Pacific Journal of Mathematics

Volume 295 No. 1 July 2018

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

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

The subscription price for 2018 is US $475/year for the electronic version, and $640/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.1

A VARIANT OF A THEOREM BY AILON–RUDNICK FOR ELLIPTIC CURVES

DRAGOS GHIOCA, LIANG-CHUNG HSIA AND THOMAS J. TUCKER

Given a smooth projective curve C defined over $\overline{\mathbb{Q}}$ and given two elliptic surfaces $\mathcal{E}_1 \to C$ and $\mathcal{E}_2 \to C$ along with sections $\sigma_{P_i}, \sigma_{Q_i}$ (corresponding to points P_i, Q_i of the generic fibers) of $\mathcal{E}_i$ (for $i = 1, 2$), we prove that if there exist infinitely many $t \in C(\overline{\mathbb{Q}})$ such that for some integers $m_{1,t}$, $m_{2,t}$, we have $[m_{i,t}](\sigma_{P_i}(t)) = \sigma_{Q_i}(t)$ on $\mathcal{E}_i$ (for $i = 1, 2$), then at least one of the following conclusions must hold:

i. There exist isogenies $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_2$ such that $\varphi(P_1) = \psi(P_2)$.
ii. Q_i is a multiple of P_i for some $i = 1, 2$.

A special case of our result answers a conjecture made by Silverman.

1. Introduction

Ailon and Rudnick [2004] showed that for two multiplicatively independent nonconstant polynomials $a, b \in \mathbb{C}[x]$ there is a nonzero polynomial $h \in \mathbb{C}[x]$, depending on a and b such that $\gcd(a^n - 1, b^n - 1) \mid h$ for all positive integer n. In this paper, we prove a similar result for elliptic curves; instead of working with the multiplicative group $\mathbb{G}_m$, we work with the group law on an elliptic curve defined over a function field. The result of Ailon–Rudnick relies crucially on the Serre–Ihara–Tate theorem (see [Lang 1965]), while our result relies crucially on recent Bogomolov-type results for elliptic surfaces due to DeMarco and Mavraki [2017].

Throughout our article, we work with elliptic surfaces over $\overline{\mathbb{Q}}$; more precisely, given a projective, smooth curve C defined over $\overline{\mathbb{Q}}$, an *elliptic surface* $\mathcal{E}/C$ is given by a morphism $\pi : \mathcal{E} \to C$ over $\overline{\mathbb{Q}}$ where the generic fiber of π is an elliptic curve E defined over $K = \overline{\mathbb{Q}}(C)$, while for all but finitely many $t \in C(\overline{\mathbb{Q}})$, the fiber $\mathcal{E}_t := \pi^{-1}(\{t\})$ is an elliptic curve defined over $\overline{\mathbb{Q}}$. Recall that a section σ of π (i.e., a map $\sigma : C \to \mathcal{E}$ such that $\pi \circ \sigma = \mathrm{id}|_C$) gives rise to a K-rational point of E. Conversely, a point $P \in E(K)$ corresponds to a section of π; if we need to indicate the dependence on P, we will denote it by σ_P. So, for all but finitely many $t \in C(\overline{\mathbb{Q}})$, the intersection of the image of σ_P in $\mathcal{E}$ with the fiber above t

MSC2010: primary 11G50; secondary 11G35, 14G25.
Keywords: heights, elliptic surfaces, unlikely intersections in arithmetic dynamics.

is a point $P_t := \sigma_P(t)$ on the elliptic curve $\mathcal{E}_t := \pi^{-1}(\{t\})$. For any integer k, the multiplication-by-k map $[k]$ on E extends to a morphism on $\mathcal{E}$; if there is no risk of confusion, we still denote the extension by $[k]$.

We prove the following result:

Theorem 1-1. *Let $\pi_i : \mathcal{E}_i \to C$ be elliptic surfaces over a curve C defined over $\overline{\mathbb{Q}}$ with generic fibers E_i, and let $\sigma_{P_i}, \sigma_{Q_i}$ be sections of π_i (for $i = 1, 2$) corresponding to points $P_i, Q_i \in E_i(\overline{\mathbb{Q}}(C))$. If there exist infinitely many $t \in C(\overline{\mathbb{Q}})$ for which there exist some $m_{1,t}, m_{2,t} \in \mathbb{Z}$ such that $[m_{i,t}]\sigma_{P_i}(t) = \sigma_{Q_i}(t)$ for $i = 1, 2$, then at least one of the following properties must hold*:

(i) *There exist isogenies $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_2$ such that $\varphi(P_1) = \psi(P_2)$.*

(ii) *For some $i \in \{1, 2\}$, there exists $k_i \in \mathbb{Z}$ such that $[k_i]P_i = Q_i$ on E_i.*

We note here that, in contrast to similar results such as [Ailon and Rudnick 2004], the ambient algebraic group ($\mathcal{E}_1 \times \mathcal{E}_2$ in our case, as opposed to $\mathbb{G}_m$ for Ailon and Rudnick) need not be defined over the field of constants in $k(C)$.

A special case of our result (when both Q_1 and Q_2 are the zero elements) answers in the affirmative [Silverman 2004b, Conjecture 7]; this is carried out in a more general setting (over the complex numbers and also, giving a more precise connection to the original GCD problem of Ailon–Rudnick) in our Proposition 4-3 from Section 4. We also note that the special case of Theorem 1-1 when $Q_1 = Q_2 = 0$ was solved by Masser and Zannier [2014] when both elliptic surfaces are defined over $\mathbb{C}$.

Silverman's question [2004b, Conjecture 7] was motivated by work of Ailon and Rudnick [2004], who showed that the greatest common divisor of $a^n - 1$ and of $b^n - 1$ for multiplicatively independent polynomials $a, b \in \mathbb{C}[T]$ has bounded degree (see also the generalization in [Corvaja and Zannier 2013b] along with the related results from [Corvaja and Zannier 2008; 2011; 2013a]). In turn, the result of Ailon and Rudnick was motivated by the work of Bugeaud–Corvaja–Zannier [Bugeaud et al. 2003] who obtained an upper bound for $\gcd(a^k - 1, b^k - 1)$ (as k varies in $\mathbb{N}$) for given $a, b \in \overline{\mathbb{Q}}$. On the other hand, Silverman [2004a] showed that the degree of $\gcd(a^m - 1, b^n - 1)$ could be quite large when $a, b \in \overline{\mathbb{F}_p}[T]$; see also the authors' previous paper [Ghioca et al. 2017], where (using as technical ingredient [Ghioca 2014] in place of [DeMarco and Mavraki 2017]) we study the $\gcd(a^m - 1, b^n - 1)$ when a and b are polynomials over arbitrary fields of positive characteristic, along with other generalizations on the same theme. Finally, we mention the work of Denis [2011] who studied the same problem of the greatest common divisor in the context of Drinfeld modules.

As hinted in [Silverman 2004b], this *greatest common divisor* (GCD) *problem* may be studied in much higher generality; for example, if one knew the result of [DeMarco and Mavraki 2017] (see Theorem 2-3 below) in the context of abelian varieties, then our method would extend to a similar conclusion for arbitrary abelian schemes over a base curve. DeMarco–Mavraki's theorem can be interpreted as an extension of Masser–Zannier's theorem (see [Masser and Zannier 2012]) in the same spirit as the Bogomolov conjecture is an extension of the classical Manin–Mumford conjecture. So, even though the extension to arbitrary abelian varieties of the results from [DeMarco and Mavraki 2017] is expected to be quite challenging, we mention that there is some progress in this direction due to Cinkir [2011], Gubler [2007], and Yamaki [2017], who proved various cases of the Bogomolov conjecture for abelian varieties defined over function fields.

Our Theorem 1-1 is related also to [Barroero and Capuano 2016, Theorem 1.1] (see also the extension from [Barroero and Capuano 2017]) where it is shown that given n linearly independent sections P_i on the Legendre elliptic family $y^2 = x(x-1)(x-t)$, there are at most finitely many parameters t such that the points $(P_i)_t$ satisfy two independent linear relations on the corresponding elliptic curve. Therefore, a special case of the result by Barroero and Capuano is that given sections P_1, P_2, Q_1, Q_2 on the Legendre elliptic surface, if these four sections are linearly independent, then there are at most finitely many t such that for some $m_t, n_t \in \mathbb{Z}$ we have $[m_t](P_1)_t = (Q_1)_t$ and $[n_t](P_2)_t = (Q_2)_t$. However, in our Theorem 1-1 we obtain the same conclusion under the weaker hypothesis that Q_i is not a multiple of P_i for $i = 1, 2$ and also that P_1 and P_2 are linearly independent. We also note that the constant case of Barroero and Capuano's theorem is covered by the results of Habegger and Pila [2016].

A special case of our Theorem 1-1 bears a resemblance to the classical Mordell–Lang problem proven by Faltings [1994] (see also [Hrushovski 1996] for the case of semiabelian varieties defined over function fields). Indeed, with the notation as in Theorem 1-1, assume there exist infinitely many $t \in C(\overline{\mathbb{Q}})$ such that for some $m_t \in \mathbb{Z}$ we have

$$[m_t](P_i)_t = (Q_i)_t \quad \text{for } i = 1, 2. \tag{1-2}$$

Also assume there is no $m \in \mathbb{Z}$ such that $[m]P_i = Q_i$ for $i = 1, 2$. Then the conclusion of Theorem 1-1 yields the existence of isogenies $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_2$ such that $\varphi(P_1) = \psi(P_2)$. Thus, using that (1-2) holds for infinitely many $t \in C(\overline{\mathbb{Q}})$ we see that

$$\varphi(Q_1) = \psi(Q_2). \tag{1-3}$$

Therefore, if we let $X \subset \mathcal{A} := \mathcal{E}_1 \times \mathcal{E}_2$ be the 1-dimensional subscheme corresponding to the section (Q_1, Q_2), and we let $\Gamma \subset \mathcal{A}$ be the subgroup spanned by $(0, P_2)$ and $(P_1, 0)$, then the existence of infinitely many $\gamma \in \Gamma$ such that for some $t \in C(\overline{\mathbb{Q}})$ we have $\gamma_t \in X$ implies that X is contained in a proper algebraic subgroup of $\mathcal{A}$ (as given by (1-3)). Such a statement can be viewed as a relative version of the classical Mordell–Lang problem; note that if $\mathcal{E}_1$ and $\mathcal{E}_2$ are constant elliptic surfaces with generic fibers E_i^0 defined over $\overline{\mathbb{Q}}$, while $\Gamma \subset (E_1^0 \times E_2^0)(\overline{\mathbb{Q}})$, then this question is a special case of Faltings's theorem [1994] (formerly known as the Mordell–Lang conjecture). It is natural to ask whether the above relative version of the Mordell–Lang problem holds more generally when $\mathcal{A} \to C$ is an arbitrary semiabelian scheme, $X \subset \mathcal{A}$ is a 1-dimensional scheme and $\Gamma \subset \mathcal{A}$ is an arbitrary finitely generated group. This more general question is also related to the bounded height problems studied in [Amoroso et al. 2017] in the context of pencils of finitely generated subgroups of $\mathbb{G}_m^n$.

In the next section of this paper, we review some preliminary material. Following that, in Section 3, we prove Theorem 1-1. The proof in the case of nonconstant sections is quite similar to the proofs of the main results of [Ailon and Rudnick 2004] and [Hsia and Tucker 2017], while the case of constant sections requires a different argument. In Section 4, we give a positive answer to Silverman's conjecture [2004b, Conjecture 7].

2. Preliminaries

From now on, we fix an elliptic surface $\pi : \mathcal{E} \to C$, where C is a projective, smooth curve defined over $\overline{\mathbb{Q}}$. We denote by E the generic fiber of $\mathcal{E}$; this is an elliptic curve defined over $\overline{\mathbb{Q}}(C)$. For all but finitely many $t \in C(\overline{\mathbb{Q}})$, we have $\mathcal{E}_t := \pi^{-1}(\{t\})$ is an elliptic curve defined over $\overline{\mathbb{Q}}$.

2.1. ***Isotriviality.*** We say that $\mathcal{E}$ is *isotrivial* if the j-invariant of the generic fiber is a constant function (on C); for isotrivial elliptic surfaces $\mathcal{E}$, all smooth fibers of π are isomorphic (to the generic fiber E). If $\mathcal{E}$ is isotrivial, then there exists a finite cover $C' \to C$ such that $\mathcal{E}' := \mathcal{E} \times_C C'$ is a *constant* (*elliptic*) *surface* over C', i.e., there exists an elliptic curve E^0 defined over $\overline{\mathbb{Q}}$ such that $\mathcal{E}' = E^0 \times_{\operatorname{Spec}(\overline{\mathbb{Q}})} C'$. Furthermore, for a constant elliptic surface $E^0 \times_{\operatorname{Spec}(\overline{\mathbb{Q}})} C'$, we say that σ_P is a *constant section* if $P \in E^0(\overline{\mathbb{Q}})$.

2.2. ***Canonical height on an elliptic surface.*** For each $t \in C(\overline{\mathbb{Q}})$ such that $\mathcal{E}_t$ is an elliptic curve, we let $\hat{h}_{\mathcal{E}_t}$ be the Néron–Tate canonical height for the points in $\mathcal{E}_t(\overline{\mathbb{Q}})$ (for more details, see [Silverman 1986]). There are two important properties of the canonical height which we will use:

(i) $\hat{h}_{\mathcal{E}_t}(P_t) = 0$ if and only if P_t is a torsion point of $\mathcal{E}_t$, i.e., there exists a positive integer k such that $[k]P_t = 0$; and

(ii) for each $k \in \mathbb{Z}$ we have $\hat{h}_{\mathcal{E}_t}([k]P_t) = k^2 \cdot \hat{h}_{\mathcal{E}_t}(P_t)$.

Also, we let $\hat{h}_E$ be the Néron–Tate canonical height on the generic fiber E constructed with respect to the Weil height on the function field $\overline{\mathbb{Q}}(C)$; for more details, see [Silverman 1994a]. Property (ii) above holds also on the generic fiber, i.e., $\hat{h}_E([k]P) = k^2 \cdot \hat{h}_E(P)$. On the other hand, property (i) above holds only if $\mathcal{E}$ is nonisotrivial. Furthermore, if $\mathcal{E} = E \times_C C$ is a constant family (where E is an elliptic curve defined over $\overline{\mathbb{Q}}$), then for any $P \in E(\overline{\mathbb{Q}}(C))$, we have that $\hat{h}_E(P) = 0$ if and only if $P \in E(\overline{\mathbb{Q}})$.

2.3. ***Variation of the canonical height.*** We let h_C be a given Weil height for points in $C(\overline{\mathbb{Q}})$ corresponding to a divisor of degree 1 on C.

Let σ_P be a section of the elliptic surface $\mathcal{E} \to C$ corresponding to a point P on the generic fiber E. Then, for all but finitely many $t \in C(\overline{\mathbb{Q}})$, the intersection of the image of σ_P in $\mathcal{E}$ with the fiber above t is a point P_t, on the elliptic curve $\mathcal{E}_t$. The following important fact will be used in our proof (see [Tate 1983; Silverman 1983]):

$$\lim_{h_C(t)\to\infty} \frac{\hat{h}_{\mathcal{E}_t}(P_t)}{h_C(t)} = \hat{h}_E(P). \tag{2-1}$$

Furthermore, the following more precise result holds, as proven by Silverman [1994b]:

$$\hat{h}_{\mathcal{E}_t}(P_t) = h_{C,\eta(P)}(t) + O_P(1), \tag{2-2}$$

where $\eta(P)$ is a divisor on C of degree equal to $\hat{h}_E(P)$ and $h_{C,\eta(P)}$ is a given Weil height for the points in $C(\overline{\mathbb{Q}})$ corresponding to the divisor $\eta(P)$, while the implicit constant from the term $O_P(1)$ is only dependent on the section σ_P (and implicitly on the divisor $\eta(P)$), but not on $t \in C(\overline{\mathbb{Q}})$.

2.4. ***Points of small height on sections.*** We will use [DeMarco and Mavraki 2017, Theorem 1.4], which extends [DeMarco et al. 2016] (and in turn, uses the extensive analysis from [Silverman 1994b] regarding the variation of the canonical height in an elliptic fibration). We also note that the case of isotrivial elliptic curves from Theorem 2-3 was previously proven by Zhang [1998], as part of Zhang's famous proof of the classical Bogomolov conjecture.

Theorem 2-3 [DeMarco and Mavraki 2017, Theorem 1.4]. *Let $\mathcal{E}_1, \mathcal{E}_2$ be elliptic fibrations over the same $\overline{\mathbb{Q}}$-curve C. Let P_i be a section of $\mathcal{E}_i$ (for $i = 1, 2$) with the property that there exists an infinite sequence $\{t_n\} \subset C(\overline{\mathbb{Q}})$ such that*

$$\lim_{n\to\infty} \hat{h}_{(\mathcal{E}_i)_{t_n}}((P_i)_{t_n}) = 0 \quad \textit{for } i = 1, 2.$$

Then there exist group homomorphisms $\phi : \mathcal{E}_1 \to \mathcal{E}_2$ and $\psi : \mathcal{E}_2 \to \mathcal{E}_2$, not both trivial, such that $\phi(P_1) = \psi(P_2)$.

3. Proof of our main result

Propositions 3-1 and 3-9 are key to our proof.

Proposition 3-1. *Let C be a projective, smooth curve defined over $\overline{\mathbb{Q}}$, and let $h_C(\cdot)$ be a Weil height for the algebraic points of C corresponding to a divisor of degree 1. Let P and Q be sections of an elliptic surface $\pi : \mathcal{E} \to C$ with generic fiber E, and assume there exists no $k \in \mathbb{Z}$ such that $[k]P = Q$. In addition, assume $\hat{h}_E(P) > 0$. If there exists an infinite sequence $\{t_i\} \subset C(\overline{\mathbb{Q}})$ such that for each $i \in \mathbb{N}$ there exists some $m_i \in \mathbb{Z}$ such that $[m_i]P_{t_i} = Q_{t_i}$, then $h_C(t_i)$ is uniformly bounded and* $\lim_{i\to\infty} \hat{h}_{\mathcal{E}_{t_i}}(P_{t_i}) = 0$.

We note that the special case of Proposition 3-1 when $\pi : \mathcal{E} \to C$ is a constant elliptic surface follows from [Silverman 1983].

Proof. Since $[m_i]P_{t_i} = Q_{t_i}$, we have

$$m_i^2 \cdot \hat{h}_{\mathcal{E}_{t_i}}(P_{t_i}) = \hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i}). \tag{3-2}$$

Since $[k]P \neq Q$ for any $k \in \mathbb{Z}$ and the sequence $\{t_i\}$ is infinite, then

$$\lim_{i\to\infty} |m_i| = \infty. \tag{3-3}$$

We claim first that $h_C(t_i)$ is uniformly bounded. Indeed, assuming (at the expense, perhaps, of replacing $\{t_i\}$ by an infinite subsequence) that $\lim_{i\to\infty} h_C(t_i) = \infty$, (2-1) coupled with (3-2) and (3-3) yields a contradiction. To see this, we divide both sides of (3-2) by $h_C(t_i)$ and then take limits. Because $\hat{h}_E(P) > 0$, (3-3) implies that the left-hand side equals

$$\lim_{i\to\infty} m_i^2 \cdot \frac{\hat{h}_{\mathcal{E}_{t_i}}(P_{t_i})}{h_C(t_i)} = \infty, \tag{3-4}$$

while the right-hand side equals

$$\lim_{i\to\infty} \frac{\hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i})}{h_C(t_i)} = \hat{h}_E(Q) < \infty, \tag{3-5}$$

which is a contradiction. So, indeed, $h_C(t_i)$ must be uniformly bounded.

Next we prove that also $\hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i})$ is uniformly bounded. Using (2-2) (see [Silverman 1994b]) we know that there exists a divisor $\eta(Q)$ of C of degree equal to $\hat{h}_E(Q)$ such that

$$\hat{h}_{\mathcal{E}_t}(Q_t) = h_{C,\eta(Q)}(t) + O(1), \tag{3-6}$$

where $h_{C,\eta(Q)}$ is a Weil height on $C(\overline{\mathbb{Q}})$ corresponding to the divisor $\eta(Q)$. Since h_C is a Weil height associated to a divisor D on C of degree 1, then for any positive integer $m > \deg(\eta(Q))$, the divisor $D_1 := mD - \eta(Q)$ has positive degree and therefore, is ample. Then [Hindry and Silverman 2000, Proposition B.3.2] implies that any Weil height h_{C,D_1} associated to the divisor D_1 satisfies $h_{C,D_1}(t) \geq O(1)$ for all $t \in C(\overline{\mathbb{Q}})$. So,

$$mh_C(t) + O(1) \geq h_{C,\eta(Q)}(t) \quad \text{for } t \in C(\overline{\mathbb{Q}}). \tag{3-7}$$

Therefore $h_{C,\eta(Q)}(t_i)$ is uniformly bounded (since $h_C(t_i)$ is uniformly bounded). Then (3-6) provides the desired claim that

$$\hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i}) \text{ is bounded as } i \to \infty. \tag{3-8}$$

Finally, the fact that $\lim_{i\to\infty} \hat{h}_{\mathcal{E}_i}(P_i) = 0$ follows easily from combining equations (3-2), (3-3), and (3-8). □

Proposition 3-9. *Let P and Q be sections of a constant elliptic fibration $\pi : \mathcal{E} \to C$, and assume there exists no $k \in \mathbb{Z}$ such that $[k]P = Q$. In addition, assume P is a nontorsion, constant section. If there exists an infinite sequence $\{t_i\} \subset C(\overline{\mathbb{Q}})$ such that for each $i \in \mathbb{N}$ there exists some $m_i \in \mathbb{Z}$ such that $[m_i]P_{t_i} = Q_{t_i}$, then* $\lim_{i\to\infty} h_C(t_i) = \infty$.

Proof. Each fiber $\mathcal{E}_{t_i}$ is isomorphic to the generic fiber E^0, and so, because P is a constant section,

$$\hat{h}_{\mathcal{E}_{t_i}}(P_{t_i}) = \hat{h}_{E^0}(P^0), \tag{3-10}$$

where P^0 is the intersection of P with the generic fiber and $\hat{h}_{E^0}(\cdot)$ is the Néron–Tate canonical height of the elliptic curve E^0 defined over $\overline{\mathbb{Q}}$ (i.e., it is not the canonical height on the generic fiber of $\mathcal{E}$ seen as an elliptic curve defined over the function field $\overline{\mathbb{Q}}(C)$).

Furthermore, since P^0 is not a torsion point of E^0, then $\hat{h}_{E^0}(P^0) > 0$. Thus, from the equality $[m_i]P_{t_i} = Q_{t_i}$, along with (3-10) coupled with the fact that $|m_i| \to \infty$ (because $[k]P \neq Q$ for all integers k), we must have

$$\hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i}) = m_i^2 \hat{h}_{E^0}(P^0) \to \infty. \tag{3-11}$$

Then, using (2-2), we have

$$\hat{h}_{\mathcal{E}_{t_i}}(Q_{t_i}) = h_{C,\eta(Q)}(t_i) + O(1), \tag{3-12}$$

where $h_{C,\eta(Q)}$ is a Weil height on C corresponding to a certain divisor $\eta(Q)$. So, (3-11) and (3-12) yield $h_{C,\eta(Q)}(t_i) \to \infty$ and thus, $h_C(t_i) \to \infty$ (see [Hindry and Silverman 2000, Proposition B.3.5], along with our similar argument from the proof of Proposition 3-1). □

Now we can prove our main result.

Proof of Theorem 1-1. First we note that if P_i is a torsion section (for some $i \in \{1, 2\}$), then conclusion (ii) holds trivially since then we would obtain that there exist infinitely many $t \in C(\overline{\mathbb{Q}})$ such that $(Q_i)_t = [k](P_i)_t$ for the same integer k. So, from now on, we assume that both P_1 and P_2 are nontorsion sections on $\mathcal{E}_1, \mathcal{E}_2$, respectively. In particular, this means that if $\hat{h}_{E_i}(P_i) = 0$, then $\mathcal{E}_i$ must be an isotrivial elliptic surface.

We assume there exists an infinite sequence $\{t_i\} \subset C(\overline{\mathbb{Q}})$ such that for each $i \in \mathbb{N}$ there exist $m_{i,1}, m_{i,2} \in \mathbb{Z}$ with the property that $[m_{i,1}](P_1)_{t_i} = (Q_1)_{t_i}$ and also $[m_{i,2}](P_2)_{t_i} = (Q_2)_{t_i}$. In addition, we assume conclusion (ii) does not hold, i.e., there is no $m \in \mathbb{Z}$ such that $[m]P_i = Q_i$ for some $i \in \{1, 2\}$. We split our analysis into two cases.

Case 1. $\hat{h}_{E_i}(P_i) > 0$ for each $i = 1, 2$.

Applying then Proposition 3-1 to the sections P_i and Q_i, we obtain

$$\lim_{i\to\infty} \hat{h}_{(\mathcal{E}_1)_{t_i}}((P_1)_{t_i}) = \lim_{i\to\infty} \hat{h}_{(\mathcal{E}_2)_{t_i}}((P_2)_{t_i}) = 0. \tag{3-13}$$

Equation (3-13) along with Theorem 2-3 implies that conclusion (i) must hold in Theorem 1-1. Note that we obtain in this case that the morphisms $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_2$ from the conclusion of Theorem 2-3 are *both* isogenies since P_1 and P_2 are nontorsion sections.

Case 2. Either $\hat{h}_{E_1}(P_1) = 0$ or $\hat{h}_{E_2}(P_2) = 0$.

Without loss of generality, we assume $\hat{h}_{E_1}(P_1) = 0$. Therefore (since P_1 is not torsion) $\mathcal{E}_1$ is an isotrivial elliptic surface, and furthermore, at the expense of replacing C by a finite cover (and also performing a base extension for $\mathcal{E}_1$ and $\mathcal{E}_2$), we may assume that $\mathcal{E}_1$ is a constant family. Thus, $\mathcal{E}_1 = E_1^0 \times_C C$ for some elliptic curve E_1^0 defined over $\overline{\mathbb{Q}}$. Then also P_1 is a constant (nontorsion) section, because $\hat{h}_{\mathcal{E}_1}(P_1) = 0$. Finally, we let $h_C(\cdot)$ be a Weil height for the algebraic points of C with respect to a divisor of degree 1.

If $\hat{h}_{E_2}(P_2) > 0$, then Proposition 3-1 applied to P_2 and Q_2 implies that $h_C(t_i)$ is uniformly bounded, which contradicts the conclusion of Proposition 3-9 applied to P_1 and Q_1. Therefore, we must have $\hat{h}_{E_2}(P_2) = 0$, and also $\mathcal{E}_2$ is an isotrivial elliptic surface. At the expense of (yet another) base extension, we may assume that also $\mathcal{E}_2 = E_2^0 \times C$ is a constant fibration. Then P_2 is a constant, nontorsion section on $\mathcal{E}_2$. We let P_i^0 be the intersection of P_i (for $i = 1, 2$) with the generic fiber of $\mathcal{E}_i$.

Now, if either Q_1 or Q_2 is also a constant section, then we get a contradiction since we assumed conclusion (ii) does not hold. Indeed, if for some $i = 1, 2$ both P_i and Q_i are constant sections on the constant elliptic surface $\mathcal{E}_i$, then the existence of a point $t \in C(\overline{\mathbb{Q}})$ such that for some $k \in \mathbb{Z}$ we have $[k](P_i)_t = (Q_i)_t$ implies that actually $[k]P_i = Q_i$ on $\mathcal{E}_i$. So, we may assume that Q_1 and Q_2 are both nonconstant sections on $\mathcal{E}_1$, respectively $\mathcal{E}_2$. Then, there is a (neither vertical, nor horizontal) curve $X \subset E_1^0 \times E_2^0$ containing all points $((Q_1)_t, (Q_2)_t)$ for $t \in C(\overline{\mathbb{Q}})$. Furthermore, our hypothesis means that this curve X intersects the subgroup $\Gamma \subset E_1^0 \times E_2^0$ spanned by the points $(P_1^0, 0)$ and $(0, P_2^0)$ in an infinite set. The classical Mordell–Lang conjecture (proven by Faltings [1994]) implies that X itself is a coset of an algebraic subgroup of $E_1^0 \times E_2^0$. Hence, because X projects dominantly onto each coordinate, there exists a nontrivial isogeny $\tau : E_1^0 \to E_2^0$, and also there exist endomorphisms ϕ_i of E_i^0, not both trivial, such that

$$\tau(\phi_1(Q_1)) = \phi_2(Q_2). \tag{3-14}$$

Then, using (for any i such that $m_{i,1}$ and $m_{i,2}$ are nonzero) that

$$[m_{i,1}]P_1^0 = (Q_1)_{t_i} \quad \text{and} \quad [m_{i,2}]P_2^0 = (Q_2)_{t_i}$$

along with the fact that $\tau\big(\phi_1((Q_1)_{t_i})\big) = \phi_2((Q_2)_{t_i})$, we obtain the conclusion in Theorem 1-1 with $\varphi := \tau \circ [m_{i,1}] \circ \phi_1$ and $\psi := [m_{i,2}] \circ \phi_2$. Finally, note that since P_1 and P_2 are nontorsion, then also φ and ψ are dominant morphisms. Indeed, if φ were trivial, then using that τ is an isogeny and that $m_{i,1} \neq 0$, we would obtain that ϕ_1 must be trivial. But then $\phi_2(Q_2) = 0$ (using (3-14)), which implies that $\phi_2 = 0$ because we assumed that Q_2 is a nontorsion section. So, if φ were trivial (and a completely similar argument works assuming ψ were trivial), we would get that both ϕ_1 and ϕ_2 are trivial, a contradiction.

This concludes the proof of Theorem 1-1. $\square$

4. Common divisors of elliptic sequences

In this section, we apply Theorem 1-1 to prove Silverman's conjecture [2004b, Conjecture 7] concerning common divisors of elliptic sequences; actually, our Proposition 4-3 provides a slightly more general statement than the original conjecture. We first recall the terminology and notation from [Silverman 2004b] that we will use in this section.

Let k be an algebraically closed field of characteristic 0. Let C be a smooth projective curve defined over k and let $K = k(C)$ be the function field of C. For any point $\gamma \in C(k)$, we let $\mathrm{ord}_\gamma(D)$ denote the coefficient of γ in $D \in \mathrm{Div}(C)$. The *greatest common divisor* for any two effective divisors $D_1, D_2 \in \mathrm{Div}(C)$ is defined as

$$\mathrm{GCD}(D_1, D_2) = \sum_{\gamma \in C} \min\{\mathrm{ord}_\gamma(D_1), \mathrm{ord}_\gamma(D_2)\} \cdot (\gamma) \in \mathrm{Div}(C).$$

For an elliptic curve E defined over K, let $\pi : \mathcal{E} \to C$ be an elliptic surface whose generic fiber is E and let $P \in E(K)$. Recall that the section corresponding to P is denoted by $\sigma_P : C \to \mathcal{E}$. We denote the image of σ_P by $\overline{P} := \sigma_P(C) \subset \mathcal{E}$.

Let E_1 and E_2 be elliptic curves defined over K, let $\mathcal{E}_i/C$ be elliptic surfaces with generic fibers E_i, and let $P_i \in E_i(K)$ for $i = 1, 2$. The greatest common divisor of P_1 and P_2 is given by

$$\mathrm{GCD}(P_1, P_2) = \mathrm{GCD}(\sigma_{P_1}^*(\overline{O}_{\mathcal{E}_1}), \sigma_{P_2}^*(\overline{O}_{\mathcal{E}_2})),$$

where $\overline{O}_{\mathcal{E}_i} := \sigma_{O_i}(C)$ is the zero section on $\mathcal{E}_i$ corresponding to the identity O_i of E_i and $\sigma_{P_i}^*(\overline{O}_{\mathcal{E}_i})$ is the pull-back under $\sigma_i : C \to \mathcal{E}_i$ of $\overline{O}_{\mathcal{E}_i}$ as a divisor of $\mathcal{E}_i$ for $i = 1, 2$. Thus, for any given $Q_i \in E_i(K)$, $\mathrm{GCD}(P_1 - Q_1, P_2 - Q_2)$ is the greatest common divisor of the two points $P_i - Q_i \in E_i$ for $i = 1, 2$. In the following, points P_1 and P_2 are called (K-) *dependent* if there are morphisms $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_2$ not both trivial such that $\varphi(P_1) = \psi(P_2)$; otherwise they are called *independent*. Note that if one of P_1 and P_2 is a torsion point, then they are automatically dependent.

Motivated by the result of [Ailon and Rudnick 2004], Silverman conjectured that an elliptic analogue also exists. For the convenience of the reader, we recall his conjecture.

Conjecture 4-1 Silverman [1994b, Conjecture 7]. *Let $K = k(C)$ be the function field of a smooth projective curve C over an algebraically closed field k of characteristic* 0, *let E_1/K and E_2/K be elliptic curves, and let $P_1 \in E_1(K)$ and $P_2 \in E_2(K)$ be K-independent points.*

(i) *There is a constant $c = c(K, E_1, E_2, P_1, P_2)$ such that*

$$\deg \mathrm{GCD}([n_1]P_1, [n_2]P_2) \le c \quad \textit{for all } n_1, n_2 \ge 1.$$

(ii) *Further, there is an equality*

$$\mathrm{GCD}([n]P_1, [n]P_2) = \mathrm{GCD}(P_1, P_2) \quad \textit{for infinitely many } n \ge 1.$$

Remark 4-2. Silverman [1994b, Theorem 8] showed that Conjecture 4-1 is true provided that both E_1 and E_2 have constant j-invariant as a consequence of Raynaud's theorem [1983].

As an application of Theorem 1-1, we prove that Conjecture 4-1 holds (even in a slightly stronger form); we strengthen further the conclusion from Conjecture 4-1 when $k = \overline{\mathbb{Q}}$.

Proposition 4-3. *Let k be an algebraically closed field of characteristic* 0. *Let C be a smooth projective curve defined over k, let $K = k(C)$ and let E_i/K, $i = 1, 2$, be elliptic curves defined over K. Let $P_i, Q_i \in E_i(K)$ for $i = 1, 2$ and furthermore, assume that P_1 and P_2 are K-independent.*

(i) *If $k = \overline{\mathbb{Q}}$, then there exists an effective divisor $D \in \mathrm{Div}(C)$ such that*

$$\mathrm{GCD}([n_1]P_1 - Q_1, [n_2]P_2 - Q_2) \le D$$

for all integers n_i such that $[n_i]P_i \ne Q_i$, $i = 1, 2$.

(ii) *For an arbitrary algebraically closed field k of characteristic* 0, *there exists an effective divisor* $D_0 \in \mathrm{Div}(C)$ *such that*

$$\mathrm{GCD}([n_1]P_1, [n_2]P_2) \leq D_0$$

for all nonzero integers n_i.

(iii) *The set*

$$\{n \geq 1 : \mathrm{GCD}([n]P_1, [n]P_2) = \mathrm{GCD}(P_1, P_2)\}$$

has positive density in $\mathbb{N}$.

(iv) *For all but finitely many primes* q, *we have*

$$\mathrm{GCD}([q]P_1, [q]P_2) = \mathrm{GCD}(P_1, P_2).$$

Remark 4-4. The conclusion of Proposition 4-3 (i) for an arbitrary algebraically closed field k of characteristic 0 would follow from our method once the validity of DeMarco–Mavraki's result [DeMarco and Mavraki 2017] (see Theorem 2-3) is extended over function fields. In turn, their result is contingent on establishing the smooth variation of the canonical height in fibers of an elliptic surface defined over a function field (over $\overline{\mathbb{Q}}$).

The proof of Proposition 4-3 relies on Theorem 1-1 and the following lemma which is a variant of [Silverman 2004b, Lemma 4] bounding $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{O}_{\mathcal{E}}))$ for $\gamma \in C$ and all integers $n \neq 0$.

Lemma 4-5. *Let k be an algebraically closed field of characteristic* 0. *Let E be an elliptic curve defined over $k(C)$ and let $\mathcal{E} \to C$ be an elliptic surface whose generic fiber is E. Let $\gamma \in C(k)$ and let $P, Q \in E(k(C))$ be given. There exists a constant $m = m(\gamma, E, P, Q)$ such that* $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \leq m$ *for all integers n such that $[n]P \neq Q$.*

Proof. Observe that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \geq 1$ if and only if $\sigma_{[n]P}(\gamma) = \sigma_Q(\gamma)$. Moreover, $\sigma_Q(\gamma)$ is a torsion point of $\mathcal{E}_\gamma$ if and only if there are more than one n such that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \geq 1$.

It suffices to prove the assertion when $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \geq 1$ for more than one integer n. Thus, we assume that $\sigma_Q(\gamma)$ is a torsion point of $\mathcal{E}_\gamma$. Let ℓ be the order of $\sigma_Q(\gamma)$ and assume that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \geq 1$ for some integer n such that $[n]P \neq Q$. It follows that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q}))$ is finite and

$$\sigma_{[\ell n]P}(\gamma) = [\ell]\sigma_{[n]P}(\gamma) = [\ell]\sigma_Q(\gamma) = O_{\mathcal{E}_\gamma}, \tag{4-6}$$

which is the zero element for the elliptic curve $\mathcal{E}_\gamma$.

If Q is the zero element of E, then it follows from [Silverman 2004b, Lemma 4] that the value of $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{O}_{\mathcal{E}}))$ is bounded independently of $n \neq 0$ and we are done in this case.

Assume that $Q \neq O$. Then (4-6) yields the inequality

$$\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q})) \leq \mathrm{ord}_\gamma(\sigma^*_{[\ell n]P}(\overline{O}_{\mathcal{E}})).$$

Note that the right-hand side of the above inequality involves only $\mathrm{ord}_\gamma(\sigma^*_{[m]P}(\overline{O}_{\mathcal{E}}))$, which is bounded independently of the integer m in question as remarked above. Hence, we conclude that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q}))$ is bounded independently of $n \neq 0$ (and n such that $[n]P \neq Q$). As $Q \neq O$, we also have that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q}))$ is finite if $n = 0$. Thus we obtain that $\mathrm{ord}_\gamma(\sigma^*_{[n]P}(\overline{Q}))$ is bounded independently of n such that $[n]P \neq Q$, which concludes our proof. □

Proof of Proposition 4-3. We first prove part (i) in Proposition 4-3. So, for each $\gamma \in C(\overline{\mathbb{Q}})$, let $m_{i,\gamma}$ be an upper bound for $\mathrm{ord}_\gamma(\sigma^*_{[n]P_i}(\overline{Q}_i))$ as in Lemma 4-5. Set $m_\gamma = \min\{m_{1,\gamma}, m_{2,\gamma}\}$. Since P_1 and P_2 are independent, by Theorem 1-1 we may take $m_\gamma = 0$ for all but finitely many points $\gamma \in C(\overline{\mathbb{Q}})$; let S be the finite set of points $\gamma \in C(\overline{\mathbb{Q}})$ for which $m_\gamma > 0$. Let

$$D := \sum_{\gamma \in S} m_\gamma(\gamma).$$

Then, D is an effective divisor of C. Now it follows directly from Lemma 4-5 that $\mathrm{GCD}([n_1]P_1 - Q_1, [n_2]P_2 - Q_2) \leq D$ for all n_i such that $[n_i]P \neq Q_i$ for both $i = 1, 2$. Indeed,

$$\begin{aligned}
&\mathrm{GCD}([n_1]P_1 - Q_1, [n_2]P_2 - Q_2)\\
&\qquad = \mathrm{GCD}(\sigma^*_{[n_1]P_1 - Q_1}(\overline{O}_{\mathcal{E}_1}), \sigma^*_{[n_2]P_2 - Q_2}(\overline{O}_{\mathcal{E}_2}))\\
&\qquad = \mathrm{GCD}(\sigma^*_{[n_1]P}(\overline{Q_1}), \sigma^*_{[n_2]P_2}(\overline{Q_2}))\\
&\qquad = \sum_{\gamma \in C(\overline{\mathbb{Q}})} \min\bigl\{\mathrm{ord}_\gamma(\sigma^*_{[n_1]P_1}(\overline{Q_1})), \mathrm{ord}_\gamma(\sigma^*_{[n_2]P_2}(\overline{Q_2}))\bigr\}\\
&\qquad \leq \sum_{\gamma \in C(\overline{\mathbb{Q}})} \min\{m_{1,\gamma}, m_{2,\gamma}\} \cdot (\gamma) \leq \sum_{\gamma \in S} m_\gamma(\gamma).
\end{aligned}$$

For the proof of part (ii) in Proposition 4-3, we let $Q_i = O_i$ be the zero element of E_i for $i = 1, 2$. If $k = \overline{\mathbb{Q}}$, then the result follows immediately from part (i). Now, for the general case, we note that it suffices to prove the existence of at most finitely many $t \in C(k)$ such that both $(P_1)_t$ and $(P_2)_t$ are torsion points on the elliptic fiber $\mathcal{E}_{1,t}$ and $\mathcal{E}_{2,t}$ respectively; indeed, the fact that the multiplicity of each such t appearing in a divisor $\mathrm{GCD}([n_1]P_1, [n_2]P_2)$ is bounded follows exactly as in the proof of part (i), using Lemma 4-5. On the other hand, if there exist infinitely many $t \in C(k)$ such that both $(P_1)_t$ and $(P_2)_t$ are torsion, then (according to [Masser and Zannier 2014, Theorem, p. 117]) P_1 and P_2 are related, which yields a contradiction.

The conclusion of part (iii) in Proposition 4-3 was proven by Silverman [2004b, Theorem 8 (b)] in the case where both E_1, E_2 have constant j-invariants. We generalize his argument as follows. For each of the finitely many $\gamma \in C(k)$ which does not appear in the support of $\mathrm{GCD}(P_1, P_2)$, but for which there exists some positive integer n such that γ is contained in the support of the divisor $\mathrm{GCD}([n]P_1, [n]P_2)$, or equivalently,

$$\text{the divisor } \mathrm{GCD}([n]P_1, [n]P_2) - (\gamma) \text{ is effective,} \tag{4-7}$$

we let n_γ be the smallest such positive integer n for which (4-7) holds. Then, it is easy to see that γ is contained in the support of $\mathrm{GCD}([n]P_1, [n]P_2)$ if and only if $n_\gamma \mid n$. Also, for each of these points γ which are not in the support of $\mathrm{GCD}(P_1, P_2)$, we have $n_\gamma > 1$. This implies that for any positive integer n which is not divisible by any of the finitely many integers n_γ, we have

$$\mathrm{GCD}([n]P_1, [n]P_2) = \mathrm{GCD}(P_1, P_2).$$

The conclusion in part (iv) in Proposition 4-3 follows from the proof of part (iii) since $\mathrm{GCD}([q]P_1, [q]P_2) = \mathrm{GCD}(P_1, P_2)$ for all primes q which do not divide any of the finitely many numbers $n_\gamma > 1$. □

Acknowledgments

We thank Myrto Mavraki and Joe Silverman for several useful conversations. We are grateful to the anonymous referee for numerous comments and suggestions which improved our paper. The research of Ghioca was partially supported by an NSERC Discovery grant. Hsia was supported by MOST grant 104-2115-M-003-004-MY2. Tucker was partially supported by NSF Grant DMS-0101636.

References

[Ailon and Rudnick 2004] N. Ailon and Z. Rudnick, "Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$", *Acta Arith.* **113**:1 (2004), 31–38. MR Zbl

[Amoroso et al. 2017] F. Amoroso, D. Masser, and U. Zannier, "Bounded height in pencils of finitely generated subgroups", *Duke Math. J.* **166**:13 (2017), 2599–2642. MR Zbl

[Barroero and Capuano 2016] F. Barroero and L. Capuano, "Linear relations in families of powers of elliptic curves", *Algebra Number Theory* **10**:1 (2016), 195–214. MR Zbl

[Barroero and Capuano 2017] F. Barroero and L. Capuano, "Unlikely intersections in products of families of elliptic curves and the multiplicative group", *Quart. J. Math.* **68**:4 (2017), 1117–1138.

[Bugeaud et al. 2003] Y. Bugeaud, P. Corvaja, and U. Zannier, "An upper bound for the GCD of $a^n - 1$ and $b^n - 1$", *Math. Z.* **243**:1 (2003), 79–84. MR Zbl

[Cinkir 2011] Z. Cinkir, "Zhang's conjecture and the effective Bogomolov conjecture over function fields", *Invent. Math.* **183**:3 (2011), 517–562. MR Zbl

[Corvaja and Zannier 2008] P. Corvaja and U. Zannier, "Some cases of Vojta's conjecture on integral points over function fields", *J. Algebraic Geom.* **17**:2 (2008), 295–333. Addendum in *Asian J. Math.* **14**:4 (2010), 581–584. MR Zbl

[Corvaja and Zannier 2011] P. Corvaja and U. Zannier, "An *abcd* theorem over function fields and applications", *Bull. Soc. Math. France* **139**:4 (2011), 437–454. MR Zbl

[Corvaja and Zannier 2013a] P. Corvaja and U. Zannier, "Algebraic hyperbolicity of ramified covers of $\mathbb{G}_m^2$ (and integral points on affine subsets of $\mathbb{P}_2$)", *J. Differential Geom.* **93**:3 (2013), 355–377. MR Zbl

[Corvaja and Zannier 2013b] P. Corvaja and U. Zannier, "Greatest common divisors of $u-1$, $v-1$ in positive characteristic and rational points on curves over finite fields", *J. Eur. Math. Soc.* **15**:5 (2013), 1927–1942. MR Zbl

[DeMarco and Mavraki 2017] L. DeMarco and N. M. Mavraki, "Variation of canonical height and equidistribution", preprint, 2017. arXiv

[DeMarco et al. 2016] L. DeMarco, X. Wang, and H. Ye, "Torsion points and the Lattès family", *Amer. J. Math.* **138**:3 (2016), 697–732. MR Zbl

[Denis 2011] L. Denis, "Facteurs communs et torsion en caractéristique non nulle", *J. Théor. Nombres Bordeaux* **23**:2 (2011), 347–352. MR Zbl

[Faltings 1994] G. Faltings, "The general case of S. Lang's conjecture", pp. 175–182 in *Barsotti Symposium in Algebraic Geometry* (Abano Terme, Italy, 1991), edited by V. Cristante and W. Messing, Perspect. Math. **15**, Academic Press, San Diego, CA, 1994. MR Zbl

[Ghioca 2014] D. Ghioca, "A Bogomolov type statement for function fields", *Bull. Inst. Math. Acad. Sin.* (*N.S.*) **9**:4 (2014), 641–656. MR Zbl

[Ghioca et al. 2017] D. Ghioca, L.-C. Hsia, and T. J. Tucker, "On a variant of the Ailon–Rudnick theorem in finite characteristic", *New York J. Math.* **23** (2017), 213–225. MR Zbl

[Gubler 2007] W. Gubler, "The Bogomolov conjecture for totally degenerate abelian varieties", *Invent. Math.* **169**:2 (2007), 377–400. MR Zbl

[Habegger and Pila 2016] P. Habegger and J. Pila, "O-minimality and certain atypical intersections", *Ann. Sci. Éc. Norm. Supér.* (4) **49**:4 (2016), 813–858. MR Zbl

[Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Graduate Texts in Mathematics **201**, Springer, 2000. MR Zbl

[Hrushovski 1996] E. Hrushovski, "The Mordell–Lang conjecture for function fields", *J. Amer. Math. Soc.* **9**:3 (1996), 667–690. MR Zbl

[Hsia and Tucker 2017] L.-C. Hsia and T. J. Tucker, "Greatest common divisors of iterates of polynomials", *Algebra Number Theory* **11**:6 (2017), 1437–1459. MR Zbl

[Lang 1965] S. Lang, "Division points on curves", *Ann. Mat. Pura Appl.* (4) **70** (1965), 229–234. MR Zbl

[Masser and Zannier 2012] D. Masser and U. Zannier, "Torsion points on families of squares of elliptic curves", *Math. Ann.* **352**:2 (2012), 453–484. MR Zbl

[Masser and Zannier 2014] D. Masser and U. Zannier, "Torsion points on families of products of elliptic curves", *Adv. Math.* **259** (2014), 116–133. MR Zbl

[Raynaud 1983] M. Raynaud, "Courbes sur une variété abélienne et points de torsion", *Invent. Math.* **71**:1 (1983), 207–233. MR Zbl

[Silverman 1983] J. H. Silverman, "Heights and the specialization map for families of abelian varieties", *J. Reine Angew. Math.* **342** (1983), 197–211. MR Zbl

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, 1986. MR Zbl

[Silverman 1994a] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994. MR Zbl

[Silverman 1994b] J. H. Silverman, "Variation of the canonical height on elliptic surfaces, III: Global boundedness properties", *J. Number Theory* **48**:3 (1994), 330–352. MR Zbl

[Silverman 2004a] J. H. Silverman, "Common divisors of $a^n - 1$ and $b^n - 1$ over function fields", *New York J. Math.* **10** (2004), 37–43. MR Zbl

[Silverman 2004b] J. H. Silverman, "Common divisors of elliptic divisibility sequences over function fields", *Manuscripta Math.* **114**:4 (2004), 431–446. MR Zbl

[Tate 1983] J. Tate, "Variation of the canonical height of a point depending on a parameter", *Amer. J. Math.* **105**:1 (1983), 287–294. MR Zbl

[Yamaki 2017] K. Yamaki, "Non-density of small points on divisors on abelian varieties and the Bogomolov conjecture", *J. Amer. Math. Soc.* **30**:4 (2017), 1133–1163. MR Zbl

[Zhang 1998] S.-W. Zhang, "Equidistribution of small points on abelian varieties", *Ann. of Math.* (2) **147**:1 (1998), 159–165. MR Zbl

Received March 8, 2017. Revised November 10, 2017.

DRAGOS GHIOCA
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF BRITISH COLUMBIA
VANCOUVER, BC
CANADA

dghioca@math.ubc.ca

LIANG-CHUNG HSIA
DEPARTMENT OF MATHEMATICS
NATIONAL TAIWAN NORMAL UNIVERSITY
TAIPEI
TAIWAN

hsia@math.ntnu.edu.tw

THOMAS J. TUCKER
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ROCHESTER
ROCHESTER, NY
UNITED STATES

ttucker@math.rochester.edu

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.17

ON THE EXACTNESS OF ORDINARY PARTS OVER A LOCAL FIELD OF CHARACTERISTIC p

JULIEN HAUSEUX

Let G be a connected reductive group over a nonarchimedean local field F of residue characteristic p, P be a parabolic subgroup of G, and R be a commutative ring. When R is artinian, p is nilpotent in R, and $\mathrm{char}(F) = p$, we prove that the ordinary part functor Ord_P is exact on the category of admissible smooth R-representations of G. We derive some results on Yoneda extensions between admissible smooth R-representations of G.

1. Results

Let F be a nonarchimedean local field of residue characteristic p. Let $\boldsymbol{G}$ be a connected reductive algebraic F-group and G denote the topological group $\boldsymbol{G}(F)$. We let $\boldsymbol{P} = \boldsymbol{M}\boldsymbol{N}$ be a parabolic subgroup of $\boldsymbol{G}$. We write $\overline{\boldsymbol{P}} = \boldsymbol{M}\overline{\boldsymbol{N}}$ for the opposite parabolic subgroup.

Let R be a commutative ring. We write $\mathrm{Mod}_G^\infty(R)$ for the category of smooth R-representations of G (i.e., $R[G]$-modules π such that for all $v \in \pi$ the stabiliser of v is open in G) and $R[G]$-linear maps. It is an R-linear abelian category. When R is noetherian, we write $\mathrm{Mod}_G^{\mathrm{adm}}(R)$ for the full subcategory of $\mathrm{Mod}_G^\infty(R)$ consisting of admissible representations (i.e., those representations π such that π^H is finitely generated over R for any open subgroup H of G). It is closed under passing to subrepresentations and extensions, thus it is an R-linear exact subcategory, but quotients of admissible representations may not be admissible when $\mathrm{char}(F) = p$ (see [Abe et al. 2017b, Example 4.4]).

Recall the smooth parabolic induction functor $\mathrm{Ind}_{\overline{P}}^G : \mathrm{Mod}_M^\infty(R) \to \mathrm{Mod}_G^\infty(R)$, defined on any smooth R-representation σ of M as the R-module $\mathrm{Ind}_{\overline{P}}^G(\sigma)$ of locally constant functions $f : G \to \sigma$ satisfying $f(m\bar{n}g) = m \cdot f(g)$ for all $m \in M$, $\bar{n} \in \overline{N}$, and $g \in G$, endowed with the smooth action of G by right translation. It is R-linear, exact, and commutes with small direct sums. In the other direction, there is the ordinary part functor $\mathrm{Ord}_P : \mathrm{Mod}_G^\infty(R) \to \mathrm{Mod}_M^\infty(R)$ [Emerton 2010a; Vignéras 2016]. It

This research was partly supported by EPSRC grant EP/L025302/1.
MSC2010: 22E50.
Keywords: local fields, reductive groups, admissible smooth representations, parabolic induction, ordinary parts, extensions.

is R-linear and left exact. When R is noetherian, Ord_P also commutes with small inductive limits, both functors respect admissibility, and the restriction of Ord_P to $\mathrm{Mod}_G^{\mathrm{adm}}(R)$ is right adjoint to the restriction of $\mathrm{Ind}_{\overline{P}}^G$ to $\mathrm{Mod}_M^{\mathrm{adm}}(R)$.

Theorem 1. *If R is artinian, p is nilpotent in R, and* $\mathrm{char}(F) = p$, *then* Ord_P *is exact on* $\mathrm{Mod}_G^{\mathrm{adm}}(R)$.

Thus the situation is very different from the case $\mathrm{char}(F) = 0$ (see [Emerton 2010b]). On the other hand, if R is artinian and p is invertible in R, then Ord_P is isomorphic on $\mathrm{Mod}_G^{\mathrm{adm}}(R)$ to the Jacquet functor with respect to P (i.e., the N-coinvariants) twisted by the inverse of the modulus character δ_P of P [Abe et al. 2017b, Corollary 4.19], so that it is exact on $\mathrm{Mod}_G^{\mathrm{adm}}(R)$ without any assumption on $\mathrm{char}(F)$.

Remark. Without any assumption on R, $\mathrm{Ind}_P^G : \mathrm{Mod}_M^\infty(R) \to \mathrm{Mod}_G^\infty(R)$ admits a left adjoint $\mathrm{L}_P^G : \mathrm{Mod}_G^\infty(R) \to \mathrm{Mod}_M^\infty(R)$ (the Jacquet functor with respect to P) and a right adjoint $\mathrm{R}_P^G : \mathrm{Mod}_G^\infty(R) \to \mathrm{Mod}_M^\infty(R)$ [Vignéras 2016, Proposition 4.2]. If R is noetherian and p is nilpotent in R, then R_P^G is isomorphic to $\mathrm{Ord}_{\overline{P}}$ on $\mathrm{Mod}_G^{\mathrm{adm}}(R)$ [Abe et al. 2017b, Corollary 4.13]. Thus under the assumptions of Theorem 1, R_P^G is exact on $\mathrm{Mod}_G^{\mathrm{adm}}(R)$. On the other hand, if R is noetherian and p is invertible in R, then R_P^G is expected to be isomorphic to $\delta_P\,\mathrm{L}_{\overline{P}}^G$ ("second adjointness"), and this is proved in the following cases: when R is the field of complex numbers [Bernstein 1987] or an algebraically closed field of characteristic $\ell \neq p$ [Vignéras 1996, II.3.8(2)]; when $\boldsymbol{G}$ is a Levi subgroup of a general linear group or a classical group with $p \neq 2$ [Dat 2009, Théorème 1.5]; when $\boldsymbol{P}$ is a minimal parabolic subgroup of $\boldsymbol{G}$ (see also [Dat 2009]). In particular, L_P^G and R_P^G are exact in all these cases.

Question. Are L_P^G and R_P^G exact when R is noetherian, p is nilpotent in R, and $\mathrm{char}(F) = p$?

We derive from Theorem 1 some results on Yoneda extensions between admissible R-representations of G. We compute the R-modules $\mathrm{Ext}_G^\bullet$ in $\mathrm{Mod}_G^{\mathrm{adm}}(R)$.

Corollary 2. *Assume R artinian, p nilpotent in R, and* $\mathrm{char}(F) = p$. *Let σ and π be admissible R-representations of M and G, respectively. For all $n \geq 0$, there is a natural R-linear isomorphism*

$$\mathrm{Ext}_M^n(\sigma, \mathrm{Ord}_P(\pi)) \xrightarrow{\sim} \mathrm{Ext}_G^n(\mathrm{Ind}_{\overline{P}}^G(\sigma), \pi).$$

This is in contrast with the case $\mathrm{char}(F) = 0$ (see [Hauseux 2016a]). A direct consequence of Corollary 2 is that under the same assumptions, $\mathrm{Ind}_{\overline{P}}^G$ induces an isomorphism between the Ext^n for all $n \geq 0$ (Corollary 5). When $R = C$ is an algebraically closed field of characteristic p and $\mathrm{char}(F) = p$, we determine the extensions between certain irreducible admissible C-representations of G using the classification of [Abe et al. 2017a] (Proposition 6). In particular, we prove that there exists no nonsplit extension of an irreducible admissible C-representation π of G by a supersingular C-representation of G when π is not the extension to G of a supersingular representation of a Levi subgroup of G (Corollary 7). For $\boldsymbol{G} = \mathrm{GL}_2$, this was first proved by Hu [2017, Theorem A.2].

2. Proofs

2.1. ***Hecke action.*** In this subsection, $\boldsymbol{M}$ denotes a linear algebraic F-group and $\boldsymbol{N}$ denotes a split unipotent algebraic F-group (see [Conrad et al. 2015, Appendix B]) endowed with an action of $\boldsymbol{M}$ that we identify with the conjugation in $\boldsymbol{M} \ltimes \boldsymbol{N}$. We fix an open submonoid M^+ of M and a compact open subgroup N_0 of N stable under conjugation by M^+.

If π is a smooth R-representation of $M^+ \ltimes N_0$, then the R-modules $\mathrm{H}^\bullet(N_0, \pi)$, computed using the homogeneous cochain complex $\mathrm{C}^\bullet(N_0, \pi)$ (see [Neukirch et al. 2008, § I.2]), are naturally endowed with the Hecke action of M^+, defined as the composite

$$\mathrm{H}^\bullet(N_0, \pi) \xrightarrow{m} \mathrm{H}^\bullet(mN_0m^{-1}, \pi) \xrightarrow{\mathrm{cor}} \mathrm{H}^\bullet(N_0, \pi)$$

for all $m \in M^+$. At the level of cochains, this action is explicitly given as follows (see [Neukirch et al. 2008, § I.5]). Fix a set of representatives $\overline{N_0/mN_0m^{-1}} \subseteq N_0$ of the left cosets N_0/mN_0m^{-1} and write $n \mapsto \bar{n}$ for the projection $N_0 \twoheadrightarrow \overline{N_0/mN_0m^{-1}}$. For $\phi \in \mathrm{C}^k(N_0, \pi)$, we have

$$(1) \quad (m \cdot \phi)(n_0, \dots, n_k) = \sum_{\bar{n} \in \overline{N_0/mN_0m^{-1}}} \bar{n}m \cdot \phi(m^{-1}\bar{n}^{-1}n_0\overline{n_0^{-1}\bar{n}}m, \dots, m^{-1}\bar{n}^{-1}n_k\overline{n_k^{-1}\bar{n}}m)$$

for all $(n_0, \dots, n_k) \in N_0^{k+1}$.

Lemma 3. *Assume p nilpotent in R and* $\mathrm{char}(F) = p$. *Let π be a smooth R-representation of $M^+ \ltimes N_0$ and $m \in M^+$. If the Hecke action $h_{N_0,m}$ of m on π^{N_0} is locally nilpotent (i.e., for all $v \in \pi^{N_0}$ there exists $r \geq 0$ such that $h_{N_0,m}^r(v) = 0$), then the Hecke action of m on* $\mathrm{H}^k(N_0, \pi)$ *is locally nilpotent for all $k \geq 0$.*

Proof. First, we prove the lemma when $pR = 0$, i.e., R is a commutative $\mathbb{F}_p$-algebra. We assume that the Hecke action of m on π^{N_0} is locally nilpotent and we prove the result together with the following fact: there exists a set of representatives $\overline{N_0/mN_0m^{-1}} \subseteq N_0$ of the left cosets N_0/mN_0m^{-1} such that the action of

$$S := \sum_{\bar{n} \in \overline{N_0/mN_0m^{-1}}} \bar{n}m \in \mathbb{F}_p[M^+ \ltimes N_0]$$

on π is locally nilpotent.

We proceed by induction on the dimension of $\boldsymbol{N}$ (recall that $\boldsymbol{N}$ is split so that it is smooth and connected). If $\boldsymbol{N}=1$, then the (Hecke) action of m on $\pi^{N_0}=\pi$ is locally nilpotent by assumption, so that the result and the fact are trivially true. Assume $\boldsymbol{N}\neq 1$ and that the result and the fact are true for groups of smaller dimension. Since $\boldsymbol{N}$ is split, it admits a nontrivial central subgroup isomorphic to the additive group. We let $\boldsymbol{N}'$ be the subgroup of $\boldsymbol{N}$ generated by all such subgroups. It is a nontrivial vector group (i.e., isomorphic to a direct product of copies of the additive group) which is central (hence normal) in $\boldsymbol{N}$ and stable under conjugation by $\boldsymbol{M}$ (since it is a characteristic subgroup of $\boldsymbol{N}$). We set $\boldsymbol{N}'' := \boldsymbol{N}/\boldsymbol{N}'$. It is a split unipotent algebraic F-group endowed with the induced action of $\boldsymbol{M}$ and $\dim(\boldsymbol{N}'') < \dim(\boldsymbol{N})$. Since $\boldsymbol{N}'$ is split, we have $N''=N/N'$. We write N_0' and N_0'' for the compact open subgroups $N'\cap N_0$ and N_0/N_0' of N' and N'', respectively. They are stable under conjugation by M^+. We fix a set-theoretic section $[-]: N_0'' \hookrightarrow N_0$.

Since $\boldsymbol{N}'$ is commutative and p-torsion, N_0' is a compact $\mathbb{F}_p$-vector space. Thus for any open subgroup N_1' of N_0', the short exact sequence of compact $\mathbb{F}_p$-vector spaces

$$0 \to N_1' \to N_0' \to N_0'/N_1' \to 0$$

splits. Indeed, it admits an $\mathbb{F}_p$-linear splitting (since $\mathbb{F}_p$ is a field) which is automatically continuous (since N_0'/N_1' is discrete). In particular, with $N_1'=mN_0'm^{-1}$, we may and do fix a section $N_0'/mN_0'm^{-1} \hookrightarrow N_0'$. We write $\overline{N_0'/mN_0'm^{-1}}$ for its image, so that $N_0' = \overline{N_0'/mN_0'm^{-1}} \times mN_0'm^{-1}$, and $n'\mapsto \bar{n}'$ for the projection $N_0' \twoheadrightarrow \overline{N_0'/mN_0'm^{-1}}$. We set

$$S' := \sum_{\bar{n}'\in \overline{N_0'/mN_0'm^{-1}}} \bar{n}'m \in \mathbb{F}_p[M^+ \ltimes N_0'].$$

For all $n_0' \in N_0'$, we have $n_0'=\bar{n}_0'(\bar{n}_0'^{-1}n_0')$ with $\bar{n}_0'^{-1}n_0' \in mN_0'm^{-1}$, thus

$$n_0'S' = \sum_{\bar{n}'\in \overline{N_0'/mN_0'm^{-1}}} (\bar{n}_0'\bar{n}')m(m^{-1}(\bar{n}_0'^{-1}n_0')m) = S'(m^{-1}(\bar{n}_0'^{-1}n_0')m)$$

with $m^{-1}(\bar{n}_0'^{-1}n_0')m \in N_0'$ (in the first equality we use the fact that N_0' is commutative and in the second one we use the fact that $\overline{N_0'/mN_0'm^{-1}}$ is a group). Therefore, there is an inclusion $\mathbb{F}_p[N_0']S' \subseteq S'\mathbb{F}_p[N_0']$.

The R-module $\pi^{N_0'}$, endowed with the induced action of N_0'' and the Hecke action of M^+ with respect to N_0', is a smooth R-representation of $M^+ \ltimes N_0''$ (see the proof of [Hauseux 2016b, Lemme 3.2.1] in degree 0). On $\pi^{N_0'}$, the Hecke action of m with respect to N_0' coincides with the action of S' by definition. On $(\pi^{N_0'})^{N_0''}=\pi^{N_0}$, the Hecke action of m with respect to N_0'' coincides with the Hecke action of m with respect to N_0 (see the proof of [Hauseux 2016b, Lemme 3.2.2]) which is locally nilpotent by assumption. Thus by the induction hypothesis, there exists a set of representatives $\overline{N_0''/mN_0''m^{-1}} \subseteq N_0''$ of the left cosets $N_0''/mN_0''m^{-1}$ such that the action of

$$S := \sum_{\bar{n}'' \in \overline{N_0''/mN_0''m^{-1}}} [\bar{n}'']S' \in \mathbb{F}_p[M^+ \ltimes N_0]$$

on $\pi^{N_0'}$ is locally nilpotent. Moreover, there is an inclusion $\mathbb{F}_p[N_0']S \subseteq S\mathbb{F}_p[N_0']$ (because N_0' is central in N_0 and $\mathbb{F}_p[N_0']S' \subseteq S'\mathbb{F}_p[N_0']$).

We prove the fact. By [Hauseux 2016c, Lemme 2.1],

$$\overline{N_0/mN_0m^{-1}} := \left\{[\bar{n}'']\bar{n}' : \bar{n}'' \in \overline{N_0''/mN_0''m^{-1}},\ \bar{n}' \in \overline{N_0'/mN_0'm^{-1}}\right\} \subseteq N_0$$

is a set of representatives of the left cosets N_0/mN_0m^{-1}, and by definition,

$$S = \sum_{\bar{n} \in \overline{N_0/mN_0m^{-1}}} \bar{n}m.$$

We prove that the action of S on π is locally nilpotent. We proceed as in the proof of [Hu 2012, Théorème 5.1(i)]. Let $v \in \pi$ and set $\pi_r := \mathbb{F}_p[N_0'] \cdot (S^r \cdot v)$ for all $r \geq 0$. Since $\mathbb{F}_p[N_0']S \subseteq S\mathbb{F}_p[N_0']$, we have $\pi_{r+1} \subseteq S \cdot \pi_r$ for all $r \geq 0$. Since N_0' is compact, we have $\dim_{\mathbb{F}_p}(\pi_r) < \infty$ for all $r \geq 0$. If $S^r \cdot v \neq 0$, i.e., $\pi_r \neq 0$, for some $r \geq 0$, then $\pi_r^{N_0'} \neq 0$ (because N_0' is a pro-p group and π_r is a nonzero $\mathbb{F}_p$-vector space) so that $\dim_{\mathbb{F}_p}(S \cdot \pi_r) < \dim_{\mathbb{F}_p} \pi_r$ (because the action of S on $\pi^{N_0'}$ is locally nilpotent). Therefore $\pi_r = 0$, i.e., $S^r \cdot v = 0$, for all $r \geq \dim_{\mathbb{F}_p}(\pi_0)$.

We prove the result. The R-modules $\mathrm{H}^\bullet(N_0', \pi)$, endowed with the induced action of N_0'' and the Hecke action of M^+, are smooth R-representations of $M^+ \ltimes N_0''$ (see the proof of [Hauseux 2016b, Lemme 3.2.1][1]). At the level of cochains, the actions of $n'' \in N_0''$ and m are explicitly given as follows. For $\phi \in \mathrm{C}^j(N_0', \pi)$, we have

$$(n'' \cdot \phi)(n_0', \ldots, n_j') = [n''] \cdot \phi(n_0', \ldots, n_j') \tag{2}$$

$$(m \cdot \phi)(n_0', \ldots, n_j') = S' \cdot \phi(m^{-1}n_0'\bar{n}_0'^{-1}m, \ldots, m^{-1}n_j'\bar{n}_j'^{-1}m) \tag{3}$$

for all $(n_0', \ldots, n_j') \in N_0'^{j+1}$ (for (2) we use the fact that N_0' is central in N_0, for (3) we use (1) and the fact that $n' \mapsto \bar{n}'$ is a group homomorphism $N_0' \to \overline{N_0'/mN_0'm^{-1}}$). Using (2) and (3), we can give explicitly the Hecke action of m on $\mathrm{H}^\bullet(N_0', \pi)^{N_0''}$ at the level of cochains as follows. For $\phi \in \mathrm{C}^j(N_0', \pi)$, we have

$$(m \cdot \phi)(n_0', \ldots, n_j') = S \cdot \phi(m^{-1}n_0'\bar{n}_0'^{-1}m, \ldots, m^{-1}n_j'\bar{n}_j'^{-1}m)$$

for all $(n_0', \ldots, n_j') \in N_0'^{j+1}$. Since the action of S on π is locally nilpotent and the image of a locally constant cochain is finite by compactness of N_0', we deduce that the Hecke action of m on $\mathrm{H}^j(N_0', \pi)^{N_0''}$ is locally nilpotent for all $j \geq 0$. Thus

[1] We do not know whether [Emerton 2010b, Proposition 2.1.11] holds true when $\mathrm{char}(F) = p$, but [Hauseux 2016b, Lemme 3.1.1] does and any injective object of $\mathrm{Mod}^\infty_{M^+ \ltimes N_0}(R)$ is still N_0-acyclic.

the Hecke action of m on $\mathrm{H}^i(N_0'', \mathrm{H}^j(N_0', \pi))$ is locally nilpotent for all $i, j \geq 0$ by the induction hypothesis. Using the spectral sequence of smooth R-representations of M^+

$$\mathrm{H}^i(N_0'', \mathrm{H}^j(N_0', \pi)) \Rightarrow \mathrm{H}^{i+j}(N_0, \pi)$$

(see the proof of [Hauseux 2016b, Proposition 3.2.3] and the footnote on page 21), we conclude that the Hecke action of m on $\mathrm{H}^k(N_0, \pi)$ is locally nilpotent for all $k \geq 0$.

Now, we prove the lemma without assuming $pR = 0$. We proceed by induction on the degree of nilpotency r of p in R. If $r \leq 1$, then the lemma is already proved. We assume $r > 1$ and that we know the lemma for rings in which the degree of nilpotency of p is $r-1$. There is a short exact sequence of smooth R-representations of $M^+ \ltimes N_0$,

$$0 \to p\pi \to \pi \to \pi/p\pi \to 0.$$

Taking the N_0-cohomology yields a long exact sequence of smooth R-representations of M^+,

$$0 \to (p\pi)^{N_0} \to \pi^{N_0} \to (\pi/p\pi)^{N_0} \to \mathrm{H}^1(N_0, p\pi) \to \cdots . \tag{4}$$

If the Hecke action of m on π^{N_0} is locally nilpotent, then the Hecke action of m on $(p\pi)^{N_0}$ is also locally nilpotent so that the Hecke action of m on $\mathrm{H}^k(N_0, p\pi)$ is locally nilpotent for all $k \geq 0$ by the induction hypothesis (since $p\pi$ is an $R/p^{r-1}R$-module). Using (4), we deduce that the Hecke action of m on $(\pi/p\pi)^{N_0}$ is also locally nilpotent so that the Hecke action of m on $\mathrm{H}^k(N_0, \pi/p\pi)$ is locally nilpotent for all $k \geq 0$ (since $\pi/p\pi$ is an $\mathbb{F}_p$-vector space). Using again (4), we conclude that the Hecke action of m on $\mathrm{H}^k(N_0, \pi)$ is locally nilpotent for all $k \geq 0$. □

2.2. ***Proof of the main result.*** We fix a compact open subgroup N_0 of N and we let M^+ be the open submonoid of M consisting of those elements m contracting N_0 (i.e., $mN_0m^{-1} \subseteq N_0$). We let Z_M denote the centre of M and we set $Z_M^+ := Z_M \cap M^+$. We fix an element $z \in Z_M^+$ strictly contracting N_0 (i.e., $\bigcap_{r\geq 0} z^r N_0 z^{-r} = 1$).

Recall that the ordinary part of a smooth R-representation π of P is the smooth R-representation of M

$$\mathrm{Ord}_P(\pi) := \left(\mathrm{Ind}_{M^+}^M(\pi^{N_0})\right)^{Z_M-\mathrm{l.fin}},$$

where $\mathrm{Ind}_{M^+}^M(\pi^{N_0})$ is defined as the R-module of functions $f : M \to \pi^{N_0}$ such that $f(mm') = m \cdot f(m')$ for all $m \in M^+$ and $m' \in M$, endowed with the action of M by right translation, and the superscript ${}^{Z_M-\mathrm{l.fin}}$ denotes the subrepresentation consisting of locally Z_M-finite elements (i.e., those elements f such that $R[Z_M] \cdot f$ is contained in a finitely generated R-submodule). The action of M on the latter is smooth by [Vignéras 2016, Remark 7.6]. If R is artinian and π^{N_0} is locally Z_M^+-finite (i.e., it may be written as the union of finitely generated Z_M^+-invariant

R-submodules), then there is a natural R-linear isomorphism,

$$\mathrm{Ord}_P(\pi) \xrightarrow{\sim} R[z^{\pm 1}] \otimes_{R[z]} \pi^{N_0} \tag{5}$$

(cf. [Emerton 2010b, Lemma 3.2.1(1)], whose proof also works when $\mathrm{char}(F) = p$ and over any artinian ring).

If σ is a smooth R-representation of M, then the R-module $\mathcal{C}_c^\infty(N, \sigma)$ of locally constant functions $f : N \to \sigma$ with compact support, endowed with the action of N by right translation and the action of M given by $(m \cdot f) : n \mapsto m \cdot f(m^{-1}nm)$ for all $m \in M$, is a smooth R-representation of P. Thus we obtain a functor $\mathcal{C}_c^\infty(N, -) : \mathrm{Mod}_M^\infty(R) \to \mathrm{Mod}_P^\infty(R)$. It is R-linear, exact, and commutes with small direct sums. The results of [Emerton 2010a, § 4.2] hold true when $\mathrm{char}(F) = p$ and over any ring, thus the functors

$$\mathcal{C}_c^\infty(N, -) : \mathrm{Mod}_M^\infty(R)^{Z_M-\mathrm{l.fin}} \to \mathrm{Mod}_P^\infty(R),$$

$$\mathrm{Ord}_P : \mathrm{Mod}_P^\infty(R) \to \mathrm{Mod}_M^\infty(R)^{Z_M-\mathrm{l.fin}}$$

are adjoint and the unit of the adjunction is an isomorphism.

Lemma 4. *Assume R artinian, p nilpotent in R, and* $\mathrm{char}(F) = p$. *Let π be a smooth R-representation of P. If π^{N_0} is locally Z_M^+-finite, then the Hecke action of z on* $\mathrm{H}^k(N_0, \pi)$ *is locally nilpotent for all $k \geq 1$.*

Proof. We set $\sigma := \mathrm{Ord}_P(\pi)$. The counit of the adjunction between $\mathcal{C}_c^\infty(N, -)$ and Ord_P induces a natural morphism of smooth R-representations of P,

$$\mathcal{C}_c^\infty(N, \sigma) \to \pi. \tag{6}$$

Taking the N_0-invariants yields a morphism of smooth R-representations of M^+,

$$\mathcal{C}_c^\infty(N, \sigma)^{N_0} \to \pi^{N_0}. \tag{7}$$

By definition, σ is locally Z_M-finite so it may be written as the union of finitely generated Z_M-invariant R-submodules $(\sigma_i)_{i \in I}$. Thus $\mathcal{C}_c^\infty(N, \sigma)^{N_0}$ is the union of the finitely generated Z_M^+-invariant R-submodules $(\mathcal{C}^\infty(z^{-r} N_0 z^r, \sigma_i)^{N_0})_{r \geq 0, i \in I}$, so it is locally Z_M^+-finite. By assumption, π^{N_0} is also locally Z_M^+-finite. Therefore, using (5) and its analogue with $\mathcal{C}_c^\infty(N, \sigma)$ instead of π, the localisation with respect to z of (7) is the natural morphism of smooth R-representations of M

$$\mathrm{Ord}_P(\mathcal{C}_c^\infty(N, \sigma)) \to \mathrm{Ord}_P(\pi)$$

induced by applying the functor Ord_P to (6), and it is an isomorphism since the unit of the adjunction between $\mathcal{C}_c^\infty(N, -)$ and Ord_P is an isomorphism.

Let κ and ι be the kernel and image, respectively, of (6), hence two short exact sequences of smooth R-representations of P,

$$0 \to \kappa \to \mathcal{C}_\mathrm{c}^\infty(N, \sigma) \to \iota \to 0, \tag{8}$$

$$0 \to \iota \to \pi \to \pi/\iota \to 0, \tag{9}$$

such that the third arrow of (8) and the second arrow of (9) fit into a commutative diagram of smooth R-representations of P whose upper arrow is (6):

$$\begin{tikzcd} \mathcal{C}_\mathrm{c}^\infty(N, \sigma) \arrow[rr] \arrow[dr, two heads] & & \pi \\ & \iota \arrow[ur, hook] & \end{tikzcd}$$

Taking the N_0-invariants yields a commutative diagram of smooth R-representations of M^+ whose upper arrow is (7):

$$\begin{tikzcd} \mathcal{C}_\mathrm{c}^\infty(N, \sigma)^{N_0} \arrow[rr] \arrow[dr] & & \pi^{N_0} \\ & \iota^{N_0} \arrow[ur, hook] & \end{tikzcd}$$

Since the localisation with respect to z of the latter is an isomorphism, the localisation with respect to z of the injection $\iota^{N_0} \hookrightarrow \pi^{N_0}$ is surjective, thus it is an isomorphism (as it is also injective by exactness of localisation). Therefore the localisation with respect to z of the morphism $\mathcal{C}_\mathrm{c}^\infty(N, \sigma)^{N_0} \to \iota^{N_0}$ is an isomorphism.

Since $\mathcal{C}_\mathrm{c}^\infty(N, \sigma) \cong \bigoplus_{n \in N/N_0} \mathcal{C}^\infty(nN_0, \sigma)$ as a smooth R-representation of N_0, it is N_0-acyclic (see [Neukirch et al. 2008, § I.3]). Thus the long exact sequence of N_0-cohomology induced by (8) yields an exact sequence of smooth R-representations of M^+,

$$0 \to \kappa^{N_0} \to \mathcal{C}_\mathrm{c}^\infty(N, \sigma)^{N_0} \to \iota^{N_0} \to \mathrm{H}^1(N_0, \kappa) \to 0, \tag{10}$$

and an isomorphism of smooth R-representations of M^+,

$$\mathrm{H}^k(N_0, \iota) \xrightarrow{\sim} \mathrm{H}^{k+1}(N_0, \kappa), \tag{11}$$

for all $k \geq 1$. Since the localisation with respect to z of the third arrow of (10) is an isomorphism, the Hecke action of z on κ^{N_0} is locally nilpotent. Thus the Hecke action of z on $\mathrm{H}^k(N_0, \kappa)$ is locally nilpotent for all $k \geq 0$ by Lemma 3. Using (11), we deduce that the Hecke action of z on $\mathrm{H}^k(N_0, \iota)$ is locally nilpotent for all $k \geq 1$.

Taking the N_0-cohomology of (9) yields a long exact sequence of smooth R-representations of M^+,

$$0 \to \iota^{N_0} \to \pi^{N_0} \to (\pi/\iota)^{N_0} \to \mathrm{H}^1(N_0, \iota) \to \cdots . \tag{12}$$

Since the localisation with respect to z of the second arrow is an isomorphism and the Hecke action of z on $\mathrm{H}^1(N_0, \iota)$ is locally nilpotent, the Hecke action of z on $(\pi/\iota)^{N_0}$ is locally nilpotent. Thus the Hecke action of z on $\mathrm{H}^k(N_0, \pi/\iota)$ is locally nilpotent for all $k \geq 0$ by Lemma 3. Using (12) and the fact that the Hecke action of z on $\mathrm{H}^k(N_0, \iota)$ is locally nilpotent for all $k \geq 1$, we conclude that the Hecke action of z on $\mathrm{H}^k(N_0, \pi)$ is locally nilpotent for all $k \geq 1$. □

Proof of Theorem 1. Assume R artinian, p nilpotent in R, and $\mathrm{char}(F) = p$. Let

$$0 \to \pi_1 \to \pi_2 \to \pi_3 \to 0 \tag{13}$$

be a short exact sequence of admissible R-representations of G. Taking the N_0-invariants yields an exact sequence of smooth R-representations of M^+,

$$0 \to \pi_1^{N_0} \to \pi_2^{N_0} \to \pi_3^{N_0} \to \mathrm{H}^1(N_0, \pi_1). \tag{14}$$

The representations $\pi_1^{N_0}, \pi_2^{N_0}, \pi_3^{N_0}$ are locally Z_M^+-finite (cf. [Emerton 2010b, Theorem 3.4.7(1)], whose proof in degree 0 also works when $\mathrm{char}(F) = p$ and over any noetherian ring) and the Hecke action of z on $\mathrm{H}^1(N_0, \pi_1)$ is locally nilpotent by Lemma 4. Therefore, using (5), the localisation with respect to z of (14) is the short sequence of admissible R-representations of M

$$0 \to \mathrm{Ord}_P(\pi_1) \to \mathrm{Ord}_P(\pi_2) \to \mathrm{Ord}_P(\pi_3) \to 0$$

induced by applying the functor Ord_P to (13), and it is exact by exactness of localisation. □

2.3. ***Results on extensions.*** We assume R noetherian. The R-linear category $\mathrm{Mod}_G^{\mathrm{adm}}(R)$ is not abelian in general, but merely exact in the sense of Quillen [1973]. An exact sequence of admissible R-representations of G is an exact sequence of smooth R-representations of G,

$$\cdots \to \pi_{n-1} \to \pi_n \to \pi_{n+1} \to \cdots,$$

such that the kernel and the cokernel of every arrow are admissible. In particular, each term of the sequence is also admissible.

For $n \geq 0$ and π, π' two admissible R-representations of G, we let $\mathrm{Ext}_G^n(\pi', \pi)$ denote the R-module of n-fold Yoneda extensions [1960] of π' by π in $\mathrm{Mod}_G^{\mathrm{adm}}(R)$, defined as equivalence classes of exact sequences,

$$0 \to \pi \to \pi_1 \to \cdots \to \pi_n \to \pi' \to 0.$$

We let $D(G)$ denote the derived category of $\mathrm{Mod}_G^{\mathrm{adm}}(R)$ [Neeman 1990; Keller 1996; Bühler 2010]. The results of [Verdier 1996, § III.3.2] on the Yoneda construction carry over to this setting (see, e.g., [Positselski 2011, Proposition A.13]), hence a natural R-linear isomorphism,

$$\mathrm{Ext}^n_G(\pi', \pi) \cong \mathrm{Hom}_{D(G)}(\pi', \pi[n]).$$

Proof of Corollary 2. Since $\mathrm{Ind}_{\overline{P}}^G$ and Ord_P are exact adjoint functors between $\mathrm{Mod}_M^{\mathrm{adm}}(R)$ and $\mathrm{Mod}_G^{\mathrm{adm}}(R)$ by Theorem 1, they induce adjoint functors between $D(M)$ and $D(G)$, hence natural R-linear isomorphisms,

$$\begin{aligned}\mathrm{Ext}^n_M(\sigma, \mathrm{Ord}_P(\pi)) &\cong \mathrm{Hom}_{D(M)}(\sigma, \mathrm{Ord}_P(\pi)[n]) \\ &\cong \mathrm{Hom}_{D(G)}\big(\mathrm{Ind}_{\overline{P}}^G(\sigma), \pi[n]\big) \\ &\cong \mathrm{Ext}^n_G\big(\mathrm{Ind}_{\overline{P}}^G(\sigma), \pi\big),\end{aligned}$$

for all $n \geq 0$. □

Remark. We give a more explicit proof of Corollary 2. The exact functor $\mathrm{Ind}_{\overline{P}}^G$ and the counit of the adjunction between $\mathrm{Ind}_{\overline{P}}^G$ and Ord_P induce an R-linear morphism,

$$\mathrm{Ext}^n_M(\sigma, \mathrm{Ord}_P(\pi)) \to \mathrm{Ext}^n_G\big(\mathrm{Ind}_{\overline{P}}^G(\sigma), \pi\big). \tag{15}$$

In the other direction, the exact (by Theorem 1) functor Ord_P and the unit of the adjunction between $\mathrm{Ind}_{\overline{P}}^G$ and Ord_P induce an R-linear morphism,

$$\mathrm{Ext}^n_G\big(\mathrm{Ind}_{\overline{P}}^G(\sigma), \pi\big) \to \mathrm{Ext}^n_M(\sigma, \mathrm{Ord}_P(\pi)). \tag{16}$$

When $n = 0$, (16) is the inverse of (15) by the so-called “unit-counit equations”. Assume $n \geq 1$ and let

$$0 \to \mathrm{Ord}_P(\pi) \to \sigma_1 \to \cdots \to \sigma_n \to \sigma \to 0 \tag{17}$$

be an exact sequence of admissible R-representations of M. By [Yoneda 1960, § 3], the image of the class of (17) under (15) is the class of any exact sequence of admissible R-representations of G

$$0 \to \pi \to \pi_1 \to \cdots \to \pi_n \to \mathrm{Ind}_{\overline{P}}^G(\sigma) \to 0 \tag{18}$$

such that there exists a commutative diagram of admissible R-representations of G in which the upper row is obtained from (17) by applying the exact functor $\mathrm{Ind}_{\overline{P}}^G$, the lower row is (18), and the leftmost vertical arrow is the natural morphism induced by the counit of the adjunction between $\mathrm{Ind}_{\overline{P}}^G$ and Ord_P:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ind}_{\overline{P}}^G(\mathrm{Ord}_P(\pi)) \arrow[r] \arrow[d] & \mathrm{Ind}_{\overline{P}}^G(\sigma_1) \arrow[r] \arrow[d] & \cdots \arrow[r] & \mathrm{Ind}_{\overline{P}}^G(\sigma_n) \arrow[r] \arrow[d] & \mathrm{Ind}_{\overline{P}}^G(\sigma) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \pi \arrow[r] & \pi_1 \arrow[r] & \cdots \arrow[r] & \pi_n \arrow[r] & \mathrm{Ind}_{\overline{P}}^G(\sigma) \arrow[r] & 0
\end{tikzcd}$$

Applying the exact functor Ord_P to the diagram and using the unit of the adjunction between $\mathrm{Ind}_{\overline{P}}^G$ and Ord_P yields a commutative diagram of admissible

R-representations of M in which the lower row is obtained from (18) by applying the exact functor Ord_P, the upper row is (17), and the rightmost vertical arrow is the natural morphism induced by the unit of the adjunction between $\mathrm{Ind}_{\overline{P}}^G$ and Ord_P:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ord}_P(\pi) \arrow[r] \arrow[d, equal] & \sigma_1 \arrow[r] \arrow[d] & \cdots \arrow[r] & \sigma_n \arrow[r] \arrow[d] & \sigma \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Ord}_P(\pi) \arrow[r] & \mathrm{Ord}_P(\pi_1) \arrow[r] & \cdots \arrow[r] & \mathrm{Ord}_P(\pi_n) \arrow[r] & \mathrm{Ord}_P(\mathrm{Ind}_{\overline{P}}^G(\sigma)) \arrow[r] & 0
\end{tikzcd}$$

The leftmost vertical arrow is the identity by one of the unit-counit equations. Thus the image of the class of (18) under (16) is the class of (17) by [Yoneda 1960, § 3]. We have proved that (16) is a left inverse of (15). The proof that it is a right inverse is dual.

Corollary 5. *Assume R artinian, p nilpotent in R, and* $\mathrm{char}(F) = p$. *Let σ and σ' be two admissible R-representations of M. The functor* $\mathrm{Ind}_{\overline{P}}^G$ *induces an R-linear isomorphism*

$$\mathrm{Ext}^n_M(\sigma', \sigma) \xrightarrow{\sim} \mathrm{Ext}^n_G\big(\mathrm{Ind}_{\overline{P}}^G(\sigma'), \mathrm{Ind}_{\overline{P}}^G(\sigma)\big)$$

for all $n \geq 0$.

Proof. The isomorphism in the statement is the composite

$$\mathrm{Ext}^n_M(\sigma', \sigma) \xrightarrow{\sim} \mathrm{Ext}^n_M\big(\sigma', \mathrm{Ord}_P\big(\mathrm{Ind}_{\overline{P}}^G(\sigma)\big)\big) \xrightarrow{\sim} \mathrm{Ext}^n_G\big(\mathrm{Ind}_{\overline{P}}^G(\sigma'), \mathrm{Ind}_{\overline{P}}^G(\sigma)\big),$$

where the first isomorphism is induced by the unit of the adjunction between $\mathrm{Ind}_{\overline{P}}^G$ and Ord_P, which is an isomorphism, and the second one is the isomorphism of Corollary 2 with σ' and $\mathrm{Ind}_{\overline{P}}^G(\sigma)$ instead of σ and π respectively. □

We fix a minimal parabolic subgroup $\boldsymbol{B} \subseteq \boldsymbol{G}$, a maximal split torus $\boldsymbol{S} \subseteq \boldsymbol{B}$, and we write Δ for the set of simple roots of $\boldsymbol{S}$ in $\boldsymbol{B}$. We say that a parabolic subgroup $\boldsymbol{P} = \boldsymbol{M}\boldsymbol{N}$ of $\boldsymbol{G}$ is *standard* if $\boldsymbol{B} \subseteq \boldsymbol{P}$ and $\boldsymbol{S} \subseteq \boldsymbol{M}$. In this case, we write $\Delta_{\boldsymbol{P}}$ for the corresponding subset of Δ, and given $\alpha \in \Delta_{\boldsymbol{P}}$ (resp. $\alpha \in \Delta \setminus \Delta_{\boldsymbol{P}}$) we write $\boldsymbol{P}^\alpha = \boldsymbol{M}^\alpha \boldsymbol{N}^\alpha$ (resp. $\boldsymbol{P}_\alpha = \boldsymbol{M}_\alpha \boldsymbol{N}_\alpha$) for the standard parabolic subgroup corresponding to $\Delta_{\boldsymbol{P}} \setminus \{\alpha\}$ (resp. $\Delta_{\boldsymbol{P}} \sqcup \{\alpha\}$).

Let C be an algebraically closed field of characteristic p. Given a standard parabolic subgroup $P = MN$ and a smooth C-representation σ of M, there exists a largest standard parabolic subgroup, $P(\sigma) = M(\sigma)N(\sigma)$, such that the inflation of σ to P extends to a smooth C-representation ${}^{\mathrm{e}}\sigma$ of $P(\sigma)$, and this extension is unique [Abe et al. 2017a, II.7 Corollary 1]. We say that a smooth C-representation of G is *supercuspidal* if it is irreducible, admissible, and does not appear as a subquotient of $\mathrm{Ind}_P^G(\sigma)$ for any proper parabolic subgroup $P = MN$ of G and any irreducible admissible C-representation σ of M. A *supercuspidal standard* $C[G]$*-triple* is a triple (P, σ, Q) where $P = MN$ is a standard parabolic subgroup,

σ is a supercuspidal C-representation of M, and Q is a parabolic subgroup of G such that $P \subseteq Q \subseteq P(\sigma)$. Attached to such a triple in [Abe et al. 2017a] is a smooth C-representation of G,

$$\mathrm{I}_G(P, \sigma, Q) := \mathrm{Ind}_{P(\sigma)}^G\big({}^{\mathrm{e}}\sigma \otimes \mathrm{St}_Q^{P(\sigma)}\big),$$

where

$$\mathrm{St}_Q^{P(\sigma)} := \mathrm{Ind}_Q^{P(\sigma)}(1) \Big/ \sum_{Q \subsetneq Q' \subseteq P(\sigma)} \mathrm{Ind}_{Q'}^{P(\sigma)}(1)$$

(here 1 denotes the trivial C-representation) is the inflation to $P(\sigma)$ of the generalised Steinberg representation of $M(\sigma)$ with respect to $M(\sigma) \cap Q$ [Grosse-Klönne 2014; Ly 2015]. It is irreducible and admissible [Abe et al. 2017a, I.3 Theorem 1].

Proposition 6. *Assume* $\mathrm{char}(F) = p$. *Let* (P, σ, Q) *and* (P', σ', Q') *be two supercuspidal standard* $C[G]$*-triples. If* $Q \not\subseteq Q'$, *then the* C*-vector space*

$$\mathrm{Ext}_G^1(\mathrm{I}_G(P', \sigma', Q'), \mathrm{I}_G(P, \sigma, Q))$$

is nonzero if and only if $P' = P$, $\sigma' \cong \sigma$, *and* $Q' = Q^\alpha$ *for some* $\alpha \in \Delta_Q$, *in which case it is one-dimensional and the unique* (*up to isomorphism*) *nonsplit extension of* $\mathrm{I}_G(P', \sigma', Q')$ *by* $\mathrm{I}_G(P, \sigma, Q)$ *is the admissible* C*-representation of* G

$$\mathrm{Ind}_{P(\sigma)^\alpha}^G(\mathrm{I}_{M(\sigma)^\alpha}(M(\sigma)^\alpha \cap P, \sigma, M(\sigma)^\alpha \cap Q)).$$

Proof. There is a natural short exact sequence of admissible C-representations of G,

$$0 \to \sum_{Q' \subsetneq Q'' \subseteq P(\sigma')} \mathrm{Ind}_{Q''}^G(\sigma') \to \mathrm{Ind}_{Q'}^G(\sigma') \to \mathrm{I}_G(P', \sigma', Q') \to 0. \tag{19}$$

Note that we can restrict the sum to those Q'' that are minimal, i.e., of the form Q'_α for some $\alpha \in \Delta_{P(\sigma')} \setminus \Delta_{Q'}$. Moreover, we deduce from [Abe et al. 2017b, Theorem 3.2] that its cosocle is isomorphic to $\bigoplus_{\alpha \in \Delta_{P(\sigma')} \setminus \Delta_{Q'}} \mathrm{I}_G(P', \sigma', Q'_\alpha)$. Now if $Q \not\subseteq Q'$, then $\mathrm{Ord}_{\overline{Q}'}(\mathrm{I}_G(P, \sigma, Q)) = 0$ by [Abe et al. 2017b, Theorem 1.1(ii) and Corollary 4.13] so that, using Corollary 2, we see that the long exact sequence of Yoneda extensions obtained by applying the functor $\mathrm{Hom}_G(-, \mathrm{I}_G(P, \sigma, Q))$ to (19) yields a natural C-linear isomorphism,

$$\mathrm{Ext}_G^{n-1}\Bigg(\sum_{Q' \subsetneq Q'' \subseteq P(\sigma')} \mathrm{Ind}_{Q''}^G(\sigma'), \mathrm{I}_G(P, \sigma, Q)\Bigg) \xrightarrow{\sim} \mathrm{Ext}_G^n(\mathrm{I}_G(P', \sigma', Q'), \mathrm{I}_G(P, \sigma, Q)),$$

for all $n \geq 1$. In particular, with $n = 1$ and using the identification of the cosocle of the sum and [Abe et al. 2017a, I.3 Theorem 2], we deduce that the C-vector space in the statement is nonzero if and only if $P' = P$, $\sigma' \cong \sigma$, and $Q = Q'_\alpha$ for some $\alpha \in \Delta_{P(\sigma')} \setminus \Delta_{Q'}$ (or equivalently $Q' = Q^\alpha$ for some $\alpha \in \Delta_Q$), in which case it is one-dimensional. Finally, using again [Abe et al. 2017b, Theorem 3.2], we see that for all $\alpha \in \Delta_Q$ the admissible C-representation of G in the statement is a nonsplit extension of $\mathrm{I}_G(P, \sigma, Q^\alpha)$ by $\mathrm{I}_G(P, \sigma, Q)$. □

Corollary 7. *Assume* $\mathrm{char}(F) = p$. *Let* π *and* π' *be two irreducible admissible* C*-representations of* G. *If* π *is supercuspidal and* π' *is not the extension to* G *of a supercuspidal representation of a Levi subgroup of* G, *then* $\mathrm{Ext}^1_G(\pi', \pi) = 0$.

Proof. By [Abe et al. 2017a, I.3 Theorem 3], there exist two supercuspidal standard $C[G]$-triples (P, σ, Q) and (P', σ', Q') such that $\pi \cong \mathrm{I}_G(P, \sigma, Q)$ and $\pi' \cong \mathrm{I}_G(P', \sigma', Q')$. The assumptions on π and π' are equivalent to $P = G$ and $Q' \neq G$. In particular, $Q \not\subseteq Q'$ and $P \neq P'$ so that $\mathrm{Ext}^1_G(\pi', \pi) = 0$ by Proposition 6. □

Acknowledgements

The author would like to thank F. Herzig and M.-F. Vignéras for several comments on the first version of this paper.

References

[Abe et al. 2017a] N. Abe, G. Henniart, F. Herzig, and M.-F. Vignéras, "A classification of irreducible admissible mod p representations of p-adic reductive groups", *J. Amer. Math. Soc.* **30**:2 (2017), 495–559. MR Zbl

[Abe et al. 2017b] N. Abe, G. Henniart, and M.-F. Vignéras, "Modulo p representations of reductive p-adic groups: functorial properties", preprint, 2017. To appear in *Trans. Amer. Math. Soc.* arXiv

[Bernstein 1987] J. Bernstein, "Second adjointness for representations of reductive p-adic groups", unpublished, 1987, Available at http://www.math.tau.ac.il/~bernstei.

[Bühler 2010] T. Bühler, "Exact categories", *Expo. Math.* **28**:1 (2010), 1–69. MR Zbl

[Conrad et al. 2015] B. Conrad, O. Gabber, and G. Prasad, *Pseudo-reductive groups*, 2nd ed., New Mathematical Monographs **26**, Cambridge University Press, 2015. MR Zbl

[Dat 2009] J.-F. Dat, "Finitude pour les représentations lisses de groupes p-adiques", *J. Inst. Math. Jussieu* **8**:2 (2009), 261–333. MR Zbl

[Emerton 2010a] M. Emerton, "Ordinary parts of admissible representations of p-adic reductive groups I: Definition and first properties", pp. 355–402 in *p-adic representations of p-adic groups, III: Global and geometrical methods*, edited by L. Berger et al., Astérisque **331**, Société Mathématique de France, 2010. MR Zbl

[Emerton 2010b] M. Emerton, "Ordinary parts of admissible representations of p-adic reductive groups, II: Derived functors", pp. 403–459 in *p-adic representations of p-adic groups, III: Global and geometrical methods*, edited by L. Berger et al., Astérisque **331**, Société Mathématique de France, 2010. MR Zbl

[Grosse-Klönne 2014] E. Grosse-Klönne, "On special representations of p-adic reductive groups", *Duke Math. J.* **163**:12 (2014), 2179–2216. MR Zbl

[Hauseux 2016a] J. Hauseux, "Parabolic induction and extensions", preprint, 2016. To appear in *Algebra and Number Theory*. arXiv

[Hauseux 2016b] J. Hauseux, "Extensions entre séries principales p-adiques et modulo p de $G(F)$", *J. Inst. Math. Jussieu* **15**:2 (2016), 225–270. MR Zbl

[Hauseux 2016c] J. Hauseux, "Sur une conjecture de Breuil–Herzig", *Journal für die reine und angewandte Mathematik* (online publication October 2016).

[Hu 2012] Y. Hu, "Diagrammes canoniques et représentations modulo p de $\mathrm{GL}_2(F)$", *J. Inst. Math. Jussieu* **11**:1 (2012), 67–118. MR Zbl

[Hu 2017] Y. Hu, "An application of a theorem of Emerton to mod p representations of GL_2", *J. London Math. Soc.* **96**:3 (2017), 545–564. Zbl

[Keller 1996] B. Keller, "Derived categories and their uses", pp. 671–701 in *Handbook of algebra, Vol. 1*, edited by M. Hazewinkel, Elsevier, Amsterdam, 1996. MR Zbl

[Ly 2015] T. Ly, "Représentations de Steinberg modulo p pour un groupe réductif sur un corps local", *Pacific J. Math.* **277**:2 (2015), 425–462. MR Zbl

[Neeman 1990] A. Neeman, "The derived category of an exact category", *J. Algebra* **135**:2 (1990), 388–394. MR Zbl

[Neukirch et al. 2008] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften **323**, Springer, 2008. MR Zbl

[Positselski 2011] L. Positselski, "Mixed Artin–Tate motives with finite coefficients", *Mosc. Math. J.* **11**:2 (2011), 317–402, 407–408. MR Zbl

[Quillen 1973] D. Quillen, "Higher algebraic K-theory, I", pp. 85–147 in *Algebraic K-theory, I: Higher K-theories*, edited by H. Bass, Lecture Notes in Math. **341**, Springer, 1973. MR Zbl

[Verdier 1996] J.-L. Verdier, *Des catégories dérivées des catégories abéliennes*, edited by G. Maltsiniotis, Astérisque **239**, Société Mathématique de France, Paris, 1996. MR Zbl

[Vignéras 1996] M.-F. Vignéras, *Représentations l-modulaires d'un groupe réductif p-adique avec $l \neq p$*, Progress in Mathematics **137**, Birkhäuser, Boston, 1996. MR Zbl

[Vignéras 2016] M.-F. Vignéras, "The right adjoint of the parabolic induction", pp. 405–425 in *Arbeitstagung Bonn 2013*, edited by W. Ballmann et al., Progr. Math. **319**, Springer, 2016. MR Zbl

[Yoneda 1960] N. Yoneda, "On Ext and exact sequences", *J. Fac. Sci. Univ. Tokyo Sect. I* **8** (1960), 507–576. MR Zbl

Received May 8, 2017. Revised August 23, 2017.

JULIEN HAUSEUX
DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ DE LILLE
FRANCE
julien.hauseux@math.univ-lille1.fr

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.31

STABILITY PROPERTIES OF POWERS OF IDEALS IN REGULAR LOCAL RINGS OF SMALL DIMENSION

JÜRGEN HERZOG AND AMIR MAFI

Let $(R, \mathfrak{m})$ be a regular local ring or a polynomial ring over a field, and let I be an ideal of R which we assume to be graded if R is a polynomial ring. Let astab I, $\overline{\text{astab}}\, I$ and dstab I, respectively, be the smallest integers n for which $\operatorname{Ass} I^n$, $\operatorname{Ass} \bar{I}^n$ and depth I^n stabilize. Here $\bar{I}^n$ denotes the integral closure of I^n.

We show that astab $I = \overline{\text{astab}}\, I =$ dstab I if $\dim R \leq 2$, while already in dimension three, astab I and $\overline{\text{astab}}\, I$ may differ by any amount. Moreover, we show that if $\dim R = 4$, there exist ideals I and J such that for any positive integer c one has astab $I -$ dstab $I \geq c$ and dstab $J -$ astab $J \geq c$.

Introduction

Let $(R, \mathfrak{m})$ be a commutative Noetherian ring and I be an ideal of R. Brodmann [1979a] proved that the set of associated prime ideals $\operatorname{Ass} I^k$ stabilizes. In other words, there exists an integer k_0 such that $\operatorname{Ass} I^k = \operatorname{Ass} I^{k_0}$ for all $k \geq k_0$. The smallest such integer k_0 is called the *index of Ass-stability* of I, and denoted by astab I. Moreover, $\operatorname{Ass} I^{k_0}$ is called the *stable set of associated prime ideals* of I. It is denoted by $\operatorname{Ass}^\infty I$. For the integral closures $\overline{I^k}$ of the powers of I, McAdam and Eakin [1979] showed that $\operatorname{Ass} \overline{I^k}$ stabilizes as well. We denote the index of stability for the integral closures of the powers of I by $\overline{\text{astab}}\, I$, and denote its stable set of associated prime ideals by $\overline{\operatorname{Ass}}^\infty I$.

Brodmann [1979b] also showed that depth R/I^k stabilizes. The smallest power of I for which depth stabilizes is denoted by dstab I. This stable depth is called the *limit depth* of I, and is denoted by $\lim_{k\to\infty} \operatorname{depth} R/I^k$. These indices of stability have been studied and compared to some extent in [Herzog and Qureshi 2015; Herzog et al. 2013]. The purpose of this work is to compare once again these stability indices. The main result is that if $(R, \mathfrak{m})$ is a regular local ring with $\dim R \leq 2$, then all 3 stability indices are equal, but if $\dim R = 3$, then we still have astab $I =$ dstab I, while astab I and $\overline{\text{astab}}\, I$ may differ by any amount. On the other hand, if $\dim R \geq 4$, we will show by examples that in general a comparison

MSC2010: 13A15, 13A30, 13C15.
Keywords: associated primes, depth stability number.

between these stability indices is no longer possible. In other words, any inequality between these invariants may occur.

Quite often, but not always, depth R/I^k is a nonincreasing function on n. In the last section we prove that if $(R, \mathfrak{m})$ is a 3-dimensional regular local ring and I satisfies $I^{k+1} : I = I^k$ for all k, then depth R/I^k is nonincreasing. For any unexplained notion or terminology, we refer the reader to [Bruns and Herzog 1993].

Several explicit examples were performed with help of the computer algebra systems [CoCoA] and [Macaulay2], as well as with the program in [Bayati et al. 2011] which allows one to compute $\operatorname{Ass}^\infty I$ of a monomial ideal I.

1. The case dim $R \leq 3$

In this section we study the behavior of the stability indices for regular rings of dimension ≤ 3. In the proofs we will use the following elementary and well known fact: let $I \subset R$ be an ideal of height 1 in the regular local ring R. Then there exists $f \in R$ such that $I = fJ$ where either $J = R$ or otherwise $\operatorname{height}(J) > 1$. Indeed, let $I = (f_1, \ldots, f_m)$. Since R is factorial, the greatest common divisor of $f_1, \ldots, f_m$ exists. Let $f = \gcd(f_1, \ldots, f_m)$, and $g_i = f_i/f$ for $i = 1, \ldots, m$. Then $I = fJ$, where $J = (g_1, \ldots, g_m)$. Suppose $\operatorname{height}(J) = 1$; then there exists a prime ideal P of height 1 with $J \subset P$. Since R is regular, P is a principal ideal, say $P = (g)$. It follows then that g divides all g_i, but $\gcd(g_1, \ldots, g_m) = 1$, a contradiction.

Remark 1.1. Let $(R, \mathfrak{m})$ be a regular local ring with $\dim R \leq 2$ and let I be an ideal of R. Then

$$\operatorname{astab} I = \overline{\operatorname{astab}}\, I = \operatorname{dstab} I = 1.$$

Proof. If $\dim R \leq 1$, then either R is a field or a principal ideal domain, and the statement is trivial. Now suppose $\dim R = 2$ that and $I \neq 0$. If $\operatorname{height}(I) = 2$, then $\mathfrak{m}$ belongs to $\operatorname{Ass} I^k$ and $\operatorname{Ass} \overline{I^k}$ for all k, and the assertion is trivial. Hence, we may assume that $\operatorname{height}(I) = 1$. Then $I = fJ$ with $J = R$ or $\operatorname{height}(J) = 2$. In the first case I is a principal ideal, and the assertion is trivial. In the second case, $I^k = f^k J^k$ for all k, and J^k is $\mathfrak{m}$-primary. Thus there exists $g \notin J^k$ with $g\mathfrak{m} \in J^k$. Then $gf^k \notin f^k J^k$ and $gf^k\mathfrak{m} \in f^k J^k$. This shows that in the second case $\mathfrak{m} \in \operatorname{Ass} I^k$ for k, so that $\operatorname{astab} I = \operatorname{dstab} I = 1$.

