpha) \cap H^n(X_d^n,\mathbb{Q}(\zeta_d)) \neq 0.$$

In fact a generator is

$$\eta_\alpha := (2\pi i)^{n/2+1}\frac{\omega_\beta}{\prod_{i=0}^{n+1}\Gamma\left(\frac{a_i}{d}\right)} \in H^n(X_d^n, \mathbb{Q}(\zeta_d))_{\text{prim}},$$

for $\beta_i = a_i - 1$, *and, for every* $t \in (\mathbb{Z}/d\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$,

$$t(\eta_\alpha) = \eta_{t\cdot\alpha}.$$

Proof. This follows directly from the definition of the action, Proposition 3.3 and Theorem 2.1. □

Definition 3.5. We say that a character $\alpha \in \mathcal{B}_d^n$ is *totally decomposable* if we can relabel the entries of α in such a way that

$$\alpha = (a_0, d - a_0, a_2, d - a_2, \ldots, a_n, d - a_n). \tag{8}$$

Remark 3.6. The polynomial P_λ given by (1) is a $\mathbb{C}$-linear combination of the monomials x^β with $\beta_{2j-2} + \beta_{2j-1} = d - 2$ for $j = 1, \ldots, \frac{n}{2}+1$. Each of these β's has an associated character $\alpha \in \mathcal{B}_d^n$ that is totally decomposable with $a_j = \beta_j + 1$. In the following proposition we restrict the field of definition of $\omega_\beta = \mathrm{res}((x^\beta\Omega)/F^{n/2+1})$ where β has associated character α totally decomposable.

Proposition 3.7. *For every* $\alpha = (a_0, a_1, \ldots, a_n, a_{n+1}) \in \mathcal{B}_d^n$ *totally decomposable of the form* (8), *and* $\beta_i = a_i - 1$,

$$\mathbb{Q}_{\omega_\beta} \subseteq \mathbb{Q}(\zeta_{2d}).$$

For every $t \in \mathrm{Gal}(\mathbb{Q}(\zeta_{2d})/\mathbb{Q}) \simeq (\mathbb{Z}/2d\mathbb{Z})^\times$,

$$t(\omega_\beta) = (-1)^{\left(\sum_{j=1}^{n/2+1}(ta_{2j-2} - \overline{ta_{2j-2}})\right)/d}\,\omega_\gamma,$$

where $\omega_\gamma \in V(t\cdot\alpha)$ *and* $\bar{a}$ *denotes the residue of* $a \in \mathbb{Z}$ *modulo* d.

Proof. Consider the class of the linear cycle $\mathbb{P}^{n/2} = \{x_0 - \zeta_{2d}x_1 = \cdots = x_n - \zeta_{2d}x_{n+1} = 0\}$. Then by [Villaflor Loyola 2022a, Theorem 1.1] and Theorem 2.1 we know that

$$\omega_P = \frac{-1}{\frac{n}{2}!\cdot d^{n/2}}[\mathbb{P}^{n/2}]_{\text{prim}} \in H^{n/2,n/2}(X_d^n)_{\text{prim}} \cap H^n(X_d^n, \mathbb{Q}),$$

where

$$P = \zeta_{2d}^{n/2+1}\sum_{\beta\in I} x^\beta \zeta_{2d}^{\beta_1+\beta_3+\cdots+\beta_{n+1}}$$

and

$$I := \left\{(\beta_0, \ldots, \beta_{n+1}) \in \{0, \ldots, d-2\}^{n+2} : \beta_{2j-2} + \beta_{2j-1} = d-2, \forall j = 1, \ldots, \frac{n}{2}+1\right\}.$$

Let us first show that $\mathbb{Q}_{\omega_\beta} \subseteq \mathbb{Q}(\zeta_{2d})$. Since $\mathbb{Q}_{\eta_\alpha} \subseteq \mathbb{Q}(\zeta_d)$ it is enough to show that

$$C_\beta := \frac{\prod_{i=0}^{n+1}\Gamma\left(\frac{a_i}{d}\right)}{(2\pi i)^{n/2+1}} \in \mathbb{Q}(\zeta_{2d}).$$

This could be shown directly by using the properties of the Gamma function, but we will give another proof. Let $K/\mathbb{Q}(\zeta_{2d})$ be a Galois extension such that $C_\beta \in K$. For any $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(\zeta_{2d}))$ we have $\sigma(\omega_P) = \omega_P$, since it is a rational class. Hence by Proposition 3.4

$$\sum_{\beta\in I} \zeta_{2d}^{a_1+a_3+\cdots+a_{n+1}} \sigma(C_\beta)\cdot\eta_\alpha = \sum_{\beta\in I} \zeta_{2d}^{a_1+a_3+\cdots+a_{n+1}} C_\beta\cdot\eta_\alpha.$$

In other words $\sigma(C_\beta) = C_\beta$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(\zeta_{2d}))$, i.e., $C_\beta \in \mathbb{Q}(\zeta_{2d})$ as claimed. Let us now compute the Galois action of $\mathrm{Gal}(\mathbb{Q}(\zeta_{2d})/\mathbb{Q})$ on ω_β. Let $t \in \mathrm{Gal}(\mathbb{Q}(\zeta_{2d})/\mathbb{Q}) \simeq (\mathbb{Z}/2d\mathbb{Z})^\times$. Then, again, $t(\omega_P) = \omega_P$, since ω_P is a rational class. Expanding this equality we have

$$\sum_{\beta\in I} \zeta_{2d}^{t(a_1+a_3+\cdots+a_{n+1})} t(\omega_\beta) = \sum_{\beta\in I} \zeta_{2d}^{a_1+a_3+\cdots+a_{n+1}} \omega_\beta.$$

Since by Proposition 3.4 we know $t(\omega_\beta) = C\cdot\omega_\gamma$ for some $C \in \mathbb{Q}(\zeta_{2d})^\times$ and $\omega_\gamma \in V(t\cdot\alpha)$, we get that

$$\zeta_{2d}^{t(a_1+a_3+\cdots+a_{n+1})} t(\omega_\beta) = \zeta_{2d}^{\overline{ta_1}+\overline{ta_3}+\cdots+\overline{ta_{n+1}}} \omega_\gamma$$

and the result follows. For the last equality just note that $t(\omega_\beta) = t(C_\beta)\cdot\eta_{t\cdot\alpha}$. □

Remark 3.8. Using Euler's reflection formula we can compute explicitly

$$C_\beta = \frac{\prod_{j=1}^{n/2+1} \Gamma\left(\frac{a_{2j-2}}{d}\right)\Gamma\left(1-\frac{a_{2j-2}}{d}\right)}{(2\pi i)^{n/2+1}} = \frac{\prod_{j=1}^{n/2+1} \frac{\pi}{\sin(\pi a_{2j-2}/d)}}{(2\pi i)^{n/2+1}} = \prod_{j=1}^{n/2+1} \frac{1}{\zeta_{2d}^{a_{2j-2}} - \zeta_{2d}^{-a_{2j-2}}}.$$

4. Artinian Gorenstein ideal associated to a Hodge cycle

For the sake of completeness we will briefly recall some known facts about Artinian Gorenstein ideals associated to Hodge cycles in smooth hypersurfaces of the projective space. Our main aim is to settle the notation we will use in the rest of the article and to gather some facts from [Villaflor Loyola 2022b].

