Algebra & Number Theory

Volume 13

2019

No. 5

On the Brauer–Siegel ratio for abelian varieties over function fields

Douglas Ulmer

msp

ALGEBRA AND NUMBER THEORY 13:5 (2019)
dx.doi.org/10.2140/ant.2019.13.1069

On the Brauer–Siegel ratio for abelian varieties over function fields

Douglas Ulmer

Hindry has proposed an analog of the classical Brauer–Siegel theorem for abelian varieties over global fields. Roughly speaking, it says that the product of the regulator of the Mordell–Weil group and the order of the Tate–Shafarevich group should have size comparable to the exponential differential height. Hindry–Pacheco and Griffon have proved this for certain families of elliptic curves over function fields using analytic techniques. Our goal in this work is to prove similar results by more algebraic arguments, namely by a direct approach to the Tate–Shafarevich group and the regulator. We recover the results of Hindry–Pacheco and Griffon and extend them to new families, including families of higher-dimensional abelian varieties.

1. Introduction

The classical Brauer–Siegel theorem [Brauer 1950] says that if K runs through a sequence of Galois extensions of $\mathbb{Q}$ with discriminants $d = d_K$ satisfying $[K : \mathbb{Q}]/\log d \to 0$, then

$$\frac{\log(Rh)}{\log\sqrt{d}} \to 1$$

where $R = R_K$ and $h = h_K$ are the regulator and class number of K. The proof uses the class number formula

$$\mathrm{Res}_{s=1}\,\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}Rh}{w\sqrt{d}}$$

and analytic methods.

Hindry [2007] conjectured an analog of the Brauer–Siegel theorem for abelian varieties. If A is an abelian variety over a global field K with regulator R, Tate–Shafarevich group Ш (assumed to be finite), and exponential differential height H (definitions below), Hindry proposed that the Brauer–Siegel ratio

$$\mathrm{BS}(A) := \frac{\log(R|Ш|)}{\log(H)}$$

should tend to 1 for any sequence of abelian varieties over a fixed K with $H \to \infty$.

MSC2010: primary 11G05; secondary 11G10, 11G40.
Keywords: abelian variety, Tate–Shafarevich group, regulator, height, Brauer–Siegel ratio, function field.

Hindry and Pacheco [2016] considered the case where K is a global function field of characteristic $p > 0$. Assuming the finiteness of Ш, they proved (Corollary 1.13) that

$$0 \leq \liminf_{A} \mathrm{BS}(A) \leq \limsup_{A} \mathrm{BS}(A) = 1, \tag{1.1}$$

where the limits are over the family of all nonconstant abelian varieties of a fixed dimension over K ordered by height. Note that this leaves open the possibility of a sequence of abelian varieties with Brauer–Siegel ratio tending to a limit < 1, a possibility not envisioned in Hindry's earlier paper. Hindry and Pacheco also conjectured and gave evidence for the claim that the lower bound $0 \leq \liminf_A \mathrm{BS}(A)$ should be an equality when A runs through the family of quadratic twists of a fixed elliptic curve. Moreover, they gave an example (Theorem 1.4) of a family of elliptic curves E with $H \to \infty$ and proved $\lim_E \mathrm{BS}(E) = 1$ without having to assume any unproven conjectures. In his Paris VII thesis, Griffon [2016] gave several other examples of families of elliptic curves where $\lim_E \mathrm{BS}(E) = 1$ again without assuming unproven conjectures.

As with the original Brauer–Siegel theorem, the analyses of Hindry–Pacheco and Griffon use analytic techniques. More precisely, finiteness of the Tate–Shafarevich group implies the conjecture of Birch and Swinnerton-Dyer (in its strong form), and so a class number formula of the shape

$$L^*(A) = \alpha \frac{|\text{Ш}|R}{H}$$

where $L^*(A)$ is the leading Taylor coefficient of the L-function at $s = 1$ and α is a relatively innocuous, nonzero factor. (We will give the precise statement below.) Hindry–Pacheco and Griffon then prove their results by estimating (and in some cases calculating quite explicitly) $L^*(A)$.

Our goal in this work is to prove several results about Brauer–Siegel ratios by more algebraic arguments, in other words through a direct approach to the Tate–Shafarevich group and the regulator. More precisely, we prove the following results without recourse to L-functions:

(1) a transparent and conceptual proof that $\liminf_A \mathrm{BS}(A) \geq 0$ via a lower bound on the regulator;

(2) a new connection between the growth of $|\text{Ш}|$ as the finite ground field is extended and the number $R|\text{Ш}|$ over the given field;

(3) a general calculation of the limiting Brauer–Siegel ratio for the sequence $E^{(p^n)}$ of Frobenius pull-backs of an elliptic curve E;

(4) a new proof that $\lim_d \mathrm{BS}(E_d) = 1$ in the families of elliptic curves studied by Hindry–Pacheco and Griffon;

(5) proofs that $\lim_d \mathrm{BS}(J_d) = 1$ for families of Jacobians of all dimensions;

(6) and results on quadratic twists that illustrate the limitations of our p-adic techniques.

"Without recourse to L-functions" means by algebraic methods. We do use the BSD formula, but this is just a bookkeeping device for the connections between cohomology and other invariants. We do not use the Euler product or any properties of $L(A, s)$ as a function of s. That said, we have not eliminated analysis entirely: points (4–6) above all require an equidistribution result for the action of multiplication by p on $\mathbb{Z}/d\mathbb{Z}$.

The plan of the paper is as follows: In Section 2, we set up notation, review and extend certain auxiliary results of Hindry–Pacheco on component groups, and prove a lemma useful for estimating heights. In Section 3, we prove a general integrality result on regulators of abelian varieties which leads immediately to a lower bound on the Brauer–Siegel ratio. In Section 4, we introduce "$\dim Ш(A)$", a new and extremely useful technical device which is closely related to slopes of L-functions and which is computable in many interesting situations. As a first application, in Section 5 we compute the limiting Brauer–Siegel ratio for the sequence of Frobenius pull-backs of an elliptic curve. Sections 6–9 develop p-adic cohomological machinery that allows one to compute $\dim Ш(A)$ and estimate $\mathrm{BS}(A)$ for Jacobians of curves with Néron models related to products of Fermat curves. In the rest of the paper, we use this machinery to recover the results of Hindry–Pacheco and Griffon and to extend them to higher genus Jacobians. Section 10 discusses curves defined by equations involving 4 monomials. Section 11 discusses curves coming from Berger's construction [2008]. Finally, in Section 12 we consider twists of constant elliptic curves.

It is a pleasure to thank Richard Griffon for several helpful comments and an anonymous referee for his or her careful reading of the paper and valuable suggestions.

2. Preliminaries

2.1. ***Notation and definitions.*** We set notation and recall definitions which will be used throughout the paper.

Fix a prime number p, a power q of p, and a smooth, projective, absolutely irreducible curve $\mathcal{C}$ of genus $g_{\mathcal{C}}$ over $k = \mathbb{F}_q$, the field of q elements. Let K be the function field $\mathbb{F}_q(\mathcal{C})$. We write v for a place of K, d_v for the degree of v, K_v for the completion of K at v, $\mathcal{O}_v$ for the ring if integers in K_v, and k_v for the residue field, a finite extension of k of degree d_v

Let A be an abelian variety over K with dual $\hat{A}$. A theorem of Lang and Néron guarantees that the *Mordell–Weil groups* $A(K)$ and $\hat{A}(K)$ are finitely generated abelian groups. (See [Lang and Néron 1959], or [Conrad 2006] for a more modern account.)

There is a bilinear pairing

$$\langle \cdot, \cdot \rangle : A(K) \times \hat{A}(K) \to \mathbb{Q}$$

which is nondegenerate modulo torsion. (This is the canonical Néron–Tate height divided by $\log q$. See [Néron 1965] for the definition and [Hindry and Silverman 2000, B.5] for a friendly introduction.) Choosing a basis $P_1, \dots, P_r$ for $A(K)$ modulo torsion and a basis $\hat{P}_1, \dots, \hat{P}_r$ for $\hat{A}(K)$ modulo torsion, we define the *regulator* of A as

$$\mathrm{Reg}(A) := |\det\langle P_i, \hat{P}_j\rangle_{1\le i,j\le r}|.$$

The regulator is a positive rational number, well-defined independently of the choice of bases.

We write $H^1(K, A)$ for the étale cohomology of K with coefficients in A and similarly for $H^1(K_v, A)$. The *Tate–Shafarevich group* of A is defined as

$$Ш(A) := \ker\left(H^1(K, A) \to \prod_v H^1(K_v, A)\right),$$

where the product of over the places of K and the map is the product of the restriction maps. This group is conjectured to be finite, and we assume this conjecture throughout the paper. However, in all of the explicit calculations below, we can in fact prove that $Ш(A)$ is finite without additional assumptions.

Let $\mathcal{A} \to \mathcal{C}$ be the Néron model of A/K. This is a smooth group scheme over $\mathcal{C}$ with a certain universal property whose generic fiber is A/K. See [Bosch et al. 1990] for a modern account. Let $s : \mathcal{C} \to \mathcal{A}$ be the zero-section. We define an invertible sheaf ω on $\mathcal{C}$ by

$$\omega := s^*(\Omega^{\dim(A)}_{\mathcal{A}/\mathcal{C}}) = \bigwedge\nolimits^{\dim(A)} s^*(\Omega^1_{\mathcal{A}/\mathcal{C}}).$$

The *exponential differential height* of A (which we often refer to simply as the *height*) is

$$H(A) := q^{\deg \omega}.$$

If A is an elliptic curve and $\mathcal{C} = \mathbb{P}^1$, then $\deg \omega$ has simple interpretation in terms of the degrees of the coefficients in a Weierstrass equation defining A. See [Ulmer 2011, Lecture 3] for details.

For each place v of K, we write c_v for the number of connected components of the special fiber of $\mathcal{A}$ at v which are defined over the residue field. We define the *Tamagawa number* of A as

$$\tau(A) := \prod_v c_v.$$

(This usage is in conflict with our earlier papers, in particular [Ulmer 2014a], where the Tamagawa number is defined to be

$$\frac{\tau(A)}{H(A) q^{\dim(A)(g_{\mathcal{C}}-1)}}.$$

The earlier usage is historically more appropriate, as the definition there is a volume defined in close analogy with Tamagawa's work on linear algebraic groups, see [Weil 1982], but the terminology we adopt here is more convenient for our current purposes.)

Next we consider the Hasse–Weil L-function of A over K, denoted $L(A, s)$. It is a function of a complex variable s defined as an Euler product over the places of K which is convergent in the half-plane $\Re s > \frac{3}{2}$ and which is known to have a meromorphic continuation to the whole s-plane. More precisely, $L(A, s)$ is a rational function in q^{-s}, and if the K/k-trace of A is trivial, then $L(A, s)$ is in fact a polynomial in q^{-s} of the form

$$\prod_i (1 - \alpha_i q^{-s}),$$

where the inverse root α_i are Weil integers of size q.

We define the leading coefficient of the L-function as

$$L^*(A) := \frac{1}{(\log q)^r}\frac{1}{r!}\left(\frac{d}{ds}\right)^r L(A,s)\bigg|_{s=1}$$

where r is the order of vanishing $r := \operatorname{ord}_{s=1} L(A,s)$. (With the factor $1/(\log q)^r$, this is the leading coefficient of L as a rational function in $T = q^{-s}$, and with this normalization, it has the virtue of being a rational number.)

All of the invariants mentioned above are connected by the conjecture of Birch and Swinnerton-Dyer ("BSD conjecture"), which we take to be the conjunction of the following three statements:

(1) $\operatorname{ord}_{s=1} L(A,s) = \operatorname{Rank} A(K)$.

(2) $Ш(A)$ is finite (with order denoted $|Ш(A)|$).