Finally observe that in the second case, $\overline{I^k} = f^k \overline{J^k}$ for all k. This shows that $\mathfrak{m} \in \operatorname{Ass} \overline{I^k}$ for all k, so that also in this case $\overline{\operatorname{astab}}\, I = 1$. $\square$

Theorem 1.2. *Let $(R, \mathfrak{m})$ be a regular local ring with $\dim R \leq 3$ and I be an ideal of R. Then $\operatorname{astab} I = \operatorname{dstab} I$.*

Proof. By Remark 1.1, we may assume that $\dim R = 3$. If $\operatorname{height}(I) \geq 2$, then $\operatorname{Ass} I^k \subseteq \operatorname{Min}(I) \cup \{\mathfrak{m}\}$ for all k. This implies at once that $\operatorname{astab} I = \operatorname{dstab} I$. Now suppose that $\operatorname{height}(I) = 1$. If I is a principal ideal, then the assertion is again trivial. Otherwise, $I = fJ$ with $\operatorname{height}(J) \geq 2$. Since I^k is isomorphic to J^k as an R-module, it follows that $\operatorname{proj\,dim} I^k = \operatorname{proj\,dim} J^k$ for all k. This implies that $\operatorname{proj\,dim} R/I^k = \operatorname{proj\,dim} R/J^k$ for all k, and consequently $\operatorname{depth} R/I^k = \operatorname{depth} R/J^k$, by the Auslander–Buchsbaum formula. Thus, $\operatorname{dstab} I = \operatorname{dstab} J$.

We claim that $\operatorname{astab} I = \operatorname{astab} J$. Since we have already seen that $\operatorname{astab} J = \operatorname{dstab} J$ if $\operatorname{height}(J) \geq 2$, the claim then implies that $\operatorname{astab} I = \operatorname{dstab} I$, as desired.

The claim follows once we have that shown

$$\operatorname{Ass} I^k = \operatorname{Ass} f^k J^k = \operatorname{Min}(f) \cup \operatorname{Ass} J^k.$$

For that we only need to prove the second equation. So let $P \in \operatorname{Spec} R$ with $f^k J^k \subset P$. Then $P \in \operatorname{Ass} f^k J^k$ if and only if $R_P/f^k J^k R_P$ has depth 0. If $J \not\subset P$, then $f^k J^k R_P = f^k R_P$, and hence $\operatorname{depth} R_P/f^k J^k R_P = 0$ if and only if $\operatorname{depth} R_P/f^k R_P = 0$, and this is the case if and only if $P \in \operatorname{Min}(f)$. If $J \subset P$, then the R_P-modules $f^k J^k R_P$ and $J^k R_P$ are isomorphic, so that with the arguments as above $\operatorname{depth} R_P/f^k J^k R_P = \operatorname{depth} R_P/J^k R_P$, which shows that in this case $P \in \operatorname{Ass} f^k J^k$ if and only if $P \in \operatorname{Ass} J^k$. This completes the proof. □

The statements shown so far and its proofs made for ideals in a regular local ring are valid as well for any graded ideal in a polynomial ring.

We now turn to some explicit examples. Hibi et al. [2016, Proposition 1.5] show that for any integer $t \geq 2$ the ideal $I = (x^t, xy^{t-2}z, y^{t-1}z) \subset K[x, y, z]$ satisfies $\operatorname{dstab} I = t$. Since by Theorem 1.2, $\operatorname{astab} I = \operatorname{dstab} I$, this example shows that in a 3-dimensional graded or local ring (we may pass to $K[|x, y, z|]$) both the index of depth stability as well as the index of Ass-stability may be any given number.

The following example shows that already for an ideal I in a 3-dimensional polynomial ring the invariants $\operatorname{astab} I$ and $\overline{\operatorname{astab}}\, I$ may differ.

Example 1.3. Let $R = K[x, y, z]$ be a polynomial ring over a field K and let $I = ((xy)^2, (xz)^2, (yz)^2) \subset R$. Then $\operatorname{astab} I = 2$ and $\overline{\operatorname{astab}}\, I = 1$.

Proof. We first claim that $I^n : (xy)^2 = I^{n-1} + z^{2n}(x^2, y^2)^{n-2}$. Indeed, let $J = ((xz)^2, (yz)^2)$. Then $I^n = J^n + (xy)^2 I^{n-1}$, and hence $I^n : (xy)^2 = J^n : (xy)^2 + I^{n-1}$. Since $J^n : (xy)^2 = z^{2n}(x^2, y^2)^n : (xy)^2 = z^{2n}(x^2, y^2)^{n-2}$, the assertion follows.

By symmetry, we also have $I^n : (xz)^2 = I^{n-1} + y^{2n}(x^2, z^2)^{n-2}$ and $I^n : (yz)^2 = I^{n-1} + x^{2n}(y^2, z^2)^{n-2}$. Thus, for all $n \geq 1$ we obtain

$$\begin{aligned} I^n : I &= (I^n : (xy)^2) \cap (I^n : (xz)^2) \cap (I^n : (yz)^2) \\ &= (I^{n-1} + z^{2n}(x^2, y^2)^{n-2}) \cap (I^{n-1} + y^{2n}(x^2, z^2)^{n-2}) \cap (I^{n-1} + x^{2n}(y^2, z^2)^{n-2}) \\ &= I^{n-1} + (z^{2n}(x^2, y^2)^{n-2}) \cap (y^{2n}(x^2, z^2)^{n-2}) \cap (x^{2n}(y^2, z^2)^{n-2}) = I^{n-1}. \end{aligned}$$

In other words, I satisfies strong persistence in the sense of [Herzog and Qureshi 2015]. In particular, $\operatorname{Ass} I^n \subset \operatorname{Ass} I^{n+1}$ for all $n \geq 1$. Now since $\operatorname{Ass} I =$

$\{(x, y), (x, z), (y, z)\}$ and $\operatorname{Ass} I^2 = \{(x, y), (x, z), (y, z), (x, y, z)\}$, we deduce from this that $\operatorname{astab} I = \operatorname{dstab} I = 2$.

With Macaulay2 one checks that $\bar{I} = \big((xy)^2, (xz)^2, (yz)^2, xyz^2, xy^2z, x^2yz\big)$ and that $\operatorname{Ass} \bar{I} = \{(x, y), (x, z), (y, z), (x, y, z)\}$. By [McAdam 1983, Corollary 11.28], one has $\operatorname{Ass} \bar{I} \subset \operatorname{Ass} \overline{I^2} \subset \cdots \subset \overline{\operatorname{Ass}}^{\infty} I$. Since $\operatorname{Ass} \overline{I^n}$ is a subset of the monomial prime ideals containing I, and since this set is $\{(x, y), (x, z), (y, z), (x, y, z)\}$, we see that $\operatorname{Ass} \bar{I} = \operatorname{Ass} \overline{I^n}$ for all n. Hence, $\overline{\operatorname{astab}}\, I = 1$. $\square$

The difference $\operatorname{astab} I - \overline{\operatorname{astab}}\, I$ may in fact be as big as we want:

Theorem 1.4. *Let $R = k[x, y, z]$ be the polynomial ring over a field K, c be a positive integer and $I = (x^{2c+2}, xy^{2c}z, y^{2c+2}z)$. Then* $\operatorname{astab} I = c+2$ *and* $\overline{\operatorname{astab}}\, I = 2$.

Proof. Note that $I = (x^{2c+2}, z) \cap (x, y^{2c+2}) \cap (y^{2c}, x^{2c+2})$, from which it follows that $\dim R/I = \operatorname{depth} R/I = 1$.

In the next step we prove that $I^n : I = I^{n-1}$ for all n. Then [Herzog and Qureshi 2015, Theorem 1.3] implies that $\operatorname{Ass} I^n \subseteq \operatorname{Ass} I^{n+1}$ for all n. In particular, if $\operatorname{depth} R/I^k = 0$ for some k, then $\operatorname{depth} R/I^r = 0$ for all $r \geq 0$. Since $\operatorname{depth} R/I^k \leq 1$ for all k, it then follows that $\operatorname{depth} R/I^k \geq \operatorname{depth} R/I^{k+1}$ for all k.

In order to show that $I^n : I = I^{n-1}$, observe that

$$I^n : x^{2c+2} = I^{n-1} + ((y^{2c}z)^n (x, y^2)^n : x^{2c+2}) = I^{n-1} + (y^{2c}z)^n (x, y^2)^{n-2(c+1)},$$

and that

$$\begin{aligned} I^n : xy^{2c}z &= I^{n-1} + ((x^{2c+2}, y^{2c+2}z)^n : xy^{2c}z) \\ &\subseteq I^{n-1} + (((x^{2c+2}, y^{2c+2}z)^n : y^{2c+2}z) : x^{2c+2}) \\ &= I^{n-1} + (x^{2c+2}, y^{2c+2}z)^{n-2}. \end{aligned}$$

Similarly we have

$$\begin{aligned} I^n : y^{2c+2}z &= I^{n-1} + (x^n (x^{2c+1}, y^{2c}z)^n : y^{2c+2}z) \\ &\subseteq I^{n-1} + (x^n (x^{2c+1}, y^{2c}z)^n : y^{4c}z^2) \\ &= I^{n-1} + x^n (x^{2c+1}, y^{2c}z)^{n-2}. \end{aligned}$$

Now since

$$\begin{aligned} I^{n-1} &\subseteq (I^n : I) \\ &\subseteq I^{n-1} + (y^{2c}z)^n (x, y^2)^{n-2(c+1)} \cap (x^{2c+2}, y^{2c+2}z)^{n-2} \cap x^n (x^{2n+1}, y^{2c}z)^{n-2} \\ &\subseteq I^{n-1} + I^n = I^{n-1}, \end{aligned}$$

it follows that $I^n : I = I^{n-1}$ for all n, as desired.

Next we claim that $I^n : x^{2c+2} = I^{n-1}$ for all $n \leq c+1$.

If $n = 1$, there is nothing to prove. Let $1 < n \leq c + 1$. By a calculation as before we see that

$$\begin{aligned} I^n : x^{2c+2} &= I^{n-1} + ((y^{2c}z)^n(x, y^2)^n : x^{2c+2}) = I^{n-1} + (y^{2c}z)^n \\ &= I^{n-1} + (y^{(2c+2)(n-1)+2c+2-2n}z^n) = I^{n-1} + (y^{2c+2}z)^{n-1}y^{2c+2-2n}z \\ &= I^{n-1}. \end{aligned}$$

We proceed by induction on n to show that depth $S/I^n = 1$ for $n \leq c + 1$. We observed already that depth $S/I = 1$, Now let $1 < n \leq c + 1$. Then, since $I^n : x^{2c+2} = I^{n-1}$, we obtain the exact sequence

$$0 \to R/I^{n-1} \xrightarrow{x^{2c+2}} R/I^n \to R/(I^n, x^{2c+2}) \to 0.$$

Since by the induction hypothesis depth $R/I^{n-1} = 1$, it follows that

$$\begin{aligned} \operatorname{depth} R/I^n &\geq \min\{\operatorname{depth} R/I^{n-1}, \operatorname{depth} R/(I^n, x^{2c+2})\} \\ &= \min\{1, \operatorname{depth} R/(I^n, x^{2c+2})\}. \end{aligned}$$

Note that $(I^n, x^{2c+2}) = ((y^{2c}z(x, y^2)^n, x^{2c+2})$, which implies that $R/(I^n, x^{2c+2}$ has depth 1. Thus we have depth $R/I^n \geq 1$. On the other hand, we have seen before that depth $R/I^n \leq$ depth $R/I = 1$, and so depth $R/I^n = 1$ for all $n \leq c + 1$.

In the next step we show that depth $R/I^{c+2} = 0$, which then implies that depth $R/I^n = 0$ for all $n \geq c + 2$. In particular, it follows that astab $I = c + 2$.

In order to prove that depth $R/I^{c+2} = 0$, we show that

$$x^{2c+2}y^{(c+1)(2c+2)-1}z^{c+1} \in (I^{c+2} : \mathfrak{m}) \setminus I^{c+2}.$$

Indeed, let $u = x^{2c+2}y^{(c+1)(2c+2)-1}z^{c+1}$. Then

$$\begin{aligned} ux &= x^{2c+2}(xy^{2c}z)(y^{2c+2}z)^c y^{2c}, \\ uy &= x^{2c+2}(y^{2c+2}z)^{c+1} \\ uz &= (xy^{2c}z)^{c+1}(xy^{2c}z)(yx^c). \end{aligned}$$

This shows that $u \in (I^{c+2} : \mathfrak{m})$.

Assume that $x^{2c+2}y^{(c+1)(2c+2)-1}z^{c+1} \in I^{c+2}$. Then

$$y^{(c+1)(2c+2)-1}z^{c+1} \in (I^{c+2} : x^{2c+2}) = I^{c+1} + (y^{2c}z)^{c+2},$$

and so $y^{(c+1)(2c+2)-1}z^{c+1} \in I^{c+1}$. Since $I^{c+1} = (x^{2c+2}, y^{2c}z(x, y^2))^{c+1}$, expansion of this power implies that

$$y^{(c+1)(2c+2)-1} \in \sum_{i=0}^{c+1}(x^{2c+2})^i(y^{2c}(x, y^2))^{c+1-i}.$$

It follows that $y^{(c+1)(2c+2)-1} \in (y^{2c}(x, y^2))^{c+1}$, which is a contradiction.

Now we compute $\overline{\operatorname{astab}}\, I$, and first prove that

$$\bar{I} = (I, (x^3 y^{2c-1} z, x^4 y^{2c-2} z, \ldots, x^{2c+1} yz)).$$

Let $J = (I, (x^3 y^{2c-1} z, x^4 y^{2c-2} z, \ldots, x^{2c+1} yz))$. For all $i \in \mathbb{Z}$ with $3 \le i \le 2c+1$, we have

$$\begin{aligned}(x^i y^{2c-i+2} z)^{2c} &= x^{2ic} y^{2c(2c-i+2)} z^{2c} = x^{2c(i-1)+i-2} x^{2c-i+2} y^{2c(2c-i+2)} z^{2c-i+2} z^{i-2} \\ &= x^{2c(i-1)+i-2} (xy^{2c} z)^{2c-i+2} z^{i-2} \\ &= (x^{2c+2})^{i-2} (xy^{2c} z)^{2c-i+2} z^{i-2} x^{2c+2-i} \in I^{2c}.\end{aligned}$$

Thus $J \subseteq \bar{I}$. We have $\operatorname{Ass} \bar{I}/J \subseteq \operatorname{Ass} J$. The primary decomposition of J shows that $\operatorname{Ass} J = \{(x, z), (x, y)\}$. Let $P = (x, z)$. Then $(\bar{I})_P = \overline{I_P} = \overline{(x^{2c+2}, z)_P} = (x^{2c+2}, z)_P$. The last equality follows by [Huneke and Swanson 2006, Proposition 1.3.5], and so $(\bar{I}/J)_P = 0$. Hence $P \notin \operatorname{Ass} \bar{I}/J$. Now let $P = (x, y)$. Then

$$(\bar{I})_P = \overline{(x^{2c+2}, xy^{2c}, y^{2c+2})_P} \subset \overline{((x, y)^{2c+2}, xy^{2c})_P} = ((x, y)^{2c+2}, xy^{2c})_P = J_P.$$

The second equality follows by [Huneke and Swanson 2006, Exercise 1.19]. Thus we have $(\bar{I}/J)_P = 0$. This shows that $\operatorname{Ass} \bar{I}/J = \varnothing$, and hence $\bar{I} = J$, as desired. In particular, we see that

$$\operatorname{Ass} \bar{I} = \{(x, z), (x, y)\}.$$

Since $\operatorname{Ass} \bar{I} \subseteq \operatorname{Ass} \overline{I^k}$ for all k, it follows that $\{(x, z), (x, y)\} \subset \operatorname{Ass} \overline{I^k}$ for all k. Suppose that $(y, z) \in \operatorname{Ass} \overline{I^k}$ for some k. Then (y, z) is a minimal prime ideal of I. However, this is not the case, as can be seen from the primary decomposition of I.

Next we show that $\mathfrak{m} = (x, y, z)$ belongs to $\operatorname{Ass} \overline{I^2}$. Then it follows that

$$\operatorname{Ass} \overline{I^k} = \{(x, z), (x, y), (x, y, z)\} \quad \text{for all } k \ge 2,$$

thereby showing that $\overline{\operatorname{astab}}\, I = 2$.

In order to prove that $\mathfrak{m} \in \operatorname{Ass} \overline{I^2}$, we first show that the ideal L, which is equal to

$$\big(I^2, (x^4 y^{4c-1} z^2, x^5 y^{4c-2} z^2, \ldots, x^{2c+2} y^{2c+1} z^2), (x^{2c+5} y^{2c-1} z, x^{2c+6} y^{2c-2} z \ldots, x^{4c+3} yz)\big),$$

is contained in $\overline{I^2}$.

Since

$$I^2 = (x^{4c+4}, x^2 y^{4c} z^2, y^{4c+4} z^2, x^{2c+3} y^{2c} z, x^{2c+2} y^{2c+2} z, xy^{4c+2} z^2),$$

it follows that for all integers i with $4 \le i \le 2c+2$ the element

$$\begin{aligned}(x^i y^{4c-i+3} z^2)^{4c} x^{4ic} y^{4c(4c-i+3)} z^{8c} &= x^{2(4c-i+3)} y^{4c(4c-i+3)} z^{2(4c-i+3)} x^{4c(i-2)+2i-6} z^{2i-6} \\ &= (x^2 y^{4c} z^2)^{4c-i+3} (x^{4c+4})^{i-3} x^{4c-2i+6} z^{2i-6}\end{aligned}$$

belongs to $(I^2)^{4c}$. Also, for all integers i with $5 \leq i \leq 2c-2$, the element

$$\begin{aligned}(x^{2c+i}y^{2c+4-i}z)^{4c} &= x^{2(2c+4-i)}y^{4c(2c+4-i)}z^{2(2c+4-i)}x^{8c^2+4ic+2i-4c-8}z^{2i-8}\\ &= (x^2y^{4c}z^2)^{2c+4-i}x^{(4c+4)(2c+i-4)}x^{4c+8-2i}z^{2i-8}\\ &= (x^2y^{4c}z^2)^{2c+4-i}(x^{4c+4})^{2c+i-4}x^{4c+8-2i}z^{2i-8}\end{aligned}$$

belongs to $(I^2)^{4c}$. This shows $L \subseteq \overline{I^2}$.

By using primary decomposition for the ideal L, we see that

$$\operatorname{Ass} L = \{(x, z), (x, y), (x, y, z)\}.$$

On the other hand, by easy calculation, one verifies that $L : (x^{2c+2}y^{2c+1}z) = \mathfrak{m}$. Finally we show that $x^{2c+2}y^{2c+1}z \notin \overline{I^2}$, which then implies that $\mathfrak{m} \in \operatorname{Ass} \overline{I^2}$, as desired.

In order to prove this we show by induction on n that $(x^{2c+2}y^{2c+1}z)^n \notin (I^2)^n$ for all n. For $n = 1$, if $x^{2c+2}y^{2c+1}z \in I^2$, then $y^{2c+1}z \in I^2 : x^{2c+2} = I + (y^{2c}z)^2 = I$, which is a contradiction.

Now let $n > 1$. Assume that $(x^{2c+2}y^{2c+1}z)^{n-1} \notin (I^2)^{n-1}$. using the induction hypothesis. If $(x^{2c+2}y^{2c+1}z)^n \in (I^2)^n$, then

$$x^{(2c+2)(n-1)}(y^{2c+1}z)^n \in (I^{2n} : x^{2c+2}) = I^{2n-1} + (y^{2c}z)^{2n}(x, y^2)^{2n-2(c+1)},$$

and so $x^{(2c+2)(n-1)}(y^{2c+1}z)^n \in I^{2n-1}$.

It follows that $x^{(2c+2)(n-1)}(y^{2c+1}z)^{n-1} \in (I^{2n-1} : y^{2c+1}z)$. Since

$$\begin{aligned}(I^{2n-1} : y^{2c+1}z) &= yI^{2n-2} + ((x^{2c+2}, xy^{2c}z)^{2n-1} : y^{2c+1}z)\\ &= yI^{2n-2} + (x^{2n-1}(x^{2c+1}, y^{2c}z)^{2n-2} : y)\\ &= yI^{2n-2} + x^{2n-1}(y^{2c-1}z(x^{2c+1}, y^{2c}z)^{2n-3} + (x^{2c+1})^{2n-2}),\end{aligned}$$

we see that $x^{(2c+2)(n-1)}(y^{2c+1}z)^{n-1} \in y(I^2)^{n-1}$, a contradiction.

Thus $(x^{2c+2}y^{2c+1}z)^n \notin (I^2)^n$ for all n, as desired. □

The theorem says that for any positive integer c there exists a monomial ideal in $K[x, y, z]$ with $\operatorname{astab} I - \overline{\operatorname{astab}}\, I = c$. However we do not know whether for all ideals in $I \subset K[x, y, z]$ one has $\overline{\operatorname{astab}}\, I \leq \operatorname{astab} I$.

2. The case dim $R > 3$

The purpose of this section is to show that for a polynomial ring S in more than 3 variables, for a graded ideal $I \subset S$ the invariants $\operatorname{astab} I$ and $\operatorname{dstab} I$ may differ by any amount.

We begin with two examples.

Example 2.1. Let $R = k[x, y, z, u]$ be the polynomial ring over a field k and consider the ideal $I = (xy, yz, zu)$ of R. Then $\operatorname{astab} I = 1$ and $\operatorname{dstab} I = 2$.

Proof. We have $\operatorname{Ass} I = \operatorname{Min}(I)$, and since I may be viewed as the edge ideal of a bipartite graph it follows from [Herzog and Hibi 2011, Definition 1.4.5, Corollary 10.3.17] that $\operatorname{Ass} I = \operatorname{Ass} I^n$ for all $n \in \mathbb{N}$. Therefore $\operatorname{astab} I = 1$. By [Herzog and Hibi 2011, Corollary 10.3.18], $\lim_{k\to\infty} \operatorname{depth} R/I^k = 1$. Moreover, it can be seen that $\operatorname{depth} R/I = 2$ and $\operatorname{depth} R/I^2 = 1$. Since I has a linear resolution, [Herzog and Hibi 2011, Theorem 10.2.6] implies that for all $k \geq 1$, I^k has a linear resolution as well. Therefore, by [Herzog et al. 2013, Proposition 2.2] we have $\operatorname{depth} R/I^{k+1} \leq \operatorname{depth} R/I^k$ for all $k \in \mathbb{N}$. Hence $\operatorname{depth} R/I^k = 1$ for all $k \geq 2$, and so $\operatorname{dstab} I = 2$. □

Example 2.2. Let $R = K[x, y, z, u]$ be the polynomial ring in 4 variables over a field K, and let $I = (x^2z, uyz, u^3)$. Then $\operatorname{astab} I = 2$ and $\operatorname{dstab} I = 1$.

Proof. Set $J = (uyz, u^3)$. For all $n \in \mathbb{N}$, it follows that

$$I^n : x^2z = (J^n + x^2zI^{n-1}) : x^2z = I^{n-1} + (J^n : x^2z) = I^{n-1}.$$

Hence, $\operatorname{Ass} I^n \subseteq \operatorname{Ass} I^{n+1}$ for all $n \in \mathbb{N}$. By using Macaulay2 and the program in [Bayati et al. 2011], we see that $\operatorname{Ass}^\infty I = \operatorname{Ass} I^2 = \{(x,u), (z,u), (x, y,u), (x,z,u)\}$. Therefore $\operatorname{astab} I = 2$. As $\operatorname{Ass} I^n \subseteq \operatorname{Ass} I^{n+1}$ for all $n \in \mathbb{N}$, it follows that $\mathfrak{m} = (x, y, z, u) \notin \operatorname{Ass} I^n$ and so we have $\operatorname{depth} R/I^n \geq 1$. Moreover $y - z \in \mathfrak{m}$ is a nonzerodivisor on R/I^n for all $n \in \mathbb{N}$. Set $\overline{R} = R/(y - z)$. Thus by [Bruns and Herzog 1993, Lemma 4.2.16] we have $\overline{R/I^n} = \overline{R}/\overline{I^n} \cong K[x, z, u]/(x^2z, uz^2, u^3)^n$. Since $xzu^{3n-1} \in (\overline{I^n}) : \overline{\mathfrak{m}} \setminus \overline{I^n}$, it follows $\operatorname{depth} \overline{R}/\overline{I^n} = 0$ and so $\operatorname{depth} R/I^n = 1$ for all $n \in \mathbb{N}$. Therefore $\operatorname{dstab} I = 1$. □

Now we come to the main result of this section.

Theorem 2.3. *Let $R = k[x, y, z, u]$ be the polynomial ring over a field k. Then for any nonnegative integer c, there exist two ideals I and J of R such that the following statements hold*:

(i) $\operatorname{astab} I - \operatorname{dstab} I \geq c$.

(ii) $\operatorname{dstab} J - \operatorname{astab} J \geq c$.

Proof. We may assume that c is a positive integer. Let $I = (x^{c+1}z^c, u^{2c-1}yz, u^{2c+1})$ and $J = (x^cy^{c-1}, y^{c-1}x^{c-1}z, z^cu^c)$. We claim that $\operatorname{astab} I = \operatorname{dstab} J = c + 1$ and $\operatorname{astab} J = \operatorname{dstab} I = 1$.

(i) In this case, by using Example 2.2, we can assume that $c \geq 2$. For all $n \in \mathbb{N}$, we have

$$\begin{aligned}(I^n : x^{c+1}z^c) &= (((u^{2c-1}yz, u^{2c+1})^n + x^{c+1}z^cI^{n-1}) : x^{c+1}z^c) \\ &= I^{n-1} + ((u^{2c-1}yz, u^{2c+1})^n : x^{c+1}z^c).\end{aligned}$$

Since $((u^{2c-1}yz, u^{2c+1})^n : x^{c+1}z^c) = ((u^{2c-1}yz, u^{2c+1})^n : z^c) \subseteq I^{n-1}$, it follows that $(I^n : x^{c+1}z^c) = I^{n-1}$ and so $\operatorname{Ass} I^n \subseteq \operatorname{Ass} I^{n+1}$. By using Macaulay2 and [Bayati et al. 2011], we have $\operatorname{Ass} I = \{(x,u), (z,u), (y,z,u), (x,y,u)\}$ and $\operatorname{Ass}^\infty I = \{(x,u), (z,u), (y,z,u), (x,z,u), (x,y,u)\}$. Set $\mathfrak{p} = (x,z,u)$. It is easily seen that $I^i : \mathfrak{p} = I^i$ for all $i \le c$ and $x^c y^{c+1} z^c u^{(2c+1)c} \in (I_{\mathfrak{p}}^{c+1} : \mathfrak{p}) \setminus I_{\mathfrak{p}}^{c+1}$. Hence $\operatorname{Ass} I = \operatorname{Ass} I^2 = \cdots = \operatorname{Ass} I^c$, $\operatorname{Ass} I^{c+1} = \operatorname{Ass}^\infty I$ and so $\operatorname{astab} I = c+1$. By the same argument as in the proof of Example 2.2, we see that $\mathfrak{m} = (x,y,z,u) \notin \operatorname{Ass} I^n$ for all $n \in \mathbb{N}$ and so we have $\operatorname{depth} R/I^n \ge 1$ and $x-y-z \in \mathfrak{m}$ is a nonzerodivisor on R/I^n for all $n \in \mathbb{N}$. Therefore $\overline{R/I^n} = \overline{R}/\overline{I^n} \cong K[y,z,u]/((y+z)^{c+1}z^c, u^{2c-1}yz, u^{2c+1})^n$, where $\overline{R} = R/(x-y-z)$. Since $z^{2c}u^{(2c+1)n-1} \in (\overline{I^n}) : \overline{\mathfrak{m}} \setminus \overline{I^n}$, it follows $\operatorname{depth} \overline{R}/\overline{I^n} = 0$ and so $\operatorname{depth} R/I^n = 1$ for all $n \in \mathbb{N}$. Therefore $\operatorname{dstab} I = 1$.

(ii) For all $n \in \mathbb{N}$, we have

$$\begin{aligned}(J^n : z^c u^c) &= (((x^c y^{c-1}, y^{c-1}x^{c-1}z)^n + z^c u^c J^{n-1}) : z^c u^c) \\ &= J^{n-1} + ((x^c y^{c-1}, y^{c-1}x^{c-1}z)^n : z^c u^c) \\ &= J^{n-1} + ((x^c y^{c-1}, y^{c-1}x^{c-1}z)^n : z^c).\end{aligned}$$

Since $((x^c y^{c-1}, y^{c-1}x^{c-1}z)^n : z^c) \subseteq J^{n-1}$, for all $n \in \mathbb{N}$ we have $(J^n : z^c u^c) = J^{n-1}$. Therefore, $\operatorname{Ass} J^n \subseteq \operatorname{Ass} J^{n+1}$ for all $n \in \mathbb{N}$. By using Macaulay2 and [Bayati et al. 2011] we have $\operatorname{Ass}^\infty J = \{(x,z), (x,u), (y,z), (y,u)\} = \operatorname{Min}(J)$ and so $\operatorname{astab} J = 1$. Since $\mathfrak{m} \notin \operatorname{Ass} J^n$ for all $n \in \mathbb{N}$, we have $2 = \dim R/J \ge \operatorname{depth} R/J^n \ge 1$ and $x-y \in \mathfrak{m}$ is a nonzerodivisor on R/J^n for all $n \in \mathbb{N}$. Again by the above argument, $\overline{R/J^n} = \overline{R}/\overline{J^n} \cong K[x,z,u]/(x^{2c-1}, x^{2c-2}z, z^c u^c)^n$, where $\overline{R} = R/(x-y)$. Since $\overline{J^i} : \overline{\mathfrak{m}} = \overline{J^i}$ for all $i \le c$ and $x^{(2c-1)n}z^{n-1}u^{c-1} \in \overline{J^n} : \overline{\mathfrak{m}} \setminus \overline{J^n}$ for all $n \ge c+1$, it follows that $\operatorname{depth} R/J = \operatorname{depth} R/J^2 = \cdots = \operatorname{depth} R/J^c = 2$ and $\operatorname{depth} R/J^n = 1$ for all $n \ge c+1$. Hence $\operatorname{dstab} J = c+1$. □

3. Nonincreasing depth functions

Theorem 3.1. *Let $(R, \mathfrak{m})$ be a regular local ring with* $\dim R = 3$ *and I be an ideal of R. If $I^{n+1} : I = I^n$ for all $n \in \mathbb{N}$, then* $\operatorname{depth} R/I^n$ *is nonincreasing.*

Proof. Suppose $\operatorname{height}(I) \ge 2$. Since $I^{n+1} : I = I^n$ for all $n \in \mathbb{N}$, it follows that $\operatorname{depth} R/I^{n+1} \le \operatorname{depth} R/I^n$. Now, let $\operatorname{height}(I) = 1$. Then there exists an ideal J of R and an element $f \in R$ such that $I = fJ$ and $\operatorname{height}(J) \ge 2$. As in the proof of Theorem 1.2, $\operatorname{depth} R/I^n = \operatorname{depth} R/J^n$ for all $n \in \mathbb{N}$. Since $I^{n+1} : I = I^n$ for all $n \in \mathbb{N}$, we have $J^{n+1} : J = J^n$. Thus $\operatorname{depth} R/J^{n+1} \le \operatorname{depth} R/J^n$ and so $\operatorname{depth} R/I^{n+1} \le \operatorname{depth} R/I^n$. This completes the proof. □

Corollary 3.2. (i) *Let $(R, \mathfrak{m})$ be a regular local ring with* $\dim R = 3$. *Then* $\operatorname{depth} R/\overline{I^n}$ *is nonincreasing.*

(ii) *Let* $R = k[x, y, z]$ *be a polynomial ring in* 3 *indeterminates over a field* k*. If* I *is an edge ideal of* R*, then* depth R/I^n *is nonincreasing.*

Example 3.3. *Let* $R = k[x, y, z, u]$ *be a polynomial ring and consider the ideal* $I = \big(xy^2z, yz^2u, zu^2(x+y+z+u), xu(x+y+z+u)^2, x^2y(x+y+z+u)\big)$ *of* R*. Then* depth $R/I =$ depth $R/I^4 = 0$ *and* depth $R/I^2 =$ depth $R/I^3 = 1$*. Thus the depth function is neither nonincreasing nor nondecreasing.*

In view of Theorem 3.1 one may ask whether in a regular local ring (of any dimension), depth R/I^n is a nonincreasing function of n, if $I^{n+1} : I = I^n$ for all n.

Acknowledgements

The second author would like to thank Universität Duisburg–Essen, especially the Department of Mathematics for its hospitality during the preparation of this work.

References

[Bayati et al. 2011] S. Bayati, J. Herzog, and G. Rinaldo, "A routine to compute the stable set of associated prime ideals of amonomial ideal", 2011, available at http://ww2.unime.it/algebra/rinaldo/stableset.

[Brodmann 1979a] M. Brodmann, "Asymptotic stability of Ass(M/I^nM)", *Proc. Amer. Math. Soc.* **74**:1 (1979), 16–18. MR Zbl

[Brodmann 1979b] M. Brodmann, "The asymptotic nature of the analytic spread", *Math. Proc. Cambridge Philos. Soc.* **86**:1 (1979), 35–39. MR Zbl

[Bruns and Herzog 1993] W. Bruns and J. Herzog, *Cohen–Macaulay rings*, Cambridge Studies in Advanced Mathematics **39**, Cambridge University Press, 1993. MR

[CoCoA] J. Abbott and A. M. Bigatti, "CoCoALib: a C++ library for doing computations in commutative algebra", available at http://cocoa.dima.unige.it/cocoalib.

[Herzog and Hibi 2011] J. Herzog and T. Hibi, *Monomial ideals*, Graduate Texts in Mathematics **260**, Springer, 2011. MR Zbl

[Herzog and Qureshi 2015] J. Herzog and A. A. Qureshi, "Persistence and stability properties of powers of ideals", *J. Pure Appl. Algebra* **219**:3 (2015), 530–542. MR Zbl

[Herzog et al. 2013] J. Herzog, A. Rauf, and M. Vladoiu, "The stable set of associated prime ideals of a polymatroidal ideal", *J. Algebraic Combin.* **37**:2 (2013), 289–312. MR Zbl

[Hibi et al. 2016] T. Hibi, K. Matsuda, T. Suzuki, and A. Tsuchiya, "Nonincreasing depth functions of monomial ideals", preprint, 2016. arXiv

[Huneke and Swanson 2006] C. Huneke and I. Swanson, *Integral closure of ideals, rings, and modules*, London Mathematical Society Lecture Note Series **336**, Cambridge University Press, 2006. MR Zbl

[Macaulay2] D. R. Grayson and M. E. Stillman, "Macaulay2, a software system for research in algebraic geometry", available at http://www.math.uiuc.edu/Macaulay2.

[McAdam 1983] S. McAdam, *Asymptotic prime divisors*, Lecture Notes in Mathematics **1023**, Springer, 1983. MR Zbl

[McAdam and Eakin 1979] S. McAdam and P. Eakin, "The asymptotic Ass", *J. Algebra* **61**:1 (1979), 71–81. MR Zbl

Received July 11, 2017. Revised November 15, 2017.

JÜRGEN HERZOG
FACHBEREICH MATHEMATIK
UNIVERSITÄT DUISBURG-ESSEN
ESSEN
GERMANY
juergen.herzog@uni-essen.de

AMIR MAFI
UNIVERSITY OF KURDISTAN
SANANDAJ 416
IRAN
a_mafi@ipm.ir

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.43

HOMOMORPHISMS OF FUNDAMENTAL GROUPS OF PLANAR CONTINUA

CURTIS KENT

We prove that every homomorphism from the fundamental group of a planar Peano continuum to the fundamental group of a planar or one-dimensional Peano continuum is induced by a continuous map up to conjugation. This is used to provide an uncountable family of planar Peano continua with pairwise nonisomorphic fundamental groups each of which is not homotopy equivalent to a one-dimensional space.

1. Introduction

Every continuous map between topological spaces induces a homomorphism between their respective homotopy and homology groups. This provides a method to translate questions about continuous functions of topological spaces into questions about homomorphisms of abstract groups. The converse statement is not true even for relatively nice spaces. For example, $\mathbb{R}P^\infty \times S^2$ and $\mathbb{R}P^2$ have isomorphic homotopy groups but there does not exist any continuous map which induces an isomorphism on all homotopy groups; see [Hatcher 2002, p. 345]. When only considering the first homotopy group, it is a classical result that any homomorphism from the fundamental group of a connected CW complex into the fundamental group of a $K(G, 1)$ space is induced by a continuous map; see [Hatcher 2002, Proposition 1B.9].

However, for spaces with local topological complications, the converse could fail even when only considering homomorphisms of the fundamental group. For example, an inner automorphism of the fundamental group of a one-dimensional continuum which is not locally simply connected at the chosen basepoint cannot be induced by a continuous map; see [Conner and Kent 2017, Proposition 3.12].

In the literature, the phrase *induced by a continuous map* has been used to mean both strictly induced by a continuous map and induced by a continuous map up to conjugation. To avoid confusion, we will say a homomorphism φ between fundamental groups is *induced by a continuous map* if $\varphi = f_*$ for some continuous map f. We will say that φ is *conjugate to a homomorphism induced by a continuous*

MSC2010: primary 20F34, 55P10, 57N05; secondary 54E45.
Keywords: Peano continuum, fundamental group, planar.

map if there exists a path α such that $\hat{\alpha}\circ\varphi = f_*$ for some continuous map f where $\hat{\alpha}$ is the change of basepoint isomorphism induced by the path α.

Katsuya Eda [1998] was the first to prove that arbitrary homomorphisms between fundamental groups of certain spaces which are not locally simply connected are induced by continuous maps up to conjugation by showing that any endomorphism of the fundamental group of the Hawaiian earring is conjugate to one induced by a continuous map. Later, Eda proved the following generalization.

Theorem A [Eda 2010]. *Every homomorphism between fundamental groups of one-dimensional Peano continua is conjugate to a homomorphism induced by a continuous map.*

Eda actually proves a stronger statement [2010, Theorem 1.2] by allowing the range to be the fundamental group of any one-dimensional metric space. Understanding the extent to which homomorphisms of fundamental groups are induced by continuous maps of the underlying topological spaces provides an additional tool to understand the homotopy type of locally complicated spaces using their fundamental groups, see [Cannon and Conner 2006; Eda 2002; Conner and Kent 2011]. Knowing when homomorphisms are induced by continuous maps allowed Eda to prove that the fundamental group is a perfect invariant of homotopy type for one-dimensional Peano continua [Eda 2010] and is the key tool to prove that the set of points at which a space is not semilocally simply connected is constructible from the fundamental group for one-dimensional and planar Peano continua [Conner and Eda 2005; Conner and Kent 2011].

In [Conner and Kent 2011], Greg Conner and the author show that many of the known results about fundamental groups of one-dimensional spaces extend to planar spaces. Specifically, it is proved that any homomorphism from the fundamental group of a one-dimensional Peano continuum to the fundamental group of a planar Peano continuum is induced by a continuous map after composing with a change of basepoint isomorphism (Theorem A when the range is a planar Peano continuum). Here we will prove the following theorem.

Theorem 2.7. *Let $\varphi : \pi_1(X, x_0) \to \pi_1(Y, y_0)$ be a homomorphism from the fundamental group of a planar Peano continuum X into the fundamental group of a one-dimensional or planar Peano continuum Y. Then there exists a continuous function $f : X \to Y$ and a path $\alpha : (I, 0, 1) \to (Y, y_0, y)$, with the property that $f_* = \hat{\alpha}\circ\varphi$.*

In one-dimensional spaces every path class contains a unique (up to reparametrization) minimal representative and every other representative can be homotoped to the unique minimal one by removing backtracking; see [Curtis and Fort 1959, Lemma 3.1] or [Cannon and Conner 2006, Theorem 3.9] for the existence and uniqueness of reduced representatives. We will say that a loop in a one-dimensional space is *reduced* if it is the unique minimal representative in its path class. Every one-dimensional Peano continuum deformation retracts to a one-dimensional Peano continuum in which every point is contained in some reduced loop [Conner and Meilstrup 2012, Theorems 4.3 and 3.1]. With these tools in hand, to prove that homomorphisms from the fundamental group of one-dimensional Peano continua are continuous up to conjugation, one starts with a one-dimensional Peano continuum such that each point is contained in a reduced loop and then uses the homomorphism to understand where to send each reduced loop.

Two of the difficulties of the planar case are the lack of a canonical deformation retract and the lack of representatives for path classes which are analogous to reduced paths in one-dimensional spaces. To prove Theorem 2.7, we will find a one-dimensional *core* of a planar Peano continuum to which we can apply Theorem A. We will show how to continuously extend this map to all of the planar continuum.

The property that homomorphisms are induced by continuous maps up to conjugation does not hold for more general spaces. For example there exists uncountable many homomorphisms from the fundamental group of the Hawaiian earring into the fundamental group of the projective plane which are not induced by a continuous function [Conner and Spencer 2005].

Homotopy dimension. The *homotopy dimension* of a space X is the smallest covering dimension of a space homotopy equivalent to X. A space is *homotopically at most k-dimensional* if its homotopy dimension is at most k.

Cannon and Conner [2007] asked the following question:

Question. If X is a planar Peano continuum whose fundamental group is isomorphic to the fundamental group of some one-dimensional Peano continuum, is it true that X is homotopy equivalent to a one-dimensional Peano continuum?

Let $\boldsymbol{S}$ be the Sierpinski curve in $\mathbb{R}^2$ obtained by the standard Cantor construction performed on the unit square in the plane. Let $\boldsymbol{S}_i$ be the planar Peano continuum obtained from $\boldsymbol{S}$ by filling in i of the removed discs, i.e.,

$$\boldsymbol{S}_i = \boldsymbol{S} \cup \Big(\bigcup_{n=1}^{i} D_n \Big),$$

where D_n are distinct bounded components of $\mathbb{R}^2 \setminus \boldsymbol{S}$. Cannon, Conner and Zastrow showed that $\boldsymbol{S}_1$ is not homotopy equivalent to any one-dimensional space [Cannon et al. 2002]. Their example, $\boldsymbol{S}_1$, illustrates that there exists some rigidity in planar sets and at least provides some motivation as to why the previous question is interesting. Karimov, Repovš, Rosicki, and Zastrow [Karimov et al. 2005] give additional examples of planar sets spaces which are not homotopically one-dimensional.

By applying Theorem 2.7, we will show that $\boldsymbol{S}_i$ cannot have the same fundamental group as any one-dimensional Peano continua and that the $\boldsymbol{S}_i$, $\boldsymbol{S}_j$ do not have isomorphic fundamental groups for $i \neq j$.

As an application of Theorem 2.7, we prove the following result.

Theorem 2.18. *There exists an uncountable family of planar Peano continua whose fundamental groups are pairwise nonisomorphic and also not isomorphic to the fundamental group of any one-dimensional Peano continuum.*

Our family of examples is constructed by filling infinitely many of the removed squares of $\boldsymbol{S}$ in a discrete fashion and then studying the limit set of the filled squares.

2. Planar to one-dimensional or planar

We will use $\mathbb{D}$ to denote the unit disc in the Euclidean plane $\mathbb{R}^2$ and I to denote the interval $[0, 1]$. For a metric space X, let $B_r^X(x) = \{y \in X \mid d(x, y) < r\}$ and $S_r^X(x) = \{y \in X \mid d(x, y) = r\}$. For planar sets X, $B_r^X(x) = B_r^{\mathbb{R}^2}(x) \cap X$ and $S_r^X(x) = S_r^{\mathbb{R}^2}(x) \cap X$. For A a subset of a metric space X, we let $\mathcal{N}_\epsilon(A) = \{x \in X \mid d(x, A) < \epsilon\}$, the open ϵ-neighborhood of A.

For a path $f : I \to X$, let $\bar{f}(t)$ denote the path $\bar{f}(t) = f(1-t)$. For a path $\alpha : (I, 0, 1) \to (X, x_0, x_1)$, let $\hat{\alpha} : \pi_1(X, x_0) \to \pi_1(X, x_1)$ by the standard change of base point isomorphism, i.e., $\hat{\alpha}([g]) = [\bar{\alpha} * g * \alpha]$. This isomorphism has inverse $\hat{\bar{\alpha}}$.

We will use $\operatorname{int}(X)$ to denote the interior of X as a subset of the plane, $\operatorname{cl}(X)$ for the closure of X in the plane and ∂X for $\operatorname{cl} X \setminus \operatorname{int}(X)$.

Theorem 2.1 [Eda 2010; Conner and Kent 2011]. *Let $\varphi : \pi_1(X, x_0) \to \pi_1(Y, y_0)$ be a homomorphism from the fundamental group of a one-dimensional Peano continuum X into the fundamental group of a one-dimensional or planar Peano continuum Y. Then there exists a continuous function $f : X \to Y$ and a path $\alpha : (I, 0, 1) \to (Y, y_0, y)$, with the property that $f_* = \hat{\alpha} \circ \varphi$.*

Lemma 2.2. *Suppose that $f : \partial\mathbb{D} \to X$ is a nullhomotopic loop into a planar or one-dimensional set. Then f is nullhomotopic in the $B_r^X(f(0))$ for every $r >$* $2 \operatorname{diam}(\operatorname{im} f)$.

Cannon and Conner [2007, Section 6: proof of Theorem 1.4] prove that every nullhomotopic loop in a planar Peano continuum bounds a disc contained in the convex hull of its image (in which case the multiplicative constant is unnecessary). However, they do not explicitly state this corollary of their proof. Another proof using the Riemann mapping theorem can be found in [Fischer and Zastrow 2005, Lemma 13]. Here we will prove a slightly weaker bound, which will be sufficient for our needs, using the Phragmén–Brouwer properties.

Proof. The lemma is trivial when X is one-dimensional since every nullhomotopic loop factors through a dendrite [Cannon and Conner 2006, Theorem 3.7] which implies that it is nullhomotopic inside of its image.

Suppose that $f : \partial\mathbb{D} \to X$ is a nullhomotopic loop into a planar set X. We will denote the smallest convex set containing a set A by $\operatorname{Hull}(A)$.

Claim. *Suppose that l is a line in the plane which is disjoint from* $\operatorname{im} f$ *and A is the component of $\mathbb{R}^2 \setminus l$ containing* $\operatorname{im} f$. *For every $\epsilon > 0$ and any extension $h : \mathbb{D} \to X$ of f, there exists an extension $\tilde{h} : \mathbb{D} \to X$ of f such that*

$$\tilde{h}(\{x \in \mathbb{D} \mid h(x) \neq \tilde{h}(x)\}) \subset X \cap \operatorname{Hull}(l \cap h(\mathbb{D})) \quad \textit{and} \quad \operatorname{im} \tilde{h} \subset X \cap \operatorname{cl}(\mathcal{N}_\epsilon(A)).$$

Proof of claim. Suppose that $h : \mathbb{D} \to X$ is a nullhomotopy of f. Let $\mathcal{C}$ be the components of $h^{-1}(\mathbb{R}^2 \setminus A)$ which intersect $\mathbb{R}^2 \setminus \mathcal{N}_\epsilon(A)$. Since $\mathbb{D}$ is compact, $\mathcal{C}$ is finite. For each $C \in \mathcal{C}$, let $\partial_M C$ be the boundary of the unbounded component of $\mathbb{R}^2 \setminus C$. Then $\partial_M C$ is a closed connected subset of $\mathbb{D}$ such that the closure of the bounded components of $\mathbb{R}^2 \setminus \partial_M C$ contains C. (This is the second of the Phragmén–Brouwer properties in [Wilder 1949, p. 47] applied to the unbounded component of $\mathbb{R}^2 \setminus C$.) We will denote the closure of the bounded components of $\mathbb{R}^2 \setminus \partial_M C$ by $\operatorname{wHull}(C)$.

By passing to a subset of $\mathcal{C}$, we may assume that for any two distinct elements $C, C' \in \mathcal{C}$ we have that C' is contained in the unbounded component of $\mathbb{R}^2 \setminus C$ while still maintaining the property that $h^{-1}\big(\mathbb{R}^2 \setminus \mathcal{N}_\epsilon(A)\big) \subset \bigcup_{c \in \mathcal{C}} \operatorname{wHull}(C)$.

Since $\partial_M C$ is connected, $h(\partial_M C)$ is contained in a connected component of $l \cap X$.

By the Tietze extension theorem, there exists $h_C : \operatorname{wHull}(C) \to l \cap X$ such that $h_C(x) = h(x)$ for all $x \in \partial_M C$. Since $h(\partial_M C)$ is contained in a connected component of $l \cap X$, we have that $X \cap \operatorname{Hull}(h(\partial_M C)) \subset l \cap X$ and h_C can be chosen to have image contained in $X \cap \operatorname{Hull}(h(\partial_M C))$.

By the pasting lemma for continuous functions, the function $\tilde{h} : \mathbb{D} \to X$ defined by $\tilde{h}(x) = h_C(x)$ if $x \in \operatorname{wHull}(C)$ for some $C \in \mathcal{C}$ and $\tilde{h}(x) = h(x)$ otherwise is a continuous function which extends f. By our choice of $\mathcal{C}$, $\operatorname{im} \tilde{h}$ is contained in $X \cap \operatorname{cl}(\mathcal{N}_\epsilon(A))$. □

Fix $\epsilon > 0$ such that $2 \operatorname{diam}(\operatorname{im} f) > \sqrt{2} \operatorname{diam}(\operatorname{im} f) + (1 + \sqrt{2})\epsilon$. Let l_1, l_2 be the two distinct vertical lines and l_3, l_4 the two distinct horizontal lines such that $d(f(0), l_i) = \operatorname{diam}(\operatorname{im} f) + \epsilon$ for $i \in \{1, \dots, 4\}$. Notice this implies that $\operatorname{im} f$ is contained in the unique bounded component of $\mathbb{R}^2 \setminus \{l_1, \dots, l_4\}$. By applying the previous claim to each l_i in turn, we obtain a nullhomotopy of f which is contained in the closure of an ϵ-neighborhood of the bounded component of $\mathbb{R}^2 \setminus \{l_1, \dots, l_4\}$.

By our choice of ϵ, this is contained in the ball of radius r for any $r > 2 \operatorname{diam}(\operatorname{im} f)$ which completes the proof of the lemma. □

Lemma 2.3. *Every bounded open set U of $\mathbb{R}^2$ is the union of a sequence of dyadic squares with disjoint interiors whose diameters form a null sequence. In addition,* *the squares can be chosen such that if* A_i *is the union of squares with side length at least* $1/2^i$, *then* $U \setminus A_i \subset \mathcal{N}_{1/2^{i-1}}(\partial U)$.

This is standard and well known. We present a proof to introduce notation that we will use later.

Proof. Set $\chi_i = \{(x, y) \mid 0 \le x \le 1/2^i,\ 0 \le y \le 1/2^i\}$ and let

$$Q_i = \{(n, m) + \chi_i \mid n, m \in (1/2^i)\mathbb{Z}\}$$

be the set of closed squares in the standard tiling of the plane by squares with side length $1/2^i$.

Let D_0 be the maximal subset of Q_0 such that $A_0 \subset U$ where $A_0 = \bigcup_{s \in D_0} s$. Then $U \setminus A_0 \subset \mathcal{N}_{1/2^{-1}}(\partial U)$.

We will inductively define D_i and A_i as follows. Let D_i be the maximal subset of Q_i such that $\bigcup_{s \in D_i} s \subset U \setminus \operatorname{int}(A_{i-1})$. Let $A_i = \left(\bigcup_{s \in D_i} s\right) \cup A_{i-1}$. Suppose $x \in U \setminus A_i$, then there exists some $s \in Q_i$ such that $x \in s$. Since the tilings are nested, if $s \cap \operatorname{int}(A_{i-1}) \neq \varnothing$, then $s \subset A_{i-1}$. Thus $s \cap \operatorname{int}(A_{i-1}) = \varnothing$. Since s is not in D_i and is disjoint from $\operatorname{int}(A_{i-1})$, we have $s \not\subset U$ and $d(x, \partial U) \le \operatorname{diam}(s) = \sqrt{2}/2^i < 1/2^{i-1}$. Thus $U \setminus A_i \subset \mathcal{N}_{1/2^{i-1}}(\partial U)$ and $\bigcup_{i=1}^{\infty} A_i = U$. $\square$

Lemma 2.4. *Let* $f : I \to X$ *be a continuous function into a metric space* X *and* $\mathcal{V}$ *be a covering of* I *by closed, possibly degenerate, intervals with disjoint interiors. Suppose that* $g : I \to X$ *is a mapping such that, for every* $V \in \mathcal{V}$, *the maps* g *and* f *agree on the endpoints of* V *and* $g|_V$ *is continuous. If there exists an* L *such that, for every* $V \in \mathcal{V}$, $\operatorname{diam}(g(V)) \le L \operatorname{diam}(f(V))$ *then* g *is continuous.*

In addition; if there exists a K *such that* $g|_V$ *is homotopic to* $f|_V$ *rel endpoints, for every* $V \in \mathcal{V}$, *by a homotopy of diameter at most* $K \operatorname{diam}(f(V))$, *then* g *is homotopic rel endpoints to* f.

Proof. Let f, g, $\mathcal{V}$, and L be defined as in the lemma. Fix $\epsilon > 0$. Since the elements of $\mathcal{V}$ have disjoint interiors and f is uniformly continuous, there exists a cofinite subset $\mathcal{V}_0 \subset \mathcal{V}$ such that the $\operatorname{diam}(f(V)) < \epsilon/(3L)$ for all $V \in \mathcal{V}_0$. Thus $\operatorname{diam}(g(V)) \le \epsilon/3$ for all $V \in \mathcal{V}_0$.

Fix $\delta > 0$ satisfying these conditions:

(i) $d(f(x), f(y)) < \epsilon/3$ for all $x, y \in I$ such that $|x - y| < \delta$.

(ii) $d(g(x), g(y)) < \epsilon/3$ for all $x, y \in V$ for some $V \in \mathcal{V} \setminus \mathcal{V}_0$ such that $|x - y| < \delta$.

Take $x, y \in I$ such that $|x - y| < \delta$. If $x, y \in V \in \mathcal{V}$, then $d(g(x), g(y)) < \epsilon/3$ by our choice of δ and $\mathcal{V}_0$. We may assume x, y are in distinct elements of $\mathcal{V}$ and without loss of generality $x < y$. There exist points x', y' such that $x \le x' \le y' \le y$ where x', y' are endpoints of the intervals of $\mathcal{V}$ containing x, y respectively. Then $|x - x'|, |y - y'|, |x' - y'| < \delta$. Thus

$$d(g(x), g(y)) \le d(g(x), g(x')) + d(f(x'), f(y')) + d(g(y'), g(y)) < \epsilon.$$

Therefore g is uniformly continuous.

Suppose $g|_V$ is homotopic to $f|_V$ rel endpoints, for each $V \in \mathcal{V}$, by a homotopy of diameter at most $K \operatorname{diam}(f(V))$. For each $V \in \mathcal{V}$, let $h_V : V \times I$ be a homotopy rel endpoints of $f|_V$ to $g|_V$ such that $\operatorname{diam}(h_V(V \times I)) \leq K \operatorname{diam}(f(V))$.

Define $h : I \times I \to X$ by $h(x,t) = h_V(x,t)$ for any $V \in \mathcal{V}$ such that $x \in V$. Since $h_V(x,t) = f(x)$ for all t if x is an endpoint of V, h is well defined. Notice that $h(x,0) = f(x)$ and $h(x,1) = g(x)$.

As before, there exists a cofinite subset $\mathcal{V}_1$ of $\mathcal{V}$ such that $\operatorname{diam}(\operatorname{im} h_V) < \epsilon/3$ for all $V \in \mathcal{V}_1$. Fix $\delta > 0$ satisfying the following:

(i) $d(f(x), f(y)) < \epsilon/3$ for all $x, y \in I$ such that $|x - y| < \delta$.

(ii) $d(h(x,t), h(y,s)) < \epsilon/3$ for all $x, y \in V$ for some $V \in \mathcal{V} \setminus \mathcal{V}_1$ such that $|x - y| + |s - t| < \delta$.

Suppose that $(x,s), (y,t) \in I \times I$ such that $|x - y| + |s - t| < \delta$. If $x, y \in V$ for some $V \in \mathcal{V}$, then $d(h(x,t), h(y,s)) < \epsilon/3$ by our choice of δ and $\mathcal{V}_1$. Thus we may assume x, y are in distinct elements of $\mathcal{V}$ and without loss of generality $x < y$. There exist points x', y' such that $x \leq x' \leq y' \leq y$ where x', y' are endpoints of the intervals of $\mathcal{V}$ containing x and y, respectively. Then $|x - x'|, |y - y'|, |x' - y'| < \delta$. Thus

$$\begin{aligned} d(h(x,t), h(y,s)) &\leq d(h(x,t), h(x',t)) + d(h(x',t), h(y',s)) + d(h(y',s), h(y,s)) \\ &< \epsilon/3 + d(f(x'), f(y')) + \epsilon/3 < \epsilon. \end{aligned}$$ □

Remark 2.5. For a planar Peano continuum X considered as a subset of $\mathbb{R}^2$, $\operatorname{int}(X)$ is on open bounded subset of the plane. By Lemma 2.3, $\operatorname{int}(X)$ can be tiled by a null sequence of dyadic squares with disjoint interiors. If A_i is the union of squares from the tiling of $\operatorname{int}(X)$ with side length at least $1/2^i$, then A_i has a natural CW structure given by the tiling and we will denote the one-skeleton of A_i by $A_i^{(1)}$. Then $X^{(1)} = \partial X \cup \left(\bigcup_i A_i^{(1)}\right)$ can be considered as a type of one-skeleton for X.

The following lemma is immediate from the construction of A_i and the diameter condition of the squares composing A_i. Alternatively, given a surjective map $f : I \to X$, it is a straightforward exercise to show how to modify it to construct a surjective map from I to $X^{(1)}$.

Lemma 2.6. *Let X be a planar Peano continuum and $X^{(1)} = \partial X \cup \left(\bigcup_i A_i^{(1)}\right)$, where A_i is as in Lemma 2.3 for the bounded open set* $\operatorname{int}(X)$. *Then $X^{(1)}$ is a one-dimensional Peano continuum.*

Theorem 2.7. *Let $\varphi : \pi_1(X, x_0) \to \pi_1(Y, y_0)$ be a homomorphism from the fundamental group of a planar Peano continuum X into the fundamental group of a one-dimensional or planar Peano continuum Y. Then there exists a continuous* *function* $f : X \to Y$ *and a path* $\alpha : (I, 0, 1) \to (Y, y_0, y)$, *with the property that* $f_* = \hat{\alpha} \circ \varphi$.

Proof. Let $X^{(1)} = \partial X \cup \big(\bigcup_i A_i^{(1)}\big)$, where A_i is as in Lemma 2.3 for the bounded open set $\operatorname{int}(X)$, and let $i : X^{(1)} \to X$ be the inclusion map. Since we are only concerned about the homomorphism up to conjugation, we may assume that $x_0 \in X^{(1)}$.

Let $B = \operatorname{int}(X) \setminus X^{(1)}$. Then B is the disjoint union of open square discs whose diameters form a null sequence.

Fix a loop $\beta : I \to X$ in X. Notice that $\beta^{-1}(B)$ is the disjoint union of open intervals in I. Let $\mathcal{V}$ be the covering of I by disjoint intervals consisting of two types: (1) the closure of a component of $\beta^{-1}(B)$ and (2) a point not contained in the closure of any interval of $\beta^{-1}(B)$. Then $\mathcal{V}$ is a cover of I by intervals with disjoint interiors.

For every nondegenerate $V \in \mathcal{V}$ there exists s_V a closed square from the tiling of $\operatorname{int}(X)$ such that $\beta(V) \subset s_V$. For every degenerate $V \in \mathcal{V}$, let $s_V = V$. Define $\beta' : I \to X$ by letting $\beta'|_V$ be a shortest path from $\beta(a)$ to $\beta(b)$ contained in ∂s_V where $V = [a, b]$. It is an elementary computation to show that $\operatorname{diam}(\beta'(V)) \le 2d(\beta(a), \beta(b)) \le 2 \operatorname{diam}(\beta(V))$. Since s_V is convex and contained in X, the map $h : I \times V \to X$ given by $h(t, v) = t\beta(v) + (1-t)\beta'(v)$ is a homotopy rel endpoints from $\beta|_V$ to $\beta'|_V$ with $\operatorname{diam}(\operatorname{im} h_V) \le 4 \operatorname{diam}(f(V))$. Lemma 2.4 implies that β' is continuous and homotopic to β. Hence i_* is surjective.

By Theorem 2.1, $\varphi \circ i_* : \pi_1(X^{(1)}, x_0) \to \pi_1(Y, y_0)$ is conjugate to being induced by a continuous map, i.e., $\varphi \circ i_* = \hat{\hat{\alpha}} \circ f_*$ where $f : X^{(1)} \to Y$ is a continuous map and $\alpha : I \to Y$ is a continuous path.

Let s be a square for our tiling of $\operatorname{int}(X)$. Then $f|_{\partial s}$ is a nullhomotopic loop in Y. Thus we can extend f to all of s such that $\operatorname{diam}(f(s)) \le 2 \operatorname{diam}(f(\partial s))$. Doing this for all the components of B defines an extension $\overline{f}$ of f to all of X. The diameter condition guarantees the continuity of $\overline{f}$ (the details are analogous to those of Lemma 2.4).

Let β be a loop in X. Then there exists a loop β' in $X^{(1)}$ homotopic (in X) to β. Then

$$\begin{aligned}\varphi([\beta]) &= \varphi \circ i_*([\beta']) = \hat{\hat{\alpha}} \circ f_*([\beta']) \\ &= \hat{\hat{\alpha}}([f \circ \beta']) = \hat{\hat{\alpha}}([\overline{f} \circ \beta']) \\ &= \hat{\hat{\alpha}}([\overline{f} \circ \beta]) = \hat{\hat{\alpha}} \circ \overline{f}_*([\beta])\end{aligned}$$

as desired. □

Applications. The Sierpinski curve in $\mathbb{R}^2$, which we will denote by $\boldsymbol{S}$, is constructed by iterating the process of subdividing $[0, 1] \times [0, 1]$ into 9 squares, removing the center one and repeating on each of the remaining 8 squares.

To be explicit, let $C_0 = ([0, 1] \times [0, 1])$ and define C_n inductively as follows.

$$C_n = C_{n-1} \setminus \Big\{ \bigcup_{0 \le i, j < 3^{n-1}} \Big(\frac{1+3i}{3^n}, \frac{2+3i}{3^n} \Big) \times \Big(\frac{1+3j}{3^n}, \frac{2+3j}{3^n} \Big) \Big\}.$$

Then $\boldsymbol{S} = \bigcap_n C_n$. Notice that $\mathbb{R}^2 \setminus \boldsymbol{S}$ is the union of countably many open squares with disjoint closures and a single unbounded component. Let $\{D_n\}$ be an enumeration of the bounded components of the complement of $\boldsymbol{S}$.

For $A \subset \mathbb{N}$, let $\boldsymbol{S}_A = \boldsymbol{S} \cup \big(\bigcup_{n \in A} D_n\big)$; i.e., $\boldsymbol{S}_A$ is the space obtained from $\boldsymbol{S}$ by filling in the squares with indices in A. For $i \in \mathbb{N}$, let $\boldsymbol{S}_i = \boldsymbol{S} \cup \big(\bigcup_{n=1}^{i} D_n\big)$.

We will say that a sequence of subsets A_n of X converges to a set $A \subset X$, if for every $\epsilon > 0$ there exists an N such that $A_n \subset \mathcal{N}_\epsilon(A)$ and $A \subset \mathcal{N}_\epsilon(A_n)$ for all $n > N$.

Lemma 2.8. *For every $x \in \boldsymbol{S}$, there exists a subsequence of natural numbers (i_n) such that D_{i_n} converges to $\{x\}$. Thus $\boldsymbol{S}$ is one-dimensional and $\bigcup_{n=1}^{\infty} \partial D_n$ is dense in $\boldsymbol{S}$.*

Proof. Notice that C_n is contained in the closed $\sqrt{2}/3^n$-neighborhood of the boundaries of the open squares removed from C_{n-1} to obtained C_n. Thus every point in $\boldsymbol{S}$ is at most $\sqrt{2}/3^n$ from the boundary of an open square contained in $\mathbb{R}^2 \setminus \boldsymbol{S}$ with side length $1/3^n$. For every n, we can choose an i_n such that D_{i_n} is a square with side length $1/3^n$ which is at most $\sqrt{2}/3^n$ from x. Then ∂D_{i_n} converges to x. Thus $\boldsymbol{S}$ is one-dimensional and $\bigcup_{n=1}^{\infty} \partial D_n$ is dense in $\boldsymbol{S}$. □

Zastrow's example in [Cannon et al. 2002] and Example (2) in [Karimov et al. 2005] appear to suggest the following lemma.

Lemma 2.9. *Suppose that $h : X \to X$ is a continuous map of a planar Peano continuum such that every loop is freely homotopic to its image under h. Then h fixes the set of points at which X is not semilocally simply connected.*

Proof. Suppose that X is not semilocally simply connected at x and $h(x) \neq x$. Then we would be able to find an $\epsilon > 0$ such that the balls $B_\epsilon^{\mathbb{R}^2}(x)$ and $B_\epsilon^{\mathbb{R}^2}(h(x))$ are disjoint and $S_\epsilon^X(x) \subsetneq S_\epsilon^{\mathbb{R}^2}(x)$. This implies that $S_\epsilon^X(x)$ is the disjoint union of closed intervals.

Since any loop is freely homotopic to its image under h, any sufficiently small loop in $B_\epsilon^X(x)$ can be homotoped into $B_\epsilon^X(h(x))$. However, any map of an annulus which takes one boundary component into $B_\epsilon^X(x)$ and the other into $B_\epsilon^X(h(x))$ can be cut along $S_\epsilon^X(x)$ to construct a nullhomotopy of the boundary loops. The details for the cutting procedure are analogous to the proof of the claim on page 47. Thus any sufficiently small loop in $B_\epsilon(x)$ must be nullhomotopic. However this contradicts the assumption that X is not semilocally simply connected at x. □

Cannon, Conner, and Zastrow showed that $\boldsymbol{S}_1$ is not homotopy equivalent to any one-dimensional Peano continuum. We can now use Theorem 2.7 to show even more, that the fundamental group of $\boldsymbol{S}_1$ is not *one-dimensional* in the following sense.

Theorem 2.10. *For any $s_0 \in \boldsymbol{S}$, the fundamental group $\pi_1(\boldsymbol{S}_i, s_0)$ is not isomorphic to the fundamental group of any one-dimensional Peano continuum.*

Proof. Suppose that there exists X a one-dimensional Peano continuum such that $\pi_1(X, x_0)$ is isomorphic to $\pi_1(\boldsymbol{S}_i, s_0)$. By Theorem 2.7, there exists a continuous map $f : \boldsymbol{S}_i \to X$ which induces an isomorphism f_* of fundamental groups.

By applying Theorem 2.1 to the homomorphism f_*^{-1}, we can find a map $g : X \to \boldsymbol{S}_i$ such that $g \circ f \circ \beta$ is freely homotopic to β for every loop β based at x_0. (Note that β might not be homotopic to $g \circ f \circ \beta$ relative to endpoints.)

Since $\boldsymbol{S}_i$ is obtained by only adding finitely many discs, every neighborhood of every point in $\boldsymbol{S}$ contains a loop which is essential in $\boldsymbol{S}_i$. Thus $g \circ f$ must fix $\boldsymbol{S}$ by Lemma 2.9.

Let D_k be a square which was filled in the construction of $\boldsymbol{S}_i$. Since f maps ∂D_k to a nullhomotopic loop in a one-dimensional space, the map f must identify two distinct points x, y on the boundary of D_k. However this is a contradiction since $\partial D_k \subset \boldsymbol{S}$. □

Corollary 2.11. *For any $s_0 \in \boldsymbol{S}$ and any pair of distinct natural numbers i and j, the groups $\pi_1(\boldsymbol{S}_i, s_0)$ and $\pi_1(\boldsymbol{S}_j, s_0)$ are not isomorphic.*

Proof. We will assume that $i > j$ and proceed by way of contradiction. As in the proof of Theorem 2.10, we may assume that there are maps $f : \boldsymbol{S}_i \to \boldsymbol{S}_j$ and $g : \boldsymbol{S}_j \to \boldsymbol{S}_i$ such that $g \circ f \circ \beta$ is freely homotopic to β for any loop β based at s_0. As before, $g \circ f$ must fix $\boldsymbol{S}$.

Let D_k be a square which was filled in the construction of $\boldsymbol{S}_i$. Notice that ∂D_k must map to a simple closed curve which is nullhomotopic in $\boldsymbol{S}_j$ ($f|_{\boldsymbol{S}}$ must be injective). Hence it must map to the boundary of a square which was filled in the construction of $\boldsymbol{S}_j$. (A simple closed curve α in the plane is nullhomotopic if and only if the bounded component of $\mathbb{R}^2 \setminus \operatorname{im} \alpha$ is simply connected.) Since $i > j$, f must map two boundary circles to the same boundary circle which contradicts that fact that f restricted to $\boldsymbol{S}$ must be injective. □

We will now show how to extend Corollary 2.11 to certain nice fillings of $\boldsymbol{S}$.

Definition 2.12. Let $A \subset \mathbb{N}$. We will use $B(\boldsymbol{S}_A)$ to denote the set of points at which $\boldsymbol{S}_A$ is not semilocally simply connected. Let $K(\boldsymbol{S}_A)$ be the set of accumulation points of $\{D_n \mid n \in A\}$, i.e.,

$$K(\boldsymbol{S}_A) = \big\{x \in \boldsymbol{S} \mid \{n \in A \mid D_n \subset B_r(x)\} \text{ is infinite for every } r > 0\big\}.$$

We will say that $\boldsymbol{S}_A$ is a *discrete* filling of $\boldsymbol{S}$ if $\operatorname{cl}(D_n) \cap K(\boldsymbol{S}_A) = \varnothing$ for all $n \in A$. We will say that Y is *sparse* in $\boldsymbol{S}$ if $Y \subset \mathcal{N}_\delta(\boldsymbol{S} \setminus Y)$ for every $\delta > 0$.

Lemma 2.13. *If $\mathbf{S}_A$ is a discrete filling then $\partial D_n \subset B(\mathbf{S}_A)$ for all $n \in A$ and $B(\mathbf{S}_A) = \mathbf{S}$.*

Proof. It is clear that $B(\mathbf{S}_A) \subset \mathbf{S}$. By construction, $\mathrm{cl}(D_n) \cap \mathrm{cl}(D_m) = \varnothing$ for all $n \neq m$. For $n \in A$, let ϵ_n be the distance from $\mathrm{cl}(D_n)$ to $K(\mathbf{S}_A) \cup \left(\bigcup_{i \in A \setminus \{n\}} D_i\right)$. Since $\mathrm{cl}(D_n) \cap K(\mathbf{S}_A) = \varnothing$, ϵ_n is strictly positive. This implies that $\mathcal{N}_{\epsilon_n}(D_n)$ is not simply connected. Even more, $B(\mathbf{S}_A) \cap \mathcal{N}_{\epsilon_n}(D_n) = \mathcal{N}_{\epsilon_n}(D_n) \setminus D_n$. Thus the only points of $\mathbf{S}$ which might possibly have simply connected neighborhoods in $\mathbf{S}_A$ are those in $K(\mathbf{S}_A)$.

Suppose that $x \in \mathbf{S} \cap K(\mathbf{S}_A)$ and let U be a neighborhood of x. We must show that U is not simply connected. Since $x \in K(\mathbf{S}_A)$, we can find $n \in A$ such that $\mathrm{cl}(D_n) \subset U$. Therefore $\mathcal{N}_\epsilon(D_n) \subset U$ for some choice of $n \in A$ and $0 < \epsilon \leq \epsilon_n$ which implies that U is not simply connected since $\partial D_n \subset B(\mathbf{S}_A)$. □

The proof of the following lemma is similar to the proof of Theorem 2.10.

Lemma 2.14. *If $\mathbf{S}_A$ is a discrete filling then $\pi_1(\mathbf{S}_A, s)$ is not isomorphic to the fundamental group of a one-dimensional Peano continuum.*

Lemma 2.15. *Every simply connected subset of $\mathbf{S}$ is a sparse subset of $\mathbf{S}$.*

Proof. Let Y be a simply connected (not necessarily connected) subset of $\mathbf{S}$. Since $\mathbf{S}$ is one-dimensional, this implies that Y can contain no simply closed curves. Fix $y \in Y$. Then there exists a sequence of natural numbers i_n such that ∂D_{i_n} converges to y. Since ∂D_{i_n} cannot be entirely contained in Y, there exists an $x_n \in \partial D_{i_n}$ such that $x_n \in \mathbf{S} \setminus Y$. The diameter of ∂D_{i_n} must converge to 0, thus x_n converges to y and $Y \subset \mathcal{N}_\delta(\mathbf{S} \setminus Y)$ for every $\delta > 0$. □

Lemma 2.16. *Let Y be a sparse closed subset of $\mathbf{S}$. Then there exists a subset $A \subset \mathbb{N}$ such that $\mathbf{S}_A$ is a discrete filling of $\mathbf{S}$ and $K(\mathbf{S}_A) = Y$.*

Proof. A subset B of a metric space X is *δ-separated* if $d(x, y) \geq \delta$ for all $x, y \in B$. A δ-separated subset B of a space X is *maximal* if $X \subset \mathcal{N}_\delta(B)$. It is an exercise to show that any δ-separated subset of X can be extended to a maximal δ-separated subset.

Since Y is compact, any δ-separated subset of Y is finite. Let Y_1 be a maximal 1-separated subset of Y. Define Y_n to be a maximal $\frac{1}{n}$-separated subset of Y which extends Y_{n-1}.

For every $y \in Y_n$ there exists $s_{y,n} \in \mathbf{S} \setminus Y$ such that $d(s_{y,n}, y) \leq 1/n$. Fix $\delta_n > 0$ such that $\delta_n < d(s_{y,n}, Y)$ for all $y \in Y_n$. Then we may choose $i(y, n) \in \mathbb{N}$ such that $d(D_{i(y,n)}, s_{y,n}) \leq \delta_n/3$ and $D_{i(y,n)}$ has side length less than $\delta_n/3$. This implies $\mathrm{cl}(D_{i(y,n)}) \cap Y = \varnothing$.

Let $A = \{i(y, n) \mid n \in \mathbb{N} \text{ and } y \in Y_n\}$. By constructions $K(\mathbf{S}_A) = Y$. Thus $\mathbf{S}_A$ is a discrete filling. □

Proposition 2.17. *Suppose that S_A, S_B are discrete fillings of S. If $\pi_1(S_A, s_0)$ is isomorphic to $\pi_1(S_B, s_1)$, then $K(S_A)$ is homeomorphic to $K(S_B)$.*

Proof. Suppose that S_A, S_B are discrete fillings of S and $\pi_1(S_A, s_0)$ is isomorphic to $\pi_1(S_B, s_1)$. Since the fundamental group is basepoint invariant, we may assume that $s_0 = s_1 \in S$.

Using Theorem 2.7 and Lemma 2.9, we can find maps $f : S_A \to S_B$ and $g : S_B \to S_A$ such that both $g \circ f$ and $f \circ g$ are the identity on S. (For discrete fillings $B(S_A) = S$ by Lemma 2.13.) For $n \in A$, the loop ∂D_n is a nullhomotopic simple closed curve in $S \subset S_A$ which implies that $f(\partial D_n)$ is a nullhomotopic simple closed curve in S_B. (A simple closed curve α in the plane is nullhomotopic if and only if the bounded component of $\mathbb{R}^2 \setminus \operatorname{im} \alpha$ is simply connected.) Thus $f(\partial D_n) = D_m$ for some $m \in B$.

Thus $f(K(S_A)) \subset K(S_B)$. We can similarly show $g(K(S_B)) \subset K(S_A)$. Since $K(S_A), K(S_B) \subset S$ and $g \circ f$ is the identity on S, it follows $K(S_A)$ is homeomorphic to $K(S_B)$. □

Theorem 2.18. *There exists an uncountable family of planar Peano continua whose fundamental groups are pairwise nonisomorphic and also not isomorphic to the fundamental group of any one-dimensional Peano continuum.*

Proof. Let $\{U_1, U_2, \ldots\}$ be a countable set of disjoint open subsets of $(0, 1) \times (0, 1)$ such that U_i converges to a point. In each U_i we can find a subset X_i such that $X_i \subset S$ and X_i is homeomorphic to the wedge of i closed intervals. Note that Sierpinski [1916] showed that any one-dimensional planar continuum embeds into S. Since every open set of S contains a scaled copy of S, it is always possible to find X_i in $U_i \cap S$.

For every $A \subset \mathbb{N}$, let $X_A = \operatorname{cl}\left(\bigcup_{i \in A} X_i\right)$ which is simply connected. It is a trivial exercise to show that X_A is homeomorphic to X_B if and only if $A = B$.

Notice that for any $A \subset \mathbb{N}$, X_A is sparse. Thus for $A \subset \mathbb{N}$, we may choose $\widetilde{A} \subset \mathbb{N}$ such that $K(S_{\widetilde{A}}) = X_A$. The corollary then follows from Proposition 2.17. □

References

[Cannon and Conner 2006] J. W. Cannon and G. R. Conner, "On the fundamental groups of one-dimensional spaces", *Topology Appl.* **153**:14 (2006), 2648–2672. MR Zbl

[Cannon and Conner 2007] J. W. Cannon and G. R. Conner, "The homotopy dimension of codiscrete subsets of the 2-sphere $\mathbb{S}^2$", *Fund. Math.* **197** (2007), 35–66. MR Zbl

[Cannon et al. 2002] J. W. Cannon, G. R. Conner, and A. Zastrow, "One-dimensional sets and planar sets are aspherical", *Topology Appl.* **120**:1-2 (2002), 23–45. MR Zbl

[Conner and Eda 2005] G. Conner and K. Eda, "Fundamental groups having the whole information of spaces", *Topology Appl.* **146/147** (2005), 317–328. MR Zbl

[Conner and Kent 2011] G. R. Conner and C. Kent, "Concerning fundamental groups of locally connected subsets of the plane", preprint, 2011. arXiv

[Conner and Kent 2017] G. R. Conner and C. Kent, "Homotopy dimension of planar continua", preprint, 2017. arXiv

[Conner and Meilstrup 2012] G. Conner and M. Meilstrup, "Deforestation of Peano continua and minimal deformation retracts", *Topology Appl.* **159**:15 (2012), 3253–3262. MR Zbl

[Conner and Spencer 2005] G. Conner and K. Spencer, "Anomalous behavior of the Hawaiian earring group", *J. Group Theory* **8**:2 (2005), 223–227. MR Zbl

[Curtis and Fort 1959] M. L. Curtis and M. K. Fort, Jr., "The fundamental group of one-dimensional spaces", *Proc. Amer. Math. Soc.* **10** (1959), 140–148. MR Zbl

[Eda 1998] K. Eda, "Free σ-products and fundamental groups of subspaces of the plane", *Topology Appl.* **84**:1-3 (1998), 283–306. MR Zbl

[Eda 2002] K. Eda, "The fundamental groups of one-dimensional spaces and spatial homomorphisms", *Topology Appl.* **123**:3 (2002), 479–505. MR Zbl

[Eda 2010] K. Eda, "Homotopy types of one-dimensional Peano continua", *Fund. Math.* **209**:1 (2010), 27–42. MR Zbl

[Fischer and Zastrow 2005] H. Fischer and A. Zastrow, "The fundamental groups of subsets of closed surfaces inject into their first shape groups", *Algebr. Geom. Topol.* **5** (2005), 1655–1676. MR Zbl

[Hatcher 2002] A. Hatcher, *Algebraic topology*, Cambridge University Press, 2002. MR Zbl

[Karimov et al. 2005] U. Karimov, D. Repovš, W. Rosicki, and A. Zastrow, "On two-dimensional planar compacta not homotopically equivalent to any one-dimensional compactum", *Topology Appl.* **153**:2-3 (2005), 284–293. MR Zbl

[Sierpiński 1916] W. Sierpiński, "Sur une courbe *cantor*ienne qui contient une image biunivoque et continue de toute courbe donnée", *C. R. Acad. Sci.* **162** (1916), 629–632. Zbl

[Wilder 1949] R. L. Wilder, *Topology of manifolds*, American Mathematical Society Colloquium Publications **32**, American Mathematical Society, New York, 1949. MR Zbl

Received November 10, 2015. Revised December 1, 2017.

CURTIS KENT
DEPARTMENT OF MATHEMATICS
BRIGHAM YOUNG UNIVERSITY
PROVO, UT
UNITED STATES
curtkent@math.byu.edu

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.57

THE GROWTH RATE OF THE TUNNEL NUMBER OF m-SMALL KNOTS

TSUYOSHI KOBAYASHI AND YO'AV RIECK

In a previous paper, we defined the *growth rate of the tunnel number of knots*, an invariant that measures the asymptotic behavior of the tunnel number under connected sum. In this paper we calculate the growth rate of the tunnel number of m-small knots in terms of their bridge indices.

Kobayashi was supported by Grant-in-Aid for scientific research, JSPS grant number 25400091. This work was partially supported by a grant from the Simons Foundation (283495 to Yo'av Rieck).
MSC2010: 57M25, 57M99.
Keywords: knots, 3-manifolds, Heegaard splittings, tunnel number, growth rate.

Part I. Introduction and background material

1. Introduction

Let M be a compact connected orientable 3-manifold and $K \subset M$ a knot. K is called *admissible* if $g(E(K)) > g(M)$ and *inadmissible* otherwise (throughout this paper $E(\cdot)$ denotes knot exterior and $g(\cdot)$ denotes the Heegaard genus; see Section 2 for these and other basic definitions). Let nK denote the connected sum of n copies of K. In [Kobayashi and Rieck 2006b] we defined the *growth rate* of the tunnel number of K to be:

$$\mathrm{gr}_t(K) = \limsup_{n\to\infty} \frac{g(E(nK)) - ng(E(K)) + n - 1}{n-1}.$$

The main result of [Kobayashi and Rieck 2006b] shows that if K is admissible then $\mathrm{gr}_t(K) < 1$, and $\mathrm{gr}_t(K) = 1$ otherwise. This concept was the key to constructing a counterexample to Morimoto's conjecture [Kobayashi and Rieck 2008; 2009]. Unless explicitly stated otherwise, all knots considered are assumed to be admissible (note that this is always the case for knots in the 3-sphere S^3).

In this paper we continue our investigation of the growth rate of the tunnel number. In Part II we give an upper bound on the growth rate of admissible knots (this is an improvement of the bound given in [Kobayashi and Rieck 2006b]), and in Part III we obtain a lower bound on the growth rate of admissible m-small knots (a knot is called *m-small* if its meridian is not a boundary slope of an essential surface). With this we obtain an exact calculation of the growth rate of m-small knots. Before stating this result we define the following notation that will be used extensively throughout the paper:

Notation 1.1. Let $K \subset M$ be an admissible knot. We denote $g(E(K)) - g(M)$ by g and for $i = 1, \dots, g$ we denote the bridge index of K with respect to Heegaard surfaces of genus $g(E(K)) - i$ by b_i^*. That is, b_i^* is the minimal integer so that K admits a b_i^* bridge position with respect to some Heegaard surface of M of genus $g(E(K)) - i$; we call such a decomposition a $(g(E(K)) - i, b_i^*)$ *decomposition*. Note that for a knot $K \subset S^3$ we have that $g = g(E(K))$, $b_g^*(K)$ is the bridge index of K, and $b_{g-1}^*(K)$ is the torus bridge index of K.

We note that, for any knot $K \subset M$, b_i^* forms an increasing sequence of positive integers: $0 < b_1^* < \cdots < b_g^*$. To see this, fix $i \geq 1$ and let Σ be a Heegaard surface that realizes the bridge index b_i^*, that is, Σ is a genus $g(E(K)) - i$ Heegaard surface for M with respect to which K has bridge index b_i^*. By tubing Σ once (see Definition 5.3) we obtain a Heegaard surface of genus $g(E(K)) - (i-1)$ that realizes a $(g(E(K)) - (i-1), b_i^* - 1)$ decomposition for K. This shows that $b_{i-1}^* \leq b_i^* - 1$.

We are now ready to state the following theorem:

Theorem 1.2. *Let M be a compact connected orientable 3-manifold and $K \subset M$ be an admissible knot. Then $gr_t(K) \leq \min_{i=1,\dots,g}\{1 - i/b_i^*\}$. If, in addition, K is m-small then equality holds*:

$$gr_t(K) = \min_{i=1,\dots,g}\left\{1 - \frac{i}{b_i^*}\right\}.$$

Moreover, for m-small knots the limit of $\frac{1}{n-1}(g(E(nK)) - ng(E(K)) + n - 1)$ *exists.*

Remark 1.3. Let X be a manifold whose boundary ∂X is a single torus. By Hatcher [1982], only finitely many slopes on ∂X are boundary slopes of an essential surface. Let M be a manifold obtained by filling any slope not in this finite set, and $K \subset M$ be the core of the attached solid torus. By construction, K is an m-small knot; this shows that m-small knots are very common indeed.

As noted in Notation 1.1, the indices b_i^* form an increasing series of positive integers. It follows that $b_i^* \geq i$; moreover, $b_i^* = i$ implies that $b_1^* = 1$. Applying this to an index i that realizes that the equality $\mathrm{gr}_t(K) = 1 - i/b_i^*$ we obtain the following simple and useful consequence of Theorem 1.2 that strengthens the main result of [Kobayashi and Rieck 2006b] in the case of m-small knots:

Corollary 1.4. *If $K \subset M$ is an admissible m-small knot, then*

$$0 \leq gr_t(K) < 1.$$

Moreover, $gr(K) = 0$ if and only if $b_1^* = 1$.

There are several results about the spectrum of the growth rate and we summarize them here. It is well known that there exist manifolds M that admit minimal genus Heegaard splittings Σ of genus at least 2 and of Hempel distance at least 3. We fix such M and Σ and for simplicity we assume that M is closed. Let C be a handlebody obtained by cutting M along Σ and K a core of C, that is, K is a core of a solid torus obtained by cutting C along appropriately chosen meridian disks. Then Σ is a Heegaard surface for $E(K)$; it follows that K is inadmissible. Clearly, the Hempel distance does not go down after drilling K. Hence the Hempel distance of $\Sigma \subset E(K)$ is at least 3. It is a well known consequence of the Thurston–Perelman geometrization theorem that manifolds that admit a Heegaard surface of genus at least 2 and Hempel distance at least 3 are hyperbolic. Thus $K \subset M$ is a hyperbolic knot in a hyperbolic manifold. As mentioned above, the growth rate of inadmissible knots is 1. This proves the existence of hyperbolic knots in hyperbolic manifolds with growth rate 1. It was shown in [Kobayashi and Rieck 2006b] that torus knots and 2-bridge knots have growth rate 0. Kobayashi and Saito [2010] constructed knots with growth rate $-\frac{1}{2}$. Theorem 1.2 enables us to calculate the growth rate of the knots constructed by Morimoto, Sakuma and Yokota in [Morimoto et al. 1996] (perhaps with finitely many exceptions), which we denote by K_{MSY}. We explain this here. The knots K_{MSY} enjoy the following properties:

(1) K_{MSY} are hyperbolic and m-small: this was announced by Morimoto [2008].

(2) $g(E(K_{\mathrm{MSY}})) = 2$: this was proved in [Morimoto et al. 1996].

(3) $b_1^*(K_{\mathrm{MSY}}) = 2$ (in other words, the torus bridge index of K_{MSY} is 2): it was shown in [Morimoto et al. 1996] that $b_1^* > 1$, and it is easy to observe that $b_1^* \leq 2$ (see, for example, [Kobayashi and Rieck 2006b]).

(4) $b_2^*(K_{\mathrm{MSY}}) \geq 4$ (in other words, the bridge index of K_{MSY} is at least 4): since $b_2^*(K_{\mathrm{MSY}}) > b_1^*(K_{\mathrm{MSY}})$, we only need to exclude the possibility $b_2^*(K_{\mathrm{MSY}}) = 3$. Assume for a contradiction that $b_2^*(K_{\mathrm{MSY}}) = 3$. Then K_{MSY} is a 3-bridge knot of tunnel number 1. Kim [2005] proved that every 3-bridge knot of tunnel number 1 has torus bridge index 1, contradicting the previous point. We note that R. Bowman, S. Taylor and A. Zupan [Bowman et al. 2015] showed that $b_2^*(K_{\mathrm{MSY}}) = 7$ for all but finitely many of the knots K_{MSY} (see Remark 1.7).

Using these facts, Theorem 1.2 implies that $\mathrm{gr}_t(K_{\mathrm{MSY}}) = \frac{1}{2}$. This is the first example of knots with growth rate in the open interval (0, 1) and provides a partial answer to questions posed in [Kobayashi and Rieck 2006b]. In summary we have the following; we emphasize that only (4) is new:

Corollary 1.5.

(1) *There exist hyperbolic knots in hyperbolic manifolds with growth rate* 1.

(2) *There exist hyperbolic knots in S^3 with growth rate* 0.

(3) *There exist knots in S^3 with growth rate* $-\frac{1}{2}$.

(4) *There exist hyperbolic knots in S^3 with growth rate* $\frac{1}{2}$.

Remark 1.6. In joint work with K. Baker [Baker et al. 2016], we use Theorem 1.2 to show that for any $\epsilon > 0$ there exists a hyperbolic knot $K \subset S^3$ with $1-\epsilon < \mathrm{gr}_t(K) < 1$. This implies, in particular, that the spectrum of the growth rate is infinite.

Remark 1.7. We take this opportunity to mention a few recent results about b_i^* that appeared since we first started writing this paper; for precise statements see references.

(1) Given positive integers $g_M < i \leq g_K$ and n, K. Ichihara and T. Saito [2013] constructed manifolds M and knots $K \subset M$ so that $g(M) = g_M$, $g(E(K)) = g_K$, and $b_i^*(K) - b_{i-1}^*(K) \geq 2$ (see [Ichihara and Saito 2013, Corollary 2]; the notation there is different from ours); their arguments can easily be applied to construct knots such that $b_i^*(K) - b_{i-1}^*(K) \geq n$ (informally, we may phrase this as an *arbitrarily large gap*).

(2) Zupan [2014] studied the bridge indices of iterated torus knots showing, in particular, that there exist iterated torus knots realizing arbitrarily large gaps between b_{i-1}^* and b_i^* for any i in the range where both indices are defined.

An easy argument shows that iterated torus knots are m-small; every knot K considered by Zupan fulfills $b_1^*(K) = 1$, and so has $\mathrm{gr}(K) = 0$ by Corollary 1.4.

(3) Bowman, Taylor, and Zupan [2015] calculated the bridge indices of generic iterated torus knots (see [Bowman et al. 2015] for definitions). They gave conditions on the parameters that imply that $b_g^* = p$, where here the knot considered is obtained by twisting the torus knot $T_{p,q}$, $p < q$. (We note that for the twisted torus knot $g = 2$). Applying this to K_{MSY} we see that all but finitely many of these knots have $b_2^* = 7$, improving on our estimate $b_2^* \geq 4$. We remark that in [Bowman et al. 2015] a linear lower bound on b_1^* was also obtained, showing that many twisted torus knots have a gap between b_1^* and b_2^*; since b_2^* can be made arbitrarily large, this can be seen as a second gap.

Before describing the structure and contents of this paper in more detail we introduce some necessary concepts. Let Σ be a Heegaard surface of a compact 3-manifold M, and A an essential annulus properly embedded in M. The annulus A is called a *Haken annulus for* Σ (Definition 4.1) if it intersects Σ in a single simple closed curve that is essential in A. For an integer $c \geq 0$, the manifold obtained by drilling c curves simultaneously parallel to meridians of K out of $E(K)$ is denoted by $E(K)^{(c)}$ (note that $E(K)^{(0)} = E(K)$). The c tori $\partial E(K)^{(c)} \setminus \partial E(K)$ are denoted by $T_1, \dots, T_c$. There are c annuli properly embedded disjointly in $E(K)^{(c)}$, denoted by $A_1, \dots, A_c$, so that one component of ∂A_i is a meridian on $\partial E(K)$ and the other is a longitude of T_i ($i = 1, \dots, c$). (We note that in general these annuli are not uniquely determined up to isotopy.) Annuli with these properties are called *a complete system of Hopf annuli* (Definition 5.1). Let Σ be a Heegaard surface for $E(K)^{(c)}$. The Hopf annuli $A_1, \dots, A_c$ are called *a complete system of Hopf–Haken Annuli for* Σ (Definition 5.2) if $\Sigma \cap A_i$ is a single simple closed curve that is essential in A_i ($i = 1, \dots, c$).

Part II starts with Section 4 where we describe basic behavior of Haken annuli under amalgamation. In Section 5 we consider (g', b) decomposition of K (that is, b-bridge decomposition of K with respect to a genus g' Heegaard surface) and relate it to existence of Hopf–Haken Annuli. Specifically, we prove that K admits a $(g(E(K)) - c, c)$ decomposition if and only if $E(K)^{(c)}$ admits a complete system of Hopf–Haken Annuli for some Heegaard surface of genus $g(E(K))$ (Theorem 5.4).

In Section 6 we prove that given knots $K_1, \dots, K_n$ and integers $c_1, \dots, c_n \geq 0$ with $\sum_{i=1}^n c_i = n - 1$, $E(K_1 \# \cdots \# K_n)$ admits a system of $n - 1$ essential tori $\mathcal{T}$ (called *swallow follow tori*) so that the components of $E(K_1 \# \cdots \# K_n)$ cut open along $\mathcal{T}$ are homeomorphic to $E(K_1)^{(c_1)}, \dots, E(K_n)^{(c_n)}$. By amalgamating Heegaard surfaces of $E(K_1)^{(c_1)}, \dots, E(K_n)^{(c_n)}$ along the tori of $\mathcal{T}$ we obtain a Heegaard surface for $E(K_1 \# \cdots \# K_n)$; this implies this special case of Corollary 6.4:

$$g(E(K_1 \# \cdots \# K_n)) \leq \sum_{i=1}^n g(E(K_i)^{(c_i)}) - (n-1).$$

In the final section of Part II, Section 7, we combine these facts to prove that for each i we have:

$$\mathrm{gr}_t(K) \le 1 - i/b_i^*.$$

Thus we obtain the upper bound stated in Theorem 1.2.
To some degree, Part III complements Part II. We begin with Section 8 that complements Sections 4 and 5. As mentioned above, in Sections 4 and 5 we prove that K admits a $(g(E(K)) - c, c)$ decomposition if and only if $E(K)^{(c)}$ admits a complete system of Hopf–Haken Annuli for some Heegaard surface of genus $g(E(K))$. We are now ready to state the strong Hopf–Haken annulus theorem, which generalizes the Hopf–Haken annulus theorem (Theorem 6.3 of [Kobayashi and Rieck 2006a]), and is one of the highlights of this work. The proof is given in Section 8. For the definition of a Heegaard splitting of $(N; F_1, F_2)$ (where N is a manifold and F_1, F_2 are partitions of some of the components of ∂N), see Section 2 .

Theorem 1.8 (Strong Hopf–Haken annulus theorem). *For $i = 1, \dots, n$, let M_i be a compact connected orientable 3-manifold and $K_i \subset M_i$ be a knot. Suppose that $E(K_i) \ncong T^2 \times I$, that $E(K_i)$ is irreducible, and that $\partial N(K_i)$ is incompressible in $E(K_i)$. Let F_1, F_2 be a partition of some of the components of ∂M, where $M = \#_{i=1}^n M_i$. Let $c \ge 0$ be an integer. Then one of the following holds*:

(1) *There exists a minimal genus Heegaard surface for $(E(\#_{i=1}^n K_i)^{(c)}; F_1, F_2)$ admitting a complete system of Hopf–Haken annuli.*

(2) *For some $1 \le i \le n$, $E(K_i)$ admits an essential meridional surface S with $\chi(S) \ge 6 - 2g(E(\#_{i=1}^n K_i)^{(c)}; F_1, F_2)$.*

One curious consequence of Theorem 1.8 (which is proved in Section 8) is the following, where b_g^* is as in Notation 1.1:

Corollary 1.9. *Let $K \subset S^3$ be a connected sum of $n \ge 1$ m-small knots. Then for $c \ge b_g^*$,*

$$g(E(K)^{(c)}) = c.$$

Section 9 complements Section 6. Recall that in Section 6 we used swallow follow tori to show that given *any* collection of integers $c_1, \dots, c_n \ge 0$ whose sum is $n-1$ we have that $g(E(K_1 \# \cdots \# K_n)) \le \sum_{i=1}^n g(E(K_i)^{(c_i)}) - (n-1)$. In Section 9 we prove that if K_i is m-small for each i, then any Heegaard splitting for $E(K_1 \# \cdots \# K_n)$ admits an iterated weak reduction to $n-1$ swallow follow tori. This implies that any minimal genus Heegaard splitting admits an iterated weak reduction to *some* $n-1$ swallow follow tori that decompose $E(K_1 \# \cdots \# K_n)$ as $E(K_1)^{(c_1)}, \dots, E(K_n)^{(c_n)}$, giving *some* integers $c_1, \dots, c_n \ge 0$ whose sum is $n-1$. The integers $c_1, \dots, c_n$ are very special (see Example 9.3).

In Section 10, which complements Section 7, we combine these results to give a lower bound on the growth rate of the tunnel number of m-small knots. Given K, we "expect" that $g(E(K)^{(c)}) = g(E(K)) + c$; so we define the function f_K that measures to what extent $g(E(K)^{(c)})$ fails to behave "as expected":

$$f_K(c) = g(E(K)) + c - g(E(K)^{(c)}).$$

For any knot K and any integer $c \geq 0$, we show that f_K fulfills

$$f_K(0) = 0 \text{ and } f_K(c) \leq f_K(c+1) \leq f_K(c) + 1.$$

We study f_K for m-small knots, calculating it exactly in terms of the bridge indices of K (Proposition 10.4). In particular, for m-small knots, f_K is bounded. In fact, for large enough c, Proposition 10.4 implies

$$f_K(c) = g(E(K)) - g(M).$$

We do not know much about the behavior of f_K in general; for example, we do not know if there exists a knot for which f_K is unbounded (see Question 10.5).

We express the growth rate of tunnel number of m-small knots in terms of f_K by showing (Corollary 10.3) that

$$\frac{g(E(nK)) - ng(E(K)) + n - 1}{n-1} = 1 - \frac{\max\left\{\sum_{i=1}^{n} f_K(c_i)\right\}}{n-1},$$

where the maximum is taken over all collections of integers $c_1, \ldots, c_n \geq 0$ whose sum is $n-1$. The growth rate is then the limit superior of this sequence. We combine this interpretation of the growth rate with the calculation of f_K to obtain the exact calculation of the growth rate of m-small knots stated in Theorem 1.2.

2. Preliminaries

By *manifold* we mean a smooth 3-dimensional manifold. All manifolds considered are assumed to be connected orientable and compact. We assume the reader is familiar with the basic terms of 3-manifold topology (see, for example, [Schultens 2014; Jaco 1980; Hempel 1976]). Thus we assume the reader is familiar with terms such as compression, boundary compression, boundary parallel, and essential surface.

We use the notation ∂, cl, and int to denote boundary, closure, and interior, respectively. For a submanifold H of a manifold M, $N(H, M)$ denotes a closed regular neighborhood of H in M. When M is understood from context we often abbreviate $N(H, M)$ to $N(H)$.

By a *knot* K in a 3-manifold M we mean a smooth embedding of S^1 into M, taken up to ambient isotopy. $E(K)$, the *exterior* of K, is $\text{cl}(M \setminus N(K))$. The slope on the torus $\partial E(K) \setminus \partial M = \partial N(K)$ that bounds a disk in $N(K)$ is called the *meridian* of K. A knot K is called *m-small* if there is no essential meridional surface in $E(K)$, that is, there is no essential surface $S \subset E(K)$ with nonempty boundary so that ∂S consists of meridians of K.

We assume the reader is familiar with the basic terms regarding Heegaard splittings, such as handlebody, compression body, meridian disk, etc. Recall that a compression body C is a connected 3-manifold obtained from $F \times [0, 1]$ (where here F is a possibly empty disjoint union of closed surfaces) and a (possibly empty) collection of 3-balls by attaching 1-handles to $F \times \{1\}$ and the boundary of the balls. Following standard conventions, we refer to $F \times \{0\}$ as $\partial_- C$ and $\partial C \setminus \partial_- C$ as $\partial_+ C$. We use the notation $C_1 \cup_\Sigma C_2$ for the Heegaard splitting given by the compression bodies C_1 and C_2. The basic concepts of reductions of a Heegaard splitting are summarized here:

Definitions 2.1. (1) A Heegaard splitting $C_1 \cup_\Sigma C_2$ is called *stabilized* if there exist meridian disks $D_1 \subset C_1$ and $D_2 \subset C_2$ such that ∂D_1 intersects ∂D_2 transversely (as submanifolds of Σ) in one point. Otherwise, the Heegaard splitting is called *nonstabilized.*

(2) A Heegaard splitting $C_1 \cup_\Sigma C_2$ is called *reducible* if there exist meridian disks $D_1 \subset C_1$ and $D_2 \subset C_2$ such that $\partial D_1 = \partial D_2$. Otherwise, the Heegaard splitting is called *irreducible.*

(3) A Heegaard splitting $C_1 \cup_\Sigma C_2$ is called *weakly reducible* if there exist meridian disks $D_1 \subset C_1$ and $D_2 \subset C_2$ such that $\partial D_1 \cap \partial D_2 = \varnothing$. Otherwise the splitting is called *strongly irreducible.*

(4) A Heegaard splitting $C_1 \cup_\Sigma C_2$ is called *trivial* if C_1 or C_2 is a trivial compression body, that is, a compression body with no 1-handles. Otherwise the Heegaard splitting is called *nontrivial.*

Let $C_1 \cup_\Sigma C_2$ be a weakly reducible Heegaard splitting of a manifold M. Let $\Delta_i \subset C_i$ be a non empty set of disjoint meridian disks so that $\Delta_1 \cap \Delta_2 = \varnothing$. By *weak reduction* along $\Delta_1 \cup \Delta_2$ we mean the (possibly disconnected) surface obtained by first compressing Σ along $\Delta_1 \cup \Delta_2$, and then removing any component that is contained in C_1 or C_2. Casson and Gordon [1987] showed that if an irreducible Heegaard splitting is weakly reducible, then an appropriately chosen weak reduction yields a (possibly disconnected) essential surface, say, F.

With F as in the previous paragraph, let $M_1, \dots, M_k$ be the components of M cut open along F. It is well known that Σ induces a Heegaard surface on each M_i, say, Σ_i. We say that Σ is obtained by *amalgamating* $\Sigma_1, \dots, \Sigma_k$. This is a special case of amalgamation; the general definition will be given below as the converse of iterated weak reduction. The genus after amalgamation is given in the following lemma; see Remark 2.7 of [Schultens 1993] for the case $m = 1$ (we leave the proof of the general case to the reader):

Lemma 2.2. *Let $C_1 \cup_\Sigma C_2$ be a weakly reducible Heegaard splitting and suppose that after weak reduction we obtain F (as above). Suppose that M cut open along*

F consists of two components, and denote the induced Heegaard splittings by $C_1^{(1)} \cup_{\Sigma_1} C_2^{(1)}$ and $C_1^{(2)} \cup_{\Sigma_2} C_2^{(2)}$. Let $F_1, \dots, F_m$ be the components of F. Then,

$$g(\Sigma) = g(\Sigma_1) + g(\Sigma_2) - \sum_{i=1}^{m} g(F_i) + (m-1).$$

In particular, if F is connected then $g(\Sigma) = g(\Sigma_1) + g(\Sigma_2) - g(F)$.

It is distinctly possible that not all the Heegaard splittings induced by weak reduction are strongly irreducible. When that happens we may weakly reduce some (possibly all) of the induced Heegaard splittings, and repeat this process. We refer to this as *repeated* or *iterated* weak reduction. The converse is called amalgamation. Scharlemann and Thompson [1994] proved that any Heegaard splitting admits a repeated weak reduction so that the induced Heegaard splittings are all strongly irreducible; we refer to this as *untelescoping*.

Let N be a manifold and $\{F_1, F_2\}$ be a partition of some components of ∂N. Note that we do *not* require every component of ∂N to be in F_1 or F_2. We say that $C_1 \cup_\Sigma C_2$ is a Heegaard splitting of $(N; F_1, F_2)$ if $F_1 \subset \partial_- C_1$ and $F_2 \subset \partial_- C_2$. We extend the terminology of Heegaard splittings to this context, so, for example, $g(N; F_1, F_2)$ is the genus of a minimal genus Heegaard splitting of $(N; F_1, F_2)$.

The following proposition allows us, in some cases, to consider weak reduction instead of iterated weak reduction. The proof is simple and left to the reader.

Proposition 2.3. *Let F be a component of the surface obtained by repeated weak reduction of $C_1 \cup_{\Sigma_1} C_2$. If F is separating, then some weak reduction of $C_1 \cup_{\Sigma_1} C_2$ yields exactly F.*

3. Relative Heegaard surfaces

In this section we study relative Heegaard surfaces. The results of this section will be used in Section 8 and the reader may postpone reading it until that section. Let $b \geq 1$ be an integer and T be a torus. For $1 \leq i \leq 2b$, let $A_i \subset T$ be an annulus. We say that $\{A_1, \dots, A_{2b}\}$ gives a *decomposition of T into annuli* (or simply a *decomposition of T*) if the following two conditions hold:

(1) $\bigcup_{i=1}^{2b} A_i = T$, and

(2) (a) If $b > 1$, then $A_i \cap A_j = \varnothing$ whenever $i \neq j$ are nonconsecutive integers (modulo $2b$), and $A_i \cap A_{i+1} = \partial A_i \cap \partial A_{i+1}$ is a single simple closed curve.
   (b) If $b = 1$, then $A_1 \cap A_2 = \partial A_1 = \partial A_2$.

We begin by defining a relative Heegaard surface; note that the definition can be made more general by considering an arbitrary collection of boundary components (below we only consider a single torus) and a decomposition into arbitrary subsurfaces (below we only consider annuli); however Definition 3.1 suffices for our purposes:

Definition 3.1 (relative Heegaard surface). Let M be a compact connected orientable 3-manifold and T a torus component of ∂M. Let $\{A_1, \dots, A_{2b}\}$ be a decomposition of T into annuli. A compact surface $S \subset M$ is called a *Heegaard surface for M relative to* $\{A_1, \dots, A_{2b}\}$ (or simply a *relative Heegaard surface,* when no confusion may arise) if the following conditions hold:

(1) $\partial S = \bigcup_{i=1}^{2b} \partial A_i$.

(2) M cut open along S consists of two components (say, C_1 and C_2).

(3) For $i = 1, 2$, C_i admits a set of compressing disks Δ_i with $\partial \Delta_i \subset S$, so that C_i compressed along Δ_i consists of
   - (a) exactly b solid tori, each containing exactly one A_i as a longitudinal annulus;
   - (b) a (possibly empty) collection of collar neighborhoods of components of $\partial M \setminus T$;
   - (c) a (possibly empty) collection of balls.

The genus of a minimal genus relative Heegaard surface is called the *relative genus.*

For an integer $c \geq 1$, let $Q^{(c)}$ be (an annulus with c holes)$\times S^1$. (To avoid confusion we remark that $Q^{(c)}$ can be described as (a sphere with $c+2$ holes)$\times S^1$, but in the context of this paper an annulus is more natural.) Note that $Q^{(c)}$ admits a unique Seifert fibration. Our goal is to calculate the genus of $Q^{(c)}$ relative to a given decomposition of a component of $\partial Q^{(c)}$ into annuli. We say that slopes β and γ of a torus are *complementary* if they are represented by simple closed curves that intersect each other transversely once.