Definition 4.1. A graded $\mathbb{C}$-algebra R is *Artinian Gorenstein* if there exist $\sigma \in \mathbb{N}$ such that

(i) $R_e = 0$ for all $e > \sigma$,

(ii) $\dim_{\mathbb{C}} R_\sigma = 1$,

(iii) the multiplication map $R_i \times R_{\sigma-i} \to R_\sigma$ is a perfect pairing for all $i = 0, \ldots, \sigma$.

The number $\sigma =: \mathrm{soc}(R)$ is the *socle of* R. We say that an ideal $I \subseteq \mathbb{C}[x_0, \ldots, x_{n+1}]$ is *Artinian Gorenstein of socle* $\sigma =: \mathrm{soc}(I)$ if the quotient ring $R = \mathbb{C}[x_0, \ldots, x_{n+1}]/I$ is Artinian Gorenstein of socle σ.

The definition of the following ideal appeared first in the work of Voisin [1989] for surfaces, and later in the work of Otwinowska [2003] for higher dimensional varieties.

Definition 4.2. Let $X = \{F = 0\} \subseteq \mathbb{P}^{n+1}$ be a smooth degree d hypersurface of even dimension n, and $\lambda \in H^{n/2,n/2}(X,\mathbb{Z})$ be a nontrivial Hodge cycle. Consider $J^F := \langle \partial F/\partial x_0, \ldots, \partial F/\partial x_{n+1}\rangle$ to be the

Jacobian ideal; we define the *Artinian Gorenstein ideal associated to* λ as

$$J^{F,\lambda} := (J^F : P_\lambda), \tag{9}$$

where $P_\lambda \in \mathbb{C}[x_0, \dots, x_{n+1}]_{(d-2)(n/2+1)}$ is such that $\lambda_{\text{prim}} = \text{res}((P_\lambda \Omega)/F^{n/2+1})^{n/2,n/2}$. This ideal is Artinian Gorenstein of $\text{soc}(J^{F,\lambda}) = (d-2)\left(\frac{n}{2}+1\right) = \frac{1}{2}\,\text{soc}(J^F)$.

The importance of this ideal is due to the following proposition which relates it to the local Hodge locus V_λ associated to the Hodge cycle λ.

Proposition 4.3. *Let $X = \{F = 0\} \subseteq \mathbb{P}^{n+1}$ be a smooth degree d hypersurface of even dimension n, and consider two Hodge cycles $\lambda_1, \lambda_2 \in H^{n/2,n/2}(X, \mathbb{Z})$. Then*

$$J^{F,\lambda_1} = J^{F,\lambda_2} \iff \exists c \in \mathbb{Q}^\times : (\lambda_1 - c \cdot \lambda_2)_{\text{prim}} = 0 \iff V_{\lambda_1} = V_{\lambda_2}.$$

Proof. See [Villaflor Loyola 2022b, Corollary 2.3]. ☐

This ideal encodes in a simple way the information of the first-order approximation of the Hodge loci. In fact the content of the following proposition is a rephrasing of the classical result of Carlson, Green, Griffiths and Harris [Carlson et al. 1983] on the infinitesimal variation of Hodge structure for hypersurfaces.

Proposition 4.4. *Let $T \subseteq \mathbb{C}[x_0, \dots, x_{n+1}]_d$ be the parameter space of smooth degree d hypersurfaces of $\mathbb{P}^{n+1}$, of even dimension n. For $t \in T$, let $X_t = \{F = 0\} \subseteq \mathbb{P}^{n+1}$ be the corresponding hypersurface. For every Hodge cycle $\lambda \in H^{n/2,n/2}(X_t, \mathbb{Z})$, we can compute the Zariski tangent space of its associated Hodge locus V_λ as*

$$T_t V_\lambda = J_d^{F,\lambda},$$

where we have identified $T_t T \simeq \mathbb{C}[x_0, \dots, x_{n+1}]_d$.

Proof. See [Villaflor Loyola 2022b, Propositions 2.1 and 2.2]. ☐

Using the previous result, we can obtain the following technical lemma which is the first step in the proof of Theorem 1.1.

Lemma 4.5. *Let $X_d^n = \{F = 0\}$ be the Fermat variety of even dimension n and degree $d \geq 2 + \frac{6}{n}$. Let $\lambda \in H^{n/2,n/2}(X_d^n, \mathbb{Z})$ be a nontrivial Hodge cycle such that*

$$\text{codim}\, T_0 V_\lambda = \binom{n/2+d}{d} - \left(\frac{n}{2}+1\right)^2.$$

Then there exist $c_\lambda, c_0, c_2, c_4, \dots, c_n \in \mathbb{C}^\times$ such that up to a permutation of the coordinates $\lambda_{\text{prim}} = \text{res}((P_\lambda \Omega)/F^{n/2+1})$, where P_λ is given by (1), that is,

$$P_\lambda = c_\lambda \prod_{j=1}^{n/2+1} \frac{x_{2j-2}^{d-1} - (c_{2j-2}x_{2j-1})^{d-1}}{x_{2j-2} - c_{2j-2}x_{2j-1}}.$$

Proof. This follows from [Villaflor Loyola 2022b, Propositions 4.1 and 5.3]. The final assertion that $\text{res}((P_\lambda \Omega)/F^{n/2+1}) = \text{res}((P_\lambda \Omega)/F^{n/2+1})^{n/2,n/2}$ follows from Theorem 2.1 [Shioda 1979, Theorem 1]. ☐

5. Proof of Theorem 1.1

In this section we will prove Theorem 1.1, thus characterizing fake linear cycles as residue forms. In order to do this we will first bound the field of definition of all fake linear cycles by computing their periods; then we will characterize them as those invariant under the Galois action.