(3) We have an equality

$$L^*(A) = \frac{\operatorname{Reg}(A)|Ш(A)|}{H(A)} \frac{\tau(A)}{q^{\dim(A)(g_C-1)}|A(K)_{tor}|\cdot|\hat{A}(K)_{tor}|}.$$

It is known that parts (1) and (2) are equivalent, and when they hold, part (3) holds as well. (See [Kato and Trihan 2003] for the end of a long line of reasoning leading to these results.)

From the point of view of the Brauer–Siegel ratio, the main terms of interest in the third part of the BSD conjecture are $\operatorname{Reg}(A)$, $|Ш(A)|$, and $H(A)$, whereas the other factors are either constant ($q^{\dim(A)(g_C-1)}$) or turn out to be negligible ($\tau(A)$ and $|A(K)_{tor} \times \hat{A}(K)_{tor}|$). We will discuss the Tamagawa number and the results of Hindry and Pacheco on it in the next section, whereas the torsion subgroups $A(K)_{tor}$ and $\hat{A}(K)_{tor}$ will play almost no role in our analysis.

2.2. *Bounds on Tamagawa numbers* (1). Hindry and Pacheco [2016, Proposition 6.8] bound the Tamagawa number in terms of the height under certain tameness assumptions. More precisely, they showed that for a fixed global field K, as A varies over all abelian varieties of fixed dimension d over K, we have

$$\tau(A) = O(H^\epsilon)$$

for all $\epsilon > 0$, provided that $p > 2\dim(A) + 1$ or A has everywhere semistable reduction.

In this section and Sections 2.5 and 2.6, we outline three improvements of this result, all motivated by applications later in the paper.

Lemma 2.2.1. *Let E run through the set of all elliptic curves over a global function field K. Then*

$$\tau(E) = O(H(E)^\epsilon)$$

for every $\epsilon > 0$.

The point is that we allow arbitrary characteristic and make no semistability hypothesis. This result was also proven by Griffon [2016, Theorem 1.5.4], but we include a proof here for the convenience of the reader.

Proof. This follows easily from Ogg's formula [1967] (see also [Saito 1988] for a more general result proven with modern methods). Indeed, if Δ_v is a minimal discriminant for E at the place v, Ogg's formula says that

$$\mathrm{ord}_v(\Delta_v) = c_v + f_v - 1$$

where f_v is the exponent of the conductor of E at v. Summing over places where E has bad reduction (i.e., where $\mathrm{ord}_v(\Delta_v) \geq 1$) and using that $f_v - 1 \geq 0$ at these places, we have

$$\sum_v c_v d_v \leq \sum_v \mathrm{ord}_v(\Delta_v) d_v \leq 12 \deg(\omega)$$

where d_v is the degree of v and where the last inequality holds because Δ can be interpreted as a section of $\omega^{\otimes 12}$. This recovers the main bound (Theorem 6.5 of [Hindry and Pacheco 2016]), and the rest of the argument — converting this additive bound to a multiplicative bound — proceeds exactly as in [Hindry and Pacheco 2016, Proposition 6.8]. □

2.3. ***Families from towers of fields.*** Let A be an abelian variety over a function field K. For each positive integer d (or positive integer d prime to p), let K_d be a geometric extension of K, and let $A_d = A \times_K K_d$. This gives a sequence of abelian varieties and one may ask about the behavior of $\mathrm{BS}(A_d)$ as $d \to \infty$.

For most of the paper, we will be concerned with the special case where there are isomorphisms $K_d \cong K$ for all d. In this case, we may view the sequence A_d as a sequence of abelian varieties over a *fixed* function field. This is the context of the results and conjectures of Hinry and Pacheco, and we will give four examples in the rest of this section. Nevertheless, the general case is also interesting, and we will give develop foundational results in a more general context in Section 2.4.

2.3.1. *Kummer families.* Let $K = \mathbb{F}_q(t)$, and for each positive integer d prime to p, let $K_d = \mathbb{F}_q(u)$ where $u^d = t$. Note that the extension K_d/K is unramified away from the places $t = 0$ and $t = \infty$ of K. Let A be an abelian variety over K, and let A_d be the abelian variety over K obtained by base change to K_d, followed by the isomorphism of fields $\mathbb{F}_q(u) \cong \mathbb{F}_q(t)$, $u \mapsto t$. (In more vivid terms, A_d is the result of substituting t^d for each appearance of t in the equations defining A.) We say that the sequence of abelian varieties A_d is the *family associated to A and the Kummer tower*. Such families have been a prime source of examples for the Brauer–Siegel ratio.

2.3.2. *Artin–Schreier families.* We may proceed analogously with the tower of Artin–Schreier extensions. Again, let $K = \mathbb{F}_q(t)$, and for each positive integer d, let $K_d = \mathbb{F}_q(u)$ where $u^{p^d} - u = t$. Note that the extension K_d/K is unramified away from the place $t = \infty$ of K. Let A be an abelian variety over K, and let A_d be the abelian variety over K obtained by base change to K_d followed by the isomorphism of fields $\mathbb{F}_q(u) \cong \mathbb{F}_q(t)$, $u \mapsto t$. (In more vivid terms, A_d is the result of substituting $t^{p^d} - t$ for each appearance of t in the equations defining A.) We say that the sequence of abelian varieties A_d is the *family associated to A and the Artin–Schreier tower*.

2.3.3. *Division tower families.* One may also consider an elliptic curve variant: Let K be the function field $\mathbb{F}_q(E)$ where E is an elliptic curve over $\mathbb{F}_q$. For each positive integer d prime to p, consider the field extension K_d/K associated to the multiplication map $d : E \to E$. Thus $[K_d : K] = d^2$, but K_d is canonically isomorphic as a field (even as an $\mathbb{F}_q$-algebra) to K. Given an abelian variety A over K, let A_d be the abelian variety over K obtained by base-changing A to K_d and then using the isomorphism of fields $K_d \cong K$. We say that the sequence A_d of abelian varieties over K is the *family associated to a division tower*. Everything we say about Kummer and Artin–Schreier towers has an obvious analog for division towers. In most cases the latter is simpler because in the division case, K_d/K is unramified.

2.3.4. PGL_2 *families.* Let $K = \mathbb{F}_q(t)$ and for each positive integer d let $K_d = \mathbb{F}_q(u)$ where $\mathbb{F}_q(u)/\mathbb{F}_q(t)$ is the field extension associated to the quotient morphism

$$\mathbb{P}^1 \to \mathbb{P}^1/\,\mathrm{PGL}_2(\mathbb{F}_{p^d}) \cong \mathbb{P}^1.$$

We normalize the isomorphism so that the $\mathbb{F}_{p^d}$-rational points on the upper $\mathbb{P}^1$ map to 0 and $\mathbb{P}^1(\mathbb{F}_{p^{2d}}) \setminus \mathbb{P}^1(\mathbb{F}_{p^d})$ maps to 1. Then the extension K_d/K is unramified away from the places $t = 0$ and $t = 1$ of K, and it is tamely ramified over $t = 1$. Given an abelian variety A over K, let A_d be the abelian variety over K obtained by base-changing A to K_d and then using the isomorphism of fields $\mathbb{F}_q(u) \cong \mathbb{F}_q(t)$, $u \mapsto t$. We say that the sequence A_d of abelian varieties over K is the *family associated to the* PGL_2 *tower*.

The discussion above gives four different meanings to the notations K_d and A_d! Which meaning is intended in each use below should be clear from the context.

We end this section with a simple lemma that plays a key role in our analysis of Tamagawa numbers in families associated to towers.

Lemma 2.3.5. *Let $K = \mathbb{F}_q(\mathcal{C})$ be a function field, and let K_d be a sequence of geometric extensions of K such that the genus of (the curve associated to) K_d is ≤ 1 for all d. Then for every place v of K, there is a constant C_v depending only on q and* $\deg v$ *such that for all d, the number of places of K_d dividing v is at most $C_v[K_d : K]/\log[K_d : K]$.*

Proof. Write $D = [K_d : K]$ and set $x = \log D/\log q$. Fix a place v of K. Then the number of places w of K_d dividing v and of absolute degree $\geq x$ is at most

$$\frac{D}{x/\deg v} = \deg v \log q \frac{D}{\log D}.$$

On the other hand, by the Weil bound, the total number of places of K_d of degree $\leq x$ is bounded by $Cq^x/x = C'D/\log D$ where C and C' depend only on q, $\deg v$ and the genus of K_d. Since the latter is either 0 or 1, the constant can be taken to depend only on q and $\deg v$. This shows that the total number of places of K_d dividing v is $\leq C_v D/\log D$ where C_v depends only on q and $\deg v$. $\square$

2.4. ***Towers of geometrically Galois extensions.*** In this section, we discuss a more general class of towers of fields K_d where we are able to bound Tamagawa numbers of the associated sequences of abelian varieties. This additional generality was suggested by the anonymous referee, to whom we are grateful.

Readers who are mainly interested in the applications to the Kummer tower later in the paper are invited to skip ahead to Section 2.5

2.4.1. *Geometrically Galois extensions.* Let k be a field and let $K = k(\mathcal{C})$ be the function field of a smooth, projective, geometrically irreducible curve over k. We say that a finite, geometric extension K_d/K is *geometrically Galois* if the Galois closure L_d of K_d over K has the form $L_d = k_d K_d$ where k_d is a finite Galois extension of k. Equivalently, there is a finite Galois extension k_d of k such that $k_d K_d$ is Galois over $k_d K$. (We take k_d to be minimal such extension.) Let $G_d = \mathrm{Gal}(L_d/k_d K)$ and $\Gamma_d = \mathrm{Gal}(k_d/k) \cong \mathrm{Gal}(k_d K/K) \cong \mathrm{Gal}(L_d/K_d)$, so that Γ_d acts on G_d by conjugation and $\mathrm{Gal}(L_d/K)$ is the semidirect product $G_d \rtimes \Gamma_d$. We call G_d, with its action of Γ_d, the *geometric Galois group* of K_d/K and we call k_d the *splitting field* of G_d. (We remark that there is a finite étale group scheme $\underline{G}_d$ over k attached to G_d with its Γ_d action, and $\underline{G}_d$ becomes a constant group over k_d, see [Milne 1980, §II.1].)

2.4.2. *Towers of geometrically Galois extensions.* We now consider a tower of geometrically Galois extensions K_d/K indexed by positive integers d (or positive integers relatively prime to p) with containments $K_d \subset K_{d'}$ whenever d divides d'. These containments induce surjections $G_{d'} \to G_d$ and $\Gamma_{d'} \to \Gamma_d$ which are compatible in the obvious sense with the actions of Γ_d and $\Gamma_{d'}$ on G_d and $G_{d'}$ respectively.

Each of the families of towers in Section 2.3 gives an example of a tower of geometrically Galois extensions.

In the case of the Kummer tower, the geometric Galois group is $G_d = \mu_d(\overline{\mathbb{F}_q})$, the splitting field k_d is $\mathbb{F}_q(\mu_d)$, and $\Gamma_d = \mathrm{Gal}(\mathbb{F}_q(\mu_d)/\mathbb{F}_q)$ is the subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by q.

In the Artin–Schreier tower, the geometric Galois group is $G_d = \mathbb{F}_{p^d}$, the splitting field k_d is the compositum $\mathbb{F}_q\mathbb{F}_{p^d}$, and $\Gamma_d = \mathrm{Gal}(\mathbb{F}_q\mathbb{F}_{p^d}/\mathbb{F}_q)$ is the cyclic group generated by the q-power Frobenius.

In the division tower corresponding to an elliptic curve E over $\mathbb{F}_q$, the geometric Galois group is $E[d]$, the splitting field k_d is $\mathbb{F}_q(E[d])$, and $\Gamma_d = \mathrm{Gal}(k_d/\mathbb{F}_q)$ is the cyclic group generated by the action of the q-power Frobenius on the d torsion points.