Proposition 3.2. *Let $\{A_1, \dots, A_{2b}\}$ be a decomposition of a component of $\partial Q^{(c)}$ (say, T) into annuli, and denote the slope defined by these annuli by β. Denote the slope defined by the Seifert fibers on T by γ. Then,*

(1) *when β and γ are complementary slopes, the genus of $Q^{(c)}$ relative to $\{A_1,\dots,A_{2b}\}$ is c;*

(2) *when β and γ are not complementary slopes, the genus of $Q^{(c)}$ relative to $\{A_1,\dots,A_{2b}\}$ is $c+1$.*

We immediately obtain:

Corollary 3.3. *The surfaces in Figure 1 are minimal genus Heegaard splittings for $Q^{(c)}$ relative to $\{A_1, \dots, A_{2b}\}$; Figure 1 (left) is of complementary slopes and Figure 1 (right) is of noncomplementary slopes.*

We postpone the proof of Proposition 3.2 to the end of this section, as it will be an application of the next proposition which is of independent interest. We fix the following notation: glue $Q^{(b)}$ to $Q^{(c)}$ along a single boundary component and

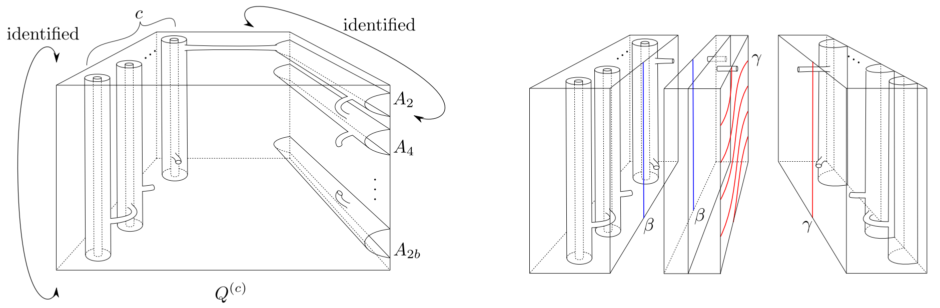


Figure 1. Relative Heegaard surfaces.

denote the slope of the Seifert fiber of $Q^{(b)}$ on the torus $Q^{(b)} \cap Q^{(c)}$ by β and the slope of the Seifert fiber of $Q^{(c)}$ by γ. The manifold obtained is denoted $Q^{(b,c)}_{\beta,\gamma}$.

Proposition 3.4. *The genus of $Q^{(b,c)}_{\beta,\gamma}$ satisfies the following*:

(1) *If β and γ are complementary slopes*, *then* $g(Q^{(b,c)}_{\beta,\gamma}) = b + c$.

(2) *If β and γ are not complementary slopes*, *then* $g(Q^{(b,c)}_{\beta,\gamma}) = b + c + 1$.

We immediately obtain:

Corollary 3.5. *The surfaces in Figure 2* (*left*) *and in Figure 2* (*right*) *are minimal genus Heegaard splittings for $Q^{(b,c)}_{\beta,\gamma}$ corresponding to* (1) *and* (2) *of Proposition 3.4*, *respectively.*

A surface in a Seifert fibered space is called *vertical* if it is everywhere tangent to the fibers and *horizontal* if it is everywhere transverse to the fibers. It is well known that given an essential surface in a Seifert fibered space we may assume it is vertical or horizontal; see, for example, [Jaco 1980].

Proof of Proposition 3.4. The surfaces in Figure 2 are Heegaard surfaces for $Q^{(b,c)}_{\beta,\gamma}$, showing the following, which we record here for future reference:

Remark 3.6. When β and γ are complementary, $g(Q^{(b,c)}_{\beta,\gamma}) \leq b + c$. When β and γ are not complementary, $g(Q^{(b,c)}_{\beta,\gamma}) \leq b + c + 1$.

Hence we only need to show that when β and γ are complementary, $g(Q^{(b,c)}_{\beta,\gamma}) \geq b + c$ and when β and γ are not complementary, $g(Q^{(b,c)}_{\beta,\gamma}) \geq b + c + 1$.

If $\beta = \gamma$ then $Q^{(b,c)}_{\beta,\gamma}$ is a $(b + c)$-times punctured annulus cross S^1 and the result was proved by Schultens [1993]. For the remainder of the proof we assume that $\beta \neq \gamma$. Then $Q^{(b,c)}_{\beta,\gamma}$ is a graph manifold whose underlying graph consists of two vertices connected by a single edge. We apply [Schultens 2004, Theorem 1.1] and refer the reader to that paper for notation and details. Following Schultens' notation, we decompose $Q^{(b,c)}_{\beta,\gamma}$ along two parallel copies of $Q^{(b)} \cap Q^{(c)}$ as $Q^{(b,c)}_{\beta,\gamma} = Q_b \cup M_e \cup Q_c$. Q_b and Q_c are called the *vertex manifolds* and M_e is the *edge manifold*. Note that $Q_b \cong Q^{(b)}$, $M_e \cong T^2 \times [0, 1]$, and $Q_c \cong Q^{(c)}$.

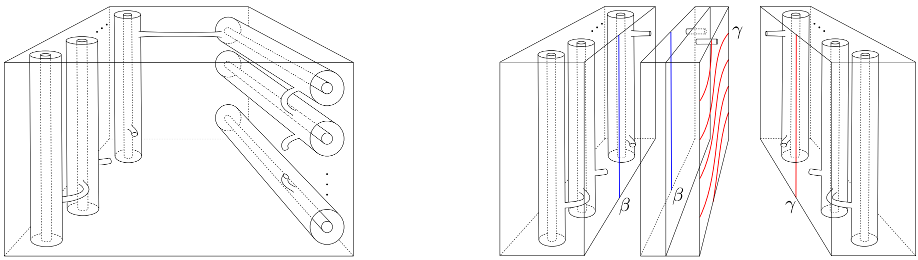


Figure 2. Heegaard surfaces for $Q^{(b,c)}_{\beta,\gamma}$.

Let S be a minimal genus Heegaard splitting for $Q^{(b,c)}_{\beta,\gamma}$. In the following claim we analyze completely what happens when $g(S)=2$ or when S is strongly irreducible:

Claim 3.7. The following three conditions are equivalent:

(1) S is strongly irreducible.

(2) β and γ are complementary, $g(S)=2$, and $b=c=1$.

(3) $g(S)=2$.

Proof of Claim 3.7. (1) implies (2). Suppose that S is strongly irreducible. By [Schultens 2004] we may assume that S is standard. In particular, $S\cap Q_b$ (respectively, $S\cap Q_c$) is either horizontal, pseudohorizontal, vertical, or pseudovertical. However, the first two cases are impossible as they require S to meet every boundary component of Q_b (respectively, Q_c). Hence $S\cap Q_b$ and $S\cap Q_c$ consist of vertical or pseudovertical components. In particular, the intersection of S with the torus $Q_b\cap M_e$ (respectively, $Q_c\cap M_e$) is a Seifert fiber of Q_b (respectively, Q_c).

Assume first that $S\cap M_e$ is as in [Schultens 2004, Theorem 1.1(1)], that is, $S\cap M_e$ is obtained from a collection of incompressible annuli, say, $\mathcal{A}$, by tubing along at most one boundary parallel arc (in [Schultens 2004], tubings are referred to as 1-*surgery*). Suppose that $\mathcal{A}$ consists of boundary parallel annuli. Since the tubing is performed, if at all, along a boundary parallel arc, we see that no component of $S\cap M_e$ connects the components of ∂M_e. This contradicts the fact that S is connected and must meet both Q_b and Q_c. Hence some component of $\mathcal{A}$ meets both components of ∂M_e, showing that $\beta=\gamma$, contradicting our assumption.

Hence [Schultens 2004, Theorem 1.1(2)] holds, and $S\cap M_e$ consists of a single component that is obtained by tubing together two boundary parallel annuli, one at each boundary component of M_e; moreover, [Schultens 2004, Theorem 1.1] shows that these annuli define complementary slopes. See Figure 3 (left). As argued above, the slopes defined by these annuli are β and γ. This gives the first condition of (2).

On the right side of Figure 3 we see two surfaces. One is $S\cap M_e$, and in its center we marked the boundary of the obvious compressing disk. It is easy to see that the other surface is isotopic to $S\cap M_e$. On it we marked the boundary of four

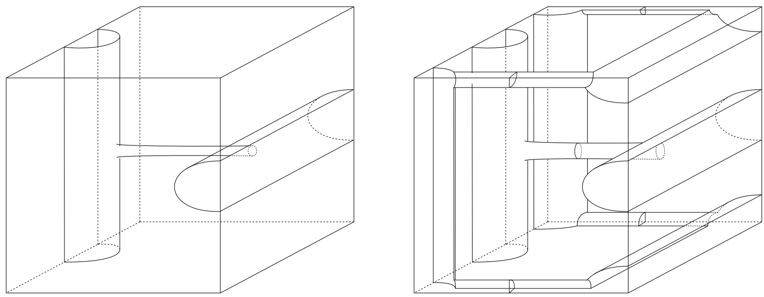


Figure 3. Heegaard surfaces in M_e.

disks, each shaped like a 90° sector. After gluing opposite sides of the cube to M_e, these sectors form a compressing disk on the opposite side of the obvious disk. This demonstrates that $S \cap M_e$ compresses into both sides. If $S \cap Q_b$ is pseudovertical then it compresses, and together with one of the compressing disks for $S \cap M_e$ we obtain a weak reduction, contradicting our assumption. Hence $S \cap Q_b$ consists of annuli; similarly, $S \cap Q_c$ consists of annuli. Hence,

$$\chi(S) = \chi(S \cap M_e) = -2.$$

The second condition of (2) follows.

Since $g(S) = 2$, $\partial Q_{\beta,\gamma}^{(b,c)}$ consists of at most four tori. On the other hand, $\partial Q_{\beta,\gamma}^{(b,c)}$ consists of $b + c + 2$ tori, for $b, c \geq 1$. Hence $b = c = 1$, fulfilling the third and final condition of (2). This completes the proof that (1) implies (2).

It is trivial that (2) implies (3).

To see that (3) implies (1), assume that S weakly reduces. Since S is a minimal genus Heegaard surface and $g(S) = 2$, an appropriate weak reduction yields an essential sphere, which contradicts the fact that $Q_{\beta,\gamma}^{(b,c)}$ is irreducible.

This completes the proof of Claim 3.7. □

If S is strongly irreducible, Proposition 3.4 follows from Claim 3.7. For the reminder of the proof we assume, as we may, that S weakly reduces to a (possibly disconnected) essential surface, say, F. By the construction of $Q_{\beta,\gamma}^{(b,c)}$ we see that every component of F separates; hence by Proposition 2.3 we may assume that F is connected. Recall that we assumed that $\beta \neq \gamma$. This clearly implies that we may suppose that (after isotopy if necessary) F is disjoint from the torus $Q^{(b)} \cap Q^{(c)}$; without loss of generality we assume that $F \subset Q^{(b)}$.

We induct on $b + c$.

Base case: $b + c = 2$. Note that in the base case $b = c = 1$. It is easy to see that the only connected essential surface in $Q_{\beta,\gamma}^{(1,1)}$ is the torus $Q^{(b)} \cap Q^{(c)}$. Hence F is isotopic to this surface and the weak reduction induces Heegaard splittings Σ_b and Σ_c on $Q^{(b)}$ and $Q^{(c)}$, respectively; note that both $Q^{(b)}$ and $Q^{(c)}$ are homeomorphic to $Q^{(1)}$. By Schultens [1993], $g(Q^{(1)}) = 2$. By Lemma 2.2, amalgamation gives

$$g(Q^{(1,1)}_{\beta,\gamma}) = g(S) = g(\Sigma_b) + g(\Sigma_c) - g(F) \geq g(Q^{(1)}) + g(Q^{(1)}) - g(F) = 2+2-1 = 3.$$

By Remark 3.6, if β and γ are complementary slopes then $g(Q^{(1,1)}_{\beta,\gamma}) \leq 2$; hence β and γ are not complementary slopes and together with Remark 3.6 the proposition follows in this case.

Inductive case: $b + c > 2$**.** Assume, by induction, that the proposition holds for any integers b', $c' > 0$, with $b' + c' < b + c$.

Case One: *F is isotopic to $Q^{(b)} \cap Q^{(c)}$.* Then weak reduction induces Heegaard splittings on $Q^{(b)}$ and $Q^{(c)}$. Similar to the argument above (using that $g(Q^{(b)}) = b+1$ and $g(Q^{(c)}) = c + 1$ by [Schultens 1993]) we have

$$g(Q^{(b,c)}_{\beta,\gamma}) \geq g(Q^{(b)}) + g(Q^{(c)}) - g(F) = b + c + 1.$$

As in the base case it follows from Remark 3.6 that β and γ are not complementary slopes. Together with Remark 3.6, the proposition follows in this case.

Case Two: *F is not isotopic to $Q^{(b)} \cap Q^{(c)}$.* Then F is essential in $Q^{(b)}$ and is therefore isotopic to a vertical or horizontal surface. Since F is closed and $\partial Q^{(b)} \neq \emptyset$, we have that F cannot be horizontal. We conclude that F is a vertical torus and decomposes $Q^{(b)}$ as $Q^{(b')}$ (for some $b' < b$) and a disk with $b - b' + 1$ holes cross S^1. By induction, the genus of $Q^{(b',c)}_{\beta,\gamma}$ fulfills the conclusion of Proposition 3.4; by [Schultens 1993], the genus of a disk with $b - b' + 1$ holes cross S^1 is $b - b' + 1$, and similar to the argument above we get

$$g(Q^{(b,c)}_{\beta,\gamma}) \geq g(Q^{(b',c)}_{\beta,\gamma}) + (b - b' + 1) - 1 = g(Q^{(b',c)}_{\beta,\gamma}) + b - b'.$$

Together with Remark 3.6, this completes the proof of Proposition 3.4. □

We are now ready to prove Proposition 3.2:

Proof of Proposition 3.2. The surfaces in Figure 1 are relative Heegaard surfaces realizing the values given in Proposition 3.2. To complete the proof we only need to show that these surfaces realize the minimal relative genus.

Let Σ be a minimal genus Heegaard surface for $Q^{(c)}$ relative to $\{A_1, \ldots, A_{2b}\}$. By tubing $\partial\Sigma$ along the annuli A_{2i} and drilling a curve parallel to the core of A_{2i} ($i = 1, \ldots, b$; recall Figure 1) we obtain a Heegaard surface for $Q^{(b,c)}_{\beta,\gamma}$ of genus $g(S) + b$. Thus $g(\Sigma) \geq g(Q^{(b,c)}_{\beta,\gamma}) - b$. By Proposition 3.4, when β and γ are complementary $g(Q^{(b,c)}_{\beta,\gamma}) = b + c$ and when β and γ are not complementary $g(Q^{(b,c)}_{\beta,\gamma}) = b + c + 1$. Thus we see that $g(\Sigma) \geq c$ (when the β and γ are complementary) and $g(\Sigma) \geq c + 1$ (otherwise).

This completes the proof of Proposition 3.2. □

Part II. An upper bound on the growth rate of the tunnel number of knots

4. Haken annuli

A primary tool in our study is the use of Haken annuli. Haken annuli were first defined in [Kobayashi and Rieck 2006a], where only a single annulus was considered. We generalize the definition to a collection of annuli below. Note the similarity between a Haken annulus and a Haken sphere or Haken disk (by a *Haken sphere* we mean a sphere that meets a Heegaard surface in a single simple closed curve that is essential in the Heegaard surface, see [Haken 1968] or [Jaco 1980, Chapter 2], and by a *Haken disk* we mean a disk that meets a Heegaard surface in a single simple closed curve that is essential in the Heegaard surface [Casson and Gordon 1987]).

Definition 4.1. Let $C_1 \cup_\Sigma C_2$ be a Heegaard splitting of a manifold M. A collection of essential annuli $\mathcal{A} \subset M$ are called *Haken annuli* for $C_1 \cup_\Sigma C_2$ (or simply *Haken annuli,* when no confusion may arise) if for every annulus $A \in \mathcal{A}$ we have that $A \cap \Sigma$ consists of a single simple closed curve that is essential in A.

Remark 4.2. For an integer $n \geq 2$, let $D(n)$ be (a disk with n holes)$\times S^1$ and denote the components of $\partial D(n)$ by $T_0, T_1, \ldots, T_n$. By the construction of minimal genus Heegaard splittings given in the proof of Proposition 2.14 of [Kobayashi and Rieck 2006a], we see that for each positive integer p with $1 \leq p \leq n$ there is a genus n Heegaard surface of $(D(n); \bigcup_{i=0}^{p-1} T_i, \bigcup_{i=p}^{n} T_i)$ which admits a collection $\{A_1, \ldots, A_p\}$ of Haken annuli connecting T_i to T_n ($i = 0, \ldots, p-1$). By Schultens [1993], we see that this is a minimal genus Heegaard splitting of $D(n)$. See Figure 4.

In Propositions 3.5 and 3.6 of [Kobayashi and Rieck 2006a] we studied the behavior of Haken annuli under amalgamation. We generalize these propositions as Proposition 4.3 below. We first explain the construction that is used in Proposition 4.3. Let $C_1 \cup_\Sigma C_2$ be a Heegaard splitting for a manifold M that weakly reduces to a (possibly disconnected) essential surface F. Suppose that M cut open along F consists of two components, say, $M^{(i)}$ ($i = 1, 2$). We

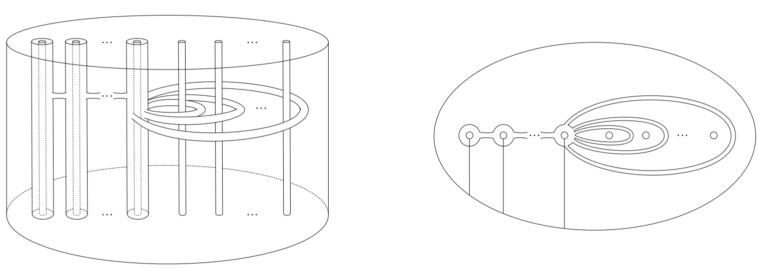


Figure 4. Heegaard surface in $D(n)$.

denote the image of F in $M^{(i)}$ by $F^{(i)}$ and the Heegaard splitting induced on $M^{(i)}$ by $C_1^{(i)} \cup_{\Sigma^{(i)}} C_2^{(i)}$. Suppose there are Haken annuli for $C_1^{(i)} \cup_{\Sigma^{(i)}} C_2^{(i)}$, say, $\mathscr{A}^{(i)}$, satisfying these conditions:

- There exists a unique component of $\mathscr{A}^{(1)}$, say, $A^{(1)}$, which intersects $F^{(1)}$ in a single simple closed curve, and other components are disjoint from $F^{(1)}$.
- Each component of $\mathscr{A}^{(2)}$ intersects $F^{(2)}$ in a single simple closed curve isotopic in F to $A^{(1)} \cap F^{(1)}$.

Then let $\tilde{\mathscr{A}}^{(1)}$ be a collection of mutually disjoint annuli obtained from $\mathscr{A}^{(1)}$ by substituting $A^{(1)}$ with $|\mathscr{A}^{(2)}|$ parallel copies of $A^{(1)}$ whose boundaries are identified with $\mathscr{A}^{(2)} \cap F^{(2)}$. Finally, let $\tilde{\mathscr{A}}$ equal $\tilde{\mathscr{A}}^{(1)} \cup \mathscr{A}^{(2)}$. Note that $\tilde{\mathscr{A}}$ is a system of mutually disjoint annuli properly embedded in M. It is easy to adopt the proofs of Propositions 3.5 and 3.6 of [Kobayashi and Rieck 2006a] and obtain:

Proposition 4.3. *Let M, $C_1 \cup_\Sigma C_2$, and $\tilde{\mathscr{A}}$ be as above. Then the components of $\tilde{\mathscr{A}}$ form Haken annuli for $C_1 \cup_\Sigma C_2$.*

5. Various decompositions of knot exteriors

In this section we compare two structures: Hopf–Haken annuli and (h, b) decompositions. After defining the two we prove (Theorem 5.4) that they are equivalent.

Let K be a knot in a 3-manifold M and $h \geq 0$, $b \geq 1$ be integers. We say that K admits a (h, b) *decomposition* (some authors use the term genus h, b-bridge position) if there exists a genus h Heegaard splitting $C_1 \cup_\Sigma C_2$ of M such that $K \cap C_i$ is a collection of b simultaneously boundary parallel arcs ($i = 1, 2$; note that in this paper we do not consider $(h, 0)$ decomposition).

Let K be a knot in a compact manifold M. Recall that $E(K)^{(c)}$ is obtained from $E(K)$ by removing c curves that are simultaneously isotopic to meridians of K. The trace of the isotopy forms c annuli which motivates the definition below (Definitions 5.1 and 5.2 generalize Definition 6.1 of [Kobayashi and Rieck 2006a]):

Definition 5.1 (a complete system of Hopf annuli). Let $K \subset M$ be a knot in a compact manifold and $c > 0$ be an integer. Let $A_1, \dots, A_c$ be annuli disjointly embedded in $E(K)^{(c)}$ so that for each i, one component of ∂A_i is a meridian of $\partial N(K)$ and the other is a longitude of T_i (recall $T_1, \dots, T_c$ denote the components of $\partial E(K)^{(c)} \setminus \partial E(K)$). Then $\{A_1, \dots, A_c\}$ is called a *complete system of Hopf annuli*. We emphasize that the complete system of Haken annuli for $E(K)^{(c)}$ is *not* unique up to isotopy.

Definition 5.2 (a complete system of Hopf–Haken annuli). Let $K \subset M$ be a knot in a compact manifold, $c > 0$ be an integer, Σ be a Heegaard surface for $E(K)^{(c)}$, and $\{A_1, \dots, A_c\}$ be a complete system of Hopf annuli. $\{A_1, \dots, A_c\}$ is called a

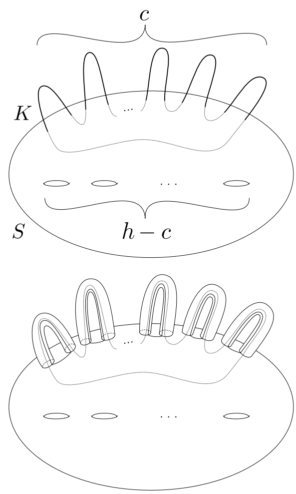


Figure 5. Tubing a $(h-c, c)$-decomposition.

complete system of Hopf–Haken annuli for Σ if for each i, $\Sigma \cap A_i$ is a single simple closed curve that is essential in A_i.

Definition 5.3 (tubing bridge decomposition). Let $K \subset M$ be a knot in a compact manifold, Σ a Heegaard surface for $E(K)$, and $c > 0$ an integer. Suppose that there exists a genus $h-c$ Heegaard surface for M (say, S) so that K is c-bridge with respect to S, and the surface obtained by tubing S along c arcs of K cut along S on one side of S is isotopic to Σ. Then we say that Σ is obtained by *tubing S to one side (along K)*. See Figure 5.

Theorem 5.4. *Let M be a compact manifold and $K \subset M$ be a knot and suppose the meridian of K does not bound a disk in $E(K)$. Let c and h be positive integers. The following two conditions are equivalent*:

(1) *K admits an $(h-c, c)$ decomposition.*

(2) *$E(K)^{(c)}$ admits a genus h Heegaard splitting that admits a complete system of Hopf–Haken annuli.*

Proof. (1) $\Longrightarrow$ (2): Let $S \subset M$ be a surface defining a $(h-c, c)$ decomposition. Then S separates M into two sides, say, "above" and "below". Pick one, say, above. Since the arcs of K above S form c boundary parallel arcs (say, $\alpha_1, \ldots, \alpha_c$), there are c disjointly embedded disks above K (say, $D_1, \ldots, D_c$) so that ∂D_i consists of two arcs, one α_i and the other along S (for this proof, see Figure 5). Tubing S c times along $\alpha_1, \ldots, \alpha_c$, we obtain a Heegaard surface for $E(K)$ (say, Σ). We may assume that the tubes are small enough so that they intersect each D_i in a single spanning arc. Denote the compression bodies obtained by cutting $E(K)$

along Σ by C_1 and C_2 with $\partial N(K) \subset \partial_- C_1$. Then each $D_i \cap C_2$ is a meridional disk. Let $A_1, \dots, A_c$ be c meridional annuli properly embedded in C_1 near the maxima of K. Then $\left(\bigcup_i A_i\right) \cap \partial N(K)$ consists of c meridians, say, $\alpha'_1, \dots, \alpha'_c$. For each i, we isotope α'_i along the annulus A_i to the curve $A_i \cap \Sigma$ and then push it slightly into C_2, obtaining c curves, say, $\beta_1, \dots, \beta_c$, parallel to meridians. Drilling $\bigcup_i \beta_i$ out of $E(K)$ gives $E(K)^{(c)}$. Using the disks $D_i \cap C_2$ it is easy to see that Σ is a Heegaard surface for $E(K)^{(c)}$. Clearly, the trace of the isotopy from $\bigcup_{i=1}^n \alpha'_i$ to $\bigcup_{i=1}^n \beta_i$ forms a complete system of Hopf annuli, and by construction every one of these annuli intersects Σ in a single curve that is essential in the annulus. This completes the proof of (1) $\Longrightarrow$ (2).

(2) $\Longrightarrow$ (1): Assume that $E(K)^{(c)}$ admits a Heegaard surface of genus h, say, Σ, with a complete system of Hopf–Haken annuli, say, $\{A_1, \dots, A_c\}$. Let

$$E(K)' = \mathrm{cl}\big(E(K)^{(c)} \setminus \textstyle\bigcup_i N(A_i)\big).$$

Note that $E(K)'$ is homeomorphic to $E(K)$. Let S' be the meridional surface $\Sigma \cap E(K)'$. We may consider M as obtained from $E(K)'$ by meridional Dehn filling and K as the core of the attached solid torus. By capping off S' we obtain a closed surface $S \subset M$. The following claim completes the proof of (2) $\Longrightarrow$ (1):

Claim 5.5. S defines a $(h-c, c)$ decomposition for K.

Proof of claim. Recall that the components of $\partial E(K)^{(c)} \setminus \partial E(K)$ were denoted by $T_1, \dots, T_c$, as in Definition 5.2, so that $A_i \cap T_i \neq \varnothing$ and $A_i \cap T_j = \varnothing$ (for $i \neq j$). Let C_1, C_2 be the compression bodies obtained from $E(K)^{(c)}$ by cutting along Σ, where $\partial N(K) \subset \partial_- C_1$. Since $\Sigma \cap A_i$ is a single simple closed curve which is essential in A_i we have $T_i \subset \partial_- C_2$ $(i = 1, \dots, c)$. Denote the annulus $A_j \cap C_i$ by $A_{i,j}$ $(i = 1, 2,\ j = 1, \dots, c)$.

Let $C'_i = C_i \cap E(K)'$ $(i = 1, 2)$. It is clear that S' cuts $E(K)'$ into C'_1 and C'_2. Since $A_i \cap \partial N(K)$ is a meridian of K, and by assumption the meridian of K does not bound a disk in $E(K)$, we have that $A_{i,j}$ is incompressible in C_i. Hence a standard innermost disk, outermost arc argument shows that there is a system of meridian disks $\mathcal{D}_i$ of C_i which cuts C_i into $\partial_- C_i \times [0, 1]$ such that $\mathcal{D}_i \cap \left(\bigcup A_{i,j}\right) = \varnothing$.

Now we consider C_2 cut along $\bigcup A_{2,j}$. Since $\mathcal{D}_2 \cap \left(\bigcup A_{2,j}\right) = \varnothing$, there are components $T_1 \times [0, 1], \dots, T_c \times [0, 1]$ of C_2 cut along $\mathcal{D}_2$, where $A_{2,j} \subset T_j \times [0, 1]$ $(j = 1, \dots, c)$. Here we note that $T_j \times [0, 1]$ cut along $A_{2,j}$ is a solid torus in which the image of $T_j \times \{0\}$ is a longitudinal annulus (note that the image of $T_j \times \{0\}$ is exactly $T_j \cap C'_2$). This shows that $\{T_1 \cap C'_2, \dots, T_c \cap C'_2\}$ is a primitive system of annuli in C'_2, that is, there is a system of meridian disks $D_{2,1}, \dots, D_{2,c}$ in C'_2 such that $D_{2,j} \cap (T_j \cap C'_2)$ consists of a spanning arc of $T_j \cap C'_2$, and $D_{2,j} \cap (T_k \cap C'_2) = \varnothing$ $(j \neq k)$. Let C''_2 be the manifold obtained from C'_2 by adding c 2-handles along $T_1 \cap C'_2, \dots, T_c \cap C'_2$. Since $\{T_1 \cap C'_2, \dots, T_c \cap C'_2\}$ is primitive, C''_2 is a genus

$(h-c)$ compression body, and the union of the co-cores of the attached 2-handles, which can be regarded as $K \cap C_2''$, are simultaneously isotopic (through the disks $\bigcup D_{2,j}$) into $\partial_+ C_2''$.

Analogously since $\mathcal{D}_1 \cap \left(\bigcup A_{1,j}\right) = \varnothing$, there are c components of C_1 cut by $\mathcal{D}_1 \cup \left(\bigcup A_{1,j}\right)$ which are solid tori such that $\partial N(K)$ intersects each solid torus in a longitudinal annulus. Then the arguments in the last paragraph show that $K \cap C_1''$ consists of c arcs which are simultaneously parallel to S.

These show that S gives a $(h-c, c)$ decomposition for K, completing the proof of the claim, and thus also of Theorem 5.4. □

Corollary 5.6. *Let K be a knot in a compact manifold M, and suppose that for some positive integers h and c, K admits a $(h-c, c)$ decomposition. Then,*

$$g(E(K)^{(c)}) \leq h.$$

Proof. This follows immediately from (1) $\Longrightarrow$ (2) of Theorem 5.4. □

6. Existence of swallow follow tori and bounding $g(E(K_1\#\cdots\#K_n)^{(c)})$ above

Definition 6.1 (swallow follow torus). Let $K \subset M$ be a knot and $c \geq 0$ an integer. An essential separating torus $T \subset E(K)^{(c)}$ is called a *swallow follow torus* if there exists an embedded annulus $A \subset E(K)^{(c)}$ with one component of ∂A a meridian of $E(K)^{(c)}$ and the other an essential curve of T, so that $\mathrm{int}(A) \cap T = \varnothing$.

In this definition (and throughout this paper) we allow K to be the unknot in S^3, in which case $E(K)^{(c)}$ is homeomorphic to a disk with c holes cross S^1, and it admits swallow follow tori whenever $c \geq 3$.

Given a swallow follow torus T and an annulus A as above, we can surger T along A to obtain a separating meridional annulus. It is easy to see that since T is an essential torus, the annulus obtained is essential as well. Conversely, given an essential separating meridional annulus we can tube the annulus to itself along the boundary obtaining a swallow follow torus (this can be done in two distinct ways).

How does a swallow follow torus decompose a knot exterior? We first consider the case $c = 0$. Let $K = K_1\#K_2$ be a composite knot (here we are not assuming that K_1 or K_2 is prime). Let $\mathcal{A}$ be a decomposing annulus corresponding to the decomposition of K as $K_1\#K_2$. Thus $E(K) = E(K_1) \cup_{\mathcal{A}} E(K_2)$. Tubing $\mathcal{A}$ along the boundary (say, into $E(K_2)$) we obtain a swallow follow torus, say, T. Clearly, one component of $E(K)$ cut open along T is homeomorphic to $E(K_2)$. The other component is homeomorphic to $E(K_1)$ with two meridional annuli identified, and hence homeomorphic to $E(K_1)^{(1)}$. Thus we see that a swallow follow torus $T \subset E(K)$ decomposes $E(K)$ as $E(K_1)^{(1)} \cup_T E(K_2)$. More generally, given K, K_1, and K_2 as above and integers c, c_1, $c_2 \geq 0$ with $c_1 + c_2 = c$, let $\mathcal{A}$ be a decomposing annulus for $E(K)^{(c)}$, so that $E(K)^{(c)} = E(K_1)^{(c_1)} \cup_{\mathcal{A}} E(K_2)^{(c_2)}$. The swallow follow torus obtained by tubing $\mathscr{A}$ into $E(K_2)^{(c_2)}$ decomposes $E(K)^{(c)}$ as $E(K_1)^{(c_1+1)} \cup_T E(K_2)^{(c_2)}$. Since the components of $E(K)^{(c)}$ cut open along a swallow follow torus are themselves of the form $E(K_1)^{(c_1+1)}$ and $E(K_2)^{(c_2)}$, we may now extend Definition 6.1 inductively:

Definition 6.2 (swallow follow tori). Let K and c be as in the previous paragraph. Let $T_1, \dots, T_r$ (for some r) be disjointly embedded tori in $E(K)^{(c)}$. Then $T_1, \dots, T_r$ are called *swallow follow tori* if the following two conditions hold, perhaps after reordering the indices:

(1) T_1 is a swallow follow torus for $E(K)^{(c)}$.

(2) For each $i \geq 2$, T_i is a swallow follow torus for some component of $E(K)^{(c)}$ cut open along $\bigcup_{j=1}^{i-1} T_j$.

We are now ready to state and prove:

Proposition 6.3 (existence of swallow follow tori). *For $i = 1, \dots, n$, let K_i be a (not necessarily prime) knot in a compact manifold and let $c \geq 0$ be an integer. Suppose that $E(K_i) \not\cong T^2 \times [0,1]$ and $\partial N(K_i)$ is incompressible in $E(K_i)$.*

Then given any integers $c_1, \dots, c_n \geq 0$ whose sum is $c + n - 1$, there exist $n - 1$ swallow follow tori, denoted $\mathcal{T}$, that decompose $E(\#_{i=1}^n K_i)^{(c)}$ as

$$E(\#_{i=1}^n K_i)^{(c)} = \bigcup\nolimits_{\mathcal{T}} E(K_i)^{(c_i)}.$$

Proof. We use the notation as in the statement of the proposition and induct on n. If $n = 1$ there is nothing to prove. We assume, as we may, that $n > 1$. We first claim that for some i we have that $c_i \leq c$. Assume, for a contradiction, that $c_i > c$ for every $1 \leq i \leq n$. Since c_i and c are integers, $c_i \geq c + 1$. Then we have:

$$c + n - 1 = \sum_{i=1}^{n} c_i \geq n(c+1) = nc + n.$$

Moving all term to the right we get that

$$0 \geq (n-1)c + 1,$$

which is absurd, since $n \geq 1$ and $c \geq 0$. By reordering the indices if necessary we may assume that $c_n \leq c$.

Let A be an annulus in $E(\#_{i=1}^n K_i)$ so that the components of $E(\#_{i=1}^n K_i)$ cut open along A are identified with $E(K_1 \# \cdots \# K_{n-1})$ and $E(K_n)$. Since the tori $\partial N(K_i)$ are incompressible, A is essential in $E(\#_{i=1}^n K_i)$. Recall that $E(\#_{i=1}^n K_i)^{(c)}$ is obtained from $E(\#_{i=1}^n K_i)$ by drilling c curves that are parallel to the meridian; since $c_n \leq c$ we may choose the curves so that exactly c_n components are contained in $E(K_n)$. After drilling, the components of $E(\#_{i=1}^n K)^{(c)}$ cut open along A are identified with $E(K_1 \# \cdots \# K_{n-1})^{(c-c_n)}$ and $E(K_n)^{(c_n)}$. Let T be the torus obtained by tubing

A into $E(K)^{(c_n)}$; clearly the components of $E(\#_{i=1}^n K)^{(c)}$ cut open along T are identified with $E(K_1\#\cdots\#K_{n-1})^{(c-c_n+1)}$ and $E(K_n)^{(c_n)}$. Since A is essential and $E(K_i) \not\cong T^2 \times [0, 1]$, we have that T is essential in $E(\#_{i=1}^n K_i)^{(c)}$. By construction, there is an essential curve on T that cobounds an annulus with a meridian of $E(\#_{i=1}^n K_i)^{(c)}$ and we conclude that T is a swallow follow torus.

We induct on $K_1, \dots, K_n$. Let $c' = c - c_n + 1$. Then we have

$$\begin{aligned}\sum_{i=1}^{n-1} c_i = \sum_{i=1}^{n} c_i - c_n = c + n - 1 - c_n \\ = (c - c_n + 1) + n - 2 = c' + (n-1) - 1.\end{aligned}$$

By induction, $E(K_1\#\cdots\#K_{n-1})^{(c')}$ admits $n-2$ swallow follow tori, which we will denote by $\mathcal{T}'$, so that $\mathcal{T}'$ decomposes

$$E(K_1\#\cdots\#K_{n-1})^{(c')} = E(K_1\#\cdots\#K_{n-1})^{(c-c_n+1)},$$

as

$$\bigcup\nolimits_{\mathcal{T}'} E(K_i)^{(c_i)}.$$

It follows that $\mathcal{T} = T \cup \mathcal{T}'$ are swallow follow tori for $E(K)^{(c)}$, and the components of $E(K)^{(c)}$ cut open along $\mathcal{T}$ are homeomorphic to $E(K_1)^{(c_1)}, \dots, E(K_n)^{(c_n)}$. $\square$

By Proposition 6.3 and repeated use of Lemma 2.2 we obtain the following.

Corollary 6.4. *With notation as in Proposition 6.3 (and in particular for any integer $c \geq 0$ and any integers $c_1, \dots, c_n$ whose sum is $c + n - 1$), we get:*

$$g(E(K)^{(c)}) \leq \Sigma_{i=1}^n g(E(K_i)^{(c_i)}) - (n-1).$$

7. An upper bound for the growth rate

Using the results in the previous sections we can easily bound the growth rate:

Proposition 7.1. *Let K be an admissible knot in a closed manifold M. Let $g = g(E(K)) - g(M)$ and the bridge indices $\{b_1^*, \dots, b_g^*\}$ be as in Notation 1.1. Then,*

$$gr_t(K) \leq \min_{i=1,\dots,g} \left\{1 - \frac{i}{b_i^*}\right\}.$$

Proof. Fix $1 \leq i \leq g$ and a positive integer n. Let $k_i > 0$ and $0 \leq r < b_i^*$ be the quotient and remainder when dividing $(n-1)$ by b_i^*; that is:

$$k_i b_i^* + r = n - 1.$$

Consider the nonnegative integers $b_i^*, \dots, b_i^*, r, 0, \dots, 0$ (where b_i^* appears k_i times and the symbol 0 appears $n - (k_i + 1)$ times). Applying Corollary 6.4 to $E(nK)^{(0)}$

we get (recalling that $E(nK)^{(0)} = E(nK)$):

$$g(E(nK)) \leq k_i g(E(K)^{(b_i^*)}) + g(E(K)^{(r)}) + (n-(k_i+1))g(E(K)) - (n-1).$$

By definition of b_i^*, K admits a $(g(E(K))-i, b_i^*)$ decomposition. Applying Corollary 5.6 with $h-c = g(E(K))-i$ and $c = b_i^*$ gives

$$g(E(K)^{(b_i^*)}) \leq g(E(K)) - i + b_i^*.$$

Thus we get:

$$\begin{aligned} g(E(nK)) &\leq k_i(g(E(K))-i+b_i^*)+g(E(K)^{(r)})+(n-(k_i+1))g(E(K))-(n-1) \\ &= (n-1)g(E(K))+g(E(K)^{(r)})-k_i i+(k_i b_i^*-(n-1)) \\ &= (n-1)g(E(K))+g(E(K)^{(r)})-k_i i-r. \end{aligned}$$

By denoting the n-th element of the sequence in the definition of the growth rate by S_n, we get:

$$\begin{aligned} S_n &= \frac{g(E(nK)) - ng(E(K)) + (n-1)}{n-1} \\ &\leq \frac{1}{n-1}\big[(n-1)g(E(K)) + g(E(K)^{(r)}) - k_i i - r - ng(E(K)) + (n-1)\big] \\ &= \frac{1}{n-1}\big[g(E(K)^{(r)}) - g(E(K)) - r - k_i i + (n-1)\big] \\ &= \frac{g(E(K)^{(r)}) - g(E(K)) - r}{n-1} + 1 - \frac{k_i i}{k_i b_i^* + r}. \end{aligned}$$

In the last equality we used $k_i b_i^* + r = n-1$. Recall that $E(K)^{(r)}$ is obtained by drilling r curves parallel to $\partial E(K)$ out of $E(K)$. Therefore, by [Rieck 2000],

$$g(E(K)^{(r)}) \leq g(E(K)) + r.$$

Hence the first summand above is nonpositive, and we may remove that term. Further, since $r < b_i^*$, $k_i b_i^* + r < (k_i+1)b_i^*$, which implies

$$S_n < 1 - \frac{i}{b_i^*}\frac{k_i}{k_i+1}. \tag{1}$$

Since $\lim_{n\to\infty} k_i = \infty$ we have:

$$\mathrm{gr}_t(K) = \limsup_{n\to\infty} S_n \leq \lim_{k_i\to\infty}\left(1 - \frac{i}{b_i^*}\frac{k_i}{k_i+1}\right) = 1 - \frac{i}{b_i^*}.$$

As i was arbitrary, we get

$$\mathrm{gr}_t(K) \leq \min_{i=1,\dots,g}\left\{1 - \frac{i}{b_i^*}\right\}.$$

This completes the proof of Proposition 7.1. $\square$

Part III. The growth rate of m-small knots

This part is devoted to calculating the growth rate of m-small knots, completing the proof of Theorem 1.2. Section 8 contains the main technical result of this paper, the strong Hopf–Haken annulus theorem (Theorem 1.8). This result guarantees the existence of Hopf–Haken annuli, and complements Sections 4 and 5. In Section 9 we prove existence of "special" swallow follow tori; this section complements Section 6. Finally, in Section 10 we calculate the growth rate of m-small knots by finding a lower bound that equals exactly the upper bound found in Section 7.

8. The strong Hopf–Haken annulus theorem

Given a knot K in a compact manifold M and an integer $c > 0$, recall that the exterior of K is denoted by $E(K)$, the manifold obtained by drilling out c curves simultaneously parallel to the meridian of $E(K)$ is denoted by $E(K)^{(c)}$, and the components of $\partial E(K)^{(c)} \setminus \partial E(K)$ are denoted by $T_1, \dots, T_c$. Recall also the definitions of Haken annuli for a given Heegaard splitting (Definition 4.1), a complete system of Hopf annuli (Definition 5.1), and a complete system of Hopf–Haken annuli for a given Heegaard splitting (Definition 5.2).

In this section we prove the strong Hopf–Haken annulus theorem (Theorem 1.8), stated in the introduction. Before proving Theorem 1.8 we prove three of its main corollaries:

Corollary 8.1. *Suppose that the assumptions of Theorem 1.8 are satisfied with $F_1 = F_2 = \emptyset$ and in addition, for each i, $E(K_i)$ does not admit an essential meridional surface S with $\chi(S) \geq 6 - 2g(E(K)^{(c)})$. Let $h \geq 0$ be an integer. Then K admits an $(h-c, c)$ decomposition if and only if $g(E(K)^{(c)}) \leq h$.*

Proof of Corollary 8.1. Assume first that K admits an $(h-c, c)$ decomposition. Then by Corollary 5.6, we have $g(E(K)^{(c)}) \leq h$. Note that this direction holds in general and does not require the assumption about meridional surfaces.

Next assume that $g(E(K)^{(c)}) \leq h$ and let $\Sigma \subset E(K)^{(c)}$ be a genus h Heegaard surface. By the assumptions of the corollary, Theorem 1.8(2) does not hold. Hence by that theorem $E(K)^{(c)}$ admits a genus h Heegaard surface that admits a complete system of Hopf–Haken annuli. By (2) $\Rightarrow$ (1) of Theorem 5.4, K admits an $(h-c, c)$ decomposition. □

Corollary 8.2. *Suppose that the assumptions of Theorem 1.8 hold and in addition, that each K_i is m-small. Then for any c and any choice of F_1 and F_2, there is a minimal genus Heegaard splitting of $(E(\#_{i=1}^n K_i)^{(c)}; F_1, F_2)$ that admits a complete system of Hopf–Haken annuli.*

Proof of Corollary 8.2. This follows immediately from Theorem 1.8. □

Next we prove Corollary 1.9 which was stated in the introduction:

Proof of Corollary 1.9. We fix the notation in the statement of the corollary. First we show that for any knot K (not necessarily the connected sum of m-small knots), if $c \geq b_g^*$, then the inequality $g(E(K)^{(c)}) \leq c$ holds: by definition of b_g^*, K admits a $(0, b_g^*)$ decomposition (recall that $K \subset S^3$ and hence b_g^* is the bridge index of K with respect to S^2). Thus for $c \geq b_g^*$, K admits a $(0, c)$ decomposition. By viewing this as a $(c - c, c)$ decomposition, Corollary 5.6 implies that $g(E(K)^{(c)}) \leq c$.

Next we note that the inequality $g(E(K)^{(c)}) \geq c$ holds for K that is a connected sum of m-small knots, and any $c \geq 0$: by Corollary 8.2, $E(K)^{(c)}$ admits a minimal genus Heegaard surface (say, Σ) admitting a complete system of Hopf–Haken annuli. Hence the c tori, $T_1, \dots, T_c$, are on the same side of Σ, which implies $g(\Sigma) \geq c$; hence $g(E(K)^{(c)}) = g(\Sigma) \geq c$. □

Proof of Theorem 1.8. We first fix the notation that will be used in the proof (in addition to the notation in the statement of the theorem). Let K denote $\#_{i=1}^n K_i$. For $c > 0$, $E(K)^{(c)}$ admits an essential torus T that decomposes $E(K)^{(c)}$ as

$$E(K)^{(c)} = X \cup_T Q^{(c)},$$

where $X \cong E(K)$ and $Q^{(c)} \cong$ (an annulus with c holes) $\times S^1$. Note that $Q^{(c)}$ fibers over S^1 in a unique way, and the fibers in T are meridian curves in $X \cap Q^{(c)}$. Since $Q^{(c)}$ is Seifert fibered it is contained in a unique component J of the characteristic submanifold [Jaco 1980; Jaco and Shalen 1979; Johannson 1979]. Since $\partial N(K_i)$ is incompressible in $E(K_i)$, using Miyazaki's result [1989] it was shown in [Kobayashi and Rieck 2006a, Claim 1] that K admits a unique prime decomposition. Therefore the number of prime factors of K is well defined. We suppose, as we may, that each knot K_i is prime; consequently, the integer n appearing in the statement of the theorem is the number of prime factors of K.

The structure of the proof. The proof is an induction on (n, c) ordered lexicographically. We begin with two preliminary special cases. In Case One we consider strongly irreducible Heegaard splittings. In Case Two we consider weakly reducible Heegaard splittings so that no component of the essential surface obtained by untelescoping is contained in J. In both cases we prove the theorem directly and without reference to the complexity (n, c). We then proceed to the inductive step assuming the theorem for $(n', c') < (n, c)$ in the lexicographic order. By Cases One and Two we may assume that a minimal genus Heegaard surface for $E(K)^{(c)}$ is weakly reducible and some component of the essential surface obtained by untelescoping it is contained in J; this component allows us to induct.

Case One: $(E(K)^{(c)}; F_1, F_2)$ *admits a strongly irreducible minimal genus Heegaard splitting.* Let $C_1 \cup_\Sigma C_2$ be a minimal genus strongly irreducible Heegaard splitting of $(E(K)^{(c)}; F_1, F_2)$. The swallow follow torus theorem [Kobayashi and Rieck 2006a, Theorem 4.1] implies that if $n > 1$, either Σ weakly reduces to a swallow follow torus (contradicting the assumption of Case One) or Theorem 1.8(2) holds. We assume, as we may, that $n = 1$ in the remainder of the proof of Case One.

Recall the notation $E(K)^{(c)} = X \cup_T Q^{(c)}$. Since $T \subset E(K)^{(c)}$ is essential and $\Sigma \subset E(K)^{(c)}$ is strongly irreducible, we may isotope Σ so that $\Sigma \cap T$ is transverse and every curve of $\Sigma \cap T$ is essential in T. Minimize $|\Sigma \cap T|$ subject to this constraint. If $\Sigma \cap T = \varnothing$ then T is contained in a compression body C_1 or C_2, and hence T is parallel to a component of $\partial_- C_1$ or $\partial_- C_2$. But then T is parallel to a component of $\partial E(K)^{(c)}$, a contradiction. Thus $\Sigma \cap T \neq \varnothing$.

Let F be a component of Σ cut open along T. Minimality of $|\Sigma \cap T|$ implies that F is not boundary parallel. Then $\partial F \subset T$; since T is a torus, boundary compression of F implies compression into the same side; this will be used extensively below. A surface in a Seifert fibered manifold is called *vertical* if it is everywhere tangent to the fibers and *horizontal* if it is everywhere transverse to the fibers (see, for example, [Jaco 1980] for a discussion). We first reduce Theorem 1.8 as follows:

Assertion 1. One of the following holds:

(1) $\Sigma \cap X$ is connected and compresses into both sides, and $\Sigma \cap Q^{(c)}$ is a collection of essential vertical annuli.

(2) Theorem 1.8 holds.

Proof. A standard argument shows that one component of Σ cut open along T compresses into both sides (in X or $Q^{(c)}$) and all other components are essential (in X or $Q^{(c)}$); for the convenience of the reader we sketch it here: Let D_1 be a compressing disk for C_1. After minimizing $|D_1 \cap T|$ either $D_1 \cap T = \varnothing$ (and hence some component of Σ cut open along T compresses into C_1) or an outermost disk of D_1 provides a boundary compression for some component of Σ cut open along T; since boundary compression implies compression into the same side, we see that in this case too some component of Σ cut open along T compresses into C_1. Similarly, some component of Σ cut open along T compresses into C_2. Strong irreducibility of Σ implies that the same component compresses into both sides and all other components are incompressible and boundary incompressible. Minimality of $|\Sigma \cap T|$ implies that no component is boundary parallel, and hence the incompressible and boundary incompressible components are essential.

The proof of Assertion 1 breaks up into three subcases:

Subcase 1: *no component of $\Sigma \cap X$ is essential.* Then $\Sigma \cap X$ is connected and compresses into both sides, and therefore $\Sigma \cap Q^{(c)}$ consists of essential surfaces. Since $Q^{(c)}$ is Seifert fibered, every component of $\Sigma \cap Q^{(c)}$ is either horizontal or vertical (see, for example, [Jaco 1980, VI.34]). Any horizontal surface in $Q^{(c)}$ must meet every component of $\partial Q^{(c)}$; by construction $\Sigma \cap \partial N(K) = \varnothing$; thus every component of $\Sigma \cap Q^{(c)}$ is vertical (we will use this argument below without reference). This gives Assertion 1(1).

Subcase 2a: *some component of $\Sigma \cap X$ is essential and some component of $\Sigma \cap Q^{(c)}$ is essential.* Let F denote an essential component of $\Sigma \cap X$. Since T is incompressible and the components of $\Sigma \cap T$ are essential in T, no component of Σ cut open along T is a disk; hence $\chi(F) \geq \chi(\Sigma)$. Let S denote an essential component of $\Sigma \cap Q^{(c)}$. Then S is a vertical annulus. In particular, $S \cap T$ consists of fibers in the Seifert fibration of $Q^{(c)}$. By construction, the fibers on T are meridians of X. We see that F is meridional, giving Theorem 1.8(2).

Subcase 2b: *some component of $\Sigma \cap X$ is essential and no component of $\Sigma \cap Q^{(c)}$ is essential.* As above let F be an essential component of $\Sigma \cap X$. By assumption, no component of $\Sigma \cap Q^{(c)}$ is essential. Hence $\Sigma \cap Q^{(c)}$ is connected and compresses into both sides. Let Δ_1 be a maximal collection of compressing disks for $\Sigma \cap Q^{(c)}$ into $Q^{(c)} \cap C_1$ and S_1 the surface obtained by compressing S along Δ_1. Since $\Delta_1 \neq \emptyset$, maximality of Δ_1 and the no nesting lemma [Scharlemann 1998] imply that S_1 is incompressible. Suppose first that some nonclosed component of S_1, say, S_1', is not boundary parallel (this is similar to Subcase 2a). Then S_1' is an essential and hence vertical annulus and we see that F is meridional, giving Theorem 1.8(2) and the assertion follows. We assume from now on that S_1 consists of boundary parallel annuli and, perhaps, closed boundary parallel surfaces and ball-bounding spheres. Furthermore, we see that:

(1) No two closed components of S_1 are parallel to the same component of $\partial Q^{(c)}$: this follows from the connectivity of $\Sigma \cap Q^{(c)}$ and strong irreducibility of Σ.

(2) No two boundary parallel annuli of S_1 are nested: otherwise, it follows from the connectivity of $\Sigma \cap Q^{(c)}$ and strong irreducibility of Σ that Σ can be isotoped out of $Q^{(c)}$; for more details see [Kobayashi and Rieck 2004, page 249].

We assume, as we may, that the analogous conditions hold after compressing $\Sigma \cap Q^{(c)}$ into $Q^{(c)} \cap C_2$. Hence $\Sigma \cap Q^{(c)}$ is a Heegaard surface for $Q^{(c)}$ relative to the annuli $\{C_1 \cap T, C_2 \cap T\}$ (relative Heegaard surfaces were defined in Definition 3.1). We may replace $\Sigma \cap Q^{(c)}$ with the minimal genus relative Heegaard surface for $Q^{(c)}$ relative to $\{C_1 \cap T, C_2 \cap T\}$ given in Corollary 3.3. By pasting this surface to $\Sigma \cap X$ we obtain a closed surface, say, Σ', satisfying the four following conditions:

(1) Σ' is a Heegaard surface for $E(K)^{(c)}$: the components of X cut open along $\Sigma \cap X$ are the same as the components of C_1 and C_2 cut open along $\{C_1 \cap T, C_2 \cap T\}$ that are contained in X. Since T is essential, the annuli $C_i \cap T$ are incompressible in C_i. It is well known that cutting a compression body along incompressible surfaces yields compression bodies; we conclude that the components of X cut open along $\Sigma \cap X$ are compression bodies. By definition of the relative Heegaard surface, the annuli of $\{C_1 \cap T, C_2 \cap T\}$ are primitive in the compression bodies obtained by cutting $Q^{(c)}$ open along any relative Heegaard surface; it follows that $E(K)^{(c)}$ cut open along Σ' consists of two compression bodies.

(2) Σ' is a Heegaard surface for $(E(K)^{(c)}; F_1, F_2)$: in addition to (1) above, we must show Σ' respects the same partition of $\partial E(K)^{(c)} \setminus (\partial N(K), T_1, \dots, T_c)$ as Σ. This follows immediately from the facts that the changes we made are contained in $Q^{(c)}$, every component of F_1 is contained in $C_1 \cap X$, and every component of F_2 is contained in $C_2 \cap X$. Note that (1) and (2) hold for any relative Heegaard surface for $Q^{(c)}$ relative to $\{C_1 \cap T, C_2 \cap T\}$.

(3) $g(\Sigma') = g(\Sigma)$: minimality of the genus of the relative Heegaard splitting used implies that $g(\Sigma') \leq g(\Sigma)$, and since Σ is a minimal genus Heegaard surface for $(E(K)^{(c)}; F_1, F_2)$, equality holds: $g(\Sigma') = g(\Sigma)$. Note that (3) holds for any minimal genus relative Heegaard surface for $Q^{(c)}$ relative to $\{C_1 \cap T, C_2 \cap T\}$.

(4) Σ' admits a complete system of Hopf–Haken annuli: by Figure 1 we see directly that Σ' admits a complete system of Hopf–Haken annuli.

Remark 8.3. As noted, in the construction above, (1), (2), and (3) hold for any minimal genus relative Heegaard surface. This is quite different in (4), when considering Hopf–Haken annuli: it is not hard to construct relative Heegaard surfaces that result in a minimal genus Heegaard surface for $(E(K)^{(c)}; F_1, F_2)$ so that all the tori $T_1, \dots, T_c$ are in the compression body containing $\partial N(K)$, and hence cannot admit even one Hopf–Haken annulus. This shows that in the course of the proof of Theorem 1.8 the given Heegaard surface must be replaced.

The Heegaard surface Σ' fulfills the conditions of Theorem 1.8(1). This completes that proof of Assertion 1. □

Before proceeding, we fix the following notation and conventions: denote $\Sigma \cap X$ by Σ_X. By Assertion 1 we may assume that Σ_X is connected and compresses into both sides and every component of $\Sigma \cap Q^{(c)}$ is an essential vertical annulus. Note that X cut open along Σ_X consists of exactly two components, denoted by $C_{i,X}$, where $C_{i,X} = C_i \cap X$ $(i = 1, 2)$. Denote the collection of annuli $T \cap C_{i,X}$ by $\mathscr{A}_i$, and the annuli in $\mathscr{A}_i$ by $A_{i,1}, \dots, A_{i,b}$, where b denotes the number of annuli in $\mathscr{A}_i$. We assume from now on that Theorem 1.8(2) does not hold.

Assertion 2. The number b satisfies $c \leq b \leq g(\Sigma)$.

Proof. Assume for a contradiction that $b < c$. Since $\Sigma \cap Q^{(c)}$ consists of b annuli, $Q^{(c)}$ cut open along $\Sigma \cap Q^{(c)}$ consists of $b + 1 < c + 1$ components. Hence some component of $Q^{(c)}$ cut open along $\Sigma \cap Q^{(c)}$ contains two of the components of $\partial Q^{(c)} \setminus T$. Hence there is a vertical annulus connecting these components which is disjoint from Σ. Since this annulus is disjoint from Σ it is contained in a compression body C_i and connects two components of $\partial_- C_i$, which is impossible.

Since Σ_X is obtained by removing the b annuli $\Sigma \cap Q^{(c)}$ and is connected, $b \leq g(\Sigma)$. □

Assertion 3. The surface Σ_X defines a $(g(\Sigma) - b, b)$ decomposition of K.

Proof. For $i = 1, 2$, let Δ_i be a maximal collection of compressing disks for Σ_X into $C_{i,X}$; by assumption, $\Delta_i \neq \varnothing$. Let S_i be the surface obtained by compressing Σ_X along Δ_i. By maximality and the no nesting lemma [Scharlemann 1998] S_i is incompressible. Since the components of $\Sigma \cap Q^{(c)}$ are vertical annuli, the boundary components of S_i are meridians. Hence, if some nonclosed component of S_i is essential, we obtain Theorem 1.8(2), contradicting our assumption. Thus S_i consists of boundary parallel annuli and, perhaps, closed boundary parallel surfaces and ball-bounding spheres. As above, strong irreducibility of Σ and connectivity of Σ_X imply that these annuli are not nested. We see that $C_{i,X}$ is a compression body and $T \cap C_{i,X}$ consists of b mutually primitive annuli. In fact, we see that Σ_X is a Heegaard surface relative to $\{\mathscr{A}_1, \mathscr{A}_2\}$. By the argument of Claim 5.5, Σ_X gives a $(g(\Sigma) - b, b)$ decomposition. □

By Assertion 3 and Theorem 5.4, $E(K)^{(b)}$ admits a genus $g(\Sigma)$ Heegaard surface admitting a complete system of Hopf–Haken annuli, say, Σ'. By Assertion 2, $c \leq b$. Hence $E(K)^{(c)}$ is obtained from $E(K)^{(b)}$ by filling the tori $T_{c+1}, \ldots, T_b$. Clearly, Σ' is a Heegaard surface for $E(K)^{(c)}$, admitting a complete system of Hopf–Haken annuli. This completes the proof of Theorem 1.8 in Case One.

Before proceeding to Case Two we introduce notation that will be used in that case. Recall that since $Q^{(c)}$ is Seifert fibered, it is contained in a component of the characteristic submanifold of $E(K)^{(c)}$ denoted by J. Since $X \cong E(K)$ and $K = \#_{i=1}^n K_i$, X admits $n-1$ decomposing annuli which we will denote by $A_1, \ldots, A_{n-1}$ ($A_1, \ldots, A_{n-1}$ are not uniquely defined). The components of X cut open along $\bigcup_{i=1}^{n-1} A_i$ are homeomorphic to $E(K_1), \ldots, E(K_n)$. Let

$$V = Q^{(c)} \cup N(A_1) \cup \cdots \cup N(A_{n-1}).$$

Then V is Seifert fibered and contains $Q^{(c)}$, and hence after isotopy $V \subset J$. Note that $V \cap \mathrm{cl}(E(K)^{(c)} \setminus V)$ consists of n tori, say, $T_1', \ldots, T_n'$. Finally note that $X^{(c)}$ cut open along $\bigcup_{i=1}^n T_i{}'$ consists of $n+1$ components, one is V, and the others are homeomorphic to $E(K_1), \ldots, E(K_n)$. We denote the component that corresponds to $E(K_i)$ by X_i. After renumbering if necessary we may assume that T_i' is a component of ∂X_i. By construction T_i' corresponds to $\partial N(K_i)$.

The proof of Assertion 4 is a simple argument using essential arcs in base orbifolds, and we leave it to the reader.

Assertion 4. If V is not isotopic to J then some $E(K_i)$ contains a meridional essential annulus.

For future reference we remark:

Remark 8.4. By Assertion 4, either we have Theorem 1.8(2), or $J = V$. Hence, in the following, we may assume that $J = V$; we will use the notation J from here on. By construction, J is homeomorphic to (a $(c+n)$-times punctured disk)$\times S^1$ and hence admits no closed nonseparating surfaces.

Case Two: $(E(K)^{(c)}; F_1, F_2)$ *admits a weakly reducible minimal genus Heegaard surface* Σ*, and no component of the essential surface obtained by untelescoping* Σ *is isotopic into* J. Let F be the (not necessarily connected) essential surface obtained by untelescoping Σ. The assumptions of Theorem 1.8 imply that $E(K)^{(c)}$ does not admit a nonseparating sphere; hence the Euler characteristic of every component of F is bounded below by $\chi(\Sigma)+4$. After an isotopy that minimizes $|F \cap \partial J|$, every component of $F \cap J$ is essential in J and every component of $F \cap \text{cl}(E(K)^{(c)} \setminus J)$ is essential in $\text{cl}(E(K)^{(c)} \setminus J)$. By the assumption of Case Two, if some component F' of F meets J, then $F' \not\subset J$ and hence each component of $F' \cap J$ is a vertical annulus and each component of $F' \cap \text{cl}(E(K)^{(c)} \setminus J)$, say, S, is a meridional essential surface with $\chi(S) \geq \chi(F' \cap E(K)^{(c)}) = \chi(F') \geq \chi(F) \geq 6-2g(\Sigma)$, giving Theorem 1.8(2). Thus we may assume $F \cap J = \varnothing$.

Let M_J be the component of $E(K)^{(c)}$ cut open along F containing J, and let Σ_J be the strongly irreducible Heegaard surface induced on M_J by untelescoping. Then Σ_J defines a partition of $\partial M_J \setminus (T_1 \cup \cdots \cup T_c \cup \partial N(K))$, say, $F_{J,1}$, $F_{J,2}$. Since Σ is minimal genus, Σ_J is a minimal genus splitting of $(M_J; F_{J,1}, F_{J,2})$.

For $i = 1, \ldots, n$, denote $X_i \cap M_J$ by X_i'. Note that $X_i' \cap J = T_i'$; the meridian of X_i defines a slope of T_i', denoted by μ_i'. By filling X_i' along μ_i' we obtain a manifold, say, M_i', and the core of the attached solid torus is a knot, say, $K_i' \subset M_i'$. Then M_J is naturally identified with $E(\#_{i=1}^n K_i')^{(c)}$, and Σ_J is a strongly irreducible Heegaard surface for $(E(\#_{i=1}^n K_i')^{(c)}; F_{J,1}, F_{J,2})$. It is easy to see that the knots K_i' fulfill the assumptions of Theorem 1.8; in particular, the assumptions of Case Two imply that $E(K_i') \not\cong T^2 \times I$. Therefore, by Case One, one of the following holds:

(1) Theorem 1.8(1): there exists a Heegaard surface Σ_J' for M_J so that the following three conditions hold:
  (a) $g(\Sigma_J') = g(\Sigma_J)$,
  (b) Σ_J' is a Heegaard splitting for $(E(\#_{i=1}^n K_i')^{(c)}; F_{J,1}, F_{J,2})$,
  (c) Σ_J' admits a complete system of Hopf–Haken annuli.

(2) Theorem 1.8(2): for some i, X_i' admits a meridional essential surface F_i' with $\chi(F_i') \geq 6-2g(\Sigma_J) \geq 6-2g(\Sigma)$.

Assume first that (1) holds. By condition (1b), Σ_J' induces the same partition on the components of $\partial M_j \setminus \{T_1, \ldots, T_c, \partial N(K)\}$ as Σ_J. Thus we may amalgamate the Heegaard surfaces induced on the components of $\text{cl}(E(K)^{(c)} \setminus M_J)$ with Σ_J', obtaining a Heegaard surface for $(E(K)^{(c)}; F_1, F_2)$, say, Σ''. By Proposition 4.3, Σ'' admits a complete system of Hopf–Haken annuli. Since $g(\Sigma_J') = g(\Sigma_J)$, we have that $g(\Sigma'') = g(\Sigma)$; hence Σ'' is a minimal genus Heegaard surface for $(E(K)^{(c)}; F_1, F_2)$. This gives Theorem 1.8(1).

Assume next that (2) happens. Since X_i' is a component of X_i cut open along the (possibly empty) surface $F \cap X_i$, and every component of $F \cap X_i$ is incompressible,

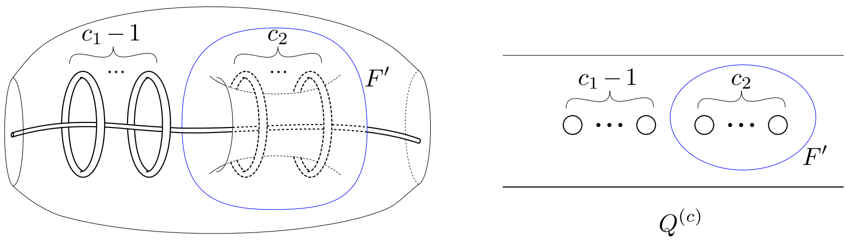


Figure 6. Subcase 1a.

we have that F'_i is essential in X_i. By construction, the meridians of X_i and X'_i are the same. Finally, $\chi(F'_i) \geq 6 - 2g(\Sigma) = 6 - 2g(E(K)^{(c)}; F_1, F_2)$. This gives Theorem 1.8(2), completing the proof of Theorem 1.8 in Case Two.

With these two preliminary cases in hand we are now ready for the inductive step. For the remainder of the proof we assume that Theorem 1.8(2) does not hold. Fix $K_1, \dots, K_n$ and $c \geq 0$ and assume, by induction, that Theorem 1.8 holds for any example with complexity $(n', c') < (n, c)$ ordered lexicographically. Let Σ be a minimal genus Heegaard surface for $E(\#_{i=1}^n K_i)^{(c)}$. By Case One, we may assume that Σ is not strongly irreducible; hence Σ admits an untelescoping. By Case Two, we may assume that some component F' of the essential surface F obtained by untelescoping Σ is isotopic into J. By Remark 8.4, J is a Seifert fibered space over a punctured disk and the components of $E(\# K_i)^{(c)} \setminus J$ are identified with $E(K_1), \dots, E(K_n)$. After isotopy we may assume that F' is horizontal or vertical (see, for example, [Jaco 1980, VI.34]; recall that a surface in a Seifert fibered space is horizontal if it is everywhere transverse to the fibers and vertical if it is everywhere tangent to the fibers). However $\partial J \neq \emptyset$ and $\partial F' = \emptyset$, and therefore F' cannot be horizontal. We conclude that F' is a vertical torus that separates J and hence $E(\#_{i=1}^n K_i)^{(c)}$. Thus F' decomposes $E(\#_{i=1}^n K_i)^{(c)}$ as:

$$E(\#_{i=1}^n K_i)^{(c)} = E(\#_{i \in I} K_i)^{(c_1)} \cup_{F'} E(\#_{i \notin I} K_i)^{(c_2)},$$

where $c_1 + c_2 = c + 1$ and $I \subset \{1, \dots, n\}$. Since F' is connected and separating, by Proposition 2.3, Σ weakly reduces to F' and the weak reduction induces (not necessarily strongly irreducible) Heegaard splittings on $E(\#_{i \in I} K_i)^{(c_1)}$ and $E(\#_{i \notin I} K_i)^{(c_2)}$. We divide the proof into Cases 1 and 2 below:

Case 1: *$I = \emptyset$ or $I = \{1, \dots, n\}$.* By symmetry we may assume that $I = \{1, \dots, n\}$. Then F' decomposes $E(\#_{i=1}^n K_i)^{(c)}$ as $E(\#_{i=1}^n K_i)^{(c_1)} \cup_{F'} D(c_2)$ where $D(c_2)$ is a c_2 times punctured disk cross S^1. There are two possibilities: $\partial N(K) \subset E(\#_{i=1}^n K_i)^{(c_1)}$ (Subcase 1a) and $\partial N(K) \subset D(c_2)$ (Subcase 1b).

Subcase 1a: *$I = \{1, \dots, n\}$ and $\partial N(K) \subset E(\#_{i=1}^n K_i)^{(c_1)}$.* For this subcase, see Figure 6. Recall that $E(\#_{i=1}^n K_i)^{(c)} = E(\#_{i=1}^n K_i)^{(c_1)} \cup_{F'} D(c_2)$ with $c_1 + c_2 = c + 1$; reordering $T_1, \dots, T_c$ if necessary we may assume $T_1, \dots, T_{c_1 - 1} \subset \partial E(\#_{i=1}^n K_i)^{(c_1)}$

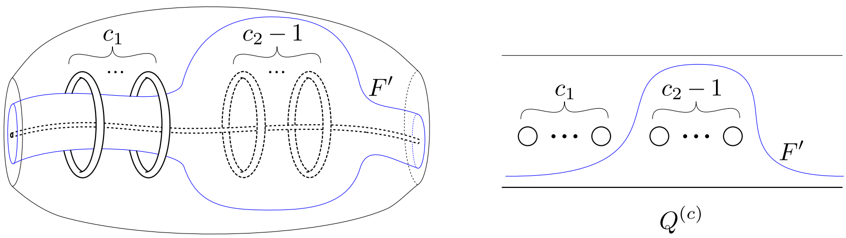


Figure 7. Subcase 1b.

and $T_{c_1}, \dots, T_c \subset \partial D(c_2)$. Since F' is not boundary parallel, $c_2 \geq 2$; thus $c_1 < c$. Thus $(n, c_1) < (n, c)$ (in the lexicographic order) and hence we may apply induction to $E(\#_{i=1}^n K_i)^{(c_1)}$. Let Σ_1' be the Heegaard surface induced on $E(\#_{i=1}^n K_i)^{(c_1)}$ by the weak reduction of Σ. By assumption, Theorem 1.8(2) does not hold; it is easy to see that $E(\#_{i=1}^n K_i)^{(c_1)}$ satisfies the assumptions of Theorem 1.8, and since $g(\Sigma_1') < g(\Sigma)$, Theorem 1.8(2) does not hold for $E(\#_{i=1}^n K_i)^{(c_1)}$. Therefore the inductive hypothesis shows that $E(\#_{i=1}^n K_i)^{(c_1)}$ admits a Heegaard surface Σ_1 fulfilling the following three conditions:

(1) $g(\Sigma_1) = g(\Sigma_1')$.

(2) Σ_1 and Σ_1' induces the same partition of the components of $\partial E(\#_{i=1}^n K_i)^{(c_1)} \setminus \{T_1, \dots, T_{c_1-1}, F', \partial N(K)\}$.

(3) Σ_1 admits a complete system of Hopf–Haken annuli.

Denote the union of the $c_1 - 1$ Hopf–Haken annuli connecting $\partial N(\#_{i=1}^n K_i)$ to $T_1, \dots, T_{c_1-1}$ by $\mathscr{A}_1$ and the Hopf–Haken annulus connecting $\partial N(\#_{i=1}^n K_i)$ to F' by A (note that $c_1 - 1 = 0$ is possible; in that case $\mathscr{A}_1 = \emptyset$). There exists a minimal genus Heegaard surface Σ_2 for $D(c_2)$ that admits c_2 Haken annuli $A_{c_1}, \dots, A_c$ so that one component of ∂A_i is a longitude of T_i and the other is on F' and parallel to $A \cap F'$ there (recall Remark 4.2). We denote $\bigcup_{i=c_1}^c A_i$ by $\mathscr{A}_2$. As shown in Proposition 4.3, the annuli obtained by attaching a parallel copy of A to each annulus of $\mathscr{A}_2$ union $\mathscr{A}_1$ are Haken annuli for the Heegaard surface obtained by amalgamating Σ_1 and Σ_2; we will denote this surface by $\hat{\Sigma}$. By construction, these annuli form a complete system of Hopf–Haken annuli for $\hat{\Sigma}$. Since $g(\hat{\Sigma}) = g(\Sigma_1) + g(\Sigma_2) - 1$ and $g(\Sigma) = g(\Sigma_1') + g(\Sigma_2) - 1$, by condition (1) above we have $g(\hat{\Sigma}) = g(\Sigma)$. By construction, Σ and $\hat{\Sigma}$ induce the same partition of the components of $\partial E(K)^{(c)} \setminus \{T_1, \dots, T_c, \partial N(K)\}$. Theorem 1.8 holds in Subcase 1a.

Subcase 1b: $I = \{1, \dots, n\}$ *and* $\partial N(K) \subset D(c_2)$. For this subcase, see Figure 7. Since Subcase 1b is similar to Subcase 1a we omit some of the easier details of the proof. As in Subcase 1a, F' decomposes $E(\#_{i=1}^n K_i)^{(c)}$ as $E(\#_{i=1}^n K_i)^{(c_1)} \cup_{F'} D(c_2)$ with $c_1 + c_2 = c + 1$; we reorder $T_1, \dots, T_c$ so that $T_1, \dots, T_{c_1} \subset \partial E(\#_{i=1}^n K_i)^{(c_1)}$ and $T_{c_1+1}, \dots, T_c \subset \partial D(c_2)$. By induction there exists a minimal genus Heegaard

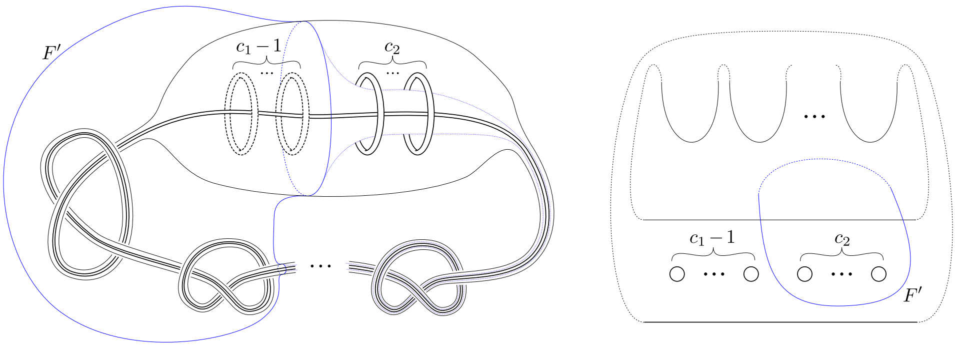


Figure 8. Case 2.

surface Σ_1 for $E(\#_{i=1}^n K_i)^{(c_1)}$ fulfilling conditions analogous to (1)–(3) listed in Subcase 1a. In particular, Σ_1 admits a complete system of c_1 Hopf– Haken annuli, say, $\mathscr{A}_1$, so that one boundary component of each annulus of $\mathscr{A}_1$ is a longitude of T_i ($i = 1, \dots, c_1$) and the other is a curve of F'. As in Subcase 1a, there exists a minimal genus Heegaard surface Σ_2 for $D(c_2)$ admitting a system of c_2 Haken annuli (recall Remark 4.2), denoted by $\mathscr{A}_2 \cup A$, so that $\mathscr{A}_2$ consists of $c_2 - 1$ annuli connecting meridians of $\partial N(\# K_i)$ to the longitudes of $T_{c_1+1}, \dots, T_c$, and A connects a meridian of $\partial N(\# K_i)$ to a curve of F'; by construction, this curve is parallel to the curves of $\mathscr{A}_1 \cap F'$. As shown in Proposition 4.3, the annuli obtained by attaching a parallel copy of A to each annulus of $\mathscr{A}_1$ union $\mathscr{A}_2$ are Haken annuli for the Heegaard surface obtained by amalgamating Σ_1 and Σ_2; we will denote this surface by $\hat{\Sigma}$. By construction, these annuli form a complete system of Hopf–Haken annuli for $\hat{\Sigma}$. As in Subcase 1a, $g(\hat{\Sigma}) = g(\Sigma)$ and $\hat{\Sigma}$ induces the same partition on the components of $\partial E(K)^{(c)} \setminus \{T_1, \dots, T_c, \partial N(K)\}$ as Σ. Theorem 1.8 holds in Subcase 1b.

Case 2: $\emptyset \neq I \neq \{1, \dots, n\}$**.** See Figure 8 for this case. Since Case 2 is similar to Subcase 1a we omit some of the easier details of the proof. By symmetry we may assume that $\partial N(K) \subset \partial E(\#_{i \in I} K_i)^{(c_1)}$. Let Σ_1' and Σ_2' be the Heegaard surfaces induced on $E(\#_{i \in I} K_i)^{(c_1)}$ and $E(\#_{i \notin I} K_i)^{(c_2)}$ (respectively) by Σ. Since both $|I|$ and $n - |I|$ are strictly less than n, we may apply induction to both $E(\#_{i \in I} K_i)^{(c_1)}$ and $E(\#_{i \notin I} K_i)^{(c_2)}$. By induction, there exist minimal genus Heegaard surfaces Σ_1 and Σ_2 for $E(\#_{i \in I} K_i)^{(c_1)}$ and $E(\#_{i \notin I} K_i)^{(c_2)}$ (respectively) fulfilling the following three conditions:

(1) $g(\Sigma_1) = g(\Sigma_1')$ and $g(\Sigma_2) = g(\Sigma_2')$.

(2) The partition of the components of $\partial E(\#_{i \in I} K_i)^{(c_1)} \setminus \{\partial N(K), T_1, \dots, T_{c_1 - 1}\}$ which Σ_1 induces is the same as that induced by Σ_1'. Similarly, Σ_2 induces the same partition of the components of $\partial E(\#_{i \notin I} K_i)^{(c_2)} \setminus \{T_{c_1}, \dots, T_{c_2}, F'\}$ as Σ_2'.

(3) Σ_1 admits a complete system of Hopf–Haken annuli, say, $A \cup \mathscr{A}_1$, where A connects $\partial N(K)$ to F' and the components of $\mathscr{A}_1$ connect $\partial N(K)$ to

$T_1, \dots, T_{c_1-1}$; similarly Σ_2 admits complete systems of Hopf–Haken annuli $\mathscr{A}_2$ whose components connect F' to $T_{c_1}, \dots, T_c$.

As shown in Proposition 4.3, the annuli obtained by attaching a parallel copy of A to each annulus of $\mathscr{A}_2$ union $\mathscr{A}_1$ are Haken annuli for the Heegaard surface obtained by amalgamating Σ_1 and Σ_2; we will denote this surface by $\hat{\Sigma}$. By construction, these annuli form a complete system of Hopf–Haken annuli for $\hat{\Sigma}$. As above $g(\hat{\Sigma}) = g(\Sigma)$ and $\hat{\Sigma}$ induces the same partition of the components of $\partial E(K)^{(c)} \setminus \{T_1, \dots, T_c, \partial N(K)\}$ as Σ. Theorem 1.8 holds in Case 2.

This completes the proof of Theorem 1.8. □

9. Weak reduction to swallow follow tori and calculating $g(E(K)^{(c)})$

Let $K_1 \subset M_1, \dots, K_n \subset M_n$ be knots in compact manifolds and $c > 0$ be an integer. When convenient, we will denote $\#_{i=1}^n K_i$ by K. Let $c_1, \dots, c_n \geq 0$ be integers such that $\sum_{i=1}^n c_i = c + n - 1$. By Proposition 6.3 there exist $n-1$ swallow follow tori $\mathcal{T} \subset E(K)^{(c)}$ that decompose it as $E(K)^{(c)} = \bigcup_{\mathcal{T}} E(K_i)^{(c_i)}$. By amalgamating minimal genus Heegaard surfaces for $E(K_i)^{(c_i)}$ we obtain a Heegaard surface for $E(K)^{(c)}$; however, it is distinctly possible that the surface obtained is not of minimal genus. This motivates the following definition:

Definition 9.1 (natural swallow follow tori). Let $K_1 \subset M_1, \dots, K_n \subset M_n$ be prime knots in compact manifolds and $c \geq 0$ an integer. Let $\mathcal{T} \subset E(\#_{i=1}^n K_i)^{(c)}$ be a collection of $n-1$ swallow follow tori giving the decomposition $E(\#_{i=1}^n K_i)^{(c)} = \bigcup_{\mathcal{T}} E(K_i)^{(c_i)}$, for some integers $c_i \geq 0$. We say that $\mathcal{T}$ is *natural* if it is obtained from a minimal genus Heegaard surface for $E(\#_{i=1}^n K_i)^{(c)}$ by iterated weak reduction; equivalently, $\mathcal{T}$ is called natural if

$$g(E(\#_{i=1}^n K_i)^{(c)}) = \sum_{i=1}^n g(E(K_i)^{(c_i)}) - (n-1).$$

Remark. As explained in Section 6, given *any* collection of $n-1$ swallow follow tori $\mathcal{T} \subset E(\#_{i=1}^n K_i)^{(c)}$ that give the decomposition $E(\#_{i=1}^n K_i)^{(c)} = \bigcup_{\mathcal{T}} E(K_i)^{(c_i)}$, the integers $c_1, \dots, c_n$ satisfy $\sum_{i=1}^n c_i = c+n-1$. We will often use this fact without reference; compare this to Proposition 6.3 where the converse was established.

Example 9.2 (knots with no natural swallow follow tori). In Theorem 9.4 below, we prove the existence of natural swallow follow tori under certain assumptions. The following example shows that a knot does not necessarily have swallow follow tori. We first analyze basic properties of knots that admit natural swallow follow tori: let $K_1, K_2 \subset S^3$ be prime knots and $T \subset E(K_1 \# K_2)$ be a natural swallow follow torus. By exchanging the subscripts if necessary we may assume that T decomposes $E(K_1 \# K_2)$ as $E(K_1)^{(1)} \cup_T E(K_2)$. By definition of naturality,

$$g(E(K_1 \# K_2)) = g(E(K_1)^{(1)}) + g(E(K_2)) - 1.$$

It is easy to see that $g(E(K_1)^{(1)}) \geq g(E(K_1))$. Combining these, we see that $g(E(K_1\#K_2)) \geq g(E(K_1))+g(E(K_2))-1$. Morimoto [1995] constructed examples of prime knots K_1, K_2 for which $g(E(K_1\#K_2)) = g(E(K_1)) + g(E(K_2)) - 2$. We conclude that for these knots, $E(K_1\#K_2)$ does not admit a natural swallow follow torus.

Example 9.3 (knots where only certain swallow follow tori are natural). This example is of a more subtle phenomenon. It shows that even when $E(K_1\#K_2)$ does admit a natural swallow follow torus, not every swallow follow torus is natural. In this sense, the weak reduction found in Theorem 9.4 is special as it finds natural swallow follow tori.

Let $K_{\mathrm{MSY}} \subset S^3$ be the knot constructed by Morimoto, Sakuma and Yokota [1996] and recall the notation $2K_{\mathrm{MSY}} = K_{\mathrm{MSY}}\#K_{\mathrm{MSY}}$. It was shown in [Morimoto et al. 1996] that $g(E(K_{\mathrm{MSY}})) = 2$ and $g(E(2K_{\mathrm{MSY}})) = 4$.

We claim that $g(E(K_{\mathrm{MSY}})^{(1)}) = 3$. By [Rieck 2000], $g(E(K_{\mathrm{MSY}})^{(1)}) = 2$ or 3. Assume for a contradiction that $g(E(K_{\mathrm{MSY}})^{(1)}) = 2$. By Corollary 6.4 (with $c = 0$, $c_1 = 1$, and $c_2 = 0$) we have

$$g(E(2K_{\mathrm{MSY}})) \leq g(E(K_{\mathrm{MSY}})^{(1)}) + g(E(K_{\mathrm{MSY}})) - 1 = 2+2-1 = 3,$$

a contradiction. Hence $g(E(K_{\mathrm{MSY}})^{(1)}) = 3$.

Let K be any nontrivial 2-bridge knot. It is well known that $g(E(K)) = 2$. We claim that $g(E(K_{\mathrm{MSY}}\#K)) = 3$. Since knots of tunnel number 1 are prime [Norwood 1982], $g(E(K_{\mathrm{MSY}}\#K)) \geq 3$. On the other hand, since K admits a $(1, 1)$ decomposition, by Theorem 5.4 we have that $g(E(K)^{(1)}) = 2$. As above, Corollary 6.4 gives

$$g(E(K_{\mathrm{MSY}}\#K)) \leq g(E(K_{\mathrm{MSY}})) + g(E(K)^{(1)}) - 1 = 2+2-1 = 3.$$

Hence $g(E(K_{\mathrm{MSY}}\#K)) = 3$.

$E(K_{\mathrm{MSY}}\#K)$ admits two swallow follow tori, say, T_1 and T_2, that decompose it as follows:

(1) $g(E(K_{\mathrm{MSY}}\#K)) = E(K_{\mathrm{MSY}})^{(1)} \cup_{T_1} E(K)$.

(2) $g(E(K_{\mathrm{MSY}}\#K)) = E(K_{\mathrm{MSY}}) \cup_{T_2} E(K)^{(1)}$.

In each case, amalgamating minimal genus Heegaard surfaces for the manifolds appearing on the right-hand side yields a Heegaard surface for $E(K_{\mathrm{MSY}}\#K)$ whose genus fulfills (Lemma 2.2):

(1) $g(E(K_{\mathrm{MSY}})^{(1)}) + g(E(K)) - g(T_1) = 3+2-1 = 4$.

(2) $g(E(K_{\mathrm{MSY}})) + g(E(K)^{(1)}) - g(T_2) = 2+2-1 = 3$.

We conclude that T_2 is a natural swallow follow torus but T_1 is not.

In this section we show that if K_i is m-small for all i, then any minimal genus Heegaard surface for $E(\#_{i=1}^n K_i)^{(c)}$ weakly reduces to a natural collection of swallow follow tori. The statement of Theorem 9.4 is more general and allows for nonminimal genus Heegaard surfaces.

Theorem 9.4. *Let $K_i \subset M_i$ be prime knots in compact manifolds so that $E(K_i)$ not homeomorphic to $T^2 \times I$, $E(K_i)$ is irreducible, and $\partial N(K_i)$ is incompressible in $E(K_i)$. Let Σ be a (not necessarily minimal genus) Heegaard surface for $E(\#_{i=1}^n K_i)^{(c)}$. Then one of the following holds:*

(1) *Σ admits iterated weak reductions that yield a collection of $n-1$ swallow follow tori, say, $\mathcal{T}$, giving the decomposition*

$$E(\#_{i=1}^n K_i)^{(c)} = \bigcup\nolimits_{\mathcal{T}} E(K_i)^{(c_i)},$$

where $c_1, \dots, c_n$ are integers such that $\sum_{i=1}^n c_i = c+n-1$.

(2) *For some i, K_i admits an essential meridional surface S with $\chi(S) \geq 6-2g(\Sigma)$.*

The main corollary of Theorem 9.4 allows us to calculate $g(E(\#_{i=1}^n K_i)^{(c)})$ in terms of $g(E(K_i)^{(c_i)})$.

Corollary 9.5. *In addition to the assumptions of Theorem 9.4, suppose that no K_i admits an essential meridional surface S with $\chi(S) \geq 6-2g(E(\#_{i=1}^n K_i)^{(c)})$. Then $E(\#_{i=1}^n K_i)^{(c)}$ admits a natural collection of $n-1$ swallow follow tori; equivalently, there exist integers $c_1, \dots, c_n \geq 0$ so that $\sum_{i=1}^n c_i = c+n-1$ and*

$$g(E(\#_{i=1}^n K_i)^{(c)}) = \sum_{i=1}^n g(E(K_i)^{(c_i)}) - (n-1).$$

Proof. Apply Theorem 9.4 to a minimal genus Heegaard splitting of $E(\#_{i=1}^n K_i)^{(c)}$ and apply Lemma 2.2. □

Corollary 9.6. *In addition to the assumptions of Theorem 9.4, suppose that no K_i admits an essential meridional surface S with $\chi(S) \geq 6-2g(E(\#_{i=1}^n K_i)^{(c)})$. Then*

$$g(E(\#_{i=1}^n K_i)^{(c)}) = \min\left\{\sum_{i=1}^n g(E(K_i)^{(c_i)}) - (n-1)\right\},$$

where the minimum is taken over all integers $c_1, \dots, c_n \geq 0$ with $\Sigma c_i = c+n-1$.

Proof. By Corollary 6.4, for any collection of integers $c_1, \dots, c_n$ such that $\sum_{i=1}^n c_i = c+n-1$ we have that

$$g(E(\#_{i=1}^n K_i)^{(c)}) \leq \sum_{i=1}^n g(E(K_i)^{(c_i)}) - (n-1)$$

and by Corollary 9.5, there exist integers $c_1, \dots, c_n$ for which equality holds. The corollary follows. □

Proof of Theorem 9.4. We induct on (n, c) ordered lexicographically. Recall that in the beginning of the proof of Theorem 1.8 we showed that (n, c) is well defined. If $n = 1$ there is nothing to prove; assume from now on $n > 1$.

Assume Theorem 9.4(2) does not hold, that is, for each i, $E(K_i)$ does not admit an essential meridional surface S with $\chi(S) \geq 6 - 2g(\Sigma)$. Then by the swallow follow torus theorem [Kobayashi and Rieck 2006a, Theorem 4.1] Σ weakly reduces to a swallow follow torus, say, T. T decomposes $E(\#_{i=1}^n K_i)^{(c)}$ as $E(K_I)^{(c_I)} \cup_T E(K_J)^{(c_J)}$, where $I \subseteq \{1, \dots, n\}$ (possibly empty), where c_I and c_J are nonnegative integers whose sum is $c+1$, $K_I = \#_{i \in I} K_i$, and $K_J = \#_{i \notin I} K_i$. Denote the Heegaard surfaces induced on $E(K_I)^{(c_I)}$ and $E(K_J)^{(c_J)}$ by Σ_I and Σ_J, respectively.

Case One: $\varnothing \neq I \neq \{1, \dots, n\}$. In this case both $E(K_I)^{(c_I)}$ and $E(K_J)^{(c_J)}$ are exteriors of knots with strictly less than n prime factors and hence we may apply induction to both. Since $g(\Sigma_I) < g(\Sigma)$, Theorem 9.4(2) does not hold for $E(K_I)^{(c_I)}$. Hence, by induction, Σ_I admits iterated weak reduction that yields a collection of $|I| - 1$ swallow follow tori (say, $\mathcal{T}_I \subset E(K_I)^{(c_I)}$) so that the following conditions hold:

(1) $\mathcal{T}_I$ decompose $E(K_I)^{(c_I)}$ as $\bigcup_{\mathcal{T}_I} E(K_i)^{(c_i)}$ (for $i \in I$).

(2) $\sum_{i \in I} c_i = c_I + |I| - 1$.

Similarly, Σ_J admits iterated weak reduction that yields a collection of $(n - |I|) - 1$ swallow follow tori (say, $\mathcal{T}_J \subset E(K_J)^{(c_J)}$) so that the following conditions hold:

(1) $\mathcal{T}_J$ decompose $E(K_J)^{(c_J)}$ as $\bigcup_{\mathcal{T}_J} E_i(K_i)^{(c_i)}$ (for $i \notin I$).

(2) $\sum_{i \notin I} c_i = c_J + (n - |I|) - 1$.

Thus, after iterated weak reduction of Σ we obtain $\mathcal{T} = T \cup \mathcal{T}_I \cup \mathcal{T}_J$. By the above, $\mathcal{T}$ decomposes $E(\#_{i=1}^n K_i)^{(c)}$ as $\bigcup_{\mathcal{T}} E(K_i)^{(c_i)}$, so that (recalling that $c_I + c_J = c + 1$)

$$\begin{aligned}\sum_{i=1}^n c_i &= \sum_{i \in I} c_i + \sum_{i \notin I} c_i \\ &= c_I + |I| - 1 + c_J + (n - |I|) - 1 = c + n - 1.\end{aligned}$$

This proves Theorem 9.4 in Case One.

Case Two: $I = \varnothing$ *or* $I = \{1, \dots, n\}$. By symmetry we may assume that $I = \{1, \dots, n\}$. In that case, $E(K_J)^{(c_J)} \cong D(c_J)$, (where $D(c_J)$ is a disk with c_J holes cross S^1), and T gives the decomposition:

$$E(\#_{i=1}^n K_i)^{(c)} = E(\#_{i=1}^n K_i)^{(c_I)} \cup_T D(c_J).$$

Since T is essential (and in particular, not boundary parallel), $c_J \geq 2$. Since $c_I + c_J = c + 1$, we have that $c_I < c$. Thus the complexity of $E(\#_{i=1}^n K_i)^{(c_I)}$ is $(n, c_I) < (n, c)$ and we may apply induction to $E(\#_{i=1}^n K_i)^{(c_I)}$. Let Σ_I be the

Heegaard surface for $E(\#_{i=1}^n K_i)^{(c_I)}$ induced by weak reduction. By induction, Σ_I admits a repeated weak reduction that yields a system of $n-1$ swallow follow tori, say, $\mathcal{T}_I$, that decomposes $E(\#_{i=1}^n K_i)^{(c_I)}$ as

$$E(\#_{i=1}^n K_i)^{(c_I)} = \bigcup_{\mathcal{T}_I} E(K_i)^{(c_i)}$$

with $\sum_{i=1}^n c_i = c_I + n - 1$. Let T' be a component of $\mathcal{T}_I$. Then T' decomposes $E(\#_{i=1}^n K_i)^{(c_I)}$ as

$$E(\#_{i=1}^n K_i)^{(c_I)} = E(\#_{i\in I'} K_i)^{(b_1)} \cup_{T'} E(\#_{i\notin I'} K_i)^{(b_2)},$$

for some $I' \subseteq \{1, \dots, n\}$ and some integers $b_1, b_2 \geq 0$ with $b_1 + b_2 = c_I + 1$. Since $T' \subset \mathcal{T}_I$, we have that $\varnothing \neq I' \neq \{1, \dots, n\}$. By Proposition 2.3, we see that Σ weakly reduces to T'. This reduces Case Two to Case One, completing the proof of Theorem 9.4. □

10. Calculating the growth rate of m-small knots

In this final section we complete the proof of Theorem 1.2. Let $K \subset M$ be an m-small admissible knot in a compact manifold. Recall the notation nK and $E(K)^{(c)}$.

The difference between $g(E(K)^{(c)})$ and $g(E(K)) + c$ is measured by a function denoted f_K that plays a key role our work:

Definition 10.1. Given a knot K, we define the function $f_K : \mathbb{Z}_{\geq 0} \to \mathbb{Z}$ to be

$$f_K(c) = g(E(K)) + c - g(E(K)^{(c)}).$$

We immediately see that f_K has the following properties, which we will often use without reference:

(1) $f_K(0) = 0$.

(2) For $c \geq 0$, $f_K(c) \leq f_K(c+1) \leq f_K(c) + 1$: this follows from the fact (proved in [Rieck 2000]) that for all $c \geq 0$,

$$g(E(K)^{(c)}) \leq g(E(K)^{(c+1)}) \leq g(E(K)^{(c)}) + 1.$$

(3) For $c \geq 0$, $0 \leq f_K(c) \leq c$ (this follows easily from (2)).

Before proceeding, we rephrase Corollaries 9.5 and 9.6 in terms of f_K:

Corollary 10.2. *Let $K \subset M$ be a knot in a compact manifold and let n be a positive integer. Suppose that $E(K)$ does not admit a meridional essential surface S with $\chi(S) \geq 6 - 2g(E(nK))$. Then there exist integers $c_1, \dots, c_n \geq 0$ with $\Sigma c_i = n - 1$ so that*:

$$g(E(nK)) = ng(E(K)) - \sum_{i=1}^n f_K(c_i).$$

Proof. By Corollary 9.5 (with $c = 0$) there exist $c_1, \dots, c_n \geq 0$ with $\Sigma c_i = n - 1$, so that $g(E(nK)) = \sum_{i=1}^{n} g(E(K)^{(c_i)}) - (n-1)$. We get:

$$\begin{aligned}
g(E(nK)) &= \Big[\sum_{i=1}^{n} g(E(K)^{(c_i)})\Big] - (n-1) \\
&= \Big[\sum_{i=1}^{n} g(E(K)) + c_i - f_K(c_i)\Big] - (n-1) \\
&= ng(E(K)) + \Big[\sum_{i=1}^{n} c_i\Big] - \Big[\sum_{i=1}^{n} f_K(c_i)\Big] - (n-1) \\
&= ng(E(K)) + (n-1) - \Big[\sum_{i=1}^{n} f_K(c_i)\Big] - (n-1) \\
&= ng(E(K)) - \sum_{i=1}^{n} f_K(c_i).
\end{aligned}$$

□

A similar argument shows that Corollary 9.6 gives:

Corollary 10.3. *Let $K \subset M$ be a knot in a compact manifold and let n be a positive integer. Suppose that $E(K)$ does not admit a meridional essential surface S with $\chi(S) \geq 6 - 2g(E(nK))$. Then,*

$$\begin{aligned}
g(E(nK)) &= \min\Big\{ng(E(K)) - \textstyle\sum_{i=1}^{n} f_K(c_i)\Big\} \\
&= ng(E(K)) - \max\Big\{\textstyle\sum_{i=1}^{n} f_K(c_i)\Big\},
\end{aligned}$$

where the minimum and maximum are taken over all integers $c_1, \dots, c_n \geq 0$ with $\sum_{i=1}^{n} c_i = n - 1$.

Recall (Notation 1.1) that we denote $g(E(K)) - g(M)$ by g and the bridge indices of K with respect to Heegaard surfaces of genus $g(E(K)) - i$ by b_i^* ($i = 1, \dots, g$), so that $0 < b_1^* < \cdots < b_i^* < \cdots < b_g^*$. We formally set $b_0^* = 0$ and $b_{g+1}^* = \infty$. Note that these properties imply that for every $c \geq 0$ there is a unique index i ($0 \leq i \leq g$), depending on c, so that $b_i^* \leq c < b_{i+1}^*$; we will use this fact below without reference.

In the following proposition we calculate $f_K(c)$ when $E(K)$ does not admit an essential meridional surface S with $\chi(S) \geq 6 - 2g(E(K)^{(c)})$.

Proposition 10.4. *Let K be a knot and $c \geq 0$ be an integer. Let $0 \leq i \leq g$ be the unique index for which $b_i^* \leq c < b_{i+1}^*$. Then $f_K(c) \geq i$. If, in addition, $E(K)$ does not admit an essential meridional surface S with $\chi(S) \geq 6 - 2g(E(K)^{(c)})$ then equality holds*:

$$f_K(c) = i.$$

Proof of Proposition 10.4. We first prove that $f_K(c) \geq i$ holds for any knot. Since f_K is a nonnegative function we may assume $i \geq 1$. By the definition of b_i^*, K admits a $(g(E(K)) - i,\, b_i^*)$ decomposition. Since $c \geq b_i^*$, K admits a $(g(E(K)) - i, c)$ decomposition. By Corollary 5.6 we have that $g(E(K)^{(c)}) \leq g(E(K)) - i + c$. Therefore,

$$f_K(c) = g(E(K)) + c - g(E(K)^{(c)}) \geq g(E(K)) + c - (g(E(K)) - i + c) = i.$$

Next we assume, in addition, that $E(K)$ does not admit an essential meridional surface S with $\chi(S) \geq 6 - 2g(E(K)^{(c)})$. We will complete the proof of the proposition by showing that $f_K(c) < i + 1$; suppose for a contradiction that $f_K(c) \geq i + 1$. Thus $g(E(K)^{(c)}) = g(E(K)) + c - f_K(c) \leq g(E(K)) + c - (i + 1)$.

Assume first that $i = g$. Then by Corollary 8.1 (with $g(E(K)) + c - (g+1)$ corresponding to h) we see that k admits a $(g(E(K)) + c - (g+1) - c,\, c)$ decomposition. In particular, M admits a Heegaard surface of genus $(g(E(K))) + c - (g + 1) - c$. Hence we see:

$$\begin{aligned} g(M) &\leq (g(E(K)) + c - (g + 1) - c \\ &= g(E(K)) - g - 1 \\ &= g(E(K)) - (g(E(K)) - g(M)) - 1 \\ &= g(M) - 1. \end{aligned}$$

This contradiction completes the proof when $i = g$.

Next assume $0 \leq i < g$. Applying Corollary 8.1 again (with $g(E(K)) + c - (i+1)$ corresponding to h in Corollary 8.1) we see that K admits a $(g(E(K)) - (i + 1), c)$ decomposition. By definition, b_{i+1}^* is the smallest integer such that K admits a $(g(E(K)) - (i + 1), b_{i+1}^*)$ decomposition; hence $c \geq b_{i+1}^*$. This contradicts our choice of i in the statement of the proposition, showing that $f_K(c) < i + 1$. This completes the proof of Proposition 10.4. □

As an illustration of Proposition 10.4, let K be an m-small knot in S^3. Suppose that $g = 3$, $b_1^* = 5$, $b_2^* = 7$, and $b_3^* = 23$. (We do not know if a knot with these properties exists.) Then

$$f_K(c) = \begin{cases} 0 & \text{if } 0 \leq c \leq 4, \\ 1 & \text{if } 5 \leq c \leq 6, \\ 2 & \text{if } 7 \leq c \leq 22, \\ 3 & \text{if } 23 \leq c. \end{cases}$$

Not much is known about f_K for knots that are not m-small.

Question 10.5. Does there exist a knot K in a manifold M with unbounded f_K? Does there exist a knot K with $f_K(c) > g(E(K)) - g(M)$ (for sufficiently large c)? What can be said about the behavior of the function f_K?

With the preparation complete, we are now ready to prove Theorem 1.2.

Proof of Theorem 1.2. Fix the notation of Theorem 1.2. Since the upper bound was obtained in Proposition 7.1, we assume from now on that K is m-small. By Corollary 10.3, $g(E(nK)) = ng(E(K)) - \max\{\sum_{i=1}^n f_K(c_i)\}$, where the maximum is taken over all integers $c_1, \dots, c_n \geq 0$ with $\sum_{i=1}^n c_i = n-1$.

Fix n and let $c_1, \dots, c_n \geq 0$ be integers with $\sum_{i=1}^n c_i = n-1$ that maximize $\sum_{i=1}^n f_K(c_i)$.

Lemma 10.6. *We may assume that the sequence $c_1, \dots, c_n$ fulfills the following conditions for some $1 \leq l \leq n$:*

(1) $c_i \geq c_{i+1}$ $(i = 1, \dots, n-1)$.

(2) *For $i \leq l$, $c_i \in \{b_1^*, \dots, b_g^*\}$.*

(3) $c_{l+1} < b_1^*$.

(4) *For $i > l+1$, $c_i = 0$.*

Proof. By reordering the indices if necessary we may assume (1) holds.

Let l be the largest index for which $f_K(c_l) \neq 0$. For $i = 1, \dots, l$, let $0 \leq j(i) \leq g$ be the unique index for which $b_{j(i)}^* \leq c_i < b_{j(i)+1}^*$ (recall that we set $b_0^* = 0$ and $b_{g+1}^* = \infty$). Define $c'_1, \dots, c'_n$ as follows:

(1) For $i \leq l$, set $c'_i = b_{j(i)}^*$ (i.e., c'_i is the largest b_j^* that does not exceed c_i).

(2) Set $c'_{l+1} = n - 1 - \left(\sum_{i=1}^l c'_i\right)$.

(3) For $i > l+1$, set $c'_i = 0$.

By Proposition 10.4, for $i \leq l$, $f_K(c_i) = f_K(b_{j(i)}^*) = f_K(c'_i)$. We get:

$$\begin{aligned}\sum_{i=1}^n f_K(c'_i) &= \sum_{i=1}^l f_K(c'_i) + \sum_{i=l+1}^n f_K(c'_i)\\ &= \sum_{i=1}^l f_K(c_i) + \sum_{i=l+1}^n f_K(c'_i)\\ &\geq \sum_{i=1}^l f_K(c_i) = \sum_{i=1}^n f_K(c_i).\end{aligned}$$

(For the last equality, recall that $f_K(c_i) = 0$ for $i > l$.)

Since $c_1, \dots, c_n$ maximizes $\sum_{i=1}^n f_K(c_i)$, we conclude that

$$\sum_{i=1}^n f_K(c_i) = \sum_{i=1}^n f_K(c'_i)$$

and hence $f_K(c'_{l+1}) = 0$; so $c'_{l+1} < b_1^*$. Thus $c'_1, \dots, c'_n$ is a maximizing sequence; it is easy to see that it fulfills conditions (1)–(4). $\square$

We will denote the n-th term of the defining sequence of the growth rate by S_n:

$$S_n = \frac{g(E(nK)) - ng(E(K)) + n - 1}{n-1}.$$

By Corollary 10.3

$$S_n = 1 - \frac{\max\left\{\sum_{i=1}^{n} f_K(c_i)\right\}}{n-1}. \tag{2}$$

In order to bound S_n below we need to understand the following optimization problem, where here we are assuming that the maximizing sequence fulfills the conditions listed in Lemma 10.6, and in particular, $f_K(c_i) = 0$ for $i > l$.

Problem 10.7. Find nonnegative integers l and $c_1,...,c_l$ that maximize $\sum_{i=1}^{l} f_K(c_i)$ subject to the constraints

(1) $\sum_{i=1}^{l} c_i \leq n-1$,
(2) $c_i \in \{b_1^*, \dots, b_g^*\}$ (for $1 \leq i \leq l$).

For $i = 1, \dots, g$, let k_i be the number of times that b_i^* appears in $c_1, \dots, c_l$. By Proposition 10.4, $f_K(b_i^*) = i$; thus Problem 10.7 can be rephrased as follows:

Problem 10.8. Maximize $\sum_{i=1}^{g} k_i i$ subject to the constraints

(1) $\sum_{i=1}^{g} k_i b_i^* \leq n-1$,
(2) k_i is a nonnegative integer.

We first solve this optimization problem over $\mathbb{R}$; we use the variables $x_1, \dots, x_g$ instead of $k_1, \dots, k_g$.

Problem 10.9. Given $n \in \mathbb{R}$, $n > 1$, maximize $\sum_{i=1}^{g} x_i i$ subject to the constraints

(1) $\sum_{i=1}^{g} x_i b_i^* \leq n-1$,
(2) $x_1 \geq 0, \dots, x_g \geq 0$.