Proposition 5.1. *In the same context of Lemma 4.5 we have that $c_\lambda \in \mathbb{Q}(\zeta_{2d})^\times$ and $c_0, c_2, \dots, c_n \in \zeta_{2d}^{-3} \cdot \mathbb{S}^1_{\mathbb{Q}(\zeta_d)} = \{\zeta_{2d}^{-3} \cdot z \in \mathbb{Q}(\zeta_{2d}) : z \in \mathbb{Q}(\zeta_d) \text{ and } |z| = 1\}$. Consequently, λ_{prim} is a $\mathbb{Q}(\zeta_{2d})$-linear combination of residue forms ω_β with $\mathbb{Q}_{\omega_\beta} \subseteq \mathbb{Q}(\zeta_{2d})$.*

Proof. Since $\lambda_{\text{prim}} = \operatorname{res}((P_\lambda\Omega)/F^{n/2+1})$ is a Hodge class, all its periods are rational numbers. Using the formula given by Proposition 3.3 together with Remark 3.8 we have that

$$\begin{aligned}
\frac{1}{(2\pi i)^{n/2}} \int_{\delta_{\beta'}} \lambda_{\text{prim}} &= \frac{c_\lambda}{d^{n/2+1} \cdot \frac{n}{2}!} \sum_{\beta \in I} \prod_{j=1}^{n/2+1} \frac{c_{2j-2}^{\beta_{2j-1}}}{\zeta_{2d}^{\beta_{2j-2}+1} - \zeta_{2d}^{-\beta_{2j-2}-1}} \prod_{i=0}^{n+1} (\zeta_d^{(\beta_i+1)(\beta'_i+1)} - \zeta_d^{(\beta_i+1)\beta'_i}) \\
&= \frac{c_\lambda}{d^{n/2+1} \cdot \frac{n}{2}!} \sum_{\beta \in I} c_0^{\beta_1} \cdot c_2^{\beta_3} \cdots c_n^{\beta_{n+1}} \zeta_{2d}^{\beta_0+\beta_2+\cdots+\beta_n+n/2+1} \cdot \zeta_d^{\sum_{i=0}^{n+1}(\beta_i+1)\beta'_i} \frac{\prod_{i=0}^{n+1}(\zeta_d^{\beta_i+1}-1)}{\prod_{j=1}^{n/2+1}(\zeta_d^{\beta_{2j-2}+1}-1)} \\
&= \frac{c_\lambda (c_0 c_2 \cdots c_n)^{-1}}{d^{n/2+1} \cdot \frac{n}{2}!} \sum_{\beta_1, \beta_3, \dots, \beta_{n+1}=0}^{d-2} \prod_{j=1}^{n/2+1} (\zeta_{2d}^{-1} c_{2j-2} \zeta_d^{\beta'_{2j-1}-\beta'_{2j-2}})^{\beta_{2j-1}+1} (1 - \zeta_d^{\beta_{2j-1}+1}) \\
&= \frac{c_\lambda (c_0 c_2 \cdots c_n)^{-1}}{d^{n/2+1} \cdot \frac{n}{2}!} \prod_{j=1}^{n/2+1} \left(\sum_{\ell=1}^{d-1} (c_{2j-2} \zeta_{2d}^{2(\beta'_{2j-1}-\beta'_{2j-2})-1})^\ell - (c_{2j-2} \zeta_{2d}^{2(\beta'_{2j-1}-\beta'_{2j-2})+1})^\ell \right) \\
&= \frac{c_\lambda (c_0 c_2 \cdots c_n)^{-1}}{d^{n/2+1} \cdot \frac{n}{2}!} \prod_{j=1}^{n/2+1} E_{j,\beta'} \in \mathbb{Q}, \quad \forall \beta' \in \{0, 1, \dots, d-2\}^{n+1},
\end{aligned}$$

where each $E_{j,\beta'}$ equals $\sum_{\ell=1}^{d-1} (c_{2j-2} \zeta_{2d}^{2(\beta'_{2j-1}-\beta'_{2j-2})-1})^\ell - (c_{2j-2} \zeta_{2d}^{2(\beta'_{2j-1}-\beta'_{2j-2})+1})^\ell$. If $c_{2j-2}^d = -1$, we can always choose some $\beta'_{2j-1}, \beta'_{2j-2} \in \{0, 1, \dots, d-2\}$ such that $E_{j,\beta'} \neq 0$. Let us define

$$S := \left\{ j \in \left\{ 1, 2, \dots, \frac{n}{2} + 1 \right\} : c_{2j-2}^d = -1 \right\}$$

and consider the set $\mathfrak{B}$ of all $\beta' \in \{0, 1, \dots, d-2\}^{n+1}$ such that the value of $E_{j,\beta'} \neq 0$ is fixed for every $j \in S$. For every $\beta' \in \mathfrak{B}$ we have that for $j \notin S$

$$E_{j,\beta'} = \frac{c_{2j-2}(c_{2j-2}^d + 1) \zeta_{2d}^{2(\beta'_{2j-1}-\beta'_{2j-2})-1} (1 - \zeta_d)}{(c_{2j-2} \cdot \zeta_{2d}^{2(\beta'_{2j-1}-\beta'_{2j-2})-1} - 1)(c_{2j-2} \cdot \zeta_{2d}^{2(\beta'_{2j-1}-\beta'_{2j-2})+1} - 1)} \neq 0.$$

It is clear that $c_{2j-2} \in \zeta_{2d}^{-3} \cdot \mathbb{S}^1_{\mathbb{Q}(\zeta_d)}$ for $j \in S$. In order to show that $c_{2j-2} \in \zeta_{2d}^{-3} \cdot \mathbb{S}^1_{\mathbb{Q}(\zeta_d)}$ for $j \notin S$, fix some $j_0 \notin S$ and consider two $\beta', \beta'' \in \mathfrak{B}$ such that $E_{j,\beta'} = E_{j,\beta''}$ for all $j \neq j_0$ and $\beta'_{2j_0-1} - \beta'_{2j_0-2} = 1$,