In the PGL_2 tower, the geometric Galois group is $G_d = \mathrm{PGL}_2(\mathbb{F}_{p^d})$, the splitting field k_d is $\mathbb{F}_q\mathbb{F}_{p^d}$, and $\Gamma_d = \mathrm{Gal}(\mathbb{F}_q\mathbb{F}_{p^d}/\mathbb{F}_q)$ is the cyclic group generated by the q-power Frobenius.

For a more general class of examples, let K_d/K be any of the towers above, and fix an extension F/K which is linearly disjoint from each K_d over K. Then the fields $F_d := FK_d$ form a tower of geometrically Galois extensions with the geometric Galois group of F_d/F isomorphic to that of K_d/K. Note however, that in general the genus of F_d tends to infinity with d.

We next consider two group-theoretic results related to these towers, both concerning the number of orbits of Γ_d acting on G_d. (As motivation, we note that the orbits of Γ_d on G_d are in bijection with the closed points of the scheme $\underline{G}_d$.)

To state the first result, we make a somewhat elaborate hypothesis on the system of groups G_d with their Γ_d actions.

Hypothesis 2.4.3. (1) There exists a function ϕ of positive integers such that $|G_d| = \sum_{e\,|\,d} \phi(e)$ for all d.

(2) There a decomposition $G_d = \cup_{e\,|\,d} G'_{d,e}$ such that $|G'_{d,e}| = \phi(e)$.

(3) The action of Γ_d on G_d respects the decomposition above, and the orbits of Γ_d on $G'_{d,e}$ have cardinality $\geq C\log|G_e|$ for some constant C independent of d and e.

This hypothesis clearly implies that the splitting field k_d has degree $[k_d : k] = |\Gamma_d| \geq C\log|G_d|$. It would be interesting to know whether the converse holds.

Lemma 2.4.4. *Hypothesis 2.4.3 is satisfied by the Kummer, Artin–Schreier, division, and* PGL_2 *towers.*

Proof. In the Kummer case, G_d consists of the d-th roots of unity in $\overline{\mathbb{F}_q}$, and we let $G'_{d,e}$ be those of order exactly e. Then $|G'_{d,e}|$ is independent of d, and we set $\phi(e) = |G'_{d,e}|$. The orbit of Γ through $\zeta \in G'_{d,e}$ has size f where f is the smallest positive integer such that $\zeta^{q^f} = \zeta$. Since ζ has order exactly e, this is the smallest f such that $q^f \equiv 1 \pmod{e}$. Clearly this f satisfies $f \geq \log e/\log q$ and this establishes Hypothesis 2.4.3.

In the Artin–Schreier case, G_d is the additive group of $\mathbb{F}_{p^d}$, and we let $G'_{d,e}$ consists of those elements of $\mathbb{F}_{p^e} \subset \mathbb{F}_{p^d}$ which do not lie in any smaller extension of $\mathbb{F}_p$, i.e., $\alpha \in G'_{d,e}$ if and only if $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^e}$. We set $\phi(e) = |G'_{d,e}|$ (which is independent of d). Since $\alpha^{p^f} \neq \alpha$ for $0 < f < e$, it follows immediately that the orbit of the q-power Frobenius through $\alpha \in G'_{d,e}$ has size at least $e/(\log q/\log p)$, and this establishes Hypothesis 2.4.3.

In the division case, G_d consists of the $\overline{\mathbb{F}_q}$-points of E of order dividing d. We let $G'_{d,e}$ be the subset of points of order exactly e, and $\phi(e) = |G'_{d,e}|$ (which is independent of d). If $P \in G'_{d,e}$ and $\mathrm{Fr}_q^f(P) = P$, then $P \in E(\mathbb{F}_{q^f})$, and this implies that $|E(\mathbb{F}_{q^f})| \geq e$. But the Weil bound implies that $|E(\mathbb{F}_{q^f})| \leq (q^{f/2}+1)^2$ which in turn implies that $f \geq C\log e$ for some constant C independent of e.

In the PGL_2 case, G_d is $\mathrm{PGL}_2(\mathbb{F}_{p^d})$. For $g \in G_d$, let $\mathbb{F}_p(g)$ be defined as follows: choose a representative of g in $\mathrm{GL}_2(\mathbb{F}_{p^d})$ one of whose entries is 1, and let $\mathbb{F}_p(g)$ be the extension of $\mathbb{F}_p$ generated by the other entries. It is easy to see that $\mathbb{F}_p(g)$ is well defined independent of the choice of representative and that $\mathrm{Fr}_p^f(g) = g$ if and only if Fr_p^f fixes $\mathbb{F}_p(g)$. We let $G'_{d,e}$ consists of those elements $g \in G_d$ with $\mathbb{F}_p(g) = \mathbb{F}_{p^e}$. We set $\phi(e) = |G'_{d,e}|$ (which is independent of d). Since $\mathrm{Fr}_p^f(g) \neq g$ for $0 < f < e$, it follows immediately that the orbit of the q-power Frobenius through $g \in G'_{d,e}$ has size at least $e/(\log q/\log p)$, and this establishes Hypothesis 2.4.3. □

Remark 2.4.5. A "dual" perspective makes Hypothesis 2.4.3 more transparent in the cases considered in Lemma 2.4.4. Namely, let $F = \mathbb{F}_q(\mathcal{C})$ be the function field of a curve of genus 0 or 1 over $\mathbb{F}_q$. (These are the cases where $\mathrm{Aut}_{\overline{\mathbb{F}_q}}(\mathcal{C})$ is infinite.) For each d, let G_d be a subgroup of $\mathrm{Aut}_{\overline{\mathbb{F}_q}}(\mathcal{C})$ which is stable under the q-power Frobenius, and let Γ_d be the group of automorphisms of G_d generated by Frobenius. The quotient $(\mathcal{C} \times \overline{\mathbb{F}_q})/G_d$ has a canonical model over $\mathbb{F}_q$; let F_d be its function field. With this notation, the extension F/F_d is geometrically Galois with group (G_d, Γ_d). Suppose further that if $e \mid d$ then $G_e \subset G_d$, so that $F_d \subset F_e$. Then it is natural to define G'_d as the set of elements in G_d which are not in G_e for any divisor of d with $e < d$. Clearly G'_e depends only on e, and the decomposition $G_d = \cup_{e\mid d} G'_e$ is evident. All of the examples of Lemma 2.4.4 can be recast in this form.

The following lemma is modeled on [Griffon 2016, Lemme 3.1.1].

Lemma 2.4.6. *Let K_d/K be a tower of geometrically Galois extensions such that for all d, $|G_d| \geq d$ and such that Hypothesis 2.4.3 holds. Then there is a constant C_1 such that the number of orbits of Γ_d on G_d satisfies*

$$|G_d/\Gamma_d| \leq C_1 \frac{|G_d|}{\log|G_d|}$$

for all $d > 1$.

Proof. Let $\psi(d) = |G_d|$, so that $\psi(d) = \sum_{e\,|\,d} \phi(e)$. Extend ψ to a function of real numbers which is continuous, increasing, and satisfies $\psi(x) \geq x$ for all x. By Hypothesis 2.4.3, for all $d > 1$ the number of orbits of Γ_d on $G'_{d,e}$ satisfies

$$|G'_{d,e}/\Gamma_d| \leq C^{-1} \frac{\phi(e)}{\log \psi(e)}.$$

Let $x > 1$ be a parameter to be chosen later. We have

$$\begin{aligned}
|\Gamma_d| &\leq C_2 \sum_{1<e\,|\,d} \frac{\phi(e)}{\log \psi(e)} && (C_2 \text{ to compensate for omitting } e = 1)\\
&= C_2 \sum_{\substack{1<e\,|\,d\\ e\leq x}} \frac{\phi(e)}{\log \psi(e)} + C_2 \sum_{\substack{1<e\,|\,d\\ e>x}} \frac{\phi(e)}{\log \psi(e)}\\
&\leq C_2 \sum_{\substack{1<e\,|\,d\\ e\leq x}} \frac{\phi(e)}{\log \psi(e)} + C_2 \frac{\psi(d)}{\log \psi(x)} && \Big(\textstyle\sum \phi(e) = \psi(d) \text{ and } \psi \text{ increasing}\Big)\\
&\leq C_2 \sum_{\substack{1<e\,|\,d\\ e\leq x}} \frac{\psi(e)}{\log \psi(e)} + C_2 \frac{\psi(d)}{\log \psi(x)} && (\phi(e) \leq \psi(e))\\
&\leq C_3 \frac{\psi(x)}{\log \psi(x)} \sum_{\substack{1<e\,|\,d\\ e\leq x}} 1 + C_2 \frac{\psi(d)}{\log \psi(x)} && (x \mapsto \psi(x) \mapsto \psi(x)/\log\psi(x), \text{ increasing for } x > 2.72)\\
&\leq C_3 \frac{x\psi(x)}{\log \psi(x)} + C_2 \frac{\psi(d)}{\log \psi(x)}\\
&\leq C_3 \frac{\psi(x)^2}{\log \psi(x)} + C_2 \frac{\psi(d)}{\log \psi(x)} && (\psi(x) \geq x)
\end{aligned}$$

Now since ψ is increasing and continuous, we may choose x so that $\psi(x)^2 = \psi(d)$, and for this choice we have

$$|G_d/\Gamma_d| \leq (2C_3 + 2C_2) \frac{\psi(d)}{\log \psi(d)}.$$

Thus setting $C_1 = 2C_3 + 2C_2$ completes the proof. □

We now consider the set of orbits of Γ on a homogeneous space for G.

Lemma 2.4.7. *Let G be a finite group and let T be a principal homogeneous space for G. Let Γ be a group acting on G (by group automorphisms) and on T (by permutations), and suppose that the actions* *of* Γ *on* G *and* T *are compatible with the action of* G *on* T *(i.e., for all* $\gamma \in \Gamma$, $g \in G$, *and* $t \in T$, $\gamma(gt) = \gamma(g)\gamma(t)$. *Then*

$$|T/\Gamma| \leq |G/\Gamma|.$$

Proof. We use the orbit counting lemma:

$$|G/\Gamma| = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}|G^\gamma|$$

where G^γ denotes the set of fixed points of γ acting on G. Similarly,

$$|T/\Gamma| = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}|T^\gamma|$$

where T^γ denotes the set of fixed points of γ acting on G. We claim that if T^γ is not empty, then it is a principal homogeneous space for G^γ. Indeed, it is clear that if $g \in G^\gamma$ and $t \in T^\gamma$, then $gt \in T^\gamma$. Conversely, if $t, t' \in T^\gamma$ and $g \in G$ is the unique element such that $gt = t'$, then

$$\gamma(g)t = \gamma(g)\gamma(t) = \gamma(gt) = \gamma(t') = t' = gt,$$

and so $\gamma(g) = g$. Therefore, for each $\gamma \in \Gamma$, $|T^\gamma| \leq |G^\gamma|$. We conclude that

$$|T/\Gamma| = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}|T^\gamma| \leq \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}|G^\gamma| = |G/\Gamma|,$$

and this completes the proof of the lemma. □

Remark 2.4.8. In fact, the conclusion of the lemma holds when we assume only that G acts transitively on T. To see this, it suffices to check that for all $\gamma \in \Gamma$, $|T^\gamma| \leq |G^\gamma|$. If T^γ is empty, there is nothing to prove. If not, choose $t_0 \in T^\gamma$, let G_0 be the stabilizer of t_0 in G, and set

$$F(\gamma) = \{g \in G \mid \gamma(gt_0) = gt_0\} = \{g \in G \mid g^{-1}\gamma(g) \in G_0\}.$$

Then G_0 acts freely on $F(\gamma)$ by right multiplication, and the quotient is T^γ. Thus $|F(\gamma)| = |G_0| \cdot |T^\gamma|$. On the other hand, G^γ acts freely on $F(\gamma)$ by left multiplication, and the quotient maps injectively to G_0 by $g \mapsto g^{-1}\gamma(g)$. Thus we find

$$|G_0| \cdot |T^\gamma| = |F(\gamma)| \leq |G^\gamma| \cdot |G_0|$$

and so $|T^\gamma| \leq |G^\gamma|$. It is also clear that $G^\gamma G_0 \subset F(\gamma)$ so in all we have

$$\frac{|G^\gamma|}{|G_0^\gamma|} \leq |T^\gamma| \leq |G^\gamma|.$$

Simple examples show that both bounds are sharp. Thanks to Alex Ryba for the proofs in this remark and the preceding lemma.