It is easy to see that for any sequence $x_1, \dots, x_g$ that realizes the maximum we have that $\sum_{i=1}^{g} x_i b_i^* = n-1$, for otherwise we can increase the value of x_1, thus increasing $\sum_{i=1}^{g} x_i i$ and contradicting maximality. Problem 10.9 is an elementary linear programming problem (known as the standard maximum problem) and is solved using the simplex method which gives:

Lemma 10.10. *There is a (not necessarily unique) index i_0, which is independent of n, such that a solution of Problem 10.9 is given by*

$$x_{i_0} = \frac{n-1}{b_{i_0}^*}, \qquad x_i = 0\,(i \neq i_0).$$

Hence the maximum is

$$\frac{(n-1)i_0}{b_{i_0}^*}.$$

Proof of Lemma 10.10. The notation used in this proof was chosen to be consistent with notation often used in linear programming texts. Let $\vec{N}$, $\vec{F}$ and $\vec{x} \in \mathbb{R}^g$ denote the vectors

$$\vec{N} = (b_1^*, \dots, b_g^*), \quad \vec{F} = (1, \dots, g), \quad \text{and} \quad \vec{x} = (x_1, \dots, x_g).$$

For $n \in \mathbb{R}$, $n > 1$, let Δ_n be

$$\Delta_n = \left\{ \vec{x} \in \mathbb{R}^g \mid \vec{N} \cdot \vec{x} = n - 1, x_1 \geq 0, \dots, x_g \geq 0 \right\}.$$

Note that Δ_n is a simplex and its codimension k faces are obtained by setting k variables to zero. Problem 10.9 can be stated as:

$$\text{maximize } \vec{F} \cdot \vec{x}, \text{ subject to } \vec{x} \in \Delta_n.$$

Since the gradient of $\vec{F} \cdot \vec{x}$ is $\vec{F}$ and the normal to Δ_n is $\vec{N}$, the gradient of the restriction of $\vec{F} \cdot \vec{x}$ to Δ_n is the projection

$$\vec{P} = \vec{F} - \frac{\vec{F} \cdot \vec{N}}{|\vec{N}|^2} \vec{N}.$$

Note that $\vec{P}$ is independent of n. The maximum of $\vec{N} \cdot \vec{x}$ on Δ_n is found by moving along Δ_n in the direction of $\vec{P}$. This shows that the maximum is obtained along a face defined by setting some of the variables to zero, and the variables set to zero are independent of n. Lemma 10.10 follows by picking i_0 to be one of the variables not set to zero. □

Fix an index i_0 as in Lemma 10.10. If $b_{i_0}^* \mid n - 1$ then the maximum (over $\mathbb{R}$) found in Lemma 10.10 is in fact an integer and hence is also the maximum for Problem 10.7. This allows us to calculate S_n in this case:

Lemma 10.11. *If $b_{i_0}^* \mid n - 1$ then $S_n = 1 - i_0 / b_{i_0}^*$.*

Proof.
$$S_n = 1 - \frac{\max\left\{\sum_{i=1}^n f_K(c_i)\right\}}{n-1} = 1 - \frac{(n-1)i_0}{(n-1)b_{i_0}^*} = 1 - \frac{i_0}{b_{i_0}^*}.$$ □

We now turn our attention to the general case, where $b_{i_0}^*$ may not divide $n - 1$. We will only consider values of n for which $n > b_{i_0}^*$. As in Section 7, let k_{i_0} and r be the quotient and remainder when dividing $n - 1$ by $b_{i_0}^*$, so that

$$n - 1 = k_{i_0} b_{i_0}^* + r, \quad 0 \leq r < b_{i_0}^*. \tag{3}$$

Let $c_j \geq 0$ $(1 \leq j \leq n)$ be integers with $\sum_{j=1}^n c_j = n-1$ that maximize $\sum_{j=1}^n f_K(c_j)$. We denote $n - r$ by n'. Let $c_j' \geq 0$ $(1 \leq j \leq n')$ be integers with $\sum_{j=1}^{n'} c_j' = n' - 1$ that maximize $\sum_{j=1}^{n'} f_K(c_j')$.

Claim 10.12. $\sum_{j=1}^n f_K(c_j) \leq \sum_{j=1}^{n'} f_K(c_j') + r$.

Proof. Starting with the sequence $c_1, \dots, c_n$, we obtain a new sequence by subtracting 1 from exactly one c_j (with $c_j > 0$). Let c'''_j be a sequence of nonnegative integers obtained by repeating this process r times. Then $\sum_{j=1}^n c'''_j = n-1-r = n'-1$. Let c''_j be the sequence obtained from c'''_j by removing r zeros (note that this is possible as there indeed are at least r zeros). We get

$$\begin{aligned}
\sum_{j=1}^{n'} f_K(c'_j) + r &\geq \sum_{j=1}^{n'} f_K(c''_j) + r \quad &&\text{(since } c'_j \text{ maximizes)} \\
&= \sum_{j=1}^{n} f_K(c'''_j) + r \quad &&\text{(since } f_K(0) = 0\text{)} \\
&\geq \sum_{j=1}^{n} f_K(c_j) \quad &&\text{(since } f_K(c) + 1 \geq f_K(c+1)\text{).} \qquad \square
\end{aligned}$$

Note that $b^*_{i_0} | n' - 1$ and so we may apply Lemma 10.11 to calculate $S_{n'}$. Using Equation (2) from page 97 for the first line, we get:

$$\begin{aligned}
S_n &= 1 - \frac{\max\{\sum_{i=1}^n f(c_i)\}}{n-1} &&\text{(Equation (2) for } S_n\text{)} \\
&\geq 1 - \frac{\max\{\sum_{j=1}^{n'} f(c'_j) + r\}}{n-1} &&\text{(Claim 10.12)} \\
&= 1 - \frac{n'-1}{n-1}\frac{\max\{\sum_{j=1}^{n'} f(c'_j)\}}{n'-1} - \frac{r}{n-1} \\
&= \frac{n'-1}{n-1}\left(1 - \frac{\max\{\sum_{j=1}^{n'} f(c'_j)\}}{n'-1}\right) + \left(1 - \frac{n'-1}{n-1}\right) - \frac{r}{n-1} \\
&= \frac{n'-1}{n-1} S_{n'} + \left(1 - \frac{n'-1}{n-1}\right) - \frac{r}{n-1} &&\text{(Equation (2) for } S_{n'}\text{)} \\
&= \frac{n'-1}{n-1}\left(1 - \frac{i_0}{b^*_{i_0}}\right) + \left(1 - \frac{n'-1}{n-1}\right) - \frac{r}{n-1} &&\text{(Lemma 10.11)} \\
&= \frac{n'-1}{n-1}\left(1 - \frac{i_0}{b^*_{i_0}}\right) + \left(1 - \frac{n'+r-1}{n-1}\right) \\
&= \frac{n-r-1}{n-1}\left(1 - \frac{i_0}{b^*_{i_0}}\right) &&\text{(substituting } n' = n-r\text{).}
\end{aligned}$$

Recall that in the proof of Proposition 7.1 we proved Equation (1) (see page 78) which says (recalling that k_{i_0} was defined in Equation (3) above):

$$S_n < 1 - \frac{i_0}{b^*_{i_0}} \frac{k_{i_0}}{k_{i_0}+1}.$$

Combining these facts we obtain

$$\frac{n-r-1}{n-1}\left(1 - \frac{i_0}{b^*_{i_0}}\right) \leq S_n < 1 - \frac{i_0}{b^*_{i_0}} \frac{k_{i_0}}{k_{i_0}+1}.$$

By Equation (3) above, $r < b^*_{i_0}$ and $\lim_{n\to\infty} k_{i_0} = \infty$. We conclude that as $n \to \infty$ both bounds limit on $1 - i_0/b^*_{i_0}$, and thus $\lim_{n\to\infty} S_n$ exists and equals $1 - i_0/b^*_{i_0}$.

This completes the proof of Theorem 1.2. □

Acknowledgements

We thank Mark Arnold and Jennifer Schultens for helpful correspondence, and Yukari Funakoshi for drawing the figures. We thank the anonymous referee for a careful reading of the paper and comments that helped improve the presentation. Yo'av Rieck: this work was carried out during several visits to the math department at Nara Women's University. I thank the department and my host Tsuyoshi Kobayashi for their generous hospitality.

References

[Baker et al. 2016] K. L. Baker, T. Kobayashi, and Y. Rieck, "The spectrum of the growth rate of the tunnel number is infinite", *Proc. Amer. Math. Soc.* **144**:8 (2016), 3609–3618. MR Zbl

[Bowman et al. 2015] R. S. Bowman, S. Taylor, and A. Zupan, "Bridge spectra of twisted torus knots", *Int. Math. Res. Not.* **2015**:16 (2015), 7336–7356. MR Zbl

[Casson and Gordon 1987] A. J. Casson and C. M. Gordon, "Reducing Heegaard splittings", *Topology Appl.* **27**:3 (1987), 275–283. MR Zbl

[Haken 1968] W. Haken, "Some results on surfaces in 3-manifolds", pp. 39–98 in *Studies in modern topology*, edited by P. J. Hilton, Math. Assoc. Amer., Englewood Cliffs, NJ, 1968. MR Zbl

[Hatcher 1982] A. E. Hatcher, "On the boundary curves of incompressible surfaces", *Pacific J. Math.* **99**:2 (1982), 373–377. MR Zbl

[Hempel 1976] J. Hempel, *3-manifolds*, Ann. of Math. Studies **86**, Princeton Univ. Press, 1976. MR Zbl

[Ichihara and Saito 2013] K. Ichihara and T. Saito, "Knots with arbitrarily high distance bridge decompositions", *Bull. Korean Math. Soc.* **50**:6 (2013), 1989–2000. MR Zbl

[Jaco 1980] W. Jaco, *Lectures on three-manifold topology*, CBMS Regional Conference Series in Mathematics **43**, American Mathematical Society, Providence, RI, 1980. MR Zbl

[Jaco and Shalen 1979] W. H. Jaco and P. B. Shalen, *Seifert fibered spaces in 3-manifolds*, Mem. Amer. Math. Soc. **220**, American Mathematical Society, Providence, RI, 1979. MR Zbl

[Johannson 1979] K. Johannson, *Homotopy equivalences of 3-manifolds with boundaries*, Lecture Notes in Mathematics **761**, Springer, Berlin, 1979. MR Zbl

[Kim 2005] S. H. Kim, "The tunnel number one knot with bridge number three is a (1, 1)-knot", *Kyungpook Math. J.* **45**:1 (2005), 67–71. MR Zbl

[Kobayashi and Rieck 2004] T. Kobayashi and Y. Rieck, "Local detection of strongly irreducible Heegaard splittings via knot exteriors", *Topology Appl.* **138**:1-3 (2004), 239–251. MR Zbl

[Kobayashi and Rieck 2006a] T. Kobayashi and Y. Rieck, "Heegaard genus of the connected sum of m-small knots", *Comm. Anal. Geom.* **14**:5 (2006), 1037–1077. MR Zbl

[Kobayashi and Rieck 2006b] T. Kobayashi and Y. Rieck, "On the growth rate of the tunnel number of knots", *J. Reine Angew. Math.* **592** (2006), 63–78. MR Zbl

[Kobayashi and Rieck 2008] T. Kobayashi and Y. Rieck, "Knot exteriors with additive Heegaard genus and Morimoto's conjecture", *Algebr. Geom. Topol.* **8**:2 (2008), 953–969. MR Zbl

[Kobayashi and Rieck 2009] T. Kobayashi and Y. Rieck, "Knots with $g(E(K)) = 2$ and $g(E(K \# K \# K)) = 6$ and Morimoto's conjecture", *Topology Appl.* **156**:6 (2009), 1114–1117. MR Zbl

[Kobayashi and Saito 2010] T. Kobayashi and T. Saito, "Destabilizing Heegaard splittings of knot exteriors", *Topology Appl.* **157**:1 (2010), 202–212. MR Zbl

[Miyazaki 1989] K. Miyazaki, "Conjugation and the prime decomposition of knots in closed, oriented 3-manifolds", *Trans. Amer. Math. Soc.* **313**:2 (1989), 785–804. MR Zbl

[Morimoto 1995] K. Morimoto, "There are knots whose tunnel numbers go down under connected sum", *Proc. Amer. Math. Soc.* **123**:11 (1995), 3527–3532. MR Zbl

[Morimoto 2008] K. Morimoto, "Essential surfaces in the exteriors of torus knots with twists on 2-strands", preprint, 2008, Available at http://tunnel-knot.sakura.ne.jp/TKSML.pdf.

[Morimoto et al. 1996] K. Morimoto, M. Sakuma, and Y. Yokota, "Examples of tunnel number one knots which have the property "$1 + 1 = 3$"", *Math. Proc. Cambridge Philos. Soc.* **119**:1 (1996), 113–118. MR Zbl

[Norwood 1982] F. H. Norwood, "Every two-generator knot is prime", *Proc. Amer. Math. Soc.* **86**:1 (1982), 143–147. MR Zbl

[Rieck 2000] Y. Rieck, "Heegaard structures of manifolds in the Dehn filling space", *Topology* **39**:3 (2000), 619–641. MR Zbl

[Scharlemann 1998] M. Scharlemann, "Local detection of strongly irreducible Heegaard splittings", *Topology Appl.* **90**:1-3 (1998), 135–147. MR Zbl

[Scharlemann and Thompson 1994] M. Scharlemann and A. Thompson, "Thin position for 3-manifolds", pp. 231–238 in *Geometric topology* (Haifa, 1992), edited by C. Gordon et al., Contemp. Math. **164**, American Mathematical Society, Providence, RI, 1994. MR Zbl

[Schultens 1993] J. Schultens, "The classification of Heegaard splittings for (compact orientable surface) $\times S^1$", *Proc. London Math. Soc.* (3) **67**:2 (1993), 425–448. MR Zbl

[Schultens 2004] J. Schultens, "Heegaard splittings of graph manifolds", *Geom. Topol.* **8** (2004), 831–876. MR Zbl

[Schultens 2014] J. Schultens, *Introduction to 3-manifolds*, vol. 151, Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 2014. MR

[Zupan 2014] A. Zupan, "Bridge spectra of iterated torus knots", *Comm. Anal. Geom.* **22**:5 (2014), 931–963. MR Zbl

Received July 18, 2016. Revised March 4, 2017.

TSUYOSHI KOBAYASHI
DEPARTMENT OF MATHEMATICS
NARA WOMEN'S UNIVERSITY
KITAUOYANISHI-MACHI, NARA 630-8506
JAPAN

tsuyoshi@cc.nara-wu.ac.jp

YO'AV RIECK
DEPARTMENT OF MATHEMATICAL SCIENCES
UNIVERSITY OF ARKANSAS
FAYETTEVILLE, AR 72701
UNITED STATES

yoav@uark.edu

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.103

EXTREMAL PAIRS OF YOUNG'S INEQUALITY FOR KAC ALGEBRAS

ZHENGWEI LIU AND JINSONG WU

In this paper, we prove a sum set estimate and the exact sum set theorem for unimodular Kac algebras. Combining the characterization of minimizers of the Donoso–Stark uncertainty principle and the Hirschman–Beckner uncertainty principle, we characterize the extremal pairs of Young's inequality and extremal operators of the Hausdorff–Young inequality for unimodular Kac algebras.

1. Introduction

Young's inequality for the real line $\mathbb{R}$ was first studied by Young [1912]. Beckner [1975] characterized the extremal pairs of Young's inequality for $\mathbb{R}$ with the sharp constant and consequently characterized the extremal functions of the Hausdorff–Young inequality. For general cases, Fournier [1977] characterized the extremal pairs of Young's inequality and the extremal functions of the Hausdorff–Young inequality for unimodular locally compact groups. (Note that Russo [1974] characterized the extremal functions of the Hausdorff–Young inequality directly.) For a long time, Young's inequality was showed for commutative algebras. Recently, S. Wang and the authors [Liu et al. 2017] proved Young's inequality for locally compact quantum groups. Bobkov, Madiman and Wang [Bobkov et al. 2011] conjectured that a fractional generalization of Young's inequality for $\mathbb{R}$ is true.

Kac algebras were introduced independently by L. I. Vainerman and G. I. Kac [Vaĭnerman 1974; Vaĭnerman and Kac 1973] and by Enock and Nest [Enock and Schwartz 1973; 1974; 1975]. These algebras generalized locally compact groups and their duals. Locally compact quantum groups introduced by J. Kustermans and S. Vaes [Kustermans and Vaes 2000; 2003] generalized Kac algebras. It is natural to ask what extremal pairs of Young's inequality for locally compact quantum groups are. Unfortunately, the methods to characterize extremal pairs of Young's inequality for locally compact groups [Fournier 1977] can not be applied to locally compact quantum groups. We plan to characterize the extremal pairs of Young's inequality for locally compact quantum groups. Our first aim in this direction is

MSC2010: 46L89, 58B32.
Keywords: Young's inequality, Kac algebras, sum set, uncertainty principles.

to characterize extremal pairs of Young's inequality for unimodular Kac algebras. Our proof for noncommutative algebras is quite different from the classical proof for commutative algebras.

In this paper, we will characterize extremal pairs of Young's inequality and extremal operators of the Hausdorff–Young inequality for unimodular Kac algebras. We show that extremal pairs and extremal operators are exactly bishifts of biprojections introduced in [Liu and Wu 2017] and we will use the notations therein. Prior to the characterization, we prove a sum set theorem for unimodular Kac algebras.

Main Theorem (sum set theorem[1], Theorem 3.1, Theorem 3.9). *Suppose $\mathbb{G}$ is a unimodular Kac algebra with a Haar tracial weight φ. Let p, q be projections in $L^\infty(\mathbb{G})$. Then*

$$\max\{\varphi(p), \varphi(q)\} \le \mathcal{S}(p * q),$$

where $\mathcal{S}(x) = \varphi(\mathcal{R}(x))$ and $\mathcal{R}(x)$ is the range projection of x, $x \in L^\infty(\mathbb{G})$. Moreover the following are equivalent:

(1) $\mathcal{S}(p * q) = \varphi(p) < \infty$;

(2) $\varphi(q)^{-1} p * q$ *is a projection in* $L^1(\mathbb{G})$;

(3) $\mathcal{S}(p * (q * R(q)^{*(m)}) * q^{*(j)}) = \varphi(p)$ *for some* $m \ge 0$, $j \in \{0, 1\}$, $m + j > 0$, $q^{*(0)}$ *means* q *vanishes*;

(4) *there exists a biprojection B such that q is a right subshift of B and* $p = \mathcal{R}(x * B)$ *for some* $x > 0$.

Combining the results above and the characterization of minimizers of the Hirschman–Beckner and the Donoho–Stark uncertainty principles for unimodular Kac algebras, we are able to characterize the extremal pairs of Young's inequality.

Theorem 4.8. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let x, y be φ-measurable. Then the following are equivalent*:

(1) $\|x * y\|_r = \|x\|_t \|y\|_s$ *for some* $1 < r, t, s < \infty$ *such that* $1/r + 1 = 1/t + 1/s$;

(2) $\|x * y\|_r = \|x\|_t \|y\|_s$ *for any* $1 \le r, t, s \le \infty$ *such that* $1/r + 1 = 1/t + 1/s$;

(3) *there exists a biprojection B such that* $x = ({}_h B a_x) * \mathcal{F}(\tilde{B}_g)$ *and* $y = \mathcal{F}(\tilde{B}_g) * (B_f a_y)$, *where $\tilde{B}$ is the range projection of $\mathcal{F}(B)$; B_g, B_f are right shifts of B; ${}_h B$ is left shift of B, and a_x, a_y are elements such that x, y are nonzero.*

Furthermore, we characterize the extremal operators of the Hausdorff–Young inequality for unimodular Kac algebra.

Theorem 5.2. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let x be φ-measurable. Then the following are equivalent*:

[1] We refer the reader to [Tao and Vu 2006] for a classical sum set theorem

(1) $\|\mathcal{F}(x)\|_{t/(t-1)} = \|x\|_t$ *for some* $1 < t < 2$;

(2) $\|\mathcal{F}(x)\|_{t/(t-1)} = \|x\|_t$ *for any* $1 \leq t \leq 2$;

(3) x *is a bishift of a biprojection.*

This paper is organized as follows. In Section 2, we recall some basic notations and properties of unimodular Kac algebras. In Section 3, we prove the sum set estimate and the exact inverse sum set theorem for unimodular Kac algebras. In Section 4, we characterize extremal pairs of Young's inequality for unimodular Kac algebras. In Section 5, we characterize extremal operators of the Hausdorff–Young inequality for unimodular Kac algebras.

2. Preliminaries

Let $\mathcal{M}$ be a von Neumann algebra acting on a Hilbert space $\mathcal{H}$ with a normal semifinite faithful tracial weight φ.

A closed densely defined operator x affiliated with $\mathcal{M}$ is called φ-measurable if for all $\epsilon > 0$ there exists a projection $p \in \mathcal{M}$ such that $p\mathcal{H} \subset \mathfrak{D}(x)$, and $\varphi(1-p) \leq \epsilon$, where $\mathfrak{D}(x)$ is the domain of x. Denote by $\widetilde{\mathcal{M}}$ the set of φ-measurable closed densely defined operators. Then $\widetilde{\mathcal{M}}$ is $*$-algebra with respect to strong sum, strong product, and adjoint operation. If x is a positive self-adjoint φ-measurable operator, then $x^\alpha \log x$ is φ-measurable for any $\alpha \in \mathbb{C}$ with $\Re\alpha > 0$, where $\Re\alpha$ is the real part of α.

For any positive self-adjoint operator x affiliated with $\mathcal{M}$, we put

$$\varphi(x) = \sup_{n \in \mathbb{N}} \varphi\left(\int_0^n t \, \mathrm{d}e_t\right),$$

where $x = \int_0^\infty t \, \mathrm{d}e_t$ is the spectral decomposition of x. Then for $t \in [1, \infty)$, the noncommutative L^t space $L^t(\mathcal{M})$ with respect to φ is given by

$$L^t(\mathcal{M}) = \{x \text{ densely defined, closed, affiliated with } \mathcal{M} \mid \varphi(|x|^t) < \infty\}.$$

The t-norm $\|x\|_t$ of x in $L^t(\mathcal{M})$ is given by $\|x\|_t = \varphi(|x|^t)^{1/t}$. We have that $L^p(\mathcal{M}) \subseteq \widetilde{\mathcal{M}}$. For more details on noncommutative L^p space we refer to [Terp 1981; 1982].

Now let us recall the definition of locally compact quantum groups in [Kustermans and Vaes 2000].

Let $\mathcal{M}$ be a von Neumann algebra with a normal semifinite faithful weight φ. Then $\mathfrak{N}_\varphi = \{x \in \mathcal{M} \mid \varphi(x^*x) < \infty\}$, $\mathfrak{M}_\varphi = \mathfrak{N}_\varphi^* \mathfrak{N}_\varphi$, $\mathfrak{M}_\varphi^+ = \{x \geq 0 \mid x \in \mathfrak{M}_\varphi\}$. Denote by $\mathcal{H}_\varphi$ the Hilbert space by taking the closure of $\mathfrak{N}_\varphi$. The map $\Lambda_\varphi : \mathfrak{N}_\varphi \mapsto \mathcal{H}_\varphi$ is the inclusion map.

A locally compact quantum group $\mathbb{G} = (\mathcal{M}, \Delta, \varphi, \psi)$ consists of

(1) a von Neumann algebra $\mathcal{M}$,

(2) a normal, unital, *-homomorphism $\Delta : \mathcal{M} \to \mathcal{M} \mathbin{\overline{\otimes}} \mathcal{M}$ such that $(\Delta \otimes \iota) \circ \Delta = (\iota \otimes \Delta) \circ \Delta$,

(3) a normal, semifinite, faithful weight φ such that $(\iota \otimes \varphi)\Delta(x) = \varphi(x)1$, $\forall x \in \mathfrak{M}_\varphi^+$; a normal, semifinite, faithful weight ψ such that $(\psi \otimes \iota)\Delta(x) = \psi(x)1$, $\forall x \in \mathfrak{M}_\psi^+$,

where $\overline{\otimes}$ denotes the von Neumann algebra tensor product and ι denotes the identity map. The normal, unital, *-homomorphism Δ is a comultiplication of $\mathcal{M}$, φ is the left Haar weight, and ψ is the right Haar weight.

We assume that $\mathcal{M}$ acts on $\mathcal{H}_\varphi$. There exists a unique unitary operator $W \in \mathcal{B}(\mathcal{H}_\varphi \otimes \mathcal{H}_\varphi)$ which is known as the multiplicative unitary defined by

$$W^*(\Lambda_\varphi(a) \otimes \Lambda_\varphi(b)) = (\Lambda_\varphi \otimes \Lambda_\varphi)(\Delta(b)(a \otimes 1)), \quad a, b \in \mathfrak{N}_\varphi.$$

Moreover for any $x \in \mathcal{M}$, $\Delta(x) = W^*(1 \otimes x)W$.

For the locally compact quantum group $\mathbb{G}$, there exists an antipode S, a scaling automorphism group τ, and a unitary antipode R and there also exists a dual locally compact quantum group $\hat{\mathbb{G}} = (\hat{\mathcal{M}}, \hat{\Delta}, \hat{\varphi}, \hat{\psi})$ of $\mathbb{G}$. The antipode, the scaling group, and the unitary antipode of $\hat{\mathbb{G}}$ are denoted by $\hat{S}$, $\hat{\tau}$, and $\hat{R}$ respectively. We refer to [Kustermans and Vaes 2000; 2003] for more details.

For any $\omega \in \mathcal{M}_*$, $\lambda(\omega) = (\omega \otimes \iota)(W)$ is the Fourier representation of ω, where $\mathcal{M}_*$ is the Banach space of all bounded normal functionals on $\mathcal{M}$. For any ω, θ in $\mathcal{M}_*$, the convolution $\omega * \theta$ is given by

$$\omega * \theta = (\omega \otimes \theta)\Delta.$$

S. Wang and the authors [Liu et al. 2017] defined the convolution of $x \in L^t(\mathbb{G})$ and $y \in L^s(\mathbb{G})$ for $1 \le t, s \le 2$. If the left Haar weights φ, $\hat{\varphi}$ of $\mathbb{G}$ and $\hat{\mathbb{G}}$ respectively are tracial weights, we have that the convolution is well-defined for $1 \le t, s \le \infty$ by the results in [Liu et al. 2017].

For any locally compact quantum group $\mathbb{G}$, the Fourier transforms $\mathcal{F}_t : L^t(\mathbb{G}) \to L^s(\hat{\mathbb{G}})$ are well-defined, where $1/t + 1/s = 1$, $1 \le t \le 2$. (See [Cooney 2010; Caspers 2013] for the definition of Fourier transforms and [Van Daele 2007] for the definition of the Fourier transform for algebraic quantum groups.) For any x in $L^1(\mathbb{G})$, we denote by $x\varphi$ the bounded linear functional on $L^\infty(\mathbb{G})$ given by $(x\varphi)(y) = \varphi(yx)$ for any y in $L^\infty(\mathbb{G})$. Recall that a projection p in $L^1(\mathbb{G}) \cap L^\infty(\mathbb{G})$ is a biprojection if $\mathcal{F}_1(p\varphi)$ is a multiple of a projection in $L^\infty(\hat{\mathbb{G}})$. A projection x in $L^1(\mathbb{G}) \cap L^2(\mathbb{G})$ is called a left shift of a biprojection B if $\varphi(x) = \varphi(B)$ and $x * B = \varphi(B)x$. A projection x in $L^1(\mathbb{G}) \cap L^2(\mathbb{G})$ is called a right shift of a biprojection B if $\varphi(x) = \varphi(B)$ and $B * x = \varphi(B)x$. Denote by $\tilde{B}$ the range projection of $\mathcal{F}(B)$. A nonzero element x in $L^\infty(\mathbb{G})$ is said to be a bishift of a biprojection B if there exists a right shift B_g of the biprojection B and a right shift $\tilde{B}_h$ of the biprojection

$\tilde{B}$ and an element y in $L^\infty(\mathbb{G})$ such that

$$x = \widehat{\mathcal{F}}(\tilde{B}_h) * (B_g y).$$

(We refer to [Jiang et al. 2017; Liu and Wu 2017; Liu et al. 2017] for more properties of biprojections and bishifts of biprojections.)

Throughout this paper, we focus on a unimodular Kac algebra $\mathbb{G}$, which is a locally compact quantum group subject to the condition that $\varphi = \psi$ is tracial. (See [Enock and Schwartz 1992] for more details.) For a unimodular Kac algebra $\mathbb{G}$, we denote by $\mathcal{F}$ the Fourier transform for simplicity.

Proposition 2.1. *Suppose $\mathbb{G}$ is a unimodular Kac algebra and $a \in L^t(\mathbb{G})$, $b \in L^s(\mathbb{G})$, $c \in L^r(\mathbb{G})$ such that $1 \le r, t, s \le \infty$ and $1/r + 1/t + 1/s = 2$. Then*

$$\varphi((a * b)c) = \varphi\big((R(c) * a)R(b)\big) = \varphi\big((b * R(c))R(a)\big).$$

Proof. Suppose that $a, b, c \in L^1(\mathbb{G}) \cap L^\infty(\mathbb{G})$. Then

$$\begin{aligned}
\varphi((a * b)c) &= (a\varphi \otimes b\varphi)(\Delta(c)) \\
&= (a\varphi R)\big((\iota \otimes \varphi)(\Delta(c)(1 \otimes b))\big) \\
&= (a\varphi R \otimes \varphi c)(\Delta(b)) \quad \text{strong left invariance} \\
&= (a\varphi R \otimes R(c)\varphi R)(\Delta(b)) \\
&= (R(c)\varphi \otimes a\varphi)(\Delta(R(b))) \\
&= \varphi\big((R(c) * a)R(b)\big) \\
&= \varphi\big((b * R(c))R(a)\big).
\end{aligned}$$

By Young's inequality [Liu et al. 2017], we see that the proposition is true for $a \in L^t(\mathbb{G})$, $b \in L^s(\mathbb{G})$, $c \in L^r(\mathbb{G})$ such that $1 \le r, t, s \le \infty$ and $1/r + 1/t + 1/s = 2$. $\square$

Proposition 2.2. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let $x \in L^t(\mathbb{G})$, $y \in L^s(\mathbb{G})$ be positive such that $1 \le t, s \le \infty$, $1/t + 1/s = 1$ Then*

$$\mathcal{R}(x * y) = \sup\{\mathcal{R}(p * q) \mid p \le \mathcal{R}(x), q \le \mathcal{R}(y),\ p, q \text{ are projections in } L^1(\mathbb{G})\}.$$

Proof. Let e_n be the spectral projection of x corresponding to $[1/n, n]$ and f_m the spectral projection of y corresponding to $[1/m, m]$ for $n, m \in \mathbb{N}$. Then we have that $e_n, f_m \in L^1(\mathbb{G})$ and

$$\frac{1}{nm} e_n * f_m \le e_n x e_n * f_m y f_m \le mn e_n * f_m.$$

Hence $\mathcal{R}(e_n * f_m) \le \mathcal{R}(x * y)$. Let $Q = \sup\{\mathcal{R}(p * q) \mid p \le \mathcal{R}(x), q \le \mathcal{R}(y), p, q$ are projections in $L^1(\mathbb{G})\}$. Then we have that $Q = \sup_{n,m} \mathcal{R}(e_n * f_m)$. Therefore $Q \le \mathcal{R}(x * y)$. Assume that there is a nonzero vector $\xi \in \mathcal{H}_\varphi$ such that $Q\xi = 0$ and $\mathcal{R}(x * y)\xi = \xi$. We have that $(e_n * f_m)\xi = 0$ for any $n, m \in \mathbb{N}$ and then

$(e_n x e_n * f_m y f_m)\xi = 0$. Therefore $(x * y)\xi = 0$, which leads a contradiction and $Q = \mathcal{R}(x * y)$. □

Definition 2.3. Suppose $\mathbb{G}$ is a unimodular Kac algebra and $x \in L^t(\mathbb{G})$, $y \in L^s(\mathbb{G})$ are positive for $1 \le t, s \le \infty$. We define the symbol $\mathcal{R}(x * y)$ in terms of x, y as

$$\mathcal{R}(x * y) = \sup\{\mathcal{R}(p * q) \mid p \le \mathcal{R}(x), q \le \mathcal{R}(y),\ p, q \text{ are projections in } L^1(\mathbb{G})\},$$

and

$$\mathcal{S}(x * y) = \varphi(\mathcal{R}(x * y)).$$

Remark 2.4. In Definition 2.3, $\mathcal{R}(x * y)$ and $\mathcal{S}(x * y)$ are symbols. Proposition 2.2 shows that the symbol $\mathcal{R}(x * y)$ is the usual one when $x * y$ is well-defined.

3. The exact inverse sum set theorem

The sum set estimate is a theory of counting the cardinalities of additive sets in additive combinatorics [Tao and Vu 2006]. The sum set estimate for Kac algebras has a different behavior, because of the different types of topology. In this section, we prove a sum set estimate and the exact inverse sum set theorem for unimodular Kac algebras.

Theorem 3.1 (sum set estimate). *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let p, q be projections in $L^\infty(\mathbb{G})$. Then*

$$\max\{\varphi(p), \varphi(q)\} \le \mathcal{S}(p * q).$$

Moreover, $\mathcal{S}(p * q) = \varphi(p) < \infty$ if and only if $\varphi(q)^{-1} p * q$ is a projection in $L^1(\mathbb{G})$.

Proof. First, we assume that p, q are projections in $L^1(\mathbb{G})$. If $\mathcal{S}(p * q) = \infty$, then the inequality is true. We assume that $\mathcal{S}(p * q) < \infty$. By Hölder's inequality,

$$\|p * q\|_1 \le \|\mathcal{R}(p * q)\|_2 \|p * q\|_2.$$

Note that

$$\|p * q\|_1 = \varphi(p * q) = \varphi(p)\varphi(q),$$

and

$$\|\mathcal{R}(p * q)\|_2^2 = \mathcal{S}(p * q).$$

By Young's inequality [Liu et al. 2017], we have

$$\|p * q\|_2 \le \|p\|_1 \|q\|_2 = \varphi(p)\varphi(q)^{1/2},$$

and

$$\|p * q\|_2 \le \|q\|_1 \|p\|_2 = \varphi(q)\varphi(p)^{1/2}.$$

Now we obtain that

$$\varphi(p)\varphi(q) \leq \mathcal{S}(p*q)^{1/2}\varphi(p)\varphi(q)^{1/2},$$

i.e., $\mathcal{S}(p*q) \geq \varphi(q)$. Similarly, we have $\mathcal{S}(p*q) \geq \varphi(p)$. Hence

$$\max\{\varphi(p), \varphi(q)\} \leq \mathcal{S}(p*q).$$

For arbitrary projections p, q in $L^\infty(\mathbb{G})$, by Definition 2.3, we have that

$$\max\{\varphi(p), \varphi(q)\} \leq \mathcal{S}(p*q).$$

If $\mathcal{S}(p*q) = \varphi(p) < \infty$, the inequalities above are equalities. Thus $p*q = \lambda\mathcal{R}(p*q)$ for some $\lambda > 0$ (by the equality of Hölder's inequality) and $\|p*q\|_2 = \|p\|_1\|q\|_2$. Now we see that $p*q = \varphi(q)^{-1}\mathcal{R}(p*q)$.

If $\varphi(q)^{-1}p*q$ is a projection, we have $\mathcal{S}(p*q) = \varphi(q)^{-1}\varphi(p*q) = \varphi(p)$. □

Remark 3.2. By the results in [Jiang et al. 2016], there is an upper bound for the finite dimensional case. But this is not always true for unimodular Kac algebras. For the real line $\mathbb{R}$, we let p be the characteristic function on the interval [0, 1] and q the characteristic function on the set $\cup_{k\in\mathbb{Z}}[k, k+1/(k^2+1)]$. Then $\mathcal{R}(p*q) = 1$.

Corollary 3.3. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let v, w be partial isometries in $L^1(\mathbb{G}) \cap L^\infty(\mathbb{G})$ such that $\|v*w\|_1 = \|v\|_1\|w\|_1$. Then*

$$\max\{\varphi(|v|), \varphi(|w|)\} \leq \mathcal{S}(v*w).$$

Moreover $\mathcal{S}(v*w) = \varphi(|w|) < \infty$ if and only if $1/\varphi(|v|)\, v*w$ is a partial isometry in $L^1(\mathbb{G})$.

Proof. The proof is similar to the one of Theorem 3.1. □

Proposition 3.4. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let p, q be projections in $L^1(\mathbb{G}) \cap L^\infty(\mathbb{G})$. Then the following are equivalent:*

(1) $\|p*q\|_t = \|p\|_t\|q\|_1$ *for some* $1 < t < \infty$;

(2) $\|p*q\|_t = \|p\|_t\|q\|_1$ *for any* $1 \leq t \leq \infty$;

(3) $\mathcal{S}(p*q) = \varphi(p)$.

Proof. (1) ⇒ (3): Suppose that $\|p*q\|_t = \|p\|_t\|q\|_1$ for some $1 < t < \infty$. Note that $\|p*q\|_\infty \leq \|q\|_1$. By the spectral decomposition, we have

$$\frac{1}{\varphi(q)}p*q = \int_0^1 \lambda\, \mathrm{d}E_\lambda,$$

where $\{E_\lambda\}_\lambda$ is a resolution of the identity for $p*q$. By the assumption, we obtain

$$\int_0^1 \lambda^t \varphi(\mathrm{d}E_\lambda) = \varphi(p).$$

Note that $\|p*q\|_1 = \|p\|_1\|q\|_1$, i.e.,

$$\int_0^1 \lambda\varphi(\mathrm{d}E_\lambda) = \varphi(p).$$

Combining the two equations above, we see that $E(\{1\}) = 1/\varphi(q)\, p*q$ and $\varphi(E(\{1\})) = \varphi(p)$, i.e., $\mathcal{S}(p*q) = \varphi(p)$.

(3) ⇒ (2): Suppose that $\mathcal{S}(p*q) = \varphi(p)$. By Theorem 3.1, we have that $1/\varphi(q)\, p*q$ is a projection. Hence for any $1 \le t \le \infty$,

$$\frac{1}{\varphi(q)}\|p*q\|_t = \left\|\frac{1}{\varphi(q)}p*q\right\|_t = \|\mathcal{R}(p*q)\|_t = \mathcal{S}(p*q)^{1/t} = \varphi(p)^{1/t} = \|p\|_t,$$

i.e., $\|p*q\|_t = \|p\|_t\|q\|_1$.

(2) ⇒ (1): It is obvious. □

Proposition 3.5. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let $x, y \in L^1(\mathbb{G}) \cap L^2(\mathbb{G})$ be nonzero positive elements. Then the following are equivalent*:

(1) $\|x*y\|_2 = \|x\|_1\|y\|_2$;

(2) *there exists a biprojection B such that $\mathcal{R}(R(x)*x) \le B$, $(y*R(y))B = \|y*R(y)\|_\infty B$ and $\|y*R(y)\|_\infty = \|y\|_2^2$.*

Proof. (1) ⇒ (2): Note that

$$\begin{aligned}\|x*y\|_2^2 &= \varphi((x*y)(x*y)) \\ &= \varphi\big(R(y)((R(y)*R(x))*x)\big) \\ &= \varphi\big((R(x)*x)(y*R(y))\big) \\ &\le \|R(x)*x\|_1\|y*R(y)\|_\infty \\ &\le \|x\|_1^2\|y\|_2^2.\end{aligned}$$

If $\|x*y\|_2 = \|x\|_1\|y\|_2$, then $\varphi((R(x)*x)(y*R(y))) = \|R(x)*x\|_1\|y*R(y)\|_\infty$ and $\|y*R(y)\|_\infty = \|y\|_2^2$. Let B be the spectral projection of $y*R(y)$ corresponding to $\|y*R(y)\|_\infty$. By [Liu and Wu 2017, Proposition 3.14 and Corollary 3.16], we have that B is a biprojection.

(2) ⇒ (1): It follows by the argument above. □

Proposition 3.6. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. If there exists a nonzero positive element $x \in L^1(\mathbb{G}) \cap L^t(\mathbb{G})$ for some $t > 1$ such that $x*x = x$, then $1/\hat{\varphi}(\mathcal{F}(x))\, x$ is a biprojection.*

Proof. By assumption, we obtain that $\|x\|_1 = 1$ and $\mathcal{F}(x)^2 = \mathcal{F}(x)$. By the Hausdorff–Young inequality [Cooney 2010], we have that $\|\mathcal{F}(x)\|_\infty \le \|x\|_1 = 1$. Hence $\mathcal{F}(x)$ is a contractive idempotent, i.e., $\mathcal{F}(x)$ is a projection. We see that $\mathcal{F}(x) = \mathcal{F}(x)^*$ and $x = R(x)$.

If $t \geq 2$, we have that $x \in L^1(\mathbb{G}) \cap L^2(\mathbb{G})$. If $1 < t < 2$, we let $\epsilon = t - 1$, then $\|x\|_{1+\epsilon} < \infty$. We show that $x \in L^2(\mathbb{G})$. Let $K(s) = 2s/(1+s)$. Then $K(s) < s$ when $s > 1$ and $K^n(s) \to 1$ as $n \to \infty$ for any $s \geq 1$. By Young's inequality [Liu et al. 2017], we have that

$$\|x\|_2 = \|x * x\|_2 \leq \|x\|_{K(2)}^2 = \|x * x\|_{K(2)}^2 \leq \cdots \leq \|x\|_{K^n(2)}^{2^n} \leq \|x\|_{1+\epsilon}^{2^n} < \infty$$

for some n large enough. Hence $x \in L^1(\mathbb{G}) \cap L^2(\mathbb{G})$. Note that $\|x * R(x)\|_2 = \|x\|_2 = \|x\|_2\|x\|_1$. By Proposition 3.5, we see that there exists a biprojection B such that $\mathcal{R}(R(x) * x) \leq B$ and $(R(x) * x)B = \|R(x) * x\|_\infty B$. Hence

$$x = R(x) * x = \|R(x) * x\|_\infty B = \|x\|_2^2 B = \hat{\varphi}(\mathcal{F}(x))B. \qquad \square$$

Definition 3.7. Suppose $\mathbb{G}$ is a unimodular Kac algebra and there exists a biprojection B in $L^1(\mathbb{G})$. A projection q in $L^1(\mathbb{G})$ is said to be a right (left) subshift of the biprojection B if there exists a right (left) shift B_g of B such that $q \leq B_g$.

Proposition 3.8. *Suppose $\mathbb{G}$ is a unimodular Kac algebra and B is a biprojection in $L^1(\mathbb{G}) \cap L^\infty(\mathbb{G})$. Let q be a projection in $L^\infty(\mathbb{G})$. Then*

$$\mathcal{R}(q * R(q)) \leq B \text{ if and only if } q \text{ is a right subshift of } B,$$

and

$$\mathcal{R}(R(q) * q) \leq B \text{ if and only if } q \text{ is a left subshift of } B.$$

Proof. Suppose that $\mathcal{R}(q * R(q)) \leq B$. Let $p_1 = \mathcal{R}(B * q)$. We shall show that p_1 is a projection in $L^1(\mathbb{G})$. Since

$$\mathcal{R}(B * q * R(q) * B) \leq \mathcal{R}(B * B * B) = B,$$

by Theorem 3.1, we see that $p_1,\ \mathcal{R}(p_1 * R(p_1)) \in L^1(\mathbb{G})$, and

$$\varphi(p_1) \leq \mathcal{S}(p_1 * R(p_1)) \leq \varphi(B) < \infty.$$

On the other hand, $\varphi(p_1) \geq \varphi(B)$ by Theorem 3.1. Then we obtain that $\varphi(p_1) = \varphi(B)$. By Theorem 3.1, we have that $1/\varphi(q)\, B * q$ is a projection and $p_1 = 1/\varphi(q)\, B * q$.

Suppose q is a right subshift of B. Let p_1 be the right subshift of B such that $q \leq p_1$. Then $q * R(q) \leq p_1 * R(p_1) = \varphi(B)B$. $\square$

Theorem 3.9 (exact inverse sum set theorem). *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let p, q be projections in $L^1(\mathbb{G}) \cap L^\infty(\mathbb{G})$. Then the following are equivalent*:

(1) $\mathcal{S}(p * q) = \varphi(p)$;

(2) $\mathcal{S}(p * (q * R(q))^{*(m)}) * q^{*(j)} = \varphi(p)$ *for some* $m \geq 0$, $j \in \{0, 1\}$, $m + j > 0$, $q^{*(0)}$ *means* q *vanishes*;

(3) *there exists a biprojection B such that q is a right subshift of B and $p = \mathcal{R}(x * B)$ for some $x > 0$.*

Proof. (1) $\Rightarrow$ (3): By Proposition 3.4, we have that $\|p * q\|_2 = \|p\|_2 \|q\|_1$. By Proposition 3.5, we see that there is a biprojection B such that $\mathcal{R}(q * R(q)) \leq B$ and $(R(p) * p)B = \|p\|_2^2 B$. Since

$$\varphi((p * B)p) = \varphi(B(R(p) * p)) = \varphi(p)\varphi(B) = \varphi(p * B),$$

we obtain that $\mathcal{R}(p * B) \leq p$. By Theorem 3.1, we have that $\mathcal{R}(p * B) = p$.
(3) $\Rightarrow$ (2): Let $p = \mathcal{R}(x * B)$. Then $\mathcal{R}(p * B) = p$ and hence $p * B = \varphi(B)p$ by Theorem 3.1. Note that

$$\mathcal{R}((q * R(q))^{*(m+j)}) \leq \mathcal{R}(B^{*(m+j)}) = B.$$

By Theorem 3.1, we have

$$\begin{aligned}
\varphi(p) &\leq \mathcal{S}(p * (q * R(q))^{*(m)} * q^{*(j)}) \\
&\leq \mathcal{S}\big(\mathcal{R}(p * (q * R(q))^{*(m)} * q^{*(j)}) * R(q)^{*(j)}\big) \\
&\leq \mathcal{S}(p * B) = \varphi(p),
\end{aligned}$$

i.e.,

$$\mathcal{S}(p * (q * R(q))^{*(m)} * q^{*(j)}) = \varphi(p).$$

(2) $\Rightarrow$ (1): By Theorem 3.1, we have that

$$\varphi(p) = \mathcal{S}(p * (q * R(q))^{*(m)} * q^{*(j)}) \geq \mathcal{S}(p * q) \geq \varphi(p).$$

Hence $\mathcal{S}(p * q) = \varphi(p)$. □

4. Extremal pairs of Young's inequality

In this section, we characterize extremal pairs of Young's inequality for unimodular Kac algebras.

Proposition 4.1. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let v, w be partial isometries in $L^1(\mathbb{G}) \cap L^\infty(\mathbb{G})$. Then the following are equivalent*:

(1) $\|v * w\|_t = \|v\|_t \|w\|_1$ *for some* $1 < t < \infty$;

(2) $\|v * w\|_t = \|v\|_t \|w\|_1$ *for any* $1 \leq t \leq \infty$;

(3) $1/(\varphi(|w|))\,|v * w|$ *is a projection and* $\|v * w\|_1 = \|v\|_1 \|w\|_1$.

Proof. By Corollary 3.3 and a similar argument of Proposition 3.4, we have the proposition proved. □

Proposition 4.2. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let v, w be partial isometries. Then the following are equivalent*:

(1) $\|v * w\|_r = \|v\|_t \|w\|_s$ *for some* $1 < t, r, s < \infty$ *such that* $1/r + 1 = 1/t + 1/s$;

(2) $\|v * w\|_r = \|v\|_t \|w\|_s$ *for any* $1 \le r, t, s \le \infty$ *such that* $1/r + 1 = 1/t + 1/s$.

(3) *there exists a biprojection* B *such that* $v = ({}_h B y_v) * \hat{\mathcal{F}}(\tilde{B}_g)$ *and* $w = \hat{\mathcal{F}}(\tilde{B}_g) * (B_f y_w)$, *where* B_g, B_f *are right shifts of* B, ${}_h B$ *is a left shift of* B *and* y_v, y_w *are elements such that* v, w *are nonzero partial isometries.*

Proof. (1) $\Rightarrow$ (2): Suppose that $\|v * w\|_r = \|v\|_t \|w\|_s$ for some $1 < r, t, s < \infty$ such that $1/r + 1 = 1/t + 1/s$. By Young's inequality in [Liu et al. 2017], we have

$$\|v * w\|_r \le \|v\|_r \|w\|_1, \quad \|v * w\|_r \le \|v\|_1 \|w\|_r,$$

and hence $\varphi(|v|) = \varphi(|w|)$. By Proposition 4.1, we see that $\|v * w\|_{\tilde{r}} = \varphi(|v|)^{1+1/\tilde{r}}$ for any $1 \le \tilde{r} \le \infty$. Therefore $\|v * w\|_{\tilde{r}} = \|v\|_{\tilde{t}} \|w\|_{\tilde{s}}$ for any $1 \le \tilde{r}, \tilde{t}, \tilde{s} \le \infty$ with $1/\tilde{r} + 1 = 1/\tilde{t} + 1/\tilde{s}$.

(2) $\Rightarrow$ (3): Let $r = 2$. Then $1 \le t, s \le 2$. By Hölder's inequality and the Hausdorff–Young inequality [Cooney 2010], we obtain that

$$\begin{aligned}\|v\|_t \|w\|_s &= \|v * w\|_2 \\ &= \|\mathcal{F}(v)\mathcal{F}(w)\|_2 \le \|\mathcal{F}(v)\|_{t/(t-1)} \|\mathcal{F}(w)\|_{s/(s-1)} \le \|v\|_t \|w\|_s.\end{aligned}$$

Hence for any $1 \le t,\ s \le 2$,

$$\|\mathcal{F}(v)\|_{t/(t-1)} = \|v\|_t, \quad \|\mathcal{F}(w)\|_{s/(s-1)} = \|w\|_s, \tag{1}$$

and

$$\|\mathcal{F}(v)\mathcal{F}(w)\|_2 = \|\mathcal{F}(v)\|_{t/(t-1)} \|\mathcal{F}(w)\|_{s/(s-1)}. \tag{2}$$

For (1), by [Liu and Wu 2017, Proposition 3.6], we have that v, w are minimizers of the Hirschman–Beckner uncertainty principle for unimodular Kac algebras. By [Liu and Wu 2017, Theorem 3.15], we see that v, w are bishifts of biprojections. By Lemma 4.4, we have that

$$\|v\|_t \|w\|_s = \|v * w\|_r \le \||v| * |w|\|_r^{1/2} \||v^*| * |w^*|\|_r^{1/2} \le \|v\|_t \|w\|_s.$$

For (2), we have that

$$|\mathcal{F}(v)| = |\mathcal{F}(w)^*|,$$

i.e., $\mathcal{R}((\mathcal{F}(v))^*) = \mathcal{R}(\mathcal{F}(w))$.

By Theorem 3.9, we have that there exists a biprojection B such that $|v|$ is a left shift ${}_h B$ of B and $|w|$ is a right shift B_f of B. By the definition of a bishift of a biprojection, we have that $w = \hat{\mathcal{F}}(\tilde{B}_g) * (B_f y_w)$ for some right shift of $\tilde{B}$. By [Liu and Wu 2017, Proposition 3.11], $\mathcal{R}(\mathcal{F}(w)) = \tilde{B}_g$. Hence $\mathcal{R}((\mathcal{F}(v))^*) = \tilde{B}_g$. By [Liu and Wu 2017, Theorem 3.18], we have that $v = ({}_h B y_v) * \hat{\mathcal{F}}(\tilde{B}_g)$.

(3) $\Rightarrow$ (2): Since v, w are bishifts of the biprojection B, we have that system of equations (1) are true. By [Liu and Wu 2017, Proposition 3.11], we have

$$\mathcal{R}(\mathcal{F}(w)) = \mathcal{R}((\mathcal{F}(v))^*) = \tilde{B}_g.$$

Note that $\varphi(|v|) = \varphi({}_hB) = \varphi(B_f) = \varphi(|w|)$ and $\mathcal{F}(v), \mathcal{F}(w)$ are multiples of partial isometries. We see $|\mathcal{F}(v)| = |\mathcal{F}(w)^*|$ and that

$$\|v * w\|_2 = \|v\|_t \|w\|_s$$

for any $1 \leq t, s \leq 2$ from the argument for "(2) $\Rightarrow$ (3)". By Proposition 4.1, we have $\|v * w\|_r = \|v\|_r \|w\|_1$ for any $1 \leq r \leq \infty$. Therefore (2) is true.

(2) $\Rightarrow$ (1): It is obvious. □

Lemma 4.3. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. For any a, b in $L^2(\mathbb{G}) \cap L^\infty(\mathbb{G})$, we define $v_{a,b} : L^2(\mathbb{G}) \otimes L^2(\mathbb{G}) \to L^2(\mathbb{G})$ given by*

$$v_{a,b}(\Lambda_\varphi(x_1) \otimes \Lambda_\varphi(x_2)) = \Lambda_\varphi(ax_1 * bx_2)$$

for any x_1, x_2 in $L^2(\mathbb{G}) \cap L^\infty(\mathbb{G})$. Then $v_{a,b}$ is bounded and $v_{a,b} v_{a,b}^* = aa^* * bb^*$. Moreover,

$$\|v_{a,b}\|_\infty = \|aa^* * bb^*\|_\infty^{1/2}.$$

Proof. For any $y \in L^2(\mathbb{G}) \cap L^\infty(\mathbb{G})$, we have that

$$\begin{aligned}
\langle v_{a,b}(\Lambda_\varphi(x_1) \otimes \Lambda_\varphi(x_2)), \Lambda_\varphi(y)\rangle &= \langle \Lambda_\varphi(ax_1 * bx_2), \Lambda_\varphi(y)\rangle \\
&= \varphi(y^*(ax_1 * bx_2)) \\
&= (\varphi \otimes \varphi)((1 \otimes y^*)(R \otimes \iota)(\Delta(bx_2))(ax_1 \otimes 1)) \\
&= (\varphi \otimes \varphi)((R \otimes \iota)(\Delta(bx_2))(ax_1 \otimes y^*)) \\
&= \varphi(R((\iota \otimes \varphi)(\Delta(bx_2)(1 \otimes y^*))ax_1) \\
&= (\varphi \otimes \varphi)((ax_1 \otimes bx_2)\Delta(y^*)) \\
&= (\varphi \otimes \varphi)((x_1 \otimes x_2)\Delta(y^*)(a \otimes b)).
\end{aligned}$$

Note that

$$\begin{aligned}
(\varphi \otimes \varphi)(\Delta(y^*)(aa^* \otimes bb^*)\Delta(y)) &= (\varphi \otimes \varphi)((aa^* \otimes bb^*)\Delta(yy^*)) \\
&= \varphi((yy^*)(aa^* * bb^*)) \leq \|aa^* * bb^*\|_\infty \varphi(yy^*) \\
&\leq \|y\|_2^2 \|a\|_2^2 \|b\|_\infty^2;
\end{aligned}$$

the last inequality follows from Young's inequality in [Liu et al. 2017]. Then we have that

$$\begin{aligned}
&\big\langle v_{a,b}(\Lambda_\varphi(x_1) \otimes \Lambda_\varphi(x_2)), \Lambda_\varphi(y)\big\rangle \\
&\qquad = \big\langle \Lambda_\varphi(x_1) \otimes \Lambda_\varphi(x_2), (\Lambda_\varphi \otimes \Lambda_\varphi)((a^* \otimes b^*)\Delta(y))\big\rangle.
\end{aligned}$$

Therefore

$$\|v_{a,b}\| \leq \|a\|_2\|b\|_\infty \quad \text{and} \quad v_{a,b}^*\Lambda_\varphi(y) = (\Lambda_\varphi \otimes \Lambda_\varphi)((a^* \otimes b^*)\Delta(y))$$

whenever $y \in L^2(\mathbb{G}) \cap L^\infty(\mathbb{G})$.

Now we have to check that $vv^* = aa^* * bb^*$. First, write $\Delta(y) = \sum_\beta y_{\beta 1} \otimes y_{\beta 2}$. Then

$$\begin{aligned} v_{a,b}v_{a,b}^*\Lambda_\varphi(y) &= v_{a,b}((\Lambda_\varphi \otimes \Lambda_\varphi)((a^* \otimes b^*)\Delta(y))) \\ &= \sum_\beta v_{a,b}(\Lambda_\varphi(a^* y_{\beta 1}) \otimes \Lambda_\varphi(b^* y_{\beta 2})) \\ &= \sum_\beta \Lambda_\varphi((aa^* y_{\beta 1}) * (bb^* y_{\beta 2})) \\ &= \sum_\beta \hat{\Lambda}(\lambda((aa^* y_{\beta 1}\varphi) * (bb^* y_{\beta 2}\varphi))) \\ &= \sum_\beta \hat{\Lambda}(\lambda((aa^* y_{\beta 1}\varphi) \otimes (bb^* y_{\beta 2}\varphi)\Delta)) \\ &= \hat{\Lambda}(\lambda((aa^* * bb^*) y\varphi)) \\ &= (aa^* * bb^*)\Lambda_\varphi(y), \end{aligned}$$

i.e., $v_{a,b}v_{a,b}^* = aa^* * bb^*$. □

For any element x in a von Neumann algebra, $x = w_x|x|$ is the polar decomposition of x.

Lemma 4.4. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let $x \in L^t(\mathbb{G})$ and $y \in L^s(\mathbb{G})$ such that $1 + 1/r = 1/t + 1/s$. Then*

$$\|x * y\|_r \leq \||x| * |y|\|_r^{1/2}\||x^*| * |y^*|\|_r^{1/2}.$$

Proof. We assume that x, y are in $L^1(\mathbb{G}) \cap L^\infty(\mathbb{G})$. By Lemma 4.3, we define $v_{w_x|x|^{1/2}, w_y|y|^{1/2}}$ and $v_{|x|^{1/2},|y|^{1/2}}$. Then by Lemma 4.3 again,

$$v_{w_x|x|^{1/2}, w_y|y|^{1/2}} v_{|x|^{1/2},|y|^{1/2}}^* = x * y.$$

Let $\tilde{x} = v_{w_x|x|^{1/2}, w_y|y|^{1/2}}$ and $\tilde{y} = v_{|x|^{1/2},|y|^{1/2}}$. Then by the polar decomposition, we obtain that

$$\tilde{x} = |\tilde{x}^*|w_{\tilde{x}}, \quad \tilde{y} = |\tilde{y}^*|w_{\tilde{y}}.$$

By Lemma 4.3, we have

$$|\tilde{x}^*|^2 = |x^*| * |y^*|, \quad |\tilde{y}^*|^2 = |x| * |y|.$$

By Hölder's inequality, we have

$$\|x*y\|_r = \|\tilde{x}\tilde{y}^*\|_r = \||\tilde{x}^*|w_{\tilde{x}}w_{\tilde{y}}^*|\tilde{y}^*|\|_r$$
$$\leq \|(|x|*|y|)^{1/2}\|_{2r}\|(|x^*|*|y^*|)^{1/2}\|_{2r} = \||x|*|y|\|_r^{1/2}\||x^*|*|y^*|\|_r^{1/2}.$$

For any x in $L^t(\mathbb{G})$ and y in $L^s(\mathbb{G})$ such that $1+1/r=1/t+1/s$, there exists nets $\{x_\alpha\}_\alpha$ and $\{y_\beta\}_\beta$ such that $x_\alpha, y_\beta \in L^1(\mathbb{G})\cap L^\infty(\mathbb{G})$ are positive and $\lim_\alpha x_\alpha = |x|$, $\lim_\beta y_\beta = |y|$ in $L^t(\mathbb{G})$ and $L^s(\mathbb{G})$ respectively. Therefore we have that

$$\|x*y\|_r \leq \||x|*|y|\|_r^{1/2}\||x^*|*|y^*|\|_r^{1/2}$$

is true for any $x \in L^t(\mathbb{G})$, $y \in L^s(\mathbb{G})$, $1+1/r = 1/t+1/s$. □

Proposition 4.5. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let $x \in L^t(\mathbb{G})$, $y \in L^1(\mathbb{G})$ for some $1<t<\infty$. If $\|x*y\|_t = \|x\|_t\|y\|_1$ for some $1<t<2$, then for any $0 \leq \Re z \leq 1$,*

$$\|w_x|x|^{t(1+z)/2} * y\|_{2/(1+\Re z)} = \|w_x|x|^{t(1+z)/2}\|_{2/(1+\Re z)}\|y\|_1.$$

If $\|x*y\|_t = \|x\|_t\|y\|_1$ for some $2<t<\infty$, then for any $0 \leq \Re z \leq 1$,

$$\|w_x|x|^{t(1-z)/2} * y\|_{2/(1-\Re z)} = \|w_x|x|^{t(1-z)/2}\|_{2/(1-\Re z)}\|y\|_1.$$

Proof. Suppose that $\|x\|_t = 1$ and $\|y\|_1 = 1$. When $1<t<2$, we define a complex function $F_1(z)$ given by

$$F_1(z) = \varphi((w_x|x|^{t(1+z)/2} * y)|x*y|^{t(1-z)/2}w_{x*y}^*),$$
$$|F_1(z)| \leq \|w_x|x|^{t(1+z)/2} * y\|_{2/(1+\Re z)}\||x*y|^{t(1-z)/2}w_{x*y}^*\|_{2/(1-\Re z)}$$
$$\leq \||x|^{t(1+z)/2}\|_{2/(1+\Re z)}\|y\|_1\varphi(|x*y|^t)^{(1-\Re z)/2} = 1.$$

Hence $F_1(z)$ is a bounded analytic function on $0<\Re z<1$. Note that

$$F_1\Big(\frac{2}{t}-1\Big) = \varphi((x*y)|x*y|^{t-1}w_{x*y}^*) = 1.$$

Therefore $F_1(z) \equiv 1$ on $0 \leq \Re z \leq 1$ by the maximum modulus theorem.

When $2<t<\infty$, we consider the function $F_2(z)$ given by

$$F_2(z) = \varphi\big((w_x|x|^{t(1-z)/2} * y)|x*y|^{t(1+z)/2}w_{x*y}^*\big).$$

Similarly, we have the proposition proved. □

Proposition 4.6. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let $x \in L^t(\mathbb{G})$, $y \in L^s(\mathbb{G})$ be such that $\|x*y\|_r = \|x\|_t\|y\|_s$ for some $1<r,t,s<\infty$, where $1/r+1 = 1/t+1/s$. Then for any $-r+1 \leq \Re z \leq r-1$,*

$$\|w_x|x|^{t\frac{r+1-z}{2r}} * w_y|y|^{s\frac{r+1+z}{2r}}\|_r = \|w_x|x|^{t\frac{r+1-z}{2r}}\|_{\frac{2r}{r+1-\Re z}}\|w_y|y|^{s\frac{r+1+z}{2r}}\|_{\frac{2r}{r+1+\Re z}}.$$

Proof. Suppose that $\|x\|_t = \|y\|_s = 1$. We define a function $F(z)$ on $-r+1 \leq \Re z \leq r-1$ given by

$$F(z) = \varphi\big((w_x|x|^{t\frac{r+1+z}{2r}} * w_y|y|^{s\frac{r+1-z}{2r}})|x*y|^{r-1}w_{x*y}^*\big).$$

$$\begin{aligned}|F(z)| &\leq \|w_x|x|^{t\frac{r+1+z}{2r}} * w_y|y|^{s\frac{r+1-z}{2r}}\|_r \||x*y|^{r-1}\|_{\frac{r}{r-1}} \\ &\leq \|w_x|x|^{t\frac{r+1+z}{2r}}\|_{\frac{2r}{r+1+\Re z}} \|w_y|y|^{s\frac{r+1-z}{2r}}\|_{\frac{2r}{r+1-\Re z}} \varphi(|x*y|^r)^{\frac{r-1}{r}} = 1.\end{aligned}$$

Hence $F(z)$ is a bounded analytic function on $-r+1 \leq \Re z \leq r-1$. Since

$$F\Big(\frac{2r}{t} - r - 1\Big) = \varphi((x*y)|x*y|^{r-1}w_{x*y}^*) = \varphi(|x*y|^r) = 1,$$

we have that $F(z) \equiv 1$ on $-r+1 \leq \Re z \leq r-1$ by the maximum modulus theorem. Therefore we have the proposition proved. $\square$

Proposition 4.7. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. If there exist positive elements $x \in L^t(\mathbb{G})$, $y \in L^s(\mathbb{G})$ such that $\|x*y\|_r = \|x\|_t\|y\|_s$ for some $1 < r, t, s < \infty$ and $1/r + 1 = 1/t + 1/s$, then there exists a biprojection B such that x is a multiple of left shift of B and y is a multiple of a right shift of B.*

Proof. By Proposition 4.6, we have

$$\|x^{t/r} * y^s\|_r = \|x^{t/r}\|_r\|y^s\|_1, \quad \|x^t * y^{s/r}\|_r = \|x^t\|_1\|y^{s/r}\|_r.$$

By Proposition 4.5, we have that

$$\|x^{t/2} * y^s\|_2 = \|x^{t/2}\|_2\|y^s\|_1, \quad \|x^t * y^{s/2}\|_2 = \|y^{s/2}\|_2\|x^t\|_1.$$

By Proposition 3.5, we have that there exist projections B_1, B_2 such that

$$\mathcal{R}(y^s * R(y^s)) \leq B_1, \quad (R(x^{t/2}) * x^{t/2})B_1 = \|R(x^{t/2}) * x^{t/2}\|_\infty B_1,$$

and

$$\mathcal{R}(x^t * R(x^t)) \leq B_2, \quad (y^{s/2} * R(y^{s/2})B_2 = \|y^{s/2}) * R(y^{s/2})\|_\infty B_2,$$

and

$$\|R(x^{t/2}) * x^{t/2}\|_\infty = \|x^{t/2}\|_2^2, \quad \|y^{s/2} * R(y^{s/2})\|_\infty = \|y^{s/2}\|_2^2.$$

Then we see that $B_1 = B_2 (= B)$. In Proposition 3.5, to obtain that B is a biprojection, it requires that $x^{t/2} \in L^1(\mathbb{G})$, but we only have $x^{t/2} \in L^2(\mathbb{G})$ here. To see that B is a biprojection, we focus on

$$R(x^{t/2}) * x^{t/2} = \|R(x^{t/2}) * x^{t/2}\|_\infty B. \tag{3}$$

Note that $B = R(B)$.

Let $q \leq B$ be a projection in $L^1(\mathbb{G})$. Then

$$\begin{aligned}\|x^{t/2}\|_2^2\varphi(q) &= \varphi\big((R(x^{t/2}) * x^{t/2})R(q)\big)\\ &= \varphi(x^{t/2}(x^{t/2} * q)) \quad \text{(by Proposition 2.1)}\\ &\leq \|x^{t/2}\|_2\|x^{t/2} * q\|_2\\ &\leq \|x^{t/2}\|_2^2\varphi(q).\end{aligned}$$

Thus $x^{t/2} * q = \varphi(q)x^{t/2}$. Then we have that $\mathcal{F}(x^{t/2})\mathcal{F}(q) = \varphi(q)\mathcal{F}(x^{t/2})$. So

$$\mathcal{R}(\mathcal{F}(x^{t/2})) \leq E, \tag{4}$$

where E is the spectral projection of $\mathcal{F}(q)$ corresponding to $\varphi(q)$.

Recall that q is a projection in $L^1(\mathbb{G})$, so q is in $L^2(\mathbb{G})$. Thus

$$\frac{1}{\varphi(q)} = \left\|\frac{\mathcal{F}(q)}{\varphi(q)}\right\|_2^2 \geq \|\mathcal{R}(\mathcal{F}(x^{t/2}))\|_2^2 = \mathcal{S}(\mathcal{F}(x^{t/2})).$$

Then we have that

$$\varphi(B) = \sup_{q\leq B}\{\varphi(q)\} \leq \frac{1}{\mathcal{S}(\mathcal{F}(x^{t/2})}. \tag{5}$$

So $x^{t/2}$ is in $L^1(\mathbb{G}) \cap L^2(\mathbb{G})$. By [Liu and Wu 2017, Proposition 3.14], B is a biprojection.

Note that since $\mathcal{S}(B)\mathcal{S}(\mathcal{F}(B)) = 1$, we obtain that $\mathcal{S}(\mathcal{F}(x^{t/2})) \leq \mathcal{S}(\mathcal{F}(B))$. Applying Theorem 3.1 to (3), we see that $\mathcal{S}(x^{t/2}) \leq \mathcal{S}(B)$. Thus

$$\mathcal{S}(F(x^{t/2}))\mathcal{S}(x^{t/2}) \leq \mathcal{S}(\mathcal{F}(B))\mathcal{S}(B) = 1.$$

By [Liu and Wu 2017, Proposition 3.6 and Theorem 3.15], $x^{t/2}$ is a multiple of left shift of B. So is x. Similarly, y is a multiple of right shift of B. □

Theorem 4.8. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let x, y be φ-measurable and nonzero. Then the following are equivalent*:

(1) $\|x * y\|_r = \|x\|_t\|y\|_s$ *for some* $1 < r, t, s < \infty$ *such that* $1/r + 1 = 1/t + 1/s$;

(2) $\|x * y\|_r = \|x\|_t\|y\|_s$ *for any* $1 \leq r, t, s \leq \infty$ *such that* $1/r + 1 = 1/t + 1/s$;

(3) *there exists a biprojection B such that $x = ({}_hBa_x) * \hat{\mathcal{F}}(\tilde{B}_g)$ and $y = \hat{\mathcal{F}}(\tilde{B}_g) * (B_f a_y)$, where B_g, B_f are right shifts of B, ${}_hB$ is a left shift of B and a_x, a_y are elements such that x, y are nonzero.*

Proof. (1) $\Rightarrow$ (3): By Lemma 4.4, we have that $\||x| * |y|\|_r = \|x\|_t\|y\|_s$. By Proposition 4.7, we have that $|x|, |y|$ are multiples of projections. By Proposition 4.2, we see (3) is true.

(3) $\Rightarrow$ (2): It is true from Proposition 4.2.

(2) $\Rightarrow$ (1): It is obvious. ☐

5. Extremal operators of the Hausdorff–Young inequality

In this section, we will characterize the extremal operators of the Hausdorff–Young inequality for unimodular Kac algebras.

Proposition 5.1. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let $x \in L^t(\mathbb{G})$ for some $1 < t < 2$. If $\|\mathcal{F}(x)\|_{t/(t-1)} = \|x\|_t$, then for any complex number z, we have*

$$\|\mathcal{F}(w_x|x|^{t(1+z)/2})\|_{2/(1-\Re z)} = \|w_x|x|^{t(1+z)/2}\|_{2/(1+\Re z)}.$$

Proof. We assume that $\|x\|_t = 1$, $t' = t/(t-1)$, and consider the function $F(z)$ given by

$$F(z) = \varphi\big(\mathcal{F}(w_x|x|^{t(1+z)/2})|\mathcal{F}(x)|^{t'(1+z)/2}w^*_{\mathcal{F}(x)}\big).$$

Since

$$\begin{aligned}|F(z)| &\le \|\mathcal{F}(w_x|x|^{t(1+z)/2})\|_{2/(1-\Re z)}\| \||\mathcal{F}(x)|^{t'(1+z)/2}w^*_{\mathcal{F}(x)}\|_{2/(1+\Re z)}\\ &\le \|w_x|x|^{t(1+z)/2}\|_{2/(1+\Re z)}\||\mathcal{F}(x)|^{t'(1+z)/2}\|_{2/(1+\Re z)} = 1,\end{aligned}$$

we see that $F(z)$ is a bounded analytic function on $0 \le \Re z \le 1$. Note that

$$F\Big(\frac{2}{t} - 1\Big) = \varphi(\mathcal{F}(x)|\mathcal{F}(x)|^{1/(t-1)}w^*_{\mathcal{F}(x)}) = \|\mathcal{F}(x)\|_{t'}^{t'} = 1.$$

By the maximum modulus theorem, we have that $F(z) \equiv 1$ on $0 \le \Re z \le 1$ and the proposition is proved. ☐

Theorem 5.2. *Suppose $\mathbb{G}$ is a unimodular Kac algebra. Let x be measurable. Then the following are equivalent*:

(1) $\|\mathcal{F}(x)\|_{t/(t-1)} = \|x\|_t$ *for some* $1 < t < 2$;

(2) $\|\mathcal{F}(x)\|_{t/(t-1)} = \|x\|_t$ *for any* $1 \le t \le 2$;

(3) *x is a bishift of a biprojection.*

Proof. (1) $\Rightarrow$ (3): By Proposition 5.1, we have that

$$\|\mathcal{F}(w_x|x|^{3t/4})\|_4 = \|w_x|x|^{3t/4}\|_{4/3}.$$

Let $y = w_x|x|^{3t/4}$. Then

$$\|y^* * R(y)\|_2 = \||\mathcal{F}(y)|^2\|_2 = \|\mathcal{F}(y)\|_4^2 = \|y\|_{4/3}^2.$$

By Theorem 4.8, we have that y is a bishift of a biprojection and so is x.

(3) $\Rightarrow$ (2): It can be checked directly.

(2) $\Rightarrow$ (1): It is obvious. ☐

Acknowledgements

Part of the work was done during visits of the authors to Hebei Normal University. The authors would like to thank Quanhua Xu for their helpful discussions. Zhengwei Liu was supported in part by grants TRT0080 and TRT0159 from the Templeton Religion Trust. Jinsong Wu was supported by NSFC (Grant no. 11401554). The authors would like to thank the referee for careful reading.

References

[Beckner 1975] W. Beckner, "Inequalities in Fourier analysis", *Ann. of Math.* (2) **102**:1 (1975), 159–182. MR Zbl

[Bobkov et al. 2011] S. Bobkov, M. Madiman, and L. Wang, "Fractional generalizations of Young and Brunn–Minkowski inequalities", pp. 35–53 in *Concentration, functional inequalities and isoperimetry*, edited by C. Houdré et al., Contemp. Math. **545**, Amer. Math. Soc., Providence, RI, 2011. MR Zbl

[Caspers 2013] M. Caspers, "The L^p-Fourier transform on locally compact quantum groups", *J. Operator Theory* **69**:1 (2013), 161–193. MR Zbl

[Cooney 2010] T. Cooney, "A Hausdorff–Young inequality for locally compact quantum groups", *Internat. J. Math.* **21**:12 (2010), 1619–1632. MR Zbl

[Enock and Schwartz 1973] M. Enock and J.-M. Schwartz, "Une dualité dans les algèbres de von Neumann", *C. R. Acad. Sci. Paris Sér. A-B* **277** (1973), A683–A685. MR Zbl

[Enock and Schwartz 1974] M. Enock and J.-M. Schwartz, "Une catégorie d'algèbres de Kac", *C. R. Acad. Sci. Paris Sér. A* **279** (1974), 643–645. MR Zbl

[Enock and Schwartz 1975] M. Enock and J.-M. Schwartz, *Une dualité dans les algèbres de von Neumann*, Société Mathématique de France, Paris, 1975. MR Zbl

[Enock and Schwartz 1992] M. Enock and J.-M. Schwartz, *Kac algebras and duality of locally compact groups*, Springer, 1992. MR Zbl

[Fournier 1977] J. J. F. Fournier, "Sharpness in Young's inequality for convolution", *Pacific J. Math.* **72**:2 (1977), 383–397. MR Zbl

[Jiang et al. 2016] C. Jiang, Z. Liu, and J. Wu, "Noncommutative uncertainty principles", *J. Funct. Anal.* **270**:1 (2016), 264–311. MR Zbl

[Jiang et al. 2017] C. Jiang, Z. Liu, and J. Wu, "Uncertainty principles for locally compact quantum groups", *Journal of Functional Analysis* (2017).

[Kustermans and Vaes 2000] J. Kustermans and S. Vaes, "Locally compact quantum groups", *Ann. Sci. École Norm. Sup.* (4) **33**:6 (2000), 837–934. MR Zbl

[Kustermans and Vaes 2003] J. Kustermans and S. Vaes, "Locally compact quantum groups in the von Neumann algebraic setting", *Math. Scand.* **92**:1 (2003), 68–92. MR Zbl

[Liu and Wu 2017] Z. Liu and J. Wu, "Uncertainty principles for Kac algebras", *J. Math. Phys.* **58**:5 (2017), 052102, 12. MR Zbl

[Liu et al. 2017] Z. Liu, S. Wang, and J. Wu, "Young's inequality for locally compact quantum groups", *J. Operator Theory* **77**:1 (2017), 109–131. MR Zbl

[Russo 1974] B. Russo, "The norm of the L^p-Fourier transform on unimodular groups", *Trans. Amer. Math. Soc.* **192** (1974), 293–305. MR Zbl

[Tao and Vu 2006] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics **105**, Cambridge University Press, 2006. MR Zbl

[Terp 1981] M. Terp, "L^p spaces associated von Neumann algebras", 1981, Available at http://www.fuw.edu.pl/~kostecki/scans/terp1981.pdf.

[Terp 1982] M. Terp, "Interpolation spaces between a von Neumann algebra and its predual", *J. Operator Theory* **8**:2 (1982), 327–360. MR Zbl

[Van Daele 2007] A. Van Daele, "The Fourier transform in quantum group theory", pp. 187–196 in *New techniques in Hopf algebras and graded ring theory*, edited by S. Caenepeel and F. Van Oystaeyen, K. Vlaam. Acad. Belgie Wet. Kunsten (KVAB), Brussels, 2007. MR

[Vaĭnerman 1974] L. I. Vaĭnerman, "Characterization of objects dual to locally compact groups", *Funkcional. Anal. i Priložen.* **8**:1 (1974), 75–76. In Russian; translated in *Funct. Anal. Appl.* **8**:1 (1974), 66–67. MR Zbl

[Vaĭnerman and Kac 1973] L. I. Vaĭnerman and G. I. Kac, "Nonunimodular ring groups, and Hopf-von Neumann algebras", *Dokl. Akad. Nauk SSSR* **211** (1973), 1031–1034. In Russian; translated in *Sov. Math. Dokl.* **14** (1973), 1144–1148. MR Zbl

[Young 1912] W. H. Young, "On the multiplication of successions of Fourier constants", *Proc. R. Soc. Lond. Ser. A* **87** (1912), 331–339. Zbl

Received April 14, 2017. Revised December 16, 2017.

ZHENGWEI LIU
DEPARTMENT OF MATHEMATICS AND DEPARTMENT OF PHYSICS
HARVARD UNIVERSITY
CAMBRIDGE, MA
UNITED STATES

zhengweiliu@fas.harvard.edu

JINSONG WU
INSTITUTE FOR ADVANCED STUDY IN MATHEMATICS
HARBIN INSTITUTE OF TECHNOLOGY
HARBIN, 150001
CHINA

wjsl@ustc.edu.cn

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.123

EFFECTIVE RESULTS ON LINEAR DEPENDENCE FOR ELLIPTIC CURVES

MIN SHA AND IGOR E. SHPARLINSKI

Given a subgroup Γ of rational points on an elliptic curve E defined over $\mathbb{Q}$ of rank $r \geq 1$ and any sufficiently large $x \geq 2$, assuming that the rank of Γ is less than r, we give upper and lower bounds on the canonical height of a rational point Q which is not in the group Γ but belongs to the reduction of Γ modulo every prime $p \leq x$ of good reduction for E.

1. Introduction

1A. ***Detecting linear dependence.*** Let A be an abelian variety defined over a number field F, and let Γ be a subgroup of the Mordell–Weil group $A(F)$. For any prime $\mathfrak{p}$ (of F) of good reduction for A and any point $Q \in A(F)$, we denote by $Q_{\mathfrak{p}}$ and $\Gamma_{\mathfrak{p}}$ the images of Q and Γ via the reduction map modulo $\mathfrak{p}$ respectively, and $F_{\mathfrak{p}}$ stands for the residue field of F modulo $\mathfrak{p}$. The following question was initiated in 2002 and was considered at the same time but independently by Wojciech Gajda in a letter to Kenneth Ribet in 2002 [Gajda and Górnisiewicz 2009, §1] and by Kowalski [2003], and it is now called *detecting linear dependence*.

Question 1.1. *Suppose that Q is a point of $A(F)$ such that for all but finitely many primes $\mathfrak{p}$ of F we have $Q_{\mathfrak{p}} \in \Gamma_{\mathfrak{p}}$. Does it then follow that $Q \in \Gamma$?*

An early result related to this question is due to Schinzel [1975], who has answered affirmatively the question for the multiplicative group in place of an abelian variety. Question 1.1 has been extensively studied in recent years and much progress has been made; see [Banaszak 2009; Banaszak et al. 2005; Banaszak and Krasoń 2011; Gajda and Górnisiewicz 2009; Jossen 2013; Jossen and Perucca 2010; Perucca 2010; Sadek 2016; Weston 2003] for more details and developments.

The answer is affirmative for all abelian varieties if the group Γ is cyclic, as proven by Kowalski [2003] (for elliptic curves) and by Perucca [2010] (in general). Banaszak, Gajda and Krasoń [Banaszak et al. 2005] established the result for all abelian varieties with the endomorphism ring $\mathrm{End}_F\, A = \mathbb{Z}$ if the group Γ is free

MSC2010: 11G05, 11G50.
Keywords: elliptic curve, linear dependence, pseudolinearly dependent point, pseudomultiple, canonical height.

and the point Q is nontorsion. More generally, Gajda and Górnisiewicz [2009] have solved the problem in the case when Γ is a free $\mathrm{End}_F\, A$-submodule and the point Q generates a free $\mathrm{End}_F\, A$-submodule, while Perucca [2010] has removed the assumption on the point Q. We remark that the answer of Question 1.1 is not always positive; see a counterexample due to Jossen and Perucca [2010].

We want to emphasize that Jossen [2013] has given an affirmative answer when A is a geometrically simple abelian variety, which automatically includes elliptic curves. Moreover, the result of [Jossen 2013] requires $Q_{\mathfrak{p}} \in \Gamma_{\mathfrak{p}}$ to hold only for a set of primes $\mathfrak{p}$ with natural density 1 (rather than for all but finitely many primes $\mathfrak{p}$ as in the settings of Question 1.1). Due to the crucial role of [Jossen 2013] in our paper, we reproduce this result as follows.

Theorem 1.2 [Jossen 2013]. *Assume that A is a geometrically simple abelian variety over F. Then, if the set of primes $\mathfrak{p}$ of F for which $Q_{\mathfrak{p}} \in \Gamma_{\mathfrak{p}}$ has natural density* 1, *we have $Q \in \Gamma$.*

In addition, to achieve the aforementioned results, one needs to apply the Chebotarev density theorem. So, it suffices to verify the condition for all primes up to a certain finite bound, which depends on the initial data (including the point Q). Banaszak and Krasoń [2011, Theorem 7.7] have established the finiteness result in a qualitative manner for certain abelian varieties which includes elliptic curves. Then, most recently Sadek [2016] has given a quantitative version for a large class of elliptic curves under the *generalized Riemann hypothesis* (GRH). However, the results in this paper (see Section 2) go in a different direction, because they imply that there is no such a bound independent of the point Q.

1B. *Pseudolinear dependence.* Following the setup of [Akbary et al. 2010], which is crucial for some of our approaches, we restrict ourselves to the case of elliptic curves over the rational numbers $\mathbb{Q}$; see Definitions 1.3 and 1.4 below. In particular, we consider Question 1.1 for an elliptic curve E over $\mathbb{Q}$.

Let r be the rank of $E(\mathbb{Q})$ and s the rank of Γ. We denote by Δ_E the minimal discriminant of E and by O_E the point at infinity of E.

For a prime p of good reduction for E (that is, $p \nmid \Delta_E$), we let $E(\mathbb{F}_p)$ be the group of $\mathbb{F}_p$-points in the reduction of E to the finite field $\mathbb{F}_p$ of p elements, and $E(\mathbb{Q})_p$ stands for the reduction of $E(\mathbb{Q})$ modulo p.

Definition 1.3 ($\mathbb{F}_p$-pseudolinear dependence). Given a prime p of good reduction for E, we call a point $Q \in E(\mathbb{Q})$ an $\mathbb{F}_p$-*pseudolinearly dependent point* with respect to Γ if $Q \notin \Gamma$ but $Q_p \in \Gamma_p$.

We remark that such a point Q is $\mathbb{F}_p$-pseudolinear dependent if and only if $Q \notin \Gamma$ but $Q \in \Gamma + \ker_p$, where $\ker_p$ denotes the kernel of the reduction map modulo p.

Definition 1.4 (x-pseudolinear dependence). We say that a point $Q \in E(\mathbb{Q})$ is an *x-pseudolinearly dependent point* with respect to Γ if $Q \notin \Gamma$ but it is an $\mathbb{F}_p$-pseudolinearly dependent point with respect to Γ for all primes $p \le x$ of good reduction for E.

We remark that the x-pseudolinear dependence trivially holds if there is no prime p of good reduction such that $p \le x$.

If $\Gamma = \langle P \rangle$, we call a point Q as in Definition 1.4 an *x-pseudomultiple* of P. This notion is an elliptic curve analogue of the notions of x-pseudosquares and x-pseudopowers over the integers, which dates back to the classical results of Schinzel [1960; 1970; 1997] and has recently been studied in [Bach et al. 1996; Bourgain et al. 2009; Konyagin et al. 2010; Pomerance and Shparlinski 2009].

1C. *Overview.* We give an explicit construction of an x-pseudolinearly dependent point Q with respect to Γ provided that $s < r$ and give upper bounds for its canonical height, and then we also deduce lower bounds for the canonical height of any x-pseudolinearly dependent point in some special cases. These upper and lower bounds are formulated in Sections 2A and 2B and proved in Sections 5 and 6, respectively.

Furthermore, we also consider the existence problem of x-pseudolinearly dependent points, with some explicit constructions; see Section 4 for precise details.

There is little doubt that one can extend [Akbary et al. 2010], and thus our results to elliptic curves over number fields, but this may require quite significant efforts.

1D. *Convention and notation.* Throughout the paper, we use the Landau symbols O and o and the Vinogradov symbol $\ll$ (sometimes written as $\gg$). We recall that the assertions $U = O(V)$ and $U \ll V$ are both equivalent to the inequality $|U| \le cV$ with some absolute constant c, while $U = o(V)$ means that $U/V \to 0$. Here, all implied constants in the symbols O and $\ll$ depend only possibly on E and Γ.

The letter p, with or without subscripts, always denotes a prime. As usual, $\pi(x)$ denotes the number of primes not exceeding x.

We use $\hat{h}$ to denote the canonical height of points on E; see Section 3A for a precise definition. For a finite set S, we use $\#S$ to denote its cardinality.

For any group G, if it is generated by some elements $g_1, \dots, g_m$, then we write $G = \langle g_1, \dots, g_m \rangle$.

From now on, we say that a prime is of good reduction, which means that the prime is of good reduction for E. When a point Q is said to be x-pseudolinearly dependent, it is automatically with respect to Γ.

2. Main results

2A. *Upper bounds.* We first state a primary result on the existence of pseudolinearly dependent points.

Theorem 2.1. *Suppose that $r \ge 1$ and $s < r$. Then for any sufficiently large x, there is a rational point $Q \in E(\mathbb{Q})$ of height*

$$\hat{h}(Q) \le \exp\bigl(2x + O(x/(\log x)^2)\bigr)$$

such that Q is an x-pseudolinearly dependent point.

With more efforts we can improve the result in Theorem 2.1 for various cases.

Theorem 2.2. *Suppose that $r \ge 1$ and $s = 0$. Then for any sufficiently large x, there is a rational point $Q \in E(\mathbb{Q})$ of height*

$$\hat{h}(Q) \le \exp\Bigl(2x - 2\log(\#\Gamma)\frac{x}{\log x} + O(x/(\log x)^2)\Bigr)$$

such that Q is an x-pseudolinearly dependent point.

Theorem 2.3. *Assume that $r \ge 2$ and $1 \le s < r$. Then for any sufficiently large x, there is a rational point $Q \in E(\mathbb{Q})$ of height*

$$\hat{h}(Q) \le \exp\Bigl(\frac{4}{s+2}x + O(x/\log x)\Bigr)$$

such that Q is an x-pseudolinearly dependent point.

Theorem 2.4. *Suppose that either $19 \le s < r$ if E is a non-CM curve, or $7 \le s < r$ if E is a CM curve. Then under the GRH and for any sufficiently large x, there is a rational point $Q \in E(\mathbb{Q})$ of height*

$$\hat{h}(Q) \le \exp\bigl(4x(\log\log x)/\log x + O(x/\log x)\bigr)$$

such that Q is an x-pseudolinearly dependent point.

The above results are proved in Section 5.

2B. ***Lower bounds.*** Notice that by Definition 1.4 the condition for x-pseudolinearly dependent points is quite strong when x tends to infinity. This convinces us that there may exist some lower bounds for the height of such points. Here, we establish some partial results. Define

$$\widetilde{\Gamma} = \{P \in E(\mathbb{Q}) : mP \in \Gamma \text{ for some nonzero } m \in \mathbb{Z}\}. \tag{2-1}$$

Theorem 2.5. *Suppose that $r \ge 1$ and $s = 0$. For any sufficiently large x and any x-pseudolinearly dependent point Q, we have*

$$\hat{h}(Q) \ge \frac{1}{\#\Gamma}x/\log x + O(x/(\log x)^2).$$

Theorem 2.6. *Assume that* $\mathrm{End}_{\overline{\mathbb{Q}}} E = \mathbb{Z}$, $r \geq 2$, $1 \leq s < r$, *and* Γ *is a free subgroup of* $E(\mathbb{Q})$. *Suppose further that* $\Gamma \equiv \widetilde{\Gamma}$ *modulo the torsion points of* $E(\mathbb{Q})$. *For any sufficiently large* x *and any* x*-pseudolinearly dependent point* Q, *we have*

$$\hat{h}(Q) \geq \exp((\log x)^{1/(2s+6)+o(1)}),$$

and furthermore assuming the GRH, we have

$$\hat{h}(Q) \geq \exp(x^{1/(4s+12)+o(1)}).$$

The above results are proved in Section 6.

We want to remark that for a non-CM elliptic curve E with no torsion points in $E(\mathbb{Q})$, assuming the GRH and some other wild conditions, Sadek [2016, Theorem 4.4] has shown that to detect whether a point $Q \in E(\mathbb{Q})$ is contained in Γ it suffices to determine whether $Q \in \Gamma_p$ for primes p of good reduction up to an explicit constant B satisfying (using only $K \geq 2$ in [Sadek 2016, Theorem 4.4])

$$B \gg \hat{h}(Q)^{3r/2+3}(\log \hat{h}(Q))^2. \tag{2-2}$$

If Q is an x-pseudolinearly dependent point, then to detect $Q \notin \Gamma$ as the above, testing primes p of good reduction up to x is not enough, and thus the constant B must satisfy $B > x$, which is consistent with the second lower bound of Theorem 2.6 and (2-2). On the other hand, the inequality $B > x$ restricts how much Theorem 2.6 and [Sadek 2016, Theorem 4.4] can be improved.

3. Preliminaries

3A. ***Heights on elliptic curves.*** We briefly recall the definitions of the Weil height and the canonical height for points in $E(\mathbb{Q})$; see [Silverman 2009, Chapter VIII, § 9] for more details.

For a point $P = (x, y) \in E(\mathbb{Q})$ with $x = a/b$, with coprime integers a and b, we define the *Weil height* and the *canonical height* of P as

$$\mathfrak{h}(P) = \log \max\{|a|, |b|\} \quad \text{and} \quad \hat{h}(P) = \lim_{n\to+\infty} \frac{\mathfrak{h}(2^n P)}{4^n},$$

respectively. These two heights are related because they satisfy

$$\hat{h}(P) = \mathfrak{h}(P) + O(1),$$

where the implied constant depends only on E. In addition, for any $P \in E(\mathbb{Q})$ and $m \in \mathbb{Z}$, we have:

- $\hat{h}(mP) = m^2 \hat{h}(P)$;
- $\hat{h}(P) = 0$ if and only if P is a torsion point.

Furthermore, for any $P, Q \in E(\mathbb{Q})$, we have

$$\hat{h}(P+Q)+\hat{h}(P-Q)=2\hat{h}(P)+2\hat{h}(Q). \tag{3-1}$$

Following the hints in [Silverman 2009, Chapter IX, Exercise 9.8] and using [Silverman 2009, Chapter VIII, Proposition 9.6], one can show that if $P_1, \dots, P_r$ is a basis for the free part of $E(\mathbb{Q})$ (assuming $r \geq 1$), then for any integers $m_1, \dots, m_r$, we have

$$\hat{h}(m_1P_1+\cdots+m_rP_r) \geq c \max_{1\leq i\leq r} m_i^2, \tag{3-2}$$

where c is a constant depending on E and $P_1, \dots, P_r$.

3B. ***A useful fact about elliptic curves.*** Every rational point $P \neq O_E$ in $E(\mathbb{Q})$ has a representation of the form

$$P=\left(\frac{m}{k^2}, \frac{n}{k^3}\right), \tag{3-3}$$

where m, n, and k are integers with $k \geq 1$ and $\gcd(m,k)=\gcd(n,k)=1$; see [Silverman and Tate 1992, p. 68]. So, for any prime p of good reduction for E, $P \equiv O_E$ modulo p if and only if $p \mid k$.

3C. ***Counting primes related to the size of Γ under reduction.*** Here, we reproduce some results on counting primes p such that the size of Γ_p is less than some given value. For any prime p, if it is of good reduction for E, we define

$$N_p=\#E(\mathbb{F}_p) \quad \text{and} \quad T_p=\#\Gamma_p,$$

otherwise we let $N_p=T_p=1$. Note that there are only finitely many primes p such that $N_p=1$.

We first quote the following result from [Akbary et al. 2010, Proposition 5.4] (see [Gupta and Murty 1986, Lemma 14] for a previous result). Recall that s is the rank of Γ.

Lemma 3.1. *Assume that $s \geq 1$. For any $x \geq 2$, we have*

$$\#\{p : T_p < x\} \ll x^{1+2/s}/\log x.$$

We then restate two general results from [Akbary et al. 2010, Theorems 1.2 and 1.4] in a form convenient for our applications.

Lemma 3.2. *Assume that E is a non-CM curve and $s \geq 19$. Under the GRH, for any $x \geq 2$ we have*

$$\#\{p \leq x : T_p < p/(\log p)^2\} \ll x/(\log x)^2.$$

Proof. We can clearly only consider the primes of good reduction. Here, we directly use the notation and follow the arguments in [Akbary et al. 2010, Proof of Part (a) of Theorem 1.2] by choosing the functions f and g as

$$f(x) = (\log x)^2, \qquad g(x) = f(x/\log x)/3. \tag{3-4}$$

Let $i_p = [E(\mathbb{F}_p) : \Gamma_p]$ for any prime p of good reduction. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be the two sets defined in [Akbary et al. 2010, p. 381]:

$$\mathcal{B}_1 = \{p \le x : p \nmid \Delta_E, i_p \in (x^{2/(s+2)} \log x, 3x]\},$$
$$\mathcal{B}_2 = \{p \le x : p \nmid m\Delta_E, m \mid i_p \text{ for some } m \in (g(x), x^{2/(s+2)} \log x]\},$$

such that

$$\#\{p \le x : p \nmid \Delta_E, T_p < p/(\log p)^2\} \le \#\mathcal{B}_1 + \#\mathcal{B}_2 + O(x/(\log x)^2),$$

where the term $O(x/(\log x)^2)$ comes from $\pi(x/\log x) = O(x/(\log x)^2)$. We note that the choice of the sets is motivated by

- for $\mathcal{B}_1$, the bound on the number of primes $p \le x$ with a small value of T_p given by [Akbary et al. 2010, Proposition 5.4] which we have presented in Lemma 3.1;
- for $\mathcal{B}_2$, the range of m compared to x in which the divisibility $m \mid i_p$ for $p \le x$ can be controlled via the Chebotarev density theorem as given by [Akbary et al. 2010, Proposition 5.3].

In particular, we have

$$\#\mathcal{B}_1 \ll \frac{x}{(\log x)^{(s+2)/s} \cdot (s(s+2)^{-1} \log x - \log\log x)}$$

and

$$\#\mathcal{B}_2 \ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O(x^{1/2+\alpha+(5+\alpha/2)\cdot(2/(s+2)+\alpha)}),$$

where the positive real number α is chosen such that

$$\tfrac{1}{2} + \alpha + \left(5 + \tfrac{1}{2}\alpha\right) \cdot \left(\frac{2}{s+2} + \alpha\right) < 1,$$

which at least requires that $\frac{1}{2} + 6\alpha < 1$, that is $\alpha < \frac{1}{12}$. Note that such α indeed exists because $s \ge 19$.

It is easy to see that

$$\#\mathcal{B}_1 \ll x/(\log x)^2 \quad \text{and} \quad \#\mathcal{B}_2 \ll x/(\log x)^2,$$

where the second upper bound comes from $2(1-\alpha) > 1$. Collecting these estimates, we get the desired upper bound. $\square$

Lemma 3.3. *Assume that E is a CM curve and $s \ge 7$. Under the GRH, for any $x \ge 2$ we have*
$$\#\{p \le x : T_p < p/(\log p)^2\} \ll x/(\log x)^2.$$

Proof. We follow the arguments in [Akbary et al. 2010, Proof of Theorem 1.4] with only minor modifications by choosing the functions f and g there as in (3-4). Let $i_p = [E(\mathbb{F}_p) : \Gamma_p]$ for any prime p of good reduction. The following can be derived as in [Akbary et al. 2010, Proof of Part (a) of Theorem 1.2]:
$$\#\big\{p \le x : p \nmid \Delta_E, T_p < p/(\log p)^2\big\} \le \#\widetilde{\mathcal{B}}_1 + \#\widetilde{\mathcal{B}}_2 + O(x/(\log x)^2),$$
where
$$\widetilde{\mathcal{B}}_1 = \{p \le x : p \nmid \Delta_E, i_p \in (x^\kappa, 3x]\},$$
$$\widetilde{\mathcal{B}}_2 = \{p \le x : p \nmid m\Delta_E, m \mid i_p, \text{ for some } m \in (g(x), x^\kappa]\},$$
with some real $\kappa > 0$ to be chosen later on. The reason for the choice of $\widetilde{\mathcal{B}}_1$ and $\widetilde{\mathcal{B}}_2$ is the same as that for $\mathcal{B}_1$ and $\mathcal{B}_2$, which is explained in the proof of Lemma 3.2. However, in the CM-case we have stronger versions of the underlying results which allow us a better choice of parameters and in turn enable us to handle smaller values of the rank s of Γ.

Applying Lemma 3.1, we have
$$\begin{aligned}\#\widetilde{\mathcal{B}}_1 &= \#\{p \le x \ : \ p \nmid \Delta_E,\ T_p < N_p/x^\kappa\} \\ &\le \#\{p \le x \ : \ p \nmid \Delta_E,\ T_p < 3x^{1-\kappa}\} \ll \frac{x^{(1-\kappa)(s+2)/s}}{(1-\kappa)\log x}.\end{aligned}$$

For any positive integer m, let $\omega(m)$ and $d(m)$ denote, respectively, the number of distinct prime divisors of m and the number of positive integer divisors of m.

Now, $\#\widetilde{\mathcal{B}}_2$ can be estimated as in [Akbary et al. 2010, p. 393] as follows:
$$\#\widetilde{\mathcal{B}}_2 \ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O\bigg(x^{1/2} \log x \cdot \sum_{1 \le m \le x^\kappa} m a^{\omega(m)/2} d(m)\bigg),$$
where α is an arbitrary real number in the interval $(0, 1)$ such that $2(1-\alpha) > 1$, and a is the absolute constant of [Akbary et al. 2010, Proposition 6.7]. Now, using [Akbary et al. 2010, Equation (6.21)] we obtain
$$\begin{aligned}\#\widetilde{\mathcal{B}}_2 &\ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O(x^{1/2+2\kappa}(\log x)^{1+\beta}) \\ &\ll \frac{x}{(\log x)^2} + O(x^{1/2+2\kappa}(\log x)^{1+\beta}),\end{aligned}$$
where $\beta > 2$ is some positive integer.

Moreover, we choose the real number κ such that

$$(1-\kappa)(s+2)/s < 1 \quad \text{and} \quad \tfrac{1}{2}+2\kappa < 1.$$

Thus, we get

$$\frac{2}{s+2} < \kappa < \tfrac{1}{4}. \tag{3-5}$$

Since $s \geq 7$, such real number κ indeed exists.

Therefore, gathering the above estimates, for any fixed real number κ satisfying (3-5) (for example, $\kappa = \frac{11}{45}$) we obtain

$$\#\{p \leq x \ :\ p \nmid \Delta_E, T_p < p/(\log p)^2\} \ll x/(\log x)^2, \qquad \square$$

which completes the proof of this lemma.

3D. ***Kummer theory on elliptic curves.*** Following [Akbary et al. 2010; Bachmakov 1970; Bertrand 1981; Gupta and Murty 1986], we recall some basic facts about the Kummer theory on elliptic curves. Here, we should assume that $E(\mathbb{Q})$ is of rank $r \geq 2$.

Let ℓ be a prime, and let $P_1, P_2, \dots, P_n \in E(\mathbb{Q})$ be linearly independent points over $\operatorname{End}_{\mathbb{Q}} E$. Consider the number field

$$L = \mathbb{Q}(E[\ell], \ell^{-1}P_1, \dots, \ell^{-1}P_n),$$

where $E[\ell]$ is the set of ℓ-torsion points on E, and each $\ell^{-1}P_i$ $(1 \leq i \leq n)$ is a fixed point whose ℓ-multiple is the point P_i. Moreover, we denote $K = \mathbb{Q}(E[\ell])$ and $K_i = \mathbb{Q}(E[\ell], \ell^{-1}P_i)$ for every $1 \leq i \leq n$.

Now, both extensions $K/\mathbb{Q}$ and $L/\mathbb{Q}$ are Galois extensions. For the Galois groups, $\operatorname{Gal}(K/\mathbb{Q})$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, and $\operatorname{Gal}(L/K)$ is a subgroup of $E[\ell]^n$. Clearly, we have

$$[K:\mathbb{Q}] < \ell^4 \quad \text{and} \quad [L:K] \leq \ell^{2n}. \tag{3-6}$$

As an analogue of the classical Kummer theory, the results of Bashmakov [1970] show that (see also the discussions in [Bertrand 1981, p. 85]):

Lemma 3.4. *Assume that the residue classes of points $P_1, \dots, P_n$ in $E(\mathbb{Q})/\ell E(\mathbb{Q})$ are linearly independent over* $\operatorname{End}_{\mathbb{Q}} E/\ell \operatorname{End}_{\mathbb{Q}} E$. *Then, we have*

$$\operatorname{Gal}(L/K) \cong E[\ell]^n.$$

For each field K_i with $1 \leq i \leq n$, the primes which ramify in the extension $K_i/\mathbb{Q}$ are exactly those primes dividing $\ell\Delta_E$. Then, the primes which ramify in the extension $L/\mathbb{Q}$ are exactly those primes dividing $\ell\Delta_E$. Now, pick a prime $p \nmid \ell\Delta_E$ which splits completely in K, and let $\mathfrak{p}_i$ be a prime ideal of $\mathcal{O}_{K_i}$ above p

for $i = 1, \dots, n$, where $\mathcal{O}_{K_i}$ the ring of integers of K_i. By the construction of K_i and noticing the choice of p, we have:

Lemma 3.5. *For each $1 \le i \le n$, the equation*

$$\ell X = P_i \tag{3-7}$$

has a solution in $E(\mathbb{F}_p)$, where X is an unknown, if and only if $[\mathcal{O}_{K_i}/\mathfrak{p}_i : \mathbb{F}_p] = 1$, that is, p splits completely in K_i.

Note that given an arbitrary finite Galois extension M/F of number fields, for each unramified prime $\mathfrak{p}$ of F, $\mathfrak{p}$ splits completely in M if and only if the Frobenius element corresponding to $\mathfrak{p}$ is the identity map. Then, we can obtain the following lemma:

Lemma 3.6. *Under the assumption in Lemma 3.4, we further assume that $n \ge 2$. Then, for any integer m with $1 \le m < n$, there is a conjugation class C in the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ such that every prime number p with the Artin symbol $\left[\frac{L/\mathbb{Q}}{p}\right] = C$ is unramified in $L/\mathbb{Q}$, p is a prime of good reduction for E, and p splits completely in the fields K_i, $1 \le i \le m$, but it does not split completely in any of the fields K_j, $m+1 \le j \le n$.*

Proof. One only needs to note that by Lemma 3.4, for any nonempty subsets I, J of $\{1, 2, \dots, n\}$ if $I \cap J = \varnothing$, we have

$$\prod_{i \in I} K_i \cap \prod_{j \in J} K_j = K,$$

where "$\prod$" means the composition of fields. □

Combining Lemma 3.5 with Lemma 3.6, we know that for the primes p in Lemma 3.6, Equation (3-7) has a solution in $E(\mathbb{F}_p)$ for $1 \le i \le m$ but for the others there is no such solution.

3E. *The Chebotarev density theorem.* For the convenience of the reader, we restate two useful results. The first one is an upper bound on the discriminant of a number field due to Hensel, see [Serre 1981, Proposition 6], while the second is about the least prime ideal as in the Chebotarev density theorem due to Lagarias, Montgomery and Odlyzko; see [Lagarias and Odlyzko 1977, p. 462] and [Lagarias et al. 1979, Theorem 1.1 and Equation (1.2)].

Lemma 3.7. *Let $L/\mathbb{Q}$ be a Galois extension of degree d and ramified only at the primes $p_1, \dots, p_m$. Then, we have*

$$\log |D_L| \le d \log d + d \sum_{i=1}^{m} \log p_i,$$

where D_L is the discriminant of $L/\mathbb{Q}$.

Lemma 3.8. *There exists an effectively computable positive absolute constant c_1 such that for any number field K, any finite Galois extension L/K and any conjugacy class C in $\mathrm{Gal}(L/K)$, there exists a prime ideal $\mathfrak{p}$ of K which is unramified in L, for which the Artin symbol $[(L/K)/\mathfrak{p}] = C$ and the norm $\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{p})$ is a rational prime satisfying the bound*

$$\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{p}) \le 2|D_L|^{c_1};$$

furthermore, under the GRH, there is an effectively computable positive absolute constant c_2 such that we can choose $\mathfrak{p}$ as above with

$$\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{p}) \le c_2(\log|D_L|)^2.$$

3F. *Effective version of Theorem 1.2.* The following result can be viewed as an effective version of Theorem 1.2 in some sense for a specific case. Recall that r and s are the ranks of $E(\mathbb{Q})$ and Γ respectively.

Lemma 3.9. *Assume that $\mathrm{End}_{\mathbb{Q}} E = \mathbb{Z}$, Γ is a free subgroup of $E(\mathbb{Q})$, and $\Gamma \equiv \widetilde{\Gamma}$ modulo the torsion points of $E(\mathbb{Q})$. Let $Q \in E(\mathbb{Q}) \setminus \Gamma$ be a point of infinite order such that $\langle Q \rangle \cap \Gamma = \{O_E\}$. Then, there exists a prime p of good reduction satisfying*

$$\log p \ll (\log \hat{h}(Q))^{2s+6} \log\log \hat{h}(Q)$$

such that $Q \notin \Gamma_p$. Assuming the GRH, we further have

$$p \ll (\log \hat{h}(Q))^{4s+12} (\log\log \hat{h}(Q))^2.$$

Proof. Let $P_1, \dots, P_r$ be a basis of the free part of $E(\mathbb{Q})$. Since $\Gamma \equiv \widetilde{\Gamma}$ modulo the torsion points, we can assume that $P_1, \dots, P_s$ form a basis of Γ. Note that, since the point Q is of infinite order, it can be represented as

$$Q = Q_0 + m_1 P_1 + \cdots + m_r P_r,$$

where Q_0 is a torsion point of $E(\mathbb{Q})$, and there is at least one $m_i \ne 0$ $(1 \le i \le r)$. Moreover, by the choice of Q, there exists j with $s+1 \le j \le r$ such that $m_j \ne 0$.

By (3-2), we have

$$\hat{h}(Q - Q_0) \gg \max_{1 \le i \le r} m_i^2.$$

Noticing that Q_0 is a torsion point, by (3-1) we obtain

$$\hat{h}(Q) \ge \tfrac{1}{2}\hat{h}(Q - Q_0) \gg \max_{1 \le i \le r} m_i^2. \tag{3-8}$$

Now, let ℓ be the smallest prime such that $\ell \nmid m_j$. Since the number $\omega(m)$ of distinct prime factors of an integer $m \ge 2$ satisfies

$$\omega(m) \ll \frac{\log m}{\log\log m}$$

(because we obviously have $\omega(m)! \le m$), using the prime number theorem we get

$$\ell \ll \log |m_j|,$$

which together with (3-8) yields that

$$\ell \ll \log \hat{h}(Q). \tag{3-9}$$

By the choice of ℓ, we see that there is no point $R \in E(\mathbb{Q})$ such that $Q = \ell R$. This implies that the number field $\mathbb{Q}(E[\ell], \ell^{-1}Q)$ is not a trivial extension of $\mathbb{Q}(E[\ell])$. Furthermore, by noticing $\ell \nmid m_j$, it is straightforward to see that the residue classes of $Q, P_1, \dots, P_s$ in $E(\mathbb{Q})/\ell E(\mathbb{Q})$ are linearly independent over $\mathrm{End}_{\mathbb{Q}} E/\ell \,\mathrm{End}_{\mathbb{Q}} E = \mathbb{Z}/\ell\mathbb{Z}$.