$\beta''_{2j_0-1} - \beta''_{2j_0-2} = 0$. Then

$$\frac{\int_{\delta_{\beta'}} \lambda_{\text{prim}}}{\int_{\delta_{\beta''}} \lambda_{\text{prim}}} = \frac{E_{j_0,\beta'}}{E_{j_0,\beta''}} = \frac{\zeta_d(c_{2j_0-2}\cdot\zeta_{2d}^{-1}-1)}{c_{2j_0-2}\cdot\zeta_{2d}^{3}-1} = q \in \mathbb{Q}^\times$$

and so

$$c_{2j_0-2} = \frac{q-\zeta_d}{\zeta_{2d}^3(q-\zeta_d^{-1})} \in \zeta_{2d}^{-3}\cdot\mathbb{S}^1_{\mathbb{Q}(\zeta_d)}.$$

Finally, since for every $\beta' \in \mathfrak{B}$ we know that $E_{j,\beta'} \in \mathbb{Q}(\zeta_{2d})$, it follows from the above formula for $1/(2\pi i)^{n/2}\int_{\delta_{\beta'}} \lambda_{\text{prim}} \in \mathbb{Q}$ that $c_\lambda \in \mathbb{Q}(\zeta_{2d})$. □

Remark 5.2. By Lemma 4.5 and Proposition 5.1 we know that all fake linear cycles are of the form

$$\lambda_{\text{prim}} = \text{res}\left(\frac{P_\lambda\Omega}{F^{n/2+1}}\right)$$

for P_λ given by (1) where $c_\lambda \in \mathbb{Q}(\zeta_{2d})^\times$ and $c_0, c_2, \dots, c_n \in \zeta_{2d}^{-3}\cdot\mathbb{S}^1_{\mathbb{Q}(\zeta_d)}$. In order to complete the proof of Theorem 1.1 we only need to prove that for any choice of $c_0, c_2, \dots, c_n \in \zeta_{2d}^{-3}\cdot\mathbb{S}^1_{\mathbb{Q}(\zeta_d)}$ there exists some $c_\lambda \in \mathbb{Q}(\zeta_{2d})^\times$ such that λ is in fact a Hodge class, that is, such that

$$\mathbb{Q}_\lambda = \mathbb{Q}.$$

In terms of Galois cohomology, to prove the existence of such c_λ, it is equivalent to find a number $c_\lambda \in \mathbb{Q}(\zeta_{2d})^\times$ such that

$$\sigma(\lambda) = \lambda$$

for all $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{2d})/\mathbb{Q})$. This in turn translates into a collection of relations of the form

$$\sigma(c_\lambda) = c_\lambda\cdot\phi_\sigma$$

for some numbers $\phi_\sigma(c_0, c_2, \dots, c_n) \in \mathbb{Q}(\zeta_{2d})^\times$ which can be explicitly computed case by case. Since the set $\{\sigma(c_\lambda)/c_\lambda\}$ is by definition a 1-coboundary in the group cohomology of $G = \text{Gal}(\mathbb{Q}(\zeta_{2d})/\mathbb{Q})$ with coefficients in $\mathbb{Q}(\zeta_{2d})^\times$, the theorem will follow if we show that $\{\phi_\sigma\}$ is a 1-cocycle by the following well-known result which can be found in [Neukirch et al. 2000].

Theorem 5.3 (Hilbert's theorem 90). *If L/K is a finite Galois extension of fields with Galois group $G = \text{Gal}(L/K)$, then the first group cohomology $H^1(G, L^\times)$ equals* $\{1\}$.

Now we are in position to prove Theorem 1.1, but we will divide the proof into the three possible cases $d = 3, 4, 6$. Along all the proofs we will denote by

$$I := \left\{(\beta_0, \dots, \beta_{n+1}) \in \{0, \dots, d-2\}^{n+2} : \beta_{2j-2}+\beta_{2j-1} = d-2, \forall j = 1, \dots, \frac{n}{2}+1\right\}$$

the set of multi-indexes corresponding to the monomials of P_λ given by (1).

Theorem 5.4. *For the Fermat cubic X_3^n with $n \geq 6$, all fake linear cycles are of the form*

$$\lambda_{\text{prim}} = \text{res}\left(\frac{P_\lambda \Omega}{F^{n/2+1}}\right)$$

for P_λ given by (1), where $c_0, c_2, \dots, c_n \in \mathbb{S}^1_{\mathbb{Q}(\zeta_6)}$ but not all are cube roots of -1 simultaneously, and $c_\lambda \in \mathbb{Q}(\zeta_6)^\times$. For any such choice of c_i's, there exists some $c_\lambda \in \mathbb{Q}(\zeta_6)^\times$ such that the class λ_{prim}, given by P_λ as in (1), is the class of a fake linear cycle.

Proof. Since all the monomials of P_λ are totally decomposable, and all their accompanying coefficients belong to $\mathbb{Q}(\zeta_6)$ we know (by Proposition 3.7) that

$$\mathbb{Q}_\lambda \subseteq \mathbb{Q}(\zeta_6).$$

In order to show that $\mathbb{Q}_\lambda = \mathbb{Q}$ it is enough to show that λ is invariant under the action of $\text{Gal}(\mathbb{Q}(\zeta_6)/\mathbb{Q}) = \{\text{id}, \sigma\}$ where $\sigma(\zeta_6) = \zeta_6^{-1} = \overline{\zeta_6}$. In particular for every $\alpha \in \mathbb{Q}(\zeta_6)$, $\alpha = a + b\zeta_6$ for $a, b \in \mathbb{Q}$, and so $\sigma(\alpha) = a + b\overline{\zeta_6} = \bar{\alpha}$. With this we conclude that for $\gamma_i = 1 - \beta_i$

$$\sigma(\lambda) = \sigma(c_\lambda) \sum_{\beta \in I} (-1)^{\left(\sum_{j=1}^{n/2+1}(5(\beta_{2j-2}+1) - \overline{5(\beta_{2j-2}+1)})\right)/3} \omega_\gamma \prod_{j=1}^{n/2+1} c_{2j-2}^{-\beta_{2j-1}}.$$

Hence

$$\sigma(\lambda) = \lambda \quad \text{if and only if} \quad \frac{\sigma(c_\lambda)}{c_\lambda} = (-1)^{n/2+1} c_0 \cdot c_2 \cdots c_n.$$

Since $N((-1)^{n/2+1}c_0 \cdot c_2 \cdots c_n) = |(-1)^{n/2+1}c_0 \cdot c_2 \cdots c_n|^2 = 1$, we know such c_λ always exists by Hilbert's theorem 90. □

Theorem 5.5. *For the Fermat quartic X_4^n with $n \geq 4$, all fake linear cycles are of the form*

$$\lambda_{\text{prim}} = \text{res}\left(\frac{P_\lambda \Omega}{F^{n/2+1}}\right)$$

for P_λ given by (1), where $c_0, c_2, \dots, c_n \in \zeta_8 \cdot \mathbb{S}^1_{\mathbb{Q}(i)}$ but not all are fourth roots of -1 simultaneously, and $c_\lambda \in \mathbb{Q}(\zeta_8)^\times$. For any such choice of c_i's, there exists some $c_\lambda \in \mathbb{Q}(\zeta_8)^\times$ such that the class λ_{prim}, given by P_λ as in (1), is the class of a fake linear cycle.