Corollary 2.4.9. *Suppose that K_d is a tower of geometrically Galois extensions of K such that $[K_d : K] \geq d$ and such that Hypothesis 2.4.3 holds. Let v be a place of K. Then there is a constant C_v depending only on K and v such that for all d the number of place of K_d over v is at most $C_v[K_d : K]/\log[K_d : K]$.*

Proof. First assume that v is unramified in K_d. Let T_d be the set of geometric points in the fiber over v (i.e., in the fiber of the map of curves corresponding to the extension K_d/K) and let $G = G_d$ be the geometric Galois group of K_d over K. Let k_v be the residue field at v and let $\Gamma_d = \mathrm{Gal}(k_d/k_v)$, a subgroup of the Galois group of the splitting field of G_d. Then T_d is a principal homogeneous space for G_d, and Γ_d acts on G_d and T_d compatibly with the action of G_d on T_d. By Lemma 2.4.7, $|T_d/\Gamma_d| \leq |G_d/\Gamma_d|$. But T_d/Γ_d is in bijection with the set of places of K_d over v, and by Lemma 2.4.6 (applied to the extensions k_vK_d/k_vK), there is a constant C_v (depending on v because the tower in question depends on v) such that

$$|G_d/\Gamma_d| \leq C_v \frac{[K_d : K]}{\log[K_d : K]}.$$

This completes the proof of the corollary when v is unramified in K_d. The general case follows from the same argument using Remark 2.4.8 in place of Lemma 2.4.7. □

2.5. ***Bounds on Tamagawa numbers*** **(2).** We now turn to a second improvement on the Hindry–Pacheco bound on Tamagawa numbers. We consider towers of fields satisfying the conclusions of Lemma 2.3.5 and Corollary 2.4.9, and we bound Tamagawa numbers using only a mild (local) semistability hypothesis and no restriction on the characteristic of the ground field.

Recall the line bundle ω_A associated to an abelian variety A defined in Section 2.1.

Proposition 2.5.1. *Let K be a global function field of characteristic p, let Z be a finite set of places of K, and let K_d be a tower of geometrically Galois extensions of K. Assume that $[K_d : K] \geq d$ and that for each place v of K there is a constant C_v such that the number of places of K_d dividing v is $\leq C_v[K_d : K]/\log[K_d : K]$ for all d. Suppose that each K_d/K is unramified outside Z. Let A be an abelian variety over K which has semistable reduction at each place $v \in Z$ and such that $\deg \omega_A > 0$. Let $A_d = A \times_K K_d$. Then*

$$\tau(A_d) = O(H(A_d)^\epsilon)$$

for every $\epsilon > 0$.

Proof. To lighten notation, let $D = [K_d : K]$. Since A has semistable reduction at the possibly ramified places Z, we have $\deg \omega_{A_d} = D \deg \omega_A \geq D$, so it will suffice to show that

$$\tau(A_d) = O(q^{D\epsilon})$$

for all $\epsilon > 0$.

For each place v of K, let c_v be the order of the group of connected components of the special fiber of the Néron model of A at v. Let $\bar{c}_v$ be the order of the group of connected components of the special fiber of the Néron model of A at a place of $\overline{\mathbb{F}}_q K$ over v. (The order is independent of the choice.) Since the former group is a subgroup of the latter, c_v divides $\bar{c}_v$. If w is a place of K_d over v, let c_w be the order of the component group of the Néron model of A over K_d.

Consider a place $v \notin Z$. Since K_d/K is unramified at v, c_w divides $\bar{c}_v$. By assumption, the number of places w over v is bounded by $C_v D/\log D$. Since there are only finitely many places of K where A has bad reduction, we may set $C_1 = \max\{\bar{c}_v^{C_v} \mid v \text{ of bad reduction}\}$ and conclude that

$$\prod_{w \mid v \notin Z} c_w \leq \prod_{v \notin Z} \bar{c}_v^{C_v D/\log D} \leq C_1^{D/\log D}.$$

Now consider a place $v \in Z$, let w be a place of K_d over v, and let r be the ramification index of w over v. Since K_d/K is geometrically Galois, r depends only on v. Since A is assumed to have semistable reduction, [Halle and Nicaise 2010, Theorem 5.7] implies that

$$c_w \leq \bar{c} r^{\dim(A)}.$$

Moreover, by assumption, the number of places of K_d over v is at most $\min\{D/r, C_v D/\log D\}$ for some constant C_v which is independent of D. If $r \leq (\log D)/C_v$, we have

$$\prod_{w \mid v} c_w \leq (\bar{c}_v r^{\dim(A)})^{C_v D/\log D} \leq C_2^{D/(\log D/\log\log D)}$$

where C_2 depends only on v and A. If $r \geq (\log D)/C_v$, we have

$$\prod_{w \mid v} c_w \leq (\bar{c}_v r^{\dim(A)})^{D/r} \leq C_3^{D \log r/r} \leq C_4^{D/(\log D/\log\log D)}$$

where again C_3 and C_4 depend only on v and A.

Taking the product over all place w of K_d and setting $C_5 = \max\{C_2, C_4\}$, we have

$$\prod_{w} c_w = \Bigg(\prod_{w \mid v \notin Z} c_w\Bigg)\Bigg(\prod_{w \mid v \in Z} c_w\Bigg) \leq (C_1^{D/\log D})(C_5^{D/(\log D/\log\log D)})^{|Z|}$$

and this is clearly $O(q^{D\epsilon})$ as d (and therefore D) tends to infinity. □

We now give the main application of the results in this section. Assume $K = \mathbb{F}_q(t)$ or $K = \mathbb{F}_q(E)$ for an elliptic curve E, and consider a family of abelian varieties A_d over K associated to the Kummer, Artin–Schreier, division, or PGL_2 towers. Recall the line bundle $\omega = \omega_A$ defined in the Section 2.1.

Corollary 2.5.2. *As d runs through positive integers prime to p (or all positive integers in the Artin–Schreier case), we have*

$$\tau(A_d) = O(H(A_d)^\epsilon)$$

for every $\epsilon > 0$ in any of the following situations:

(1) *A is an abelian variety over $K = \mathbb{F}_q(t)$, A_d is the family associated to the Kummer tower*, $\deg(\omega) > 0$, *and A has semistable reduction at $t = 0$ and $t = \infty$.*

(2) *A is an abelian variety over $K = \mathbb{F}_q(t)$, A_d is the family associated to the Artin–Schreier tower*, $\deg(\omega) > 0$, *and A has semistable reduction at $t = \infty$.*

(3) *A is an abelian variety over $K = \mathbb{F}_q(E)$, A_d is the family associated to the division tower, and* $\deg(\omega) > 0$.

(4) *A is an abelian variety over $K = \mathbb{F}_q(t)$, A_d is the family associated to the* PGL_2 *tower*, $\deg(\omega) > 0$, *and A has semistable reduction at $t = 0$ and $t = 1$.*

Proof. This is an immediate consequence of Proposition 2.5.1 together with Lemma 2.3.5. □

2.6. *Bounds on Tamagawa numbers* (3). Our third improvement on the Hindry–Pacheco bound on Tamagawa numbers is to note that we can get by with a weaker hypotheses in case (1) of Corollary 2.5.2. Namely, we claim that the conclusion of the corollary holds if there exists an integer e relatively prime to p such that A has semistable reduction at the places $u = 0$ and $u = \infty$ of $\mathbb{F}_q(u)$ where $u^e = t$. (The corollary is the case where $e = 1$.)

To check the claim, we first recall a result of Halle and Nicaise: Let A be an abelian variety over $\overline{\mathbb{F}_p}((t))$. For d prime to p, let c_d denote the order of the component group of the special fiber of the Néron model of A over $\overline{\mathbb{F}_p}((t^{1/d}))$. Then [Halle and Nicaise 2010, Theorem 6.5] states that if we assume that A acquires semistable reduction over $\overline{\mathbb{F}_p}((t^{1/e}))$ for some e prime to p, then the series

$$\sum_{(p,d)=1} c_d T^d$$

is a rational function in T and $1/(T^j - 1)$ for $j \geq 1$. This implies in particular that the c_d have at worst polynomial growth: $c_d = O(d^N)$ for some N.

Applying this result in the context of part (1) of the lemma for the places $t = 0$ and $t = \infty$ of $\mathbb{F}_q(t)$, we see that

$$\tau(A_d) \leq C_1^{d/\log d} d^{C_6} = O(H(A_d)^{\epsilon})$$

for all $\epsilon > 0$.

2.7. *Estimating* $\deg(\omega_J)$. When $A = J$ is the Jacobian of a curve X over a function field, computing $\deg(\omega_J)$ typically involves knowledge of a regular model of X (or a mildly singular model), information which is sometimes difficult to obtain. The following lemma allows us to reduce to easy cases in two examples later in the paper.

Lemma 2.7.1. *Let $K = k(\mathcal{C})$ be the function field of a curve over a perfect field k. Let X be a smooth, projective curve of genus g over K. Let J be the Jacobian of X, let $\pi : \mathcal{X} \to \mathcal{C}$ be a regular minimal model of X over K, and let $\mathcal{J} \to \mathcal{C}$ be the Néron model of J with zero-section $z : \mathcal{C} \to \mathcal{J}$. Let*

$$\omega_J := \bigwedge\nolimits^g (z^* \Omega^1_{\mathcal{J}/\mathcal{C}})$$

be the Hodge bundle of J.

Let K' be a finite, separable, geometric extension of K, and let $\rho : \mathcal{C}' \to \mathcal{C}$ be the corresponding morphism of curves over k. Let $R = (2g_{\mathcal{C}'} - 2) - [K' : K](2g_{\mathcal{C}} - 2)$.

Let $X' = X \times_K K'$ with Jacobian J', models $\mathcal{X}'$ and $\mathcal{J}'$, and Hodge bundle $\omega_{J'}$. Then

$$[K' : K] \deg(\omega_J) \le \deg(\omega_{J'}) + gR.$$

The point of the lemma is that we do not lose much information in passing to a finite extension.

Proof of Lemma 2.7.1. Since $\mathcal{X}$ is regular and π has a section, we have that

$$\omega_J \cong \bigwedge^g (\pi_* \Omega^2_{\mathcal{X}/k} \otimes (\Omega^1_{\mathcal{C}/k})^{-1}) \cong \left(\bigwedge^g \pi_* \Omega^2_{\mathcal{X}/k}\right) \otimes (\Omega^1_{\mathcal{C}/k})^{\otimes^{-g}}$$

and similarly for $\omega_{J'}$. This argument, which uses results on Néron models and relative duality, is given in the proof of [Berger et al. 2015, Prop. 7.4].