Consider the number field

$$L = \mathbb{Q}(E[\ell], \ell^{-1}Q, \ell^{-1}P_1, \dots, \ell^{-1}P_s),$$

and set $K = \mathbb{Q}(E[\ell])$. Now, combining Lemma 3.5 with Lemma 3.6, we can choose a conjugation class C in the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ such that every prime number p with Artin symbol $[(L/\mathbb{Q})/p] = C$ is unramified in $L/\mathbb{Q}$, p is a prime of good reduction for E, and especially the equation $\ell X = P_i$ has solution in $E(\mathbb{F}_p)$ for each $1 \le i \le s$ but the equation $\ell X = Q$ has no such solution. This implies that

$$Q \notin \Gamma_p.$$

By Lemma 3.8, we can choose such a prime p such that

$$\log p \ll \log |D_L|; \tag{3-10}$$

if under the GRH, we even have

$$p \ll (\log |D_L|)^2. \tag{3-11}$$

From Lemma 3.7 and noticing that only the primes dividing $\ell \Delta_E$ ramify in the extension $L/\mathbb{Q}$, we get

$$\log |D_L| \le d \log d + d \log(\ell \Delta_E) \ll d \log d + d \log \ell, \tag{3-12}$$

where $d = [L : \mathbb{Q}]$. Using (3-6), we obtain

$$d \le \ell^{2s+6}. \tag{3-13}$$

Combining (3-9), (3-10), (3-11), and (3-12) with (3-13), we unconditionally have

$$\log p \ll (\log \hat{h}(Q))^{2s+6} \log\log \hat{h}(Q),$$

and under the GRH we have

$$p \ll (\log \hat{h}(Q))^{4s+12} (\log\log \hat{h}(Q))^2. \qquad \square$$

4. The existence and construction of x-pseudolinearly dependent points

4A. *Existence.* Before proving our main results, we want to first consider the existence problem of pseudolinearly dependent points. Recall that r is the rank of $E(\mathbb{Q})$ and s is the rank of Γ.

If $s < r$, then x-pseudolinearly dependent points with respect to Γ do exist. Indeed, since $s < r$, we can take a point $R \in E(\mathbb{Q})$ of infinite order such that $\langle R \rangle \cap \Gamma = \{O_E\}$. Pick an arbitrary point $P \in \Gamma$; it is easy to see that the point

$$Q = P + \operatorname{lcm}\{\#E(\mathbb{Q})_p \, \#\Gamma_p : p \le x \text{ of good reduction}\} R \tag{4-1}$$

is an x-pseudolinearly dependent point for any $x > 0$, where the least common multiple of the empty set is defined to be 1.

In the construction (4-1), we can see that $\langle Q \rangle \cap \Gamma = \{O_E\}$. Actually, when x is sufficiently large, any x-pseudolinearly dependent point with respect to Γ must satisfy this property.

Proposition 4.1. *There exists a constant M depending on E and Γ such that for any $x > M$, every x-pseudolinearly dependent point Q is nontorsion and satisfies $\langle Q \rangle \cap \Gamma = \{O_E\}$.*

Proof. Consider the subgroup $\widetilde{\Gamma}$ defined in (2-1). Notice that $\widetilde{\Gamma}$ is a finitely generated group containing the torsion points of $E(\mathbb{Q})$, and by construction each element in the quotient group $\widetilde{\Gamma}/\Gamma$ is of finite order. So, $\widetilde{\Gamma}/\Gamma$ is a finite group. Then, we let $n = [\widetilde{\Gamma} : \Gamma]$ and assume that $\widetilde{\Gamma}/\Gamma = \{P_0 = O_E, P_1, \ldots, P_{n-1}\}$. If $n = 1$, that is $\widetilde{\Gamma} = \Gamma$, then for any $P \in E(\mathbb{Q}) \setminus \Gamma$ we have $\langle P \rangle \cap \Gamma = \{O_E\}$, and thus everything is done. Now, we assume that $n > 1$.

For any P_i, $1 \le i \le n-1$, since $P_i \notin \Gamma$, by Theorem 1.2 there exists a prime p_i of good reduction such that $P_i \notin \Gamma_{p_i}$. Then, we choose a constant, say M, such that $M \ge p_i$ for any $1 \le i \le n-1$. Thus, when $x > M$, any P_i $(1 \le i \le n-1)$ is not an x-pseudolinearly dependent point with respect to Γ, and then any point $P \in \widetilde{\Gamma}$ is also not such a point. So, the x-pseudolinearly dependent point Q is not in $\widetilde{\Gamma}$. This actually completes the proof. $\square$

The above result clearly implies the following:

Corollary 4.2. *If Γ is a full rank subgroup of $E(\mathbb{Q})$ (that is $s = r$), then there exists a constant M depending on E and Γ such that for any $x > M$, there is no x-pseudolinearly dependent point.*

In other words, the case (that is $s < r$) in (4-1) is the only one meaningful case for x-pseudolinearly dependent points when x is sufficiently large. We also remark that directly by Theorem 1.2, any fixed point in $E(\mathbb{Q})$ is not an x-pseudolinearly dependent point with respect to Γ for x sufficiently large.

4B. ***Construction.*** In this section, we assume that the rank r of $E(\mathbb{Q})$ and the rank s of Γ satisfy $r \ge 1$ and $s < r$.

In order to get upper bounds on the height of pseudolinearly dependent points, the following construction is slightly different from what we give in (4-1).

Recalling N_p and T_p defined in Section 3C, given any $x \ge 2$, we define

$$L_x = \operatorname{lcm}\{N_p/T_p : p \le x\}.$$

Take a point $R \in E(\mathbb{Q})$ of infinite order such that $\langle R\rangle \cap \Gamma = \{O_E\}$, then pick an arbitrary point $P \in \Gamma$ and set

$$Q = P + L_x R.$$

It is easy to see that $Q \notin \Gamma$ but $Q_p \in \Gamma_p$ for every prime $p \le x$ of good reduction, and so Q is an x-pseudolinearly dependent point.

Since the coordinates of points in $E(\mathbb{Q})$ are rational numbers, for any subset $S \subseteq E(\mathbb{Q})$ there exists a point with smallest Weil height among all the points in S. So, noticing $s < r$, we choose a point with smallest Weil height in the subset consisting of nontorsion points R in $E(\mathbb{Q}) \setminus \Gamma$ with $\langle R\rangle \cap \Gamma = \{O_E\}$; we denote this point by $R_{\min}$.

Now, we define a point $Q_{\min} \in E(\mathbb{Q})$ as follows:

$$Q_{\min} = L_x R_{\min}. \tag{4-2}$$

As before, $Q_{\min} \notin \Gamma$ but $Q_{\min} \in \Gamma_p$ for every prime $p \le x$ of good reduction. We also have

$$\hat{h}(Q_{\min}) = L_x^2 \hat{h}(R_{\min}) = L_x^2(\mathfrak{h}(R_{\min}) + O(1)) \ll L_x^2, \tag{4-3}$$

which comes from the fact that $\mathfrak{h}(R_{\min})$ is fixed when E and Γ are given.

The point $Q_{\min}$ is exactly the point we claim in Theorems 2.1, 2.2, 2.3, and 2.4. So, it remains to prove the claimed upper bounds for $\hat{h}(Q_{\min})$.

5. Proofs of upper bounds

5A. ***Outline.*** As mentioned above, to achieve our purpose, it suffices to bound the canonical height of $Q_{\min}$ given by (4-2), that is, $\hat{h}(Q_{\min})$.

By definition, we directly have

$$L_x \le \prod_{p \le x} N_p/T_p.$$

In view of (4-3), our approach is to get upper and lower bounds respectively for

$$\prod_{p \le x} N_p \quad \text{and} \quad \prod_{p \le x} T_p.$$

5B. *Proof of Theorem 2.1.* Recalling the Hasse bound

$$|N_p - p - 1| \le 2p^{1/2}$$

for any prime p of good reduction (see [Silverman 2009, Chapter V, Theorem 1.1]), we derive the inequality

$$\begin{aligned}\prod_{p\le x} N_p &\le \prod_{p\le x}(p+2p^{1/2}+1) = \prod_{p\le x} p(1+p^{-1/2})^2 \\ &= \exp\Bigl(\sum_{p\le x}\log p + 2\sum_{p\le x}\log(1+p^{-1/2})\Bigr) \\ &\le \exp\Bigl(\sum_{p\le x}\log p + 2\sum_{p\le x} p^{-1/2}\Bigr) \\ &= \exp(O(\sqrt{x}/\log x))\prod_{p\le x} p.\end{aligned} \tag{5-1}$$

Now using the prime number theorem in a simple form:

$$\sum_{p\le x}\log p = x + O(x/(\log x)^2), \tag{5-2}$$

we obtain

$$\prod_{p\le x} N_p \le \exp(x + O(x/(\log x)^2)). \tag{5-3}$$

Combining (5-3) with (4-3), we derive the following upper bound for $\hat{h}(Q_{\min})$:

$$\hat{h}(Q_{\min}) \ll L_x^2 \le \prod_{p\le x} N_p^2 \le \exp(2x + O(x/(\log x)^2)). \tag{5-4}$$

This completes the proof.

We remark that a better error term for the prime number theorem such as that of [Iwaniec and Kowalski 2004, Corollary 8.30] would improve the result, however, the improvement is not substantial, as seen by regarding the main term.

5C. *Proof of Theorem 2.2.* Since Γ has rank zero, by the injectivity of the reduction map restricted to the torsion subgroup, we can see that $T_p = \#\Gamma$ for any prime p of good reduction and coprime to the size of the torsion subgroup.

We also recall the prime number theorem in the following simplified form

$$\pi(x) = \frac{x}{\log x} + O(x/(\log x)^2), \tag{5-5}$$

which follows from (5-2).

Now, using (5-3) and (5-5) we have

$$L_x \ll (\#\Gamma)^{-\pi(x)} \prod_{p \le x} N_p \le \exp\Bigl(x - \log(\#\Gamma)\frac{x}{\log x} + O(x/(\log x)^2)\Bigr).$$

From (4-3) we conclude that for any sufficiently large $x > 0$, we have

$$\hat{h}(Q_{\min}) \le \exp\Bigl(2x - 2\log(\#\Gamma)\frac{x}{\log x} + O(x/(\log x)^2)\Bigr),$$

which completes the proof.

5D. *Proof of Theorem 2.3.* For any sufficiently large x, we define

$$J = \Big\lfloor \frac{s}{s+2}\log x \Big\rfloor \ge 1 \quad \text{and} \quad Z_j = x^{s/(s+2)}e^{-j}, \quad j = 0, \dots, J,$$

where e is the base of the natural logarithm. Note that $1 \le Z_J < e$.

Since $s \ge 1$, the number of primes p such that $T_p = 1$ or 2 is finite; we denote this number by N, which depends on Γ. Let M_0 be the number of primes $p \le x$ with $T_p \ge Z_0$. Furthermore, for $j = 1, \dots, J$, we define M_j as the number of primes $p \le x$ with $Z_{j-1} > T_p \ge Z_j$. Clearly

$$N + \sum_{j=0}^{J} M_j \ge \pi(x).$$

So, noticing $Z_0 = x^{s/(s+2)}$ we now derive

$$\prod_{p \le x} T_p \ge \prod_{j=0}^{J} Z_j^{M_j} \ge Z_0^{\pi(x)-N} \prod_{j=0}^{J} e^{-jM_j} = Z_0^{\pi(x)-N}\exp(-\Lambda),$$

where

$$\Lambda = \sum_{j=1}^{J} jM_j.$$

Recalling the definition of Z_0, and using (5-5), we obtain

$$\prod_{p \le x} T_p \ge \exp\Bigl(\frac{s}{s+2}x - \Lambda + O(x/\log x)\Bigr). \tag{5-6}$$

To estimate Λ, we note that by Lemma 3.1, for any positive integer $I \le J$ we have

$$\sum_{j=I}^{J} M_j \le \#\{p : T_p < Z_0 e^{-I+1}\} \ll \frac{(Z_0 e^{-I+1})^{1+2/s}}{\log Z_0 - I + 1}.$$

Thus for $I \le \frac{1}{2}J$, noticing $J \le \log Z_0$ we obtain

$$\sum_{j=I}^{J} M_j \ll \frac{(Z_0 e^{-I})^{1+2/s}}{\log Z_0} \ll e^{-I(1+2/s)} \frac{x}{\log x}, \tag{5-7}$$

while for any $\frac{1}{2}J < I \le J$ we use the bound

$$\sum_{j=I}^{J} M_j \ll (Z_0 e^{-I+1})^{1+2/s} \ll (\sqrt{Z_0})^{1+2/s} = x^{1/2}. \tag{5-8}$$

Hence, via partial summation, combining (5-7) and (5-8), we derive

$$\begin{aligned}\Lambda = \sum_{I=1}^{J} \sum_{j=I}^{J} M_j &\ll \frac{x}{\log x} \sum_{1 \le I \le J/2} e^{-I(1+2/s)} + x^{1/2} \sum_{J/2 < I \le J} 1 \\ &\ll \frac{x}{\log x} + J x^{1/2} \ll \frac{x}{\log x}.\end{aligned}$$

This bound on Λ, together with (5-6), implies

$$\prod_{p \le x} T_p \ge \exp\Big(\frac{s}{s+2} x + O(x/\log x)\Big).$$

Therefore using (5-3), we obtain

$$L_x \le \prod_{p \le x} N_p / T_p \le \exp\Big(\frac{2}{s+2} x + O(x/\log x)\Big).$$

Therefore, the desired result follows from the bound (4-3).

5E. ***Proof of Theorem 2.4.*** First, we have

$$\begin{aligned}\prod_{p \le x} T_p &\ge \prod_{\substack{p \le x \\ T_p \ge p/(\log p)^2}} \frac{p}{(\log p)^2} \cdot \prod_{\substack{p \le x \\ T_p < p/(\log p)^2}} T_p \\ &= \prod_{p \le x} \frac{p}{(\log p)^2} \cdot \prod_{\substack{p \le x \\ T_p < p/(\log p)^2}} \frac{T_p (\log p)^2}{p}.\end{aligned}$$

Using the trivial lower bound $T_p \ge 1$, we derive

$$\begin{aligned}\prod_{p \le x} T_p &\ge \prod_{p \le x} p \cdot \prod_{p \le x} (\log p)^{-2} \cdot \prod_{\substack{p \le x \\ T_p < p/(\log p)^2}} (\log p)^2 / p \\ &\ge \Big(\frac{(\log x)^2}{x}\Big)^{O(x/(\log x)^2)} \prod_{p \le x} p \cdot \prod_{p \le x} (\log p)^{-2},\end{aligned}$$

where the last inequality follows from Lemma 3.2 and Lemma 3.3.

Thus, using (5-1), we obtain

$$L_x \le \prod_{p\le x} N_p/T_p \le \exp(O(x/\log x)) \prod_{p\le x} (\log p)^2$$
$$\le \exp\Bigl(2\frac{x\log\log x}{\log x} + O(x/\log x)\Bigr),$$

where the last inequality is derived from (5-5) and the trivial estimate

$$\sum_{p\le x} \log\log p \le \pi(x)\log\log x.$$

Therefore, the desired result follows from the bound $\hat{h}(Q_{\min}) \ll L_x^2$.

6. Proofs of lower bounds

6A. ***Proof of Theorem 2.5.*** By assumption, Γ is a torsion subgroup of $E(\mathbb{Q})$. Let $Q \in E(\mathbb{Q})$ be an arbitrary x-pseudolinearly dependent point for a sufficiently large x. Let m be the number of primes of bad reduction for E. Then, since $Q \in \Gamma_p$ for any prime $p \le x$ of good reduction, there exists a rational point $P \in \Gamma$ such that for at least $(\pi(x) - m)/\#\Gamma$ primes $p \le x$ of good reduction we have

$$Q \equiv P \pmod p.$$

In view of (3-3), this implies that

$$\mathfrak{h}(Q-P) \ge 2\log \prod_{p\le(\pi(x)-m)/\#\Gamma} p \ge \frac{2}{\#\Gamma} x/\log x + O(x/(\log x)^2),$$

where the last inequality follows from (5-2) and (5-5). Note that P is a torsion point; then using (3-1) we obtain

$$\hat{h}(Q) = \hat{h}(Q) + \hat{h}(P) \ge \tfrac{1}{2}\hat{h}(Q-P) \ge \tfrac{1}{2}\mathfrak{h}(Q-P) + O(1) \tag{6-1}$$
$$\ge \frac{1}{\#\Gamma} x/\log x + O(x/(\log x)^2),$$

which gives the claimed lower bound for the height of the point Q.

6B. ***Proof of Theorem 2.6.*** For any sufficiently large x, by Proposition 4.1, any x-pseudolinearly dependent point Q of Γ is nontorsion and satisfies $\langle Q\rangle \cap \Gamma = \{O_E\}$. Then, from Lemma 3.9, there is an unconditional prime p of good reduction for E satisfying

$$\log p \ll (\log \hat{h}(Q))^{2s+6} \log\log \hat{h}(Q)$$

such that $Q \notin \Gamma_p$. Since $x < p$, by definition we obtain

$$\log x \ll (\log \hat{h}(Q))^{2s+6} \log\log \hat{h}(Q),$$

which implies that $\hat{h}(Q) \geq \exp((\log x)^{1/(2s+6)+o(1)})$.

Similarly, assuming the GRH, we obtain

$$\hat{h}(Q) \geq \exp(x^{1/(4s+12)+o(1)}),$$

which completes the proof.

7. Comments

In Section 6, we get some partial results on the lower bound for the height of x-pseudolinearly dependent points. In fact, the height of such points certainly tends to infinity as $x \to +\infty$.

Indeed, let E be an elliptic curve over $\mathbb{Q}$ of rank $r \geq 1$, and let Γ be a subgroup of $E(\mathbb{Q})$ with rank $s < r$. We have known that for any sufficiently large x, there exist infinitely many x-pseudolinearly dependent points with respect to Γ. For any $x > 0$, if such points exist, as before we can choose a point, denoted by Q_x, with smallest Weil height among all these points; otherwise if there are no such points, we let $Q_x = O_E$. Thus, we get a subset

$$S = \{Q_x : x > 0\}$$

of $E(\mathbb{Q})$, and for any $x < y$ we have $\mathfrak{h}(Q_x) \leq \mathfrak{h}(Q_y)$. By Theorem 1.2, we know that for any fixed point $Q \in E(\mathbb{Q})$, it can not be an x-pseudolinearly dependent point for any sufficiently large x. So, S is an infinite set. Since it is well-known that there are only finitely many rational points of $E(\mathbb{Q})$ with bounded height, we obtain

$$\lim_{x\to+\infty} \mathfrak{h}(Q_x) = +\infty,$$

which implies that $\lim_{x\to+\infty} \hat{h}(Q_x) = +\infty$. This immediately implies that for the point $Q_{\min}$ constructed in Section 4B, its height $\hat{h}(Q_{\min})$ also tends to infinity as $x \to +\infty$.

Moreover, let p_n denote the n-th prime, that is $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$ For any $n \geq 1$, denote by T_n the set of p_n-pseudolinearly dependent points of Γ. Obviously, $T_{n+1} \subseteq T_n$ and $\mathfrak{h}(Q_{p_{n+1}}) \geq \mathfrak{h}(Q_{p_n})$ for any $n \geq 1$. For any sufficiently large n, we conjecture that $T_{n+1} \subsetneq T_n$. If furthermore one could prove that $\mathfrak{h}(Q_{p_{n+1}}) > \mathfrak{h}(Q_{p_n})$ for any sufficiently large n, this would lead to a lower bound of the form

$$\mathfrak{h}(Q_x) \geq \log x + O(\log\log x),$$

as the values of $\mathfrak{h}(Q_x)$ are logarithms of rational integers and there are about $x/\log x$ primes not greater than x.

In Lemma 3.9, if we choose Γ as a torsion subgroup, we can also get a similar unconditional upper bound. Indeed, for a prime p of good reduction for E, suppose that $Q \in \Gamma_p$. Then, $Q - P \equiv O_E$ modulo p for some $P \in \Gamma$. According to (3-3), we have $p \le \exp(\mathfrak{h}(Q-P)/2)$. Since P is a torsion point, as in (6-1) we get $p \le \exp(\hat{h}(Q)+O(1))$. Thus, we can choose a prime p of good reduction satisfying

$$p \le \exp(\hat{h}(Q) + O(1))$$

such that $Q \notin \Gamma_p$.

Acknowledgements

The authors are very grateful to the referees for their careful reading and valuable comments and suggestions. The authors also thank Wojciech Gajda for his very stimulating discussions which led to the idea of this work and also for his valuable comments on an early version of the paper. These discussions took place at the Max Planck Institute for Mathematics, Bonn, whose support and hospitality are gratefully acknowledged.

This work was also supported in part by the Australian Research Council Grants DP140100118 and DP170100786.

References

[Akbary et al. 2010] A. Akbary, D. Ghioca, and V. K. Murty, "Reductions of points on elliptic curves", *Math. Ann.* **347**:2 (2010), 365–394. MR

[Bach et al. 1996] E. Bach, R. Lukes, J. Shallit, and H. C. Williams, "Results and estimates on pseudopowers", *Math. Comp.* **65**:216 (1996), 1737–1747. MR Zbl

[Bachmakov 1970] M. Bachmakov, "Un théorème de finitude sur la cohomologie des courbes elliptiques", *C. R. Acad. Sci. Paris Sér. A-B* **270** (1970), A999–A1001. MR Zbl

[Banaszak 2009] G. Banaszak, "On a Hasse principle for Mordell–Weil groups", *C. R. Math. Acad. Sci. Paris* **347**:13-14 (2009), 709–714. MR Zbl

[Banaszak and Krasoń 2011] G. Banaszak and P. Krasoń, "On arithmetic in Mordell–Weil groups", *Acta Arith.* **150**:4 (2011), 315–317. MR Zbl

[Banaszak et al. 2005] G. Banaszak, W. Gajda, and P. Krasoń, "Detecting linear dependence by reduction maps", *J. Number Theory* **115**:2 (2005), 322–342. MR Zbl

[Bertrand 1981] D. Bertrand, "Kummer theory on the product of an elliptic curve by the multiplicative group", *Glasgow Math. J.* **22**:1 (1981), 83–88. MR

[Bourgain et al. 2009] J. Bourgain, S. V. Konyagin, C. Pomerance, and I. E. Shparlinski, "On the smallest pseudopower", *Acta Arith.* **140**:1 (2009), 43–55. MR Zbl

[Gajda and Górnisiewicz 2009] W. Gajda and K. Górnisiewicz, "Linear dependence in Mordell–Weil groups", *J. Reine Angew. Math.* **630** (2009), 219–233. MR Zbl

[Gupta and Murty 1986] R. Gupta and M. R. Murty, "Primitive points on elliptic curves", *Compositio Math.* **58**:1 (1986), 13–44. MR Zbl

[Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications **53**, American Mathematical Society, Providence, RI, 2004. MR Zbl

[Jossen 2013] P. Jossen, "Detecting linear dependence on an abelian variety via reduction maps", *Comment. Math. Helv.* **88**:2 (2013), 323–352. MR Zbl

[Jossen and Perucca 2010] P. Jossen and A. Perucca, "A counterexample to the local-global principle of linear dependence for abelian varieties", *C. R. Math. Acad. Sci. Paris* **348**:1-2 (2010), 9–10. MR Zbl

[Konyagin et al. 2010] S. V. Konyagin, C. Pomerance, and I. E. Shparlinski, "On the distribution of pseudopowers", *Canad. J. Math.* **62**:3 (2010), 582–594. MR Zbl

[Kowalski 2003] E. Kowalski, "Some local-global applications of Kummer theory", *Manuscripta Math.* **111**:1 (2003), 105–139. MR Zbl

[Lagarias and Odlyzko 1977] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem", pp. 409–464 in *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham)* (Durham, NC, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR Zbl

[Lagarias et al. 1979] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, "A bound for the least prime ideal in the Chebotarev density theorem", *Invent. Math.* **54**:3 (1979), 271–296. MR Zbl

[Perucca 2010] A. Perucca, "On the problem of detecting linear dependence for products of abelian varieties and tori", *Acta Arith.* **142**:2 (2010), 119–128. MR Zbl

[Pomerance and Shparlinski 2009] C. Pomerance and I. E. Shparlinski, "On pseudosquares and pseudopowers", pp. 171–184 in *Combinatorial number theory*, edited by B. Landman et al., Walter de Gruyter, Berlin, 2009. MR Zbl

[Sadek 2016] M. Sadek, "On dependence of rational points on elliptic curves", *C. R. Math. Acad. Sci. Soc. R. Can.* **38**:2 (2016), 75–84. MR Zbl

[Schinzel 1960] A. Schinzel, "On the congruence $a^x \equiv b \pmod{p}$", *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **8** (1960), 307–309. MR Zbl

[Schinzel 1970] A. Schinzel, "A refinement of a theorem of Gerst on power residues", *Acta Arith.* **17** (1970), 161–168. MR Zbl

[Schinzel 1975] A. Schinzel, "On power residues and exponential congruences", *Acta Arith.* **27** (1975), 397–420. MR Zbl

[Schinzel 1997] A. Schinzel, "On pseudosquares", pp. 213–220 in *New trends in probability and statistics* (Palange, 1996), vol. 4, edited by A. Laurinčikas et al., VSP, Utrecht, The Netherlands, 1997. MR Zbl

[Serre 1981] J.-P. Serre, "Quelques applications du théorème de densité de Chebotarev", *Inst. Hautes Études Sci. Publ. Math.* 54 (1981), 323–401. MR Zbl

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, 2009. MR Zbl

[Silverman and Tate 1992] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer, 1992. MR Zbl

[Weston 2003] T. Weston, "Kummer theory of abelian varieties and reductions of Mordell–Weil groups", *Acta Arith.* **110**:1 (2003), 77–88. MR Zbl

Received June 10, 2016. Revised October 18, 2017.

MIN SHA
SCHOOL OF MATHEMATICS AND STATISTICS
UNIVERSITY OF NEW SOUTH WALES
SYDNEY, NSW
AUSTRALIA

shamin2010@gmail.com

IGOR E. SHPARLINSKI
SCHOOL OF MATHEMATICS AND STATISTICS
UNIVERSITY OF NEW SOUTH WALES
SYDNEY, NSW
AUSTRALIA

igor.shparlinski@unsw.edu.au

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.145

GOOD REDUCTION AND SHAFAREVICH-TYPE THEOREMS FOR DYNAMICAL SYSTEMS WITH PORTRAIT LEVEL STRUCTURES

JOSEPH H. SILVERMAN

Let K be a number field, let S be a finite set of places of K, and let R_S be the ring of S-integers of K. A K-morphism $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ has simple good reduction outside S if it extends to an R_S-morphism $\mathbb{P}^1_{R_S} \to \mathbb{P}^1_{R_S}$. A finite Galois invariant subset $X \subset \mathbb{P}^1_K(\bar{K})$ has good reduction outside S if its closure in $\mathbb{P}^1_{R_S}$ is étale over R_S. We study triples (f, Y, X) with $X = Y \cup f(Y)$. We prove that for a fixed K, S, and d, there are only finitely many $\mathrm{PGL}_2(R_S)$-equivalence classes of triples with $\deg(f) = d$ and $\sum_{P \in Y} e_f(P) \ge 2d+1$ and X having good reduction outside S. We consider refined questions in which the weighted directed graph structure on $f : Y \to X$ is specified, and we give an exhaustive analysis for degree 2 maps on $\mathbb{P}^1$ when $Y = X$.

1. Introduction

Let K be a number field, let S be a finite set of places of K including all archimedean places, and let R_S be the ring of S-integers of K. We recall that an abelian variety A/K is said to have *good reduction outside S* if there exists a proper R_S-group scheme $\mathcal{A}/R_S$ whose generic fiber is K-isomorphic to A/K. Then we have

Research supported by Simons Collaboration Grant #241309.
MSC2010: primary 37P45; secondary 37P15.
Keywords: good reduction, dynamical system, portrait, Shafarevich conjecture.

the following famous conjecture of Shafarevich, which was proven by Shafarevich in dimension 1 and by Faltings in general.

Theorem 1 [Faltings 1983]. *There are only finitely many K-isomorphism classes of abelian varieties A/K having good reduction outside S.*

Our goal in this paper is to study an analogue of Shafarevich's conjecture for dynamical systems on projective space. The first requirement is a definition of good reduction for self-maps of $\mathbb{P}^N$, such as the following.

Definition [Morton and Silverman 1995]. Let $f : \mathbb{P}^N_K \to \mathbb{P}^N_K$ be a nonconstant K-morphism. Then f has (*simple*) *good reduction outside* S if there exists an R_S-morphism $\mathbb{P}^N_{R_S} \to \mathbb{P}^N_{R_S}$ whose generic fiber is $\mathrm{PGL}_{N+1}(K)$-conjugate to f.

If f has simple good reduction outside S, and if $\varphi \in \mathrm{PGL}_{N+1}(R_S)$, then it is clear that the conjugate map

$$f^{\varphi} := \varphi^{-1} \circ f \circ \varphi : \mathbb{P}^N_K \to \mathbb{P}^N_K$$

also has simple good reduction. But even modulo this equivalence, it is easy to see that a dynamical analogue of Shafarevich's conjecture using simple good reduction is false. For example, every map $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ of the form

$$f(X, Y) = [X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d, Y^d] \quad \text{with } a_i \in R_S$$

has simple good reduction outside S, and these maps represent infinitely many $\mathrm{PGL}_2(R_S)$-conjugacy classes. And as noted in [Morton and Silverman 1995, Example 4.1], there are also infinite nonpolynomial families such as

$$[aX^2 + bXY + Y^2, X^2] \quad \text{with } a, b \in R_S.$$

It is thus of interest to formulate alternative definitions of good reduction for which a Shafarevich conjecture might hold in the dynamical setting. The literature contains several papers [Petsche 2012; Petsche and Stout 2015; Stout 2014; Szpiro and Tucker 2008] along these lines. We refer the reader to Section 2 for a description of these earlier results and a comparison with the present paper.

Our approach is to study pairs consisting of a map f and a set of points $Y \in \mathbb{P}^N$ such that the map $f : Y \to f(Y)$ "does not collapse" when it is reduced modulo $\mathfrak{p}$ for primes not in S; see Remark 5 for a discussion of why this is a natural analogue of the classical Shafarevich–Faltings result. To make this precise, we need to define good reduction for sets of points.

Definition. Let $X \subset \mathbb{P}^N(\bar{K})$ be a finite $\mathrm{Gal}(\bar{K}/K)$-invariant subset, say $X = \{P_1, \ldots, P_n\}$. Then X has *good reduction outside* S if for every prime $\mathfrak{p} \notin S$, and every prime $\mathfrak{P}$ of $K(P_1, \ldots, P_n)$ lying over $\mathfrak{p}$, the reduction map[1]

$$X \to \tilde{X} \bmod \mathfrak{P} \quad \text{is injective.}$$

We observe that good reduction is preserved by the natural action of $\mathrm{PGL}_{N+1}(R_S)$ on $\mathbb{P}^N(\bar{K})$.

Our dynamical analogue of the Shafarevich–Faltings theorem is a statement about triples (f, Y, X) consisting of a morphism f and sets of points that have good reduction. We restrict attention to $\mathbb{P}^1$, since this is the setting for which we are currently able to prove a strong Shafarevich-type theorem; but see Section 8 for a brief discussion of possible extensions to $\mathbb{P}^N$ and why the naive generalization fails.

Definition. We define $\mathcal{GR}_d^1[n](K, S)$ to be the set of triples (f, Y, X), where $f : \mathbb{P}_K^1 \to \mathbb{P}_K^1$ is a degree d morphism defined over K and $Y \subseteq X \subset \mathbb{P}^1(\bar{K})$ are finite sets, satisfying the following conditions:

- $X = Y \cup f(Y)$,
- X is $\mathrm{Gal}(\bar{K}/K)$-invariant,
- $\sum_{P \in Y} e_f(P) = n$, where $e_f(P)$ is the ramification index of f at P,
- f and X have good reduction outside S.

We also define a potentially larger set $\widetilde{\mathcal{GR}}_d^1[n](K, S)$ by dropping the requirement that f has good reduction. We observe that if $Y = X$, then the points in X have finite f-orbits, in which case we say that (f, X, X) is a *preperiodic triple*.

There is a natural action of $\mathrm{PGL}_2(R_S)$ on $\mathcal{GR}_d^1[n](K, S)$ and on $\widetilde{\mathcal{GR}}_d^1[n](K, S)$ given by

$$\varphi \cdot (f, Y, X) := \bigl(f^\varphi, \varphi^{-1}(Y), \varphi^{-1}(X)\bigr).$$

Our dynamical Shafarevich-type theorem for $\mathbb{P}^1$ says that if n is sufficiently large, then $\widetilde{\mathcal{GR}}_d^1[n](K, S)$ has only finitely many $\mathrm{PGL}_2(R_S)$-orbits.

Theorem 2 (dynamical Shafarevich theorem for $\mathbb{P}^1$). *Let $d \geq 2$.*

(a) *Let $K/\mathbb{Q}$ be a number field, and let S be a finite set of places of K. Then for all $n \geq 2d+1$, the set*

$$\widetilde{\mathcal{GR}}_d^1[n](K, S) / \mathrm{PGL}_2(R_S) \text{ is finite.}$$

[1] In scheme-theoretic terms, the set X is a reduced 0-dimensional K-subscheme of $\mathbb{P}_K^N$. Let $\mathcal{X} \subset \mathbb{P}_{R_S}^N$ be the scheme-theoretic closure of X. Then X has good reduction outside S if $\mathcal{X}$ is étale over R_S.

(b) *Let S be the set of rational primes less than $2d-2$. Then*

$$\mathcal{GR}_d^1[2d](\mathbb{Q}, S)/\operatorname{PGL}_2(\mathbb{Z}_S) \textit{ is infinite.}$$

Indeed, there are infinitely many $\operatorname{PGL}_2(\mathbb{Z}_S)$*-equivalence classes of preperiodic triples* (f, X, X) *in* $\mathcal{GR}_d^1[2d](\mathbb{Q}, S)$.

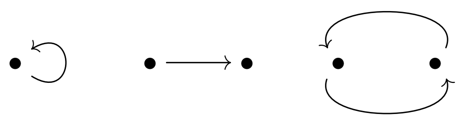
Proof. See Section 3 for the proof of (a), and Section 4, specifically Proposition 11, for the proof of (b). □

In some sense, Theorem 2 is the end of the story for $\mathbb{P}^1$, since it says:

> "The dynamical Shafarevich conjecture is true for sets of weight at least $2d+1$, but it is not true for sets of smaller weight."

However, rather than merely specifying the total weight, we might consider the weighted graph structure that $f : Y \to X$ imposes on X, where each point $P \in Y$ is assigned an outgoing arrow $P \to f(P)$ of weight $e_f(P)$. In dynamical parlance, we want to classify triples (f, Y, X) according to their *portrait structure*.[2] The following example of an (unweighted) portrait illustrates the general idea:

$\mathcal{P}$:



A model for this portrait $\mathcal{P}$ is a triple (f, Y, X) with $Y = \{P_1, P_2, P_4, P_5\}$ and $X = \{P_1, P_2, P_3, P_4, P_5\}$ satisfying

- P_1 is a fixed point of f,
- $f(P_2) = P_3$,
- P_4 and P_5 form a periodic 2-cycle for f.

If each point $P \in \mathcal{P}$ is assigned a weight $\epsilon(P)$, then we might further require that $e_f(P) = \epsilon(P)$, although there are other natural possibilities. Indeed, we consider three ways to define good reduction for dynamical systems and weighted portraits. We start with the largest set and work our way down:

Definition. Let $\mathcal{P}$ be a weighted portrait. We define $\mathcal{GR}_d^1[\mathcal{P}](K, S)$ to be the set of triples (f, Y, X), where $f : \mathbb{P}_K^1 \to \mathbb{P}_K^1$ is a degree d morphism defined over K and $Y \subseteq X \subset \mathbb{P}^1(\bar{K})$ are finite sets, satisfying the conditions

- $X = Y \cup f(Y)$ and $f : Y \to X$ looks like $\mathcal{P}$ (ignoring the weights),
- X is $\operatorname{Gal}(\bar{K}/K)$-invariant,
- f and X have good reduction outside S.

[2]Portrait structures, especially on critical point orbits, are important tools in the study of complex dynamics on $\mathbb{P}^1(\mathbb{C})$; see for example [Arfeux 2016].

We then define three subsets of $\mathcal{GR}_d^1[\mathcal{P}](K,S)$ by imposing the following additional conditions on the triple (f,Y,X) that reflect the weights assigned by $\mathcal{P}$:[3]

$$\begin{aligned}
&\mathcal{GR}_d^1[\mathcal{P}]^\bullet(K,S)\colon\ e_f(P)\ge\epsilon(P) \text{ for all } P\in Y,\\
&\mathcal{GR}_d^1[\mathcal{P}]^\circ(K,S)\colon\ e_f(P)=\epsilon(P) \text{ for all } P\in Y,\\
&\mathcal{GR}_d^1[\mathcal{P}]^\star(K,S)\colon\ e_{\tilde f}(\tilde P \bmod \mathfrak{p})=\epsilon(P) \text{ for all } P\in Y \text{ and all } \mathfrak{p}\notin S.
\end{aligned}$$

We refer the reader to Section 6 for rigorous definitions of portraits, both weighted and unweighted, and their models. See also the companion paper [Doyle and Silverman ≥ 2018], in which we construct parameter spaces and moduli spaces for dynamical systems with portraits via geometric invariant theory and study some of their geometric and arithmetic properties.

This leads to fundamental questions:

Question 3. For a given $d\ge 2$, classify the portraits $\mathcal{P}$ having the property that for all number fields K and all finite sets of places S, the set

$$\mathcal{GR}_d^N[\mathcal{P}]^x(K,S)/\operatorname{PGL}_2(R_S) \text{ is finite,}\quad \text{where } x\in\{\bullet,\circ,\star\}.$$

If $\mathcal{P}$ has this property, then we say that $\mathcal{P}$ is an (x,d)-*Shafarevich portrait*, or that (x,d)-*Shafarevich finiteness holds for* $\mathcal{P}$.

For example, Theorem 2(a) says that if the total weight of the points in $\mathcal{P}$ is at least $2d+1$, then $(\bullet,d)$-Shafarevich finiteness holds for $\mathcal{P}$. This is quite satisfactory. But the converse result, which is Theorem 2(b), says only that there exists at least one portrait of total weight $2d$ such that $(\bullet,d)$-Shafarevich finiteness fails for $\mathcal{P}$. It says nothing about the full set of such portraits. And indeed, we will prove that among the many portraits of total weight 4, $(\bullet,2)$-Shafarevich finiteness holds for some and not for others! Thus the answer to Question 3 appears to be fairly subtle for portraits of weight at most $2d$.

In those cases that $\mathcal{GR}_d^1[\mathcal{P}]^x(K,S)$ is infinite, we might ask for a more refined measure of its size. This is provided by looking at its image in the moduli space $\mathcal{M}_d^1$, where $\mathcal{M}_d^1:=\operatorname{End}_d^1/\!/\operatorname{SL}_2$ is the moduli space of dynamical systems of degree d morphisms on $\mathbb{P}^1$. (See [Milnor 1993; Silverman 1998] for the construction of $\mathcal{M}_d^1$, and [Levy 2011; Petsche et al. 2009] for an analogous construction for $\mathbb{P}^N$.) This prompts the following definition.

Definition. Let $d\ge 2$, let $x\in\{\bullet,\circ,\star\}$, and let $\mathcal{P}$ be a portrait. The (x,d)-*Shafarevich dimension of* $\mathcal{P}$ is the quantity

$$\operatorname{ShafDim}_d^1[\mathcal{P}]^x=\sup_{\substack{K \text{ a number field}\\ S \text{ a finite set of places}}}\dim\overline{\operatorname{Image}\bigl(\mathcal{GR}_d^1[\mathcal{P}]^x(K,S)\to\mathcal{M}_d^1\bigr)},$$

where the overline denotes the Zariski closure.

[3]We note that $\star$-good reduction was first defined and studied by Petsche and Stout [2015], specifically for $d=2$ and $\mathcal{P}$ consisting of two fixed points or one 2-cycle.

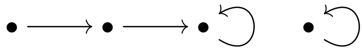
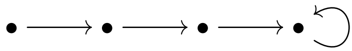
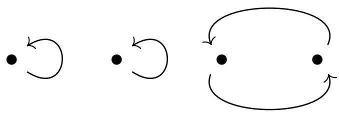
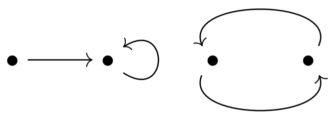
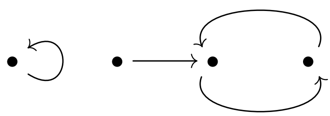
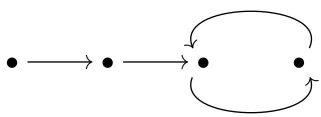
$\mathcal{P}$	(1, 2)-Shafarevich finiteness true?
	yes
	no
	yes
	yes
	yes
	no
	yes
	yes

Table 1. Some weight 4 portraits for degree 2 maps.

By definition, we have

$$\mathcal{P} \text{ is a } (x, d)\text{-Shafarevich portrait} \quad \Longrightarrow \quad \operatorname{ShafDim}_d^1[\mathcal{P}]^x = 0.$$

A natural generalization of Question 3 is to ask for a formula (or algorithm, or ...) for $\operatorname{ShafDim}_d^1[\mathcal{P}]^x$ as a function of $\mathcal{P}$.

In this paper we start to answer this refined question by performing an exhaustive computation of $\operatorname{ShafDim}_2^1[\mathcal{P}]^x$ for preperiodic portraits of weight up to 4, since Theorem 2(a) says that the dimension is 0 for portraits whose weight is strictly greater than 4.

To partially illustrate the complete results that are given in Section 7, we refer the reader to Table 1. This table lists eight preperiodic portraits of weight 4 that arise for degree 2 maps of $\mathbb{P}^1$. For six of them, the $(\bullet, 2)$-Shafarevich finiteness property holds, while for two of them it does not. It is not clear (to this author) how to distinguish this dichotomy directly from the geometry of the portraits, other than by performing a detailed analysis. It turns out that there are 34 possible portraits of weight at most 4 for degree 2 maps of $\mathbb{P}^1$. See Section 7 for an analysis of all 34 portraits and a computation of their various Shafarevich dimensions.

We can also turn the question around by fixing $\mathcal{P}$ and letting $d \to \infty$. We note that the Shafarevich dimension is never more than $\dim \mathcal{M}_d^1 = 2d-2$.

Question 4. For a given unweighted portrait $\mathcal{P}$, what is the limiting behavior of the *Shafarevich discrepancy*[4]

$$2d-2-\mathrm{ShafDim}_d^1[\mathcal{P}] \quad \text{as } d \to \infty?$$

We note that Question 4 is quite interesting even for $\mathcal{P} = \varnothing$. We will show in Proposition 12 that

$$d \le \mathrm{ShafDim}_d^1[\varnothing] \le 2d-2.$$

This gives the exact value for $d = 2$, a result that is also proven in [Petsche and Stout 2015] using a slightly different argument.

Remark 5. Returning to the case of abelian varieties for motivation and inspiration, we note that an abelian variety is really a pair $(A, \mathcal{O})$ consisting of a variety and a marked point. As noted by Petsche and Stout [2015], if we discard the marked point, then Shafarevich finiteness is no longer true. For example, there may be infinitely many K-isomorphism classes of curves of genus 1 having good reduction outside S. Hence in order to prove Shafarevich finiteness for a collection of geometric object (varieties, maps, etc.), it is very natural to add level structure in the form of one or more points. We also remark that if we add further level structure to an abelian variety, for example specifying an n-torsion point Q, then an ostensibly stronger form of good reduction would require that the points Q and $\mathcal{O}$ remain distinct modulo the primes not in S. But if we enlarge S so that $n \in R_S^*$, then the two forms of good reduction are actually identical due to the standard result on injectivity of torsion under reduction; cf. [Hindry and Silverman 2000, Theorem C.1.4] or [Mumford 1970, Appendix II, Corollary 1]. To make the dynamical analogy complete, we note that torsion points are exactly the points of A that are preperiodic for the doubling map.

2. Earlier results

It has long been realized that dynamical Shafarevich finiteness does not hold for morphisms $f : \mathbb{P}^1 \to \mathbb{P}^1$ if the definition of good reduction is simple good reduction; cf. [Morton and Silverman 1995, Example 4.1]. This has led a number of authors to impose additional good reduction conditions on f and to prove a variety of finiteness theorems. We briefly mention a few of these results.

[4]If $\mathcal{P}$ has weights ϵ, it is more natural to consider the quantity $2d-2-\sum_{P\in Y}\bigl(\epsilon(P)-1\bigr) - \mathrm{ShafDim}_d^1[\mathcal{P}]^x$ for $x \in \{\bullet, \circ, \star\}$.

Closest in spirit to the present paper is work of Petsche and Stout [2015] in which they study good reduction of degree 2 maps of $\mathbb{P}^1$. They define (with similar notation) the sets that we've denoted by $\mathcal{GR}_d^1(K, S)[\varnothing]$ and they pose the question of whether the maps in this set are Zariski dense in the moduli space $\mathcal{M}_d^1$. They prove that this is true for $d = 2$, which is a special case of our Proposition 12. They also study maps with $\star$-good reduction relative to various portraits, i.e., the sets $\mathcal{GR}_d^1[\mathcal{P}]^\star$ defined earlier. For example, they prove that $\operatorname{ShafDim}_2^1[\mathcal{P}]^\star = 1$ when $\mathcal{P}$ is a portrait consisting of two unramified fixed points, and similarly when $\mathcal{P}$ is a portrait consisting of a single unramified 2-cycle. (These are the portraits labeled $\mathcal{P}_{2,3}$ and $\mathcal{P}_{2,4}$ in Table 2.) We will show later that $\operatorname{ShafDim}_2^1[\mathcal{P}]^\circ = 1$ and $\operatorname{ShafDim}_2^1[\mathcal{P}]^\bullet = 2$ for these two portraits. More generally, in Section 7 we compute the three Shafarevich dimensions for the 34 preperiodic portraits of weight at most 4 for degree 2 maps of $\mathbb{P}^1$.

Other approaches to a dynamical Shafarevich conjecture also consider pairs (f, X) or triples (f, Y, X) of maps and points, but impose different function-theoretic constraints. Thus in [Szpiro and Tucker 2008; Szpiro et al. 2017; Szpiro and West 2017], maps are classified according to what Szpiro characterizes as "differential good reduction". For a given map $f : \mathbb{P}^1 \to \mathbb{P}^1$, let $\mathcal{R}(f)$ denote the set of ramified points of f and let $\mathcal{B}(f) = f(\mathcal{R}(f))$ denote the set of branch points.[5]

Definition. The map f has *critical good reduction* outside S if each of the sets $\mathcal{R}(f)$ and $\mathcal{B}(f)$ has good reduction outside S. The map f has *critical excellent reduction* outside S if the union $\mathcal{R}(f) \cup \mathcal{B}(f)$ has good reduction outside S.

Canci, Peruginelli, and Tossici [Canci et al. 2013] prove that f has critical good reduction if and only if f has simple good reduction and the branch locus $\mathcal{B}(f)$ has good reduction.

Theorem 6 [Szpiro et al. 2017; Szpiro and West 2017]. *Fix a number field K, a finite set of places S, and an integer $d \geq 2$. Then up to $\mathrm{PGL}_2(K)$-conjugacy, there are only finitely many degree d maps $f : \mathbb{P}_K^1 \to \mathbb{P}_K^1$ that are ramified at 3 or more points and have critically good reduction outside S.*

Theorem 6 of Szpiro, Tucker, and West fits into the framework of our Theorem 2, since their maps f correspond to triples

$$\bigl(f, \mathcal{R}(f), \mathcal{R}(f) \cup \mathcal{B}(f)\bigr) \in \widetilde{\mathcal{GR}}_d^1[n](K, S),$$

where

$$n = \sum_{P \in \mathcal{R}(f)} e_f(P) = \sum_{P \in \mathcal{R}(f)} \bigl(e_f(P) - 1\bigr) + \#\mathcal{R}(f) = 2d - 2 + \#\mathcal{R}(f).$$

[5]In dynamical terminology, $\mathcal{R}(f)$ is the set of *critical points* and $\mathcal{B}(f)$ is the set of *critical values*.

If we assume that $\#\mathcal{R}(f) \ge 3$ as in Theorem 6, then $n \ge 2d+1$, so we see that Theorem 6 follows from Theorem 2(a).

The proof of Theorem 6 in [Szpiro et al. 2017; Szpiro and West 2017] uses a finiteness result for sets of points in $\mathbb{P}^1(K)$ having good reduction outside S, similar to our Lemmas 7 and 8, which in turn rely on classical results of Hermite and Minkowski together with the finiteness of solutions to the S-unit equation. The other ingredient used by Szpiro, Tucker, and West in their proof of Theorem 6 is a special case of a theorem of Grothendieck that computes the tangent space of the parameter scheme of morphisms. We remark that [Szpiro et al. 2017; Szpiro and West 2017; Szpiro and Tucker 2008] also deal with the case of function fields, which can present additional complications.

The earlier paper of Szpiro and Tucker [2008] proved a result similar to Theorem 6, but with a two-sided conjugation equivalence relation, i.e., f_1 and f_2 are considered equivalent if there are maps $\varphi, \psi \in \mathrm{PGL}_2$ such that $f_2 = \psi \circ f_1 \circ \varphi$. This equivalence relation, while interesting, is not well suited for studying dynamics.

There is an article of Stout [2014] in which he proves that for a fixed rational map f, there are only finitely many $\bar{K}/K$ twists of f having simple good reduction outside of S. And a paper of Petsche [2012] proves a Shafarevich finiteness theorem for certain families of critically separable maps, which he defines to be maps f of degree $d \ge 2$ such that for every prime not in S, the reduced map has $2d-2$ distinct critical points. In other words, $\#\mathcal{R}(f) = 2d-2$ and $\mathcal{R}(f)$ has good reduction outside S. This is not enough to obtain finiteness, so Petsche restricts to certain codimension 3 families in Rat_d^1 that are modeled after Lattès maps, and he proves that the dynamical Shafarevich conjecture holds for these families.

A number of authors have studied the resultant equation $\mathrm{Res}(F, G) = c$, where the coefficients of F and G are viewed as indeterminates [Evertse and Győry 1993; Győry 1990; 1993]. Taking c to be an S-unit, this is clearly related to the question of simple good reduction of the map $f = [F, G] \in \mathrm{End}_d^1$. Rephrasing the results in our notation,[6] Evertse and Győry [1993, Corollary 1] prove that up to $\mathrm{PGL}_2(R_S)$-equivalence, there are only finitely many $f = [F, G] \in \mathrm{End}_d^1$ having the property that FG is square-free and splits completely over K. Alternatively, their conditions may be phrased in terms of f as requiring that 0 and ∞ are not critical values of f and that the points in $f^{-1}(0) \cup f^{-1}(\infty)$ are in $\mathbb{P}^1(K)$, and their conclusion is that Shafarevich finiteness is true for this collection of maps. We note that the condition that $f^{-1}(0) \cup f^{-1}(\infty) \subset \mathbb{P}^1(K)$ means, more or less, that the maps in question correspond to S-integral points on a $2d$-to-1 finite cover of an open subset of End_d^1.

Finally, we mention two topics that seem at least tangentially related. There are a number of papers that fix a map f and a wandering point P and ask which portraits

[6] We have restricted to the case that $\deg(F) = \deg(G)$, although the cited papers do not require this.

arise when one reduces the orbit of P modulo various primes; see for example [Faber and Granville 2011; Ghioca et al. 2015]. And there are two articles of Doyle [2016; 2018] in which he classifies periodic point portraits that are permitted for unicritical polynomials, i.e., polynomials of the form $ax^d + b$. These results could be useful in studying the geometry and arithmetic of our portrait moduli spaces studied in [Doyle and Silverman $\geq$ 2018].

3. Dynamical Shafarevich finiteness holds on $\mathbb{P}^1$ for weight $\geq 2d+1$

In this section we prove Theorem 2(a); namely we prove that the dynamical Shafarevich finiteness holds for maps f of $\mathbb{P}^1$ and f-invariant sets X of weight at least $2d+1$. The first step is to show that there are only finitely many choices for the set X.

Definition. Let K be a number field, let S be a finite set of places including all archimedean places, and let $n \geq 1$ be an integer. We define $\mathcal{X}[n](K, S)$ to be the collection of subsets $X \subset \mathbb{P}^1(\bar{K})$ satisfying

- $\#X = n$,
- X is $\mathrm{Gal}(\bar{K}/K)$-invariant,
- X has good reduction outside S.

We note that if $\varphi \in \mathrm{PGL}_2(R_S)$ and $X = \{P_1, \ldots, P_n\} \in \mathcal{X}[n](K, S)$, then

$$\varphi(X) := \{\varphi(P_1), \ldots, \varphi(P_n)\} \in \mathcal{X}[n](K, S), \tag{1}$$

so there is a natural action of $\mathrm{PGL}_2(R_S)$ on $\mathcal{X}[n](K, S)$. More generally, we use (1) to define an action of $\mathrm{PGL}_2(\bar{K})$ on n-tuples of points in $\mathbb{P}^1(\bar{K})$.

The following lemma is well known, but for lack of a suitable reference and as a convenience to the reader, we include the proof.

Lemma 7. *Fix a number field K, a finite set of places S including all archimedean places, and an integer $n \geq 3$. Then*

$$\mathcal{X}[n](K, S)/\,\mathrm{PGL}_2(R_S)$$

is finite.

We start with a sublemma that will allow us to restrict attention to set of points defined over a single field K.

Sublemma 8. *Let K be a number field, let S be a finite set of places including all archimedean places, and let $n \geq 3$ be an integer. Then there is a constant $C(K, S, n)$ such the map*

$$\mathcal{X}[n](K, S)/\,\mathrm{PGL}_2(R_S) \to \{X \subset \mathbb{P}^1(\bar{K}) : \#X = n\}/\,\mathrm{PGL}_2(\bar{K})$$

is at most $C(K, S, n)$-to-1.

Proof. Let $X = \{P_1, \dots, P_n\} \in \mathcal{X}[n](K, S)$. The fact that X is Galois invariant implies that the field

$$K_X := K(P_1, \dots, P_n)$$

is a Galois extension of degree dividing $n!$. Further, the good reduction assumption on X implies that K_X/K is unramified outside S. It follows from the Hermite–Minkowski theorem [Neukirch 1999, Section III.2] that there are only finitely many possibilities for the field K_X.[7] It follows that the field

$$K' := \prod_{X \in \mathcal{X}[n](K,S)} K_X \tag{2}$$

is a finite Galois extension of K that depends only on K, S, and n.

We now fix an n-tuple $X_0 \in \mathcal{X}[n](K, S)$, say $X_0 = \{Q_1, \dots, Q_n\}$, and consider the set of n-tuples in $\mathcal{X}[n](K, S)$ that are $\mathrm{PGL}_2(\bar{K})$-equivalent to X_0. Our goal is to prove that the set

$$\mathrm{PGL}_2(K, S, X_0) := \{\varphi \in \mathrm{PGL}_2(\bar{K}) : \varphi(X_0) \in \mathcal{X}[n](K, S)\}$$

has the property that $\mathrm{PGL}_2(K, S, X_0)/\mathrm{PGL}_2(R_S)$ is finite and has order bounded solely in terms of K, S, and n.

Our first observation is that if $\varphi \in \mathrm{PGL}_2(K, S, X_0)$, then in particular we have $Q_i \in \mathbb{P}^1(K')$ and $\varphi(Q_i) \in \mathbb{P}^1(K')$ for all $1 \le i \le n$, where K' is the field (2). A fractional linear transformation is determined by its values at three points, so our assumption that $n \ge 3$ tells us that $\varphi \in \mathrm{PGL}_2(K')$, i.e., every $\varphi \in \mathrm{PGL}_2(K, S, X_0)$ is defined over the finite extension K' of K, where K' does not depend on X_0.

Next let S' be the places of K' lying over S. The good reduction assumption on X_0 and $\varphi(X_0)$ implies that $Q_1, \dots, Q_n$ remain distinct modulo all primes $\mathfrak{P}$ of L with $\mathfrak{P} \notin S'$, and similarly for $\varphi(Q_1), \dots, \varphi(Q_n)$. Since $n \ge 3$, we can apply the following elementary result to conclude that φ has simple good reduction at $\mathfrak{P}$, and since this holds for all $\mathfrak{P} \notin S'$, we see that $\varphi \in \mathrm{PGL}_2(R_{S'})$.

Sublemma 9. *Let R be a discrete valuation ring with maximal ideal $\mathfrak{P}$ and fraction field K. Let $P_1, P_2, P_3 \in \mathbb{P}^1(K)$ be points whose reductions modulo $\mathfrak{P}$ are distinct, and let $Q_1, Q_2, Q_3 \in \mathbb{P}^1(K)$ also be points with distinct mod $\mathfrak{P}$ reductions. Let $\varphi \in \mathrm{PGL}_2(K)$ be the unique linear fractional transformation satisfying $\varphi(P_i) = Q_i$ for $1 \le i \le 3$. Then $\varphi \in \mathrm{PGL}_2(R)$, i.e., φ has good reduction modulo $\mathfrak{P}$.*

Proof. The fact that the reductions of P_1, P_2, P_3 are distinct means that we can find a linear fractional transformation $\psi \in \mathrm{PGL}_2(R)$ satisfying $\psi(P_1) = 0$, $\psi(P_2) = 1$, $\psi(P_3) = \infty$. Similarly, we can find a $\lambda \in \mathrm{PGL}_2(R)$ satisfying $\lambda(Q_1) = 0$, $\lambda(Q_2) = 1$,

[7] More precisely, our assumptions imply that for $\mathfrak{p} \notin S$, we have $\operatorname{ord}_{\mathfrak{p}} \mathfrak{D}_{L/K} = 0$, while for all primes $\mathfrak{p}$ one has the standard estimate $\operatorname{ord}_{\mathfrak{p}} \mathfrak{D}_{L/K} \le [L : K] - 1$. This proves that $\mathsf{N}_{L/K}\mathfrak{D}_{L/K}$ is bounded, and then for a fixed K, Hermite–Minkowski says that there are only finitely many L.

$\lambda(Q_3)=\infty$. Then $\lambda\circ\varphi\circ\psi^{-1}$ fixes 0, 1, and ∞, so it is the identity map. Hence $\varphi=\lambda^{-1}\circ\psi\in\mathrm{PGL}_2(R)$. $\square$

We next observe that if $\varphi\in\mathrm{PGL}_2(K,S,X_0)$, then by definition and from what we proved earlier, both of the sets X_0 and $\varphi(X_0)$ are composed of points in $\mathbb{P}^1(K')$ and both are $\mathrm{Gal}(K'/K)$-invariant. Hence for any $\sigma\in\mathrm{Gal}(K'/K)$, we find that

$$\varphi(X_0)=(\varphi(X_0))^\sigma=\varphi^\sigma(X_0^\sigma)=\varphi^\sigma(X_0).$$

Thus $\varphi^{-1}\circ\varphi^\sigma : X_0\to X_0$, i.e., the map $\varphi^{-1}\circ\varphi^\sigma$ is a permutation of the set X_0. We thus obtain a map

$$\begin{gathered}\mathrm{PGL}_2(K,S,X_0)\to\mathrm{Map}_{\mathsf{Set}}(\mathrm{Gal}(K'/K),\mathcal{S}_{X_0}),\\ \varphi\mapsto(\sigma\mapsto\varphi^{-1}\circ\varphi^\sigma),\end{gathered}$$

where $\mathcal{S}_{X_0}$ denotes the group of permutations of the set X_0. (The map $\sigma\mapsto\varphi^{-1}\circ\varphi^\sigma$ is actually some sort of cocycle, but that is irrelevant for our purposes.) Since $\mathrm{Gal}(K'/K)$ and $\mathcal{S}_{X_0}$ are both finite and have order bounded in terms of K, S, and n, it suffices to fix some $\varphi_0\in\mathrm{PGL}_2(K,S,X_0)$ and to bound the number of $\mathrm{PGL}_2(R_S)$ equivalence classes of maps $\varphi\in\mathrm{PGL}_2(K,S,X_0)$ that have the same image in $\mathrm{Map}_{\mathsf{Set}}(\mathrm{Gal}(K'/K),\mathcal{S}_{X_0})$. This means that for all $\sigma\in\mathrm{Gal}(K'/K)$, the maps $\varphi^{-1}\circ\varphi^\sigma=\varphi_0^{-1}\circ\varphi_0^\sigma$ have the same effect on X_0; and since $\#X_0=n\geq 3$ and linear fractional transformations are determined by their values on three points, it follows that $\varphi^{-1}\circ\varphi^\sigma=\varphi_0^{-1}\circ\varphi_0^\sigma$ as elements of $\mathrm{PGL}_2(K')$. Thus

$$\varphi\circ\varphi_0^{-1}=\varphi^\sigma\circ(\varphi_0^\sigma)^{-1}=(\varphi\circ\varphi_0^{-1})^\sigma\quad\text{for all }\sigma\in\mathrm{Gal}(K'/K).$$

Hence $\varphi\circ\varphi_0^{-1}\in\mathrm{PGL}_2(K)$. But we also know that φ_0 and φ are in $\mathrm{PGL}_2(R_{S'})$, so

$$\varphi\circ\varphi_0^{-1}\in\mathrm{PGL}_2(K)\cap\mathrm{PGL}_2(R_{S'}).$$

It remains to show that

$$\mathrm{PGL}_2(K)\cap\mathrm{PGL}_2(R_{S'})=\mathrm{PGL}_2(R_S),\tag{3}$$

since that will show that up to composition with elements of $\mathrm{PGL}_2(R_S)$, there are only finitely many choices for φ. In order to prove (3), we start with some $\psi\in\mathrm{PGL}_2(K)\cap\mathrm{PGL}_2(R_{S'})$. Then for each prime $\mathfrak{p}\notin S$, we need to show that ψ has good reduction at $\mathfrak{p}$. We write ψ in normalized form as

$$\psi(X,Y)=[aX+bY,cX+dY]\quad\text{with }a,b,c,d\in K\text{ and}\tag{4}$$
$$\min\{\mathrm{ord}_\mathfrak{p}(a),\mathrm{ord}_\mathfrak{p}(b),\mathrm{ord}_\mathfrak{p}(c),\mathrm{ord}_\mathfrak{p}(d)\}=0,$$

i.e., a,b,c,d are all $\mathfrak{p}$-integral, and at least one of them is a $\mathfrak{p}$-unit. Now let $\mathfrak{P}$ be a prime of K' lying above $\mathfrak{p}$. We are given that ψ has good reduction at $\mathfrak{P}$, which means that if we choose a $\mathfrak{P}$-normalized equation for ψ, its reduction modulo $\mathfrak{P}$

has good reduction. But (4) is already normalized for $\mathfrak{P}$, since $\operatorname{ord}_{\mathfrak{P}} = e(\mathfrak{P}/\mathfrak{p}) \operatorname{ord}_{\mathfrak{p}}$. Hence

$$ad - bc \text{ is a } \mathfrak{P}\text{-adic unit.}$$

But $ad - bc \in K$, so $ad - bc$ is a $\mathfrak{p}$-adic unit, and hence ψ has good reduction at $\mathfrak{p}$. This holds for all $\mathfrak{p} \notin S$, which completes the proof that $\psi \in \mathrm{PGL}_2(R_S)$, and thus completes the proof of Sublemma 8. □

Proof of Lemma 7. Let L/K be a finite Galois extension, and let T be a finite of places of L whose restriction to K contains S. Then we get a natural map

$$\mathcal{X}[n](K, S)/\mathrm{PGL}_2(R_S) \to \mathcal{X}[n](L, T)/\mathrm{PGL}_2(R_T), \tag{5}$$

since if $X \subset \mathbb{P}^1(\bar{K})$ is $\mathrm{Gal}(\bar{K}/K)$ invariant and has good reduction outside S, it is clear that X is also $\mathrm{Gal}(\bar{L}/L)$ invariant and has good reduction outside T. However, what is not clear *a priori* is that the map (5) is finite-to-one, since $\mathrm{PGL}_2(R_T)$ may be larger than $\mathrm{PGL}_2(R_S)$.

However Sublemma 8 says not only that the map

$$\mathcal{X}[n](K, S)/\mathrm{PGL}_2(R_S) \to \{X \subset \mathbb{P}^1(\bar{K}) : \#X = n\}/\mathrm{PGL}_2(\bar{K})$$

is finite-to-one, but it also says that the number of elements in each $\mathrm{PGL}_2(\bar{K})$-equivalence class of $\mathcal{X}[n](K, S)/\mathrm{PGL}_2(R_S)$ is bounded solely in terms of K, S, and n. Hence using (5), it suffices to prove Lemma 7 for any such L and T.

As shown in the proof of Sublemma 8, there is a finite extension K'/K such that every $X \in \mathcal{X}[n](K, S)$ is an n-tuple of points in $\mathbb{P}^1(K')$. We then let S' be a finite set of places of K' such that S' restricted to K contains S and such that $R_{S'}$ is a PID. Replacing K and S with K' and S', we are reduced to studying the $\mathrm{PGL}_2(R_S)$-equivalence classes of the set of $X \in \mathcal{X}[n](K, S)$ such that

$$X = \{P_1, \ldots, P_n\} \quad \text{with } P_1, \ldots, P_n \in \mathbb{P}^1(K),$$

with the further condition that R_S is a PID. This allows us to choose normalized coordinates for the points in X, say

$$P_i = [a_i, b_i] \quad \text{with } a_i, b_i \in R_S \text{ and } \gcd_{R_S}(a_i, b_i) = 1.$$

The good reduction assumption says that $P_1, \ldots, P_n$ are distinct modulo all primes not in S, which given our normalization of the coordinates of the P_i, is equivalent to the statement that

$$a_i b_j - a_j b_i \in R_S^* \quad \text{for all } 1 \le i < j \le n.$$

This means that we can find a linear fractional transformation $\varphi \in \mathrm{PGL}_2(R_S)$ that moves the first three points in our list to the points

$$\varphi(P_1) = [1, 0], \quad \varphi(P_2) = [0, 1], \quad \varphi(P_3) = [1, 1].$$

Replacing X by $\varphi(X)$, the remaining points in X are S-integral points of the scheme

$$\mathbb{P}^1_{R_S} \smallsetminus \{[1,0],[0,1],[1,1]\}, \tag{6}$$

and it is well known that there are only finitely many such points. More precisely, a normalized point $P = [a, b]$ is an S-integral point of the scheme (6) if and only if a, b, and $a - b$ are S-units. But this implies that $\left(\frac{a}{a-b}, \frac{b}{b-a}\right)$ is a solution to the S-unit equation $U + V = 1$, and hence that there are only finitely many values for each of $\frac{a}{a-b}$ and $\frac{b}{b-a}$ [Silverman 2009, IX.4.1]. Further, each S-unit solution (u, v) to $u + v = 1$ gives one point $P = [a, b] = [u, -v]$. This concludes the proof that there are only finitely many $\mathrm{PGL}_2(R_S)$-equivalence classes of sets X having n elements and good reduction outside S. □

The following geometric result is also undoubtedly well known, but for lack of a suitable reference and the convenience of the reader, we include the short proof.[8]

Lemma 10. *Let K be a field, and let $f, g : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be rational maps of degree $d \geq 1$. Suppose that*

$$\sum_{\substack{P\in\mathbb{P}^1(K)\\ f(P)=g(P)}} \min\{e_f(P), e_g(P)\} \geq 2d+1.$$

Then $f = g$.

Proof. We may assume that K is algebraically closed. We fix a basepoint $P_0 \in \mathbb{P}^1(K)$, and we take

$$H_1 = \{P_0\} \times \mathbb{P}^1 \quad \text{and} \quad H_2 = \mathbb{P}^1 \times \{P_0\}$$

as generators for $\mathrm{Pic}(\mathbb{P}^1 \times \mathbb{P}^1) \cong \mathbb{Z} \oplus \mathbb{Z}$. We consider the divisors

$$\Delta = \{(P,P) : P \in \mathbb{P}^1(K)\} \in \mathrm{Div}(\mathbb{P}^1 \times \mathbb{P}^1),$$
$$\Gamma_{f,g} = (f \times g)_*\Delta \in \mathrm{Div}(\mathbb{P}^1 \times \mathbb{P}^1).$$

We write $|\Delta|$ and $|\Gamma_{f,g}|$ for the supports of Δ and $\Gamma_{f,g}$, respectively, and we note that these supports are irreducible, since they are the images of $\mathbb{P}^1$ under, respectively, the diagonal map and the map $f \times g$.

We use the push-pull formula to compute the global intersection

$$\Gamma_{f,g} \cdot H_1 = (f \times g)_*(\Delta) \cdot H_1 = \Delta \cdot (f \times g)^*(H_1) = \Delta \cdot (f^*(P_0) \times \mathbb{P}^1) = d.$$

Similarly, we have $\Gamma_{f,g} \cdot H_2 = d$. Hence

$$\Gamma_{f,g} = dH_1 + dH_2 \quad \text{in } \mathrm{Pic}(\mathbb{P}^1 \times \mathbb{P}^1).$$

[8]Mike Zieve has pointed out that this lemma may also be proven by writing f and g as quotients of polynomials $f = f_1/f_2$ and $g = g_1/g_2$, and then analyzing the factorization of $f_1g_2 - f_2g_1$.

This allows us to compute

$$\Gamma_{f,g} \cdot \Delta = dH_1 \cdot \Delta + dH_2 \cdot \Delta = 2d. \tag{7}$$

Choose some $P \in \mathbb{P}^1(K)$ satisfying $f(P) = g(P)$, and let z be a local uniformizer at P. We may assume that $z(f(P)) \neq \infty$, since otherwise we can replace z by $z/(z-1)$. By assumption we have $c := f(P) = g(P)$, so locally near P the functions f and g satisfy

$$f(z) \in c + az^{e_f(P)} + z^{e_f(P)+1} K[\![z]\!], \qquad g(z) \in c + bz^{e_g(P)} + z^{e_g(P)+1} K[\![z]\!]$$

for some nonzero a and b. This allows us to estimate the following local intersection index:

$$\begin{aligned} \bigl((f \times g)_* \Delta \cdot \Delta\bigr)_{(f(P),g(P))} &= \dim_K \frac{K[\![x, y, z]\!]}{\bigl(x - f(z), y - g(z), x - y\bigr)} \\ &= \dim_K \frac{K[\![z]\!]}{\bigl(f(z) - g(z)\bigr)} \\ &\geq \min\{e_f(P), e_g(P)\}. \end{aligned} \tag{8}$$

Suppose that $|\Gamma_{f,g}| \cap |\Delta|$ is finite. Then we can calculate $\Gamma_{f,g} \cdot \Delta$ as a sum of local intersections. Combined with (8), this yields

$$\begin{aligned} 2d &= \Gamma_{f,g} \cdot \Delta \quad \text{from (7)}, \\ &= \sum_{Q \in \mathbb{P}^1(K)} \bigl((f \times g)_* \Delta \cdot \Delta\bigr)_{(Q,Q)} \quad \text{since } |\Gamma_{f,g}| \cap |\Delta| \text{ is finite}, \\ &= \sum_{\substack{Q \in \mathbb{P}^1(K) \text{ such that} \\ \exists P \in \mathbb{P}^1(K) \text{ with } f(P) = g(P) = Q}} \bigl((f \times g)_* \Delta \cdot \Delta\bigr)_{(Q,Q)} \\ &\geq \sum_{\substack{P \in \mathbb{P}^1(K) \\ f(P) = g(P)}} \min\{e_f(P), e_g(P)\} \quad \text{from (8)}, \\ &\geq 2d + 1 \quad \text{by assumption}. \end{aligned}$$

Thus the assumption that $|\Gamma_{f,g}| \cap |\Delta|$ is finite leads to a contradiction. It follows that $|\Delta|$ and $|\Gamma_{f,g}|$ have a common positive dimensional component. But as noted earlier, both $|\Delta|$ and $|\Gamma_{f,g}|$ are irreducible curves, and hence $|\Delta| = |\Gamma_{f,g}|$. Thus f and g take on the same value at every point of $\mathbb{P}^1(K)$, and therefore $f = g$, which completes the proof of Lemma 10. $\square$

We now have the tools needed to prove dynamical Shafarevich finiteness for $\mathbb{P}^1$.

Proof of Theorem 2(a). Our goal is to prove that

$$\widetilde{\mathcal{GR}}_d^1[n](K, S)/\operatorname{PGL}_2(R_S) \text{ is finite.}$$

Let $(f, Y, X) \in \widetilde{\mathcal{GR}}_d^1[n](K, S)$, and let $\ell = \#X$. We note that

$$2d + 1 \le n = \sum_{P \in Y} e_f(P) \le d \cdot \#Y \le d \cdot \#X = d\ell,$$

so $\ell \ge 3$. Further, the set X is $\operatorname{Gal}(\bar{K}/K)$-invariant and has good reduction outside of S. Lemma 7 tells us that up to $\mathrm{PGL}_2(R_S)$-equivalence, there are only finitely many possibilities for X. So without loss of generality, we may assume that $X = \{P_1, \dots, P_\ell\}$ is fixed.

The set Y is subset of X, so there are only finitely many choices for Y. Relabeling the points in X, we may thus also assume that $Y = \{P_1, \dots, P_m\}$ is fixed.

By definition, the map f satisfies $X = f(Y) \cup Y$, so in particular, $f(Y) \subset X$. Thus f induces a map

$$\nu_f : \{1, \dots, m\} \to \{1, \dots, \ell\} \quad \text{characterized by} \quad f(P_i) = P_{\nu_f(i)}.$$

There are only m^ℓ maps ν from the set $\{1, \dots, m\}$ to the set $\{1, \dots, \ell\}$, so again without loss of generality, we may fix one map ν and restrict attention to maps f satisfying $\nu_f = \nu$. This means that the value of f is specified at each of the points $P_1, \dots, P_m$ in Y.

We define the map

$$\widetilde{\mathcal{GR}}_d^1[n](K, S) \to \mathbb{Z}^m, \quad (f, X) \mapsto \bigl(e_f(P_1), \dots, e_f(P_m)\bigr).$$

Since $e_f(P)$ is an integer between 1 and d, there are only finitely many possibilities for the image. We may thus restrict attention to triples (f, Y, X) such that the ramification indices of f at the points in Y are fixed.

But now any two triples (f, Y, X) and (g, Y, X) have the same values and the same ramification indices at the points in Y, and by assumption the sum of those ramification indices is at least $2d + 1$, so Lemma 10 tells us that $f = g$. This completes the proof that $\widetilde{\mathcal{GR}}_d^1[n](K, S)$ contains only finitely many $\mathrm{PGL}_2(R_S)$-equivalence classes of triples (f, Y, X). $\square$

4. Dynamical Shafarevich finiteness fails on $\mathbb{P}^1$ for weight $\le 2d$

In this section we prove Theorem 2(b). More precisely, we prove that the dynamical Shafarevich finiteness is false for maps $f : \mathbb{P}^1 \to \mathbb{P}^1$ and f-invariant sets X containing $2d$ points. We do this by analyzing a particular family of maps.

Proposition 11. *Let $d \ge 2$, let $K/\mathbb{Q}$ be a number field, and let S be the set of primes of K dividing $(2d-2)!$. For each $a \in \bar{K}^*$, let $f_a(x)$ be the map*

$$f_a(x) = \frac{ax(x-1)(x-2)\cdots(x-d+1)}{(x+1)(x+2)\cdots(x+d-1)} \in \mathrm{End}_d^1,$$

and let $X \subset \mathbb{P}^1$ *be the set*

$$X = \{0, 1, 2, \dots, d-1\} \cup \{-1, -2, \dots, -(d-1)\} \cup \{\infty\}.$$

(a) *For all* $a \in R_S^*$, *we have*

$$(f_a, X, X) \in \mathcal{GR}_d^1[2d](K, S).$$

(b) *For a given* $a \in \bar{K}^*$, *there are only finitely many* $b \in \bar{K}^*$ *such that* f_b *is* $\mathrm{PGL}_2(\bar{K})$-*conjugate to* f_a.

(c) $\#\mathcal{GR}_d^1[2d](K, S)/\mathrm{PGL}_2(R_S) = \infty$.

Proof. (a) The resultant of f_a is

$$\mathrm{Res}(f_a) = a^d \prod_{i=0}^{d-1} \prod_{j=1}^{d-1} (i+j).$$

In particular, if $a \in R_S^*$, then our choice of S implies that $\mathrm{Res}(f_a) \in R_S^*$, so the map f_a has simple good reduction outside S. We also observe that our choice of S implies that the set X has good reduction outside S, and from the formula for f_a we see that $f_a(X) = \{0, \infty\} \subset X$. For example, the case $d = 4$ looks like

$$\begin{tikzcd} 1 \arrow[dr] & & -1 \arrow[dr] & \\ 2 \arrow[r] & 0 \arrow[loop right] & -2 \arrow[r] & \infty \arrow[loop right] \\ 3 \arrow[ur] & & -3 \arrow[ur] & \end{tikzcd} \qquad \text{with } S = \{2, 3, 5\}.$$

Since $\#X = 2d$, this completes the proof that $(f_a, X, X) \in \mathcal{GR}_d^1[2d](K, S)$.

(b) We consider the $\bar{K}$-valued points of the morphism

$$\bar{K}^* \to \mathcal{M}_d^1(\bar{K}) = \mathrm{End}_d^1(\bar{K})/\mathrm{PGL}_2(\bar{K}), \quad a \mapsto [f_a]. \tag{9}$$

We claim that the map (9) is nonconstant. To see this, we note that 0 is a fixed point of f_a, and that the multiplier of f_a at 0 is

$$\lambda(f_a, 0) := f_a'(0) = (-1)^{d-1} a.$$

But for any rational map $f \in \mathrm{End}_d^1$, the set of fixed point multipliers $\{\lambda(f, P) : P \in \mathrm{Fix}(f)\}$ is a PGL_2-conjugation invariant [Silverman 2007, Proposition 1.9]. So if (9) were constant, there would be a single map $g \in \mathrm{End}_d^1(\bar{K})$ with the property that for every $a \in \bar{K}^*$, the map f_a is $\mathrm{PGL}_2(\bar{K})$-conjugate to g. In particular, for every $a \in \bar{K}^*$, the multiplier $(-1)^{d-1}a = \lambda(f_a, 0)$ would be one of the finitely many fixed-point multipliers of g. This contradiction completes the proof of (b).

(c) It follows from (a) and (b) that $\{(f_a, X, X) : a \in R_S^*\}$ is contained in $\mathcal{GR}_d^1[2d](K, S)$ and that it contains infinitely many distinct $\mathrm{PGL}_2(R_S)$-conjugacy classes. $\square$

5. How large is the set of maps having simple good reduction?

As noted in the Introduction, it would be very interesting to know the behavior of the "Shafarevich discrepancy",

$$2d - 2 - \mathrm{ShafDim}_d^N[\mathcal{P}] \quad \text{as } d \to \infty,$$

even for the case $\mathcal{P} = \varnothing$. It has long been noted that monic polynomial maps on $\mathbb{P}^1$ have everywhere simple good reduction. This gives a set of such maps in $\mathcal{M}_d^1$ whose Zariski closure has dimension $d-1$. With a little work, we can increase this dimension by 1 for $d = 2$ and by 2 for $d \geq 3$.

Proposition 12. *We have*

$$\mathrm{ShafDim}_2^1[\varnothing] = \dim \mathcal{M}_2^1 = 2,$$

and for all $d \geq 3$ we have

$$\mathrm{ShafDim}_d^1[\varnothing] \geq d + 1.$$

Proof. We fix a number field K and a set of places S so that R_S^* is infinite. For $\boldsymbol{a} = (a_0, a_2, \ldots, a_{d-1}, a_d)$ we define a rational map

$$f_{\boldsymbol{a}}(x) := \frac{a_0 x^d + a_1 x^{d-1} + \cdots + a_{d-2} x^2 + a_{d-1} x + a_d}{x(x-1)}.$$

We have

$$\mathrm{Res}(f_{\boldsymbol{a}}) = a_0^{d-2} a_d (a_0 + a_1 + \cdots + a_{d-1} + a_d).$$

Hence $f_{\boldsymbol{a}}$ will have simple good reduction if we take $a_0, a_d \in R_S^*$, $a_2, \ldots, a_{d-1} \in R_S$, and set $a_1 = w - a_0 - a_2 - \cdots - a_d$ for some $w \in R_S^*$. In other words, the image of the map

$$\begin{aligned} (R_S^*)^3 \times R_S^{d-2} &\to \mathbb{A}^{d+1}(K), \\ \bigl((u, v, w), (a_2, \ldots, a_{d-1})\bigr) &\mapsto (u, w - u - a_2 - \cdots - a_{d-1} - v, a_2, \ldots, a_{d-1}, v), \end{aligned}$$

gives values of $\boldsymbol{a}$ for which $f_{\boldsymbol{a}}$ has simple good reduction. The image of this map is Zariski dense in $\mathbb{A}^{d+1}$, so it remains to show that the map $\mathbb{A}^{d+1} \to \mathcal{M}_d^1$ given by $\boldsymbol{a} \mapsto \langle f_{\boldsymbol{a}} \rangle$ is generically finite-to-one.

Suppose that $\varphi \in \mathrm{PGL}_2(\bar{K})$ has the property that $f_{\boldsymbol{a}}^\varphi = f_{\boldsymbol{b}}$. We start with the case $d \geq 4$. Then $f_{\boldsymbol{a}}$ is ramified at the fixed point ∞, since $e_{f_{\boldsymbol{a}}}(\infty) = d - 2$, and similarly for $f_{\boldsymbol{b}}$. Generically, ∞ will be the only ramified fixed point of $f_{\boldsymbol{a}}$ and $f_{\boldsymbol{b}}$, so $\varphi(\infty) = \infty$. Next we use the fact that

$$f_{\boldsymbol{a}}^{-1}(\infty) = f_{\boldsymbol{b}}^{-1}(\infty) = \{\infty, 1, 0\}$$

to conclude that $\varphi(\{0,1\}) = \{0,1\}$. Thus φ fixes ∞ and either fixes or swaps 0 and 1, so the only possibilities are $\varphi(x) = x$ or $\varphi(x) = 1 - x$. Thus $f_{\boldsymbol{a}}$ is PGL_2-conjugate to only one other map of the same form. This concludes the proof for $d \geq 4$. For $d = 3$, the point ∞ is fixed by $f_{\boldsymbol{a}}$ and $f_{\boldsymbol{b}}$, but ∞ is not a critical point, so we cannot conclude that φ fixes ∞. However, we can argue as follows. A generic map of the form $f_{\boldsymbol{a}}$ has 3 fixed points, say $\{\infty, \gamma_1, \gamma_2\}$, and each fixed point has 3 points in its inverse image, one of which is itself, say

$$f_{\boldsymbol{a}}^{-1}(\infty) = \{\infty, 0, 1\}, \quad f_{\boldsymbol{a}}^{-1}(\gamma_1) = \{\gamma_1, \alpha_1, \beta_1\}, \quad f_{\boldsymbol{a}}^{-1}(\gamma_2) = \{\gamma_2, \alpha_2, \beta_2\}.$$

It follows that $\varphi(\infty) \in \{\infty, \gamma_1, \gamma_2\}$, and that

$$\varphi(\{0,1\}) = \begin{cases} \{0,1\} & \text{if } \varphi(\infty) = \infty, \\ \{\alpha_1, \beta_1\} & \text{if } \varphi(\infty) = \gamma_1, \\ \{\alpha_2, \beta_2\} & \text{if } \varphi(\infty) = \gamma_2. \end{cases}$$

Since φ is determined by its values at on $\{0, 1, \infty\}$, we see that there are (at most) 6 maps φ for which $f_{\boldsymbol{a}}^{\varphi}$.

Finally, for $d = 2$, we first note that the above proof fails because ∞ is no longer a fixed point. And it is good that the proof fails, since otherwise we would conclude that $\mathrm{ShafDim}_2^1[\varnothing] \geq 3$, which would contradict $\dim \mathcal{M}_2^1 = 2$. So for $d = 2$ we instead use the family of maps

$$g_{a,b}(x) := \frac{ax^2 + x + b}{x}.$$

These satisfy $\mathrm{Res}(g_{a,b}) = ab$, so they have good reduction for all $a, b \in R_S^*$. We could argue as above that there are only finitely many φ preserving this form, and thus the image in $\mathcal{M}_2^1$ is 2-dimensional. But to illustrate an alternative method of proof, we instead use the Milnor isomorphism $s : \mathcal{M}_2^1 \xrightarrow{\sim} \mathbb{A}^2$; see [Silverman 2007, Theorem 4.5.6]. The map $g_{a,b}$ has Milnor coordinates

$$s(g_{a,b}) = \left(\frac{4a^2b - 2ab - a + b}{ab}, \frac{4a^3b - 4a^2b - a^2 + 5ab - 2b - 1}{ab} \right).$$

We used Magma [Bosma et al. 1997] to verify that these two rational functions are algebraically independent in $K(a,b)$. Hence under our assumption that $\#R_S^* = \infty$, we see that $\{s(a,b) : a, b \in R_S^*\}$ is Zariski dense in $\mathbb{A}^2$. $\square$

6. Abstract portraits and models for portraits

In this section we briefly construct a category of portraits and use it to describe dynamical systems that model a given portrait. See [Doyle and Silverman $\geq$ 2018] for further development and the construction of parameter and moduli spaces for dynamical systems with portraits.

Definition. An (*abstract*) *weighted portrait* is a 4-tuple $\mathcal{P} = (\mathcal{W}, \mathcal{V}, \Phi, \epsilon)$, where

- $\mathcal{W} \subseteq \mathcal{V}$ are finite sets (of vertices),
- $\Phi : \mathcal{W} \to \mathcal{V}$ is a map (which specifies directed edges),
- $\mathcal{V} = \mathcal{W} \cup \Phi(\mathcal{W})$,
- $\epsilon : \mathcal{W} \to \mathbb{N}$ is a map (assigning weights to vertices).

The *weight of* $\mathcal{P}$ is the total weight

$$\mathrm{wt}(\mathcal{P}) := \sum_{w \in \mathcal{W}} \epsilon(w).$$

We say that the portrait is *unweighted* if $\epsilon(w) = 1$ for every $w \in \mathcal{W}$, or equivalently if $\mathrm{wt}(\mathcal{P}) = \#\mathcal{W}$, in which case we sometimes write $\mathcal{P} = (\mathcal{W}, \mathcal{V}, \Phi)$. We say that the portrait is *preperiodic* if $\mathcal{W} = \mathcal{V}$.

We now explain how a self-map of $\mathbb{P}^1$ can be used to model a portrait.

Definition. Let $\mathcal{P} = (\mathcal{W}, \mathcal{V}, \Phi, \epsilon)$ be a portrait. A *model for* $\mathcal{P}$ is a triple (f, Y, X) consisting of a morphism $f : \mathbb{P}^1 \to \mathbb{P}^1$ and subsets $Y \subset X \subset \mathbb{P}^1$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{W} & \xrightarrow{\ i\ } & \mathbb{P}^1 \\ {\scriptstyle\Phi}\big\downarrow & & \big\downarrow{\scriptstyle f} \\ \mathcal{V} & \xrightarrow{\ i\ } & \mathbb{P}^1 \end{array} \tag{10}$$

We say that (f, Y, X) is a $\bullet$-*model* if in addition

$$e_f(i(w)) \ge \epsilon(w) \quad \text{for all } w \in \mathcal{W};$$

and similarly we say that (f, Y, X) is a $\circ$-*model* if

$$e_f(i(w)) = \epsilon(w) \quad \text{for all } w \in \mathcal{W}.$$

With this formalism, we can now define our three Shafarevich-type sets.

Definition. Let $\mathcal{P} = (\mathcal{W}, \mathcal{V}, \Phi, \epsilon)$ be a portrait and let $n = \mathrm{wt}(\mathcal{P})$. Then

$$\mathcal{GR}_d^1[\mathcal{P}]^\bullet(K, S) = \{(f, Y, X) \in \mathcal{GR}_d^1[n](K, S) : (f, Y, X) \text{ is a } \bullet\text{-model for } \mathcal{P}\},$$

$$\mathcal{GR}_d^1[\mathcal{P}]^\circ(K, S) = \{(f, Y, X) \in \mathcal{GR}_d^1[n](K, S) : (f, Y, X) \text{ is a } \circ\text{-model for } \mathcal{P}\},$$

$$\begin{aligned}\mathcal{GR}_d^1[\mathcal{P}]^\star(K, S) = \{(f, Y, X) \in \mathcal{GR}_d^1[n](K, S) : e_{\tilde{f}_\mathfrak{p}}(\widetilde{i(w) \bmod \mathfrak{p}}) = \epsilon(w) \\ \text{for all } w \in \mathcal{W} \text{ and all } \mathfrak{p} \notin S\}.\end{aligned}$$

It may happen that a portrait has no models using maps of a given degree. For example, if the portrait $\mathcal{P}$ contains 4 fixed points, then it cannot be modeled by a map of degree 2, and similarly if $\mathcal{P}$ contains a pair of 2-cycles. In order to describe more generally the constraints on a model, we set an ad hoc piece of notation. (A better definition of $\mathcal{M}_d^1[\mathcal{P}]^\bullet$ as a $\mathbb{Z}$-scheme is given in [Doyle and Silverman $\geq$ 2018].)

Definition. Let $\mathcal{P}$ be a portrait and let $d \geq 2$. We define

$$\mathcal{M}_d^1[\mathcal{P}]^\bullet := \{f \in \mathcal{M}_d^1(\bar{K}) : \text{there exist sets } Y \subseteq X \subseteq \mathbb{P}^1(\bar{K}) \\ \text{such that } (f, Y, X) \text{ is a } \bullet\text{-model for } \mathcal{P}\}.$$

Proposition 13. *Let $d \geq 2$, and let $\mathcal{P} = (\mathcal{W}, \mathcal{V}, \Phi, \epsilon)$ be a portrait such that $\mathcal{M}_d^1[\mathcal{P}] \neq \varnothing$. Then $\mathcal{P}$ satisfies the following conditions*:

$$\text{(I)} \quad \sup_{v \in \mathcal{V}} \sum_{w \in \Phi^{-1}(v)} \epsilon(w) \leq d, \qquad \text{(II)} \quad \sum_{w \in \mathcal{W}} \bigl(\epsilon(w) - 1\bigr) \leq 2d - 2.$$

For all $n \geq 1$,

$$(\mathrm{III}_n) \quad \#\{w \in \mathcal{W} : \Phi^n(w) = w \text{ and } \Phi^m(w) \neq w \text{ for all } m < n\} \leq \sum_{m \mid n} \mu\left(\frac{n}{m}\right)(d^m + 1).$$

(*Here μ is the Möbius function.*)

Proof. Constraint I comes from the fact that f is a map of degree d, constraint II follows from the Riemann–Hurwitz formula $\sum\bigl(e_f(P) - 1\bigr) = 2d - 2$ [Silverman 2007, Theorem 1.1], and constraint III_n from the fact that a degree d map on $\mathbb{P}^1$ has at most the indicated number of points of exact period n [Silverman 2007, Remark 43]. □

If we fix a preperiodic portrait $\mathcal{P}$ and allow the degree d to grow, then we expect that $\mathcal{M}_d^1[\mathcal{P}]^\bullet$ has exactly the expected dimension, as in the following conjecture. This is in marked contrast to our uncertainty regarding the size of $\mathrm{ShafDim}_d^1[\mathcal{P}]^\bullet$ as $d \to \infty$; cf. Question 4.

Conjecture 14. *Let $\mathcal{P} = (\mathcal{W}, \mathcal{V}, \Phi, \epsilon)$ be a preperiodic portrait. There is a constant $d_0(\mathcal{P})$ such that for all $d \geq d_0(\mathcal{P})$ we have*

$$\begin{aligned} \dim \overline{\mathcal{M}_d^1[\mathcal{P}]^\bullet} &= \dim \mathcal{M}_d^1 - \sum_{w \in \mathcal{W}} \bigl(\epsilon(w) - 1\bigr) \\ &= 2d - 2 - \mathrm{wt}(\mathcal{P}) + \#\mathcal{W}. \end{aligned}$$

Remark 15. The local conditions used to define $\mathcal{GR}_d^1[\mathcal{P}]^\star(K, S)$ reflect the viewpoint adopted by Petsche and Stout [2015]. We note that since f and $i(\mathcal{V})$ are assumed to have good reduction outside S, there is a well-defined map $\tilde{f}_{\mathfrak{p}} : \mathbb{P}^1 \to \mathbb{P}^1$ defined over the residue field of $\mathfrak{p}$, and so it makes sense to look at the ramification indices of $\tilde{f}_{\mathfrak{p}}$ at the $\mathfrak{p}$-reductions of the points in $i(\mathcal{W})$.

Remark 16. Since the primary goal of this paper is the study of Shafarevich-type finiteness theorems, we have been content to define our sets of good reduction purely as sets. In a subsequent paper [Doyle and Silverman $\ge$ 2018] we will take up the more refined question of constructing moduli spaces for dynamical systems with portraits, after which the results of the present paper can be reinterpreted as characterizing the S-integral points on these spaces, with the caveat that there may be field-of-moduli versus field-of-definition issues.

Since our goal is to understand the size of the various sets of good reduction triples (f, Y, X), we are prompted to make the following definitions.

Definition. Let $x \in \{\bullet, \circ, \star\}$. The associated *Shafarevich dimension* is the quantity

$$\operatorname{ShafDim}_d^1[\mathcal{P}]^x = \sup_{\substack{K \text{ a number field} \\ S \text{ a finite set of places}}} \dim \overline{\operatorname{Image}\bigl(\mathcal{GR}_d^1[\mathcal{P}]^x(K,S) \to \mathcal{M}_d^1\bigr)}.$$

We record some elementary properties for future reference.

Proposition 17. *Let $d \ge 2$, and let $\mathcal{P} = (\mathcal{W}, \mathcal{V}, \Phi, \epsilon)$ be a portrait.*

(a) *Let $\epsilon' : \mathcal{V} \to \mathbb{N}$ be a weight function satisfying $\epsilon' \ge \epsilon$, let $\mathcal{P}' = (\mathcal{W}, \mathcal{V}, \Phi, \epsilon')$, and let $x \in \{\bullet, \circ, \star\}$. Then*

$$\mathcal{GR}_d^1[\mathcal{P}']^x(K,S) \subseteq \mathcal{GR}_d^1[\mathcal{P}]^x(K,S).$$

(b) *We have*

$$\mathcal{GR}_d^1[\mathcal{P}]^\star(K,S) \subseteq \mathcal{GR}_d^1[\mathcal{P}]^\circ(K,S) \subseteq \mathcal{GR}_d^1[\mathcal{P}]^\bullet(K,S).$$

(c) *We have*

$$\operatorname{ShafDim}_d^1[\mathcal{P}]^\star \le \operatorname{ShafDim}_d^1[\mathcal{P}]^\circ \le \operatorname{ShafDim}_d^1[\mathcal{P}]^\bullet \le \dim \mathcal{M}_d^1 = 2d-2.$$

Proof. (a) and (b) are clear from the definitions of the various sets of good reduction, and (c) follows (b) and the definition of Shafarevich dimension. We note that if a map f has good reduction at $\mathfrak{p}$, then its ramification index can only increase when f is reduced modulo $\mathfrak{p}$. $\square$

Example 18. Consider the following two preperiodic portraits:

$$\mathcal{P}_1 \quad \begin{tikzcd} \bullet \arrow[r] & \bullet \arrow[dl] \\ \bullet \arrow[u] & \end{tikzcd} \qquad\qquad \mathcal{P}_2 \quad \begin{tikzcd} \bullet \arrow[r] & \bullet \arrow[dl] \\ \bullet \arrow[u, "2"] & \end{tikzcd}$$

We note that the portrait $\mathcal{P}_2$ is strictly larger than the portrait $\mathcal{P}_1$ in the sense of Proposition 17(a), so that result tells us that $\mathcal{GR}_d^1[\mathcal{P}_2]^\circ(K,S) \subseteq \mathcal{GR}_d^1[\mathcal{P}_1]^\circ(K,S)$. However, we will see in Section 7 that if $\#R_S^* = \infty$, then

$$\#\,\mathcal{GR}_2^1[\mathcal{P}_1]^\circ(K,S) < \infty \quad \text{and} \quad \#\,\mathcal{GR}_2^1[\mathcal{P}_2]^\circ(K,S) = \infty.$$

In words, there are only finitely many degree 2 rational maps with good reduction outside S that have an *unramified* good reduction 3-cycle, but if we allow one of the points in the 3-cycle to be ramified, then there are infinitely many such maps. In terms of Shafarevich dimensions, we have $\operatorname{ShafDim}_d^1[\mathcal{P}_1]^\circ = 0$ and $\operatorname{ShafDim}_d^1[\mathcal{P}_2]^\circ = 1$. On the other hand, we will show that with the more restrictive Petsche–Stout good reduction criterion, we have $\operatorname{ShafDim}_d^1[\mathcal{P}_1]^\star = \operatorname{ShafDim}_d^1[\mathcal{P}_2]^\star = 0$. Another example of this phenomenon, where more ramification leads to more maps of good reduction, is given by portraits $\mathcal{P}_{3,3}$ and $\mathcal{P}_{4,7}$ in Tables 2 and 3, respectively.

7. Good reduction for preperiodic portraits of weight ≤ 4 for degree 2 maps of $\mathbb{P}^1$

We know from Theorem 2 with $N = 1$ and $d = 2$ that if a portrait $\mathcal{P}$ satisfies $\operatorname{wt}(\mathcal{P}) \geq 5$, then $\operatorname{ShafDim}_2^1[\mathcal{P}]^\bullet = 0$. In other words, dynamical Shafarevich finiteness holds for degree 2 maps $f : \mathbb{P}^1 \to \mathbb{P}^1$ that model a portrait $\mathcal{P}$ of weight at least 5. In this section we give a complete analysis of preperiodic portraits of weights 1 to 4. For example, it turns out that there are 22 such portraits of weight 4, and dynamical Shafarevich finiteness holds for some of them, but not for others. For notational convenience, we label portraits as $\mathcal{P}_{w,m}$, where w is the weight and $m \in \{1, 2, 3, \dots\}$.

Theorem 19. *We consider moduli spaces of degree* 2 *maps* $\mathbb{P}^1 \to \mathbb{P}^1$ *with weighted preperiodic portraits.*

(a) *There is* 1 *portrait* $\mathcal{P}$ *of weight* 1 *such that* $\mathcal{M}_2^1$ *contains a map that can be used to model* $\mathcal{P}$.

(b) *There are* 4 *portraits* $\mathcal{P}$ *of weight* 2 *such that* $\mathcal{M}_2^1$ *contains a map that can be used to model* $\mathcal{P}$.

(c) *There are* 8 *portraits* $\mathcal{P}$ *of weight* 3 *such that* $\mathcal{M}_2^1$ *contains a map that can be used to model* $\mathcal{P}$.

(d) *There are* 22 *portraits* $\mathcal{P}$ *of weight* 4 *such that* $\mathcal{M}_2^1$ *contains a map that can be used to model* $\mathcal{P}$.

These portraits are as catalogued in Tables 2, 3 *and* 4, *which also give the values of the following quantities*:

$$\mathcal{MD} := \dim \overline{\mathcal{M}_2^1[\mathcal{P}]^\bullet}, \qquad \mathcal{SD}^\bullet := \operatorname{ShafDim}_2^1[\mathcal{P}]^\bullet,$$
$$\mathcal{SD}^\circ := \operatorname{ShafDim}_2^1[\mathcal{P}]^\circ, \quad \mathcal{SD}^\star := \operatorname{ShafDim}_2^1[\mathcal{P}]^\star.$$

Proof. Since we will be dealing entirely with preperiodic portraits, we write the triple (f, X, X) as a pair (f, X). For degree 2 maps, we see that $\mathcal{M}_2^1[\mathcal{P}]^\bullet = \varnothing$ unless the following four conditions are true; cf. Proposition 13.

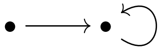
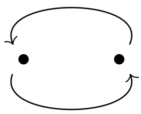
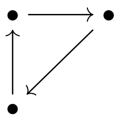
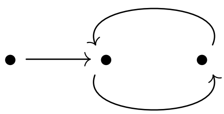
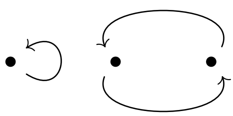
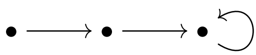
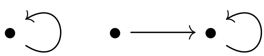
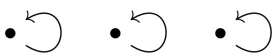
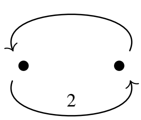
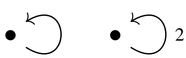
#	$\mathcal{P}$	wt($\mathcal{P}$)	$\mathcal{MD}$	$\mathcal{SD}^\bullet$	$\mathcal{SD}^\circ$	$\mathcal{SD}^\star$
$\mathcal{P}_{1,1}$		1	2	2	2	2
$\mathcal{P}_{2,1}$		2	1	1	1	1
$\mathcal{P}_{2,2}$		2	2	2	2	2
$\mathcal{P}_{2,3}$		2	2	2	2	1
$\mathcal{P}_{2,4}$		2	2	2	2	1
$\mathcal{P}_{3,1}$		3	2	1	0	0
$\mathcal{P}_{3,2}$		3	2	2	2	1
$\mathcal{P}_{3,3}$		3	2	1	0	0
$\mathcal{P}_{3,4}$		3	2	2	2	1
$\mathcal{P}_{3,5}$		3	2	2	2	1
$\mathcal{P}_{3,6}$		3	2	1	0	0
$\mathcal{P}_{3,7}$		3	1	1	1	1
$\mathcal{P}_{3,8}$		3	1	1	1	1

Table 2. Weight 1, 2, and 3 preperiodic portraits for degree 2 maps.

(I) Each point has at most weight 2 worth of incoming arrows.

(II) There are at most 2 critical points.

(III_1) There are at most 3 fixed points.

(III_2) There is at most one periodic cycle of length 2.

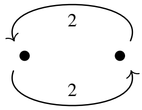
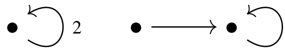
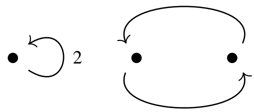
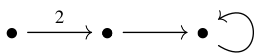
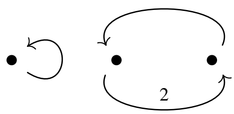
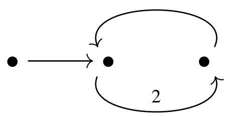
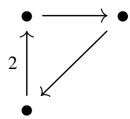
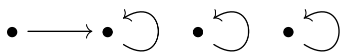
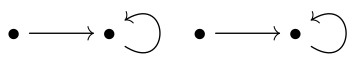
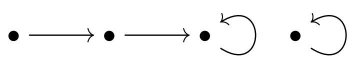
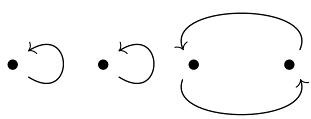
#	$\mathcal{P}$	$\mathrm{wt}(\mathcal{P})$	$\mathcal{MD}$	$\mathcal{SD}^\bullet$	$\mathcal{SD}^\circ$	$\mathcal{SD}^\star$
$\mathcal{P}_{4,1}$		4	0	0	0	0
$\mathcal{P}_{4,2}$		4	0	0	0	0
$\mathcal{P}_{4,3}$		4	1	1	1	0
$\mathcal{P}_{4,4}$		4	1	1	1	1
$\mathcal{P}_{4,5}$		4	1	1	1	0
$\mathcal{P}_{4,6}$		4	1	1	1	1
$\mathcal{P}_{4,7}$		4	1	1	1	0
$\mathcal{P}_{4,8}$		4	1	1	1	1
$\mathcal{P}_{4,9}$		4	1	1	1	0
$\mathcal{P}_{4,10}$		4	2	0	0	0
$\mathcal{P}_{4,11}$		4	2	1	1	1
$\mathcal{P}_{4,12}$		4	2	0	0	0
$\mathcal{P}_{4,13}$		4	2	0	0	0

Table 3. Weight 4 preperiodic portraits for degree 2 maps (part 1).

Sublemma 8 says that in order to prove that $\mathcal{GR}_2^1[\mathcal{P}]^\circ(K, S)/\operatorname{PGL}_2(R_S)$ is finite for all K and S, it suffices to prove finiteness after extending K and enlarging S. And the definition of $\operatorname{ShafDim}_d^1[\mathcal{P}]^\bullet$ and its variants is a supremum over all K and all S. So we may assume throughout our discussion that in every model (f, X)

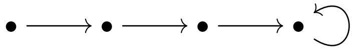
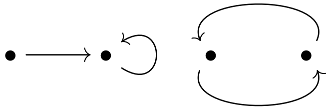
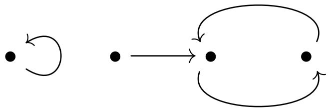
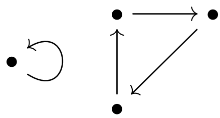
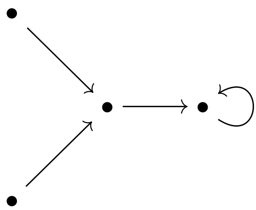
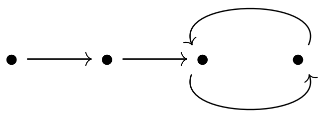
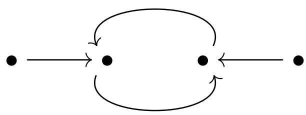
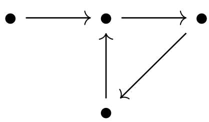
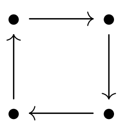
#	$\mathcal{P}$	wt($\mathcal{P}$)	$\mathcal{MD}$	$\mathcal{SD}^{\bullet}$	$\mathcal{SD}^{\circ}$	$\mathcal{SD}^{\star}$
$\mathcal{P}_{4,14}$		4	2	0	0	0
$\mathcal{P}_{4,15}$		4	2	0	0	0
$\mathcal{P}_{4,16}$		4	2	0	0	0
$\mathcal{P}_{4,17}$		4	2	0	0	0
$\mathcal{P}_{4,18}$		4	2	1	1	1
$\mathcal{P}_{4,19}$		4	2	0	0	0
$\mathcal{P}_{4,20}$		4	2	1	1	1
$\mathcal{P}_{4,21}$		4	2	0	0	0
$\mathcal{P}_{4,22}$		4	2	0	0	0

Table 4. Weight 4 preperiodic portraits for degree 2 maps (part 2).

for $\mathcal{P}$, the points in X are in $\mathbb{P}^1(K)$, and further that S is chosen so that

$$R_S \text{ is a PID;} \quad R_S^* \text{ is infinite;} \quad 2, 3 \in R_S^*.$$

Using the assumptions that the points in our portraits are in $\mathbb{P}^1(K)$ and that R_S is a PID, Sublemma 9 and the Chinese remainder theorem tell us that we can find an element of $\mathrm{PGL}_2(R_S)$ to move three of the points in X to the points 0, 1, and ∞. (Or just to 0 and ∞ if $\#X = 2$.)