Proof. Note first that $\zeta_8^{-3} \cdot \mathbb{S}^1_{\mathbb{Q}(\zeta_4)} = \zeta_8 \cdot \mathbb{S}^1_{\mathbb{Q}(i)}$. Since all the monomials of P_λ are totally decomposable, and all their accompanying coefficients belong to $\mathbb{Q}(\zeta_8)$, we see that

$$\mathbb{Q}_\lambda \subseteq \mathbb{Q}(\zeta_8).$$

In order to show that $\mathbb{Q}_\lambda = \mathbb{Q}$ it is enough to show that λ is invariant under the action of $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \{\text{id}, \sigma_3, \sigma_5, \sigma_7\}$ where $\sigma_j(\zeta_8) = \zeta_8^j$. Observe that $\sigma_7(\zeta_8) = \zeta_8^{-1} = \overline{\zeta_8}$. In particular for every $\alpha = a\zeta_8 + b\zeta_8^3 \in \zeta_8 \cdot \mathbb{S}^1_{\mathbb{Q}(i)}$ we have

$$\sigma_3(\alpha) = -\bar{\alpha}, \quad \sigma_5(\alpha) = -\alpha, \quad \sigma_7(\alpha) = \bar{\alpha}.$$

With this and Proposition 3.7 we conclude that for $\gamma_i = 2-\beta_i$

$$\sigma_7(\lambda) = \sigma_7(c_\lambda) \sum_{\beta\in I} (-1)^{\left(\sum_{j=1}^{n/2+1}(7(\beta_{2j-2}+1)-\overline{7(\beta_{2j-2}+1)})\right)/4} \omega_\gamma \prod_{j=1}^{n/2+1} c_{2j-2}^{-\beta_{2j-1}}.$$

Hence

$$\sigma_7(\lambda)=\lambda \quad \text{if and only if} \quad \frac{\sigma_7(c_\lambda)}{c_\lambda} = (-1)^{n/2+1}(c_0\cdot c_2\cdots c_n)^2. \tag{10}$$

On the other hand for $\gamma_i = \beta_i$

$$\sigma_5(\lambda) = \sigma_5(c_\lambda) \sum_{\beta\in I} (-1)^{\left(\sum_{j=1}^{n/2+1}(5(\beta_{2j-2}+1)-\overline{5(\beta_{2j-2}+1)})\right)/4} \omega_\gamma \prod_{j=1}^{n/2+1} (-c_{2j-2})^{\beta_{2j-1}}.$$

Hence

$$\sigma_5(\lambda)=\lambda \quad \text{if and only if} \quad \frac{\sigma_5(c_\lambda)}{c_\lambda} = (-1)^{n/2+1}. \tag{11}$$

Finally for $\gamma_j = 2-\beta_j$

$$\sigma_3(\lambda) = \sigma_3(c_\lambda) \sum_{\beta\in I} (-1)^{\left(\sum_{j=1}^{n/2+1}(3(\beta_{2j-2}+1)-\overline{3(\beta_{2j-2}+1)})\right)/4} \omega_\gamma \prod_{j=1}^{n/2+1} (-c_{2j-2})^{-\beta_{2j-1}}.$$

Hence

$$\sigma_3(\lambda)=\lambda \quad \text{if and only if} \quad \frac{\sigma_3(c_\lambda)}{c_\lambda} = (c_0\cdot c_2\cdots c_n)^2. \tag{12}$$

Equations (10), (11) and (12) imply the existence of the desired c_λ such that $\mathbb{Q}_\lambda = \mathbb{Q}$ if and only if the map $\phi : \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \to \mathbb{Q}(\zeta_8)^\times$ given by

$$\phi(\mathrm{id}) = 1, \quad \phi(\sigma_3) = (c_0\cdot c_2\cdots c_n)^2, \quad \phi(\sigma_5) = (-1)^{n/2+1}, \quad \phi(\sigma_7) = (-1)^{n/2+1}(c_0\cdot c_2\cdots c_n)^2$$

is a 1-coboundary. By Hilbert's theorem 90 we know $H^1(G, L^\times) = \{1\}$ for $L = \mathbb{Q}(\zeta_8)$ and $G = \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ and so we get the existence of the desired $c_\lambda \in \mathbb{Q}(\zeta_8)$ after noting that ϕ is a 1-cocycle by definition. □

Theorem 5.6. *For the Fermat sextic X_6^n with $n \geq 2$, all fake linear cycles are of the form*

$$\lambda_{\mathrm{prim}} = \mathrm{res}\left(\frac{P_\lambda \Omega}{F^{n/2+1}}\right)$$

for P_λ given by (1), where $c_0, c_2, \ldots, c_n \in i\cdot \mathbb{S}^1_{\mathbb{Q}(\zeta_6)}$ but not all are sixth roots of -1 simultaneously, and $c_\lambda \in \mathbb{Q}(\zeta_{12})^\times$. For any such choice of c_i's, there exists some $c_\lambda \in \mathbb{Q}(\zeta_{12})^\times$ such that the class λ_{prim}, given by P_λ as in (1), is the class of a fake linear cycle.