There is a dominant rational map $\mathcal{X}' \dashrightarrow \mathcal{X}$ covering ρ, so pull back of 2-forms induces a nonzero morphism of sheaves

$$\rho^* \bigwedge^g (\pi_* \Omega^2_{\mathcal{X}/k}) \to \bigwedge^g (\pi'_* \Omega^2_{\mathcal{X}'/k}).$$

By Riemann–Hurwitz, we have

$$\rho^*(\Omega^1_{\mathcal{C}/K}) \cong \Omega^1_{\mathcal{C}'/k} \otimes \mathcal{O}_{\mathcal{C}'}(D)$$

where D is a divisor on $\mathcal{C}'$ of degree R.

Thus we get a nonzero morphism of sheaves

$$\rho^*(\omega_J) \to \omega_{J'} \otimes \mathcal{O}_{\mathcal{C}'}(gD).$$

Taking degrees, we conclude that

$$[K' : K] \deg(\omega_J) \le \deg(\omega_{J'}) + gR$$

as desired. □

3. Integrality of the regulator and general lower bounds

In this section, we give a lower bound on the regulator $\mathrm{Reg}(A)$ in terms of Tamagawa numbers. Combined with the bounds on $\tau(A)$ given in the preceding section, this yields a lower bound on the Brauer–Siegel ratio. A more general version of the same lower bound was proven in [Hindry and Pacheco 2016, Proposition 7.6], but our proof is arguably simpler and more uniform, and avoids a forward reference in [Hindry and Pacheco 2016].

3.1. *Integrality of regulators.* We continue with the standard notations introduced in Section 2. In particular, A is an abelian variety over the function field $K = k(\mathcal{C})$ with Néron model $\mathcal{A}$ and dual abelian variety $\hat{A}$. We consider the height pairing $A(K) \times \hat{A}(K) \to \mathbb{Q}$ (which we recall is the canonical Néron–Tate height divided by $\log q$ and which takes values in $\mathbb{Q}$) and its determinant $\mathrm{Reg}(A)$.

Our main goal in this section is to bound the denominator of the regulator in terms of the orders c_v of the component groups of $\mathcal{A}$ at places v of K. Recall that $\tau(A) = \prod_v c_v$.

Proposition 3.1.1. *The rational number*

$$\tau(A)\,\mathrm{Reg}(A)$$

is an integer.

Proof. We refer to [Hindry and Silverman 2000] for general background on heights. Given an invertible sheaf $\mathcal{L}$ on A and a point $x \in A(K)$, the general theory of heights on abelian varieties defines a rational number $h_{\mathcal{L}}(x)$. The canonical height pairing we are discussing is defined using this machine and the identification of $\hat{A}$ with $\mathrm{Pic}^0(A)$, the group of invertible sheaves algebraically equivalent to zero. In other words, given $x \in A(K)$ and $y \in \hat{A}(K)$, we take $\mathcal{L}$ to be the invertible sheaf associated to y and define

$$\langle x, y\rangle = h_{\mathcal{L}}(x).$$

Néron's theory [1965] decomposes the height $h_{\mathcal{L}}(x)$ into a sum of local terms indexed by the places of K. In [Moret-Bailly 1985, III.1], Moret-Bailly proves that the contribution at a place v has denominator at most $2c_v$, and at most c_v if c_v is odd. Moreover, he gives an example which shows that this is in general best possible. The upper bound on the denominator comes from a property of "pointed maps of degree 2," [Moret-Bailly 1985, I.5.6], namely that a pointed map of degree 2 from a group of exponent n has exponent at worst $2n$, or n if n is odd. (These terms will be defined just below.)

In our situation there is slightly more structure: Since $\mathcal{L}$ is algebraically equivalent to zero, it is antisymmetric, i.e., if $[-1]$ is the inverse map on A, the $[-1]^*\mathcal{L} \cong \mathcal{L}^{-1}$. The functoriality in [Moret-Bailly 1985, III.1.1] then shows that the corresponding pointed map of degree 2 is also antisymmetric. In the next lemma, we define antisymmetric pointed maps of degree 2, and we prove that such a map from a group of exponent c has exponent dividing c.

Thus we see that $\langle x, y\rangle$ is a sum of local terms, and the term at a place v has denominator at worst c_v. It follows from the bilinearity of the local terms $\langle , \rangle_v$ that if x passes through the identity component at v, then $\langle x, y\rangle_v$ is an integer. We define a "reduced Mordell–Weil group"

$$A(K)^{\mathrm{red}} := \{x \in A(K) \mid x \text{ meets the identity component of } \mathcal{A} \text{ at every } v\},$$

and note that if $x \in A(K)^{\mathrm{red}}$, then $\langle x, y\rangle$ is an integer for every $y \in \hat{A}(K)$. Since the index of $A(K)^{\mathrm{red}}$ in $A(K)$ divides $\tau(A) = \prod_v c_v$, we see that

$$\mathrm{Reg}(A) \in \tau^{-1}\mathbb{Z}$$

as desired. The proposition thus follows from the next lemma. □

Lemma 3.1.2. *Let A and G be abelian groups and let $f : A \to G$ be a function such that*:

(1) *f is a "pointed map of degree 2," namely*,

$$f(x_1+x_2+x_3) - f(x_1+x_2) - f(x_1+x_3) - f(x_2+x_3) + f(x_1) + f(x_2) + f(x_3) = 0$$

for all $x_1, x_2, x_3 \in A$.

(2) f *is "antisymmetric," i.e.,* $f(-x) = -f(x)$ *for all* $x \in A$.

Then for all integers n and all $x \in A$, $f(nx) = nf(x)$. *In particular, if A has exponent c, then* $cf = 0$, *i.e.,* $cf(x) = 0$ *for all* $x \in A$.

Proof. This follows from a simple inductive argument. Clearly it suffices to treat the case $n \geq 0$. Taking $x_1 = x_2 = x_3 = 0$ in the pointed map property shows that $f(0) = 0$. Taking $x_1 = x_2 = x$ and $x_3 = -x$ then shows that $f(2x) = 2f(x)$. Finally, for $n \geq 2$, taking $x_1 = (n-1)x$, $x_2 = x_3 = x$, we have

$$\begin{aligned} f((n+1)x) &= f((n-1)x + x + x) \\ &= f(nx) + f(nx) + f(2x) - f((n-1)x) - f(x) - f(x) \\ &= (n + n + 2 - (n-1) - 1 - 1) f(x) \\ &= (n+1)x, \end{aligned}$$

where we use induction to pass from the second displayed line to the third. This yields the lemma. □

Without the antisymmetry hypothesis, we would have

$$f(nx) = \frac{n(n+1)}{2} f(x) + \frac{n(n-1)}{2} f(-x),$$

by the same argument leading from the theorem of the cube [Hindry and Silverman 2000, A.7.2.1] to Mumford's formula [Hindry and Silverman 2000, A.7.2.5].

3.2. ***Further comments on integrality.*** Let $\mathcal{X} \to \mathcal{C}$ be a fibered surface with generic fiber X/K and assume X has a K-rational point. Let A be the Jacobian J_X. In [Berger et al. 2015, Proposition 7.2], we proved that the rational number

$$\frac{|\mathrm{NS}(\mathcal{X})_{tor}|^2}{|A(K)_{tor}|^2} \tau(A) \operatorname{Reg}(A) \tag{3.2.1}$$

is an integer. (By the factorization of birational maps into blow-ups and the blow-up formula, $\mathrm{NS}(\mathcal{X})_{tor}$ is a birational invariant, so the displayed quantity depends only on X and K.)

Note that this bound on the denominator of $\operatorname{Reg}(A)$ is in general stronger than that of Proposition 3.1.1. For example, for the Jacobians studied in [Ulmer 2014b; Berger et al. 2015], (3.2.1) is stronger than Proposition 3.1.1.

When X has genus 1, it is known that $\mathrm{NS}(\mathcal{X})_{tor}$ is trivial, so (3.2.1) says that

$$\frac{\tau(A)}{|A(K)_{tor}|^2} \operatorname{Reg}(A) \in \mathbb{Z} \tag{3.2.2}$$

This bound (unlike (3.2.1)) makes sense for general abelian varieties, and it is reasonable to ask whether it holds in general. In the rest of this subsection, we sketch a proof that (3.2.2) does not hold in general, not even for Jacobians over $\mathbb{F}_q(t)$.

Let $\mathcal{Y}$ be a classical Enriques surface over $\mathbb{F}_p$. It is known that

$$\mathrm{NS}(\mathcal{Y})_{tor} \cong \mathbb{Z}/2\mathbb{Z}, \quad \mathrm{NS}(\mathcal{Y})/tor \cong \mathbb{Z}^{10}, \quad \text{and} \quad \det(\mathrm{NS}(\mathcal{Y})) = 1;$$

see [Cossec and Dolgachev 1989].

Next, embed $\mathcal{Y}$ in some projective space and take a Lefschetz pencil, extending $\mathbb{F}_p$ to $\mathbb{F}_q$ if necessary. Let $\mathcal{X}$ be the result of blowing up $\mathcal{Y}$ at the base points of the pencil. Thus we have $\pi : \mathcal{X} \to \mathbb{P}^1$ over $\mathbb{F}_q$ whose fibers are irreducible and either smooth or with single a node. Moreover π has a section. Choose such a section O and a fiber F. We have intersection pairings $O^2 = -1$, $F^2 = 0$, and $F.O = 1$. Also, the Néron–Severi groups satisfy

$$\mathrm{NS}(\mathcal{X}) = \mathrm{NS}(\mathcal{Y}) \oplus \langle -1 \rangle^d$$

where the direct sum is orthogonal, $\langle -1 \rangle$ stands for a copy of $\mathbb{Z}$ whose generator has self-intersection -1, and d is the number of blow-ups. Thus $\det(\mathrm{NS}(\mathcal{X})) = 1$.

Let $X/K = \mathbb{F}_q(t)$ be the generic fiber of π. This is a smooth curve with a K-rational point. Let $A = J_X$ be its Jacobian. We will see shortly that A is a counterexample to (3.2.2).

Since $\mathrm{Pic}^0(\mathcal{X}) = \mathrm{Pic}^0(\mathcal{Y}) = 0$, we have $\mathrm{Tr}_{K/\mathbb{F}_q}(A) = 0$. The Shioda–Tate theorem gives an exact sequence

$$0 \to (\mathbb{Z}O + \mathbb{Z}F) \to \mathrm{NS}(\mathcal{X}) \to A(K) \to 0.$$

Moreover, the fact that π has irreducible fibers implies that there is a splitting $A(K) \to \mathrm{NS}(\mathcal{X})$ which sends the canonical height (divided by $\log q$) to the intersection pairing on $\mathrm{NS}(\mathcal{X})$. It follows from the intersection formulas for O and F noted above that

$$\mathrm{Reg}(A) := \det(A(K)/tor) = \det(NS(\mathcal{X})/tor) = 1.$$

Since π has irreducible fibers, $\tau(A) = 1$. The Shioda–Tate exact sequence above shows that $A(K)_{tor}$ has order at least 2 (in fact, exactly 2), so

$$\frac{\tau(A)}{|A(K)_{tor}|^2} \mathrm{Reg}(A) = \frac{1}{4}.$$

Thus (3.2.2). fails for A.

3.3. ***Lower bounds on Brauer–Siegel ratio from integrality.*** We now state the main consequence for the Brauer–Siegel ratio of our Proposition 3.1.1.