As in the proof of Proposition 12, we will frequently use the Milnor isomorphism [Silverman 2007, Theorem 4.5.6]

$$s = (s_1, s_2) : \mathcal{M}_2^1 \xrightarrow{\sim} \mathbb{A}^2,$$

which we implemented in PARI [2016], to help distinguish the $\mathrm{PGL}_2(\bar{K})$-conjugacy classes of our maps, and we often use Magma [Bosma et al. 1997] to verify that the images of certain maps are Zariski dense in $\mathcal{M}_2^1$.

$\mathcal{P}_{\mathbf{1,1}}$: This case was done by Petsche and Stout [2015, Remark 3], but for completeness, we include a proof. Let $f(x) = (x^2 + ax)/(bx + 1)$ with $\mathrm{Res}(f) = 1 - ab$, so $(f, \{0\}) \in \mathcal{GR}_2^1[\mathcal{P}_{1,1}]^\bullet(K, S)$ for all $a, b \in R_S$ satisfying $1 - ab \in R_S^*$. Further, $f'(0) = a$, so if we take $a \in R_S^*$, then 0 is not critical modulo v for all $v \notin S$. This suggests that we change variables via $b = (1 - u)a^{-1}$. Then $f(x) = (ax^2 + a^2x)/((1 - u)x + a)$ with $\mathrm{Res}(f) = a^4u$ and $f'(0) = a$, so $(f, \{0\}) \in \mathcal{GR}_2^1[\mathcal{P}_{1,1}]^\star(K, S)$ for all $a, u \in R_S^*$. The Milnor image of this map in $\mathcal{M}_2 \cong \mathbb{A}^2$ is

$$s\left(\frac{ax^2+a^2x}{(1-u)x+a}\right) = \left(\frac{a^2(u-1)+2a-(u-1)^2}{au},\right.$$
$$\left.\frac{-a^4+2a^3-a^2(u-1)(u-2)-2a(u-1)-(u-1)^2}{a^2u}\right).$$

We used Magma to verify that the two rational functions $s_1(a, u)$ and $s_2(a, u)$ are algebraically independent in $K(a, u)$. Hence under our assumption that $\#R_S^* = \infty$, we see that $\{s(a, u) : a, u \in R_S^*\}$ is Zariski dense in $\mathbb{A}^2$. This completes the proof that $\mathrm{ShafDim}_2^1[\mathcal{P}_{1,1}]^\star = 2$, and the other Shafarevich dimensions are also 2 by the standard inequalities in Proposition 17(e).

$\mathcal{P}_{\mathbf{2,1}}$: Moving the totally ramified fixed point to ∞, the map f has the form $f(x) = ax^2 + bx + c$. It has good reduction if and only if $a \in R_S^*$. Then we can conjugate by a map of the form $x \mapsto a^{-1}x + e$ to put $f(x)$ in the form $f(x) = x^2 + c$. Since the ramification at ∞ can't increase when we reduce modulo primes not in S, we see that

$$(x^2 = c, \{\infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{2,1}]^\star(K, S) \quad \text{for all } c \in R_S^*.$$

The closure of the image in $\mathcal{M}_2^1$ is the line $s_1 = 2$ of polynomials.

$\mathcal{P}_{\mathbf{2,2}}$: Move the two points to $0, \infty$; then f has the form $f(x) = (ax^2 + bx + c)/dx$. This map has $\mathrm{Res}(f) = acd^2$, so we can dehomogenize $d = 1$. Thus $f(x) = ax + b + cx^{-1}$ with $ac \in R_S$. Conjugating by $x \to ux$ gives $u^{-1}f(ux) = ax + bu^{-1} + cu^{-2}x^{-1}$, so going to $K(\sqrt{c})$, which is unramified over S, we may assume that $c = 1$

and $f(x) = (ax^2 + bx + 1)/x$. We also observe that $f^{-1}(f(\infty)) = \{0, \infty\}$ and in $f^{-1}(f(0)) = \{0, \infty\}$, so 0 and ∞ are unramified modulo all primes. (Alternatively, one could compute derivatives, after moving ∞ to a more amenable point.) Hence

$$(f, \{0, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{2,2}]^\star(K, S) \quad \text{for all } a \in R_S^* \text{ and } b \in R_S.$$

The Milnor image is

$$s\left(\frac{ax^2+bx+1}{x}\right) = \left(\frac{4a^2-ab^2-2a+1}{a}, \frac{4a^3-a^2b^2-4a^2+5a-b^2-2}{a}\right).$$

We used Magma to verify that the rational functions $s_1(a, u)$ and $s_2(a, u)$ are algebraically independent in $K(a, u)$. Hence under our assumption that $\#R_S^* = \infty$, we see that $\{s(a, u) : a, u \in R_S^*\}$ is Zariski dense in $\mathbb{A}^2$. This completes the proof that $\operatorname{ShafDim}_2^1[\mathcal{P}_{2,2}]^\star = 2$, and the other Shafarevich dimensions are also 2 by the standard inequalities in Proposition 17(e).

$\boldsymbol{\mathcal{P}_{2,3}}$: Moving the two fixed points to 0 and ∞, the map f has the form $f(x) = (ax^2+bx)/(cx+d)$. The resultant is $\operatorname{Res}(f) = ad(ad-bc)$. Good reduction implies in particular that $a, d \in R_S^*$, so we can dehomogenize $d = 1$ and replace f with $af(a^{-1}x) = (x^2+bx)/(a^{-1}cx+1)$. We can also replace $a^{-1}c$ with c, so $f(x) = (x^2+bx)/(cx+1)$ with $\operatorname{Res}(f) = 1-bc$. Hence

$$(f, \{0, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{2,3}]^\circ(K, S) \quad \text{for all } b, c \in R_S \text{ satisfying } 1-bc \in R_S^*.$$

We note that this set of (b, c) is Zariski dense in $\mathbb{A}^2$, under our assumption that $\#R_S^* = \infty$. For example, if $u \in R_S^*$ has infinite order, then for every $n \geq 1$ we can take $b = 1-u$ and $c = 1+u+u^2+\cdots+u^n$, and this set of points is Zariski dense. The Milnor image is

$$s\left(\frac{x^2+bx}{cx+1}\right) = \left(\frac{-b^2c-bc^2+2}{1-bc}, \frac{-b^2c^2-b^2-bc+2b-c^2+2c}{1-bc}\right).$$

We used Magma to verify that the rational functions $s_1(a, u)$ and $s_2(a, u)$ are algebraically independent in $K(a, u)$. Hence under our assumption that $\#R_S^* = \infty$, we see that $\{s(a, u) : a, u \in R_S^*\}$ is Zariski dense in $\mathbb{A}^2$. This completes the proof that $\operatorname{ShafDim}_2^1[\mathcal{P}_{2,3}]^\circ = 2$.

However, the set $\mathcal{GR}_2^1[\mathcal{P}_{2,3}]^\star(K, S)$ is more restrictive, since we need the fixed points to be unramified for all primes not in S. Thus $(f, \{0, \infty\})$ is in this set if and only if $f'(0) = b \in R_S^*$ and $f'(\infty) = c \in R_S^*$. We thus need $b, c, 1-bc$ to be S-units. Then $(bc, 1-bc)$ is a solution to the S-unit equation $u+v = 1$, so there are only finitely many possible values for bc. On the other hand, any fixed solution (u, v) gives a map $f(x) = (x^2+bx)/(b^{-1}ux+1)$ satisfying

$$(f, \{0, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{2,3}]^\star(K, S) \quad \text{for all } b \in R_S^*.$$

Each (u, v) value gives points lying on a curve in $\mathcal{M}_2^1$. And there is at least one such curve, since our assumption that $2 \in S$ says that we can take $(u, v) = (-1, 2)$, leading to the Milnor image

$$s\left(\frac{x^2+bx}{-b^{-1}x+1}\right) = \left(\frac{b^2+2b-1}{2b}, \frac{-b^4+2b^3-2b-1}{2b^2}\right).$$

Hence $\operatorname{ShafDim}[\mathcal{P}_{2,3}]^\star = 1$, a result that was first proven by Petsche and Stout [2015, Section 4].

$\boldsymbol{\mathcal{P}_{2,4}}$: We move the two points to 0 and ∞, so $f(x) = (ax+b)/(cx^2+dx)$ with $\operatorname{Res}(f) = bc(ad-bc)$. Good reduction implies in particular that $b, c \in R_S^*$, so we can dehomogenize $b = 1$. Conjugating f gives $u^{-1}f(ux) = (aux+1)/(cu^3x^2+du^2x)$. Going to the field $K(\sqrt[3]{c})$, which is unramified outside S, we can take $u = c^{-1/3}$ and adjust a and d accordingly to put f in the form $f(x) = (ax+1)/(x^2+dx)$. Then

$$(f, \{0, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{2,4}]^\circ(K, S) \quad \text{for all } a, d \in R_S \text{ with } 1-ad \in R_S^*.$$

The map f is unramified at 0 if and only if $d \neq 0$ and f is unramified at ∞ if and only if $a \neq 0$. The Milnor image is

$$s\left(\frac{ax+1}{x^2+dx}\right) = \left(\frac{a^3+4ad+d^3-6}{1-ad}, \frac{-2a^3-a^2d^2-7ad-2d^3+12}{1-ad}\right).$$

We used Magma to verify that the rational functions $s_1(a, u)$ and $s_2(a, u)$ are algebraically independent in $K(a, u)$. Hence under our assumption that $\#R_S^* = \infty$, we see that $\{s(a, u) : a, u \in R_S^*\}$ is Zariski dense in $\mathbb{A}^2$. This completes the proof that $\operatorname{ShafDim}_2^1[\mathcal{P}_{2,4}]^\circ = 2$.

The multiplier of the 2-cycle is $(f^2)'(0) = ad$, so the points 0 and ∞ are unramified modulo all primes not in S if and only if $a, d \in R_S^*$. So in this case $(ad, 1-ad)$ is a solution to the S-unit equation $u+v = 1$, and each of the finitely many such solutions yields a family of maps $f(x) = (ax+1)/(x^2+ua^{-1}x)$ with

$$(f, \{0, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{2,4}]^\star(K, S) \quad \text{for all } a \in R_S^*.$$

The Zariski closure of these points form a nonempty finite collection of curves, since for example $(u, v) = (-1, 2)$ gives

$$s\left(\frac{ax+1}{x^2-a^{-1}x}\right) = \left(\frac{a^6-10a^3-1}{2a^3}, \frac{-a^6+9a^3+1}{a^3}\right).$$

Hence $\operatorname{ShafDim}[\mathcal{P}_{2,4}]^\star = 1$, a result that was first proven by Petsche and Stout [2015, Section 5].

$\boldsymbol{\mathcal{P}_{3,1}}$: We first note that almost all rational maps of degree 2 have a 3-cycle [Beardon 1991, Section 6.8]. Hence the image of $\mathcal{M}_2^1[\mathcal{P}_{3,1}]^\bullet$ omits only finitely many points, and thus $\dim \overline{\mathcal{M}_2^1[\mathcal{P}_{3,1}]^\bullet} = 2$. We next move the 3-cycle to 0, 1, ∞, so f has the form $f(x) = (ax^2 - (a+c)x + c)/(ax^2 + ex)$ with $\operatorname{Res}(f) = ac(a+e)(c+e)$. We dehomogenize $a = 1$. Then

$$(f, \{0, 1, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{3,1}]^\bullet(K, S) \iff c(1+e)(c+e) \in R_S^*.$$

This leads to solutions to the 4-term S-unit equation

$$c + (1+e) - (c+e) - 1 = 0.$$

The multivariable S-unit sum theorem [Evertse 1984; van der Poorten and Schlickewei 1991] says that there are finitely many solutions with no subsum equal to 0. Ignoring those finitely many solutions, there are three subsum 0 cases:

(1) $c + (1+e) = 0$, which implies that $e_f(\infty) = 2$.

(2) $c - (c+e) = 0$, which implies that $e_f(0) = 2$.

(3) $c - 1 = 0$, which implies that $e_f(1) = 2$.

This gives three families of pairs (f, X) in $\mathcal{GR}_2^1[\mathcal{P}_{3,1}]^\bullet(K, S)$, but every f is ramified at one of the three points in X, so these pairs are not in $\mathcal{GR}_2^1[\mathcal{P}_{3,1}]^\circ(K, S)$. Instead, they are in $\mathcal{GR}_2^1[\mathcal{P}_{4,9}]^\circ(K, S)$. These three families are in fact $\mathrm{PGL}_2(R_S)$-conjugate via permutation of the points in $\{0, 1, \infty\}$. Taking, say, the $e = 0$ family, we have good reduction for all $c \in R_S^*$, and the Milnor image is

$$s\left(\frac{x^2 - (1+c)x + c}{x^2}\right) = \left(\frac{-c^3 - 5c^2 + c - 1}{c^2}, \frac{2c^3 + 7c^2 - 2c + 1}{c^2}\right).$$

This proves that $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,1}]^\bullet = 1$ and $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,1}]^\circ = 0$.

$\boldsymbol{\mathcal{P}_{3,2}}$: We move the three points to $1, 0, \infty$, and then f has the form $f(x) = a(x-1)/(bx^2+cx)$. This map has $\operatorname{Res}(f) = -a^2b(b+c)$, so we can dehomogenize $a = 1$ and replace c with $c - b$. This gives the map $f(x) = (x-1)/(bx^2 + (c-b)x)$ with $\operatorname{Res}(f) = bc$. Hence

$$(f, \{1, 0, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{3,2}]^\circ(K, S) \iff b, c \in R_S^*,$$

and it is in $\mathcal{GR}_2^1[\mathcal{P}_{3,2}]^\circ(K, S)$ if further f is not ramified at the points $\{0, 1, \infty\}$. The map f is never ramified at 1, while its multiplier at the 2-cycle is $(f^2)'(0) = (b-c)/c$. The Milnor image is

$$s\left(\frac{x-1}{bx^2 + (c-b)x}\right) = \left(\frac{b^3 - 3b^2c - 2b^2 + 3bc^2 - 4bc + b - c^3}{bc}, \frac{-2b^3 + 6b^2c + 4b^2 - 6bc^2 + 9bc - 2b + 2c^3 - c^2}{bc}\right).$$

We used Magma to verify that the rational functions $s_1(b, c)$ and $s_2(b, c)$ are algebraically independent in $K(b, c)$. Hence under our assumption that $\#R_S^* = \infty$, we find that $\mathrm{ShafDim}_2^1[\mathcal{P}_{3,2}]^\circ = 2$.

However, if we also require the reduction of f to be unramified at $\{0, 1, \infty\}$ for all primes not in S, then we must also require that $b - c \in R_S^*$. Then $(c/b, 1 - c/b)$ is a solution to the S-unit equation $u + v = 1$, so there are only finitely many choices for the ratio c/b. For each such choice, say $c = ub$ with u fixed, the image in $\mathcal{M}_2^1$ lies on a curve. And taking, say, $u = -1$ gives the set of points

$$s\left(\frac{x-1}{bx^2-2bx}\right) = \left(\frac{-8b^2-2b-1}{b} \frac{16b^2+6b+2}{b}\right), \quad b \in R_S^*.$$

The Zariski closure of this set in $\mathcal{M}_2^1$ is a curve, more precisely, it is the line $2s_1 + s_2 = 2$. Hence $\mathrm{ShafDim}_2^1[\mathcal{P}_{3,2}]^\star = 1$.

$\boldsymbol{\mathcal{P}_{3,3}}$: We move the fixed point to ∞ and the 2-cycle to $\{0, 1\}$, which puts f into the form $f(x) = (x-1)(ax+b)/(cx-b)$. The resultant is $\mathrm{Res}(f) = ab(a+c)(b-c)$, so we may dehomogenize $b = 1$. This puts f in the form $f(x) = (x-1)(ax+1)/(cx-1)$ with resultant $\mathrm{Res}(f) = a(a+c)(1-c)$. Thus f has good reduction if and only if $a, a+c, 1-c \in R_S^*$, which gives a solution to the 4-term S-unit equation

$$a - (a+c) - (1-c) + 1 = 0.$$

The multivariable S-unit sum theorem [Evertse 1984; van der Poorten and Schlickewei 1991] says that there are finitely many solutions with no subsum equal to 0. Ignoring those finitely many solutions, there are three subsum 0 cases:

(1) $a - (a+c) = 0$, which implies that $e_f(\infty) = 2$.

(2) $a - (1-c) = 0$, which implies that $e_f(0) = 2$.

(3) $a + 1 = 0$, which implies that $e_f(1) = 2$.

This gives three families of pairs (f, X) in $\mathcal{GR}_2^1[\mathcal{P}_{3,3}]^\bullet(K, S)$, but every f is ramified at one of the three points in X, so these pairs are not in $\mathcal{GR}_2^1[\mathcal{P}_{3,3}]^\circ(K, S)$. Instead, they are $\mathcal{GR}_2^1[\mathcal{P}_{4,5}]^\circ(K, S)$ in case (1) and in $\mathcal{GR}_2^1[\mathcal{P}_{4,7}]^\circ(K, S)$ in cases (2) and (3). These give sets of points whose closures are curves:

$$\mathcal{P}_{4,5}: \qquad s\bigl(-ax^2 + (a-1)x + 1\bigr) = (2, -a^2 - 3), \quad a \in R_S^*,$$

$$\mathcal{P}_{4,7}: \qquad s\left(\frac{-x^2+2x-1}{cx-1}\right) = \left(\frac{-c^3+2}{(c-1)^2} \frac{2c^3-4}{(c-1)^2}\right), \quad c \in R_S^*.$$

More precisely, they give the curves $s_1 = 2$ and $2s_1 + s_2 = 0$. This completes the proof that $\mathrm{ShafDim}_2^1[\mathcal{P}_{3,3}]^\bullet = 1$ and $\mathrm{ShafDim}_2^1[\mathcal{P}_{3,3}]^\circ = 0$.

$\boldsymbol{\mathcal{P}_{3,4}}$: We move the three points to $1, 0, \infty$, and then f has the form $f(x) = (x-1)(ax+b)/cx$. This map has $\mathrm{Res}(f) = -abc^2$, so we can dehomogenize $c = 1$.

Then $f(x)=(x-1)(ax+b)/x$ has good reduction if and only if $a,b\in R_S^*$. The multiplier at the fixed point is $f'(\infty)=a^{-1}$, so f is not ramified at ∞, and similarly since $f^{-1}(f(0))=\{0,\infty\}$, the map f is not ramified at 0. And these statements are true even modulo primes not in S. Finally we observe that $f'(1)=a+b$, so f is ramified at 1 if and only if $a+b=0$. The Milnor image is

$$s\left(\frac{(x-1)(ax+b)}{x}\right)=\left(\frac{a^3+2a^2b+ab^2-2ab+b}{ab},\right.$$
$$\left.\frac{a^4+2a^3b+a^2b^2-4a^2b+a^2+3ab+b^2-2b}{ab}\right),$$

We used Magma to verify that the rational functions $s_1(b,c)$ and $s_2(b,c)$ are algebraically independent in $K(b,c)$. Hence under our assumption that $\#R_S^*=\infty$, we find that $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,4}]^\circ=2$.

However, if we also require the reduction of f to be unramified at $\{0,1,\infty\}$ for all primes not in S, then we must also require that $a+b\in R_S^*$. Then $(-b/a,1+b/a)$ is a solution to the S-unit equation $u+v=1$, so there are only finitely many choices for the ratio b/a. For each such choice, say $b=ua$ with u fixed, the image in $\mathcal{M}_2^1$ lies on a curve. And taking, say, $u=1$ gives the set of points

$$s\left(\frac{a(x^2-1)}{x}\right)=\left(\frac{4a^2-2a+1}{a},\frac{4a^3-4a^2+5a-2}{a}\right),\quad a\in R_S^*.$$

The Zariski closure in $\mathcal{M}_2^1$ is a curve. Hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,4}]^\star=1$.

$\boldsymbol{\mathcal{P}_{3,5}}$: We move the three points to $0,1,\infty$, which puts f in the form $f(x)=(ax^2+(b-a)x)/c(x-1)$ with $\operatorname{Res}(f)=abc^2$. We dehomogenize $c=1$, so $f(x)=(ax^2+(b-a)x)/(x-1)$. We have $f'(\infty)=a^{-1}$ and $f^{-1}(f(1))=\{1,\infty\}$, so $a\in R_S^*$ implies that f is unramified at ∞ and at 1, even modulo primes not in S. Further, $f'(0)=a-b$, so f is unramified at 0 if and only if $a\neq b$. The Milnor image is

$$s\left(\frac{ax^2+(b-a)x}{x-1}\right)=\left(\frac{-a^3+2a^2b+2a^2-ab^2-a+b}{ab},\right.$$
$$\left.\frac{-a^4+2a^3b+2a^3-a^2b^2-2a^2b-2a^2+3ab+2a-b^2-1}{ab}\right).$$

We used Magma to verify that the rational functions $s_1(a,b)$ and $s_2(a,b)$ are algebraically independent in $K(a,b)$. Hence under our assumption that $\#R_S^*=\infty$, we find that $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,5}]^\circ=2$.

However, if we also require the reduction of f to be unramified at $\{0,1,\infty\}$ for all primes not in S, then we must also require that $a-b\in R_S^*$. Then $(b/a,1-b/a)$ is a solution to the S-unit equation $u+v=1$, so there are only finitely many choices for the ratio b/a. For each such choice, say $b = ua$ with u fixed, the image in $\mathcal{M}_2^1$ lies on a curve. And taking, say, $u = -1$ gives the set of points

$$s\left(\frac{a(x^2-2x)}{x-1}\right) = \left(\frac{4a^2-2a+2}{a}, \frac{4a^4-4a^3+6a^2-2a+1}{a^2}\right), \quad a \in R_S^*.$$

The Zariski closure in $\mathcal{M}_2^1$ is a curve, so $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,5}]^\star = 1$.

$\boldsymbol{\mathcal{P}_{3,6}}$: We move the three fixed points to $0, 1, \infty$, so that f has the form $f(x) = (ax^2+bx)/((a-c)x+b+c)$ with $\operatorname{Res}(f) = ac(a+b)(b+c)$. We dehomogenize $a = 1$, so $f(x) = (x^2+bx)/((1-c)x+b+c)$, and we compute the three multipliers: $f'(0) = b/(b+c)$, $f'(1) = (b+c+1)/(b+c)$, $f'(\infty) = 1-c$. We have

$$(f, \{0, 1, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{3,6}]^\bullet(K, S) \quad \Longleftrightarrow \quad c, 1+b, b+c \in R_S^*.$$

These maps give a solution to the 4-term S-unit equation

$$(b+c) - c - (1+b) + 1 = 0.$$

The multivariable S-unit sum theorem [Evertse 1984; van der Poorten and Schlickewei 1991] says that there are finitely many solutions with no subsum equal to 0. Ignoring those finitely many solutions, there are three subsum 0 cases:

$$\begin{aligned}
(b+c)-c=0 &\implies f(x) = \frac{x^2}{(1-c)x+c} &&\implies e_f(0)=2,\\
(b+c)-(1+b)=0 &\implies f(x) = \frac{x^2+bx}{b+1} &&\implies e_f(\infty)=2,\\
(b+c)+1=0 &\implies f(x) = \frac{x^2+bx}{(b+2)x-1} &&\implies e_f(1)=2.
\end{aligned}$$

This proves that $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,6}]^\circ = 0$, since the subsum 0 cases have a ramified point, and hence are actually in $\mathcal{GR}_2^1[\mathcal{P}_{4,3}]^\circ(K, S)$. The closure of these maps in $\mathcal{M}_2^1$ is a finite set of curves, since for example the family with $c = 1$ gives the family of polynomials $f(x) = (x^2+bx)/(b+1)$ whose closure in $\mathcal{M}_2$ for $b+1 \in R_S^*$ is the line $s_1 = 2$. This proves that $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,6}]^\bullet = 1$, and also (for future reference) that $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,3}]^\circ = 1$.

$\boldsymbol{\mathcal{P}_{3,7}}$: Moving the two points to 0 and ∞ with 0 critical, the map f has the form $f(x) = (ax+b)/cx^2$ with $\operatorname{Res}(f) = b^2c^2$. Dehomogenizing $c = 1$ gives the map $f(x) = (ax+b)/x^2$, which has good reduction if and only if $b \in R_S^*$. We conjugate $u^{-1}f(ux)$ with $u = \sqrt[3]{b}$, which is okay since $K(\sqrt[3]{b})$ is unramified outside S. This puts f into the form $f(x) = (ax+1)/x^2$ with $\operatorname{Res}(f) = 1$. We also note that f is ramified at ∞ if and only if $a = 0$, so taking $a \in R_S^*$ gives maps such that ∞ is unramified modulo all primes not in S. This map has Milnor coordinates

$$s\left(\frac{ax+1}{x^2}\right) = (a^3-6, -2a^3+12),$$

so taking the Zariski closure for $a \in R_S^*$ gives the line $2s_1 + s_2 = 0$. Hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,7}]^\bullet = \operatorname{ShafDim}_2^1[\mathcal{P}_{3,7}]^\star = 1$.

$\boldsymbol{\mathcal{P}_{3,8}}$: Moving the totally ramified fixed point to ∞ and the other fixed point to 0, we have $f(x) = ax^2 + bx$ with $\operatorname{Res}(f) = a^2$. Conjugating by $x \mapsto a^{-1}x$ puts f into the form $f(x) = x^2 + bx$, and then $(f, \{0, \infty\})$ is in $\mathcal{GR}_2^1[\mathcal{P}_{3,8}]^\circ(K, S)$ for all $b \in R_S$ with $b \neq 0$, and $\mathcal{GR}_2^1[\mathcal{P}_{3,8}]^\star(K, S)$ for all $b \in R_S^*$. The Zariski closure of the Milnor image of these maps in $\mathcal{M}_2^1 \cong \mathbb{A}^2$ is the line $s_1 = 2$. Hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,8}]^\bullet = \operatorname{ShafDim}_2^1[\mathcal{P}_{3,8}]^\star = 1$.

This completes our analysis of the 13 portraits of weights 1, 2, and 3 in Table 2. We move on to analyzing the 22 portraits of weight 4 in Tables 3 and 4.

$\boldsymbol{\mathcal{P}_{4,1}}$: Moving the two totally ramified fixed points to 0 and ∞, the map has the form $f(x) = ax^2$. Good reduction forces $a \in R_S^*$, and then conjugation $af(a^{-1}x)$ yields $f(x) = x^2$. Hence $\mathcal{GR}_2^1[\mathcal{P}_{4,1}]^\bullet(K, S)/\operatorname{PGL}_2(R_S)$ consists of a single element.

$\boldsymbol{\mathcal{P}_{4,2}}$: Moving the two totally period 2 points to 0 and ∞, the map has the form $f(x) = ax^{-2}$. Good reduction forces $a \in R_S^*$, and then conjugation $a^{-1}f(ax)$ yields $f(x) = x^{-2}$. Hence $\mathcal{GR}_2^1[\mathcal{P}_{4,2}]^\bullet(K, S)/\operatorname{PGL}_2(R_S)$ consists of a single element.

$\boldsymbol{\mathcal{P}_{4,3}}$: Moving the fixed points to $0, 1, \infty$ with ∞ ramified, the map f has the form $f(x) = ax^2 + (1-a)x$ with $\operatorname{Res}(f) = a^2$. Conjugating gives $af(a^{-1}x) = x^2 + (1-a)x$. The multipliers at 0 and 1 are $f'(0) = 1-a$ and $f'(1) = 3-a$. The Milnor image is $s\bigl(x^2 + (1-a)x\bigr) = (2, 1-a^2)$, so $a \in R_S^*$ gives a Zariski dense set of points in the line $s_1 = 2$, and the same is true if we disallow $a = 1$ and $a = 3$. This proves that $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,3}]^\circ = 1$; cf. the analysis of $\mathcal{P}_{3,6}$. However, if we also insist that 0 and 1 are unramified modulo all primes outside S, then we need $1-a \in R_S^*$ and $3-a \in R_S^*$. In particular, $(a, 1-a)$ is a solution to the S-unit equation $u + v = 1$, so there are only finitely many values of a. This proves that $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,3}]^\star = 0$.

$\boldsymbol{\mathcal{P}_{4,4}}$: Moving the ramified fixed point to ∞, the unramified fixed point to 0, and the other point to 1, we find that f has the form $f(x) = ax^2 - ax$ with $\operatorname{Res}(f) = a^2$. Since $f'(0) = -a$ and $f'(1) = a$, we see that f is unramified at 0 and 1 modulo all primes not in S, and hence $(f, \{0, 1, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{4,4}]^\star(K, S)$ for all $a \in R_S^*$. The Milnor image is $s(ax^2 - ax) = (2, -a^2 - 2a)$, so $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,4}]^\star = 1$.

$\boldsymbol{\mathcal{P}_{4,5}}$: We move the ramified fixed point to ∞ and the other two points to 0 and 1. Then f has the form $f(x) = ax^2 - (a+1)x + 1$ with $\operatorname{Res}(f) = a^2$ and Milnor image $s(ax^2 - (a+1)x + 1) = (2, -a^2 - 3)$. The multiplier for the 2-cycle is

$(f^2)'(0) = 1 - a^2$. Hence

$$(f, \{0, 1, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{4,5}]^\circ(K, S) \quad \Longleftrightarrow \quad a \in R_S^* \text{ and } a \neq \pm 1.$$

In particular, we see that $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,5}]^\circ = 1$; cf. the analysis of $\mathcal{P}_{3,3}$. However, if we also require that the 2-cycle be unramified modulo all primes not in S, then we need $1 - a^2 \in R_S^*$. This gives solutions $(a, 1-a)$ to the S-unit equation $u + v = 1$, so there are only finitely many maps, and hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,5}]^\star = 0$.

$\boldsymbol{\mathcal{P}_{4,6}}$: We move the points to $0, 1, \infty$ so that $1 \to 0 \to \infty \to \infty$. Before imposing the condition that f is ramified at 1, this put f in the form $f(x) = (ax^2 + bx + c)/ex$ with $a + b + c = 0$ and $\operatorname{Res}(f) = ace^2$. We dehomogenize $e = 1$, and then setting $f'(1) = 0$, we find that f has the form $f(x) = a(x-1)^2/x$. Then $f'(\infty) = a^{-1}$ and $f^{-1}(f(0)) = \{0, \infty\}$, so f is unramified at 0 and ∞ modulo all primes not in S. This gives

$$(f, \{0, 1, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{4,6}]^\star(K, S) \quad \Longleftrightarrow \quad a \in R_S^*.$$

The Milnor image is

$$s\left(\frac{a(x-1)^2}{x}\right) = \left(\frac{-2a+1}{a}, \frac{-4a^2+a-2}{a}\right),$$

so the Zariski closure is a curve, and hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,6}]^\star = 1$.

$\boldsymbol{\mathcal{P}_{4,7}}$: We move 0 to the fixed point and ∞ and 1 to the 2-cycle with ∞ ramified. Ignoring the ramification at ∞ for the moment, we find that f has the form $(ax^2+bx)/(x-1)(ax+c)$. Then we see that f is ramified at ∞ if and only if $c = a + b$, so $f(x) = (ax^2 + bx)/(x-1)(ax + a + b)$. We compute $\operatorname{Res}(f) = a^2(a+b)^2$, so we can dehomogenize $a = 1$, and for convenience replace b with $b - 1$, to get $f(x) = (x^2 + (b-1)x)/(x-1)(x+b)$ with $\operatorname{Res}(f) = b^2$. Further, we see that f is unramified at 0 if and only if $b \neq 1$ and f is unramified at 1 if and only if $b \neq -1$. Hence

$$(f, \{0, 1, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{4,7}]^\circ(K, S) \quad \Longleftrightarrow \quad b \in R_S^* \text{ and } b \neq \pm 1.$$

The Milnor image of f is

$$s\left(\frac{x^2+(b-1)x}{(x-1)(x+b)}\right) = \left(\frac{b^3+3b^2-3b+1}{b}, \frac{-2b^3-6b^2+6b-2}{b}\right),$$

which proves that $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,7}]^\circ = 1$. Indeed, we have again landed on the line $2s_1 + s_2 = 0$; cf. the analysis of $\mathcal{P}_{3,3}$. However, if we want f to be unramified at 0 and 1 modulo all primes not in S, then we need $1 \pm b \in R_S^*$. In particular, $(b, 1-b)$ is one of the finitely many solutions of the S-unit equation $u + v = 1$, so $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,7}]^\star = 0$.

$\mathcal{P}_{4,8}$: We move the 2-cycle to 0 and ∞ with 0 ramified and the other point to 1. Then f has the form $f(x) = a(x-1)/bx^2$ with $\operatorname{Res}(f) = a^2b^2$, so we can dehomogenize $a = 1$ to get $f(x) = (x-1)/bx^2$. Assuming that $b \in R_S^*$, we observe that f is unramified at 1 and ∞, even modulo primes not in S. Hence

$$(f, \{0, 1, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{4,8}]^\star(K, S) \quad \text{for all } b \in R_S^*.$$

The Milnor image is

$$s\left(\frac{x-1}{bx^2}\right) = \left(\frac{-6b+1}{b}, \frac{12b-2}{b}\right),$$

so the Zariski closure in $\mathcal{M}_2^1$ of $\mathcal{GR}_2^1[\mathcal{P}_{4,8}]^\star(K, S)$ is the line $2s_1 + s_2 = 0$.

$\mathcal{P}_{4,9}$: We move the 3-cycle to $1 \to 0 \to \infty \to 1$ with 1 a ramification point. This puts f in the form $f(x) = a(x-1)^2/(ax^2+ex)$ with $\operatorname{Res}(f) = a^2(a+e)^2$. We dehomogenize $a = 1$ and replace e with $e-1$ to get $f(x) = (x-1)^2/(x^2+(e-1)x)$ with $\operatorname{Res}(f) = e^2$. The fact that 1 is a ramification point in a 3-cycle tells us that $(f^3)'(1) = 0$, and one of the other points in the 3-cycle will also be ramified if and only if $(f^3)''(1) = 2(1-e^2)/e = 0$. Hence

$$(f, \{0, 1, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{4,9}]^\circ(K, S) \quad \Longleftrightarrow \quad e \in R_S^* \text{ and } e \ne \pm 1.$$

The Milnor image is

$$s\left(\frac{(x-1)^2}{x^2+(e-1)x}\right) = \left(\frac{e^3-5e^2-e-1}{e^2}, \frac{-2e^3+7e^2+2e+1}{e^2}\right),$$

so the closure of $\mathcal{GR}_2^1[\mathcal{P}_{4,9}]^\circ(K, S)$ is a curve and $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,9}]^\circ = 1$. However, if we want the 3-cycle to contain only one ramification point modulo primes not in S, then we need $e^2 - 1 \in R_S^*$. This yields solutions $(e, 1-e)$ to the S-unit equation $u + v = 1$, so there are only finitely many such maps and $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,9}]^\star = 0$.

$\mathcal{P}_{4,10}$: We move the three fixed points to 0, 1, and ∞, and let the fourth point be α with $f(\alpha) = 0$. Then f has the form $f(x) = (ax^2+bx)/(ex+a+b-e)$ with $\alpha = -b/a$ and

$$\operatorname{Res}(f) = a(a+b)(a-e)(a+b-e).$$

We dehomogenize $a = 1$, so $f(x) = (x^2+bx)/(ex+1+b-e)$ and $\alpha = -b$. Then

$$\begin{aligned}
\{0, 1, \infty, -b\} \text{ has good reduction} &\iff b,\, 1+b \in R_S^*,\\
f \text{ has good reduction} &\iff 1+b,\, 1-e,\, 1+b-e \in R_S^*,\\
\bigl(f(x), \{0, 1, \infty, -b\}\bigr) \in \mathcal{GR}_2^1[\mathcal{P}_{4,10}]^\bullet(K, S) &\iff b,\, 1+b,\, 1-e,\, 1+b-e \in R_S^*.
\end{aligned}$$

But this means that $(-b, 1+b)$ is a solution to the S-unit equation $u+v=1$, so there are only finitely many values for b; and then the fact that $\bigl(b^{-1}(e-1), b^{-1}(1+b-e)\bigr)$

is also a solution to the S-unit equation proves that there are only finitely many values for e. This completes the proof that $\mathcal{GR}_2^1[\mathcal{P}_{4,10}]^\bullet(K,S)/\operatorname{PGL}_2(R_S)$ is finite.

$\boldsymbol{\mathcal{P}_{4,11}}$: We move the points so that 0 and ∞ are fixed by f and $f(1)=0$. This puts f in the form $f(x)=ax(x-1)/(bx-c)$, with $\operatorname{Res}(f)=a^2c(c-b)$. We dehomogenize $c=1$, so $f(x)=ax(x-1)/(bx-1)$. Then $f^{-1}(\infty)=\{\infty,b^{-1}\}$, and our assumption that we have a good reduction model for $\mathcal{P}_{4,11}$ requires that b^{-1} be distinct from $\{0,1,\infty\}$ for all primes not in S. Thus $b^{-1}\in R_S^*$ and $b^{-1}-1\in R_S^*$. The S-unit equation $u-v=1$ has only finitely many solutions, so there are finitely many values for b. We observe that for these b values, the map f is unramified modulo all primes not in S, since $f^{-1}(f(0))=f^{-1}(f(1))=\{0,1\}$ and $f^{-1}(f(\infty))=f^{-1}(f(b^{-1}))=\{\infty,b^{-1}\}$. We also note that we can take $b=2$, since $2\in R_S^*$ by assumption. Thus for every $a\in R_S^*$, we see that $\bigl(ax(x-1)/(2x-1),\{0,1,2^{-1},\infty\}\bigr)$ is in $\mathcal{GR}_2^1[\mathcal{P}_{4,11}]^\star(K,S)$. The Milnor image is

$$s\left(\frac{ax(x-1)}{2x-1}\right)=\left(\frac{2a^2-2a+4}{a},\frac{a^4-2a^3+6a^2-4a+4}{a^2}\right),$$

and hence the Zariski closure of $\mathcal{GR}_2^1[\mathcal{P}_{4,11}]^\circ(K,S)$ in $\mathcal{M}_2^1$ is a nonempty finite union of curves. (We remark that the pairs (f,X) studied in Section 4, when restricted to the case $d=2$, have portrait $\mathcal{P}_{4,11}$.)

$\boldsymbol{\mathcal{P}_{4,12}}$: We move the points so that 0 and ∞ are fixed by f and $f(1)=0$. This puts f in the form $f(x)=ax(x-1)/(bx-c)$, with $\operatorname{Res}(f)=a^2c(c-b)$. We dehomogenize $a=1$, so $f(x)=x(x-1)/(bx-c)$. The portrait $\mathcal{P}_{4,12}$ includes a point in $f^{-1}(1)=\{x^2-(1+b)x+c=0\}$, and this point is in K, since the portrait is assumed to be $\operatorname{Gal}(\bar{K}/K)$-invariant. Thus $(1+b)^2-4c=t^2$ for some $t\in K$. Then $(1+b+t)(1+b-t)=4c\in R_S^*$, so if we have a good reduction portrait for f, then $c,c-b,1+b\pm t\in R_S^*$. This gives us a 5-term S-unit sum

$$(1+b+t)+(1+b-t)+2(c-b)-2c-2=0.$$

There are only finitely many solutions with no subsum equal to 0 [Evertse 1984; van der Poorten and Schlickewei 1991], so it remains to analyze the 10 cases where some subsum vanishes.

<u>$(1+b+t)+(1+b-t)=0.$</u> So $b=-1$ and $f(x)=-x(x-1)/(x+c)$. Then c and $c+1$ are in R_S^*, so there are only finitely many choices for c.

<u>$(1+b\pm t)+2(c-b)=0.$</u> So $a-b+2c\pm t=0$. Substituting into $(1+b)^2-4c=t^2$ to eliminate t yields $b=c(c+2)/(c+1)$, and from that we find that $c/(b-c)=1+c$. We know that $c,b-c\in R_S^*$, so this shows that $1+c\in R_S^*$. But then $(1+c,-c)$ is a solution to the S-unit equation $u+v=1$, so there are only finitely many possibilities for c.

<u>$(1+b\pm t)-2c=0.$</u> So $1+b\pm t=2c$. Substituting into $(1+b)^2-4c=t^2$ to eliminate t yields $c^2-bc=0$, so either $c=0$ or $c-b=0$. This contradicts the fact that c and $c-b$ are S-units.

<u>$(1+b\pm t)-2=0.$</u> So $1+b\pm t=2$. Substituting into $(1+b)^2-4c=t^2$ to eliminate t yields $c-b=0$, contradicting the fact that $c-b\in R_S^*$.

<u>$2(c-b)-2c=0.$</u> So $b=0$ and $f(x)=x(x-1)/c$. We have $c\in R_S^*$ and $1-4c=t^2$. We write $a=\gamma u^3$ with $u\in R_S^*$ and γ chosen from a finite set of representatives for $R_S^*/(R_S^*)^3$. Then (u,t) is an R_S-integral point on the genus 1 curve $y^2=1-4\gamma x^3$. Siegel's theorem [Hindry and Silverman 2000, D.9.1] says that there are only finitely many such points.

<u>$2(c-b)-2=0.$</u> So $c=b+1$ and $f(x)=x(x-1)/(bx-b-1)$. We have $c\in R_S^*$ and $c^2-4c=t^2$. We write $c=\gamma u^3$ with $u\in R_S^*$ and γ chosen from a finite set of representatives for $R_S^*/(R_S^*)^2$. Then $(u,t/u)$ is an R_S-integral point on the genus 1 curve $y^2=\gamma^2x^4-4\gamma x$. Siegel's theorem [Hindry and Silverman 2000, D.9.1] says that there are only finitely many such points.

<u>$-2c-2=0.$</u> So $c=-1$ and $f(x)=x(x-1)/(bx+1)$. We have $1+b\in R_S^*$ and $(1+b)^2+4=t^2$. We write $1+b=\gamma u^2$ with $u\in R_S^*$ and γ chosen from a finite set of representatives for $R_S^*/(R_S^*)^2$. Then (u,t) is an R_S-integral point on the genus 1 curve $y^2=\gamma^2u^4+4$. Siegel's theorem [Hindry and Silverman 2000, D.9.1] says that there are only finitely many such points.

$\boldsymbol{\mathcal{P}_{4,13}}$: We move the 2-cycle to $0,\infty$, so $f(x)=(ax+b)/(cx^2+dx)$. The resultant is $-bc(ad-bc)$, so we can dehomogenize $c=1$. Moving a fixed point to 1, we have $a+b=d+1$, so $f(x)=(ax+b)/(x^2+(a+b-1)x)$ with $\operatorname{Res}(f)=-b(a-1)(a+b)$. The good reduction assumption for f tells us that $b, a-1, a+b\in R_S^*$, so we obtain a 4-term S-unit equation

$$(a+b)-(a-1)-b-1=0.$$

The multivariable S-unit sum theorem [Evertse 1984; van der Poorten and Schlickewei 1991] says that there are finitely many solutions with no subsum equal to 0. Ignoring those finitely many solutions, there are three subsum 0 cases:

(1) $(a+b)-(a-1)=0$, so $b=-1$.

(2) $(a+b)-b=0$, so $a=0$.

(3) $(a+b)-1=0$, so $a=1-b$.

The portrait $\mathcal{P}_{4,13}$ has a second fixed point. The fixed points of f are the roots of

$$(x-1)(x^2+(a+b)x+b)=0.$$

We have assumed that the points in $\mathcal{P}_{4,13}$ are defined over K, so the quadratic has a root in K. Thus there is a $t \in K$ such that

$$(a+b)^2 - 4b = t^2.$$

And since $a, b \in R_S$, we have $t \in R_S$. From earlier we know that $a+b$ and b are in R_S^*, so we can write $a+b = \gamma u^2$ and $b = \delta v^4$, with $u, v \in R_S^*$ and γ, δ chosen from a finite set of representatives for $R_S^*/(R_S^*)^4$. Then (uv^{-1}, tv^{-2}) is a R_S-integral point on the genus 1 curve $y^2 = \gamma^2 x^4 - 4\delta$. Siegel's theorem [Hindry and Silverman 2000, D.9.1] says that there are only finitely many such points. Hence there are only finitely many possibilities for the ratio u/v, and thus only finitely many possibilities for $\gamma^2\delta^{-1}(u/v)^4 = (a+b)^2/b$. But we know from the three cases described earlier that either $b = -1$ or $a = 0$ or $a = 1-b$. Substituting these into $(a+b)^2/b$, we find that there are finitely many values for, respectively, $-(a-1)^2$, b, and $1/b$.

$\boldsymbol{\mathcal{P}_{4,14}}$: We move the points to $\alpha \to 1 \to 0 \to \infty$ with ∞ fixed. Ignoring α for the moment, this means that f has the form $f(x) = (ax^2 - (a+c)x + c)/ex$. We have $\operatorname{Res}(f) = -ace^2$, so good reduction forces $a, c, e \in R_S^*$. We dehomogenize by setting $e = 1$. At this stage the pair $(f, \{0, 1, \infty\})$ has good reduction. However, we need to adjoin the point α to the set X. The point α is a root of the numerator of $f(x) - 1$, so α is a root of the polynomial

$$ax^2 - (a+c+1)x + c = 0. \tag{11}$$

Since we are assuming that $\alpha \in K$, the discriminant of this quadratic polynomial is a square in K, say

$$t^2 = (a+c+1)^2 - 4ac \quad \text{with } t \in R_S.$$

Then

$$(a+c+1+t)(a+c+1-t) = 4ac \in R_S^*,$$

so $a+c+1 \pm t \in R_S^*$. So we now know four S-units,

$$a,\ c,\ a+c+1+t,\ a+c+1-t \in R_S^*,$$

which yields a 5-term S-unit sum

$$(a+c+1+t) + (a+c+1-t) - 2a - 2c - 2 = 0.$$

There are only finitely many solutions with no subsum equal to 0 [Evertse 1984; van der Poorten and Schlickewei 1991], so it remains to analyze the 10 cases where some subsum vanishes.

$\underline{(a+c+1+t)+(a+c+1-t)=0.}$ Substituting $c = -a-1$, we find that $t^2 = -4a(a-1)$. Since $a \in R_S^*$, we may write $a = \gamma u^3$ with $u \in R_S^*$ and γ chosen from a finite set of representatives for $R_S^*/(R_S^*)^3$. Then (u, tu^{-1}) is an S-integral point on the genus 1 curve $y^2 = -4\gamma^2x^4 + 4\gamma^2x$. Siegel's theorem [Hindry and Silverman 2000, D.9.1] says that there are only finitely many such points.

$\underline{(a+c+1\pm t)-2a=0.}$ Then $0=(a+c+1)^2-4ac-t^2=4a$, contradicting $a\in R_S^*$.

$\underline{(a+c+1\pm t)-2c=0.}$ Then $0=(a+c+1)^2-4ac-t^2=4c$, contradicting $c\in R_S^*$.

$\underline{(a+c+1\pm t)-2=0.}$ Then

$$0=(a+c+1)^2-4ac-t^2=4(a+c-ac).$$

Hence $1=(a-11)(c-1)$, so $a-1$ and $c-1$ are S-units. Thus $(1-a, a)$ and $(1-c, c)$ are each solutions to the S-unit equation $u+v=1$, which has finitely many solutions.

$\underline{-2a-2c=0.}$ Substituting $a=-c$, we find that $t^2=1+4a^2$. Since $a\in R_S^*$, we may write $a=\gamma u^2$ with $u\in R_S^*$ and γ chosen from a finite set of representatives for $R_S^*/(R_S^*)^2$. Then (u, t) is an R_S-integral point on the genus 1 curve $y^2=1+4\gamma^2x^4$. Siegel's theorem [Hindry and Silverman 2000, D.9.1] says that there are only finitely many such points.

$\underline{-2a-2=0.}$ Substituting $a=-1$, we find that $t^2=c^2+4c$. Since $c\in R_S^*$, we may write $c=\gamma u^3$ with $u\in R_S^*$ and γ chosen from a finite set of representatives for $R_S^*/(R_S^*)^3$. Then (u, tu^{-1}) is an S-integral point on the genus 1 curve $y^2=\gamma^2x^4+4\gamma x$. Siegel's theorem [Hindry and Silverman 2000, D.9.1] says that there are only finitely many such points.

$\underline{-2c-2=0.}$ Substituting $c=-1$, we find that $t^2=a^2+4a$. The analysis is then identical to the previous case with $-2a-2=0$.

$\boldsymbol{\mathcal{P}_{4,15}}$: The portrait $\mathcal{P}_{4,15}$ contains the portrait $\mathcal{P}_{3,3}$ as a subportrait, and we already proved that $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,3}]^\circ=0$, so the same is true for $\mathcal{P}_{4,15}$. On the other hand, if we allow any of the points in $\mathcal{P}_{4,15}$ to have weight greater than 1, then the total weight would be at least 5, in which case Theorem 2(a) gives us finiteness. Hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,15}]^\bullet=0$.

$\boldsymbol{\mathcal{P}_{4,16}}$: The portrait $\mathcal{P}_{4,16}$ contains the portrait $\mathcal{P}_{3,3}$ as a subportrait, and we already proved that $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,3}]^\circ=0$, so the same is true for $\mathcal{P}_{4,16}$. On the other hand, if we allow any of the points in $\mathcal{P}_{4,16}$ to have weight greater than 1, then the total weight would be at least 5, in which case Theorem 2(a) gives us finiteness. Hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,16}]^\bullet=0$.

$\boldsymbol{\mathcal{P}_{4,17}}$: The portrait $\mathcal{P}_{4,17}$ contains the portrait $\mathcal{P}_{3,1}$ as a subportrait, and we already proved that $\operatorname{ShafDim}_2^1[\mathcal{P}_{3,1}]^\circ=0$, so the same is true for $\mathcal{P}_{4,17}$. On the other hand, if we allow any of the points in $\mathcal{P}_{4,17}$ to have weight greater than 1, then the total weight would be at least 5, in which case Theorem 2(a) gives us finiteness. Hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,17}]^\bullet=0$.

$\boldsymbol{\mathcal{P}_{4,18}}$: Moving the four points to b, 1, 0, ∞, we see that $f(x) = a(x-1)(x-b)/ex$ with $\operatorname{Res}(f) = a^2be^2$, so we can dehomogenize $a = 1$. Then

$$\bigl(f(x), \{b, 1, 0, \infty\}\bigr) \in \mathcal{GR}_2^1[\mathcal{P}_{4,18}]^\bullet(K, S) \iff b, 1-b, e \in R_S^*.$$

(Note that $b, 1-b \in R_S^*$ is the condition for $\{b, 0, 1, \infty\}$ to have good reduction outside S.) Then $(b, 1-b)$ is a solution to the S-unit equation $u + v = 1$, so there are finitely many values for b. Each value of b, for example $b = 2$, yields a curve in $\mathcal{M}_2^1$, for example, the Milnor image with $b = 2$ is

$$s\left(\frac{(x-1)(x-2)}{ex}\right) = \left(\frac{2e^2-4e+17}{2e}, \frac{-4e^3+19e^2-8e+17}{2e^2}\right).$$

Hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,18}]^\circ = 1$. However, since $f^{-1}(f(1)) = f^{-1}(f(b)) = \{1, b\}$ and $f^{-1}(f(0)) = f^{-1}(f(\infty)) = \{0, \infty\}$, we see that f modulo primes not in S is unramified at the points in $\{b, 1, 0, \infty\}$, so the above maps with $b = 2$ and $e \in R_S^*$ are in $\mathcal{GR}_2^1[\mathcal{P}_{4,18}]^\star(K, S)$, and hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,18}]^\circ = 1$.

$\boldsymbol{\mathcal{P}_{4,19}}$: Moving $0, \infty$ to the 2-cycle and 1 to the incoming point, we see that $f(x) = a(x-1)/(bx^2+cx)$. This has $\operatorname{Res}(f) = a^2b(b+c)$. We dehomogenize $b = 1$, so $f(x) = a(x-1)/x(x+c)$ with $a, 1+c \in R_S^*$. The fourth point of the portrait is in $f^{-1}(1)$, so it is a root of $x^2+(c-a)x+a$. Since that point is in K by assumption, we see that the discriminant $(c-a)^2-4a$ must be a square in K, say equal to t^2. Then

$$(c-a+t)(c-a-t) = 4a \in R_S^*,$$

so $c-a \pm t \in R_S^*$. This gives us a 5-term S-unit sum

$$(c-a+t)+(c-a-t)-2(1+c)+2a+2 = 0.$$

There are only finitely many solutions with no subsum equal to 0 [Evertse 1984; van der Poorten and Schlickewei 1991], so it remains to analyze the 10 cases where some subsum vanishes.

$\underline{-2(1+c)+2a = 0.}$ Then $a = c+1$ and $f(x) = a(x-1)/x(x+a-1)$. We have $1-4a = t^2$. We write $a = \gamma u^4$ with $u \in R_S^*$ and γ chosen from a finite set of representatives for $R_S^*/(R_S^*)^4$. Then $1-4\gamma u^4 = t^2$, so (u, t) is an R_S-integral point on the genus 1 curve $Y^2 = 1-4\gamma X^4$. Siegel's theorem [Hindry and Silverman 2000, D.9.1] tells us that there are only finitely many solutions.

$\underline{-2(1+c)+2 = 0.}$ Then $c = 0$ and $f(x) = a(x-1)/x^2$. This map has $e_f(0) = 2$, so we do not get the portrait $\mathcal{P}_{4,19}$ in which every point has multiplicity 1.

$\underline{2a+2 = 0.}$ Then $a = -1$ and $f(x) = (-x+1)/x(x+c)$. We have $(c+1)^2+4 = t^2$. We write $c+1 = \gamma u^2$ with $u \in R_S^*$ and γ chosen from a finite set of representatives for $R_S^*/(R_S^*)^2$. Then $\gamma^2u^4+4 = t^2$, so (u, t) is an R_S-integral point on the genus 1 curve $Y^2 = \gamma^2 X^4 + 4$. Siegel's theorem [Hindry and Silverman 2000, D.9.1] tells us that there are only finitely many solutions.

$\underline{(c-a+t)+(c-a-t)=0.}$ Then $a=c$ and $f(x)=a(x-1)/x(x+a)$. We have $a,\, 1+a \in R_S^*$, so $(-a,\, 1+a)$ is a solution to the S-unit equation $u+v=1$. Here there are only finitely many choices for a.

$\underline{(c-a\pm t)-2(1+c)=0.}$ Then $\pm t = a+c+2$, and the equation $(c-a)^2-4a=t^2$ becomes $ac+2a+c+1=0$. We rewrite this as $a(c+1)+(c+1)+1=0$. Thus $\bigl(a(c+1),\, c+1\bigr)$ is a solution to the S-unit equation $u+v+1=0$, so has only finitely many solutions.

$\underline{(c-a\pm t)+2a=0.}$ Then $\pm t=a+c$, and the equation $(c-a)^2-4a=t^2$ becomes $4a(c+1)=0$. This contradicts the fact that a and c are in R_S^*.

$\underline{(c-a\pm t)+2=0.}$ Then $\pm t = c-a+2$, and the equation $(c-a)^2-4a=t^2$ becomes $4(c+1)=0$, contradicting $c+1 \in R_S^*$.

This completes the proof that $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,19}]^\circ = 0$. But if we assign a weight greater than 1 to any of the points in $\mathcal{P}_{4,19}$, then the resulting portrait will have total weight at least 5, so Theorem 2(a) gives us finiteness. Hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,19}]^\bullet = 0$.

$\boldsymbol{\mathcal{P}_{4,20}}$: Moving $0, \infty$ to the 2-cycle and 1 to an incoming point, we see that $f(x)=a(x-1)/(bx^2+cx)$. This has $\operatorname{Res}(f)=a^2b(b+c)$. In particular, $a,\, b \in R_S^*$, so we can dehomogenize $b=1$ and $f(x)=a(x-1)/x(x+c)$ with $a,\, 1+c \in R_S^*$. The fourth point of the portrait in $f^{-1}(\infty)$, so it is the point $-c$. Then $\{0, 1, \infty, -c\}$ has good reduction if and only if $c,\, 1+c \in R_S^*$, so $(-c,\, 1+c)$ is a solution to the S-unit equation $u+v=1$. There are thus only finitely many choices for c. For example, since $2 \in R_S^*$, we may could take $c=1$. Then $a(x-1)/x(x+1) \in \mathcal{GR}_2^1[\mathcal{P}_{4,20}]^\circ(K, S)$ for all $a \in R_S^*$. The Milnor image is

$$s\left(\frac{a(x-1)}{x(x+1)}\right) = \left(\frac{a^2-10a-1}{2a},\, \frac{-a^2+9a+1}{a}\right),$$

which shows that the Zariski closure of $\mathcal{GR}_2^1[\mathcal{P}_{4,20}]^\circ(K,S)$ in $\mathcal{M}_2^1$ is a nonempty finite union of curves. Further, since

$$\begin{aligned} f^{-1}(f(1)) &= f^{-1}(f(\infty)) = \{1, \infty\}, \\ f^{-1}(f(0)) &= f^{-1}(f(-1)) = \{0, -1\}, \end{aligned}$$

we see that f modulo primes not in S is unramified at the points in $\{-1, 1, 0, \infty\}$, so the above maps with $c=1$ and $a \in R_S^*$ are in $\mathcal{GR}_2^1[\mathcal{P}_{4,20}]^\star(K,S)$, and hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,20}]^\star = 1$. Finally, we note that $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,20}]^\bullet = \operatorname{ShafDim}_2^1[\mathcal{P}_{4,20}]^\circ$, since if we assign a weight greater than 1 to any of the points in $\mathcal{P}_{4,20}$, then the resulting portrait will have total weight at least 5, so Theorem 2(a) gives us finiteness. Hence $\operatorname{ShafDim}_2^1[\mathcal{P}_{4,20}]^\bullet = 1$.

$\mathcal{P}_{4,21}$: The portrait $\mathcal{P}_{4,21}$ contains the portrait $\mathcal{P}_{3,1}$ as a subportrait, and we already proved that $\mathrm{ShafDim}_2^1[\mathcal{P}_{3,1}]^\circ = 0$, so the same is true for $\mathcal{P}_{4,21}$. On the other hand, if we allow any of the points in $\mathcal{P}_{4,21}$ to have weight greater than 1, then the total weight would be at least 5, in which case Theorem 2(a) gives us finiteness. Hence $\mathrm{ShafDim}_2^1[\mathcal{P}_{4,21}]^\bullet = 0$.

$\mathcal{P}_{4,22}$: We move three of the points in the 4-cycle to 0, 1, and ∞, and we denote the fourth point by c. The map f then has the form

$$f(x) = \frac{c(x-1)(x+a)}{x\bigl(x-c+(c-1)(c+a)\bigr)},$$
$$\mathrm{Res}(f) = ac^2(1-c)(2-c)(a+c)(1-a-c).$$

The set $\{c, 0, 1, \infty\}$ has good reduction outside S if and only if $c, 1-c \in R_S^*$. Hence $(f, \{c, 0, 1, \infty\}) \in \mathcal{GR}_2^1[\mathcal{P}_{4,22}]^\bullet$ if and only if

$$a, c, 1-c, 2-c, a+c, 1-a-c \in R_S^*.$$

Then $(c, 1-c)$ is a solution to the S-unit equation $u+v=1$, so there are only finitely many values of c. Then the fact that $(a+c, 1-a-c)$ is also a solution to the S-unit equation shows that there are only finitely many values of a. Hence $\mathrm{ShafDim}_2^1[\mathcal{P}_{4,22}]^\bullet = 0$.

This completes our analysis of the 22 weight 4 portraits in Tables 3 and 4, and with it, the proof of Theorem 19. □

8. Possible generalizations

It is natural to attempt to generalize Theorem 2(a) to self-maps of $\mathbb{P}^N$ with $N \geq 2$. The naive generalization fails. Indeed, suppose that we define $\mathcal{GR}_d^N[n](K, S)$ to be the set of triples (f, Y, X) such that $f : \mathbb{P}_K^N \to \mathbb{P}_K^N$ is a degree d morphism defined over K and $Y \subseteq X \subset \mathbb{P}^1(\bar{K})$ are finite sets satisfying the following conditions:[9]

- $X = Y \cup f(Y)$,
- X is $\mathrm{Gal}(\bar{K}/K)$-invariant,
- $\#Y = n$,
- f and X have good reduction outside S.

Then it is easy to see that for any fixed d and N, the set $\mathcal{GR}_d^N[n](K, S)$ can be infinite for arbitrarily large n. We illustrate with $d = N = 2$, since the general case is then clear.

Consider the family of maps $f_{a,b} : \mathbb{P}^2 \to \mathbb{P}^2$ defined by

$$f_{a,b}(X, Y, Z) = [aXZ + X^2, bYZ + Y^2, Z^2] \quad \text{with } a, b \in R_S. \tag{12}$$

[9] This definition is not entirely consistent with our definition of $\mathcal{GR}_d^1[n](K, S)$, since we've replaced the earlier ramification condition on Y with the simpler condition that Y contain n points.

Then $f_{a,b}$ has good reduction at all primes $\mathfrak{p} \notin S$. And it is not an isotrivial family, since for example the characteristic polynomial of $f_{a,b}$ acting on the tangent space at the fixed point $[0, 0, 1]$ is easily computed to be $(T-a)(T-b)$. For a given n, we take $K = \mathbb{Q}$ and we take S to be the set of primes dividing $2\prod_{i=1}^{n}(2^i - 1)$, and we let

$$X_n := \{[1, 2^i, 0] \in \mathbb{P}^N(\mathbb{Q}) : 0 \le i \le n\}.$$

Then X_n has good reduction at all $p \notin S$, and, since $f([1, y, 0]) = [1, y^2, 0]$, we see that $f_{a,b}(X_{n-1}) \subset X_n$. Hence

$$(f_{a,b}, X_{n-1}, X_n) \in \mathcal{GR}_2^2[n](\mathbb{Q}, S)/\operatorname{PGL}_3(\mathbb{Z}_S)$$

gives infinitely many inequivalent triples as a and b range over $\mathbb{Z}_S$.

One key step in the proof of Theorem 2(a) that goes wrong when we try to generalize to $\mathbb{P}^N$ is Lemma 10, which says that if two maps $f, g : \mathbb{P}^1 \to \mathbb{P}^1$ agree at enough points, then $f = g$. This is false in higher dimension, and indeed, the maps $f_{a,b}$ defined by (12) take identical values at all points on the line $Z = 0$.

This suggests two ways to rescue the theorem.

First, we might simply say that two maps are "the same" if they take the same values on a nontrivial subvariety of $\mathbb{P}^N$. This is a somewhat drastic solution, but the following partial generalization of Lemma 10, whose proof we leave to the reader, makes it a reasonable solution.

Lemma 20. *Let K be a field, and let $f, g : \mathbb{P}_K^N \to \mathbb{P}_K^N$ be morphisms of degrees d and e, respectively. Suppose that*

$$\#\{P \in \mathbb{P}^N(K) : f(P) = g(P)\} \ge (d+e)^N + 1.$$

Then there is a curve $C \subset \mathbb{P}_K^N$ such that $f(P) = g(P)$ for all $P \in C$.

Second, we might insist that the marked points in the set X are in sufficiently general position to ensure that $f|_X = g|_X$ forces $f = g$. Thus writing End_d^N for the space of degree d self-morphisms of $\mathbb{P}^N$, we might say that a set $Y \subset \mathbb{P}^N$ is in *d-general position for $\mathbb{P}^N$* if the map

$$\operatorname{End}_d^N \to (\mathbb{P}^N)^{\#Y}, \quad f \mapsto (f(P))_{P \in Y}$$

is injective. Then a version of Theorem 2(a) might be true if we restrict to triples $(f, Y, X) \in \mathcal{GR}_d^N[n](K, S)$ for which Y is in d-general position for $\mathbb{P}^N$.

In this paper, we will not further pursue these, or other potential, generalizations of Theorem 2(a) to $\mathbb{P}^N$.

A second possible generalization of our results would be to extend them to other types of fields, for example taking $K = k(C)$ to be the function field of a curve over an algebraically closed field k. If k has characteristic 0, then much of the argument in this paper should carry over, although there may be issues with isotrivial maps;

while if k has characteristic $p > 0$, then issues of wild ramification arise, as does the fact that the theorem on S-unit equations is more restrictive in requiring more than the simple "no vanishing subsum" condition. Again, we have chosen not to pursue such function field generalizations in the present paper.

Acknowledgements

The author would like to thank Dan Abramovich, Rob Benedetto, Noah Giansiracusa, Jeremy Kahn, Sarah Koch, Clay Petsche, Mike Zieve, and the referee for their helpful advice.

References

[Arfeux 2016] M. Arfeux, "Approximability of dynamical systems between trees of spheres", *Indiana Univ. Math. J.* **65**:6 (2016), 1945–1977. MR Zbl

[Beardon 1991] A. F. Beardon, *Iteration of rational functions: complex analytic dynamical systems*, Graduate Texts in Mathematics **132**, Springer, 1991. 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

[Canci et al. 2013] J. K. Canci, G. Peruginelli, and D. Tossici, "On some notions of good reduction for endomorphisms of the projective line", *Manuscripta Math.* **141**:1–2 (2013), 315–331. MR Zbl

[Doyle 2016] J. R. Doyle, "Preperiodic portraits for unicritical polynomials", *Proc. Amer. Math. Soc.* **144**:7 (2016), 2885–2899. MR Zbl

[Doyle 2018] J. R. Doyle, "Preperiodic portraits for unicritical polynomials over a rational function field", *Trans. Amer. Math. Soc.* **370**:5 (2018), 3265–3288. MR

[Doyle and Silverman $\geq$ 2018] J. R. Doyle and J. H. Silverman, "Moduli spaces of dynamical systems with portraits", in preparation.

[Evertse 1984] J.-H. Evertse, "On sums of S-units and linear recurrences", *Compositio Math.* **53**:2 (1984), 225–244. MR Zbl

[Evertse and Győry 1993] J.-H. Evertse and K. Győry, "Lower bounds for resultants, I", *Compositio Math.* **88**:1 (1993), 1–23. MR Zbl

[Faber and Granville 2011] X. Faber and A. Granville, "Prime factors of dynamical sequences", *J. Reine Angew. Math.* **661** (2011), 189–214. MR Zbl

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. MR Zbl

[Ghioca et al. 2015] D. Ghioca, K. Nguyen, and T. J. Tucker, "Portraits of preperiodic points for rational maps", *Math. Proc. Cambridge Philos. Soc.* **159**:1 (2015), 165–186. MR Zbl

[Győry 1990] K. Győry, "On arithmetic graphs associated with integral domains", pp. 207–222 in *A tribute to Paul Erdős*, edited by A. Baker et al., Cambridge University Press, 1990. MR Zbl

[Győry 1993] K. Győry, "On the number of pairs of polynomials with given resultant or given semi-resultant", *Acta Sci. Math.* (*Szeged*) **57**:1–4 (1993), 515–529. MR Zbl

[Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Graduate Texts in Mathematics **201**, Springer, 2000. MR Zbl

[Levy 2011] A. Levy, "The space of morphisms on projective space", *Acta Arith.* **146**:1 (2011), 13–31. MR Zbl

[Milnor 1993] J. Milnor, "Geometry and dynamics of quadratic rational maps", *Experiment. Math.* **2**:1 (1993), 37–83. MR Zbl

[Morton and Silverman 1995] P. Morton and J. H. Silverman, "Periodic points, multiplicities, and dynamical units", *J. Reine Angew. Math.* **461** (1995), 81–122. MR Zbl

[Mumford 1970] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics **5**, Oxford University Press, London, 1970. MR Zbl

[Neukirch 1999] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften **322**, Springer, 1999. MR Zbl

[PARI 2016] PARI group, PARI/GP version 2.9.0, 2016, available at http://pari.math.u-bordeaux.fr.

[Petsche 2012] C. Petsche, "Critically separable rational maps in families", *Compos. Math.* **148**:6 (2012), 1880–1896. MR Zbl

[Petsche and Stout 2015] C. Petsche and B. Stout, "On quadratic rational maps with prescribed good reduction", *Proc. Amer. Math. Soc.* **143**:3 (2015), 1145–1158. MR Zbl

[Petsche et al. 2009] C. Petsche, L. Szpiro, and M. Tepper, "Isotriviality is equivalent to potential good reduction for endomorphisms of $\mathbb{P}^N$ over function fields", *J. Algebra* **322**:9 (2009), 3345–3365. MR Zbl

[van der Poorten and Schlickewei 1991] A. J. van der Poorten and H. P. Schlickewei, "Additive relations in fields", *J. Austral. Math. Soc. Ser. A* **51**:1 (1991), 154–170. MR Zbl

[Silverman 1998] J. H. Silverman, "The space of rational maps on $\mathbf{P}^1$", *Duke Math. J.* **94**:1 (1998), 41–77. MR Zbl

[Silverman 2007] J. H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics **241**, Springer, 2007. MR Zbl

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, 2009. MR Zbl

[Stout 2014] B. J. Stout, "A dynamical Shafarevich theorem for twists of rational morphisms", *Acta Arith.* **166**:1 (2014), 69–80. MR Zbl

[Szpiro and Tucker 2008] L. Szpiro and T. J. Tucker, "A Shafarevich–Faltings theorem for rational functions", *Pure Appl. Math. Q.* **4**:3 (2008), 715–728. MR Zbl

[Szpiro and West 2017] L. Szpiro and L. West, "A dynamical Shafarevich theorem for rational maps over number fields and function fields", preprint, 2017. arXiv

[Szpiro et al. 2017] L. Szpiro, T. Tucker, and L. West, "Proof of the Shafarevich conjecture for self-maps of $\mathbb{P}^1$", lecture at Workshop on Heights and Applications to Unlikely Intersections, Fields Institute, Toronto, February 13–17, 2017, available at http://www.fields.utoronto.ca/talks/Proof-Shafarevich-conjecture-self-maps-mathbbP1.

Received April 4, 2017. Revised September 15, 2017.

JOSEPH H. SILVERMAN
DEPARTMENT OF MATHEMATICS
BROWN UNIVERSITY
PROVIDENCE, RI
UNITED STATES
jhs@math.brown.edu

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.191

BLOCKS IN FLAT FAMILIES OF FINITE-DIMENSIONAL ALGEBRAS

ULRICH THIEL

We study the behavior of blocks in flat families of finite-dimensional algebras. In a general setting we construct a finite directed graph encoding a stratification of the base scheme according to the block structures of the fibers. This graph can be explicitly obtained when the central characters of simple modules of the generic fiber are known. We show that the block structure of an arbitrary fiber is completely determined by "atomic" block structures living on the components of a Weil divisor. As a byproduct, we deduce that the number of blocks of fibers defines a lower semicontinuous function on the base scheme. We furthermore discuss how to obtain information about the simple modules in the blocks by generalizing and establishing several properties of decomposition matrices by Geck and Rouquier.

1. Introduction

It is a classical fact in ring theory that a nonzero noetherian ring A can be decomposed as a direct product $A = \prod_{i=1}^{n} B_i$ of indecomposable rings B_i. Such a decomposition is unique up to permutation and isomorphism of the factors. Let us denote by $\mathrm{Bl}(A)$ the set of the B_i, called the *blocks* of A. The decomposition of

MSC2010: primary 16G10; secondary 14DXX, 16T20, 20C08.

Keywords: finite-dimensional algebras, block theory, flat families, representation theory, Brauer reciprocity, decomposition matrices.

A into blocks induces the decomposition $A\text{-Mod} = \bigoplus_{i=1}^n B_i\text{-Mod}$ of the category of (left) A-modules. In particular, a simple A-module is a simple B_i-module for a unique block B_i and so we get the induced decomposition $\operatorname{Irr} A = \coprod_{i=1}^n \operatorname{Irr} B_i$ of the set of simple modules. Let us denote by $\operatorname{Fam}(A)$ the set of the $\operatorname{Irr} B_i$, called the *families* of A. The blocks and families of a ring are important invariants which help to organize and simplify its representation theory. The aim of this paper is to investigate how these invariants vary in a flat family of finite-dimensional algebras.

More precisely, we consider a *finite flat* algebra A over an integral domain R; i.e., A is finitely generated and flat as an R-module. This yields a family of algebras parametrized by $\operatorname{Spec}(R)$ consisting of the *specializations* (or *fibers*)

$$A(\mathfrak{p}) := \mathrm{k}(\mathfrak{p}) \otimes_R A \simeq A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}} A_{\mathfrak{p}}, \tag{1}$$

where $\mathrm{k}(\mathfrak{p}) = \operatorname{Frac}(R/\mathfrak{p})$ is the residue field of $\mathfrak{p} \in \operatorname{Spec}(R)$ in R and $A_{\mathfrak{p}}$ is the localization of A in $\mathfrak{p}$. Note that the fiber $A(\mathfrak{p})$ is a finite-dimensional $\mathrm{k}(\mathfrak{p})$-algebra. Now, the primary goal would be to describe for any $\mathfrak{p}$ the blocks of $A(\mathfrak{p})$, e.g., the number of blocks, and to describe the simple modules in each block, e.g., the number of such modules and their dimensions.

It is clear that there will be no general theory giving the precise solutions to these problems for arbitrary A. For example, we can take the group ring $A = \mathbb{Z}\mathrm{S}_n$ of the symmetric group. The fibers of A are precisely the group rings $\mathbb{Q}\mathrm{S}_n$ and $\mathbb{F}_p\mathrm{S}_n$ for all primes p, and the questions above are still unanswered. Nonetheless, and this is the point of this paper, there are some general phenomena, some patterns in the behavior of blocks and simple modules along the fibers, which are true quite generally.

1A. ***The setting.*** We assume that R is noetherian and normal, and that the generic fiber A^K is a *split* K-algebra, where K is the fraction field of R; i.e., all simple modules of A^K remain simple under field extension. This setting includes many interesting examples in representation theory, like Brauer algebras, Hecke algebras, (restricted) rational Cherednik algebras, etc. We note that some results we mention below actually hold more generally and refer to the main body of the paper.

At the very end we also establish a semicontinuity property of blocks in the (important) case of a nonsplit generic fiber; see Theorem 1.6. This then applies also to quantized enveloping algebras of semisimple Lie algebras at roots of unity, enveloping algebras of semisimple Lie algebras in positive characteristic, quantized function algebras of semisimple groups at roots of unity, etc. More generally, this applies to Hopf PI triples as introduced by Brown and Goodearl [2002]; see also [Brown and Gordon 2001; Gordon 2001].

1B. ***Block stratification.*** Under the assumptions described above, we prove the following theorem (see Corollary 4.3), which is the backbone of this paper:

Theorem 1.1. *For any* $\mathfrak{p} \in \operatorname{Spec}(R)$ *the natural map* $A_{\mathfrak{p}} \twoheadrightarrow A(\mathfrak{p})$ *is* ***block bijective****; i.e., it induces a bijection between the block idempotents.*

This allows us to reduce the study of blocks of specializations to blocks of localizations, and this is much simpler from the general perspective. Since a block idempotent of a localization $A_{\mathfrak{p}}$ splits into a sum of block idempotents of the generic fiber A^K, we can view the blocks of $A_{\mathfrak{p}}$ as being a *partition* of the set of blocks of A^K; see Section 3 for details. This gives us a direct and natural way of comparing the block structures among the fibers — something which is in general, without the above theorem, not possible. Let

$$\mathrm{Bl}_A : \operatorname{Spec}(R) \to \operatorname{Part}(\mathrm{Bl}(A^K))$$

be the map just described. We equip the image $\mathrm{Bl}(A)$ of this map with the partial order $\leq$ on partitions, where $\mathscr{P}' \leq \mathscr{P}$ if the members of $\mathscr{P}'$ are unions of members of $\mathscr{P}$. We let $\mathrm{Bl}_A^{-1}(\mathscr{P})$, respectively $\mathrm{Bl}_A^{-1}(\leq \mathscr{P})$, be the locus of all $\mathfrak{p} \in \operatorname{Spec}(R)$ such that the block structure of $A_{\mathfrak{p}}$, and thus of $A(\mathfrak{p})$ under the above bijection, is equal to a given partition $\mathscr{P}$, respectively coarser than $\mathscr{P}$. We then obtain as Theorem 3.3:

Theorem 1.2. *The sets* $\mathrm{Bl}_A^{-1}(\leq \mathscr{P})$ *are closed in* $\operatorname{Spec}(R)$, *the sets* $\mathrm{Bl}_A^{-1}(\mathscr{P})$ *are locally closed in* $\operatorname{Spec}(R)$, *and* $\operatorname{Spec}(R) = \coprod_{\mathscr{P}} \mathrm{Bl}_A^{-1}(\mathscr{P})$ *is a stratification of* $\operatorname{Spec}(R)$.

Denoting by $\bullet$ the generic point of $\operatorname{Spec}(R)$, so that $A_\bullet = A(\bullet) = A^K$, this implies in particular that the set

$$\begin{aligned} \mathrm{BlGen}(A) :=\ & \mathrm{Bl}_A^{-1}(\mathrm{Bl}_A(\bullet)) \\ &= \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathrm{Bl}_A(\mathfrak{p}) = \mathrm{Bl}_A(\bullet)\} \end{aligned}$$

of primes $\mathfrak{p}$ where the block structure of the fiber $A(\mathfrak{p})$ is equal to the one of the generic fiber A^K is an open (dense) subset of $\operatorname{Spec}(R)$. Hence, the set

$$\mathrm{BlEx}(A) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathrm{Bl}_A(\mathfrak{p}) < \mathrm{Bl}_A(\bullet)\}$$

of primes where the block structure of the fiber is coarser than the one of the generic fiber is closed. This set has a nice property; see Corollary 3.5:

Theorem 1.3. *If R is a Krull domain* (*e.g., if R is normal*), *then* $\mathrm{BlEx}(A)$ *is a reduced Weil divisor*; *i.e., it is either empty or pure of codimension* 1 *in* $\operatorname{Spec}(R)$.

We thus call $\mathrm{BlEx}(A)$ the *block divisor* of A. This is an interesting new *discriminant* of A. Let $\mathrm{At}(A)$ be the set of irreducible components of $\mathrm{BlEx}(A)$. On any $Z \in \mathrm{At}(A)$ there is a unique maximal block structure $\mathrm{Bl}_A(Z)$, namely the one in the generic point. In Section 3C we show that these block structures have an *atomic character*:

Theorem 1.4. *For* $\mathfrak{p} \in \operatorname{Spec}(R)$ *we have*

$$\mathrm{Bl}_A(\mathfrak{p}) = \bigwedge_{\substack{Z \in \mathrm{At}(A) \\ \mathfrak{p} \in Z}} \mathrm{Bl}_A(Z),$$

where $\wedge$ *is the meet of partitions*; *i.e., the members are the unions of all members with nonempty intersection.*

Hence, once we know $\mathrm{At}(A)$ and the *atomic block structures* $\mathrm{Bl}_A(Z)$ for $Z \in \mathrm{At}(A)$, we know the block structure for any $\mathfrak{p} \in \operatorname{Spec}(R)$. By considering sets of the form

$$\bigcap_{Z \in \mathscr{Z}} Z \setminus \bigcup_{Z \notin \mathscr{Z}} Z$$

for subsets $\mathscr{Z} \subseteq \mathrm{At}(A)$, we obtain a stratification of $\operatorname{Spec}(R)$ refining the one introduced above. We call this the *block stratification* of A.

1C. ***Blocks via central characters.*** In Section 5 we discuss an approach to explicitly compute the block stratification and the block structures on the strata. This is based on the knowledge of central characters of simple A^K-modules. Since A^K splits, each simple A^K-module S has a central character $\Omega'_S : \mathrm{Z}(A) \to R$, the image lying in R since R is normal. In Theorem 5.9 we show:

Theorem 1.5. *Two simple* A^K*-modules* S *and* T *lie in the same* $A_{\mathfrak{p}}$*-block if and only if* $\Omega'_S \equiv \Omega'_T \bmod \mathfrak{p}$.

The key ingredient in the proof is a (rather nontrivial) result by B. Müller stating that the cliques of a noetherian ring, which is a finite module over its center, are fibered over the center. We address this in detail in Section 5A.

If $z_1, \ldots, z_n$ is an R-algebra generating system of $\mathrm{Z}(A)$, then $\Omega'_S \equiv \Omega'_T \bmod \mathfrak{p}$ if and only if $\Omega'_S(z_i) \equiv \Omega'_T(z_i) \bmod \mathfrak{p}$ for all i. Hence, Theorem 1.5 gives a computational tool to explicitly determine $\mathrm{Bl}_A(\mathfrak{p})$ once the central characters of the generic fiber are known. Moreover, it follows from Theorem 1.5 that $\mathrm{At}(A)$ is the set of maximal irreducible components of the zero loci of the sets

$$\{\Omega'_S(z_i) - \Omega'_T(z_i) \mid i = 1, \ldots, n\} \tag{2}$$

for $\Omega'_S \neq \Omega'_T$. The atomic block structures can then be determined by the vanishing of the differences $\Omega'_S - \Omega'_T$ on the $Z \in \mathrm{At}(A)$, and from these we obtain all block structures as described above.

1D. ***An example.*** Let us illustrate this with an explicit example. Let A be the generic Brauer algebra for $n = 3$ over the polynomial ring $R := \mathbb{Z}[\delta]$; see [Graham and Lehrer 1996]. There are four simple A^K-modules, labeled by the partitions $(0, (1, 1, 1))$, $(0, (3))$, $(0, (2, 1))$, and $(1, (1))$. We will simply label these by

$1, \dots, 4$ from now on. Since A^K is semisimple, we can identify the blocks of A^K with the simple modules of A^K; i.e., we can label the blocks by $1, \dots, 4$. We can thus view blocks of specializations of A as partitions of $\{1, \dots, 4\}$ as described above. It is not too difficult to explicitly compute the central characters of the simple A^K-modules. From these we deduce that the block structure of the fibers of A over $\mathbb{Z}[\boldsymbol{\delta}]$ are distributed as in the following graph:

$$\begin{tikzcd}[column sep=small]
 & & & \begin{array}{c}\{1\},\{2\},\{3\},\{4\}\\(0)\end{array} \arrow[dlll] \arrow[dl] \arrow[dr] \arrow[drrr] & & & \\
\begin{array}{c}\{1,2,3\},\{4\}\\(3)\end{array} \arrow[dr] & & \begin{array}{c}\{1\},\{2\},\{3,4\}\\(\boldsymbol{\delta}-1)\end{array} \arrow[dl] \arrow[dr] & & \begin{array}{c}\{1,2\},\{3\},\{4\}\\(2)\end{array} \arrow[dl] \arrow[dr] & & \begin{array}{c}\{1\},\{2,4\},\{3\}\\(\boldsymbol{\delta}+2)\end{array} \arrow[dl] \\
 & \begin{array}{c}\{1,2,3,4\}\\(\boldsymbol{\delta}-1,3)\end{array} & & \begin{array}{c}\{1,2\},\{3,4\}\\(\boldsymbol{\delta}-1,2)\end{array} & & \begin{array}{c}\{1,2,4\},\{3\}\\(\boldsymbol{\delta},2)\end{array} &
\end{tikzcd}$$

This graph encodes the block stratification of the two-dimensional base scheme $\mathrm{Spec}(\mathbb{Z}[\boldsymbol{\delta}])$, along with the block structures on the strata. We see that $\mathrm{BlEx}(A)$ has four components of codimension 1, the generic points of these components are 3, $\delta-1$, 2, and $\delta+2$, respectively. The block structure on any other point $\mathfrak{p}$ is uniquely determined as the meet of the block structures on the components of $\mathrm{BlEx}(A)$ containing $\mathfrak{p}$.

We want to point out that it is central for us to work with (affine) schemes. For example, we have one skeleton with generic point (2); i.e., we consider the Brauer algebra in characteristic 2. Now, we do not only have the case $\boldsymbol{\delta} \in \{0, 1\} = \mathbb{F}_2$, which is described by the two strata below (2), but we also have a generic characteristic-2 case, described by the generic point of $\mathbb{F}_2[\boldsymbol{\delta}]$, and this is really different from the case of specialized $\boldsymbol{\delta}$, as we can see from the block structures.

Note that the components of $\mathrm{BlEx}(A)$ are precisely the parameters where the Brauer algebra is not semisimple anymore (the precise parameters have been determined by Rui [2005] for all $n \in \mathbb{N}$). We show in Lemma 6.7 that this is always the case for cellular algebras.

1E. ***Blocks and decomposition matrices.*** In Section 6 we address questions about the simple modules in a block. The main tool here is the decomposition matrices introduced by Geck and Rouquier. In Theorem 6.2 we show that they satisfy Brauer reciprocity in a rather general setting in which it was not known to hold before. In Section 6C we generalize the concept of Brauer graphs and show how these relate to blocks.

1F. ***An open problem.*** In Section 6B we contrast the preservation of simple modules with the preservation of blocks under specialization, and this leads to an interesting problem: In [Thiel 2016] we showed that decomposition matrices of A

are trivial precisely on an open subset $\mathrm{DecGen}(A)$ of $\mathrm{Spec}(R)$. In Theorem 6.3 we show

$$\mathrm{DecGen}(A) \subseteq \mathrm{BlGen}(A).$$

The obvious question is: are these two sets equal, and if not, when are they equal? We show in Example 6.5 that in general we do not have equality. In Lemma 6.7, on the other hand, we establish a context where we have equality (this includes Brauer algebras and explains why our Weil divisor is given by the nonsemisimple parameters). It is an open problem to understand the complement $\mathrm{BlGen}(A) \setminus \mathrm{DecGen}(A)$.

1G. ***Semicontinuity of blocks in the case of a nonsplit generic fiber.*** In Section 7 we consider the case of a nonsplit generic fiber. In this case we can no longer identify blocks of specializations with blocks of localizations, and so there is no natural way of comparing block structures among the fibers. However, it still makes sense to compare the *number* of blocks of the fibers, i.e., to consider the map $\mathrm{Spec}(R) \to \mathbb{N}$, $\mathfrak{p} \mapsto \#\mathrm{Bl}(A(\mathfrak{p}))$. In the case R is normal and A^K splits, this map is lower semicontinuous by the results discussed above. Without the splitting of A^K, this is no longer true; see Example 7.4. The problem is that we consider this map on all of $\mathrm{Spec}(R)$. In Corollary 7.1 we construct a setting in which the restriction of $\mathfrak{p} \mapsto \#\mathrm{Bl}(A(\mathfrak{p}))$ to certain subsets of $\mathrm{Spec}(R)$ is still lower semicontinuous without assuming that the generic fiber splits. From this we obtain a rather nice result; see Corollary 7.3:

Theorem 1.6. *Suppose that R is a finite-type algebra over an algebraically closed field. Let X be the set of closed points of* $\mathrm{Spec}(R)$. *Then the map $X \to \mathbb{N}$, $\mathfrak{m} \mapsto \#\mathrm{Bl}(A(\mathfrak{m}))$, is lower semicontinuous. In particular, X admits a stratification according to the number of blocks of fibers of A over X.*

1H. ***Remark.*** The behavior of blocks under specialization has been studied in several situations already. All of our results are well known in modular representation theory of finite groups due to the work of R. Brauer and C. Nesbitt [1941]. Our Corollary 4.3 and Theorem 6.9 generalize results by S. Donkin and R. Tange [2010] about algebras over Dedekind domains. Our results about lower semicontinuity of the number of blocks generalize a result by P. Gabriel [1975] to mixed characteristic and nonalgebraically closed settings; see also the corresponding result by I. Gordon [2001]. In general, K. Brown and I. Gordon [2001; 2002] used Müller's theorem [1976] to study blocks under specialization. Theorem 5.8 has been treated in a more special setting by K. Brown and K. Goodearl [2002]. The codimension-1 property in Corollary 4.3 and Theorem 5.9 was proven by C. Bonnafé and R. Rouquier [2017] in a more special setting. Their work is without doubt one of the main motivations for this paper. Blocks and decomposition matrices of generically semisimple algebras over discrete valuation rings have been studied by M. Geck and G. Pfeiffer [2000], and more generally by M. Chlouveraki [2009]. Brauer reciprocity has been studied more generally by M. Geck and R. Rouquier [1997], and by M. Neunhöffer [2003]. M. Neunhöffer and S. Scherotzke [2008] showed generic triviality of $\mathrm{e}_A^{\mathfrak{p}}$ over Dedekind domains.

2. Base change of blocks

The basic principle underlying the behavior of blocks in a family of algebras is *base change* of blocks. In this section, we introduce a few basic notions about this principle. Appendix A contains some further material which will later be used in some proofs.

Let us fix some basic notation for block theory. For us, a *ring* is always a ring with identity and a *module* is always a *left* module unless we explicitly say it is a *right* module. Let A be a ring and let Z be its center. If c is a central idempotent of A, then $Ac = cA$ is a two-sided ideal of A and at the same time a ring with identity element equal to c (so, not a subring). This yields a bijection between the set of decompositions of $1 \in A$ into a sum of pairwise orthogonal central idempotents and finite direct sum decompositions of the ring A into nonzero two-sided ideals of A up to permutation of the summands. Such decompositions are in turn in bijection with finite direct product decompositions of the ring A into nonzero rings up to permutation of the factors. Primitive idempotents of Z are also called *centrally primitive* idempotents of A. A central idempotent c is centrally primitive if and only if Ac is an indecomposable ring. It is a standard fact — and the starting point of block theory — that if there is a decomposition of $1 = \sum_i c_i$ into pairwise orthogonal centrally primitive idempotents c_i, then this is unique and any central idempotent of A is a sum of a subset of the c_i. We then say that A has a *block decomposition*, call the centrally primitive idempotents of A also the *block idempotents*, and call the corresponding rings Ac the *blocks* of A. We denote by $\mathrm{Bl}(A)$ the set of centrally primitive idempotents of A. To avoid pathologies we set $\mathrm{Bl}(0) := \varnothing$ for the zero ring 0. It is well known that noetherian rings have block decompositions (the block idempotents are the class sums with respect to the linkage relation of a decomposition of $1 \in A$ into pairwise orthogonal primitive idempotents).

Let $\mathscr{C} := \{c_i\}_{i \in I}$ be a finite set of pairwise orthogonal central idempotents whose sum is equal to $1 \in A$. Let $B_i := Ac_i$. If V is a nonzero A-module, then $V = \bigoplus_{i \in I} c_i V$ as A-modules and each summand $c_i V$ is a B_i-module. In this way we obtain a decomposition $A\text{-Mod} = \bigoplus_{i \in I} B_i\text{-Mod}$ of module categories, which also restricts to a decomposition of the category of finitely generated modules. If a nonzero A-module V is under this decomposition obtained from a B_i-module, then V is said to *belong* to B_i. This is equivalent to $c_i V = V$ and $c_j V = 0$ for all $j \neq i$. An indecomposable A-module clearly belongs to a unique B_i, and so this is true for any simple A-module. We thus get a decomposition $\operatorname{Irr} A = \coprod_{i \in I} \operatorname{Irr} B_i$ of the set of (isomorphism classes of) simple modules. We call the sets $\operatorname{Irr} B_i$ the *$\mathscr{C}$-families* of A and denote the set of $\mathscr{C}$-families by $\operatorname{Fam}_{\mathscr{C}}(A)$. Note that we have a natural bijection

$$\mathscr{C} \xrightarrow{\sim} \operatorname{Fam}_{\mathscr{C}}(A) \tag{3}$$

given by $c_i \mapsto \operatorname{Irr} B_i$. In the case $\mathscr{C}$ is actually a block decomposition, we call the $\mathscr{C}$-families simply the *families* of A and set $\operatorname{Fam}(A) := \operatorname{Fam}_{\mathscr{C}}(A)$. Recall that any central idempotent of A is a sum of a subset of the block idempotents of A. Hence, for general $\mathscr{C}$ as above the families are a finer partition of $\operatorname{Irr} A$ than the $\mathscr{C}$-families; i.e., any $\mathscr{C}$-family is a union of families.

Now, consider a morphism $\phi : R \to S$ of commutative rings. If V is an R-module, we write

$$V^S := \phi^* V := S \otimes_R V$$

for the scalar extension of V to S and by $\phi_V : V \to V^S$ we denote the canonical map $v \mapsto 1 \otimes v$. In most situations we consider, this map will be injective:

Lemma 2.1. *In each of the following cases the map $\phi_V : V \to V^S$ is injective*:

(a) *ϕ is injective and V is R-projective.*

(b) *ϕ is faithfully flat.*

(c) *ϕ is the localization morphism for a multiplicatively closed subset $\Sigma \subseteq R$ and V is Σ-torsion-free.*

Proof. The first case follows from [Bourbaki 1989, II, §5.1, Corollary to Proposition 4], the second follows from [Bourbaki 1972, I, §3.5, Proposition 8(i,iii)], and the last case follows from the fact that ϕ is flat in conjunction with [Bourbaki 1972, I, §2.2, Proposition 4]. □

If A is an R-algebra, then the S-module A^S is naturally an S-algebra and the map $\phi_A : A \to A^S$ is a ring morphism. Moreover, if V is an A-module, then the underlying S-module of $A^S \otimes_A V$ is simply V^S. Our aim is to study the behavior of blocks under the morphism $\phi_A : A \to A^S$. Clearly, if $e \in A$ is an idempotent, also $\phi_A(e) \in A^S$ is an idempotent, and if e is central, so is $\phi_A(e)$ by the elementary fact

$$\phi_A(\mathrm{Z}(A)) \subseteq \mathrm{Z}(A^S). \tag{4}$$

Definition 2.2. We say that ϕ_A is (central) *idempotent stable* if $\phi_A(e) \neq 0$ for any nonzero (central) idempotent e of A. We say that ϕ_A is *block bijective* if ϕ_A induces a bijection between the centrally primitive idempotents of A and the centrally primitive idempotents of A^S.

Note that in the case ϕ_A is idempotent stable, respectively central idempotent stable, it induces a map between the sets of decompositions of $1 \in A$ and $1 \in A^S$

into pairwise orthogonal idempotents, respectively into pairwise orthogonal central idempotents. The following lemma shows two situations in which ϕ_A is idempotent stable (and thus central idempotent stable). We denote by $\mathrm{Rad}(A)$ the Jacobson radical of A.

Lemma 2.3. *If* $\mathrm{Ker}(\phi_A) \subseteq \mathrm{Rad}(A)$, *then ϕ_A is idempotent stable. This holds in the following two cases*:

(a) *ϕ_A is injective* (*see Lemma 2.1*),

(b) *ϕ is surjective*, $\mathrm{Ker}(\phi) \subseteq \mathrm{Rad}(R)$, *and A is finitely generated as an R-module.*

Proof. If $e \in A$ is an idempotent contained in $\mathrm{Rad}(A)$, then by a well-known characterization of the Jacobson radical, see [Curtis and Reiner 1981, 5.10], we conclude that $e^\dagger = 1 - e \in A^\times$ is a unit, and since $e^\dagger$ is also an idempotent, we must have $e^\dagger = 1$, implying that $e = 0$. If ϕ_A is injective, the condition clearly holds. In the second case we have $\mathrm{Ker}(\phi_A) = \mathrm{Ker}(\phi)A \subseteq \mathrm{Rad}(R)A \subseteq \mathrm{Rad}(A)$, where the last inclusion follows from [Lam 1991, Corollary 5.9]. □

Suppose that ϕ_A is idempotent stable and that both A and A^S have block decompositions. Let $\{c_i\}_{i\in I}$ be the block idempotents of A and let $\{c'_j\}_{j\in J}$ be the block idempotents of A^S. Since ϕ_A is idempotent stable, the set $\mathrm{Bl}_\phi(A^S) := \phi_A(\{c_i\}_{i\in I})$ is a decomposition of $1 \in A^S$ into pairwise orthogonal idempotents. We call the $\phi_A(c_i)$ the *ϕ-blocks* of A^S and call the corresponding families (see above) the *ϕ-families* of A^S, denoted by $\mathrm{Fam}_\phi(A^S)$. As explained above, each ϕ-block $\phi_A(c_i)$ is a sum of a subset of the block idempotents of A^S and the ϕ-families are coarser than the families in the sense that each ϕ-family is a union of A^S-families. In particular, we have

$$\#\,\mathrm{Bl}(A) = \#\,\mathrm{Bl}_\phi(A^S) \le \#\,\mathrm{Bl}(A^S). \tag{5}$$

The following picture illustrates this situation:

$$
\begin{array}{ccccc}
\underset{c'_{1_1}}{\bullet}\ \underset{c'_{1_2}}{\bullet}\cdots\ \underset{c'_{1_{m_1}}}{\bullet} & \underset{c'_{2_1}}{\bullet}\ \underset{c'_{2_2}}{\bullet}\cdots\ \underset{c'_{2_{m_2}}}{\bullet} & \cdots & \underset{c'_{n_1}}{\bullet}\ \underset{c'_{n_2}}{\bullet}\cdots\ \underset{c'_{n_{m_n}}}{\bullet} & A^S\text{-blocks} \\
\nwarrow\ \uparrow\ \nearrow & \nwarrow\ \uparrow\ \nearrow & & \nwarrow\ \uparrow\ \nearrow & \\
\underset{\phi_A(c_1)}{\bullet} & \underset{\phi_A(c_2)}{\bullet} & \cdots & \underset{\phi_A(c_n)}{\bullet} & \phi\text{-blocks} \\
\phi_A \big\uparrow & \phi_A \big\uparrow & & \phi_A \big\uparrow & \\
\underset{c_1}{\bullet} & \underset{c_2}{\bullet} & \cdots & \underset{c_n}{\bullet} & A\text{-blocks}
\end{array}
\tag{6}
$$

This paper is about this picture in the special case of specializations of an algebra in prime ideals. Before we begin investigating this, we record the following useful fact.

Lemma 2.4. *Suppose that $\phi_A : A \to A^S$ is central idempotent stable. If A^S has a block decomposition*, *then A has a block decomposition.*

Proof. If A does not contain any nontrivial central idempotent, then A is indecomposable and thus has a block decomposition. So, assume that A is not indecomposable and let c be a nontrivial central idempotent. Then $A = Ac \oplus Ac^\dagger$. We can now continue this process to get finer and finer decompositions of A as a ring. Since ϕ_A is central idempotent stable, we get decompositions of A^S of the same size. As A^S has a block decomposition, this process has to end after finitely many steps. We thus arrive at a ring decomposition of A with finitely many and indecomposable factors, hence, at a block decomposition of A. □

Corollary 2.5. *A nonzero finite flat algebra over an integral domain has a block decomposition.*

Proof. Let R be an integral domain with fraction field K, let $\phi : R \hookrightarrow K$ be the embedding, and let A be a finite flat R-algebra. Since A is R-torsion-free, it follows from Lemma 2.1(c) that ϕ_A is injective and so ϕ_A is idempotent stable by Lemma 2.3(a). Since $\phi_A^* A = A^K$ is a finite-dimensional algebra over a field, it has a block decomposition. Hence, A has a block decomposition by Lemma 2.4. □

The point of the corollary above is that we do *not* have to assume R to be noetherian — otherwise A is noetherian and we already know it has a block decomposition.

3. Blocks of localizations

Before we consider blocks of specializations, we first take a look at blocks of localizations as these are much easier to control and are still strongly related to blocks of specializations as we will see in the next paragraph.

> ***Throughout the next paragraph, we assume A is a finite flat algebra over an integral domain R with fraction field K.***

It follows from Corollary 2.5 that A and any localization $A_\mathfrak{p}$ for $\mathfrak{p} \in \mathrm{Spec}(R)$ have a block decomposition, even if A is not necessarily noetherian. Since the canonical map $\phi_\mathfrak{p} : A_\mathfrak{p} \to A^K$ is injective by Lemma 2.1, we have the notion of $\phi_\mathfrak{p}$-blocks and $\phi_\mathfrak{p}$-families of A^K, as defined in Section 2. To shorten notations, we call them the $\mathfrak{p}$-*blocks* and $\mathfrak{p}$-*families*, and write $\mathrm{Fam}_\mathfrak{p}(A^K)$ for the $\mathfrak{p}$-families. Recall that we have a natural bijection

$$\mathrm{Bl}(A_\mathfrak{p}) \simeq \mathrm{Fam}_\mathfrak{p}(A^K). \tag{7}$$

3A. ***Block structure stratification.*** There is the following more concrete point of view of $\mathfrak{p}$-blocks. Let $(c_i)_{i \in I}$ be the block idempotents of A^K. If $c \in A_\mathfrak{p}$ is any block idempotent, we know from Section 2 that there is $I' \subseteq I$ with $c = \sum_{i \in I'} c_i$ in A^K. Hence, to any block idempotent of $A_\mathfrak{p}$ we can associate a subset of I, and if we take all block idempotents of $A_\mathfrak{p}$ into account, we get a partition $\mathrm{Bl}_A(\mathfrak{p})$ of the set I, from which we can recover the block idempotents of $A_{\mathfrak{p}}$ by taking sums of the c_i over the members of $\mathrm{Bl}_A(\mathfrak{p})$. In this way we get a map

$$\mathrm{Bl}_A : \mathrm{Spec}(R) \to \mathrm{Part}(I) \tag{8}$$

to the set of partitions of the set I. We denote by

$$\mathrm{Bl}(A) := \mathrm{Im}\,\mathrm{Bl}_A \tag{9}$$

the image of this map and call the partitions therein the *block structures* of A.

The set $\mathrm{Part}(I)$ is equipped with the partial order $\leq$ defined by $\mathscr{P} \leq \mathscr{Q}$ if $\mathscr{P}$ is a coarser partition than $\mathscr{Q}$, i.e., the members of $\mathscr{P}$ are unions of members of $\mathscr{Q}$. If $\mathfrak{q} \subseteq \mathfrak{p}$, then we have an embedding $A_{\mathfrak{p}} \hookrightarrow A_{\mathfrak{q}}$ and by the same argument as above, the block idempotents of $A_{\mathfrak{p}}$ are obtained by summing up block idempotents of $A_{\mathfrak{q}}$, so

$$\mathfrak{q} \subseteq \mathfrak{p} \implies \mathrm{Bl}_A(\mathfrak{p}) \leq \mathrm{Bl}_A(\mathfrak{q}). \tag{10}$$

Hence, the map Bl_A is actually a morphism of posets if we equip $\mathrm{Spec}(R)$ with the partial order $\leq$ defined by $\mathfrak{p} \leq \mathfrak{q}$ if $\mathfrak{q} \subseteq \mathfrak{p}$ (i.e., $\mathrm{V}(\mathfrak{p}) \subseteq \mathrm{V}(\mathfrak{q})$).

For $\mathscr{P} \in \mathrm{Part}(I)$, we call the fiber $\mathrm{Bl}_A^{-1}(\mathscr{P}) \subseteq \mathrm{Spec}(R)$ the *$\mathscr{P}$-stratum* and

$$\mathrm{Bl}_A^{-1}(\leq\mathscr{P}) := \bigcup_{\mathscr{P}' \leq \mathscr{P}} \mathrm{Bl}_A^{-1}(\mathscr{P}') = \bigcup_{\substack{\mathscr{P}' \leq \mathscr{P} \\ \mathscr{P}' \in \mathrm{Bl}(A)}} \mathrm{Bl}_A^{-1}(\mathscr{P}') \tag{11}$$

the *$\mathscr{P}$-skeleton*. The $\mathscr{P}$-stratum ($\mathscr{P}$-skeleton) is simply the locus of all $\mathfrak{p} \in \mathrm{Spec}(R)$ where the block structure of $A_{\mathfrak{p}}$ is equal to $\mathscr{P}$ (respectively coarser than $\mathscr{P}$). Since

$$\mathrm{Bl}_A^{-1}(\mathscr{P}) = \mathrm{Bl}_A^{-1}(\leq\mathscr{P}) \setminus \bigcup_{\mathscr{P}' < \mathscr{P}} \mathrm{Bl}_A^{-1}(\leq\mathscr{P}'), \tag{12}$$

we can recover the strata from the skeleta. We get the finite decomposition

$$\mathrm{Spec}(R) = \coprod_{\mathscr{P}} \mathrm{Bl}_A^{-1}(\mathscr{P}) \tag{13}$$

and we call this the *block structure stratification*. Our aim is now to show that this is indeed a stratification, i.e., the strata are *locally closed* subsets of $\mathrm{Spec}(R)$ and the closure of a stratum is contained in its skeleton. The key ingredient in proving this is the following general proposition, which is essentially due to Bonnafé and Rouquier [2017, Proposition D.2.11] but is proven here in a more general form.

Proposition 3.1. *Let R be an integral domain with fraction field K, let A be a finite flat R-algebra, and let $\mathscr{F} \subseteq A^K$ be a finite set. Then*

$$\mathrm{Gen}_A(\mathscr{F}) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathscr{F} \subseteq A_{\mathfrak{p}}\}$$

*is a **neighborhood** of the generic point of* $\mathrm{Spec}(R)$. *If A is finitely presented flat, then* $\mathrm{Gen}_A(\mathscr{F})$ *is an **open** subset of* $\mathrm{Spec}(R)$, *and if moreover R is a Krull domain, the complement* $\mathrm{Ex}_A(\mathscr{F})$ *of* $\mathrm{Gen}_A(\mathscr{F})$ *in* $\mathrm{Spec}(R)$ *is a **reduced Weil divisor**, i.e., it is either empty or pure of codimension* 1 *with finitely many irreducible components.*

Proof. Let us first assume that A is actually R-free. For an element $\alpha \in K$ we define $I_\alpha := \{r \in R \mid r\alpha \in R\}$. This is a nonzero ideal in R, and it has the property that $\alpha \in R_\mathfrak{p}$ if and only if $I_\alpha \nsubseteq \mathfrak{p}$. To see this, suppose that $\alpha \in R_\mathfrak{p}$. Then we can write $\alpha = r/x$ for some $x \in R \setminus \mathfrak{p}$. Hence, $x\alpha = r \in R$ and therefore $x \in I_\alpha$. Since $x \notin \mathfrak{p}$, it follows that $I_\alpha \nsubseteq \mathfrak{p}$. Conversely, if $I_\alpha \nsubseteq \mathfrak{p}$, then there exists $x \in I_\alpha$ with $x \notin \mathfrak{p}$. By the definition of I_α we have $x\alpha =: r \in R$ and since $x \notin \mathfrak{p}$, we can write $\alpha = r/x \in R_\mathfrak{p}$. Now, let $(a_1, \dots, a_n)$ be an R-basis of A. Then we can write every element $f \in \mathscr{F}$ as $f = \sum_{i=1}^n \alpha_{f,i} a_i$ with $\alpha_{f,i} \in K$. Let I be the radical of the ideal

$$\prod_{f \in \mathscr{F},\, i=1,\dots,n} I_{\alpha_{f,i}} \trianglelefteq R.$$

By the properties of the ideals I_α we have the following logical equivalences:

$$\begin{aligned} \mathscr{F} \subseteq A_\mathfrak{p} &\iff \alpha_{f,i} \in R_\mathfrak{p} \quad \text{for all } f \in \mathscr{F},\ i = 1, \dots, n \\ &\iff I_{\alpha_{f,i}} \nsubseteq \mathfrak{p} \quad \text{for all } f \in \mathscr{F},\ i = 1, \dots, n \\ &\iff I \nsubseteq \mathfrak{p}, \end{aligned}$$

the last equivalence following from the fact that $\mathfrak{p}$ is prime. Hence,

$$\mathrm{Ex}_A(\mathscr{F}) = \mathrm{Spec}(R) \setminus \mathrm{Gen}_A(\mathscr{F}) = \mathrm{V}(I) = \bigcup_{f \in \mathscr{F},\, i=1,\dots,n} \mathrm{V}(I_{\alpha_{f,i}}), \tag{14}$$

implying that $\mathrm{Gen}_A(\mathscr{F})$ is an open subset of $\mathrm{Spec}(R)$.