Proof. Note first that all the elements of $\zeta_{12}^{-3}\cdot \mathbb{S}^1_{\mathbb{Q}(\zeta_6)} = i\cdot \mathbb{S}^1_{\mathbb{Q}(\zeta_6)}$ are of the form $a\zeta_{12} + b\zeta_{12}^3$ for $a, b \in \mathbb{Q}$. Since all the monomials of P_λ are totally decomposable, and all their accompanying coefficients belong to $\mathbb{Q}(\zeta_{12})$ we see that

$$\mathbb{Q}_\lambda \subseteq \mathbb{Q}(\zeta_{12}).$$

In order to show that $\mathbb{Q}_\lambda = \mathbb{Q}$ it is enough to show that λ is invariant under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) = \{\mathrm{id}, \sigma_5, \sigma_7, \sigma_{11}\}$ where $\sigma_j(\zeta_{12}) = \zeta_{12}^j$. Observe that $\sigma_{11}(\zeta_{12}) = \zeta_{12}^{-1} = \overline{\zeta_{12}}$. In particular for every $\alpha = a\zeta_{12} + b\zeta_{12}^3$ with $a, b \in \mathbb{Q}$, we have

$$\sigma_5(\alpha) = -\bar{\alpha}, \quad \sigma_7(\alpha) = -\alpha, \quad \sigma_{11}(\alpha) = \bar{\alpha}.$$

With this and Proposition 3.7 we conclude that for $\gamma_i = 4 - \beta_i$

$$\sigma_{11}(\lambda) = \sigma_{11}(c_\lambda) \sum_{\beta \in I} (-1)^{\left(\sum_{j=1}^{n/2+1} (11(\beta_{2j-2}+1) - \overline{11(\beta_{2j-2}+1)})\right)/6} \omega_\gamma \prod_{j=1}^{n/2+1} c_{2j-2}^{-\beta_{2j-1}}.$$

Hence

$$\sigma_{11}(\lambda) = \lambda \quad \text{if and only if} \quad \frac{\sigma_{11}(c_\lambda)}{c_\lambda} = (-1)^{n/2+1}(c_0 \cdot c_2 \cdots c_n)^4. \tag{13}$$

On the other hand for $\gamma_i = \beta_i$

$$\sigma_7(\lambda) = \sigma_7(c_\lambda) \sum_{\beta \in I} (-1)^{\left(\sum_{j=1}^{n/2+1} (7(\beta_{2j-2}+1) - \overline{7(\beta_{2j-2}+1)})\right)/6} \omega_\gamma \prod_{j=1}^{n/2+1} (-c_{2j-2})^{\beta_{2j-1}}.$$

Hence

$$\sigma_7(\lambda) = \lambda \quad \text{if and only if} \quad \frac{\sigma_7(c_\lambda)}{c_\lambda} = (-1)^{n/2+1}. \tag{14}$$

Finally for $\gamma_j = 4 - \beta_j$

$$\sigma_5(\lambda) = \sigma_5(c_\lambda) \sum_{\beta \in I} (-1)^{\left(\sum_{j=1}^{n/2+1} (5(\beta_{2j-2}+1) - \overline{5(\beta_{2j-2}+1)})\right)/6} \omega_\gamma \prod_{j=1}^{n/2+1} (-c_{2j-2})^{-\beta_{2j-1}}.$$

Hence

$$\sigma_5(\lambda) = \lambda \quad \text{if and only if} \quad \frac{\sigma_5(c_\lambda)}{c_\lambda} = (c_0 \cdot c_2 \cdots c_n)^4. \tag{15}$$

Equations (13)–(15) imply the existence of the desired c_λ if and only if $\phi : \mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) \to \mathbb{Q}(\zeta_{12})^\times$ given by

$$\phi(\mathrm{id}) = 1, \quad \phi(\sigma_5) = (c_0 \cdot c_2 \cdots c_n)^4, \quad \phi(\sigma_7) = (-1)^{n/2+1}, \quad \phi(\sigma_{11}) = (-1)^{n/2+1}(c_0 \cdot c_2 \cdots c_n)^4$$

is a 1-coboundary. By Hilbert's theorem 90 we know $H^1(G, L^\times) = \{1\}$ for $L = \mathbb{Q}(\zeta_{12})$ and $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q})$. Thus $c_\lambda \in \mathbb{Q}(\zeta_{12})$ exists since ϕ is by definition a 1-cocycle. □

Remark 5.7. We want to highlight that using the Galois action in cohomology it is also possible to obtain another proof of [Villaflor Loyola 2022b, Theorem 1.1] as follows.

Proposition 5.8. *There are no fake linear cycles inside X_d^n for $d \geq 2 + \frac{6}{n}$ and $d \neq 3, 4, 6$. In other words, for P_λ given by (1) such that $c_\lambda \in \mathbb{Q}(\zeta_{2d})^\times$ and $c_0, c_2, \ldots, c_n \in \mathbb{S}^1_{\mathbb{Q}(\zeta_{2d})}$, we have*

$$c_{2i-2}^d = -1, \quad \textit{for all } i = 1, \ldots, \frac{n}{2} + 1.$$

Proof. Let $t \in (\mathbb{Z}/2d\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{2d})/\mathbb{Q})$. Since ω_{P_λ} is a Hodge class, it is a rational class and so it is invariant under the Galois action, i.e., $t(\omega_{P_\lambda}) = \omega_{P_\lambda}$. Hence we can write

$$\omega_{P_\lambda} = c_\lambda \sum_{\beta\in I} \omega_\beta \prod_{j=1}^{n/2+1} c_{2j-2}^{\beta_{2j-1}}.$$

Applying the action of t we get that

$$t(c_\lambda) \sum_{\beta\in I} t(\omega_\beta) \prod_{j=1}^{n/2+1} t(c_{2j-2}^{\beta_{2j-1}}) = c_\lambda \sum_{\beta\in I} \omega_\beta \prod_{j=1}^{n/2+1} c_{2j-2}^{\beta_{2j-1}},$$

and so

$$t(c_\lambda)\cdot t(\omega_\beta) \prod_{j=1}^{n/2+1} t(c_{2j-2}^{\beta_{2j-1}}) = c_\lambda \cdot \omega_\gamma \prod_{j=1}^{n/2+1} c_{2j-2}^{\gamma_{2j-1}}$$

for $\omega_\beta \in V(\alpha)$, $\omega_\gamma \in V(t\cdot\alpha)$. It follows from Proposition 3.7 that

$$t(c_\lambda)(-1)^{\left(\sum_{j=1}^{n/2+1}(ta_{2j-2}-\overline{ta_{2j-2}})\right)/d} \prod_{j=1}^{n/2+1} t(c_{2j-2}^{d-a_{2j-2}-1}) = c_\lambda \prod_{j=1}^{n/2+1} c_{2j-2}^{\overline{-ta_{2j-2}}-1}$$

holds for all choices of $a_0, a_2, \dots, a_n \in \{1, \dots, d-1\}$. For each $j = 1, \dots, \frac{n}{2}+1$, fix the values of $a_{2i-2} = 1$ for all $i \neq j$, and let a_{2j-2} take two arbitrary values $a, b \in \{1, \dots, d-1\}$ in turn. Dividing one of the resulting identities by the other we obtain

$$(-1)^{(ta-tb-\overline{ta}+\overline{tb})/d}\, t(c_{2j-2}^{b-a}) = c_{2j-2}^{\overline{-ta}-\overline{-tb}}$$

for all $a, b \in \{1, \dots, d-1\}$, or, equivalently,

$$t(\zeta_{2d}^{a-b} c_{2j-2}^{b-a}) = \zeta_{2d}^{\overline{ta}-\overline{tb}} c_{2j-2}^{\overline{tb}-\overline{ta}}. \tag{16}$$