Proposition 3.3.1. *Let A_d be a family of abelian varieties over K with $H(A_d) \to \infty$. Assume that $\tau(A_d) = O(H(A_d)^\epsilon)$ for all $\epsilon > 0$. Then $\liminf \mathrm{BS}(A_d) \geq 0$.*

Proof. Noting that $|Ш(A_d)|$ is a positive integer and is therefore ≥ 1, we have that

$$\log(|Ш(A_d)| \, \mathrm{Reg}(A_d)) \geq \log(\mathrm{Reg}(A_d)).$$

Proposition 3.1.1 implies that

$$\log(\mathrm{Reg}(A_d)) \geq -\log(\tau(A_d)).$$

It follows from the hypothesis $\tau(A_d) = O(H(A_d)^\epsilon)$ that

$$\mathrm{BS}(A_d) = \frac{\log(|\text{Ш}(A_d)|\,\mathrm{Reg}(A_d))}{\log(H(A_d))} \geq \frac{-\log(\tau(A_d))}{\log(H(A_d))}$$

has $\liminf \geq 0$ as $d \to \infty$. □

Corollary 3.3.2. *If A_d is a family of abelian varieties over K such that $H(A_d) \to \infty$, then in any of the following situations* $\liminf \mathrm{BS}(A_d) \geq 0$:

(1) $\dim(A_d) = 1$ *for all d.*

(2) *A is an abelian variety over $K = \mathbb{F}_q(t)$, A_d is the family associated to A and the Kummer tower, and A has semistable reduction at $t = 0$ and $t = \infty$.*

(3) *A is an abelian variety over $K = \mathbb{F}_q(t)$, A_d is the family associated to A and the Artin–Schreier tower, and A has semistable reduction at $t = \infty$.*

(4) *A is an abelian variety over $K = \mathbb{F}_q(E)$, and A_d is the family associated to A and the division tower.*

(5) *A is an abelian variety over $K = \mathbb{F}_q(t)$, A_d is the family associated to A and the* PGL_2 *tower, and A has semistable reduction at $t = 0$ and $t = 1$.*

Proof. This is immediate from Lemma 2.2.1, Corollary 2.5.2, and Proposition 3.3.1. □

4. Lower bounds via the dimension of the Tate–Shafarevich functor

In this section, we assume that the conjecture of Birch and Swinnerton-Dyer (more precisely, the finiteness of $\text{Ш}(A)$) holds for all abelian varieties considered. Given an abelian variety A over $K = \mathbb{F}_q(\mathcal{C})$, we will consider the functor from finite extensions of $\mathbb{F}_q$ to groups given by

$$\mathbb{F}_{q^n} \mapsto \text{Ш}(A \times_{\mathbb{F}_q(\mathcal{C})} \mathbb{F}_{q^n}(\mathcal{C}))$$

and we will show that the dimension of this functor (to be defined below) gives information on the Brauer–Siegel ratio of A over K. This technical device will be extremely convenient as it allows us to bound the Brauer–Siegel ratio without considering the regulator.

Proposition/Definition 4.1. *For each positive integer n, let $K_n := \mathbb{F}_{q^n}(\mathcal{C})$. Given an abelian variety A over $K = K_1$, write A/K_n for $A \times_K K_n$. Then the limit*

$$\lim_{n\to\infty} \frac{\log|\text{Ш}(A/K_n)[p^\infty]|}{\log(q^n)}$$

exists and is an integer. We call it the dimension of $\text{Ш}(A)$, *and denote it* $\dim \text{Ш}(A)$.

The proof of the proposition will be given later in this section, after giving a formula for $\dim \text{Ш}(A)$ in terms of the L-function of A. We give a justification of the terminology “dimension” in Remarks 4.3 below.

In order to state a formula for $\dim Ш(A)$, we recall some well-known results on the L-function $L(A,s)$. Let $A_0 = \mathrm{Tr}_{K/k}(A)$ be the K/k-trace of A, an abelian variety over k (where as usual $k = \mathbb{F}_q$). (See [Conrad 2006] for a modern account of the K/k-trace.) Then $L(A,s)$ has the form

$$L(A,s) = \frac{P(q^{-s})}{Q(q^{-s})Q(q^{1-s})}$$

where P and Q are polynomials with the following properties:

(1) $P(T) = \prod_i (1 - \alpha_i T)$ where the α_i are Weil numbers of size q.

(2) Q has degree $2\dim(A_0)$ and $Q(T) = \prod_j (1 - \beta_j T)$ where the β_j are the Weil numbers of size $q^{1/2}$ associated to A_0. (In other words, they are the eigenvalues of Frobenius on $H^1(A_0 \times \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)$ for any $\ell \neq p$.)

(3) $Q(1) = |A_0(\mathbb{F}_q)|$ and $Q(q^{-1}) = q^{-d_0}|A_0(\mathbb{F}_q)|$.

(4) Replacing A with A/K_n has the effect of replacing the α_i and β_j with α_i^n and β_j^n.

Let F be the number field generated by the α_i, and choose a prime of F over p with associated valuation v normalized so that $v(q) = 1$. We define the *slopes* associated to A to be the rational numbers $\lambda_i = v(\alpha_i)$. It is known that the set of slopes (with multiplicities) is independent of the choice of v, that $0 \le \lambda_i \le 2$ for all i, and that the set of slopes is invariant under $\lambda_i \mapsto 2 - \lambda_i$.

We can now state a formula for the dimension of $Ш(A)$.

Proposition 4.2. $$\dim Ш(A) = \deg(\omega) + \dim(A)(g_C - 1) + \dim(A_0) - \sum_{\lambda_i < 1} (1 - \lambda_i).$$

The last sum is over indices i such that $\lambda_i < 1$.

Before giving the proof of Propositions 4.1 and 4.2, we record an elementary lemma on p-adic numbers.

Lemma 4.2.1. *Let E be a finite extension of $\mathbb{Q}_p$, let $\mathfrak{m}$ be the maximal ideal of E, and let* $\mathrm{ord} : E^\times \to \mathbb{Z}$ *be the valuation of E. If $\gamma \in E^\times$ has* $\mathrm{ord}(\gamma) = 0$ *and is not a root of unity, then*

$$\mathrm{ord}(1 - \gamma^n) = O(\log n).$$

Proof. First we note that replacing γ with γ^a, we may assume without loss of generality that γ is a 1-unit, i.e., that $\mathrm{ord}(1-\gamma) > 0$. Next, if $n = p^e m$ with $p \nmid m$, then

$$\frac{1-\gamma^n}{1-\gamma^{p^e}} = 1 + \gamma^{p^e} + \cdots + \gamma^{p^e(m-1)} \equiv m \not\equiv 0 \pmod{\mathfrak{m}},$$

so $\mathrm{ord}(1-\gamma^n) = \mathrm{ord}(1-\gamma^{p^e})$. Thus it suffices to treat the case where $n = p^e$.

We write $\exp_p$ and $\log_p$ for the p-adic exponential and logarithm respectively. (See, e.g., [Koblitz 1984, IV.1] for basic facts on these functions.) For y sufficiently close to 1 (namely for $|y-1| < |p^{1/(p-1)}|$), we have $y = \exp_p(\log_p(y))$. Also, it follows from the power series definition of $\exp_p$, the ultrametric property of E, and the estimate $v_p(n!) \leq n/(p-1)$ that if $x \neq 0$ and $\mathrm{ord}(x)$ is sufficiently large (e.g., $\mathrm{ord}(x) > 2/(p-1)$ suffices), then

$$\mathrm{ord}(1-\exp_p(x)) = \mathrm{ord}(x).$$

Now if e is sufficiently large, then γ^{p^e} is close to 1, and $x = \log_p(\gamma^{p^e}) = p^e \log_p(\gamma)$ has large valuation and is not zero, so we may apply the estimate above to deduce that

$$\mathrm{ord}(1-\gamma^{p^e}) = \mathrm{ord}(1-\exp_p(\log_p(\gamma^{p^e}))) = \mathrm{ord}(\log_p(\gamma^{p^e})) = \mathrm{ord}(p^e) + \mathrm{ord}(\log_p(\gamma)).$$

This last quantity is a linear function of e and thus a linear function of $\log(p^e)$, and this proves our claim. □

Proof of Propositions 4.1 and 4.2. We use the leading coefficient part of the BSD conjecture and consider the p-adic valuations of the elements of the formula. For simplicity, we first consider the case where $A_0 := \mathrm{Tr}_{K/k}(A) = 0$ and then discuss the modifications needed to handle the general case at the end.

As a first step, we establish that several factors in the BSD formula do not contribute to the limit in Proposition/Definition 4.1. More precisely, as n varies, $\mathrm{Reg}(A/K_n)$, $\tau(A/K_n)$, and $|A(K_n)_{tor}| \cdot |\hat{A}(K_n)_{tor}|$ are bounded. To see that $\mathrm{Reg}(A/K_n)$ is bounded, we note that it is sensitive to the ground field $\mathbb{F}_{q^n}$ only via the Mordell–Weil group $A(K_n)/tor$. In other words, if $A(K_n)/tor = A(K_m)/tor$, then $\mathrm{Reg}(A/K_n) = \mathrm{Reg}(A/K_m)$. This follows from the geometric nature of the definition of Reg (i.e, its definition in terms of intersection numbers). From the Lang–Néron theorem on the finite generation of $A(K\overline{\mathbb{F}_q})$, it follows that there are only finitely many possibilities for $A(K_n)/tor$, so only finitely many possibilities for $\mathrm{Reg}(A/K_n)$. It also follows that $|A(K_n)_{tor}|$ and $|\hat{A}(K_n)_{tor}|$ are bounded. (Our use of the Lang–Néron theorem here depends on the assumption that $A_0 = 0$.) Similarly, since the orders of the component groups of the fibers of the Néron model of A over $\overline{\mathbb{F}_q}(\mathcal{C})$ are bounded, there are only finitely possibilities for $\tau(A/K_n)$. Finally, we note that the geometric quantities $\deg(\omega)$, $\dim(A)$, and $g_{\mathcal{C}}$ do not vary with n.

Write $L^*(A/K_n)_p$ for the p-part of the rational number $L^*(A/K_n)$. Then the BSD formula and the remarks above imply that

$$\begin{aligned}\lim_{n\to\infty} \frac{\log|Ш(A/K_n)[p^\infty]|}{\log(q^n)} &= \lim_{n\to\infty} \frac{\log(L^*(A/K_n)_p q^{n(\deg(\omega)+\dim(A)(g_{\mathcal{C}}-1))})}{\log(q^n)} \\ &= \lim_{n\to\infty} \frac{\log(L^*(A/K_n)_p)}{\log(q^n)} + \deg(\omega) + \dim(A)(g_{\mathcal{C}}-1).\end{aligned}$$

Thus to complete the proof of the existence of the limit in Proposition/Definition 4.1 and the formula of Proposition 4.2 in the case $A_0 = 0$, we need only check that

$$\lim_{n\to\infty} \frac{\log(L^*(A/K_n)_p)}{\log q^n} = \sum_{\lambda_i<1} (\lambda_i - 1).$$

Again under the assumption that $A_0 = 0$, we have

$$L^*(A/K_n) = \prod_i{}' (1 - (\alpha_i/q)^n)$$

where $\prod_i'$ is the product over indices i such that $(\alpha_i/q)^n \neq 1$. We view the right hand side as an element of the number field F introduced above to define the slopes, and we let E (as in Lemma 4.2.1) be the completion of F at the chosen prime of F over p. If $\lambda = v(\alpha_i) < 1$, then

$$v(1 - (\alpha_i/q)^n) = v((\alpha_i/q)^n) = n(\lambda_i - 1),$$

whereas is $\lambda_i > 1$, then

$$v(1 - (\alpha_i/q)^n) = v(1) = 0.$$

In the intermediate case where $\lambda_i = 1$, there are two cases: if α_i/q is not a root of unity, then Lemma 4.2.1 implies that

$$v(1 - (\alpha_i/q)^n) = O(\log n).$$

If α_i/q is a root of unity, then there are only finitely many possibilities for $v(1-(\alpha_i/q)^n)$ with $(\alpha_i/q)^n \neq 1$, and if $(\alpha_i/q)^n = 1$, then it does not contribute to $L^*(A/K_n)$. Taking the product over i, we find that

$$\lim_{n\to\infty} \frac{\log(L^*(A/K_n)_p)}{\log q^n} = \sum_{\lambda_i<1} (\lambda_i - 1).$$

This establishes the formula in Proposition 4.2.