Next, still assuming that A is R-free, suppose that R is a Krull domain. To show that $\mathrm{Ex}_A(\mathscr{F})$ is either empty or pure of codimension 1 in $\mathrm{Spec}(R)$ with finitely many irreducible components, it suffices to show this for the closed subsets $\mathrm{V}(I_\alpha) = \mathrm{V}(\sqrt{I}_\alpha)$. If $\alpha \in R$, then $I_\alpha = R$ and therefore $\mathrm{V}(I_\alpha) = \varnothing$. So, let $\alpha \notin R$. Let $\mathrm{V}(I_\alpha) = \bigcup_{\lambda \in \Lambda} \mathrm{V}(\mathfrak{q}_\lambda)$ be the decomposition into irreducible components. Note that this decomposition is unique and contains every irreducible component of $\mathrm{V}(I_\alpha)$. The inclusion $\mathrm{V}(I_\alpha) \supseteq \mathrm{V}(\mathfrak{q}_\lambda)$ is equivalent to $I_\alpha \subseteq \sqrt{I_\alpha} \subseteq \sqrt{\mathfrak{q}_\lambda} = \mathfrak{q}_\lambda$. Since an irreducible component is a maximal proper closed subset, we see that the $\mathfrak{q}_\lambda$ are the minimal prime ideals of $\mathrm{Spec}(R)$ containing I_α. Let $\mathfrak{q} = \mathfrak{q}_\lambda$ for an arbitrary $\lambda \in \Lambda$. We will show that $\mathrm{ht}(\mathfrak{q}) = 1$. Since $I_\alpha \subseteq \mathfrak{q}$, we have seen above that $\alpha \notin R_\mathfrak{q}$. As R is a Krull domain, also $R_\mathfrak{q}$ is a Krull domain by [Matsumura 1986, Theorem 12.1]. By [Bourbaki 1972, VII, §1.6, Theorem 4] we have

$$R_\mathfrak{q} = \bigcap_{\substack{\mathfrak{q}' \in \mathrm{Spec}(R_\mathfrak{q}) \\ \mathrm{ht}(\mathfrak{q}')=1}} (R_\mathfrak{q})_{\mathfrak{q}'} = \bigcap_{\substack{\mathfrak{q}' \in \mathrm{Spec}(R) \\ \mathfrak{q}' \subseteq \mathfrak{q} \\ \mathrm{ht}(\mathfrak{q}')=1}} R_{\mathfrak{q}'}.$$

Since $\alpha \notin R_\mathfrak{q}$, this shows that there exists $\mathfrak{q}' \in \mathrm{Spec}(R)$ with $\mathfrak{q}' \subseteq \mathfrak{q}$, $\mathrm{ht}(\mathfrak{q}') = 1$ and $\alpha \notin R_{\mathfrak{q}'}$. The last property implies $I_\alpha \subseteq \mathfrak{q}'$ and now the minimality in the choice of $\mathfrak{q}$

implies that $\mathfrak{q}' = \mathfrak{q}$. Hence, $\mathrm{ht}(\mathfrak{q}) = 1$ and this shows $\mathrm{V}(I_\alpha)$ is pure of codimension 1. Since $I_\alpha \neq 0$, there is some $0 \neq r \in I_\alpha$. This element is contained in all the height-1 prime ideals $\mathfrak{q}_\lambda$. As R is a Krull domain, a nonzero element of R can only be contained in finitely many height-1 prime ideals, see [Huneke and Swanson 2006, 4.10.1], so Λ must be finite.

Now, assume that R is an arbitrary integral domain and that A is finite flat. Then Grothendieck's generic freeness lemma [1965, Lemme 6.9.2] shows that there exists a nonzero $f \in R$ such that A_f is a free R_f-module. Note that $\mathrm{Spec}(R_f)$ can be identified with the distinguished open subset $\mathrm{D}(f)$ of $\mathrm{Spec}(R)$. We obviously have

$$\mathrm{Gen}_{A_f}(\mathscr{F}) = \mathrm{Gen}_A(\mathscr{F}) \cap \mathrm{D}(f).$$

By the arguments above, $\mathrm{Gen}_{A_f}(\mathscr{F})$ is an open subset of $\mathrm{D}(f)$, and thus of $\mathrm{Spec}(R)$. This shows that $\mathrm{Gen}_A(\mathscr{F})$ is a neighborhood in $\mathrm{Spec}(R)$.

Next, let R be arbitrary and assume that A is finitely presented flat. It is a standard fact, see [Stacks 2005–, Tag 00NX], that the assumptions on A imply that A is already finite locally free; i.e., there exists a family $(f_i)_{i \in I}$ of elements of R such that the standard open affines $\mathrm{D}(f_i)$ cover $\mathrm{Spec}(R)$ and A_{f_i} is a finitely generated free R_{f_i}-module for all $i \in I$. Since $\mathrm{Spec}(R)$ is quasicompact, see [Görtz and Wedhorn 2010, Proposition 2.5], we can assume that I is finite. Again note that $\mathrm{Spec}(R_{f_i})$ can be identified with $\mathrm{D}(f_i)$ and that

$$\mathrm{Gen}_{A_{f_i}}(\mathscr{F}) = \mathrm{Gen}_A(\mathscr{F}) \cap \mathrm{D}(f_i). \tag{15}$$

By the above, the set $\mathrm{Gen}_{A_{f_i}}(\mathscr{F})$ is open and since the $\mathrm{D}(f_i)$ cover $\mathrm{Spec}(R)$, it follows that $\mathrm{Gen}_A(\mathscr{F})$ is open. Now, suppose that R is a Krull domain. Much as in (15) we have

$$\mathrm{Ex}_{A_{f_i}}(\mathscr{F}) = \mathrm{Ex}_A(\mathscr{F}) \cap \mathrm{D}(f_i). \tag{16}$$

Suppose that $\mathrm{Ex}_A(\mathscr{F})$ is not empty and let Z be an irreducible component of $\mathrm{Ex}_A(\mathscr{F})$. There is an $i \in I$ with $Z \cap \mathrm{D}(f_i) \neq \varnothing$. The map $T \mapsto \overline{T}$ defines a bijection between irreducible closed subsets of $\mathrm{D}(f_i)$ and irreducible closed subsets of $\mathrm{Spec}(R)$ which meet $\mathrm{D}(f_i)$; see [Görtz and Wedhorn 2010, §1.5]. This implies that $Z \cap \mathrm{D}(f_i)$ is an irreducible component of $\mathrm{Ex}_A(\mathscr{F}) \cap \mathrm{D}(f_i) = \mathrm{Ex}_{A_{f_i}}(\mathscr{F})$. It follows from the above that $Z \cap \mathrm{D}(f_i)$ is of codimension 1 in $\mathrm{D}(f_i)$. Hence, Z is of codimension 1 in $\mathrm{Spec}(R)$ by [Stacks 2005–, Tag 02I4]. All irreducible components of $\mathrm{Ex}_A(\mathscr{F})$ are thus of codimension 1 in $\mathrm{Spec}(R)$. Since each set $\mathrm{Ex}_{A_{f_i}}(\mathscr{F})$ has only finitely many irreducible components and since I is finite, also $\mathrm{Ex}_A(\mathscr{F})$ has only finitely many irreducible components. □

Remark 3.2. We note that A is finitely presented flat if and only if it is finite projective; see [Lam 1999, Theorem 4.30; Stacks 2005–, Tag 058R]. Hence, we could have equally assumed that A is finite projective in Proposition 3.1 but we preferred the seemingly more general notion.

From now on, we assume that A is finitely presented as an R-module.

For $\mathfrak{p} \in \operatorname{Spec}(R)$ let us denote by $\mathscr{B}_A(\mathfrak{p}) \subseteq A^K$ the set of block idempotents of $A_\mathfrak{p}$. Clearly, $\mathscr{B}_A(\mathfrak{p})$ and $\mathrm{Bl}_A(\mathfrak{p})$ are in bijection by taking sums of the c_i over the subsets in $\mathrm{Bl}_A(\mathfrak{p})$. Note that $\mathscr{B}_A(\mathfrak{p})$ is constant on $\mathrm{Bl}_A^{-1}(\mathscr{P})$ for any $\mathscr{P}$. We can thus define $\mathrm{Gen}_A(\mathscr{P}) := \mathrm{Gen}_A(\mathscr{B}_A(\mathfrak{p}))$ where $\mathfrak{p} \in \mathrm{Bl}_A^{-1}(\mathscr{P})$ is arbitrary.

Theorem 3.3. *Then* $\mathrm{Bl}_A^{-1}(\mathscr{P})$ *is a closed subset of* $\operatorname{Spec}(R)$ *for any partition* $\mathscr{P}$. *Thus, each stratum* $\mathrm{Bl}_A^{-1}(\mathscr{P})$ *is* ***open*** *in* $\mathrm{Bl}_A^{-1}(\leq \mathscr{P})$, *and hence* ***locally closed*** *in* $\operatorname{Spec}(R)$, *and*

$$\overline{\mathrm{Bl}_A^{-1}(\mathscr{P})} \subseteq \mathrm{Bl}_A^{-1}(\leq \mathscr{P}). \tag{17}$$

In particular, the decomposition (13) is a ***stratification*** *of* $\operatorname{Spec}(R)$.

Proof. First, assume that $\mathscr{P}$ is actually a block structure, i.e., $\mathscr{P} \in \mathrm{Bl}(A)$. Since $\operatorname{Spec}(R) = \coprod_{\mathscr{P}'} \mathrm{Bl}_A^{-1}(\mathscr{P}')$, we have

$$\operatorname{Spec}(R) \setminus \mathrm{Bl}_A^{-1}(\leq \mathscr{P}) = \bigcup_{\mathscr{P}' \not\leq \mathscr{P}} \mathrm{Bl}_A^{-1}(\mathscr{P}').$$

Let $\mathscr{P}' \not\leq \mathscr{P}$ and $\mathfrak{p}' \in \mathrm{Gen}_A(\mathscr{P}')$. Then $\mathscr{P}' \leq \mathrm{Bl}_A(\mathfrak{p}')$. But this implies $\mathrm{Bl}_A(\mathfrak{p}') \not\leq \mathscr{P}$ since otherwise $\mathscr{P}' \leq \mathrm{Bl}_A(\mathfrak{p}') \leq \mathscr{P}$. Hence, $\mathrm{Gen}_A(\mathscr{P}') \subseteq \operatorname{Spec}(R) \setminus \mathrm{Bl}_A^{-1}(\leq \mathscr{P})$. Conversely, we clearly have $\mathrm{Bl}_A^{-1}(\mathscr{P}') \subseteq \mathrm{Gen}_A(\mathscr{P}')$. This shows that

$$\operatorname{Spec}(R) \setminus \mathrm{Bl}_A^{-1}(\leq \mathscr{P}) = \bigcup_{\mathscr{P}' \not\leq \mathscr{P}} \mathrm{Bl}_A^{-1}(\mathscr{P}') = \bigcup_{\mathscr{P}' \not\leq \mathscr{P}} \mathrm{Gen}_A(\mathscr{P}').$$

This set is open by Proposition 3.1, so

$$\mathrm{Bl}_A^{-1}(\leq \mathscr{P}) = \bigcap_{\mathscr{P}' \not\leq \mathscr{P}} \mathrm{Ex}_A(\mathscr{P}') \tag{18}$$

is closed. From (11) we see $\mathrm{Bl}_A^{-1}(\leq \mathscr{P})$ is also closed for an arbitrary partition $\mathscr{P}$. Using (12), we see $\mathrm{Bl}_A(\mathscr{P})$ is locally closed. Moreover, we have $\mathrm{Bl}_A^{-1}(\mathscr{P}) \subseteq \mathrm{Bl}_A^{-1}(\leq \mathscr{P})$, so

$$\overline{\mathrm{Bl}_A^{-1}(\mathscr{P})} \subseteq \overline{\mathrm{Bl}_A^{-1}(\leq \mathscr{P})} = \mathrm{Bl}_A^{-1}(\leq \mathscr{P}). \qquad \square$$

Remark 3.4. In general it is *not* true that we have $\overline{\mathrm{Bl}_A^{-1}(\mathscr{P})} = \mathrm{Bl}_A^{-1}(\leq \mathscr{P})$, so the stratification (13) is in general not a so-called *good* stratification: in the Brauer algebra example in the Introduction we have

$$\mathscr{P}' := \mathrm{Bl}_A((3)) = \{\{1,2,3\},\{4\}\} < \{\{1,2\},\{3\},\{4\}\} = \mathrm{Bl}_A((2)) =: \mathscr{P},$$

so $(3) \in \mathrm{Bl}_A^{-1}(\leq \mathscr{P})$, but (3) is not contained in $\overline{\mathrm{Bl}_A^{-1}(\mathscr{P})} = \mathrm{V}((2))$. The problem here is that the skeleton $\mathrm{Bl}_A^{-1}(\leq \mathscr{P})$ has an irreducible component on which the maximal block structure is strictly smaller than the maximal one on the entire skeleton.

The poset $\mathrm{Bl}(A)$ has a unique maximal element, namely the block structure $\mathrm{Bl}_A(\bullet)$ of A in the generic point $\bullet := (0)$ of $\mathrm{Spec}(R)$; i.e., $\mathrm{Bl}_A(\bullet) = \{\{i\} \mid i \in I\}$ is the block structure of the generic fiber $A^K = A_\bullet$. The deviation of block structures from the generic one thus takes place on the closed subset

$$\mathrm{BlEx}(A) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathrm{Bl}_A(\mathfrak{p}) < \mathrm{Bl}_A(\bullet)\} = \bigcup_{\mathscr{P} < \mathrm{Bl}_A(\bullet)} \mathrm{Bl}_A^{-1}(\leq \mathscr{P}). \tag{19}$$

We call this set the *block structure divisor* of A. In fact, since $\mathrm{BlEx}(A) = \mathrm{Ex}_A(\mathscr{B}_A(\bullet))$, Proposition 3.1 implies:

Corollary 3.5. *Suppose that R is a **Krull domain**. Then* $\mathrm{BlEx}(A)$ *is a reduced Weil divisor.*

The generic block structure lives precisely on the open dense subset

$$\begin{aligned} \mathrm{BlGen}(A) &:= \mathrm{Spec}(R) \setminus \mathrm{BlEx}(A) \\ &= \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathrm{Bl}_A(\mathfrak{p}) = \mathrm{Bl}_A(\bullet)\} = \mathrm{Bl}_A^{-1}(\bullet). \end{aligned} \tag{20}$$

3B. ***Block number stratification.*** From the map $\mathrm{Bl}_A : \mathrm{Spec}(R) \to \mathrm{Part}(I)$ we obtain the numerical invariant

$$\#\mathrm{Bl}_A : \mathrm{Spec}(R) \to \mathbb{N}, \quad \mathfrak{p} \mapsto \#\mathrm{Bl}_A(\mathfrak{p}) = \#\mathrm{Bl}(A_\mathfrak{p}). \tag{21}$$

This map is again a morphism of posets, so

$$\mathfrak{q} \subseteq \mathfrak{p} \implies \#\mathrm{Bl}_A(\mathfrak{p}) \leq \#\mathrm{Bl}_A(\mathfrak{q}). \tag{22}$$

For $n \in \mathbb{N}$ we have

$$\#\mathrm{Bl}_A^{-1}(n) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \#\mathrm{Bl}(A_\mathfrak{p}) = n\} \tag{23}$$

and we get the decomposition

$$\mathrm{Spec}(R) = \coprod_{n \in \mathbb{N}} \#\mathrm{Bl}_A^{-1}(n). \tag{24}$$

We call this the *block number stratification*. This decomposition is of course coarser than the one defined by the fibers of Bl_A. We define

$$\#\mathrm{Bl}_A^{-1}(\leq n) := \bigcup_{m \leq n} \#\mathrm{Bl}_A^{-1}(m) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \#\mathrm{Bl}(A_\mathfrak{p}) \leq n\}. \tag{25}$$

Since

$$\#\mathrm{Bl}_A^{-1}(\leq n) = \bigcup_{\#\mathscr{P} \leq n} \mathrm{Bl}_A^{-1}(\mathscr{P}), \tag{26}$$

this set is closed in $\mathrm{Spec}(R)$ by Theorem 3.3. This means that the map $\#\mathrm{Bl}_A : \mathrm{Spec}(R) \to \mathbb{N}$ is lower semicontinuous. Hence, $\#\mathrm{Bl}_A^{-1}(n)$ is open in $\#\mathrm{Bl}_A^{-1}(\leq n)$, thus locally closed in $\mathrm{Spec}(R)$, and

$$\overline{\#\mathrm{Bl}_A^{-1}(n)} \subseteq \#\mathrm{Bl}_A^{-1}(\leq n). \tag{27}$$

In particular, the partition (24) is a stratification of $\mathrm{Spec}(R)$. Again, in general it will not be a *good* stratification. Note that

$$\mathrm{BlEx}(A) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \#\mathrm{Bl}_A(\mathfrak{p}) < \#\mathrm{Bl}_A(\bullet)\} = \mathrm{Bl}_A^{-1}(\leq \#\mathrm{Bl}_A(\bullet) - 1). \tag{28}$$

3C. *Block stratification.* The poset $\mathrm{Part}(I)$ is actually a lattice; i.e., it has *meets* $\wedge$ and *joins* $\vee$. The meet $\mathscr{P} \wedge \mathscr{P}'$ of two partitions is the finest partition of I that is coarser than both $\mathscr{P}$ and $\mathscr{P}'$, and this is obtained by joining members with nonempty intersection. The maximal elements in $\mathrm{Part}(I)$ not equal to the maximal element itself (the trivial partition) are the partitions $\{i, j\} \cup (I \setminus \{i, j\})$ with $i \neq j$. We call these the *atoms* of $\mathrm{Part}(I)$ and we denote by $\mathrm{At}(I)$ the set of atoms. This terminology comes from the fact that an arbitrary partition $\mathscr{P}$ is the meet of all atoms lying above it:

$$\mathscr{P} = \bigwedge_{\substack{T \in \mathrm{At}(I) \\ \mathscr{P} \leq T}} T.$$

Because of this property, we say that $\mathrm{Part}(I)$ is *atomic*.

The poset of block structures of A has a similar atomic character. For $i, j \in I$ with $i \neq j$ let us write

$$\mathrm{Gl}_A(\{i, j\}) := \mathrm{Bl}_A^{-1}\big(\leq \{i, j\} \cup (I \setminus \{i, j\})\big). \tag{29}$$

This is the locus of all $\mathfrak{p} \in \mathrm{Spec}(R)$ such that the block idempotents c_i and c_j belong to the same block of $A_{\mathfrak{p}}$; i.e., they are "glued" over $\mathfrak{p}$. We thus call this set a *gluing locus*. By Theorem 3.3 it is a closed subset of $\mathrm{Spec}(R)$. It is clear that

$$\mathrm{BlEx}(A) = \bigcup_{i \neq j} \mathrm{Gl}_A(\{i, j\}). \tag{30}$$

Let $\mathrm{At}(A)$ be the set of maximal elements of the set of irreducible components of the gluing loci, ordered by inclusion. Then we still have

$$\mathrm{BlEx}(A) = \bigcup_{Z \in \mathrm{At}(A)} Z. \tag{31}$$

Lemma 3.6. *The $Z \in \mathrm{At}(A)$ are precisely the irreducible components of* $\mathrm{BlEx}(A)$.

Proof. Let Y be an irreducible component of $\mathrm{BlEx}(A)$ and let ξ be the generic point of Y. Since $\mathrm{Bl}_A(\xi)$ is not the trivial partition, there is $i \neq j$ with $\mathrm{Bl}_A(\xi) \leq \{i, j\} \cup (I \setminus \{i, j\})$. Hence, $Y \subseteq \mathrm{Gl}_A(\{i, j\})$. Since Y is a maximal irreducible closed subset of $\mathrm{BlEx}(A)$ and $\mathrm{Gl}_A(\{i, j\}) \subseteq \mathrm{BlEx}(A)$, it is also a maximal irreducible closed subset of $\mathrm{Gl}_A(\{i, j\})$, and thus equal to an irreducible component Z of $\mathrm{Gl}_A(\{i, j\})$. It is clear that $Z \in \mathrm{At}(A)$. Conversely, let $Z \in \mathrm{At}(A)$. Since $Z \subseteq \mathrm{BlEx}(A)$, there is an irreducible component Y of $\mathrm{BlEx}(A)$ containing Z. With the same argument as above, there is $Z' \in \mathrm{At}(A)$ with $Y \subseteq Z'$. Hence, $Z \subseteq Y \subseteq Z'$, and therefore $Z = Y$ by maximality of the elements in $\mathrm{At}(A)$. □

It now follows that for any $\mathfrak{p} \in \mathrm{Spec}(R)$ we have

$$\mathrm{Bl}_A(\mathfrak{p}) = \bigwedge_{\substack{\mathscr{P} \in \mathrm{At}(I) \\ \mathrm{Bl}_A(\mathfrak{p}) \leq \mathscr{P}}} \mathscr{P} = \bigwedge_{\substack{Z \in \mathrm{At}(A) \\ \mathfrak{p} \in Z}} \mathrm{Bl}_A(Z), \tag{32}$$

where $\mathrm{Bl}_A(Z)$ denotes the block structure in the generic point of Z, i.e., the unique maximal block structure on Z. Hence, any block structure of A is a meet of *atomic block structures* $\mathrm{Bl}_A(Z)$ for $Z \in \mathrm{At}(A)$. Recall from Corollary 3.5 that if R is a Krull domain, the $Z \in \mathrm{At}(A)$ are all of codimension 1 in $\mathrm{Spec}(R)$.

Following this observation, we introduce a refined stratification of $\mathrm{Spec}(R)$. For a subset $\mathscr{Z} \subseteq \mathrm{At}(I)$ we define

$$\mathrm{Bl}_A^{-1}(\leq \mathscr{Z}) := \bigcap_{Z \in \mathscr{Z}} Z, \tag{33}$$

$$\mathrm{Bl}_A^{-1}(\mathscr{Z}) := \bigcap_{Z \in \mathscr{Z}} Z \setminus \bigcup_{Z \in \mathrm{At}(A) \setminus \mathscr{Z}} Z. \tag{34}$$

It is clear that $\mathrm{Bl}_A^{-1}(\leq \mathscr{Z})$ is closed in $\mathrm{Spec}(R)$, that $\mathrm{Bl}_A^{-1}(\mathscr{Z})$ is locally closed in $\mathrm{Spec}(R)$ and that the block structure on $\mathrm{Bl}_A^{-1}(\mathscr{Z})$ is in any point equal to $\bigwedge_{Z \in \mathscr{Z}} \mathrm{Bl}_A(Z)$. Note that in this notation $\mathrm{Bl}_A^{-1}(\leq \varnothing) = \mathrm{Spec}(R)$ and

$$\mathrm{Bl}_A^{-1}(\varnothing) = \mathrm{Spec}(R) \setminus \bigcup_{Z \in \mathrm{At}(A)} Z = \mathrm{BlGen}(A). \tag{35}$$

Clearly,

$$\overline{\mathrm{Bl}_A^{-1}(\mathscr{Z})} \subseteq \bigcap_{Z \in \mathscr{Z}} Z = \mathrm{Bl}_A^{-1}(\leq \mathscr{Z}), \tag{36}$$

so we obtain the stratification

$$\mathrm{Spec}(R) = \coprod_{\mathscr{Z} \subseteq \mathrm{At}(A)} \mathrm{Bl}_A^{-1}(\mathscr{Z}) \tag{37}$$

refining the block structure stratification (13). We call this the *block stratification* of A.

4. Blocks of specializations

We now turn to our actual problem, namely blocks of specializations of A. Compared to blocks of localizations there is in general no possibility to compare the actual block structures of specializations. However, there is a rather general setting where blocks of specializations are naturally identified with blocks of localizations, namely when R is normal and A^K splits. In this case we can compare the actual block structures of specializations and all results from the preceding paragraph are actually also results about blocks of specializations. For the proof we need the following general result.

Theorem 4.1. *Let $\phi : R \hookrightarrow S$ be a faithfully flat morphism of integral domains and let A be a finite flat R-algebra. Let K and L be the fraction fields of R and S, respectively. If $\#\mathrm{Bl}(A^K) = \#\mathrm{Bl}(A^L)$, then the morphism $\phi_A : A \to A^S$ is block bijective.*

Proof. Recall from Corollary 2.5 that both A and A^S have block decompositions. The map $\phi_A : A \to A^S$ is injective by Lemma 2.1(b) since ϕ is faithfully flat. Hence, ϕ_A is idempotent stable by Lemma 2.3(a) and therefore $\#\mathrm{Bl}(A) \leq \#\mathrm{Bl}(A^S)$ by (5). We thus have to show that $\#\mathrm{Bl}(A) \geq \#\mathrm{Bl}(A^S)$. We split the proof of this fact into several steps.

The case $R = K$ and $S = L$ holds by assumption. Assume that $R = K$ and that S is general as in the theorem. Since A is R-flat, the extension A^S is S-flat and thus S-torsion-free. Hence, the map $A^S \to A^L$ is injective by Lemma 2.1(c). In particular, it is idempotent stable by Lemma 2.3(a) and so $\#\mathrm{Bl}(A^S) \leq \#\mathrm{Bl}(A^L)$ by (5). In total, we have

$$\#\mathrm{Bl}(A) \leq \#\mathrm{Bl}(A^S) \leq \#\mathrm{Bl}(A^L) = \#\mathrm{Bl}(A^K) = \#\mathrm{Bl}(A).$$

Hence, $\#\mathrm{Bl}(A) = \#\mathrm{Bl}(A^S)$.

Finally, let both R and S be general as in the theorem. Let $\Sigma := R \setminus \{0\}$ and $\Omega := S \setminus \{0\}$. Then $K = \Sigma^{-1}R$ and $L = \Omega^{-1}S$. Set $T := \Sigma^{-1}S$. Since R and S are integral domains, we can naturally view all rings as subrings of L and so we get the two commutative diagrams

$$\begin{tikzcd} & L & \\ & T \arrow[u, hook] & \\ K \arrow[uur, hook, bend left] \arrow[ur, hook] & & S \arrow[uul, hook', bend right] \arrow[ul, hook'] \\ & R \arrow[ul, hook'] \arrow[ur, hook] & \end{tikzcd} \qquad \begin{tikzcd} & A^L & \\ & A^T \arrow[u] & \\ A^K \arrow[uur, bend left] \arrow[ur] & & A^S \arrow[uul, bend right] \arrow[ul] \\ & A \arrow[ul] \arrow[ur] & \end{tikzcd} \tag{38}$$

the right one being induced by the left one. All morphisms in the left diagram are clearly injective. We claim the same holds for the right diagram. We have noted at the beginning that the map $A \to A^S$ is injective. Since A is R-flat, it is R-torsion-free and so the map $A \to A^K$ is injective by Lemma 2.1(c). We have argued above already that the map $A^S \to A^L$ is injective. Since $S \hookrightarrow T$ is a localization map, the induced scalar extension functor is exact so that A^T is a flat T-module. In particular, A^T is T-torsion-free and so $A^T \to A^L$ is injective by Lemma 2.1(c). The map $A^K \to A^L$ is injective by Lemma 2.1(a). Due to the commutativity of the diagram, the remaining maps must be injective, too. We can thus view all scalar extensions of A naturally as subsets of A^L. We claim that

$$A = A^K \cap A^S \tag{39}$$

as subsets of A^L. Because of the commutative diagram above, this intersection already takes place in A^T. Consider A^K as an R-module now. We have a natural identification

$$\begin{aligned}\phi^*(A^K) &= S \otimes_R A^K = S \otimes_R (\Sigma^{-1} A) \\ &= (\Sigma^{-1} S) \otimes_R A = T \otimes_R A = A^T\end{aligned}$$

as S-modules by [Bourbaki 1972, II, §2.7, Proposition 18]. Note that the map $A^K \to A^T$ in the diagram above is the map ϕ_{A^K}, when considering A^K as an R-module. The R-submodule A of A^K is now identified with $\phi_{A^K}(A)$ and the S-submodule of A^T generated by $A \subseteq A^T$ is identified with A^S. Since ϕ is faithfully flat, it follows from [Bourbaki 1972, I, §3.5, Proposition 10(ii)] applied to the R-module A^K and the submodule A that

$$A = A^K \cap A^S$$

inside A^T. Let $(c_i)_{i \in I}$ be the block idempotents of A^S and let $(d_j)_{j \in J}$ be the block idempotents of A^K. By assumption the morphism $A^K \to A^L$ is block bijective, which means that $(d_j)_{j \in J}$ are the block idempotents of A^L. Since $A^S \to A^L$ is idempotent stable, there exists by the arguments preceding (5) a partition $(J_i)_{i \in I}$ of J such that the nonzero central idempotent c_i can in A^L be written as $c_i = \sum_{j \in J_i} d_j$. But this shows that $c_i \in A^K \cap A^S$, hence $c_i \in A$ and so $(c_i)_{i \in I}$ gives a decomposition of $1 \in A$ into pairwise orthogonal centrally primitive idempotents of A by (39). Hence, $\# \mathrm{Bl}(A) = \# \mathrm{Bl}(A^S)$. □

To formulate the next proposition more generally, we use the property *block-split* introduced in Definition A.2 but note that the reader might just simply replace it by the more special property *split*. Moreover, we recall that a local integral domain R is called *unibranch* if its henselization R^h is again an *integral* (local) domain. This is equivalent to the normalization of R being again *local*; see [Raynaud 1970, IX, Corollaire 1]. This clearly holds if R is already *normal*. Examples of nonnormal unibranch rings are the local rings in ordinary cusp singularities of curves.

Proposition 4.2. *Let R be an integral domain and let A be a finite flat R-algebra with* ***block-split*** *generic fiber A^K (e.g., if A^K splits). Let $\mathfrak{p} \in \mathrm{Spec}(R)$ and suppose that $R_\mathfrak{p}$ is unibranch (e.g., if $R_\mathfrak{p}$ is normal). Then the quotient morphism $A_\mathfrak{p} \twoheadrightarrow A(\mathfrak{p})$ is block bijective.*

Proof. By assumption, $R_\mathfrak{p}$ and its henselization $R_\mathfrak{p}^h$ are integral domains. Since A is R-flat, it follows that $A_\mathfrak{p} = R_\mathfrak{p} \otimes_R A$ is $R_\mathfrak{p}$-flat and that $A_\mathfrak{p}^h := R_\mathfrak{p}^h \otimes_{R_\mathfrak{p}} A_\mathfrak{p}$ is $R_\mathfrak{p}^h$-flat. Hence, both $A_\mathfrak{p}$ and $A_\mathfrak{p}^h$ have block decompositions by Corollary 2.5. Let $\mathfrak{p}_\mathfrak{p}^h$ be the maximal ideal of $R_\mathfrak{p}^h$. The henselization morphism $R_\mathfrak{p} \to R_\mathfrak{p}^h$ is local and faithfully flat by [Grothendieck 1967, Théorème 18.6.6(iii)]. We now have the commutative diagram

$$\begin{array}{ccc} A_{\mathfrak{p}} & \hookrightarrow & A_{\mathfrak{p}}^h \\ \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow \\ A(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}A_{\mathfrak{p}} & \hookrightarrow & A_{\mathfrak{p}}^h/\mathfrak{p}_{\mathfrak{p}}^h A_{\mathfrak{p}}^h \end{array}$$

of idempotent stable morphisms. We know from Lemmas A.12(b) and A.10 that $A_{\mathfrak{p}}^h \to A_{\mathfrak{p}}^h/\mathfrak{p}_{\mathfrak{p}}^h A_{\mathfrak{p}}^h$ is block bijective. Since A has block-split generic fiber and $R_{\mathfrak{p}} \to R_{\mathfrak{p}}^h$ is a faithfully flat morphism of integral domains, we can use Theorem 4.1 to deduce that $A_{\mathfrak{p}} \to A_{\mathfrak{p}}^h$ is block bijective. In [Grothendieck 1967, Théorème 18.6.6(iii)] it is proven that $R_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}} \simeq R_{\mathfrak{p}}^h/\mathfrak{p}_{\mathfrak{p}}^h$. Hence, the map $A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}A_{\mathfrak{p}} \to A_{\mathfrak{p}}^h/\mathfrak{p}_{\mathfrak{p}}^h A_{\mathfrak{p}}^h$ is an isomorphism and so in particular block bijective. We thus have

$$\#\operatorname{Bl}(A_{\mathfrak{p}}^h) = \#\operatorname{Bl}(A_{\mathfrak{p}}) \le \#\operatorname{Bl}(A(\mathfrak{p})) = \#\operatorname{Bl}(A_{\mathfrak{p}}^h/\mathfrak{p}_{\mathfrak{p}}^h A_{\mathfrak{p}}^h) = \#\operatorname{Bl}(A_{\mathfrak{p}}^h)$$

by (5). Hence, $\#\operatorname{Bl}(A_{\mathfrak{p}}) = \#\operatorname{Bl}(A(\mathfrak{p}))$, so $A_{\mathfrak{p}} \twoheadrightarrow A(\mathfrak{p})$ is block bijective. □

Corollary 4.3. *Suppose that R is normal and A^K splits. Then $A_{\mathfrak{p}} \twoheadrightarrow A(\mathfrak{p})$ is block bijective for all $\mathfrak{p} \in \operatorname{Spec}(R)$. Hence, all results from Section 3 apply also to blocks of specializations of A.*

5. Blocks via central characters

In this section we discuss an approach to explicitly compute the block structure of A in any point $\mathfrak{p} \in \operatorname{Spec}(R)$, and so to compute the whole block stratification. This is based on the knowledge of the central characters of the generic fiber of A. Parts of the arguments presented here are due to Bonnafé and Rouquier [2017, Appendix D].

5A. ***Müller's theorem.*** The central ingredient to establish a relationship between blocks and central characters is the general Lemma 5.6 below, which is usually referred to as *Müller's theorem*. We were not able to find a proof of it in this generality in the literature, so we include a proof here but note that this is known. The main ingredient is an even more general result by B. Müller [1976] about the fibration of cliques of prime ideals in a noetherian ring over its center; see Lemma 5.5. We will recall only a few basic definitions from the excellent exposition in [Goodearl and Warfield 2004, §12] and refer to it for more details.

Throughout the next paragraph, we assume that A is a noetherian ring.

If $\mathfrak{p}$, $\mathfrak{q}$ are prime ideals of A, we say that there is a *link* from $\mathfrak{p}$ to $\mathfrak{q}$, written $\mathfrak{p} \rightsquigarrow \mathfrak{q}$, if there is an ideal $\mathfrak{a}$ of A such that $\mathfrak{p} \cap \mathfrak{q} \supsetneq \mathfrak{a} \supseteq \mathfrak{p}\mathfrak{q}$ and $(\mathfrak{p} \cap \mathfrak{q})/\mathfrak{a}$ is nonzero and torsion-free both as a left $(A/\mathfrak{p})$-module and as a right $(A/\mathfrak{q})$-module. The bimodule $(\mathfrak{p} \cap \mathfrak{q})/\mathfrak{q}$ is then called a *linking bimodule* between $\mathfrak{q}$ and $\mathfrak{p}$. The equivalence classes of the equivalence relation on $\operatorname{Spec}(A)$ generated by $\rightsquigarrow$ are called the *cliques* of A.

We write $\mathrm{Clq}(A)$ for the set of cliques of A and $\mathrm{Clq}(\mathfrak{p})$ for the unique clique of A containing $\mathfrak{p}$. For the proof of Lemma 5.6 we will need a few preparatory lemmas.

We call the supremum of lengths of chains of prime ideals in A the *classical Krull dimension* of A. The following lemma is standard.

Lemma 5.1. *Suppose that A is noetherian and of classical Krull dimension zero. Then there is a canonical bijection*

$$\begin{aligned} \mathrm{Bl}(A) &\xrightarrow{\sim} \mathrm{Clq}(A), \\ c &\longmapsto X_c := \{\mathfrak{m} \in \mathrm{Max}(A) \mid c^\dagger \in \mathfrak{m}\}, \end{aligned} \tag{40}$$

where $c^\dagger = 1 - c$. If moreover A is ***commutative****, then the cliques are singletons; i.e., there is a unique $\mathfrak{m}_c \in \mathrm{Max}(A)$ with $c^\dagger \in \mathfrak{m}_c$. Hence, in this case we have*

$$\mathrm{Bl}(A) \simeq \mathrm{Max}(A) \simeq \mathrm{Spec}(A).$$

Proof. The first assertion is proven in [Goodearl and Warfield 2004, Corollary 12.13]. In a commutative noetherian ring the cliques are singletons, see [loc. cit., Exercise 12F], and this immediately implies the second assertion. □

Lemma 5.2. *Let $\mathfrak{p}$ be a prime ideal of a noetherian ring A and let V be a nonzero A-module with $\mathfrak{p} \subseteq \mathrm{Ann}(V)$. If V is torsion-free as an $(A/\mathfrak{p})$-module, then $\mathfrak{p} = \mathrm{Ann}(V)$.*

Proof. Suppose that $\mathfrak{p} \subsetneq \mathrm{Ann}(V)$. Then $\mathrm{Ann}(V)/\mathfrak{p}$ is a nonzero ideal of the noetherian prime ring $A/\mathfrak{p}$ and thus contains a regular element $\bar{x}$ by [Jategaonkar 1986, Corollary 2.3.11]. But then $\bar{x}V = 0$, contradicting the assumption that V is a torsion-free $(A/\mathfrak{p})$-module. □

Lemma 5.3. *The following hold*:

(a) *If $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals of A and if $\mathfrak{b}$ is an ideal of A with $\mathfrak{b} \subseteq \mathfrak{p} \cap \mathfrak{q}$ such that $\mathfrak{p}/\mathfrak{b} \rightsquigarrow \mathfrak{q}/\mathfrak{b}$ in $A/\mathfrak{b}$, then $\mathfrak{p} \rightsquigarrow \mathfrak{q}$ in A.*

(b) *Let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals of A with $\mathfrak{p} \rightsquigarrow \mathfrak{q}$ and let $\mathfrak{b}$ be an ideal of A. If there exists a linking ideal $\mathfrak{a}$ from $\mathfrak{p}$ to $\mathfrak{q}$ with $\mathfrak{b} \subseteq \mathfrak{a}$, then $\mathfrak{p}/\mathfrak{b} \rightsquigarrow \mathfrak{q}/\mathfrak{b}$ in $A/\mathfrak{b}$.*

Proof. (a) We can write a linking ideal from $\mathfrak{p}/\mathfrak{b}$ to $\mathfrak{q}/\mathfrak{b}$ as $\mathfrak{a}/\mathfrak{b}$ for an ideal $\mathfrak{a}$ containing $\mathfrak{b}$. By definition, we have

$$(\mathfrak{p} \cap \mathfrak{q})/\mathfrak{b} = (\mathfrak{p}/\mathfrak{b}) \cap (\mathfrak{q}/\mathfrak{b}) \supsetneq \mathfrak{a}/\mathfrak{b} \supseteq (\mathfrak{p}/\mathfrak{b}) \cdot (\mathfrak{q}/\mathfrak{b}) = (\mathfrak{p}\mathfrak{q})/\mathfrak{b},$$

implying that $\mathfrak{p} \cap \mathfrak{q} \supsetneq \mathfrak{a} \supseteq \mathfrak{p}\mathfrak{q}$. Moreover, we have

$$((\mathfrak{p} \cap \mathfrak{q})/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b}) \cong (\mathfrak{p} \cap \mathfrak{q})/\mathfrak{a}$$

as $(A/\mathfrak{b})$-bimodules. By definition, $(\mathfrak{p} \cap \mathfrak{q})/\mathfrak{a}$ is torsion-free as a left module over the ring

$$(A/\mathfrak{b})/(\mathfrak{p}/\mathfrak{b}) \cong A/\mathfrak{p}.$$

Similarly, it follows that $(\mathfrak{p} \cap \mathfrak{q})/\mathfrak{a}$ is torsion-free as a right module over the ring $A/\mathfrak{q}$. Hence, $\mathfrak{a}$ is a linking ideal from $\mathfrak{p}$ to $\mathfrak{q}$.

(b) We have

$$\mathfrak{p}/\mathfrak{b} \cap \mathfrak{q}/\mathfrak{b} = (\mathfrak{p} \cap \mathfrak{q})/\mathfrak{b} \supsetneq \mathfrak{a}/\mathfrak{b} \supseteq (\mathfrak{p}\mathfrak{q} + \mathfrak{b})/\mathfrak{b} = (\mathfrak{p}/\mathfrak{b}) \cdot (\mathfrak{q}/\mathfrak{b}).$$

Since

$$((\mathfrak{p} \cap \mathfrak{q})/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b}) \cong (\mathfrak{p} \cap \mathfrak{q})/\mathfrak{a}, \quad (A/\mathfrak{b})/(\mathfrak{p}/\mathfrak{b}) \cong A/\mathfrak{p}, \quad (A/\mathfrak{b})/(\mathfrak{q}/\mathfrak{b}) \cong A/\mathfrak{q},$$

it follows that $\mathfrak{a}/\mathfrak{b}$ is a linking ideal from $\mathfrak{p}/\mathfrak{b}$ to $\mathfrak{q}/\mathfrak{b}$. □

Lemma 5.4. *Let $\mathfrak{p}$ and $\mathfrak{q}$ be distinct prime ideals of a noetherian ring A with $\mathfrak{p} \rightsquigarrow \mathfrak{q}$. If $\mathfrak{z}$ is a centrally generated ideal of A with $\mathfrak{z} \subseteq \mathfrak{p}$ or $\mathfrak{z} \subseteq \mathfrak{q}$, then $\mathfrak{z} \subseteq \mathfrak{p} \cap \mathfrak{q}$ and $\mathfrak{p}/\mathfrak{z} \rightsquigarrow \mathfrak{q}/\mathfrak{z}$ in $A/\mathfrak{z}$.*

Proof. This is proven in [Müller 1985] but we also give a proof here for the sake of completeness. First note that since $\mathfrak{z}$ is centrally generated and $\mathfrak{p} \rightsquigarrow \mathfrak{q}$, it follows from [Goodearl and Warfield 2004, Lemma 12.15] that already $\mathfrak{z} \subseteq \mathfrak{p} \cap \mathfrak{q}$. Let $\mathfrak{a}$ be a linking ideal from $\mathfrak{p}$ to $\mathfrak{q}$. We claim that $\mathfrak{z}$ is contained in $\mathfrak{a}$. To show this, suppose that $\mathfrak{z}$ is not contained in $\mathfrak{a}$. Then $(\mathfrak{a}+\mathfrak{z})/\mathfrak{a}$ is a nonzero submodule of $(\mathfrak{p}\cap\mathfrak{q})/\mathfrak{a}$ which is torsion-free as a left $(A/\mathfrak{p})$-module and as a right $(A/\mathfrak{q})$-module. In conjunction with the fact that $\mathfrak{z}$ is centrally generated it now follows from Lemma 5.2 that

$$\mathfrak{p} = \mathrm{Ann}({}_A((\mathfrak{a}+\mathfrak{z})/\mathfrak{a})) = \mathrm{Ann}(((\mathfrak{a}+\mathfrak{z})/\mathfrak{a})_A) = \mathfrak{q},$$

contradicting the assumption $\mathfrak{p} \neq \mathfrak{q}$. Hence, we must have $\mathfrak{z} \subseteq \mathfrak{a}$ and it thus follows from Lemma 5.3(b) that $\mathfrak{p}/\mathfrak{z} \rightsquigarrow \mathfrak{q}/\mathfrak{z}$. □

Lemma 5.5. *Let $\mathfrak{z}$ be a centrally generated ideal of a noetherian ring A. Let $\mathfrak{p}$ be a prime ideal of A with $\mathfrak{z} \subseteq \mathfrak{p}$. Then all prime ideals in* $\mathrm{Clq}(\mathfrak{p})$ *contain $\mathfrak{z}$ and the map*

$$\begin{aligned} \mathrm{Clq}(\mathfrak{p}) &\longrightarrow \mathrm{Clq}(\mathfrak{p}/\mathfrak{z}), \\ \mathfrak{q} &\longmapsto \mathfrak{q}/\mathfrak{z}, \end{aligned}$$

is a bijection between a clique of A and a clique of $A/\mathfrak{z}$.

Proof. It follows immediately from [Goodearl and Warfield 2004, Lemma 12.15] that all prime ideals in $\mathrm{Clq}(\mathfrak{p})$ contain $\mathfrak{z}$. If $\mathfrak{q} \in \mathrm{Clq}(\mathfrak{p})$, then there exists a chain $\mathfrak{p} = \mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_{r-1}, \mathfrak{p}_r = \mathfrak{q}$ of prime ideals of A with $\mathfrak{p}_i \rightsquigarrow \mathfrak{p}_{i+1}$ or $\mathfrak{p}_{i+1} \rightsquigarrow \mathfrak{p}_i$ for all indices i. An inductive application of Lemma 5.4 shows now that $\mathfrak{p}_i/\mathfrak{z} \rightsquigarrow \mathfrak{p}_{i+1}/\mathfrak{z}$ or $\mathfrak{p}_{i+1}/\mathfrak{z} \rightsquigarrow \mathfrak{p}_i/\mathfrak{z}$ for all i. Hence, $\mathfrak{p}/\mathfrak{z}$ and $\mathfrak{q}/\mathfrak{z}$ lie in the same clique of $A/\mathfrak{z}$ so that the map $\mathrm{Clq}(\mathfrak{p}) \to \mathrm{Clq}(\mathfrak{p}/\mathfrak{z})$ is well-defined. On the other hand, similar arguments and Lemma 5.3(a) show that if $\mathfrak{q}/\mathfrak{z} \in \mathrm{Clq}(\mathfrak{p}/\mathfrak{z})$, then also $\mathfrak{q} \in \mathrm{Clq}(\mathfrak{p})$, so that we also have a well-defined map $\mathrm{Clq}(\mathfrak{p}/\mathfrak{z}) \to \mathrm{Clq}(\mathfrak{p})$. It is evident that both maps defined are pairwise inverse thus proving the first assertion. The second assertion is now obvious. □

Lemma 5.6 (B. Müller). *Let A be a ring with center Z such that Z is noetherian and A is a finite Z-module. If $\mathfrak{z}$ is a centrally generated ideal of A such that $A/\mathfrak{z}A$ is of classical Krull dimension zero, then the inclusion $(Z+\mathfrak{z})/\mathfrak{z} \hookrightarrow A/\mathfrak{z}A$ is block bijective. In other words, the block idempotents of $A/\mathfrak{z}A$ are already contained in the central subalgebra $(Z+\mathfrak{z})/\mathfrak{z}$.*

Proof. Let $\bar{A} := A/\mathfrak{z}$ and let $\bar{Z} := (Z+\mathfrak{z})/\mathfrak{z}$. Then $\bar{A}$ is a finitely generated $\bar{Z}$-module since A is a finitely generated Z-module. Hence, $\bar{Z} \subseteq \bar{A}$ is a finite centralizing extension and now it follows from going up in finite centralizing extensions [McConnell and Robson 2001, Theorem 10.2.9] that the classical Krull dimension of $\bar{Z}$ is equal to that of $\bar{A}$, which is zero by assumption. Hence, by Lemma 5.1 we have $\mathrm{Bl}(\bar{Z}) \simeq \mathrm{Clq}(\bar{Z})$ and $\mathrm{Bl}(\bar{A}) \simeq \mathrm{Clq}(\bar{A})$. Since $\#\,\mathrm{Bl}(\bar{Z}) \leq \#\,\mathrm{Bl}(\bar{A})$, the claim is thus equivalent to the claim that over each clique of $\bar{Z}$, there is just one clique of $\bar{A}$. So, let $X, Y \in \mathrm{Clq}(\bar{A})$ be two cliques. We pick $\mathfrak{M}/\mathfrak{z} \in X$ and $\mathfrak{N}/\mathfrak{z} \in Y$ with $\mathfrak{M}, \mathfrak{N}$ maximal ideals of A. Assume that X and Y lie over the same clique of $\bar{Z}$. Since $\bar{Z}$ is commutative, we know from Lemma 5.1 that all cliques are singletons and so the assumption implies that $\mathfrak{M}/\mathfrak{z}$ and $\mathfrak{N}/\mathfrak{z}$ lie over the same maximal ideal of $\bar{Z}$; i.e.,

$$(\mathfrak{M}/\mathfrak{z}) \cap ((Z+\mathfrak{z})/\mathfrak{z}) = (\mathfrak{N}/\mathfrak{z}) \cap ((Z+\mathfrak{z})/\mathfrak{z}).$$

Hence

$$\mathfrak{M} \cap (Z+\mathfrak{z}) = \mathfrak{N} \cap (Z+\mathfrak{z}).$$

Since $Z \subseteq Z+\mathfrak{z}$, we thus get

$$\mathfrak{M} \cap Z = \mathfrak{M} \cap Z \cap (Z+\mathfrak{z}) = \mathfrak{N} \cap Z \cap (Z+\mathfrak{z}) = \mathfrak{N} \cap Z.$$

Now, Müller's theorem [Goodearl and Warfield 2004, Theorem 13.10] implies that $\mathfrak{M}$ and $\mathfrak{N}$ lie in the same clique of A. An application of Lemma 5.5 thus implies that $\mathfrak{M}/\mathfrak{z}$ and $\mathfrak{N}/\mathfrak{z}$ lie in the same clique of $A/\mathfrak{z}$, so $X = Y$. □

5B. ***Blocks as fibers of a morphism.***

We assume A is a finite flat algebra over a noetherian integral domain R.

By Lemma B.2 the morphism

$$\Upsilon : \mathrm{Spec}(Z) \to \mathrm{Spec}(R), \tag{41}$$

induced by the canonical morphism from R to the center Z of A is finite, closed, and surjective. The center Z of A is naturally an R-algebra and so we can consider its fibers

$$Z(\mathfrak{p}) = \mathrm{k}(\mathfrak{p}) \otimes_R Z/\mathfrak{p}Z = Z_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} Z_\mathfrak{p} \tag{42}$$

in prime ideals $\mathfrak{p}$ of R. On the other hand, the image of $Z_\mathfrak{p} = \mathrm{Z}(A_\mathfrak{p})$ under the canonical (surjective) morphism $A_\mathfrak{p} \twoheadrightarrow A(\mathfrak{p})$ yields a central subalgebra

$$\mathrm{Z}_\mathfrak{p}(A) := (Z_\mathfrak{p} + \mathfrak{p}_\mathfrak{p} A_\mathfrak{p})/\mathfrak{p}_\mathfrak{p} A_\mathfrak{p} \tag{43}$$

of $A(\mathfrak{p})$. In general this subalgebra is *not* equal to the center of $A(\mathfrak{p})$ itself. We have a surjective morphism

$$\phi_{\mathfrak{p}} : Z(\mathfrak{p}) \twoheadrightarrow \mathrm{Z}_{\mathfrak{p}}(A) \tag{44}$$

of finite-dimensional $\mathrm{k}(\mathfrak{p})$-algebras. This morphism is in general *not* injective — it is if and only if $\mathfrak{p}_{\mathfrak{p}} A_{\mathfrak{p}} \cap Z_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}} Z_{\mathfrak{p}}$. Nonetheless, we have the following result.

Lemma 5.7. *The map $\phi_{\mathfrak{p}} : Z(\mathfrak{p}) \to \mathrm{Z}_{\mathfrak{p}}(A)$ in (44) is block bijective.*

Proof. Since $\phi_{\mathfrak{p}}$ is surjective, the induced map ${}^a\phi_{\mathfrak{p}} : \mathrm{Spec}(\mathrm{Z}_{\mathfrak{p}}(A)) \to \mathrm{Spec}(Z(\mathfrak{p}))$ is injective, so $\#\,\mathrm{Bl}(\mathrm{Z}_{\mathfrak{p}}(A)) \leq \#\,\mathrm{Bl}(Z(\mathfrak{p}))$ by Lemma 5.1. Now we just need to show that $\phi_{\mathfrak{p}}$ does not map any nontrivial idempotent to zero. Since $R_{\mathfrak{p}}$ is noetherian, also $A_{\mathfrak{p}}$ is noetherian. The Artin–Rees lemma [Matsumura 1986, Theorem 8.5] applied to the $R_{\mathfrak{p}}$-module $A_{\mathfrak{p}}$, the submodule $Z_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$, and the ideal $\mathfrak{p}_{\mathfrak{p}}$ of $R_{\mathfrak{p}}$ shows that there is an integer $k \in \mathbb{N}_{>0}$ such that for any $n > k$ we have

$$\mathfrak{p}_{\mathfrak{p}}^n A_{\mathfrak{p}} \cap Z_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}^{n-k}((\mathfrak{p}_{\mathfrak{p}}^k A_{\mathfrak{p}}) \cap Z_{\mathfrak{p}}).$$

In particular, there is $n \in \mathbb{N}_{>0}$ such that $\mathfrak{p}_{\mathfrak{p}}^n A_{\mathfrak{p}} \cap Z_{\mathfrak{p}} \subseteq \mathfrak{p}_{\mathfrak{p}} Z_{\mathfrak{p}}$. Now, let $\bar{e} \in Z(\mathfrak{p}) = Z_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}} Z_{\mathfrak{p}}$ be an idempotent with $\phi_{\mathfrak{p}}(\bar{e}) = 0$. By assumption, $\bar{e} \in \mathrm{Ker}(\phi_{\mathfrak{p}}) = (\mathfrak{p}_{\mathfrak{p}} A_{\mathfrak{p}} \cap Z_{\mathfrak{p}})/\mathfrak{p}_{\mathfrak{p}} Z_{\mathfrak{p}}$. Hence, if $e \in Z_{\mathfrak{p}}$ is a representative of $\bar{e}$, we have $e \in \mathfrak{p}_{\mathfrak{p}} A_{\mathfrak{p}} \cap Z_{\mathfrak{p}}$. We have $e^n \in \mathfrak{p}_{\mathfrak{p}}^n A_{\mathfrak{p}} \cap Z_{\mathfrak{p}} \subseteq \mathfrak{p}_{\mathfrak{p}} Z_{\mathfrak{p}}$, so already $\bar{e} = 0$. □

Theorem 5.8. *For any $\mathfrak{p} \in \mathrm{Spec}(R)$ there are canonical bijections*

$$\mathrm{Bl}(A(\mathfrak{p})) \simeq \mathrm{Bl}(\mathrm{Z}_{\mathfrak{p}}(A)) \simeq \mathrm{Bl}(Z(\mathfrak{p})) \simeq \Upsilon^{-1}(\mathfrak{p}). \tag{45}$$

The first bijection $\mathrm{Bl}(A(\mathfrak{p})) \simeq \mathrm{Bl}(\mathrm{Z}_{\mathfrak{p}}(A))$ is induced by the embedding $\mathrm{Z}_{\mathfrak{p}}(A) \hookrightarrow A(\mathfrak{p})$. In other words, all block idempotents of $A(\mathfrak{p})$ are already contained in the central subalgebra $\mathrm{Z}_{\mathfrak{p}}(A)$ of $A(\mathfrak{p})$. The second bijection is the bijection from Lemma 5.7. The last bijection $\mathrm{Bl}(Z(\mathfrak{p})) \simeq \Upsilon^{-1}(\mathfrak{p})$ maps a block idempotent c of $Z(\mathfrak{p})$ to the (by the theorem, unique) maximal ideal $\mathfrak{m}_c$ of Z lying above $\mathfrak{p}$ such that $c^\dagger \in (\mathfrak{m}_c + \mathfrak{p}_{\mathfrak{p}} Z_{\mathfrak{p}})/\mathfrak{p}_{\mathfrak{p}} Z_{\mathfrak{p}}$, where $c^\dagger = 1 - c$.

Proof. The first bijection follows directly from Lemma 5.6 applied to $A_{\mathfrak{p}}$ and the centrally generated ideal $\mathfrak{z} := \mathfrak{p}_{\mathfrak{p}} A_{\mathfrak{p}}$. Let $\Upsilon_{\mathfrak{p}} : \mathrm{Spec}(Z_{\mathfrak{p}}) \to \mathrm{Spec}(R_{\mathfrak{p}})$ be the morphism induced by the canonical map $R_{\mathfrak{p}} \to Z_{\mathfrak{p}}$. Recall from Lemma B.2 that $R_{\mathfrak{p}} \subseteq Z_{\mathfrak{p}}$ is a finite extension so that $\Upsilon_{\mathfrak{p}}$ is surjective. We have

$$\begin{aligned}\Upsilon_{\mathfrak{p}}^{-1}(\mathfrak{p}_{\mathfrak{p}}) &= \{\mathfrak{Q} \in \mathrm{Spec}(Z_{\mathfrak{p}}) \mid \mathfrak{Q} \cap R_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}\} \\ &= \{\mathfrak{Q} \in \mathrm{Spec}(Z_{\mathfrak{p}}) \mid \mathfrak{p}_{\mathfrak{p}} \subseteq \mathfrak{Q}\} \\ &= \{\mathfrak{Q} \in \mathrm{Spec}(Z_{\mathfrak{p}}) \mid \mathfrak{p}_{\mathfrak{p}} Z_{\mathfrak{p}} \subseteq \mathfrak{Q}\} \simeq \mathrm{Spec}(Z(\mathfrak{p})).\end{aligned}$$

In the second equality we used the fact that $R_{\mathfrak{p}} \to Z_{\mathfrak{p}}$ is a finite morphism and $R_{\mathfrak{p}}$ is local with maximal ideal $\mathfrak{p}_{\mathfrak{p}}$. The identification with $\mathrm{Spec}(Z(\mathfrak{p}))$ is canonical since $Z(\mathfrak{p}) = Z_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} Z_\mathfrak{p}$. The morphism $\Theta_\mathfrak{p} : \mathrm{Spec}(Z_\mathfrak{p}) \to \mathrm{Spec}(Z)$ induced by the localization map $Z \to Z_\mathfrak{p}$ is injective by [Eisenbud 1995, Proposition 2.2(b)]. We claim that this map induces $\Upsilon_\mathfrak{p}^{-1}(\mathfrak{p}_\mathfrak{p}) \simeq \Upsilon^{-1}(\mathfrak{p})$. If $\mathfrak{Q} \in \Upsilon_\mathfrak{p}^{-1}(\mathfrak{p}_\mathfrak{p})$, then clearly

$$(\mathfrak{Q} \cap Z) \cap R = \mathfrak{Q} \cap R \subseteq R \cap \mathfrak{p}_\mathfrak{p} = \mathfrak{p}$$

and therefore $\Theta_\mathfrak{p}$ induces an injective map $\Upsilon_\mathfrak{p}^{-1}(\mathfrak{p}_\mathfrak{p}) \to \Upsilon^{-1}(\mathfrak{p})$. If $\mathfrak{Q} \in \Upsilon^{-1}(\mathfrak{p})$, then, since $\mathfrak{Q} \cap R = \mathfrak{p}$, we have $\mathfrak{Q} \cap (R \setminus \mathfrak{p}) = \varnothing$ so that $\mathfrak{Q}_\mathfrak{p} \in \mathrm{Spec}(Z_\mathfrak{p})$ and clearly $\mathfrak{p}_\mathfrak{p} \subseteq \mathfrak{Q}_\mathfrak{p}$, implying that $\mathfrak{Q}_\mathfrak{p} \in \Upsilon_\mathfrak{p}^{-1}(\mathfrak{p}_\mathfrak{p})$. The map $\Upsilon_\mathfrak{p}^{-1}(\mathfrak{p}_\mathfrak{p}) \to \Upsilon^{-1}(\mathfrak{p})$ is thus bijective. Hence, we have a canonical bijection $\mathrm{Spec}(Z(\mathfrak{p})) \simeq \Upsilon^{-1}(\mathfrak{p})$. Now, recall from Lemma 5.1 that $\mathrm{Spec}(Z(\mathfrak{p})) \simeq \mathrm{Bl}(Z(\mathfrak{p}))$. $\square$

5C. *Blocks via central characters.*

We assume that R is noetherian and normal, and that A is a finite flat R-algebra with split generic fiber A^K.

Recall from Corollary 4.3 that the quotient map $A_\mathfrak{p} \twoheadrightarrow A(\mathfrak{p})$ induces $\mathrm{Bl}(A_\mathfrak{p}) \simeq \mathrm{Bl}(A(\mathfrak{p}))$, so together with Theorem 5.8 we have the canonical bijection

$$\mathrm{Bl}(A_\mathfrak{p}) \simeq \Upsilon^{-1}(\mathfrak{p}). \tag{46}$$

Recall from Section 3 that $\mathrm{Fam}_\mathfrak{p}(A^K)$ is the partition of $\mathrm{Irr}\, A^K$ induced by the blocks of $A_\mathfrak{p}$ and that we naturally have $\mathrm{Bl}(A_\mathfrak{p}) \simeq \mathrm{Fam}_\mathfrak{p}(A^K)$. Altogether, we now have canonical bijections

$$\mathrm{Fam}_\mathfrak{p}(A) \simeq \mathrm{Bl}(A_\mathfrak{p}) \simeq \Upsilon^{-1}(\mathfrak{p}) \simeq \mathrm{Bl}(A(\mathfrak{p})). \tag{47}$$

Since A has split generic fiber A^K, we have a central character $\Omega_S : \mathrm{Z}(A^K) \to K$ for every simple A^K-module S. Recall that $\Omega_S(z)$ is the scalar by which $z \in \mathrm{Z}(A^K)$ acts on S. Since R is normal, the image of the restriction of Ω_S to $\mathrm{Z}(A) \subseteq \mathrm{Z}(A^K)$ is contained in $R \subseteq K$. We thus get a well-defined R-algebra morphism

$$\Omega'_S : \mathrm{Z}(A) \to R. \tag{48}$$

It is a classical fact that $S, T \in \mathrm{Irr}\, A^K$ lie in the same family if and only if $\Omega'_S = \Omega'_T$. We can thus label the central characters of A^K as $\Omega_\mathcal{F}$ with $\mathcal{F}$ a family (block) of A^K. Using Theorem 5.8 this description generalizes modulo $\mathfrak{p}$ so that we get an explicit description of the $\mathfrak{p}$-families, and thus of the block stratification. For $\mathfrak{p} \in \mathrm{Spec}(R)$ let

$$\Omega_S^\mathfrak{p} : \mathrm{Z}(A) \to R/\mathfrak{p} \tag{49}$$

be the composition of Ω'_S with the quotient map $R \twoheadrightarrow R/\mathfrak{p}$.

Theorem 5.9. *Under the bijection $\Upsilon^{-1}(\mathfrak{p}) \simeq \mathrm{Fam}_\mathfrak{p}(A)$ from (47) the $\mathfrak{p}$-family of a simple A^K-module S corresponds to* $\mathrm{Ker}\, \Omega_S^\mathfrak{p}$. *Hence, two simple A^K-modules S and T lie in the same $\mathfrak{p}$-family if and only if $\Omega'_S(z) \equiv \Omega'_T(z) \mod \mathfrak{p}$ for all $z \in \mathrm{Z}(A)$.*

So, if $z_1, \dots, z_n$ is an R-algebra generating system of $\mathrm{Z}(A)$ and $\mathscr{F}, \mathscr{F}'$ are two distinct A^K-families, then the corresponding gluing locus is given by

$$\mathrm{Gl}_A\big(\le\{\mathscr{F}, \mathscr{F}'\}\big) = \mathrm{V}\big(\{\Omega_{\mathscr{F}}(z_i) - \Omega_{\mathscr{F}'}(z_i) \mid i = 1, \dots, n\}\big). \tag{50}$$

Proof. Considering the explicit form of the bijection given in Theorem 5.8 we see that the bijection (46) maps a block idempotent c of $A_{\mathfrak{p}}$ to the (by the theorem, unique) maximal ideal $\mathfrak{Q}_c$ of Z lying above $\mathfrak{p}$ and satisfying $c^\dagger \in (\mathfrak{Q}_c)_{\mathfrak{p}}$. Let $c_{\mathfrak{Q}}$ be the block idempotent of $A_{\mathfrak{p}}$ corresponding to $\mathfrak{Q} \in \Upsilon^{-1}(\mathfrak{p})$.

For $S \in \operatorname{Irr} A^K$ let $\Omega_S^{\mathfrak{p}} : Z \to R/\mathfrak{p}$ be the composition of Ω'_S and the quotient morphism $R \to R/\mathfrak{p}$. It is clear that $\operatorname{Ker}(\Omega_S^{\mathfrak{p}}) \in \Upsilon^{-1}(\mathfrak{p})$. Note that $\Omega'_S(z) \equiv \Omega'_T(z) \bmod \mathfrak{p}$ for all $z \in \mathrm{Z}(A)$ if and only if $\Omega_S^{\mathfrak{p}} = \Omega_T^{\mathfrak{p}}$. We have an exact sequence

$$0 \longrightarrow \operatorname{Ker}(\Omega'_S) \longrightarrow Z \xrightarrow{\Omega'_S} R \longrightarrow 0$$

of R-modules. Since Ω'_S is an R-algebra morphism, the canonical map $R \to Z$ is a section of Ω'_S and therefore $Z = R \oplus \operatorname{Ker}(\Omega'_S)$ as R-modules. Similarly, we have $Z = R \oplus \operatorname{Ker}(\Omega'_T)$. Since $\operatorname{Ker}(\Omega'_S) \subseteq \operatorname{Ker}(\Omega_S^{\mathfrak{p}})$ and $\operatorname{Ker}(\Omega'_T) \subseteq \operatorname{Ker}(\Omega_T^{\mathfrak{p}})$, this implies that $\Omega_S^{\mathfrak{p}} = \Omega_T^{\mathfrak{p}}$ if and only if $\operatorname{Ker}(\Omega_S^{\mathfrak{p}}) = \operatorname{Ker}(\Omega_T^{\mathfrak{p}})$.

Now, suppose that $\operatorname{Ker}(\Omega_S^{\mathfrak{p}}) = \operatorname{Ker}(\Omega_T^{\mathfrak{p}})$. Denote this common kernel by $\mathfrak{Q}$. Clearly, $\mathfrak{Q} \in \Upsilon^{-1}(\mathfrak{p})$. We know that the corresponding block idempotent $c_{\mathfrak{Q}}$ of $A_{\mathfrak{p}}$ has the property that $c_{\mathfrak{Q}}^\dagger \in \mathfrak{Q}_{\mathfrak{p}}$. Since $\operatorname{Ker}(\Omega'_S) \subseteq \operatorname{Ker}(\Omega_S^{\mathfrak{p}}) = \mathfrak{Q} = \operatorname{Ker}(\Omega_T^{\mathfrak{p}}) \supseteq \operatorname{Ker}(\Omega'_T)$, this certainly implies that $c_{\mathfrak{Q}}^\dagger S = 0 = c_{\mathfrak{Q}}^\dagger T$. Hence, S and T lie in the same $\mathfrak{p}$-family.

Conversely, suppose that S and T lie in the same $\mathfrak{p}$-family. We can write the corresponding block idempotent of $A_{\mathfrak{p}}$ as $c_{\mathfrak{Q}}$ for some $\mathfrak{Q} \in \Upsilon^{-1}(\mathfrak{p})$. By definition, $c_{\mathfrak{Q}}^\dagger S = 0 = c_{\mathfrak{Q}}^\dagger T$. We know that $c_{\mathfrak{Q}}^\dagger \in \mathfrak{Q}_{\mathfrak{p}}$ and $c_{\mathfrak{Q}} \notin \mathfrak{Q}_{\mathfrak{p}}$ and therefore $\operatorname{Ker}((\Omega'_S)_{\mathfrak{p}}) = \mathfrak{Q}_{\mathfrak{p}} = \operatorname{Ker}((\Omega'_T)_{\mathfrak{p}})$. Hence, $\mathfrak{Q} \subseteq \operatorname{Ker}(\Omega'_S) \subseteq \operatorname{Ker}(\Omega_S^{\mathfrak{p}})$ and $\mathfrak{Q} \subseteq \operatorname{Ker}(\Omega'_T) \subseteq \operatorname{Ker}(\Omega_T^{\mathfrak{p}})$. Since $\mathfrak{Q}$, $\operatorname{Ker}(\Omega_S^{\mathfrak{p}})$, $\operatorname{Ker}(\Omega_T^{\mathfrak{p}}) \in \Upsilon^{-1}(\mathfrak{p})$ and all prime ideals in $\Upsilon^{-1}(\mathfrak{p})$ are incomparable, we thus conclude that $\operatorname{Ker}(\Omega_S^{\mathfrak{p}}) = \operatorname{Ker}(\Omega_T^{\mathfrak{p}})$.

The equation for the gluing locus is now clear. $\square$

6. Blocks and decomposition matrices

To obtain information about the actual members of the $A(\mathfrak{p})$-families we use decomposition maps as introduced by Geck and Rouquier [1997]; see also [Geck and Pfeiffer 2000; Thiel 2016]. For a ring A we denote by $\mathrm{G}_0(A) := \mathrm{K}_0(A\text{-mod})$ the *Grothendieck group* and by $\mathrm{K}_0(A) := \mathrm{K}_0(A\text{-proj})$ the *projective class group*. In the case A is semiperfect (e.g., artinian), $\mathrm{K}_0(A)$ is the free abelian group with basis the isomorphism classes of the projective indecomposable modules. In the case A is artinian, $\mathrm{G}_0(A)$ is the free abelian group with basis the isomorphism classes of simple modules and $\mathrm{K}_0(A) \simeq \mathrm{G}_0(A)$ mapping P to $\mathrm{Hd}(P)$.

For the theory of decomposition maps we need the following (standard) assumption:

> ***A is finite free with split generic fiber and for any nonzero $\mathfrak{p} \in \mathbf{Spec}(R)$ there is a discrete valuation ring $\mathscr{O}$ with maximal ideal $\mathfrak{m}$ in K dominating $R_{\mathfrak{p}}$ such that the canonical map $\mathbf{G_0}(A(\mathfrak{p})) \to \mathbf{G_0}(A^{\mathscr{O}}(\mathfrak{m}))$ of Grothendieck groups is an isomorphism.***

We call a ring $\mathscr{O}$ as above a *perfect A-gate* in $\mathfrak{p}$. We refer to [Thiel 2016] for more details. The following lemma lists two standard situations in which the above assumptions hold. Part (a) is obvious and part (b) was proven in [Thiel 2016, Theorem 1.22].

Lemma 6.1. *A finite free R-algebra A with split generic fiber satisfies the above assumptions in the following two cases*:

(a) *R is a Dedekind domain.*

(b) *R is noetherian and A has split fibers.*

If $\mathscr{O}$ is a perfect A-gate in $\mathfrak{p}$, then there is a group morphism

$$\mathrm{d}_A^{\mathfrak{p},\mathscr{O}} : \mathrm{G}_0(A^K) \to \mathrm{G}_0(A(\mathfrak{p})) \tag{51}$$

between Grothendieck groups generalizing reduction modulo $\mathfrak{p}$. In the case R is normal, it was proven by Geck and Rouquier [1997] that this map is independent of the choice of $\mathscr{O}$ and in this case we just write $\mathrm{d}_A^{\mathfrak{p}}$. We note that in the case R is noetherian and A has split fibers, any decomposition map in the sense of Geck and Rouquier can be realized by a perfect A-gate; see [Thiel 2016, Theorem 1.22].

6A. ***Brauer reciprocity.*** An important tool for relating decomposition maps and blocks is *Brauer reciprocity*, which we prove in Theorem 6.2 below in our general setup (this was known to hold before only in special settings). Recall that the *intertwining form* for a finite-dimensional algebra B over a field F is the $\mathbb{Z}$-linear pairing $\langle \cdot , \cdot \rangle_B : \mathrm{K}_0(B) \times \mathrm{G}_0(B) \to \mathbb{Z}$ uniquely defined by

$$\langle [P], [V] \rangle := \dim_F \mathrm{Hom}_B(P, V) \tag{52}$$

for a finite-dimensional projective B-module P and a finite-dimensional B-module V; see [Geck and Rouquier 1997, §2]. Here, $\mathrm{K}_0(B)$ is the zeroth K-group of the category of finite-dimensional projective B-modules. The intertwining form is always nondegenerate; see Lemma A.6. Due to the nondegeneracy of $\langle \cdot , \cdot \rangle_{A^K}$ there is at most one adjoint

$$\mathrm{e}_A^{\mathfrak{p},\mathscr{O}} : \mathrm{K}_0(A(\mathfrak{p})) \to \mathrm{K}_0(A^K) \tag{53}$$

of $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}} : \mathrm{G}_0(A^K) \to \mathrm{G}_0(A(\mathfrak{p}))$ with respect to $\langle \cdot , \cdot \rangle_{A(\mathfrak{p})}$, characterized by the relation

$$\langle \mathrm{e}_A^{\mathfrak{p},\mathscr{O}}([\bar{P}]), [V] \rangle_{A^K} = \langle [\bar{P}], \mathrm{d}_A^{\mathfrak{p},\mathscr{O}}([V]) \rangle_{A(\mathfrak{p})}. \tag{54}$$

for all finitely generated A^K-modules V and all finitely generated projective $A(\mathfrak{p})$-modules $\bar{P}$; see Lemma A.6. Brauer reciprocity is about the existence of this adjoint.

Theorem 6.2. *The (unique) adjoint* $\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}$ *of* $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}$ *exists. Moreover, the diagram*

$$\begin{tikzcd} \mathrm{K}_0(A^K) \arrow[r, "\mathrm{c}_{A^K}"] & \mathrm{G}_0(A^K) \arrow[d, "\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}"] \\ \mathrm{K}_0(A(\mathfrak{p})) \arrow[u, "\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}"] \arrow[r, "\mathrm{c}_{A(\mathfrak{p})}"'] & \mathrm{G}_0(A(\mathfrak{p})) \end{tikzcd} \tag{55}$$

commutes, where the horizontal morphisms are the canonical ones (Cartan maps) mapping a class $[P]$ *of a projective module* P *to its class* $[P]$ *in the Grothendieck group. If* R *is normal, the morphism* $\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}$ *does not depend on the choice of* $\mathscr{O}$ *and we denote it by* $\mathrm{e}_A^{\mathfrak{p}}$.

Proof. Since $\langle\cdot,\cdot\rangle_{A^K}$ is nondegenerate by Lemma A.6, it follows that $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}$ has at most one adjoint $\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}$, characterized by (54); see [Scheja and Storch 1988, Satz 78.1]. By assumption there is a perfect A-gate $\mathscr{O}$ in $\mathfrak{p}$. Let $\mathfrak{m}$ be the maximal ideal of $\mathscr{O}$. Since A^K splits by assumption, Corollary A.14 implies that $A^{\mathscr{O}}$ is semiperfect. The morphism $\mathrm{K}_0(A^{\mathscr{O}}) \to \mathrm{K}_0(A^{\mathscr{O}}(\mathfrak{m}))$ induced by the quotient map $A^{\mathscr{O}} \twoheadrightarrow A^{\mathscr{O}}(\mathfrak{m})$ is thus an isomorphism by lifting of idempotents. Furthermore, by assumption the morphism $\mathrm{d}_A^{\mathfrak{p},\mathfrak{m}} : \mathrm{G}_0(A(\mathfrak{p})) \to \mathrm{G}_0(A^{\mathscr{O}}(\mathfrak{m}))$ is an isomorphism and then the proof of Theorem 4.1 shows that the canonical morphism $\mathrm{e}_A^{\mathfrak{p},\mathfrak{m}} : \mathrm{K}_0(A(\mathfrak{p})) \to \mathrm{K}_0(A^{\mathscr{O}}(\mathfrak{m}))$ is also an isomorphism. We can thus define the morphism $\mathrm{e}_A^{\mathfrak{p},\mathscr{O}} : \mathrm{K}_0(A(\mathfrak{p})) \to \mathrm{K}_0(A^K)$ as the following composition:

$$\begin{tikzcd} \mathrm{K}_0(A(\mathfrak{p})) \arrow[r, "\simeq"] \arrow[rrr, bend right, "\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}"'] & \mathrm{K}_0(A^{\mathscr{O}}(\mathfrak{m})) \arrow[r, "\simeq"] & \mathrm{K}_0(A^{\mathscr{O}}) \arrow[r] & \mathrm{K}_0(A^K) \end{tikzcd} \tag{56}$$

We will now show that $\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}$ is indeed an adjoint of $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}$. The arguments in the proof of [Curtis and Reiner 1981, 18.9] can, with some refinements, be transferred to our more general situation and this is what we will do. Let $\bar{P}$ be a finitely generated projective $A(\mathfrak{p})$-module and let V be a finitely generated A^K-module. Since $\mathrm{K}_0(A^{\mathscr{O}}) \simeq \mathrm{K}_0(A^{\mathscr{O}}(\mathfrak{m}))$, there exists a finitely generated projective $A^{\mathscr{O}}$-module P such that $(\mathrm{e}_A^{\mathfrak{p},\mathfrak{m}})^{-1}([P/\mathfrak{m}P]) = [\bar{P}]$ and then we have $\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}([\bar{P}]) = [P^K]$. Let $\widetilde{V}$ be an $A^{\mathscr{O}}$-lattice in V. Then by the definition of $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}$, see [Thiel 2016, Corollary 1.14], we have $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}([V]) = (\mathrm{d}_A^{\mathfrak{p},\mathfrak{m}})^{-1}([\widetilde{V}(\mathfrak{m})])$. We denote by $\bar{V}$ a representative of $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}([V])$. Since P is a finitely generated projective $A^{\mathscr{O}}$-module, we can write $P \oplus Q = (A^{\mathscr{O}})^n$ for some finitely generated projective $A^{\mathscr{O}}$-module Q and some $n \in \mathbb{N}$. Since $\mathrm{Hom}_{A^{\mathscr{O}}}$ is additive, we get

$$\begin{aligned} \mathrm{Hom}_{A^{\mathscr{O}}}(P, \widetilde{V}) \oplus \mathrm{Hom}_{A^{\mathscr{O}}}(Q, \widetilde{V}) &= \mathrm{Hom}_{A^{\mathscr{O}}}(P \oplus Q, \widetilde{V}) = \mathrm{Hom}_{A^{\mathscr{O}}}((A^{\mathscr{O}})^n, \widetilde{V}) \\ &= (\mathrm{Hom}_{A^{\mathscr{O}}}(A^{\mathscr{O}}, \widetilde{V}))^n \simeq \widetilde{V}^n. \end{aligned}$$

This shows that $\mathrm{Hom}_{A^{\mathscr{O}}}(P, \widetilde{V})$ is a direct summand of $\widetilde{V}^n$ and as $\widetilde{V}^n$ is $\mathscr{O}$-free, we conclude that $\mathrm{Hom}_{A^{\mathscr{O}}}(P, \widetilde{V})$ is $\mathscr{O}$-projective and thus even $\mathscr{O}$-free since $\mathscr{O}$ is a discrete valuation ring. Since P is a finitely generated projective $A^{\mathscr{O}}$-module, it follows from Lemma B.3 that there is a canonical K-vector space isomorphism

$$K \otimes_{\mathscr{O}} \mathrm{Hom}_{A^{\mathscr{O}}}(P, \widetilde{V}) \simeq \mathrm{Hom}_{A^K}(P^K, V)$$

and a canonical $\mathrm{k}(\mathfrak{m})$-vector space isomorphism

$$\mathrm{k}(\mathfrak{m}) \otimes_{\mathscr{O}} \mathrm{Hom}_{A^{\mathscr{O}}}(P, \widetilde{V}) \simeq \mathrm{Hom}_{A^{\mathscr{O}}(\mathfrak{m})}(P/\mathfrak{m}P, \widetilde{V}/\mathfrak{m}\widetilde{V}).$$

Combining all results and the fact that both $\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}$ and $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}$ preserve dimensions by construction, we can now conclude that

$$\begin{aligned}
\langle \mathrm{e}_A^{\mathfrak{p},\mathscr{O}}([\bar{P}]), [V]\rangle_{A^K} &= \dim_K \mathrm{Hom}_{A^K}(P^K, V) = \dim_{\mathscr{O}} \mathrm{Hom}_{A^{\mathscr{O}}}(P, \widetilde{V}) \\
&= \dim_{\mathrm{k}(\mathfrak{m})} \mathrm{Hom}_{A^{\mathscr{O}}(\mathfrak{m})}(P/\mathfrak{m}P, \widetilde{V}/\mathfrak{m}\widetilde{V}) \\
&= \dim_{\mathrm{k}(\mathfrak{p})} \mathrm{Hom}_{A(\mathfrak{p})}(\bar{P}, \bar{V}) \\
&= \langle [\bar{P}], \mathrm{d}_A^{\mathfrak{p},\mathscr{O}}([V])\rangle_{A(\mathfrak{p})}.
\end{aligned}$$

Proving the commutativity of diagram (55) amounts to proving that $\mathrm{c}_{A(\mathfrak{p})}([\bar{P}]) = \mathrm{d}_A^{\mathfrak{p},\mathscr{O}} \circ \mathrm{c}_{A^K} \circ \mathrm{e}_A^{\mathfrak{p},\mathscr{O}}([\bar{P}])$ for every finitely generated projective $A(\mathfrak{p})$-module $\bar{P}$. To prove this, note that the diagram

$$\begin{array}{ccc}
\mathrm{K}_0(A^{\mathscr{O}}(\mathfrak{m})) & \xrightarrow{\mathrm{c}_{A^{\mathscr{O}}(\mathfrak{m})}} & \mathrm{G}_0(A^{\mathscr{O}}(\mathfrak{m})) \\
{\scriptstyle \mathrm{e}_A^{\mathfrak{p},\mathfrak{m}}}\uparrow & & \uparrow{\scriptstyle \mathrm{d}_A^{\mathfrak{p},\mathfrak{m}}} \\
\mathrm{K}_0(A(\mathfrak{p})) & \xrightarrow[\mathrm{c}_{A(\mathfrak{p})}]{} & \mathrm{G}_0(A(\mathfrak{p}))
\end{array}$$

commutes. As above we know that there exists a finitely generated projective $A^{\mathscr{O}}$-module P such that $(\mathrm{e}_A^{\mathfrak{p},\mathfrak{m}})^{-1}([P/\mathfrak{m}P]) = [\bar{P}]$ and $\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}([\bar{P}]) = [P^K]$. Since P is a finitely generated projective $A^{\mathscr{O}}$-module and A is a finite $\mathscr{O}$-module, it follows that P is also a finitely generated projective $\mathscr{O}$-module. As $\mathscr{O}$ is a discrete valuation ring, we conclude that P is actually $\mathscr{O}$-free of finite rank. Hence, P is an $A^{\mathscr{O}}$-lattice in P^K and therefore

$$\begin{aligned}
\mathrm{d}_A^{\mathfrak{p},\mathscr{O}} \circ \mathrm{c}_{A^K} \circ \mathrm{e}_A^{\mathfrak{p},\mathscr{O}}([\bar{P}]) &= \mathrm{d}_A^{\mathfrak{p},\mathscr{O}}([P^K]) = (\mathrm{d}_A^{\mathfrak{p},\mathfrak{m}})^{-1}([P/\mathfrak{m}P]) \\
&= (\mathrm{d}_A^{\mathfrak{p},\mathfrak{m}})^{-1} \circ \mathrm{c}_{A(\mathfrak{m})}([P/\mathfrak{m}P]) \\
&= \mathrm{c}_{A(\mathfrak{p})} \circ (\mathrm{e}_A^{\mathfrak{p},\mathfrak{m}})^{-1}([P/\mathfrak{m}P]) = \mathrm{c}_{A(\mathfrak{p})}([\bar{P}]).
\end{aligned}$$

If R is normal, then the independence of $\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}$ from the choice of $\mathscr{O}$ follows from the independence of $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}$ from the choice of $\mathscr{O}$ and the fact that $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}$ has at most one adjoint. $\square$

6B. ***Preservation of simple modules vs. preservation of blocks.*** In [Thiel 2016] we studied the set

(57) $$\mathrm{DecGen}(A) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathrm{d}_A^{\mathfrak{p},\mathscr{O}} \text{ is trivial for any } A\text{-gate in } \mathfrak{p}\},$$

where $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}$ being *trivial* means that it induces a bijection between simple modules. We have proven in [Thiel 2016, Theorem 2.3] that $\mathrm{DecGen}(A)$ is open if R is noetherian and A has split fibers. Brauer reciprocity implies that $\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}$ is trivial if and only if $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}$ is trivial, so we deduce that the locus of all $\mathfrak{p}$ such that $\mathrm{e}_A^{\mathfrak{p},\mathscr{O}}$ is trivial for any $\mathscr{O}$ is an open subset of $\mathrm{Spec}(R)$.

If $\mathfrak{p} \in \mathrm{DecGen}(A)$, then the simple modules of A^K and $A(\mathfrak{p})$ are "essentially the same"; in particular their dimensions are the same. This is why explicit knowledge about $\mathrm{DecGen}(A)$ is quite helpful to understand the representation theory of the fibers of A; see [Thiel 2016]. So far, we do not have an explicit description of $\mathrm{DecGen}(A)$, however. Brauer reciprocity enables us to prove the following relation between decomposition maps and blocks.

Theorem 6.3. *We have the inclusion*

(58) $$\mathrm{DecGen}(A) \subseteq \mathrm{BlGen}(A).$$

Proof. Let $\mathfrak{p} \in \mathrm{Spec}(R)$ be nonzero. By assumption there is a perfect A-gate $\mathscr{O}$ in $\mathfrak{p}$. If $\mathfrak{p} \in \mathrm{DecGen}(A)$, then by definition $\mathrm{d}_A^{\mathfrak{p},\mathscr{O}}$ is trivial, so the matrix $\mathrm{D}_A^{\mathfrak{p},\mathscr{O}}$ of this morphism in bases given by isomorphism classes of simple modules of A^K and $A(\mathfrak{p})$, respectively, is equal to the identity matrix when ordering the bases appropriately. It now follows from Brauer reciprocity, Theorem 6.2, that $\mathrm{C}_{A(\mathfrak{p})} = \mathrm{C}_{A^K}$ in appropriate bases, where $\mathrm{C}_{A(\mathfrak{p})}$ is the matrix of the Cartan map $\mathrm{c}_{A(\mathfrak{p})}$ and C_{A^K} is the matrix of the Cartan map c_{A^K}. Due to the linkage relation explained in Section 2, the families of A^K and of $A(\mathfrak{p})$ are determined by the respective Cartan matrices. Since $\mathrm{C}_{A(\mathfrak{p})} = \mathrm{C}_{A^K}$, it follows that $\#\mathrm{Bl}(A(\mathfrak{p})) = \#\mathrm{Bl}(A^K)$, so $\mathfrak{p} \in \mathrm{BlGen}(A)$. □

Remark 6.4. Suppose that A has split fibers and that R is noetherian. Then the fact that $\#\mathrm{Bl}(A(\mathfrak{p})) = \#\mathrm{Bl}(Z(\mathfrak{p}))$ by Theorem 5.8 together with Lemma A.9 yields the equivalence

(59) $$\mathfrak{p} \in \mathrm{BlGen}(A) \iff \dim_K(Z^K + \mathrm{Rad}(A^K)) = \dim_{\mathrm{k}(\mathfrak{p})}(Z(\mathfrak{p}) + \mathrm{Rad}(A(\mathfrak{p}))).$$

Let $\mathscr{O}$ be a perfect A-gate in $\mathfrak{p}$. This exists by Lemma 6.1(b). Suppose that $\mathfrak{p} \in \mathrm{DecGen}(A)$. In [Thiel 2016, Theorem 2.2] we have proven that this implies

$$\dim_K \mathrm{Rad}(A^K) = \dim_{\mathrm{k}(\mathfrak{p})} \mathrm{Rad}(A(\mathfrak{p})).$$

Let $X := Z + J$, where $J := \mathrm{Rad}(A^K) \cap A^{\mathscr{O}}$. The arguments in [Thiel 2016] show that X is an $A^{\mathscr{O}}$-lattice of $Z^K + \mathrm{Rad}(A^K)$ and that the reduction in the maximal ideal $\mathfrak{m}$ of $\mathscr{O}$ is equal to $Z^{\mathscr{O}}(\mathfrak{m}) + \mathrm{Rad}(A^{\mathscr{O}}(\mathfrak{m}))$. We thus have

$$\dim_K(Z^K + \mathrm{Rad}(A^K)) = \dim_{\mathrm{k}(\mathfrak{m})}(Z^{\mathscr{O}}(\mathfrak{m}) + \mathrm{Rad}(A^{\mathscr{O}}(\mathfrak{m}))).$$

Since $A(\mathfrak{p})$ splits, the $\mathrm{k}(\mathfrak{m})$-dimension of $Z^{\mathscr{O}}(\mathfrak{m})+\mathrm{Rad}(A^{\mathscr{O}}(\mathfrak{m}))$ is equal to the $\mathrm{k}(\mathfrak{p})$-dimension of $Z(\mathfrak{p})+\mathrm{Rad}(A(\mathfrak{p}))$. Hence, we have $\mathfrak{p} \in \mathrm{BlGen}(A)$ by (59). This yields another proof of the inclusion $\mathrm{DecGen}(A) \subseteq \mathrm{BlGen}(A)$ in the case A has split fibers.

Example 6.5. The following example due to C. Bonnafé shows that in the generality of Theorem 6.3 we do not have equality in (58). Let R be a discrete valuation ring with fraction field K and uniformizer π; i.e., $\mathfrak{p} := (\pi)$ is the maximal ideal of R. Denote by $k := R/\mathfrak{p}$ the residue field in $\mathfrak{p}$. Let

$$A := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(R) \;\middle|\; b, c \in \mathfrak{p} \right\}.$$

This is an R-subalgebra of $\mathrm{Mat}_2(R)$ and it is R-free with basis

$$e := E_{11},\ f := E_{22},\ x := \pi E_{12},\ y := \pi E_{21}, \tag{60}$$

where $E_{ij} = (\delta_{i,k}\delta_{j,l})_{kl}$ is the elementary matrix. Clearly, $A^K = \mathrm{Mat}_2(K)$, so the generic fiber of A is split semisimple. In particular, A^K has just one block, and this block contains just one simple module we denote by S. Now, consider the specialization $\bar{A} := A(\mathfrak{p}) = A/\mathfrak{p}A$. We know from Corollary A.14 that the quotient map $A \twoheadrightarrow \bar{A}$, $a \mapsto \bar{a}$, is block bijective, so we must have $\#\mathrm{Bl}(A(\mathfrak{p})) \le \mathrm{Bl}(A^K)$ and therefore $\#\mathrm{Bl}(A(\mathfrak{p})) = 1$, so $\mathfrak{p} \in \mathrm{BlGen}(A)$. Let $\bar{J}$ be the k-subspace of $\bar{A}$ generated by $\bar{x}$ and $\bar{y}$. This is in fact a two-sided ideal of $\bar{A}$ since it is stable under multiplication by the generators (60). Moreover, we have $\bar{x}^2 = 0 = \bar{y}^2$, so $\bar{J}$ is a nilpotent ideal of $\bar{A}$. Hence, $\dim_k \mathrm{Rad}(\bar{A}) \ge 2$. The number of simple modules of $\bar{A}$ is by [Lam 1991, Theorem 7.17] equal to $\dim_k \bar{A}/(\mathrm{Rad}(\bar{A}) + [\bar{A}, \bar{A}])$, so $\#\,\mathrm{Irr}\,\bar{A} \le 2$ since $\dim_k \bar{A} = \dim_K A^K = 4$. The two elements $\bar{e}$ and $\bar{f}$ are orthogonal idempotents and so the constituents of the two $\bar{A}$-modules $\bar{A}\bar{e}$ and $\bar{A}\bar{f}$ are nonisomorphic. So, we have $\#\,\mathrm{Irr}\,\bar{A} \ge 2$ and due to the aforementioned we conclude that $\#\,\mathrm{Irr}\,\bar{A} = 2$. Let $\bar{S}_1$ and $\bar{S}_2$ be these two simple modules. Since R is a discrete valuation ring, reduction modulo $\mathfrak{p}$ yields the well-defined decomposition map $\mathrm{d}_A^{\mathfrak{p}} : \mathrm{G}_0(A^K) \to \mathrm{G}_0(A(\mathfrak{p}))$; see [Thiel 2016, Corollary 1.14]. It is an elementary fact that all simple $\bar{A}$-modules must be constituents of $\mathrm{d}_A^{\mathfrak{p}}([S]) = [S/\mathfrak{p}S]$. Since $\dim_K S = 2$, the only possibility is that $\mathrm{d}_A^{\mathfrak{p}}([S]) = [\bar{S}_1] + [\bar{S}_2]$ and $\dim_k \bar{S}_i = 1$. In particular, $\mathfrak{p} \notin \mathrm{DecGen}(A)$, so $\mathfrak{p} \in \mathrm{BlGen}(A) \setminus \mathrm{DecGen}(A)$. Finally, we note that $\bar{A}$ also splits since $\#\,\mathrm{Irr}(\bar{A}) = 2$ implies by the above formula that $\dim_k \mathrm{Rad}(\bar{A}) = 2$ and we have

$$\dim_k \bar{A} = \dim_k \mathrm{Rad}(\bar{A}) + \sum_{i=1}^{2} (\dim_k \bar{S}_i)^2,$$

so $\bar{A}$ is split by [Lam 1991, Corollary 7.8].

Lemma 6.6. *Assume that the A^K-families are singletons, and that* $\#\operatorname{Irr} A(\mathfrak{p}) \le \#\operatorname{Irr} A^K$ *for all* $\mathfrak{p} \in \operatorname{Spec}(R)$. *Then*

$$\operatorname{BlGen}(A) \setminus \operatorname{DecGen}(A) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathrm{D}_A^{\mathfrak{p}} \text{ is diagonal but not the identity}\}.$$

Proof. Since the A^K-families are singletons, we have $\#\operatorname{Irr}(A^K) = \#\operatorname{Bl}(A^K)$. We clearly have $\#\operatorname{Irr} A(\mathfrak{p}) \ge \#\operatorname{Bl}(A(\mathfrak{p}))$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$. Assume that $\mathfrak{p} \in \operatorname{BlGen}(A)$. Then we have $\#\operatorname{Irr} A(\mathfrak{p}) \ge \#\operatorname{Irr}(A^K)$, so $\#\operatorname{Irr} A(\mathfrak{p}) = \#\operatorname{Irr} A^K$ by our assumption. Hence, the decomposition matrix $\mathrm{D}_A^{\mathfrak{p}}$ is quadratic. By Theorem 6.9 the $\mathfrak{p}$-families are equal to the Brauer $\mathfrak{p}$-families. Since $\mathfrak{p} \in \operatorname{BlGen}(A)$ and the A^K-families are singletons, it follows that $\mathrm{D}_A^{\mathfrak{p}}$ is a diagonal matrix. The claim is now obvious. □

Lemma 6.7. *Let R be a noetherian integral domain with fraction field K and let A be a cellular R-algebra of finite dimension such that A^K is semisimple. Then* $\operatorname{DecGen}(A) = \operatorname{BlGen}(A)$.

Proof. First of all, specializations of A are again cellular by [Graham and Lehrer 1996, 1.8]. Moreover, it follows from Proposition 3.2 of the same paper that A has split fibers, so A satisfies Lemma 6.1(b) and therefore our basic assumption in this paragraph. Let Λ be the poset of the cellular structure of A^K. Since A^K is semisimple, each cell module M_λ has simple head S_λ and $\#\operatorname{Irr} A^K = \#\Lambda$. Let $\mathfrak{p} \in \operatorname{Spec}(R)$. The poset for the cellular structure of $A(\mathfrak{p})$ is again Λ. Denote by $M_\lambda^{\mathfrak{p}}$ the corresponding cell modules of $A(\mathfrak{p})$. There is a subset Λ' of Λ such that $M_\lambda^{\mathfrak{p}}$ has simple head $S_\lambda^{\mathfrak{p}}$ for all $\lambda \in \Lambda'$ and that these heads are precisely the simple $A(\mathfrak{p})$-modules. In particular, we have $\#\operatorname{Irr} A(\mathfrak{p}) \le \#\operatorname{Irr} A^K$. Now, assume that $\mathfrak{p} \in \operatorname{BlGen}(A)$. By Lemma 6.6 we just need to show that the decomposition matrix $\mathrm{D}_A^{\mathfrak{p}}$, which is square by the proof of Lemma 6.6, cannot be a nonidentity diagonal matrix. By [Graham and Lehrer 1996, Proposition 3.6] we know that $[M_\lambda : S_\lambda] = 1$ and $[M_\lambda^{\mathfrak{p}} : S_\lambda^{\mathfrak{p}}] = 1$. By construction, it is clear that $\mathrm{d}_A^{\mathfrak{p}}([M_\lambda]) = [M_\lambda^{\mathfrak{p}}]$. Hence, if $\mathrm{d}_A^{\mathfrak{p}}([S_\lambda]) = n_\lambda [S_\lambda^{\mathfrak{p}}]$, we have $n_\lambda = [M_\lambda^{\mathfrak{p}} : S_\lambda^{\mathfrak{p}}] = 1$. Hence, $\mathrm{D}_A^{\mathfrak{p}}$ is the identity matrix, so $\mathfrak{p} \in \operatorname{BlGen}(A)$. □

6C. *The Brauer graph.* Geck and Pfeiffer [2000] introduced the so-called Brauer $\mathfrak{p}$-graph of A in our general context but assumed that A^K is semisimple so that the A^K-families are singletons. For general A this definition seems not to be the correct one. We introduce the following generalization of this concept.

Definition 6.8. Suppose that R is normal so that we have unique decomposition maps. The *Brauer $\mathfrak{p}$-graph* of A is the graph with vertices the simple A^K-modules and an edge between S and T if and only if in the A^K-family of S there is some S' and in the A^K-family of T there is some T' such that $\mathrm{d}_A^{\mathfrak{p}}([S'])$ and $\mathrm{d}_A^{\mathfrak{p}}([T'])$ have a common constituent. The connected components of this graph are called the *Brauer $\mathfrak{p}$-families* of A.

If the A^K-families are singletons, we have an edge between S and T if and only if $\mathrm{d}_A^{\mathfrak{p}}([S])$ and $\mathrm{d}_A^{\mathfrak{p}}([T])$ have a common constituent, so this indeed generalizes the Brauer $\mathfrak{p}$-graph from [Geck and Pfeiffer 2000] for A^K semisimple. Our final theorem shows that decomposition maps are compatible with $\mathfrak{p}$-families and $A(\mathfrak{p})$-families, and relates the Brauer $\mathfrak{p}$-families to the $\mathfrak{p}$-families.

Theorem 6.9. *Assume that R is normal. The following hold*:

(a) *A finite-dimensional A^K-module V belongs to a $\mathfrak{p}$-block of A if and only if $\mathrm{d}_A^{\mathfrak{p}}([V])$ belongs to a block of $A(\mathfrak{p})$.*

(b) *Two finite-dimensional A^K-modules V and W lie in the same $\mathfrak{p}$-block if and only if $\mathrm{d}_A^{\mathfrak{p}}([V])$ and $\mathrm{d}_A^{\mathfrak{p}}([W])$ lie in the same block of $A(\mathfrak{p})$.*

(c) *If $\mathcal{F} \in \mathrm{Fam}_{\mathfrak{p}}(A)$ is a $\mathfrak{p}$-family, then*

$$\mathrm{d}_A^{\mathfrak{p}}(\mathcal{F}) := \{T \mid T \text{ is a constituent of } \mathrm{d}_A^{\mathfrak{p}}([S]) \text{ for some } S \in \mathcal{F}\}$$

is a family of $A(\mathfrak{p})$, and all families of $A(\mathfrak{p})$ are obtained in this way.

(d) *The Brauer $\mathfrak{p}$-families are equal to the $\mathfrak{p}$-families.*

Proof. (a) By assumption there is a perfect A-gate $\mathscr{O}$ in $\mathfrak{p}$. Let $\mathfrak{m}$ be the maximal ideal of $\mathscr{O}$. We have the following commutative diagram of canonical morphisms which are all idempotent stable:

$$\begin{tikzcd} A_{\mathfrak{p}} \arrow[r, hook] \arrow[d, two heads] & A^{\mathscr{O}} \arrow[r, hook] \arrow[d, two heads] & A^K \\ A(\mathfrak{p}) \arrow[r, hook] & A^{\mathscr{O}}(\mathfrak{m}) & \end{tikzcd} \tag{61}$$

Since R is assumed to be normal, it follows from Proposition 4.2 that $A_{\mathfrak{p}} \twoheadrightarrow A(\mathfrak{p})$ is block bijective. By assumption the morphism $\mathrm{d}_A^{\mathfrak{p},\mathfrak{m}} : \mathrm{G}_0(A(\mathfrak{p})) \to \mathrm{G}_0(A^{\mathscr{O}}(\mathfrak{m}))$ is an isomorphism and therefore $A(\mathfrak{p}) \hookrightarrow A^{\mathscr{O}}(\mathfrak{m})$ is block bijective by Theorem 4.1. Furthermore, by assumption the generic fiber A^K is split and therefore $A^{\mathscr{O}} \twoheadrightarrow A^{\mathscr{O}}(\mathfrak{m})$ is block bijective by Corollary A.14. Because of (5) it thus follows that $A_{\mathfrak{p}} \hookrightarrow A^{\mathscr{O}}$ is block bijective.

Now, let V be a finite-dimensional A^K-module and let $\widetilde{V}$ be an $A^{\mathscr{O}}$-lattice of V. Suppose that V belongs to an $A_{\mathfrak{p}}$-block of A^K. Since $A_{\mathfrak{p}} \hookrightarrow A^{\mathscr{O}}$ is block bijective, the $A_{\mathfrak{p}}$-blocks of A^K coincide with the $A^{\mathscr{O}}$-blocks of A^K and therefore V belongs to an $A^{\mathscr{O}}$-block of A^K. Since $\widetilde{V}$ is $\mathscr{O}$-free, it follows from Lemma A.1 that $\widetilde{V}$ belongs to a block of $A^{\mathscr{O}}$. Again by Lemma A.1 and the fact that $A^{\mathscr{O}} \twoheadrightarrow A^{\mathscr{O}}(\mathfrak{m})$ is block bijective, it follows that $\widetilde{V}/\mathfrak{m}\widetilde{V}$ belongs to a block of $A^{\mathscr{O}}(\mathfrak{m})$. Since $A(\mathfrak{p}) \hookrightarrow A^{\mathscr{O}}(\mathfrak{m})$ is block bijective, Lemma A.1 shows that $\mathrm{d}_A^{\mathfrak{p}}([V])$ belongs to a block of $A(\mathfrak{p})$.

Conversely, suppose that $\mathrm{d}_A^{\mathfrak{p}}([V])$ belongs to a block of $A(\mathfrak{p})$. Then $\widetilde{V}/\mathfrak{m}\widetilde{V}$ belongs to a block of $A^{\mathscr{O}}(\mathfrak{m})$ and therefore $\widetilde{V}$ belongs to a block of $A^{\mathscr{O}}$ by Lemma A.1.

But then V belongs to an $A^{\mathscr{O}}$-block of A^K and thus to an $A_{\mathfrak{p}}$-block of A^K by Lemma A.1.

(b) This follows now from part (a).

(c) Fix a $\mathfrak{p}$-family $\mathcal{F}$ of A^K. If $S \in \mathcal{F}$, then $\mathrm{d}_A^{\mathfrak{p}}([S])$ belongs to an $A(\mathfrak{p})$-block by (a) and therefore all constituents of $\mathrm{d}_A^{\mathfrak{p}}([S])$ belong to a fixed family $\bar{\mathcal{F}}_S$. If $S' \in \mathcal{F}$ is another simple module, then by (b) the constituents of $\mathrm{d}_A^{\mathfrak{p}}([S'])$ also lie in $\bar{\mathcal{F}}_S$. Hence, $\mathrm{d}_A^{\mathfrak{p}}(\mathcal{F})$ is contained in a fixed $A(\mathfrak{p})$-family $\bar{\mathcal{F}}$. Let $T \in \bar{\mathcal{F}}$ be arbitrary. Due to the properties of decomposition maps there is some $S \in \mathrm{Irr}\, A^K$ such that T is a constituent of $\mathrm{d}_A^{\mathfrak{p}}([S])$. Since T and $\mathrm{d}_A^{\mathfrak{p}}([S])$ lie in the same $A(\mathfrak{p})$-block by (a) and (b), we must have $S \in \mathcal{F}$ by (b). Hence, $\bar{\mathcal{F}} = \mathrm{d}_A^{\mathfrak{p}}(\mathcal{F})$ is an $A(\mathfrak{p})$-family. Since every simple $A(\mathfrak{p})$-module is a constituent of $\mathrm{d}_A^{\mathfrak{p}}([S])$ for some simple A^K-module S, it is clear that any $A(\mathfrak{p})$-family is of the form $\mathrm{d}_A^{\mathfrak{p}}(\mathcal{F})$ for a $\mathfrak{p}$-family $\mathcal{F}$.

(d) Let S and T be simple A^K-modules contained in the same Brauer $\mathfrak{p}$-family; i.e., in the A^K-family of S there is some S' and in the A^K-family of T there is some T' such that $\mathrm{d}_A^{\mathfrak{p}}([S'])$ and $\mathrm{d}_A^{\mathfrak{p}}([T'])$ have a common constituent. It follows from part (b) that S' and T' lie in the same $\mathfrak{p}$-family of A^K. Since S' is in the same A^K-family as S, it is also in the same $\mathfrak{p}$-family as S because the $\mathfrak{p}$-families are unions of A^K-families. Similarly, T' is in the same $\mathfrak{p}$-family as T. Hence, S and T lie in the same $\mathfrak{p}$-family.