Now, let $q := \min\{p \text{ prime} : p \nmid 2d\}$ as in Lemma 2.5; hence, $\gcd(2d, 2d-q) = 1$ and $q < \frac{d}{2}$ or $q = \frac{d+1}{2}$. If $q < \frac{d}{2}$, there exists $k \in \{2, 3, \dots, d-2\}$ such that $\frac{d}{k+1} < q < \frac{d}{k}$. In this case we have

$$(1-k)(\overline{2d-q}) - \overline{(k+1)(2d-q)} + k(\overline{2(2d-q)}) = -d. \tag{17}$$

Using (16) for $t = 2d-q$ we have

$$\begin{aligned}\zeta_{2d}^{k(2d-q)+\overline{2d-q}-\overline{(k+1)(2d-q)}} c_{2j-2}^{\overline{(k+1)(2d-q)}-\overline{2d-q}} &= t(c_{2j-2}^k) \\ &= \zeta_{2d}^{k((2d-q)+\overline{2d-q}-\overline{2(2d-q)})} c_{2j-2}^{k(\overline{2(2d-q)}-\overline{2d-q})},\end{aligned}$$

and therefore $\zeta_{2d}^{(1-k)(\overline{2d-q})-\overline{(k+1)(2d-q)}+k(\overline{2(2d-q)})} = c_{2j-2}^{(1-k)(\overline{2d-q})-\overline{(k+1)(2d-q)}+k(\overline{2(2d-q)})}$. By (17) we conclude that $c_{2j-2}^d = -1$. In the case where $q = \frac{d+1}{2}$ the argument above works taking $k = 2$ in (17), which is then equal to d instead of $-d$. $\square$

6. Quadratic fundamental form and proof of Theorem 1.2

In this final section we recall the quadratic fundamental form described in [Maclean 2005]. Her result was described in the context of surfaces for the classical Noether–Lefschetz loci, however in higher dimensions it also gives a partial description of the quadratic fundamental form which is enough for our purposes. Since the original proof applies word by word to the general case we will omit it.

Definition 6.1. Let M be a smooth m-dimensional analytic scheme, V a vector bundle on M and σ a section of V. Let W be the zero locus of σ and let $x \in W$. The *quadratic fundamental form of σ at x* is

$$q_{\sigma,x} : T_x W \otimes T_x W \to V_x / \operatorname{Im}(d\sigma_x)$$

given in local coordinates $(z_1, \dots, z_m)$ around x by

$$q_{\sigma,x}\left(\sum_{i=1}^{m} \alpha_i \frac{\partial}{\partial z_i}, \sum_{j=1}^{m} \beta_j \frac{\partial}{\partial z_j}\right) = \sum_{i=1}^{m} \alpha_i \frac{\partial}{\partial z_i}\left(\sum_{j=1}^{m} \beta_j \frac{\partial}{\partial z_j}(\sigma)\right).$$

In our context we will take $M = (T, 0)$, $V = \bigoplus_{p=0}^{n/2-1} \mathcal{F}^p/\mathcal{F}^{p+1}$ and $x = 0$, where $T \subseteq H^0(\mathcal{O}_{\mathbb{P}^{n+1}}(d))$ is the parameter space of smooth degree d hypersurfaces of $\mathbb{P}^{n+1}$, $\pi : X \to T$ is the corresponding family, $\mathcal{F}^p = R^n \pi_* \Omega^{\bullet \geq p}_{X/T}$, and $0 \in T$ corresponds to the Fermat variety. In order to construct a section σ of V around x, let $\lambda \in H^{n/2,n/2}(X^n_d)_{\mathrm{prim}} \cap H^n(X^n_d, \mathbb{Z})$ be a Hodge cycle, and consider $\bar{\lambda}$ its induced flat section in $\mathcal{F}^0/\mathcal{F}^{n/2}$. If we fix a holomorphic splitting $\mathcal{F}^0/\mathcal{F}^{n/2} \simeq V$ and we take σ as the image of $\bar{\lambda}$ under this splitting, then $W = V_\lambda$. In this context we can identify $T_x W = J^{F,\lambda}_d$ (Proposition 4.4), $V_x = \bigoplus_{q=n/2+1}^{n} R^F_{d(q+1)-n-2}$ and $d\sigma_x = \cdot P_\lambda$. The computation of the degree $d\left(\frac{n}{2}+2\right) - n - 2$ piece of $q = q_{\sigma,x}$ under these identifications was done in Theorem 7 of [Maclean 2005] as follows.

Theorem 6.2 (Maclean). *The degree $r := d\left(\frac{n}{2}+2\right) - n - 2$ piece of the fundamental quadratic form*

$$q : \operatorname{Sym}^2(J^{F,\lambda}_d) \to \bigoplus_{q=n/2+1}^{n} R^F_{d(q+1)-n-2}/\langle P_\lambda \rangle$$

is given by

$$q_r(G, H) = \sum_{i=0}^{n+1} \left(H \frac{\partial Q_i}{\partial x_i} - R_i \frac{\partial G}{\partial x_i} \right),$$

where

$$G \cdot P_\lambda = \sum_{i=0}^{n+1} Q_i \frac{\partial F}{\partial x_i} \quad \textit{and} \quad H \cdot P_\lambda = \sum_{i=0}^{n+1} R_i \frac{\partial F}{\partial x_i}.$$

Proposition 6.3. *Let $\lambda \in H^{n/2,n/2}(X^n_d)_{\mathrm{prim}} \cap H^n(X^n_d, \mathbb{Z})$ be a fake linear cycle given by (1), and consider*

$$G := (x_{2i-2} - c_{2i-2} x_{2i-1}) \cdot D \in J^{F,\lambda}_d.$$

Then

$$q_r(G, G) = \frac{-c_\lambda}{d} \prod_{j \neq i} \left(\frac{x^{d-1}_{2j-2} - (c_{2j-2} x_{2j-1})^{d-1}}{x_{2j-2} - c_{2j-2} x_{2j-1}} \right) \cdot D^2 \cdot (c^d_{2i-2} + 1).$$