Since the break points of a Newton polygon have integer coordinates, $\sum_{\lambda_i<1}(\lambda_i - 1)$ is an integer. In the case $A_0 = 0$, we have thus established that the limit in Proposition/Definition 4.1 exists and is an integer, and we have established the formula in Proposition 4.2 for the limit, i.e., for $\dim Ш(A)$.

In case $A_0 = \mathrm{Tr}_{K/k}(A)$ is nonzero, the L-function is more complicated, the torsion is not uniformly bounded, and we have to be slightly more careful with the regulator. Here are the details: The Lang–Néron theorem says that $A(K\overline{\mathbb{F}_q})/A_0(\overline{\mathbb{F}_q})$ is finitely generated. This implies that there are only finitely many possibilities for $A(K_n)/A_0(\mathbb{F}_{q^n})$ and for the regulator (since $A(K_n)/tor$ is a quotient of $A(K_n)/A_0(\mathbb{F}_{q^n})$). Moreover,

$$|A(K_n)_{tor}| = |(A(K_n)/A_0(\mathbb{F}_{q^n}))_{tor}| \cdot |A_0(\mathbb{F}_{q^n})_{tor}|$$

and similarly for $\hat{A}$. On the other hand, writing

$$L(A,s) = \frac{P(q^{-s})}{Q(q^{-s})Q(q^{1-s})} = \frac{\prod_i (1 - \alpha_i q^{-s})}{\prod_j (1 - \beta_j q^{-s})(1 - \beta_j q^{1-s})},$$

we have that

$$L^*(A/K_n) = \frac{\prod_{(\alpha_i/q)^n \neq 1} (1 - (\alpha_i/q)^n)}{\prod_j (1 - (\beta_j/q)^n)(1 - \beta_j^n)}.$$

The denominator is

$$q^{-n\dim(A_0)}|A_0(\mathbb{F}_{q^n})|^2 = q^{-n\dim(A_0)}|A_0(\mathbb{F}_{q^n})|\cdot|\hat{A}_0(\mathbb{F}_{q^n})|$$

so the ratio

$$\frac{|A(K_n)_{tor}|\cdot|\hat{A}(K_n)_{tor}|}{\prod_j(1-(\beta_j/q)^n)(1-\beta_j^n)} = q^{n\dim(A_0)}|(A(K_n)/A_0(\mathbb{F}_{q^n}))_{tor}|\cdot|(\hat{A}(K_n)/\hat{A}_0(\mathbb{F}_{q^n}))_{tor}|$$

is $q^{n\dim(A_0)}$ times a quantity which is bounded as n varies. It then follows that

$$\lim_{n\to\infty}\frac{\log(|A(K_n)_{tor}|\cdot|\hat{A}(K_n)_{tor}|\cdot L^*(A/K_n)_p)}{\log q^n} = \dim(A_0)+\sum_{\lambda_i<1}(\lambda_i-1).$$

Therefore,

$$\begin{aligned}\lim_{n\to\infty}\frac{\log|\text{Ш}(A/K_n)|}{\log(q^n)} &= \lim_{n\to\infty}\frac{\log(|A(K_n)_{tor}|\cdot|\hat{A}(K_n)_{tor}|\cdot L^*(A/K_n)q^{n(\deg(\omega)+\dim(A)(g_C-1))})}{\log(q^n)}\\ &= \dim(A_0)+\sum_{\lambda_i<1}(\lambda_i-1)+\deg(\omega)+\dim(A)(g_C-1).\end{aligned}$$

This completes the proof of Propositions 4.1 and 4.2. □

Remarks 4.3. (1) In our applications, we will compute $\dim \text{Ш}(A)$ directly from its definition using crystalline methods. Proposition 4.2 suggests that these methods will succeed exactly in those situations where one can compute the slopes λ_i, i.e., exactly in the cases where the methods of Hindry–Pacheco and Griffon succeed.

(2) We explain why the terminology "dimension of $\text{Ш}(A)$" is reasonable. Assume that A is a Jacobian. If $\mathrm{Sel}(A, p^m)$ denotes the Selmer group for multiplication by p^m on A, then it is known that the functor $\mathbb{F}_{q^n} \mapsto \mathrm{Sel}(A\times_K K\mathbb{F}_{q^n}, p^m)$ from finite extensions of $\mathbb{F}_q$ to groups is represented by a group scheme which is an extension of an étale group scheme by a unipotent connected quasialgebraic group $U[p^m]$, and the dimension of $U[p^m]$ is constant for large m [Artin 1974]. (One may even replace "finite extensions of $\mathbb{F}_q$" with "affine perfect $\mathbb{F}_q$-schemes," but unfortunately, not with "general affine schemes.") Since the order of $A(K\mathbb{F}_{q^n})/p^mA(K\mathbb{F}_{q^n})$ is bounded for varying n, we may detect the dimension of $U[p^m]$ by computing the order of $\text{Ш}(A\times K\mathbb{F}_{q^n})[p^m]$ asymptotically as $n\to\infty$. Thus $\dim \text{Ш}(A)$ as we have defined it in this paper is equal to the dimension of the unipotent quasialgebraic group $U[p^m]$. (Note however that $\mathbb{F}_{q^n}\mapsto \text{Ш}(A\times_k K\mathbb{F}_{q^n})[p^\infty]$ is not in general represented by a group scheme.)

(3) The formula in Proposition 4.2 for $\dim \text{Ш}(A)$ is proven using the BSD formula. Conversely, in case A is a Jacobian, Milne [1975, §7] computes the dimension of the group scheme mentioned in the previous remark, and this calculation is a key input into his proof of the leading coefficient formula of the BSD and Artin–Tate conjectures. Our approach is thus somewhat ahistorical, but it is elementary (modulo the BSD conjecture) and completely general.

(4) In the case where A is a Jacobian, the formula of Proposition 4.2 is equivalent to the formula of Milne for the unipotent group scheme mentioned above, i.e., to the last displayed equation in [Milne 1975, §7].

(5) The proof of Proposition 4.2 suggests that $\dim Ш(A)$ can be viewed as an analog of the Iwasawa μ-invariant.

(6) If $K_n = \mathbb{F}_{q^n}(\mathcal{C})$, A is an abelian variety over K_1 with $\deg(\omega_A) > 0$, and we define the "p-Brauer–Siegel ratio of A" by

$$\mathrm{BS}_p(A) := \frac{\log(R|Ш(A)|)_p}{\log H(A)}$$

where $(x)_p$ denotes the p-part of the rational number x, then we have

$$\lim_{n\to\infty} \mathrm{BS}_p(A/K_n) = \frac{\dim Ш(A)}{\deg(\omega_A)}.$$

This gives an interpretation of $\dim Ш$ in terms of a modified Brauer–Siegel ratio.

In situations where we can control $\tau(A)$, the following proposition gives a tool to bound the Brauer–Siegel ratio of A from below.

Proposition 4.4. *We have*

$$\frac{\log(|Ш(A)|\,\mathrm{Reg}(A)\tau(A))}{\log(q)} \geq \dim Ш(A).$$

Proof. We keep the notation of the proof of Proposition 4.2. In particular, A_0 denotes the K/k trace of A. Using the BSD formula and estimating the denominator of $L^*(A)$, we have

$$\begin{aligned}
|Ш(A)|\,\mathrm{Reg}(A)\tau(A) &\geq \frac{|Ш(A)|\,\mathrm{Reg}(A)\tau(A)}{|(A(K_n)/A_0(\mathbb{F}_{q^n}))_{tor}| \cdot |(\hat{A}(K_n)/\hat{A}_0(\mathbb{F}_{q^n}))_{tor}|} \\
&= |A_0(\mathbb{F}_{q^n})| \cdot |\hat{A}_0(\mathbb{F}_{q^n})| L^*(A) q^{\deg(\omega)+\dim(A)(g_{\mathcal{C}}-1)} \\
&\geq q^{\deg(\omega)+\dim(A)(g_{\mathcal{C}}-1)+\dim(A_0)-\sum(1-\lambda_i)} \\
&= q^{\dim Ш(A)}
\end{aligned}$$

and this yields the proposition. □

Remark 4.5. The bound of the proposition is more subtle than it may seem at first: $\dim Ш(A)$ is defined in terms of the asymptotic growth of $Ш(A)$ as the ground field grows (i.e., replacing $\mathbb{F}_q$ with $\mathbb{F}_{q^n}$), whereas the left-hand side of the inequality concerns invariants over the given ground field $\mathbb{F}_q$. In fact, a lower bound on the dimension of $Ш(A)$ is not sufficient to give nontrivial lower bounds on $Ш(A)$ itself. (This is related to the nonrepresentability of $Ш$ mentioned above.) For example, if E denotes the Legendre curve studied in [Ulmer 2014b] over $K = \mathbb{F}_{p^{2f}}(t^{1/(p^f+1)})$, then [Ulmer 2014b, Corollary 10.2] shows that $\dim Ш(E) = (p^f - 1)/2$, whereas [Ulmer 2014c, Theorem 1.1] shows that when $f \leq 2$, $Ш(E)$ is trivial. This example also shows that the second inequality displayed above is sharp.

Next, we state the result which is our main motivation for considering $\dim Ш(A)$.

Proposition 4.6. *Let A_d be a family of abelian varieties over K with $H(A_d) \to \infty$. Assume that $\tau(A_d) = O(H(A_d)^\epsilon)$ for all $\epsilon > 0$. Then*

$$\liminf_{d\to\infty} \mathrm{BS}(A_d) \geq \liminf_{d\to\infty} \frac{\dim Ш(A_d)}{\deg(\omega_{A_d})}.$$

Proof. The hypothesis $\tau(A_d) = O(H(A_d)^\epsilon)$ for all $\epsilon > 0$ implies that

$$\lim_{d\to\infty} \log(\tau(A_d))/\log(H(A_d)) = 0,$$

so the proposition follows immediately from the estimate of Proposition 4.4. □

Corollary 4.7. *If A_d is a family of abelian varieties over K such that $H(A_d) \to \infty$, then*

$$\liminf_{d\to\infty} \mathrm{BS}(A_d) \geq \liminf_{d\to\infty} \frac{\dim Ш(A_d)}{\deg(\omega_{A_d})}$$

in any of the following situations:

(1) $\dim(A_d) = 1$ *for all n*

(2) *A is an abelian variety over $K = \mathbb{F}_q(t)$, A_d is the family associated to the Kummer tower, and A has semistable reduction at $t = 0$ and $t = \infty$.*

(3) *A is an abelian variety over $K = \mathbb{F}_q(t)$, A_d is the family associated to the Artin–Schreier tower, and A has semistable reduction at $t = \infty$.*

(4) *A is an abelian variety over $K = \mathbb{F}_q(E)$, and A_d is the family associated to the division tower.*

(5) *A is an abelian variety over $K = \mathbb{F}_q(t)$, A_d is the family associated to the PGL_2 tower, and A has semistable reduction at $t = 0$ and $t = 1$.*

Proof. This is immediate from Lemma 2.2.1, Corollary 2.5.2, and Proposition 4.6. □

5. Brauer–Siegel ratio and Frobenius

As a first application of our results on the dimension of Ш, we compute the Brauer–Siegel ratio for sequences of abelian varieties associated to the Frobenius isogeny.

More precisely, let E be an elliptic curve over the function field $K = \mathbb{F}_q(\mathcal{C})$, and for $n \geq 1$, let E_n be the Frobenius base change:

$$E_n := E^{(p^n)} = E \times_K K$$

where the right hand morphism $K \to K$ is the p^n-power Frobenius.

Our goal is the following result.