Conversely, suppose that S and T lie in the same $\mathfrak{p}$-family. We have to show that they lie in the same Brauer $\mathfrak{p}$-family. Let $(S_i)_{i=1}^n$ be a system of representatives of the isomorphism classes of simple A^K-modules and let $(U_j)_{j=1}^m$ be a system of representatives of the isomorphism classes of simple $A(\mathfrak{p})$-modules. Let $\mathscr{Q} := (Q_i)_{i=1}^n$ with Q_i being the projective cover of S_i, and let $\mathscr{P} := (P_j)_{j=1}^m$ with P_j being the projective cover of U_j. Let $\mathrm{C}_{A(\mathfrak{p})}$ be the matrix of the Cartan map $\mathrm{c}_{A(\mathfrak{p})}$ with respect to the chosen bases, and similarly let C_{A^K} be the matrix of c_{A^K}. Furthermore, let $\mathrm{D}_A^{\mathfrak{p}}$ be the matrix of $\mathrm{d}_A^{\mathfrak{p}}$ with respect to the chosen bases. Since

$$\mathrm{C}_{A(\mathfrak{p})} = \mathrm{D}_A^{\mathfrak{p}} \mathrm{C}_{A^K} (\mathrm{D}_A^{\mathfrak{p}})^{\mathrm{T}}$$

by Brauer reciprocity, Theorem 6.2, we have

$$(\mathrm{C}_{A(\mathfrak{p})})_{p,q} = (\mathrm{D}_A^{\mathfrak{p}} \mathrm{C}_{A^K} (\mathrm{D}_A^{\mathfrak{p}})^{\mathrm{T}})_{p,q} = \sum_{k,l=1}^{n} (\mathrm{D}_A^{\mathfrak{p}})_{p,k} (\mathrm{C}_{A^K})_{k,l} (\mathrm{D}_A^{\mathfrak{p}})_{q,l} \tag{62}$$

for all p, q. Let U be a constituent of $\mathrm{d}_A^{\mathfrak{p}}([S])$ and let V be a constituent of $\mathrm{d}_A^{\mathfrak{p}}([T])$. Since S and T lie in the same $\mathfrak{p}$-family of A^K, both $\mathrm{d}_A^{\mathfrak{p}}([S])$ and $\mathrm{d}_A^{\mathfrak{p}}([T])$ lie in the same block of $A(\mathfrak{p})$ by (b), and therefore U and V lie in the same family of $A(\mathfrak{p})$. As the families of $A(\mathfrak{p})$ are equal to the $\mathscr{P}$-families of $A(\mathfrak{p})$ by Section 2, there exist functions $f : [1, r] \to [1, m]$, $g : [1, r-1] \to [1, m]$ with the following properties: $U_{f(1)} = U$, $U_{f(r)} = V$, and for any $j \in [1, r-1]$ both $P_{f(j)}$ and $P_{f(j+1)}$ have $U_{g(j)}$

as a constituent. We can visualize the situation as follows:

$$\begin{tikzcd}
P_{f(j)} & & P_{f(j+1)} \\
U_{f(j)} \arrow[u] & U_{g(j)} \arrow[ul] \arrow[ur] & U_{f(j+1)} \arrow[u]
\end{tikzcd}$$

where an arrow $U \to P$ signifies that U is a constituent of P. For any $j \in [1, r-1]$ we have $(\mathrm{C}_{A(\mathfrak{p})})_{g(j),f(j)} \neq 0$ and so it follows from (62) that there are indices $k(j)$ and $l(j)$ such that

$$(\mathrm{D}_A^{\mathfrak{p}})_{g(j),k(j)} \neq 0, \quad (\mathrm{C}_{A^K})_{k(j),l(j)} \neq 0, \quad (\mathrm{D}_A^{\mathfrak{p}})_{f(j),l(j)} \neq 0.$$

Similarly, since $(\mathrm{C}_{A(\mathfrak{p})})_{g(j),f(j+1)} \neq 0$, there exist indices $k'(j)$ and $l'(j)$ such that

$$(\mathrm{D}_A^{\mathfrak{p}})_{g(j),k'(j)} \neq 0, \quad (\mathrm{C}_{A^K})_{k'(j),l'(j)} \neq 0, \quad (\mathrm{D}_A^{\mathfrak{p}})_{f(j+1),l'(j)} \neq 0.$$

This can be visualized as follows:

$$\begin{tikzcd}
\mathrm{d}_A^{\mathfrak{p}}([S_{l(j)}]) \arrow[r, dash, dashed] & \mathrm{d}_A^{\mathfrak{p}}([S_{k(j)}]) & & \mathrm{d}_A^{\mathfrak{p}}([S_{k'(j)}]) \arrow[r, dash, dashed] & \mathrm{d}_A^{\mathfrak{p}}([S_{l'(j)}]) \\
U_{f(j)} \arrow[u] & & U_{g(j)} \arrow[ul] \arrow[ur] & & U_{f(j+1)} \arrow[u]
\end{tikzcd}$$

Here, the dashed edges in the upper row signify that the respective simple A^K-modules lie in the same A^K-family. Since $U_{f(1)} = U$ and $U_{f(r)} = V$, this shows that S and T lie in the same Brauer $\mathfrak{p}$-family of A^K. □

7. Semicontinuity of blocks in the case of a nonsplit generic fiber

Let A be a finite flat algebra over an integral domain R with fraction field K. We have the map

$$\#\mathrm{Bl}'_A : \mathrm{Spec}(R) \to \mathbb{N}, \quad \mathfrak{p} \mapsto \#\mathrm{Bl}(A(\mathfrak{p})); \tag{63}$$

i.e., $\#\mathrm{Bl}'_A(\mathfrak{p})$ is the number of blocks of the *specialization* $A(\mathfrak{p})$. Recall that in (21) we considered the map $\#\mathrm{Bl}_A$ with $\#\mathrm{Bl}_A(\mathfrak{p}) = \#\mathrm{Bl}(A_{\mathfrak{p}})$ being the number of blocks of the *localization* $A_{\mathfrak{p}}$. In the case R is normal and A^K splits, we know from Proposition 4.2 that $\#\mathrm{Bl}'_A = \#\mathrm{Bl}_A$. In particular, the map $\#\mathrm{Bl}'_A$ is lower semicontinuous and thus defines a stratification of $\mathrm{Spec}(R)$, the block number stratification; see Section 3B.

In the case A^K does not split, it still makes perfect sense to consider the map (63) and ask if it is lower semicontinuous so that we have a stratification of $\mathrm{Spec}(R)$ by the number of blocks of specializations. But since we do not have the connection from Proposition 4.2 between blocks of localizations and blocks of specializations anymore, we cannot directly apply the results from Section 3.

In this section, we will establish a setting where the map $\#\mathrm{Bl}'_A$ is still lower semicontinuous without assuming that the generic fiber A^K splits, the main result being Corollary 7.3. To achieve this, however, we have to restrict this map to a subset of $\mathrm{Spec}(R)$. As we will see, in general it is not possible to have lower semicontinuity on all of $\mathrm{Spec}(R)$.

First of all, because of the difference between blocks of localizations and blocks of specializations, we introduce the sets

$$\beta(A) := \max\{\#\mathrm{Bl}(A(\mathfrak{p})) \mid \mathfrak{p} \in \mathrm{Spec}(R)\}, \tag{64}$$

$$\mathrm{BlEx}'(A) := \#\mathrm{Bl}'^{-1}_A(\leq \beta(A) - 1), \tag{65}$$

$$\mathrm{BlGen}'(A) := \mathrm{Spec}(R) \setminus \mathrm{BlEx}'(A). \tag{66}$$

Note that if R is normal and A^K splits, then $\beta(A) = \#\mathrm{Bl}(A^K)$, so $\mathrm{BlEx}'(A) = \mathrm{BlEx}(A)$ and $\mathrm{BlGen}'(A) = \mathrm{BlGen}(A)$, as defined in (19) and (20).

Now, assume that R' is an integral extension of R which is also an integral domain. Let K' be the fraction field of R' and let $\psi : \mathrm{Spec}(R') \twoheadrightarrow \mathrm{Spec}(R)$ be the morphism induced by $R \subseteq R'$. The scalar extension $A' := R' \otimes_R A$ is again a finitely presented flat R'-algebra (using Remark 3.2). For any $\mathfrak{p} \in \mathrm{Spec}(R)$ and any $\mathfrak{p}' \in \mathrm{Spec}(R')$ lying over $\mathfrak{p}$ we have the diagram

$$\begin{tikzcd} & A'_{\mathfrak{p}'} \arrow[d, two heads] \\ A(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}A_{\mathfrak{p}} \arrow[r, hook] & A'(\mathfrak{p}') = A'_{\mathfrak{p}'}/\mathfrak{p}'_{\mathfrak{p}'}A'_{\mathfrak{p}'} \end{tikzcd} \tag{67}$$

and it then follows from (5) that

$$\#\mathrm{Bl}(A(\mathfrak{p})) \leq \#\mathrm{Bl}(A'(\mathfrak{p}')) \geq \#\mathrm{Bl}(A'_{\mathfrak{p}'}). \tag{68}$$

Let X be a set contained in

$$X_{R'}(A) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \#\mathrm{Bl}(A(\mathfrak{p})) = \#\mathrm{Bl}(A'(\mathfrak{p}')) = \#\mathrm{Bl}(A'_{\mathfrak{p}'}) \text{ for all } \mathfrak{p}' \in \psi^{-1}(\mathfrak{p})\}. \tag{69}$$

We have seen in Corollary 4.3 that in the case R is normal and A^K splits we can choose $R = R'$ and have $X = \mathrm{Spec}(R)$. In general X will be a proper subset of $\mathrm{Spec}(R)$ and we have to choose R' appropriately to enlarge it a bit more. Let us first concentrate on what we can say when restricting to X. We introduce the following restricted versions of our invariants:

$$\#\mathrm{Bl}'_{A,X} := \#\mathrm{Bl}'_A|_X : X \to \mathbb{N}, \tag{70}$$

$$\#\mathrm{Bl}'^{-1}_{A,X}(\leq n) := \#\mathrm{Bl}'^{-1}_A(\leq n) \cap X = \psi(\#\mathrm{Bl}^{-1}_{A'}(\leq n)) \cap X, \tag{71}$$

$$\#\mathrm{Bl}'^{-1}_{A,X}(n) := \#\mathrm{Bl}'^{-1}_{A}(n) \cap X = \psi(\#\mathrm{Bl}^{-1}_{A'}(n)) \cap X, \tag{72}$$

$$\beta_X(A) := \max\{\#\mathrm{Bl}(A(\mathfrak{p})) \mid \mathfrak{p} \in X\}, \tag{73}$$

$$\mathrm{BlEx}'_X(A) := \mathrm{Bl}'^{-1}_{A,X}(\leq \beta_X(A) - 1), \tag{74}$$

$$\mathrm{BlGen}'_X(A) := X \setminus \mathrm{BlEx}'_X(A). \tag{75}$$

Corollary 7.1. *The map* $X \to \mathbb{N}$, $\mathfrak{p} \mapsto \#\mathrm{Bl}(A(\mathfrak{p}))$, *is lower semicontinuous on* X, *so* $X = \coprod_{n \in \mathbb{N}} \mathrm{Bl}'^{-1}_{A,X}(n)$ *is a stratification of* X *into locally closed subsets. Moreover*,

$$\beta_X(A) \leq \#\mathrm{Bl}(A^{K'}). \tag{76}$$

Proof. Since ψ is a closed morphism and $\#\mathrm{Bl}^{-1}_{A'}(\leq n)$ is closed in $\mathrm{Spec}(R')$ by (26), it follows that $\psi(\#\mathrm{Bl}^{-1}_{A'}(\leq n))$ is closed in $\mathrm{Spec}(R)$, hence $\#\mathrm{Bl}'^{-1}_{A,X}(\leq n)$ is closed in X by (71). Since

$$\#\mathrm{Bl}'^{-1}_{A,X}(n) = \#\mathrm{Bl}'^{-1}_{A,X}(\leq n) \setminus \#\mathrm{Bl}'^{-1}_{A,X}(\leq n-1),$$

it is clear that $\#\mathrm{Bl}'^{-1}_{A,X}(n)$ is locally closed in X. We have seen in (27) that

$$\overline{\#\mathrm{Bl}^{-1}_{A'}(n)} \subseteq \bigcup_{m \leq n} \mathrm{Bl}^{-1}_{A'}(m).$$

Hence, since ψ is closed, we obtain

$$\overline{\#\mathrm{Bl}'^{-1}_{A,X}(n)} = \psi(\overline{\#\mathrm{Bl}^{-1}_{A'}(n)}) \cap X \subseteq \bigcup_{m \leq n} \psi(\#\mathrm{Bl}^{-1}_{A'}(m)) \cap X = \bigcup_{m \leq n} \#\mathrm{Bl}'^{-1}_{A,X}(m). \quad \square$$

Note that in (76) we could only bound $\beta_X(A)$ above by $\#\mathrm{Bl}(A^{K'})$, and not by $\#\mathrm{Bl}(A^K)$. In fact, we will see in Example 7.4 that we may indeed have $\beta_X(A) > \#\mathrm{Bl}(A^K)$ in general. This is an important difference to blocks of localizations where we always have the maximal number of blocks in the generic point.

In the following lemma we describe a situation where we have $\beta_X(A) = \#\mathrm{Bl}(A^{K'})$. We recall that X is called *very dense* if the embedding $X \hookrightarrow \mathrm{Spec}(R)$ is a *quasihomeomorphism*; i.e., the map $Z \mapsto Z \cap X$ is a bijection between the closed (equivalently, open) subsets of the two spaces. This notion was introduced by Grothendieck [1966, §10].

Lemma 7.2. *Suppose that* X *is* ***very dense*** *in* $\mathrm{Spec}(R)$, *that* R *is noetherian*, *and that* ψ *is finite. Then* $\beta_X(A) = \#\mathrm{Bl}(A^{K'})$, *and thus* $\mathrm{BlEx}'_X(A) = \psi(\mathrm{BlEx}(A')) \cap X$. *If moreover* R' *is normal and* R *is universally catenary*, *then* $\mathrm{BlEx}'_X(A)$ *is a reduced Weil divisor in* X.

Proof. The assumptions imply that R' is noetherian, too. We know from Theorem 3.3 that $\mathrm{BlGen}(A')$ is a nonempty open subset of $\mathrm{Spec}(R')$. In particular, it is constructible. Since $\mathrm{Spec}(R)$ is quasicompact, the morphism ψ is quasicompact by

[Görtz and Wedhorn 2010, Remark 10.2.(1)]. It thus follows from Chevalley's constructibility theorem, see [Görtz and Wedhorn 2010, Corollary 10.71], that $\psi(\mathrm{BlGen}(A'))$ is constructible in $\mathrm{Spec}(R)$. Since X is very dense in $\mathrm{Spec}(R)$, we conclude that $\psi(\mathrm{BlGen}(A')) \cap X \neq \varnothing$ by [Grothendieck 1966, Proposition 10.1.2]. Hence, there is $\mathfrak{p} \in X$ and $\mathfrak{p}' \in \mathrm{BlGen}(A')$ with $\psi(\mathfrak{p}') = \mathfrak{p}$. But then we have $\#\mathrm{Bl}(A(\mathfrak{p})) = \#\mathrm{Bl}(A'(\mathfrak{p}')) = \#\mathrm{Bl}(A^{K'})$, so $\beta_X(A) = \#\mathrm{Bl}(A^{K'})$. Now, assume that R' is normal and R is universally catenary. We know that $\mathrm{BlEx}(A')$ is either empty or pure of codimension 1 in $\mathrm{Spec}(R')$ by Corollary 3.5. In [Huneke and Swanson 2006, Theorem B.5.1] it is shown that the extension $R \subseteq R'$ satisfies the dimension formula; hence $\psi(\mathrm{BlEx}(A'))$ is either empty or pure of codimension 1. Since X is very dense in $\mathrm{Spec}(R)$, the same is also true for

$$X \cap \psi(\mathrm{BlEx}(A')) = \mathrm{BlEx}'_X(A). \qquad \square$$

Corollary 7.3. *Suppose that R is a finite-type algebra over an algebraically closed field. Let X be the set of closed points of* $\mathrm{Spec}(R)$. *Then the map $X \to \mathbb{N}$, $\mathfrak{m} \mapsto \#\mathrm{Bl}(A(\mathfrak{m}))$, is lower semicontinuous and so $X = \coprod_{n\in\mathbb{N}} \#\mathrm{Bl}'^{-1}_{A,X}(n)$ is a stratification of X. Moreover, $\beta_X(A) = \#\mathrm{Bl}(A^{\overline{K}})$, where $\overline{K}$ is an algebraic closure of K. If R is also universally catenary, then $\mathrm{BlEx}'_X(A)$ is a reduced Weil divisor in X.*

Proof. Let K' be a finite extension of K such that $A^{K'}$ splits (this is always possible, see [Curtis and Reiner 1981, Proposition 7.13]) and let R' be the integral closure of R in K'. Now, $\#\mathrm{Bl}(A'(\mathfrak{p}')) = \#\mathrm{Bl}(A'_{\mathfrak{p}'})$ for all $\mathfrak{p}' \in \mathrm{Spec}(R)$ by Proposition 4.2. Since R is a finite-type algebra over an algebraically closed field k, the residue field in a closed point $\mathfrak{m}$ of $\mathrm{Spec}(R)$ is just k. Hence, the specialization $A(\mathfrak{m})$ is a finite-dimensional algebra over an algebraically closed field, thus splits and we therefore have $\#\mathrm{Bl}(A(\mathfrak{m})) = \#\mathrm{Bl}(A'(\mathfrak{m}'))$ for any $\mathfrak{m}' \in \psi^{-1}(\mathfrak{m})$ by Lemma A.3. Hence, $X \subseteq X_{R'}(A)$. The claim about semicontinuity and the stratification thus follows from Corollary 7.1. It is shown in [Görtz and Wedhorn 2010, Proposition 3.35] that X is very dense in $\mathrm{Spec}(R)$. Since R is a finite-type algebra over a field, it is Japanese, so ψ is a finite morphism. Hence, $\beta_X(A) = \#\mathrm{Bl}(A^{K'}) = \#\mathrm{Bl}(A^{\overline{K}})$ by Lemma 7.2. The claim that $\mathrm{BlEx}'_X(A)$ is a reduced Weil divisor if R is universally catenary also follows from Lemma 7.2. $\square$

Example 7.4. The following example due to K. Brown shows that in the setting of Corollary 7.3 we may indeed have $\beta_X(A) > \#\mathrm{Bl}(A^K)$ so that the map $\mathfrak{p} \mapsto \#\mathrm{Bl}(A(\mathfrak{p}))$ will not be lower semicontinuous on the whole of $\mathrm{Spec}(R)$. Let k be an algebraically closed field of characteristic zero, let X be an indeterminate over k, let $R := k[X^n]$ for some $n > 1$, and let $A := k[X]$. Let C_n be the cyclic group of order n. We fix a generator of C_n and let it act on X by multiplication with a primitive n-th root of unity. Then $R = k[X]^{C_n}$, so A is free of rank n over R. Moreover, $\mathrm{Frac}(A) = k(X)$ is a Galois extension of degree n of $K := \mathrm{Frac}(R)$

by [Benson 1993, Proposition 1.1.1], so in particular $K \neq k(X)$ since $n > 1$. By [Goodearl and Warfield 2004, Exercise 6R] we have

$$A^K = A \otimes_R K = A[(R \setminus \{0\})^{-1}] = \mathrm{Frac}(A) = k(X),$$

so the K-algebra $A^K = \mathrm{Z}(A^K)$ is *not* split (and thus also not block-split by Lemma A.3). It is clear that

$$\#\,\mathrm{Bl}(A^K) = 1. \tag{77}$$

Now, let $\mathfrak{m} := (X^n - 1) \in \mathrm{Max}(R)$. Then $\mathrm{k}(\mathfrak{p}) = k$ and since k is algebraically closed, we have $A(\mathfrak{m}) = A/\mathfrak{m}A \simeq k^n$ as k-algebras. In particular,

$$\#\,\mathrm{Bl}(A(\mathfrak{m})) = n > 1 = \#\,\mathrm{Bl}(A^K). \tag{78}$$

We close with a setting where our base ring is not necessarily normal but we still get a global result on $\mathrm{Spec}(R)$.

Lemma 7.5. *Suppose that A has split fibers*; *i.e.*, *$A(\mathfrak{p})$ splits for all $\mathfrak{p} \in \mathrm{Spec}(R)$. Then the map $\mathrm{Spec}(R) \to \mathbb{N}$, $\mathfrak{p} \mapsto \#\,\mathrm{Bl}(A(\mathfrak{p}))$, is lower semicontinuous and so $\mathrm{Spec}(R) = \coprod_{n\in\mathbb{N}} \mathrm{Bl}_A'^{-1}(n)$ is a partition into locally closed subsets. Moreover*, *$\beta(A) = \#\,\mathrm{Bl}(A^K)$. If R is also universally catenary*, *Japanese*, *and noetherian*, *then $\mathrm{BlEx}'(A)$ is a reduced Weil divisor in $\mathrm{Spec}(R)$.*

Proof. Let R' be the integral closure of R in K. Then $\#\,\mathrm{Bl}(A'(\mathfrak{p}')) = \#\,\mathrm{Bl}(A'_{\mathfrak{p}'})$ for all $\mathfrak{p}' \in \mathrm{Spec}(R')$ by Proposition 4.2. Since $A(\mathfrak{p})$ splits, we moreover have $\#\,\mathrm{Bl}(A(\mathfrak{p})) = \#\,\mathrm{Bl}(A'(\mathfrak{p}'))$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$ $\mathfrak{p}' \in \psi^{-1}(\mathfrak{p})$ by Lemma A.3. Hence, $X_{R'}(A) = \mathrm{Spec}(R)$. The claim about semicontinuity and the partition follows from Corollary 7.1. Now, assume that R is universally catenary, Japanese, and noetherian. Since R is Japanese, it follows by definition that ψ is finite. The claim about $\mathrm{BlEx}'(A)$ being a reduced Weil divisor now follows from Lemma 7.2. □

Appendix A: More on base change of blocks

In this appendix we collect several facts about base change of blocks. Some results here should also be of independent interest.

Block compatibility of scalar extension of modules. Recall the decomposition of the module category of a ring A relative to a decomposition of $1 \in A$ into pairwise orthogonal central idempotents described in Section 2. We have the following compatibility.

Lemma A.1. *Let $\phi : R \to S$ be a morphism of commutative rings and let A be an R-algebra. Suppose that ϕ_A is central idempotent stable and let V be a nonzero A-module. In any of the following cases the A-module V belongs to the block c_i if and only if the A^S-module V^S belongs to the ϕ-block $\phi_A(c_i)$:*

(a) *ϕ is injective and V is R-projective.*

(b) *ϕ is faithfully flat.*

(c) *R is local or a principal ideal domain and V is R-free.*

Proof. As $c_j V$ is a direct summand of V, it follows that we have a canonical isomorphism between isomorphisms $\phi_A^*(c_j V) \simeq \phi_A(c_j)\phi_A^* V$ of A^S-modules for all j. The claim thus holds if we can show that no nonzero direct summand V' of V is killed by ϕ_A^*, i.e., $\phi_A^* V' \neq 0$. But this is implied by the assumptions in each case. Namely, in the first two cases it follows from Lemma 2.1 that ϕ_V is injective, which implies that $\phi_{V'}$ is also injective, so $\phi_A^* V'$ cannot be zero for nonzero V'. In the third case neither ϕ nor ϕ_V needs to be injective, so this needs extra care. First of all, since V is assumed to be R-free, the assumptions on R imply that a direct summand V' of V, which a priori is only R-projective, is already R-free, too. In the case R is local, this follows from Kaplansky's theorem [1958] and in the case R is a principal ideal domain, this is a standard fact. Now, if V is R-free with basis $(v_\lambda)_{\lambda \in \Lambda}$, then it is a standard fact, see [Bourbaki 1989, II, §5.1, Proposition 4], that $\phi_A^* V$ is S-free with basis $(\phi_V(v_\lambda))_{\lambda \in \Lambda}$. This shows that $\phi_A^* V \neq 0$ for any nonzero R-free A-module V. This applied to direct summands of V, which are R-free as shown, proves the claim. □

Field extensions. Throughout this paragraph let A be a finite-dimensional algebra over a field K. From (5) we know that $\#\,\mathrm{Bl}(A) \leq \#\,\mathrm{Bl}(A^L)$ for any extension field L of K.

Definition A.2. We say that A is *block-split* if $\#\,\mathrm{Bl}(A) = \#\,\mathrm{Bl}(A^L)$ for any extension field L of K.

Our aim is to show the following lemma.

Lemma A.3. *If* $\mathrm{Z}(A)$ *is a split K-algebra* (*e.g., if A itself splits*), *then A is block-split. The converse holds if K is perfect.*

The first assertion of the lemma is essentially obvious since $\mathrm{Z}(A)$ is semiperfect and therefore

$$\#\,\mathrm{Bl}(A) = \#\,\mathrm{Bl}(\mathrm{Z}(A)) = \mathrm{rk}_{\mathbb{Z}}\ \mathrm{K}_0(\mathrm{Z}(A)) = \#\mathrm{rk}_{\mathbb{Z}}\ \mathrm{G}_0(\mathrm{Z}(A)) = \#\,\mathrm{Irr}\,\mathrm{Z}(A), \tag{79}$$

where the second equality follows from the fact that idempotents in a commutative ring are isomorphic if and only if they are equal; see [Lam 1991, §22, Exercise 2]. The same equalities of course also hold for $\mathrm{Z}(A)^L = \mathrm{Z}(A^L)$, where L is an extension field of K. Hence, if $\mathrm{Z}(A)$ is split, then A is block-split. If A itself is split, it is a standard fact that its center splits, so A is block-split.

We will prove the converse (assuming that K is perfect) from a more general point of view as the results might be of independent interest and we reuse some of them in the last section. First of all, the field extension $K \subseteq L$ induces natural group morphisms

$$\mathrm{d}_A^L : \mathrm{G}_0(A) \to \mathrm{G}_0(A^L) \quad \text{and} \quad \mathrm{e}_A^L : \mathrm{K}_0(A) \to \mathrm{K}_0(A^L). \tag{80}$$

Without any assumptions on the field K we have the following property.

Lemma A.4. *The morphisms* d_A^L *and* e_A^L *are injective.*

Proof. Let $(S_i)_{i\in I}$ be a system of representatives of the isomorphism classes of simple A-modules. For each i let $(T_{ij})_{j\in J_i}$ be a system of representatives of the isomorphism classes of simple A^L-modules which occur as constituents of S_i^L. Then by [Lam 1991, Proposition 7.13] the set $(T_{ij})_{i\in I, j\in J_i}$ is a system of representatives of the isomorphism classes of simple A^L-modules. Hence, the matrix D_A^L of d_A^L in bases given by the isomorphism classes of simple modules is in column-echelon form, has no zero columns, and no zero rows. In particular, d_A^L is injective.

For each $i \in I$ let P_i be the projective cover of S_i and for each $j \in J_i$ let Q_{ij} be the projective cover of T_{ij}. By the above, $(Q_{ij})_{i\in I, j\in J_i}$ is a system of representatives of the isomorphism classes of projective indecomposable A^L-modules. We claim that in the direct sum decomposition of the finitely generated projective A^L-module P_i^L into projective indecomposable A^L-modules, only the Q_{ij} with $j \in J_i$ occur. With the same argument as above, this implies that e_A^L is injective. So, let us write $P_i^L = \bigoplus_{\lambda\in\Lambda} U_\lambda$ for (not necessarily nonisomorphic) projective indecomposable A^L-modules U_λ. The U_λ are the, up to isomorphism, unique projective indecomposable A^L-modules occurring as direct summands of P_i^L. As the radical is additive by [Lam 1991, Proposition 24.6(ii)], we have $\mathrm{Rad}(P_i^L) = \bigoplus_{\lambda\in\Lambda} \mathrm{Rad}(U_\lambda)$, so

$$S_i^L = (P_i/\mathrm{Rad}(P_i))^L = P_i^L/\mathrm{Rad}(P_i)^L = \bigoplus_{\lambda\in\Lambda} U_\lambda/(\mathrm{Rad}(P_i)^L \cap U_\lambda). \tag{81}$$

Moreover, we have $\mathrm{Rad}(P_i)^L \subseteq \mathrm{Rad}(P_i^L)$. This follows from the fact that $\mathrm{Rad}(A)^L \subseteq \mathrm{Rad}(A^L)$ by [Lam 1991, Theorem 5.14] and the fact that $\mathrm{Rad}(P_i) = \mathrm{Rad}(A)P_i$ and $\mathrm{Rad}(P_i^L) = \mathrm{Rad}(A^L)P_i^L$ by [Lam 1991, Theorem 24.7] since P_i and P_i^L are projective. For each $\lambda \in \Lambda$ the radical of U_λ is a proper submodule of U_λ and therefore

$$\mathrm{Rad}(P_i)^L \cap U_\lambda \subseteq \mathrm{Rad}(P_i^L) \cap U_\lambda = \mathrm{Rad}(U_\lambda) \subsetneq U_\lambda.$$

Hence, the head of U_λ is a constituent of $U_\lambda/(\mathrm{Rad}(P_i^L) \cap U_\lambda)$, and since all constituents of the latter are constituents of S_i^L, we must have $\mathrm{Hd}(U_\lambda) \simeq S_{ij_\lambda}$ for some $j_\lambda \in J_i$ by the above. This implies that $U_\lambda = Q_{ij_\lambda}$, thus proving the claim. □

Lemma A.5. *The following hold*:

(a) *The morphism* d_A^L *is an isomorphism if and only if it induces a bijection between isomorphism classes of simple modules. Similarly, the morphism* e_A^L

is an isomorphism if and only if it induces a bijection between isomorphism classes of projective indecomposable modules.

(b) *If* d_A^L *is an isomorphism, so is* e_A^L*. The converse holds if* K *is perfect.*

For the proof of Lemma A.5 we will need the following well-known elementary lemma that is also used in the last section. Recall from (52) the intertwining form $\langle \cdot , \cdot \rangle_A$ of A.

Lemma A.6. *Let* P *be a projective indecomposable* A*-module and let* V *be a finitely generated* A*-module. Then*

$$\langle [P], [V] \rangle_A = [V : \mathrm{Hd}(P)] \cdot \dim_K \mathrm{End}_A(\mathrm{Hd}(P)), \tag{82}$$

where $\mathrm{Hd}(P) = P / \mathrm{Rad}(P)$ *is the head of* P*. In particular,* $\langle \cdot , \cdot \rangle_A$ *is nondegenerate.*

Proof. We first consider the case $V = \mathrm{Hd}(P)$. Let $f \in \mathrm{Hom}_A(P, \mathrm{Hd}(P))$ be nonzero. Since $\mathrm{Hd}(P)$ is simple, this morphism is already surjective and thus induces an isomorphism $P/\mathrm{Ker}(f) \cong \mathrm{Hd}(P)$. But as $\mathrm{Rad}(P)$ is the unique maximal submodule of P, we must have $\mathrm{Ker}(f) = \mathrm{Rad}(P)$ and thus get an induced morphism $\mathrm{Hd}(P) \to \mathrm{Hd}(P)$. This yields a K-linear morphism $\Phi : \mathrm{Hom}_A(P, \mathrm{Hd}(P)) \to \mathrm{End}_A(\mathrm{Hd}(P))$. On the other hand, if $f \in \mathrm{End}_A(\mathrm{Hd}(P))$, then composing it with the quotient morphism $P \to P/\mathrm{Rad}(P) = \mathrm{Hd}(P)$ yields a morphism $P \to \mathrm{Hd}(P)$. In this way we also get a K-linear morphism $\Psi : \mathrm{End}_A(\mathrm{Hd}(P)) \to \mathrm{Hom}_A(P, \mathrm{Hd}(P))$. By construction, Φ and Ψ are pairwise inverse; hence

$$\langle [P], [\mathrm{Hd}(P)] \rangle_A = \dim_K \mathrm{Hom}_A(P, \mathrm{Hd}(P)) = \dim_K \mathrm{End}_A(\mathrm{Hd}(P))$$

as claimed.

Now, suppose that V is a simple A-module not isomorphic to $\mathrm{Hd}(P)$. We can write $P = Ae$ for some primitive idempotent $e \in A$. Since A is artinian, e is already local and now it follows from [Lam 1991, Proposition 21.19] that $\mathrm{Hom}_A(Ae, V)$ is nonzero if and only if V has a constituent isomorphic to $\mathrm{Hd}(Ae)$. This is not true by assumption, and therefore $\mathrm{Hom}_A(P, V) = 0$, so $\langle [P], [V] \rangle_A = 0$.

Finally, for V general we have $[V] = \sum_{S \in \mathrm{Irr}\, A} [V : S][S]$ in $\mathrm{G}_0(A)$. By the above we get

$$\begin{aligned}\langle [P], [V] \rangle_A &= \sum_{S \in \mathrm{Irr}\, A} [V : S] \langle [P], [S] \rangle_A = [V : \mathrm{Hd}(P)] \langle [P], [\mathrm{Hd}(P)] \rangle_A \\ &= [V : \mathrm{Hd}(P)] \cdot \dim_K \mathrm{End}_A(\mathrm{Hd}(P))\end{aligned}$$

as claimed. It follows that the Gram matrix $\mathscr{G}$ of $\langle \cdot , \cdot \rangle$ with respect to the basis $(\mathrm{P}(S))_{S \in \mathrm{Irr}\, A}$ of $\mathrm{K}_0(A)$ and the basis $(S)_{S \in \mathrm{Irr}\, A}$ of $\mathrm{G}_0(A)$ is diagonal with positive diagonal entries. The determinant of $\mathscr{G}$ is thus a nonzero divisor on $\mathbb{Z}$ and since both $\mathrm{K}_0(A)$ and $\mathrm{G}_0(A)$ are $\mathbb{Z}$-free of the same finite dimension, it follows that $\langle \cdot , \cdot \rangle_A$ is nondegenerate; see [Scheja and Storch 1988, Satz 70.5]. □

Proof of Lemma A.5. We use the same notation as in the proof of Lemma A.4. Since ${}_AA$ is a projective A-module, there is a decomposition ${}_AA = \bigoplus_{i \in I} P_i^{r_i}$ for some $r_i \in \mathbb{N}$. Using Lemma A.6 we see that

$$\begin{aligned}\dim_K \mathrm{Hd}(P_j) &= \langle [{}_AA], [\mathrm{Hd}(P_j)] \rangle_A \\ &= \sum_{i \in I} r_i \langle [P_i], [\mathrm{Hd}(P_j)] \rangle_A = r_j \langle [P_j], [\mathrm{Hd}(P_j)] \rangle_A \\ &= r_j \dim_K \mathrm{End}_A(\mathrm{Hd}(P_i)).\end{aligned}$$

Hence, $r_i = n_i / m_i$, where $n_i := \dim_K S_i$ and $m_i := \dim_K \mathrm{End}_A(S_i)$. In particular,

$$\dim_K A = \sum_{i \in I} \frac{n_i}{m_i} \dim_K P_i. \tag{83}$$

Now, suppose that d_A^L is an isomorphism. Then clearly $\#\,\mathrm{Irr}\,A = \#\,\mathrm{Irr}\,A^L$. The properties of the matrix D_A^L of the morphism d_A^L derived in the proof of Lemma A.4 immediately imply D_A^L is diagonal. Since it is invertible with natural numbers on the diagonal, it must already be the identity matrix; i.e., d_A^L induces a bijection between the isomorphism classes of simple modules. In particular, $(S_i^L)_{i \in I}$ is a system of representatives of the isomorphism classes of simple A^L-modules. The properties of the matrix E_A^L of e_A^L derived in the proof of Lemma A.4 now imply that we must have $P_i^L \simeq Q_i^{s_i}$ for some $s_i \in \mathbb{N}$. We argue that $s_i = 1$. This shows that e_A^L is an isomorphism inducing a bijection between the isomorphism classes of projective indecomposable modules. In the same way we deduced (83) we now get

$$\dim_K A = \dim_L A^L = \sum_{i \in I} \frac{n_i'}{m_i'} \dim_L Q_i \tag{84}$$

with

$$n_i' = \dim_L \mathrm{Hd}(Q_i) = \dim_L S_i^L = \dim_K S_i = n_i$$

and

$$m_i' = \dim_L \mathrm{End}_{A^L}(\mathrm{Hd}(Q_i)) = \dim_L \mathrm{End}_{A^L}(S_i^L) = \dim_K \mathrm{End}_K(S_i) = m_i,$$

using the fact that $L \otimes_K \mathrm{End}_A(S_i) \simeq \mathrm{End}_{A^L}(S_i^L)$; see [Reiner 2003, Theorem 2.38]. Since $\dim_L Q_i \le \dim_L P_i^L = \dim_K P_i$, (83) and (84) imply that $\dim_L Q_i = \dim_K P_i$, so $Q_i = P_i^L$.

Conversely, suppose that e_A^L is an isomorphism. With the properties of the matrix E_A^L of e_A^L established in the proof of Lemma A.4, we see much as above that e_A^L already induces a bijection between the projective indecomposable modules. In particular, $P_i^L \simeq Q_i$. Due to the properties of the matrix D_A^L of d_A^L established in the proof of Lemma A.4, the only constituent of S_i^L is T_i. Since P_i is the projective cover of P_i, we have a surjective morphism $\phi : P_i \twoheadrightarrow S_i$ with $\mathrm{Ker}(\phi) = \mathrm{Rad}(P_i)$. Scalar extension induces a surjective morphism $\phi^L : P_i^L \twoheadrightarrow S_i^L$ with $\mathrm{Ker}(\phi^L) =$

$\mathrm{Ker}(\phi)^L = \mathrm{Rad}(P_i)^L \subseteq \mathrm{Rad}(P_i^L)$. It thus follows from [Curtis and Reiner 1981, Corollary 6.25(i)] that P_i^L is the projective cover of S_i^L. Now, we assume that K is perfect. Then by [loc. cit., Theorem 7.5] all simple A-modules are separable, so $S_i^L = T_i^{s_i}$ for some s_i. Since projective covers are additive, we get $P_i^L = Q_i^{s_i}$. As $P_i^L = Q_i$, this implies that $s_i = 1$, so $S_i^L = T_i$ is simple. Hence, d_A^L induces a bijection between the isomorphism classes of simple modules. □

Remark A.7. With the same arguments as in the proof of Lemma A.5 we can show that the converse in Lemma A.5(b) still holds when we only assume that all simple A-modules are separable, i.e., they remain semisimple under field extension. This holds for example when A splits or if A is a group algebra (over any field). We do not know whether it holds more generally.

Proof of Lemma A.3. Let $Z := \mathrm{Z}(A)$. Suppose that L is an extension field of K with $\#\,\mathrm{Bl}(A) = \#\,\mathrm{Bl}(A^L)$. By (79) we know that $\#\,\mathrm{Irr}\, Z = \#\,\mathrm{Irr}\, Z^L$. The arguments in the proof of Lemma A.4 thus imply that the matrix D_A^L of the morphism $\mathrm{d}_Z^L : \mathrm{G}_0(Z) \to \mathrm{G}_0(Z^L)$ must be a diagonal matrix. We claim that it is the identity matrix. Since this holds for any L, it means that the simple modules of Z remain simple under any field extension, so Z splits. Our assumption implies that Z and Z^L have the same number of primitive idempotents, so every primitive idempotent $e \in Z$ remains primitive in Z^L. This shows that $\mathrm{e}_A^L : \mathrm{K}_0(Z) \to \mathrm{K}_0(Z^L)$ induces a bijection between projective indecomposable modules. In particular, it is an isomorphism. Now, Lemma A.5 shows that also d_A^L is an isomorphism. Since its matrix D_A^L is invertible with natural numbers on the diagonal, it must be the identity. □

Remark A.8. In the proof of Lemma A.3 we have deduced that for a commutative finite-dimensional K-algebra Z the condition $\mathrm{rk}_{\mathbb{Z}}\, \mathrm{K}_0(Z) = \mathrm{rk}_{\mathbb{Z}}\, \mathrm{K}_0(Z^L)$ already implies that e_Z^L induces a bijection between projective indecomposable modules. This follows from the fact that idempotents in a commutative ring are isomorphic if and only if they are equal. This is not true for a noncommutative ring A. Here, we can have $\mathrm{rk}_{\mathbb{Z}}\, \mathrm{K}_0(A) = \mathrm{rk}_{\mathbb{Z}}\, \mathrm{K}_0(A^L)$ but still a primitive idempotent $e \in A$ can split into a sum of *isomorphic* orthogonal primitive idempotents of A^L. Then the matrix E_A^L of e_A^L is diagonal but not the identity.

Let us record the following additional fact:

Lemma A.9. *If* $\mathrm{Z}(A)$ *splits*, *then*

$$\begin{aligned} \#\,\mathrm{Bl}(A) &= \dim_K \mathrm{Z}(A) - \dim_K \mathrm{Rad}(\mathrm{Z}(A)) \\ &= \dim_K \mathrm{Z}(A) - \dim_K (\mathrm{Z}(A) \cap \mathrm{Rad}(A)). \end{aligned} \tag{85}$$

Proof. This is an immediate consequence of (79) and the fact that $\mathrm{Rad}(\mathrm{Z}(A)) = \mathrm{Z}(A) \cap \mathrm{Rad}(A)$ since $\mathrm{Z}(A) \subseteq A$ is a finite normalizing extension; see [Lorenz 1981, Theorem 1.5]. □

Reductions. Now, we consider a situation which in a sense is opposite to the one considered in the last paragraph; namely we consider the quotient morphism $\phi : R \twoheadrightarrow R/\mathfrak{m} =: S$ for a local commutative ring R with maximal ideal $\mathfrak{m}$ and a finitely generated R-algebra A. By Lemma 2.3(b) the morphism $\phi_A : A \twoheadrightarrow A^S \simeq A/\mathfrak{m}A =: \overline{A}$ is idempotent stable. We say that ϕ is *idempotent surjective* if for each idempotent $e' \in A^S$ there is an idempotent $e \in A$ with $\phi_A(e) = e'$. We say that ϕ_A is *primitive idempotent bijective* if it induces a bijection between the *isomorphism classes* of primitive idempotents of A and the isomorphism classes of primitive idempotents of A^S. The question of whether ϕ_A is idempotent surjective is precisely the question of whether idempotents of $\overline{A}$ can be lifted to A, and this is a classical topic in ring theory. The following lemma is standard; we omit the proof.

Lemma A.10. *If $\phi_A : A \twoheadrightarrow \overline{A}$ is idempotent surjective, it is primitive idempotent bijective and block bijective.*

Theorem A.11 [Neunhöffer 2003, Proposition 5.10]. *The morphism $\phi_A : A \twoheadrightarrow \overline{A}$ is idempotent surjective if and only if A is semiperfect.*

We recall two standard situations of idempotent surjective reductions.

Lemma A.12. *In the following two cases the morphism $\phi_A : A \twoheadrightarrow \overline{A}$ is idempotent surjective*:

(a) *R is noetherian and $\mathfrak{m}$-adically complete.*

(b) *R is henselian.*

Proof. For a proof of the first case, see [Lam 1991, Proposition 21.34]. For a proof of the second case assuming that A is *commutative*, see [Raynaud 1970, I, §3, Proposition 2]. To give a proof for noncommutative A let $\bar{e} \in \overline{A}$ be an idempotent. Let $k := R/\mathfrak{m}$ and let $\overline{B} := k[\bar{e}]$ be the k-subalgebra of $\overline{A}$ generated by $\bar{e}$. Since $\overline{A}$ is a finite-dimensional k-algebra, also $\overline{B}$ is finite-dimensional. Moreover, $\overline{B}$ is commutative. Let $e \in A$ be an arbitrary element with $\phi_A(e) = \bar{e}$. Let $B := R[e]$, a commutative subalgebra of A. Note that $\overline{B} = B/\mathfrak{m}B$. Since A is a finitely generated R-module, the Cayley–Hamilton theorem implies that B is a finitely generated R-algebra. Now, by the commutative case, the map $\phi_B : B \twoheadrightarrow \overline{B}$ is idempotent surjective and so there is an idempotent $e' \in B \subseteq A$ with $\phi_A(e') = \phi_B(e') = \bar{e}$. This shows that ϕ_A is idempotent surjective. □

The next theorem was again proven by Neunhöffer [2003, Proposition 6.2]. It is one of our key ingredients in proving Brauer reciprocity for decomposition maps in a general setting.

Theorem A.13 (M. Neunhöffer). *Suppose that R is a valuation ring with fraction field K and that A is a finite flat R-algebra with split generic fiber A^K. If $\widehat{R} \otimes_R A$ is semiperfect*, *where $\widehat{R}$ is the completion of R with respect to the topology defined by a valuation on K defining R*, *then also A is semiperfect.*

Corollary A.14 (J. Müller, M. Neunhöffer). *Suppose that R is a discrete valuation ring and that A is a finite flat R-algebra with split generic fiber. Then A is semiperfect. In particular, $\phi_A : A \twoheadrightarrow \bar{A}$ is primitive idempotent bijective and block bijective.*

Proof. Since R is a discrete valuation ring, its valuation topology coincides with its $\mathfrak{m}$-adic topology so that the topological completion $\widehat{R}$ is $\hat{\mathfrak{m}}$-adically complete, where $\mathfrak{m}$ denotes the maximal ideal of R and $\hat{\mathfrak{m}}$ denotes the maximal ideal of $\widehat{R}$. Hence, $\widehat{R} \otimes_R A$ is semiperfect by Lemma A.12(a) and Theorem A.11. Now, Theorem A.13 shows that A is semiperfect, too. □

Remark A.15. One part of Corollary A.14, the fact that idempotents lift, was also stated earlier by Curtis and Reiner [1981, Exercise 6.16] in the special case where A^K is assumed to be semisimple. The semisimplicity assumption was later removed by J. Müller [1995, Satz 3.4.1] using the Wedderburn–Malcev theorem (this can be applied without a perfectness assumption on the base field if A^K splits since then $A^K / \operatorname{Rad}(A^K)$ is separable; see [Curtis and Reiner 1962, Theorem 72.19]).

Appendix B: Further elementary facts

Here, we prove three further elementary facts that we used in the paper.

Lemma B.1. *A finitely generated module M over an integral domain R is flat if and only if it is faithfully flat. In particular, if $M \neq 0$, we have $0 \neq \mathrm{k}(\mathfrak{p}) \otimes_R M = M(\mathfrak{p})$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$.*

Proof. We can assume that $M \neq 0$. Since M is flat, it is torsion-free and so the localization map $M \to M_\mathfrak{p}$ is injective; see Lemma 2.1(c). Hence, $M_\mathfrak{p} \neq 0$. Since M is a finitely generated R-module, also $M_\mathfrak{p}$ is a finitely generated $R_\mathfrak{p}$-module and now Nakayama's lemma implies that $0 \neq M_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} M_\mathfrak{p} = \mathrm{k}(\mathfrak{p}) \otimes_R M$. Hence, M is faithfully flat by [Matsumura 1986, Theorem 7.2]. □

Lemma B.2. *Let A be a finite flat algebra over an integral domain R. Then the structure map $R \to A$, $r \mapsto r \cdot 1_A$, is injective. Hence, we can identify $R \subseteq \mathrm{Z}(A)$. If R is noetherian, the induced map $\Upsilon : \operatorname{Spec}(\mathrm{Z}(A)) \to \operatorname{Spec}(R)$ is finite, closed, and surjective.*

Proof. It follows from Lemma B.1 that A is already faithfully flat. Let $\phi : R \to A$ be the structure map. This is an R-module map and applying $- \otimes_R A$ yields a map

$$A \simeq R \otimes_R A \xrightarrow{\phi \otimes_R A} A \otimes_R A$$

of right A-modules, mapping a to $1 \otimes a$. This map has an obvious section mapping $a \otimes a'$ to aa'; hence it is injective. Since A is faithfully flat, the original map ϕ has to be injective, too. As the image of ϕ is contained in the center Z of A, the structure map is actually an injective map $R \hookrightarrow Z$. Now, assume that R is noetherian. Since

A is a finitely generated R-module, also Z is a finitely generated R-module. Hence, $R \subseteq Z$ is a finite ring extension and now it is an elementary fact that Υ is closed and surjective. □

The following lemma about base change of homomorphism spaces is well known but we could not find a reference in this generality; see [Bourbaki 1972, II, §5.3] for a proof in the case of a *commutative* base ring.

Lemma B.3. *Let A be an algebra over a commutative ring R and let $\phi : R \to S$ be a morphism into a commutative ring S. Let V and W be A-modules. If V is finitely generated and projective as an A-module, then there is a canonical S-module isomorphism*:

$$S \otimes_R \operatorname{Hom}_A(V, W) \simeq \operatorname{Hom}_{A^S}(V^S, W^S). \tag{86}$$

Proof. We can define a map $\gamma : S \otimes_R \operatorname{Hom}_A(V, W) \to \operatorname{Hom}_{A^S}(V^S, W^S)$ by mapping $s \otimes f$ with $s \in S$ and $f \in \operatorname{Hom}_A(V, W)$ to $s_r \otimes f$, where s_r denotes right multiplication by s. It is a standard fact that this is an S-module morphism; see [Reiner 2003, (2.36)]. Recall that $\operatorname{Hom}_A(-, W)$ commutes with *finite* direct sums by [Bourbaki 1989, II, §1.6, Corollary 1 to Proposition 6]. This shows that the canonical isomorphism $\operatorname{Hom}_A(A, W) \simeq W$ induces a canonical isomorphism $\operatorname{Hom}_A(A^n, W) \simeq W^n$ for any $n \in \mathbb{N}$ and now we conclude that there is a canonical isomorphism

$$S \otimes_R \operatorname{Hom}_A(A^n, W) \simeq S \otimes_R W^n \simeq (S \otimes_R W)^n \simeq \operatorname{Hom}_{A^S}((A^S)^n, W^S),$$

which is easily seen to be equal to γ. The assertion thus holds for finitely generated *free* A-modules. Now, the assumption on V allows us to write without loss of generality $A^n = V \oplus X$ for some A-module X. It is not hard to see that we get a commutative diagram

$$\begin{array}{ccc} S \otimes_R \operatorname{Hom}_A(A^n, W) & \xrightarrow{\simeq} & (S \otimes_R \operatorname{Hom}_A(V, W)) \oplus (S \otimes_R \operatorname{Hom}_A(X, W)) \\ \simeq\downarrow & & \downarrow \qquad\qquad\qquad\qquad \downarrow \\ \operatorname{Hom}_{A^S}((A^S)^n, W^S) & \xrightarrow{\simeq} & (\operatorname{Hom}_{A^S}(V^S, W^S)) \oplus (\operatorname{Hom}_{A^S}(X^S, W^S)) \end{array}$$

where the horizontal morphisms are obtained by the projections and the vertical morphisms are the morphisms γ in the respective situation. The commutativity of this diagram implies that the morphism $S \otimes_R \operatorname{Hom}_A(V, W) \to \operatorname{Hom}_{A^S}(V^S, W^S)$ also has to be an isomorphism. □

Acknowledgements

I would like to thank Cédric Bonnafé for many helpful discussions about this topic, for providing Example 6.5, and for showing and explaining to me the relevant part of the manuscript [Bonnafé and Rouquier 2017]. That manuscript is without doubt one of the main motivations for this paper. I would furthermore like to thank Gwyn Bellamy, Ken Brown, Meinolf Geck, and Gunter Malle for commenting on parts of a preliminary version of this article. Moreover, I thank Ken Brown for providing Example 7.4. I was partially supported by DFG SPP 1489 and by the Australian Research Council Discovery Projects grant no. DP160103897.

References

[Benson 1993] D. J. Benson, *Polynomial invariants of finite groups*, London Mathematical Society Lecture Note Series **190**, Cambridge University Press, 1993. MR Zbl

[Bonnafé and Rouquier 2017] C. Bonnafé and R. Rouquier, "Cherednik algebras and Calogero–Moser cells", preprint, 2017. arXiv

[Bourbaki 1972] N. Bourbaki, *Elements of mathematics: commutative algebra*, Hermann, Paris, 1972. MR Zbl

[Bourbaki 1989] N. Bourbaki, *Algebra, I: Chapters 1–3*, Springer, 1989. MR Zbl

[Brauer and Nesbitt 1941] R. Brauer and C. Nesbitt, "On the modular characters of groups", *Ann. of Math.* (2) **42** (1941), 556–590. MR Zbl

[Brown and Goodearl 2002] K. A. Brown and K. R. Goodearl, *Lectures on algebraic quantum groups*, Birkhäuser, Basel, 2002. MR Zbl

[Brown and Gordon 2001] K. A. Brown and I. Gordon, "The ramification of centres: Lie algebras in positive characteristic and quantised enveloping algebras", *Math. Z.* **238**:4 (2001), 733–779. MR Zbl

[Brown and Gordon 2002] K. A. Brown and I. Gordon, "The ramifications of the centres: quantised function algebras at roots of unity", *Proc. London Math. Soc.* (3) **84**:1 (2002), 147–178. MR Zbl

[Chlouveraki 2009] M. Chlouveraki, *Blocks and families for cyclotomic Hecke algebras*, Lecture Notes in Mathematics **1981**, Springer, 2009. MR Zbl

[Curtis and Reiner 1962] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics **11**, Interscience, New York, 1962. MR Zbl

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

[Donkin and Tange 2010] S. Donkin and R. Tange, "The Brauer algebra and the symplectic Schur algebra", *Math. Z.* **265**:1 (2010), 187–219. MR Zbl

[Eisenbud 1995] D. Eisenbud, *Commutative algebra: with a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer, 1995. MR Zbl

[Gabriel 1975] P. Gabriel, "Finite representation type is open", pp. 132–155 in *Proceedings of the International Conference on Representations of Algebras*, edited by V. Dlab and P. Gabriel, Lecture Notes in Mathematics **488**, Springer, 1975. MR Zbl

[Geck and Pfeiffer 2000] M. Geck and G. Pfeiffer, *Characters of finite Coxeter groups and Iwahori–Hecke algebras*, London Mathematical Society Monographs. New Series **21**, Oxford Univ. Press, New York, 2000. MR Zbl

[Geck and Rouquier 1997] M. Geck and R. Rouquier, "Centers and simple modules for Iwahori–Hecke algebras", pp. 251–272 in *Finite reductive groups* (Luminy, 1994), edited by M. Cabanes, Progr. Math. **141**, Birkhäuser, Boston, 1997. MR Zbl

[Goodearl and Warfield 2004] K. R. Goodearl and R. B. Warfield, Jr., *An introduction to noncommutative Noetherian rings*, 2nd ed., London Mathematical Society Student Texts **61**, Cambridge Univ. Press, 2004. MR Zbl

[Gordon 2001] I. Gordon, "Representations of semisimple Lie algebras in positive characteristic and quantum groups at roots of unity", pp. 149–167 in *Quantum groups and Lie theory* (Durham, 1999), edited by A. Pressley, London Mathematical Society Lecture Note Series **290**, Cambridge Univ. Press, 2001. MR Zbl

[Görtz and Wedhorn 2010] U. Görtz and T. Wedhorn, *Algebraic geometry, I: Schemes with examples and exercises*, Vieweg + Teubner, Wiesbaden, 2010. MR Zbl

[Graham and Lehrer 1996] J. J. Graham and G. I. Lehrer, "Cellular algebras", *Invent. Math.* **123**:1 (1996), 1–34. MR Zbl

[Grothendieck 1965] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, II", *Inst. Hautes Études Sci. Publ. Math.* **24** (1965), 5–231. MR Zbl

[Grothendieck 1966] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, III", *Inst. Hautes Études Sci. Publ. Math.* **28** (1966), 5–255. MR Zbl

[Grothendieck 1967] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, IV", *Inst. Hautes Études Sci. Publ. Math.* **32** (1967), 5–361. MR Zbl

[Huneke and Swanson 2006] C. Huneke and I. Swanson, *Integral closure of ideals, rings, and modules*, London Mathematical Society Lecture Note Series **336**, Cambridge Univ. Press, 2006. MR Zbl

[Jategaonkar 1986] A. V. Jategaonkar, *Localization in Noetherian rings*, London Mathematical Society Lecture Note Series **98**, Cambridge Univ. Press, 1986. MR Zbl

[Kaplansky 1958] I. Kaplansky, "Projective modules", *Ann. of Math* (2) **68** (1958), 372–377. MR Zbl

[Lam 1991] T. Y. Lam, *A first course in noncommutative rings*, Graduate Texts in Mathematics **131**, Springer, 1991. MR Zbl

[Lam 1999] T. Y. Lam, *Lectures on modules and rings*, Graduate Texts in Mathematics **189**, Springer, 1999. MR Zbl

[Lorenz 1981] M. Lorenz, "Finite normalizing extensions of rings", *Math. Z.* **176**:4 (1981), 447–484. MR Zbl

[Matsumura 1986] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge Univ. Press, 1986. MR Zbl

[McConnell and Robson 2001] J. C. McConnell and J. C. Robson, *Noncommutative Noetherian rings*, Graduate Studies in Mathematics **30**, American Mathematical Society, Providence, RI, 2001. MR Zbl

[Müller 1976] B. J. Müller, "Localization in non-commutative Noetherian rings", *Canad. J. Math.* **28**:3 (1976), 600–610. MR Zbl

[Müller 1985] B. J. Müller, "Affine Noetherian PI-rings have enough clans", *J. Algebra* **97**:1 (1985), 116–129. MR Zbl

[Müller 1995] J. Müller, *Zerlegungszahlen für generische Iwahori–Hecke-Algebren von exzeptionellen Typ*, Ph.D. thesis, RWTH Aachen University, 1995, www.math.rwth-aachen.de/~Juergen.Mueller/preprints/jm3.ps. Zbl

[Neunhöffer 2003] M. Neunhöffer, *Untersuchungen zu James' Vermutung über Iwahori–Hecke-Algebren vom Typ A*, Ph.D. thesis, RWTH Aachen University, 2003, http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Publications/pdf/phd.pdf.

[Neunhöffer and Scherotzke 2008] M. Neunhöffer and S. Scherotzke, "Formulas for primitive idempotents in Frobenius algebras and an application to decomposition maps", *Represent. Theory* **12** (2008), 170–185. MR Zbl

[Raynaud 1970] M. Raynaud, *Anneaux locaux henséliens*, Lecture Notes in Mathematics **169**, Springer, 1970. MR Zbl

[Reiner 2003] I. Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series **28**, Oxford University Press, 2003. MR Zbl

[Rui 2005] H. Rui, "A criterion on the semisimple Brauer algebras", *J. Combin. Theory Ser. A* **111**:1 (2005), 78–88. MR Zbl

[Scheja and Storch 1988] G. Scheja and U. Storch, *Lehrbuch der Algebra, II: Unter Einschluss der linearen Algebra*, B. G. Teubner, Stuttgart, 1988. MR Zbl

[Stacks 2005–] P. Belmans, A. J. de Jong, et al., "The Stacks project", electronic reference, Columbia University, 2005–, http://stacks.math.columbia.edu.

[Thiel 2016] U. Thiel, "Decomposition matrices are generically trivial", *Int. Math. Res. Not.* **2016**:7 (2016), 2157–2196. MR

Received October 11, 2016. Revised November 3, 2017.

ULRICH THIEL
SCHOOL OF MATHEMATICS AND STATISTICS
UNIVERSITY OF SYDNEY
SYDNEY, NSW
AUSTRALIA
ulrich.thiel@sydney.edu.au

PACIFIC JOURNAL OF MATHEMATICS
Vol. 295, No. 1, 2018
dx.doi.org/10.2140/pjm.2018.295.241

DISTINGUISHED RESIDUAL SPECTRUM FOR $\mathrm{GL}_2(D)$

MAHENDRA KUMAR VERMA

Let $G = \mathrm{GL}_2(D)$ where D is a quaternion division algebra over a number field F and $H = \mathrm{Sp}_2(D)$ is the unique inner form of $\mathrm{Sp}_4(F)$. We study the period of an automorphic form on $G(\mathbb{A})$ relative to $H(\mathbb{A})$ and we provide a formula, similar to the split case, for an automorphic form in the residual spectrum. We confirm the conjecture due to Dipendra Prasad for noncuspidal automorphic representations, which says that symplectic period is preserved under the global Jacquet–Langlands correspondence.

1. Introduction

Let F be a number field and $\mathbb{A}$ its ring of adeles. Let G be a connected reductive group defined over F and H be the fixed point subgroup of an involution on G. For Q an algebraic group defined over F, we let $Y(Q)$ be the group of F-rational characters of Q and

$$Q(\mathbb{A})^1 = \{q \in Q(\mathbb{A}) : |\chi(q)| = 1, \forall \chi \in Y(Q)\}.$$

Let ϕ be an automorphic form on $G(\mathbb{A})$. If ϕ is a cusp form, the period integral $P^H(\phi)$ is defined by the convergent integral

$$\int_{H(F)\backslash(H(\mathbb{A})\cap G(\mathbb{A})^1)} \phi(h)\, dh. \tag{1}$$

We say ϕ is distinguished by H if $P^H(\phi) \neq 0$. A cuspidal automorphic representation π of G is said to be distinguished by H if there exists a $\phi \in \pi$ distinguished by H. It is reasonable to ask for a characterization of H-distinguished cuspidal representations or more generally representations in the discrete spectrum. For a more general automorphic form the period integral may not converge and it is of interest to study the convergence of $P^H(\phi)$.

Let D be a quaternion division algebra over F with involution $\bar{\cdot}$. Let G be the group $\mathrm{GL}_n(D)$ and $H = \mathrm{Sp}_n(D)$ the nonsplit inner form of $\mathrm{Sp}_{2n}(F)$ which we can define as

$$\mathrm{Sp}_n(D) = \{A \in \mathrm{GL}_n(D) : AJ\,{}^t\bar{A} = J\},$$

MSC2010: 11F41, 11F67, 11F70.
Keywords: symplectic period, Jacquet–Langlands correspondence.

where ${}^t\bar{A} = (\bar{a}_{ji})$ for $A = (a_{ij})$ and

$$J = \begin{pmatrix} & & & & 1 \\ & & & 1 & \\ & & 1 & & \\ & \iddots & & & \\ 1 & & & & \end{pmatrix}$$

Similarly when $D = F$ we denote these group by $G' = \mathrm{GL}_{2n}(F)$ and $H' = \mathrm{Sp}_{2n}(F)$. Set $D_{\mathbb{A}} = D \otimes_F \mathbb{A}$. Given an automorphic representation π' of $G'(\mathbb{A})$, for some automorphic form $\phi \in \pi'$, when the above integral (1) is nonzero, we say that π' has symplectic period. When $D = F$, H. Jacquet and S. Rallis [1992] proved that a cuspidal automorphic representation of $G'(\mathbb{A})$ cannot have symplectic period. Further they computed the symplectic period for the most cuspidal elements in the residual spectrum and showed that it is nonzero. Offen [2006a; 2006b] considered H'-distinguished representations of the group G'.

The global Jacquet–Langlands correspondence associates to each automorphic representation π of $\mathrm{GL}_n(D_{\mathbb{A}})$ in the discrete spectrum an automorphic representation π' of $\mathrm{GL}_{2n}(\mathbb{A})$ such that $\pi_v \equiv \pi'_v$ at all the places where $\mathrm{GL}_n(D_v) \equiv \mathrm{GL}_{2n}(F_v)$. In [Verma 2014] we studied the symplectic period for the pair $(\mathrm{GL}_n(D), \mathrm{Sp}_n(D))$ both locally and globally. In this paper Dipendra Prasad suggested the conjecture that π' is distinguished if and only if π is distinguished. We will go into more details about the conjecture and partial results in Section 2.

For an algebraic group X defined over F, we will also write X for the group of F-points. Let P be a minimal parabolic F-subgroup of $\mathrm{GL}_2(D)$ (which is unique up to conjugacy) consisting of upper triangular matrices in $\mathrm{GL}_2(D)$ with Levi decomposition $P = MU$, where M is the diagonal subgroup and U is the unipotent subgroup. We will denote by δ_P the modulus function of $P(\mathbb{A})$. Let K be the maximal compact subgroup of $\mathrm{GL}_2(D_{\mathbb{A}})$ such that $\mathrm{GL}_2(D_{\mathbb{A}}) = U(D_{\mathbb{A}})M(D_{\mathbb{A}})K$ is the Iwasawa decomposition. We define a function H on $M(D_{\mathbb{A}})$ by

$$\begin{pmatrix} m_1 & 0 \\ 0 & m_2 \end{pmatrix} = |\mathrm{nrd}\, m_1|^{1/2} |\mathrm{nrd}\, m_2|^{-1/2}.$$

Here nrd is the reduced norm map from $\mathrm{GL}_2(D_{\mathbb{A}})$ to $\mathbb{A}^\times$. Using the Iwasawa decomposition, we extend trivially H on $\mathrm{GL}_2(D_{\mathbb{A}})$ by

$$H(g) = H(m),$$

where $g = umk$ with $k \in K, m \in M(D_{\mathbb{A}})$ and $u \in U(D_{\mathbb{A}})$.

Let σ be an irreducible cuspidal automorphic representation of $\mathrm{GL}_1(D_{\mathbb{A}})$. Assume that σ is trivial on the center. Then $\sigma \otimes \sigma$ is a cuspidal automorphic representation of $M(D_{\mathbb{A}})$. We first realize the cuspidal automorphic representation $\sigma \otimes \sigma$

in the space of square integrable automorphic functions $L^2(Z_M(D_{\mathbb{A}})M \setminus M(D_{\mathbb{A}}))$ with Z_M being the center of M. Let ϕ be a $K \cap M(D_{\mathbb{A}})$-finite automorphic form in the space of $\sigma \otimes \sigma$ which is extended to a function on $\mathrm{GL}_2(D_{\mathbb{A}})$, so that for $g = muk \in \mathrm{GL}_2(D_{\mathbb{A}})$

$$\phi(g) = \delta_P(m)^{1/2}\phi(mk)$$

and for any fixed $k \in K$, the function

$$m \mapsto \phi(mk)$$

is a $K \cap M(D_{\mathbb{A}})$-finite automorphic form in the space $\sigma \otimes \sigma$. We define

$$F(g, \phi, s) = \phi(g)H(g)^s.$$

Then the Eisenstein series is given by

$$E(g, \phi, s) = \sum_{\gamma \in P\backslash \mathrm{GL}_2(D)} F(\gamma g, \phi, s),$$

which converges absolutely for $\mathrm{Re}(s)$ large. The Eisenstein series $E(g, \phi, s)$ can be analytically continued to a meromorphic function of s. It has a simple pole inside $\mathrm{Re}(s) \geq 0$ and depending on σ the only possible pole in that region is either at $s = 1$ or $s = 2$ [Badulescu 2008]. For $s_0 \in \{1, 2\}$, we define the residue $E_{-s_0}(\phi)$ by

$$E_{-s_0}(g, \phi) = \lim_{s \to s_0} (s - s_0)E(g, \phi, s).$$

The functions $E_{-s_0}(\phi)$ are L^2-automorphic forms. As ϕ ranges above, the multiresidue $E_{-s_0}(\phi)$ generates an irreducible representation of $\mathrm{GL}_2(D_{\mathbb{A}})$ in the residual spectrum corresponding to σ which we will denote by $J(2, \sigma)$.

To compute symplectic periods of noncuspidal automorphic representations in the discrete spectrum, we are therefore by Theorem 5 and Remark 12 reduced to the study of the symplectic period of $E_{-1}(\phi)$, residue of the Eisenstein series corresponding to $s_0 = 1$ constructed from an automorphic representation σ of $\mathrm{GL}_1(D_{\mathbb{A}})$ which is not one-dimensional. Now we state the main theorems of this article. We need the notation H for $\mathrm{Sp}_2(D)$ as an algebraic group defined over F.

Theorem 1. *The function $E_{-1}(g, \phi)$ is integrable over $\mathrm{Sp}_2(D) \setminus \mathrm{Sp}_2(D_{\mathbb{A}})$ and*

$$\int_{\mathrm{Sp}_2(D)\backslash \mathrm{Sp}_2(D_{\mathbb{A}})} E_{-1}(\phi, h)\, dh = \int_{K\cap \mathrm{Sp}_2(D_{\mathbb{A}})} \int_{(M\cap H)\backslash (M\cap H)(D_{\mathbb{A}})^1} \phi(mk)\, dm\, dk. \tag{2}$$

Moreover, there exists a choice of ϕ such that the above integral is nonzero.

As a consequence of the above theorem we have the following result.

Theorem 2. *Any noncuspidal automorphic representation in the discrete spectrum of $\mathrm{GL}_2(D_{\mathbb{A}})$ is of the form $\pi = J(2, \sigma)$ and is distinguished by $\mathrm{Sp}_2(D_{\mathbb{A}})$. Further,* *its image under the global Jacquet–Langlands correspondence is distinguished by* $\mathrm{Sp}_4(\mathbb{A})$.

Structure of the paper. In Section 2 we will recall the global Jacquet–Langlands correspondence and state it explicitly for $n=2$. This explicit description reduces to consider residual Eisenstein series described in Section 1 for $s_0=1$. We have described the existence of distinguished cuspidal automorphic representations. We introduce Arthur's truncation operator in Section 3 and proved the convergence of the period integral of $E_{-1}(g,\phi)$. Section 4 gives a description of double cosets $P\setminus G/H$ which is required to compute the formula for the period integral (2). In Section 5 we compute the contribution to the period integral associated to double cosets. Finally we show the nonvanishing of (2) by constructing an automorphic form Φ on $\mathrm{GL}_2(D_{\mathbb{A}})$ by choosing suitable Φ_v at the every place v of F.

2. Discrete spectrum and the global Jacquet–Langlands

For the first half of this section we take D to be an arbitrary division algebra of degree d over F. An irreducible representation of $G(\mathbb{A})$ is called a discrete automorphic representation of G if it occurs as a direct summand in the space $L^2(G(F)\setminus G(\mathbb{A})^1)$. The discrete spectrum of $\mathrm{GL}_n(\mathbb{A})$ is described by Moeglin and Waldspurger [1995] and a similar description for $\mathrm{GL}_n(D_{\mathbb{A}})$ is given by Badulescu [2008].

We first recall the original global Jacquet–Langlands correspondence which is carried out in [Deligne et al. 1984; Heumos and Rallis 1990; Jacquet and Langlands 1970]. Note that all irreducible automorphic representations of $D^\times(\mathbb{A})$ are cuspidal. Originally the correspondence is a bijection between (cuspidal) automorphic representations of $D^\times(\mathbb{A})$ which are not one-dimensional and so called compatible automorphic representations of $\mathrm{GL}_d(\mathbb{A})$. This is extended in [Badulescu 2008; Badulescu and Renard 2010] to one-dimensional automorphic representations of $D^\times(\mathbb{A})$. These correspond to the residual representations of $\mathrm{GL}_d(\mathbb{A})$, which are all one-dimensional as well.

The global correspondence between discrete spectrum of a general linear group $\mathrm{GL}_{nd}(\mathbb{A})$ and its inner form $\mathrm{GL}_n(D_{\mathbb{A}})$ is defined and proved in [Badulescu 2008; Badulescu and Renard 2010].

Theorem 3. *There is a unique map* JL *from the set of irreducible constituents of* $L^2_{\mathrm{disc}}(\mathrm{GL}_n(D)\setminus\mathrm{GL}_n(D_{\mathbb{A}}))$ *to the set of irreducible constituents of* $L^2_{\mathrm{disc}}(\mathrm{GL}_{dn}(F)\setminus\mathrm{GL}_{dn}(\mathbb{A}))$, *such that if* $\mathrm{JL}(\pi)=\pi'$ *then* π' *is compatible* (*with respect to* D), $\pi'_v\equiv\pi_v$ *where places* v *at which* D *splits and* π_v *corresponds to* π'_v *by the local Jacquet–Langlands correspondence for places* v *at which* D *does not split. The map* JL *is injective*, *and the image consists of all compatible constituents of* $L^2_{\mathrm{disc}}(\mathrm{GL}_{dn}(F)\setminus\mathrm{GL}_{dn}(\mathbb{A}))$ *with respect to* D.

The following more precise description of the global correspondence is also proved in [Badulescu 2008]. For a positive integer l, let R_l be the standard parabolic F-subgroup of $\mathrm{GL}_{ln}(F)$ consisting of block upper triangular matrices corresponding to the partition $(n, n, \ldots, n)$ of ln. Its Levi factor L_{R_l} is isomorphic to the direct product of l copies of $\mathrm{GL}_n(F)$. Let π' be a cuspidal automorphic representation of $\mathrm{GL}_n(\mathbb{A})$. Then, we denote by $I(l, \pi')$ the representation of $\mathrm{GL}_{ln}(\mathbb{A})$ induced from the representation

$$\pi'|\det|^{(l-1)/2} \otimes \cdots \otimes \pi'|\det|^{(1-l)/2}$$

of the Levi factor $L_{R_l}(\mathbb{A})$. This representation has a unique irreducible quotient which we denote by $J'(l, \pi')$. It is a residual representation of $\mathrm{GL}_{ln}(\mathbb{A})$ if $l > 1$. For $l = 1$, we have by definition $J'(1, \pi') = \pi'$. All residual representations of $\mathrm{GL}_N(\mathbb{A})$, for $N > 1$, are obtained in this way for some divisor $l > 1$ of N.

Now we describe the discrete spectrum of $\mathrm{GL}_n(D_{\mathbb{A}})$. The notation $J(m, \pi)$ for inner forms is in analogy with the split case which will be obvious from the theorem below.

Theorem 4. *Let π' be an irreducible cuspidal automorphic representation of the group $\mathrm{GL}_n(\mathbb{A})$. There is a unique positive integer $s_{\pi',D}$, depending only on π' and the division algebra D, which is defined by the condition that $J'(l, \pi')$ is globally compatible (with respect to D) if and only if $s_{\pi',D}$ divides l. Moreover, $s_{\pi',D}$ divides the degree d of the division algebra.*

A representation of the form $J'(s_{\pi',D}, \pi')$ of $\mathrm{GL}_{ns_{\pi',D}}(\mathbb{A})$ corresponds to a cuspidal automorphic representation π of the inner form. A representation of the form $J'(ms_{\pi',D}, \pi')$, with $m > 1$, corresponds to a residual representation $J(m, \pi)$ of the inner form, which is unique irreducible quotient of the representation induced from the representation

$$\pi|\mathrm{nrd}|^{(s_{\pi',D}(m-1))/2} \otimes \cdots \otimes \pi|\mathrm{nrd}|^{(s_{\pi',D}(1-m))/2}.$$

From now on let D be the quaternion division algebra over F and we will describe the discrete spectrum of $\mathrm{GL}_2(D_{\mathbb{A}})$ more explicitly [Grbac and Schwermer 2011]. In this case the only possibilities for $s_{\pi',D}$ are 1 and 2. To simplify the notations, we will write $[G]$ for $\mathrm{GL}_2(D) \backslash \mathrm{GL}_2(D_{\mathbb{A}})$ in the following theorem.

Theorem 5. *The discrete spectrum $L^2_{\mathrm{disc}}([G])$ decomposes into*

$$L^2_{\mathrm{disc}}([G]) = L^2_{\mathrm{cusp}}([G]) \oplus L^2_{\mathrm{res}}([G])$$

where $L^2_{\mathrm{cusp}}([G])$ is the cuspidal spectrum consisting of cuspidal elements, and $L^2_{\mathrm{res}}([G])$ is its orthogonal complement called the residual spectrum. The cuspidal part $L^2_{\mathrm{cusp}}([G])$ decomposes into a Hilbert space direct sum of irreducible cuspidal automorphic representations, each appearing with multiplicity one, and obtained by the global Jacquet–Langlands correspondence either from a cuspidal automorphic *representation of* $G' = \mathrm{GL}_4(\mathbb{A})$, *or from a residual automorphic representation* $J'(ms_{\pi',D}, \pi')$ *with* $m = 1$ *and* $s_{\pi',D} = 2$. *The residual part* $L^2_{\text{res}}([G])$ *decomposes into a Hilbert space direct sum*

$$L^2_{\text{res}}([G]) = \bigoplus_{\mu} \mu \circ \mathrm{nrd} \oplus \bigoplus_{\sigma} J(2, \sigma)$$

where the first sum ranges over all unitary characters μ *of* $\mathbb{A}^\times$ *and* $\mu \circ \mathrm{nrd}$ *is obtained by the Jacquet–Langlands correspondence from* $\mu \circ \det$ *and corresponds to* $m = 2$ *and* $s_{\pi',D} = 2$, *while the second sum, which corresponds to* $m = 2$ *and* $s_{\pi',D} = 1$, *ranges over all cuspidal automorphic representations* σ *of* $D^\times(\mathbb{A})$ *which are not one-dimensional.*

One aims to give a complete classification of distinguished automorphic representations in the discrete spectrum of $\mathrm{GL}_n(D_{\mathbb{A}})$. Dipendra Prasad made a conjecture regarding global distinction.

Conjecture 6 [Verma 2014]. *An automorphic representation* π *in the discrete spectrum of* $\mathrm{GL}_n(D_{\mathbb{A}})$ *is distinguished by* $\mathrm{Sp}_n(D_{\mathbb{A}})$ *if and only if its Jacquet–Langlands lift* $\mathrm{JL}(\pi)$, *an automorphic representation of* $\mathrm{GL}_{2n}(\mathbb{A})$, *is distinguished by* $\mathrm{Sp}_{2n}(\mathbb{A})$.

Remark 7. Suppose $\pi = \otimes \pi_v$ is an automorphic representation of $\mathrm{GL}_1(D_{\mathbb{A}})$ which is distinguished by $\mathrm{Sp}_1(D_{\mathbb{A}})$ then π_v as a representation of $\mathrm{GL}_1(D_v)$ is $\mathrm{Sp}_1(D_v)$-distinguished at all the places v. Then by Lemma 4.1 of [Verma 2014], π_v is one-dimensional for all v and so π is one-dimensional. Its Jacquet–Langlands lift $\mathrm{JL}(\pi)$ lies in residual spectrum which is one-dimensional. This verifies that the above conjecture is true for $n = 1$.

Then we have the following theorem from [Verma 2014] which proves the above conjecture partially.

Theorem 8. *If an automorphic representation* π *of* $\mathrm{GL}_n(D_{\mathbb{A}})$ *occurs in the discrete spectrum and is distinguished by* $\mathrm{Sp}_n(D_{\mathbb{A}})$, *then* $\mathrm{JL}(\pi)$ *is distinguished by* $\mathrm{Sp}_{2n}(\mathbb{A})$.

When $s_{\pi',D}$ equals 1, cuspidal representations correspond to cuspidal representations under Jacquet–Langlands and the symplectic period vanishes on both sides. When $s_{\pi',D}$ equals 2, we have the above conjecture, which gives more precise information about distinguished cuspidal representation of $\mathrm{GL}_n(D_{\mathbb{A}})$.

Conjecture 9. *A cuspidal automorphic representation* π *of* $\mathrm{GL}_n(D_{\mathbb{A}})$ *is distinguished by* $\mathrm{Sp}_n(D_{\mathbb{A}})$ *if and only if* $\mathrm{JL}(\pi) = J'(2, \sigma')$ *for some cuspidal automorphic representation* σ' *of* $\mathrm{GL}_n(\mathbb{A})$.

Remark 10. For $n = 2$, in the above conjecture, the places v of F where D splits (which happens at almost all places), the local component π_v of π is locally distinguished. At the remaining finitely many places where D does not split, the local component π_v of π at the nonsplit places v is either a tempered representation of $\mathrm{GL}_2(D_v)$ which is fully induced from a tensor product of two unitary characters of $D_v^\times$ or a complementary series representation of $\mathrm{GL}_2(D_v)$, attached to a unitary character of $D_v^\times$ and a real number $0 < \alpha < \frac{1}{2}$ [Grbac and Schwermer 2011]. These π_v are distinguished by $\mathrm{Sp}_2(D_v)$ by result of [Verma 2014]. This shows that π is locally distinguished at all the places but we can not conclude that π is globally distinguished.

Further thanks to Dipendra, we have constructed $\mathrm{Sp}_n(D_v)$-distinguished supercuspidal representations of $\mathrm{GL}_n(D_v)$ for n odd. Then by the globalization result of [Prasad and Schulze-Pillot 2008], we have the following theorem.

Theorem 11. *There exists a cuspidal automorphic representation π of $\mathrm{GL}_n(D_{\mathbb{A}})$ for $n \geq 1$ odd, and an automorphic form $\phi \in \pi$ such that*

$$\int_{\mathrm{Sp}_n(D)\backslash \mathrm{Sp}_n(D_{\mathbb{A}})} \phi(h)\, dh \neq 0.$$

Remark 12. In the Theorem 5 first sum ranges over $\mu \circ \mathrm{nrd}$ where μ is the unitary character of $\mathbb{A}^\times$. Any one-dimensional automorphic representation of $\mathrm{GL}_2(D_{\mathbb{A}})$ factors through the reduced norm and they are all $\mathrm{Sp}_2(D_{\mathbb{A}})$-distinguished. Therefore the study of the distinguished residual spectrum of $\mathrm{GL}_2(D_{\mathbb{A}})$ reduces to the study of an automorphic representation of the form $J(2, \sigma)$ as in Theorem 5 corresponding to $m = 2$ and $s_{\pi', D} = 1$. An automorphic representation of the form $J(2, \sigma)$ is generated by the residue of the Eisenstein series $E_{-1}(\phi)$.

3. The truncation of the Eisenstein series

From this section onwards since we are dealing only groups defined over D, we will write $\mathbb{A}$ instead of $D_{\mathbb{A}}$ for simplicity. For the rest of the paper we fix $G = \mathrm{GL}_2(D)$ and $H = \mathrm{Sp}_2(D)$. We will write $[H]$ for $\mathrm{Sp}_2(D) \setminus \mathrm{Sp}_2(\mathbb{A})$. We also recall from Section 1 that P, M, and U denote the F-points of algebraic groups denoted by the same letters. We begin by recalling a special case of the Arthur's truncation method and applying it to our study of the period integral. Let $c > 1$ and denote by τ_c the characteristic function of the set of real numbers greater than c. The truncation operator on the space of automorphic forms on $G(\mathbb{A})$ is defined by

$$\Lambda^c \phi(g) = \phi(g) - \sum_{\gamma \in P\backslash G} \phi_P(\gamma g) \tau_c(H(\gamma g)),$$

where ϕ_P is the constant term of ϕ along P defined as

$$\phi_P(g) = \int_{U\backslash U(\mathbb{A})} \phi(ng)\, dn,$$

for all $g \in G$. For fixed $g \in G$ and c, the above sum is finite.

If ϕ is an automorphic form on $G(\mathbb{A})$ then $\Lambda^c\phi$ is a rapidly decreasing function on $G(\mathbb{A})$. In particular, $\Lambda^c E(\phi, s)$ may be viewed as a meromorphic function of s, with values in the space of rapidly decreasing functions, with residue at $s = s_0$ equal to $\Lambda^c E_{-s_0}(\phi)$. The constant term of E along P is given by

$$E_P(g, \phi, s) = F(g, \phi, s) + F(g, M(s)\phi, -s),$$

where $M(s)$ denotes the standard intertwining operator [Moeglin and Waldspurger 1995]. After applying the truncation operator to the Eisenstein series, we have

$$\Lambda^c E(g, \phi, s) = E(g, \phi, s) - \sum_{\gamma\in P\backslash G} E_P(\gamma g, \phi, s)\tau_c(H(\gamma g)).$$

Whenever the Eisenstein series converges, we can write this as

$$\sum_{\gamma\in P\backslash G} F(\gamma g, \phi, s) - \sum_{\gamma\in P\backslash G} (F(\gamma g, \phi, s) + F(\gamma g, M(s)\phi, -s))\tau_c(H(\gamma g)) := \mathcal{E}_1 - \mathcal{E}_2,$$

where

$$\mathcal{E}_1 = \sum_{\gamma\in P\backslash G} H(\gamma g)^s \phi(\gamma g)(1 - \tau_c(H(\gamma g)))$$

and

$$\mathcal{E}_2 = \sum_{\gamma\in P\backslash G} H(\gamma g)^{-s} M(s)\phi(\gamma g)\tau_c(H(\gamma g)).$$

Let s_0 be a positive real number. Assume that the Eisenstein series $E(g, \phi, s)$ has a simple pole at $s = s_0$. We denote by $E_{-s_0}(g, \phi)$ the nonzero residue of $E(g, \phi, s)$ at s_0.

The truncation of the residue $\Lambda^c E_{-s_0}(g, \phi)$ is

$$\Lambda^c E_{-s_0}(g, \phi) = E_{-s_0}(g, \phi) - \mathcal{E}_3 \tag{3}$$

where $\mathcal{E}_3 = \sum_{\gamma\in P\backslash G} F(\gamma g, M_{-s_0}\phi(\gamma g), -s)\tau_c(H(\gamma g))$. Here M_{-s_0} is the residue of $M(s)$ at $s = s_0$. Consider the period integral $\int_{[H]} \Lambda^c E_{-s_0}(h, \phi)\, dh$ which converges absolutely because of the rapid decay of $\Lambda^c E_{-s_0}(g, \phi)$. By (3), we have

$$\int_{[H]} E_{-s_0}(h, \phi)\, dh = \int_{[H]} \mathcal{E}_3\, dh + \int_{[H]} \Lambda^c E_{-s_0}(h, \phi)\, dh.$$

Since $\Lambda^c E(h, s, \phi)$ is rapidly decreasing, the period

$$\int_{[H]} \Lambda^c E(h, s, \phi)\, dh$$

converges absolutely, the period integral $\int_{[H]} \Lambda^c E(h, s, \phi)\, dh$ defines a meromorphic function in s with possible poles contained in the set of possible poles of the

Eisenstein series $E(g, \phi, s)$ and hence in that of the global intertwining operator $M(s)$. It follows that

$$\mathrm{Res}_{s=s_0} \int_{[H]} \Lambda^c E(h, s, \phi)\, dh = \int_{[H]} \Lambda^c E_{-s_0}(h, \phi)\, dh.$$

Proposition 13. *The periods $\int_{[H]} \mathcal{E}_i\, dh$, for $i = 1, 2$, converge absolutely for large* $\mathrm{Re}(s)$ *and have meromorphic continuation to the whole complex plane. Also period $\int_{[H]} \mathcal{E}_3\, dh$ converges absolutely.*

We will prove the above proposition in Section 5 during the course of computing those periods. By meromorphic continuation, we have

$$\int_{[H]} \Lambda^c E(h, s, \phi)\, dh = \int_{[H]} \mathcal{E}_1\, dh - \int_{[H]} \mathcal{E}_2\, dh$$

for all s. Hence we have, at $s_0 = 1$, which is the only point of interest

$$\mathrm{Res}_{s=1} \int_{[H]} \Lambda^c E(h, s, \phi)\, dh = \mathrm{Res}_{s=1} \int_{[H]} \mathcal{E}_1\, dh - \mathrm{Res}_{s=1} \int_{[H]} \mathcal{E}_2\, dh.$$

Therefore

$$\int_{[H]} E_{-1}(h, \phi)\, dh = \mathrm{Res}_{s=1} \left[\int_{[H]} \mathcal{E}_1\, dh - \int_{[H]} \mathcal{E}_2\, dh \right] + \int_{[H]} \mathcal{E}_3\, dh. \tag{4}$$

This shows that $E_{-1}(g, \phi)$ is integrable over $[H]$.

4. Double cosets

From Section 3 we have the task of integrating $\mathcal{E}_i$ over $[H]$. More generally, let F be a function on $G(\mathbb{A})$ which is left invariant by P and $U(\mathbb{A})$ on the left. Consider the series

$$\theta(g) = \sum_{\gamma \in P \backslash G} F(\gamma g).$$

Let $\{\xi\}$ be the finite set of representatives for the double cosets $P \backslash G / H$. Then the integral of θ over $[H]$ can be written as

$$\begin{aligned} \int_{[H]} \theta(h)\, dh &= \int_{H \backslash H(\mathbb{A})} \sum_{\gamma \in P \backslash G} F(\gamma h)\, dh \\ &= \sum_{\xi} \int_{P \cap \xi H \xi^{-1} \backslash \xi H(\mathbb{A}) \xi^{-1}} F(h\xi)\, dh. \end{aligned}$$

Therefore we will now describe the double cosets $P \backslash G / H$.

Let V be a 2-dimensional Hermitian right D-vector space with a basis $\{e_1, e_2\}$ of V with $(e_1, e_1) = (e_2, e_2) = 0$ and $(e_1, e_2) = 1$. The one-dimensional subspace generated by a vector v is called isotropic if $(v, v) = 0$; otherwise, it is called anisotropic. For a right D-vector space, let $\mathrm{GL}_D(V)$ be the group of all invertible linear transformations on V. Similarly, let $\mathrm{Sp}_D(V)$ be the group of all invertible linear transformations on V which preserve the Hermitian form on V. Let X be the set of all 1-dimensional D-subspaces of V. The group $G = \mathrm{GL}_D(V)$ acts naturally on V, and induces a transitive action on X, realizing X as homogeneous space for G. The stabilizer of a line W in G is a parabolic subgroup P of G, with $X \simeq G/P$. Using the above basis, $\mathrm{GL}_D(V)$ can be identified with $\mathrm{GL}_2(D)$. For $W = \langle e_1 \rangle$, P is the parabolic subgroup consisting of upper triangular matrices in $\mathrm{GL}_2(D)$. As we have a Hermitian structure on V, $H = \mathrm{Sp}_D(V) \subset \mathrm{GL}_D(V)$.

We want to understand the space $H\backslash G/P$. This space can be seen as the orbit space of H on the flag variety X. This action has two orbits. One of them, say O_1, consists of all 1-dimensional isotropic subspaces of V and the other, say O_2, consists of all 1-dimensional anisotropic subspaces of V.

Theorem 14 (Witt's Theorem). *Let V be a nondegenerate quadratic space and $W \subset V$ any subspace. Then any isometric embedding $f : W \to V$ extends to an isometry of V.*

The fact that $\mathrm{Sp}_D(V)$ acts transitively on O_1 and O_2 follows from Witt's theorem, together with the well-known theorem that the reduced norm $N_{D/F} : D^\times \to F^\times$ is surjective, and the result that if a vector $v \in V$ is anisotropic, in the line $\langle v \rangle = \langle v \cdot D \rangle$ generated by v, there exists a vector v' such that $(v', v') = 1$.

It is easily seen that the stabilizer of the line $\langle e_1 \rangle$ in $\mathrm{Sp}_D(V)$ is

$$P \cap H = P_H = \left\{ \begin{pmatrix} a & b \\ 0 & \bar{a}^{-1} \end{pmatrix} : a \in D^\times, b \in D, a\bar{b} + b\bar{a} = 0 \right\}.$$

The parabolic subgroup P_H of $\mathrm{Sp}_2(D)$ has a Levi decomposition $P_H = M_H U_H$ with Levi subgroup

$$M \cap H = M_H = \left\{ \begin{pmatrix} a & 0 \\ 0 & \bar{a}^{-1} \end{pmatrix} : a \in D^\times \right\}.$$

Now we consider the line $\langle e_1 + e_2 \rangle$ inside O_2. To calculate the stabilizer of this line in $\mathrm{Sp}_D(V)$, note that if an isometry of V stabilizes the line generated by $e_1 + e_2$, it also stabilizes its orthogonal complement which is the line generated by $e_1 - e_2$. Hence, the stabilizer of the line $\langle e_1 + e_2 \rangle$ in $\mathrm{Sp}_D(V)$ stabilizes the orthogonal decomposition of V as

$$V = \langle e_1 + e_2 \rangle \oplus \langle e_1 - e_2 \rangle,$$

and also acts on the vectors $\langle e_1 + e_2 \rangle$ and $\langle e_1 - e_2 \rangle$ by scalars. Thus the stabilizer in $\mathrm{Sp}_D(V)$ of the line $\langle e_1 + e_2 \rangle$ is $D_1 \times D_1$ sitting in a natural way in the Levi

$D^\times \times D^\times$ of the parabolic P in $\mathrm{GL}_2(D)$. Here D_1 is the subgroup of $D^\times$ consisting of reduced norm 1 elements in $D^\times$. The above description of the orbits O_1 and O_2 suggests representatives in $\mathrm{GL}_2(D)$ for double cosets $P \setminus G/H$ which we can take, respectively, to be the 2×2 identity matrix and

$$\xi = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Now we describe the parabolic subgroup of $H_\xi = \xi H \xi^{-1}$ which is conjugate to H and defined by the form $\xi J \xi^{-1} = J'$. Therefore

$$H_\xi = \{g \in \mathrm{GL}_2(D) : gJ'g^T = J'\}.$$

Then parabolic subgroup P_ξ of H_ξ is described by

$$P_\xi = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in D_1 \right\}.$$

Also $P \cap H_\xi = D_1 \times D_1$.

5. Computation of integrals $\mathcal{E}_i$

The task at hand is now to compute the contribution of both orbits to $\mathcal{E}_1$, $\mathcal{E}_2$ and $\mathcal{E}_3$ separately and to analyze their absolute convergence. We begin by computing formally, but the computation will be justified by the absolute convergence of the final integral. We recall that

$$\mathcal{E}_1 = \sum_{\gamma \in P \setminus G} H(\gamma g)^s \phi(\gamma g)(1 - \tau_c(H(\gamma g))),$$

$$\mathcal{E}_2 = \sum_{\gamma \in P \setminus G} H(\gamma g)^{-s} M(s)\phi(\gamma g)\tau_c(H(\gamma g)), \quad \text{and}$$

$$\mathcal{E}_3 = \sum_{\gamma \in P \setminus G} F(\gamma g, M_{-s_0}\phi(\gamma g), -s)\tau_c(H(\gamma g)).$$

We can write

$$\int_{[H]} \mathcal{E}_1 \, dh = I_{11} + I_{12}$$

where

$$I_{11} = \int_{P \cap H \setminus H(\mathbb{A})} \phi(h\xi) H(h\xi)^s (1 - \tau_c(H(h))) \, dh$$

and

$$I_{12} = \int_{P \cap \xi H \xi^{-1} \setminus \xi H(\mathbb{A}) \xi^{-1}} \phi(h\xi) H(h\xi)^s (1 - \tau_c(H(h\xi))) \, dh.$$

We will use notation H_ξ for $\xi H \xi^{-1}$.

To compute I_{11}, we choose the Haar measure so that following integration formula is true on $H(\mathbb{A})$.

$$\int_{H(\mathbb{A})} f(h)\,dh = \iiiint f(umak)\delta_{P\cap H}^{-1/2}(a)\,du\,dm\,\frac{dt}{t}\,dk.$$

Here u is integrated over $(U\cap H)(\mathbb{A})$, m over $(M\cap H)(\mathbb{A})^1$, t over $\mathbb{R}^{\times+}$ with $t=|a|$ and k over $K\cap H(\mathbb{A})$.

Then

$$\begin{aligned}
I_{11} &= \int_{K\cap H(\mathbb{A})}\int_{M_H\backslash M_H(\mathbb{A})^1}\int_0^c \phi(mk)\delta_P^{1/2}(a)H(a)^s\delta_{H\cap P}^{-1/2}(a)\,\frac{dt}{t}\,dm\,dk\\
&= \int_{K\cap H(\mathbb{A})}\int_{M_H\backslash M_H(\mathbb{A})^1}\int_0^c \phi(mk)|a||a|^s|a|^{-2}\,\frac{dt}{t}\,dm\,dk\\
&= \int_{K\cap H(\mathbb{A})}\int_{M_H\backslash M_H(\mathbb{A})^1}\int_0^c \phi(mk)|a|^{s-2}\,dt\,dm\,dk.
\end{aligned}$$

The inner integral converges for $\mathrm{Re}(s)>1$ and its range of integration is 0 to c. Since ϕ is a cusp form in the space $\sigma\otimes\sigma$, the middle integral is bounded and therefore converges. Thus we obtain:

$$I_{11} = \frac{c^{s-1}}{s-1}\int_{K\cap H(\mathbb{A})}\int_{M_H\backslash M_H(\mathbb{A})^1}\phi(mk)\,dm\,dk.$$

At this point we begin the computation for I_{12} and for that purpose one needs the Jacquet–Friedberg [1993] result which is about a majorization of a cusp form.

Lemma 15. *Let ϕ be a cusp form on a reductive group $G(\mathbb{A})$ which is invariant under the connected component of the center of $G(\mathbb{A})$. Let R be the maximal parabolic subgroup of $G(\mathbb{A})$ and δ_R be the module of the group $R(\mathbb{A})$. Let Ω be any compact subset of $G(\mathbb{A})$. Then for every $N\geq 0$, there exist a constant $D>0$ such that*

$$|\phi(rk)|\leq D\delta_R(r)^{-N},$$

for every $r\in R$ and $k\in\Omega$.

Using the Iwasawa decomposition we can write

$$I_{12} = \int_{K\cap H_\xi(\mathbb{A})}\int_{P_\xi\backslash P_\xi(\mathbb{A})}\phi(pk\xi)H(pk\xi)^{-s}(1-\tau_c(H(pk\xi)))\,dp\,dk.$$

We replace $1-\tau_c$ by 1 and by the lemma above we can majorize by a constant multiple of $\delta_P(p)^N$. Since $D_1\setminus D_1(\mathbb{A})$ has finite volume, the above integral converges. Since $\xi\in K$ and the function H takes value 1 on the subgroup $P_\xi(\mathbb{A})$, we can write the above integral

$$I_{12} = \int_{K \cap H_\xi(\mathbb{A})} \int_{D_1 \times D_1 \backslash D_1(\mathbb{A}) \times D_1(\mathbb{A})} \phi(pk)\, dp\, dk.$$

The inner integral, which is defined over $D_1 \times D_1 \backslash D_1(\mathbb{A}) \times D_1(\mathbb{A})$, vanishes because ϕ is a vector in the space $\sigma \otimes \sigma$ and σ is not one-dimensional. Therefore,

$$\int_{[H]} \mathcal{E}_1 dh = \frac{c^{s-1}}{s-1} \int_{K \cap H(\mathbb{A})} \int_{M_H \backslash M_H(\mathbb{A})^1} \phi(mk)\, dm\, dk.$$

Now we show that the period integral of $\mathcal{E}_2$ converges and get a simplified expression for it. Write

$$\int_{[H]} \mathcal{E}_2\, dh = I_{21} + I_{22}$$

where

$$I_{21} = \int_{P \cap H \backslash H(\mathbb{A})} M(s)\phi(h\xi) H(h\xi)^{-s} \tau_c(H(h))\, dh$$

and

$$I_{22} = \int_{P \cap H_\xi \backslash H(\mathbb{A})_\xi} M(s)\phi(h\xi) H(h\xi)^{-s} \tau_c(H(h\xi))\, dh.$$

Similar to the computation done above for I_{11} we have

$$I_{21} = \int_{P \cap H \backslash H(\mathbb{A})} \int_{P \cap H_\xi \backslash H(\mathbb{A})_\xi} \int_c^\infty M(s)\phi(mk)|a|^{-s-1} \frac{dt}{t}\, dm\, dk.$$

The integral I_{21} converges for $\mathrm{Re}(s) > -1$ and

$$I_{21} = \frac{c^{-(s+1)}}{s+1} \int_{K \cap H(\mathbb{A})} \int_{M_H \backslash M_H(\mathbb{A})^1} M(s)\phi(mk)\, dm\, dk.$$

Further, using Iwasawa decomposition, one can show that I_{22} converges absolutely for all s and vanishes identically because $c > 1$ and the support of τ_c is empty. Therefore,

$$\int_{[H]} \mathcal{E}_2\, dh = I_{21}.$$

The explicit computations of $\int_{[H]} \mathcal{E}_1\, dh$ and $\int_{[H]} \mathcal{E}_2\, dh$ also proves Proposition 13.

Similar computation and the argument that ϕ is a cusp form in the space $\sigma \otimes \sigma$ shows that $\int_{[H]} \mathcal{E}_3\, dh$ converges and

$$\int_{[H]} \mathcal{E}_3\, dh = \frac{c^{-2}}{2} \int_{K \cap H(\mathbb{A})} \int_{M_H \backslash M_H(\mathbb{A})^1} M_{-1}\phi(mk)\, dm\, dk.$$

Then by (4), we have completed the first half of the proof of Theorem 1.

6. Nonvanishing of the period integral

After proving the convergence of the period integral of the residue of the Eisenstein series and a nice formula to compute it, it remains in Theorem 1 to find out a suitable function ϕ such that the right-hand side of the formula is nonzero. We will achieve this by considering analogous local integrals at every place v of F.

Theorem 16. *There is a K-finite automorphic form Φ on $U(\mathbb{A})M \setminus \mathrm{GL}_2(D_{\mathbb{A}})$ such that the right-hand side of (2) is nonzero.*

Proof. We follow the proof of Jacquet–Rallis [1992] given for the split case. Define a linear form b on the space of smooth vectors in $\sigma \otimes \sigma \subset L^2(M \setminus M(\mathbb{A}))$ given by

$$b(\phi) = \int_{M\setminus M(\mathbb{A})} \phi\left(\begin{pmatrix} g & 0 \\ 0 & \bar{g}^{-1} \end{pmatrix}\right) dg.$$

Since ϕ is a cusp form, the integral is well defined. Consider a function $\Phi : K \to \sigma \otimes \sigma$ such that

$$\Phi(pk) = \sigma \otimes \sigma(p)\Phi(k)$$

when $p \in K \cap P(\mathbb{A})$. Then set

$$I(\Phi) = \int_{K\cap H(\mathbb{A})} b(\Phi(k))\, dk$$

which is equal to the right hand side of (2). We have to choose a K-finite function Φ such that the integral $I(\Phi)$ is nonzero. The linear form b is nonzero because it is a pairing (unique up to scalar) between σ and its contragredient. The linear form b has the following property:

$$b(\sigma(g) \otimes \sigma(\bar{g}^{-1})u) = b(u),$$

for all $g \in D^\times(\mathbb{A})$. Since b is not zero, we can choose a $K \cap M(\mathbb{A})$-finite vector $w = \otimes w_v$ in the space of $\sigma \otimes \sigma$. Then we can write $b = \otimes b_v$ and b_v have same property as b with $b_v(w_v) \neq 0$. Define the local integral

$$I(\Phi_v) = \int_{K_v\cap H_v} b_v(\Phi_v(k_v))\, dk_v.$$

Now we claim that $I(\Phi_v)$ is nonzero for some K_v-finite function $\Phi_v : K_v \to \sigma_v \otimes \sigma_v$ which satisfies

$$\Phi_v(pk) = (\sigma_v \otimes \sigma_v)(p)\Phi_v(k)$$

for $p \in K_v \cap P_v$.

At the finite places v where w_v is $K_v \cap M_v$-invariant, define $\Phi(k_v) = w_v$ for all $k_v \in K_v$. At all of the other remaining finite places, we choose an open compact subgroup Ω_v of $\overline{U_v}$ so small that the points of the form $m_v u_v \omega_v$ with $m_v \in K_v \cap M_v$, $u_v \in U_v \cap K_v$ and $\omega_v \in \Omega_v$ form an open subset of K_v. Then we take Φ_v with support in that set with the property that

$$\Phi_v(m_v u_v \omega_v) = (\sigma_v \otimes \sigma_v)(m_v) w_v.$$

At an infinite place v, by continuity it is enough to choose a smooth function Φ_v such that $I(\Phi_v)$ is not zero. Then Φ_v is any smooth function on K_v such that

$$\Phi_v(m_v k_v) = \sigma_v \otimes \sigma_v(m_v) w_v \Phi_v(k_v)$$

if $m_v \in M_v \cap K_v$. We choose a complement of the Lie algebra of $M_v \cap H_v \cap K_v$ in the Lie algebra of K_v and a small neighborhood of zero in this complement. Let Ω_v be the image of this under exponential map. We also choose a smooth function of compact support $f_v \geq 0$ on Ω_v with $f_v(1) > 0$. Then we define Φ_v by the condition that its support be contained in $(M_v \cap K_v)\Omega_v$ and equal to

$$\sigma_v \otimes \sigma_v(m_v) w_v f_v(\omega_v)$$

where $m_v \in M_v \cap K_v$ and $\omega_v \in \Omega_v$.

The product of the functions Φ_v has then required property. $\square$

Proof of Theorem 2. We recall from [Badulescu 2008] that the automorphic representation $J(2, \sigma)$ is generated by $E_{-1}(g, \phi)$. When σ is a one-dimensional automorphic representation of $\mathrm{GL}_1(D_{\mathbb{A}})$, then $J(2, \sigma)$ is also one-dimensional. Under the global Jacquet–Langlands one-dimensional representations of $\mathrm{GL}_2(D_{\mathbb{A}})$ corresponds to one-dimensional representations of $\mathrm{GL}_4(\mathbb{A})$. When σ is not one-dimensional then $J(2, \sigma)$ is distinguished by the above theorem and under the global Jacquet–Langlands this corresponds to the automorphic representation $J'(2, \sigma')$ of $\mathrm{GL}_4(\mathbb{A})$ which is also distinguished by $\mathrm{Sp}_4(\mathbb{A})$ [Offen 2006b].

Acknowledgments. I would like to thanks Dipendra Prasad, Eitan Sayag, Ravi Raghunathan and Omer Offen for helpful comments. This work was done during my postdoctoral fellowship at Ben-Gurion University of Negev, Israel. The author gratefully thanks the referee for the constructive comments and recommendations which definitely helped improve the readability and quality of the paper.

References

[Badulescu 2008] A. I. Badulescu, "Global Jacquet–Langlands correspondence, multiplicity one and classification of automorphic representations", *Invent. Math.* **172**:2 (2008), 383–438. MR Zbl

[Badulescu and Renard 2010] A. I. Badulescu and D. Renard, "Unitary dual of $\mathrm{GL}(n)$ at Archimedean places and global Jacquet–Langlands correspondence", *Compos. Math.* **146**:5 (2010), 1115–1164. MR Zbl

[Deligne et al. 1984] P. Deligne, D. Kazhdan, and M.-F. Vignéras, "Représentations des algèbres centrales simples p-adiques", pp. 33–117 in *Représentations des groupes réductifs sur un corps local*, Hermann, Paris, 1984. MR Zbl

[Friedberg and Jacquet 1993] S. Friedberg and H. Jacquet, "Linear periods", *J. Reine Angew. Math.* **443** (1993), 91–139. MR Zbl

[Grbac and Schwermer 2011] N. Grbac and J. Schwermer, "An exercise in automorphic cohomology: the case GL_2 over a quaternion algebra", pp. 209–252 in *Arithmetic geometry and automorphic forms*, edited by J. Cogdell et al., Adv. Lect. Math. **19**, Int. Press, Somerville, MA, 2011. MR Zbl

[Heumos and Rallis 1990] M. J. Heumos and S. Rallis, "Symplectic-Whittaker models for Gl_n", *Pacific J. Math.* **146**:2 (1990), 247–279. MR Zbl

[Jacquet and Langlands 1970] H. Jacquet and R. P. Langlands, *Automorphic forms on* GL(2), Lecture Notes in Math. **114**, Springer, 1970. MR Zbl

[Jacquet and Rallis 1992] H. Jacquet and S. Rallis, "Symplectic periods", *J. Reine Angew. Math.* **423** (1992), 175–197. MR Zbl

[Moeglin and Waldspurger 1995] C. Moeglin and J.-L. Waldspurger, *Spectral decomposition and Eisenstein series*, Cambridge Tracts in Mathematics **113**, Cambridge Univ. Press, 1995. MR Zbl

[Offen 2006a] O. Offen, "On symplectic periods of the discrete spectrum of GL_{2n}", *Israel J. Math.* **154**:1 (2006), 253–298. MR Zbl

[Offen 2006b] O. Offen, "Residual spectrum of GL_{2n} distinguished by the symplectic group", *Duke Math. J.* **134**:2 (2006), 313–357. MR Zbl

[Prasad and Schulze-Pillot 2008] D. Prasad and R. Schulze-Pillot, "Generalised form of a conjecture of Jacquet and a local consequence", *J. Reine Angew. Math.* **616** (2008), 219–236. MR Zbl

[Verma 2014] M. K. Verma, "On symplectic periods for inner forms of GL_n", 2014. To appear in *Math. Res. Letters*. arXiv

Received August 31, 2017. Revised December 5, 2017.

MAHENDRA KUMAR VERMA
DEPARTMENT OF MATHEMATICS
BEN-GURION UNIVERSITY OF NEGEV
ISRAEL
mahendra1091@gmail.com

Guidelines for Authors

Authors may submit articles at msp.org/pjm/about/journal/submissions.html and choose an editor at that time. Exceptionally, a paper may be submitted in hard copy to one of the editors; authors should keep a copy.

By submitting a manuscript you assert that it is original and is not under consideration for publication elsewhere. Instructions on manuscript preparation are provided below. For further information, visit the web address above or write to pacific@math.berkeley.edu or to Pacific Journal of Mathematics, University of California, Los Angeles, CA 90095–1555. Correspondence by email is requested for convenience and speed.

Manuscripts must be in English, French or German. A brief abstract of about 150 words or less in English must be included. The abstract should be self-contained and not make any reference to the bibliography. Also required are keywords and subject classification for the article, and, for each author, postal address, affiliation (if appropriate) and email address if available. A home-page URL is optional.

Authors are encouraged to use LaTeX, but papers in other varieties of TeX, and exceptionally in other formats, are acceptable. At submission time only a PDF file is required; follow the instructions at the web address above. Carefully preserve all relevant files, such as LaTeX sources and individual files for each figure; you will be asked to submit them upon acceptance of the paper.

Bibliographical references should be listed alphabetically at the end of the paper. All references in the bibliography should be cited in the text. Use of BibTeX is preferred but not required. Any bibliographical citation style may be used but tags will be converted to the house format (see a current issue for examples).

Figures, whether prepared electronically or hand-drawn, must be of publication quality. Figures prepared electronically should be submitted in Encapsulated PostScript (EPS) or in a form that can be converted to EPS, such as GnuPlot, Maple or Mathematica. Many drawing tools such as Adobe Illustrator and Aldus FreeHand can produce EPS output. Figures containing bitmaps should be generated at the highest possible resolution. If there is doubt whether a particular figure is in an acceptable format, the authors should check with production by sending an email to pacific@math.berkeley.edu.

Each figure should be captioned and numbered, so that it can float. Small figures occupying no more than three lines of vertical space can be kept in the text ("the curve looks like this:"). It is acceptable to submit a manuscript will all figures at the end, if their placement is specified in the text by means of comments such as "Place Figure 1 here". The same considerations apply to tables, which should be used sparingly.

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.

Page proofs will be made available to authors (or to the designated corresponding author) at a website in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

PACIFIC JOURNAL OF MATHEMATICS

Volume 295 No. 1 July 2018