Proof. Just note that

$$G \cdot P_\lambda = c_\lambda \prod_{j\neq i}\left(\frac{x_{2j-2}^{d-1}-(c_{2j-2}x_{2j-1})^{d-1}}{x_{2j-2}-c_{2j-2}x_{2j-1}}\right)\cdot D\cdot (x_{2i-2}^{d-1}-(c_{2i-2}x_{2i-1})^{d-1}).$$

Hence $Q_j=0$ for $j\neq 2i-2, 2i-1$ and

$$Q_{2i-2}=\frac{c_\lambda}{d}\prod_{j\neq i}\left(\frac{x_{2j-2}^{d-1}-(c_{2j-2}x_{2j-1})^{d-1}}{x_{2j-2}-c_{2j-2}x_{2j-1}}\right)\cdot D,\quad Q_{2i-1}=\frac{-c_\lambda\cdot c_{2i-2}^{d-1}}{d}\prod_{j\neq i}\left(\frac{x_{2j-2}^{d-1}-(c_{2j-2}x_{2j-1})^{d-1}}{x_{2j-2}-c_{2j-2}x_{2j-1}}\right)\cdot D.$$

The result follows now by a direct computation of Maclean's formula. □

Proof of Theorem 1.2. After Theorem 1.1 we just need to show that

$$\operatorname{codim} V_\lambda > \binom{n/2+d}{d}-\left(\frac{n}{2}+1\right)^2$$

for all fake linear cycles $\lambda\in H^{n/2,n/2}(X_d^n)_{\mathrm{prim}}\cap H^n(X_d^n,\mathbb{Z})$. In fact, otherwise V_λ is smooth and reduced at the Fermat point, and so the quadratic fundamental form $q=0$ vanishes. In particular its degree $r:=d\left(\frac{n}{2}+2\right)-n-2$ piece also vanishes, that is, $q_r=0$, and so by Proposition 6.3 we conclude that $c_{2i-2}^d+1=0$ for all $i=1,\dots,\frac{n}{2}+1$, contrary to the fact that λ is a fake linear cycle. □

Acknowledgements

Duque Franco was partially supported by the Fondecyt ANID postdoctoral grant 3220631. Villaflor Loyola was supported by the Fondecyt ANID postdoctoral grant 3210020.

References

[Beauville 2014] A. Beauville, "Some surfaces with maximal Picard number", *J. Éc. Polytech. Math.* **1** (2014), 101–116. MR Zbl

[Carlson et al. 1983] J. Carlson, M. Green, P. Griffiths, and J. Harris, "Infinitesimal variations of Hodge structure, I", *Compos. Math.* **50**:2-3 (1983), 109–205. MR Zbl

[Cifani et al. 2023] M. G. Cifani, G. P. Pirola, and E. Schlesinger, "Reconstructing curves from their Hodge classes", *Rend. Circ. Mat. Palermo* (2) **72**:2 (2023), 945–958. MR Zbl

[Deligne 1982] P. Deligne, "Hodge cycles on abelian varieties", pp. 9–10 in *Hodge cycles, motives, and Shimura varieties*, Lect. Notes in Math. **900**, Springer, 1982. Zbl

[Green 1988] M. L. Green, "A new proof of the explicit Noether–Lefschetz theorem", *J. Differential Geom.* **27**:1 (1988), 155–159. MR Zbl

[Griffiths 1969a] P. A. Griffiths, "On the periods of certain rational integrals, I", *Ann. of Math.* (2) **90** (1969), 460–495. MR Zbl

[Griffiths 1969b] P. A. Griffiths, "On the periods of certain rational integrals, II", *Ann. of Math.* (2) **90** (1969), 496–541. MR Zbl

[Maclean 2005] C. Maclean, "A second-order invariant of the Noether–Lefschetz locus and two applications", *Asian J. Math.* **9**:3 (2005), 373–399. MR Zbl

[Movasati 2017] H. Movasati, "Gauss–Manin connection in disguise: Noether–Lefschetz and Hodge loci", *Asian J. Math.* **21**:3 (2017), 463–481. MR Zbl

[Movasati 2021] H. Movasati, *A course in Hodge theory: with emphasis on multiple integrals*, Int. Press, Somerville, MA, 2021. MR Zbl

[Movasati and Sertöz 2021] H. Movasati and E. C. Sertöz, "On reconstructing subvarieties from their periods", *Rend. Circ. Mat. Palermo* (2) **70**:3 (2021), 1441–1457. MR Zbl

[Neukirch et al. 2000] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundlehren der Math. Wissenschaften **323**, Springer, 2000. MR Zbl

[Otwinowska 2002] A. Otwinowska, "Sur la fonction de Hilbert des algèbres graduées de dimension 0", *J. Reine Angew. Math.* **545** (2002), 97–119. MR Zbl

[Otwinowska 2003] A. Otwinowska, "Composantes de petite codimension du lieu de Noether–Lefschetz: un argument asymptotique en faveur de la conjecture de Hodge pour les hypersurfaces", *J. Algebraic Geom.* **12**:2 (2003), 307–320. MR Zbl

[Shioda 1979] T. Shioda, "The Hodge conjecture for Fermat varieties", *Math. Ann.* **245**:2 (1979), 175–184. MR Zbl

[Villaflor Loyola 2022a] R. Villaflor Loyola, "Periods of complete intersection algebraic cycles", *Manuscripta Math.* **167**:3-4 (2022), 765–792. MR Zbl

[Villaflor Loyola 2022b] R. Villaflor Loyola, "Small codimension components of the Hodge locus containing the Fermat variety", *Commun. Contemp. Math.* **24**:7 (2022), art. id. 2150053. MR Zbl

[Voisin 1988] C. Voisin, "Une précision concernant le théorème de Noether", *Math. Ann.* **280**:4 (1988), 605–611. MR Zbl

[Voisin 1989] C. Voisin, "Composantes de petite codimension du lieu de Noether–Lefschetz", *Comment. Math. Helv.* **64**:4 (1989), 515–526. MR Zbl

Communicated by Vasudevan Srinivas
Received 2022-01-06 Revised 2022-08-06 Accepted 2022-11-28

georgy11235@gmail.com *Departamento de Matemáticas, Universidad de Chile, Santiago, Chile*

roberto.villaflor@mat.uc.cl *Facultad de Matemáticas, Pontificia Universidad Católica de Chile, Santiago, Chile*

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 17 No. 10 2023