Theorem 5.1. *Assume that E is nonisotrivial. Then*

$$\lim_{n\to\infty} \mathrm{BS}(E_n) = 1.$$

Proof. First we note that since E is nonisotrivial, $H(E_n) \to \infty$ as $n \to \infty$. Indeed, the j-invariant of E has a pole, say of order e, at some place of K, so the j invariant of E_n has a pole of order ep^n at the same place. This implies that the degrees of the divisors of one or both of $c_4(E_n)$ and $c_6(E_n)$ also tend to infinity, and this is possible only if $\deg(\omega_{E_n})$ also tends to infinity. Since $H(E_n) = q^{\deg(\omega_{E_n})}$, we have that $H(E_n) \to \infty$.

Next we note that Proposition 4.2 shows that $\dim Ш(E_n) - \deg(\omega_{E_n})$ depends only on the L-function of E_n, indeed only on the slopes of the L-function. Since E and E_n are isogenous, they have the same L-function, so we have

$$\dim Ш(E_n) - \deg \omega_{E_n} = \dim Ш(E) - \deg \omega_E$$

for all n.

Dividing the last displayed equation by $\deg \omega_{E_n}$ and taking the limit as $n \to \infty$, we get

$$\frac{\dim Ш(E_n)}{\deg \omega_{E_n}} \to 1$$

since $\deg(\omega_{E_n}) \to \infty$.

Applying part (1) of Corollary 4.7, we see that $\liminf_{n\to\infty} \mathrm{BS}(E_n) \geq 1$. On the other hand, by [Hindry and Pacheco 2016, Corollary 1.13], $\limsup_{n\to\infty} \mathrm{BS}(E_n) \leq 1$, so we find that $\lim_{n\to\infty} \mathrm{BS}(E_n) = 1$, as desired. □

Remark 5.2. The same argument works for an abelian variety A as long as $\deg(\omega_{A^{(p^n)}}) \to \infty$ with n and $\tau(A^{(p^n)}) = o(H(A^{(p^n)}))$.

Remark 5.3. The theorem says that the product $|Ш(E_n)|\,\mathrm{Reg}(E_n)$ grows with n. Our earlier results on p-descent [Ulmer 1991] can be used to show directly that $Ш(E_n)$ grows with n. Full details require an unilluminating consideration of many cases, so we limit ourselves to a sketch in the simplest situation. First, let $V : E^{(p)} \to E$ be the Verschiebung isogeny, and note that the Selmer group $\mathrm{Sel}(E^{(p)}, p)$ contains $\mathrm{Sel}(E, V)$. Also, let L be the (Galois) extension of K obtained by adjoining the $(p-1)$-st root of a Hasse invariant of E, and let $G = \mathrm{Gal}(L/K)$. In [Ulmer 1991, Theorem 3.2 and Lemma 1.4], we computed that

$$\mathrm{Sel}(E, V) \cong \mathrm{Hom}(J_{\mathfrak{m}}/<\text{cusps}>, \mathbb{Z}/p\mathbb{Z})^G$$

where $J_{\mathfrak{m}}$ is the generalized Jacobian of the curve whose function field is L for a "modulus" $\mathfrak{m}$ related to the places of bad and/or supersingular reduction of E. Rosenlicht showed that $J_{\mathfrak{m}}$ is an extension of J by a linear group (see [Serre 1988]), and the unipotent part of this group contributes to the "dimension" of $\mathrm{Sel}(E, V)$ and therefore to $\dim Ш(E^{(p)})$. The contribution is roughly the number of zeroes (with multiplicity) of the Hasse invariant, namely $(p-1)\deg(\omega_E)$ which is approximately $\deg(\omega_{E^{(p)}}) - \deg(\omega)$. Thus we find

$$\dim Ш(E^{(p)}) \geq \deg(\omega_{E^{(p)}}) - \deg(\omega),$$

in agreement with what we deduced from Proposition 4.2.

6. Bounding Ш for a class of Jacobians

In this section, we review a general method for computing the p-part of the Tate–Shafarevich group of certain Jacobians, generalizing our previous work [Ulmer 2014c] on the Legendre elliptic curve. Although these methods suffice to compute the p-part of Ш on the nose, for simplicity we focus just on dim Ш as this is what is needed to bound the Brauer–Siegel ratio from below.

6.1. ***Jacobians related to products of curves.*** Let k be the finite field $\mathbb{F}_q$ of characteristic p with q elements. Let $\mathcal{C}$ and $\mathcal{D}$ be curves over k, and let $\mathcal{S}=\mathcal{C}\times_k\mathcal{D}$. Suppose that Δ is a group of k-automorphisms of $\mathcal{S}$ with order prime to p and such that

$$\Delta\subset \mathrm{Aut}_k(\mathcal{C})\times\mathrm{Aut}_k(\mathcal{D})\subset\mathrm{Aut}_k(\mathcal{S}).$$

Suppose that the quotient $\mathcal{S}/\Delta$ is birational to a smooth, projective surface $\mathcal{X}$ over k and that $\mathcal{X}$ is equipped with a surjective and generically smooth morphism $\pi:\mathcal{X}\to C$ where C is a smooth projective curve over k. Let $K=k(C)$ and let X be the generic fiber of π, a smooth projective curve over K. We assume that X has a K-rational point. (A vast supply of such data is given in [Berger 2008; Ulmer 2013].)

Let J be the Jacobian of X. We write $\mathrm{Br}(\mathcal{X})$ for the cohomological Brauer group of $\mathcal{X}$: $\mathrm{Br}(\mathcal{X})=H^2(\mathcal{X},\mathrm{G}_m)$.

Proposition 6.2. (1) *$\text{Ш}(J_X)$ and $\mathrm{Br}(\mathcal{X})$ are finite groups.*

(2) *There is a canonical isomorphism $\text{Ш}(J_X)\cong\mathrm{Br}(\mathcal{X})$.*

(3) *There is a canonical isomorphism*

$$\mathrm{Br}(\mathcal{X})[p^\infty]\cong(\mathrm{Br}(\mathcal{S})[p^\infty])^\Delta.$$

Proof. In substance, parts (2) and (3) are due to Grothendieck [1968] and part (1) is due to Tate [1966]. The details to deduce the statements here are given in [Ulmer 2014c, §4]. □

6.3. ***Brauer group of a product of curves.*** We keep the notation of the preceding subsection. In addition, let $W=W(k)$ be the ring of Witt vectors over k with Frobenius endomorphism σ. We write $H^1(\mathcal{C})$ for the crystalline cohomology $H^1_{crys}(\mathcal{C}/W)$ and similarly for $H^1(\mathcal{D})$. These are modules over the Dieudonné ring $A=W\{F,V\}$, which is the noncommutative polynomial ring generated over W by symbols F and V with relations $FV=VF=p$, $F\alpha=\sigma(\alpha)F$, and $\alpha V=V\sigma(\alpha)$ for all $\alpha\in W$.

The following crystalline calculation of the p part of the Brauer group of $\mathcal{S}$ is originally due to Dummigan (with additional hypotheses) using results of Milne, and is proven in general in [Ulmer 2014c, §10].

Proposition 6.4. *There is a canonical isomorphism*

$$\mathrm{Br}(\mathcal{S})[p^n]\cong\frac{\mathrm{Hom}_A(H^1(\mathcal{C})/p^n,H^1(\mathcal{D})/p^n)}{\mathrm{Hom}_A(H^1(\mathcal{C}),H^1(\mathcal{D}))/p^n}$$

which is compatible with the actions of Δ on both sides.

Here Hom_A denotes W-linear homomorphisms which commute with F and V.

Propositions 6.2 and 6.4 give us a powerful tool for bounding $\dim Ш(J)$ from below. Recall that this means bounding the growth of the order of $Ш(J)$ as we extend the ground field from $\mathbb{F}_q$ to $\mathbb{F}_{q^\nu}$. The denominator on the right hand side of the displayed equation in Proposition 6.4 is known to be bounded as ν varies (a fact we will see explicitly in Section 8 for the examples we consider), so we have:

Corollary 6.5. *For all sufficiently large n,*

$$\dim Ш(J) = \dim \mathrm{Hom}_A(H^1(\mathcal{C})/p^n, H^1(\mathcal{D})/p^n)^\Delta.$$

Here the dim on the right-hand side is defined analogously to that on the left:

$$\dim \mathrm{Hom}_A(H^1(\mathcal{C})/p^n, H^1(\mathcal{D})/p^n)^\Delta := \lim_{\nu\to\infty} \frac{\log|\mathrm{Hom}_A(H^1(\mathcal{C}\times_k \mathbb{F}_{q^\nu})/p^n, H^1(\mathcal{D}\times_k \mathbb{F}_{q^\nu})/p^n)^\Delta|}{\log(q^\nu)}.$$

Computing the cardinality of the numerator on the right amounts to an interesting exercise in p-linear algebra, at least for certain curves $\mathcal{C}$ and $\mathcal{D}$. We carry out these exercises in Section 8.

7. Cohomology of Fermat curves

We review some well-known result on the cohomology of Fermat curves.

As usual, let $k = \mathbb{F}_q$ be the finite field of cardinality q and characteristic p. We write $\bar{k}$ for the algebraic closure of k. For a positive integer d relatively prime to p, let F_d be the smooth projective curve over k given by

$$x_0^d + x_1^d + x_2^d = 0.$$

We write μ_d for the group of d-th roots of unity in $\bar{k}$. There is an evident action of μ_d^3 on $F_d \times_k \bar{k}$ under which $(\zeta_i) \in \mu_d^3$ acts via $x_i \mapsto \zeta_i x_i$, and the diagonal $(\zeta_0 = \zeta_1 = \zeta_2)$ acts trivially, so we have $G := \mu_d^3/\mu_d \subset \mathrm{Aut}\,\bar{k}(F_d)$.

Let

$$A = \left\{(a_0, a_1, a_2) \;\middle|\; \sum a_i = 0\right\} \subset (\mathbb{Z}/d\mathbb{Z})^3.$$

Abusively writing ζ both for a root of unity in $\bar{k}$ and for its Teichmüller lift to the Witt vectors $W(\bar{k})$, we may identify A with the character group $\mathrm{Hom}(G, W(\bar{k})^\times)$. Let

$$A' = \{(a_i) \in A \mid a_i \neq 0, i = 0, 1, 2\}.$$

Given $(a_0, a_1, a_2) \in A$, let $\langle a_i/d\rangle$ be the fractional part of $\tilde{a}_i/d$, where $\tilde{a}_i$ is any representative in $\mathbb{Z}$ of the class a_i. Define subsets A_0 and A_1 as follows:

$$A_0 = \left\{(a_i) \in A' \;\middle|\; \left\langle\frac{a_0}{d}\right\rangle + \left\langle\frac{a_1}{d}\right\rangle + \left\langle\frac{a_2}{d}\right\rangle = 2\right\}$$

and

$$A_1 = \left\{(a_i) \in A' \;\middle|\; \left\langle\frac{a_0}{d}\right\rangle + \left\langle\frac{a_1}{d}\right\rangle + \left\langle\frac{a_2}{d}\right\rangle = 1\right\}$$

It is a simple exercise to see that A' is the disjoint union of A_0 and A_1. Let $\langle p\rangle$ be the subgroup of $\mathbb{Q}^\times$ generated by p. Then $\langle p\rangle$ acts on A' coordinatewise: $p(a_0, a_1, a_2) = (pa_0, pa_1, pa_2)$.

Let $H = H^1_{crys}(F_d/W(k))$ be the crystalline cohomology of F_d equipped with its action of the p-power Frobenius F and Verschiebung V. Then $\overline{H} := H \otimes_{W(k)} W(\bar{k})$ inherits an action of G.

The following summarizes the main results on H. The argument in [Dummigan 1995, §6], stated in the special case where $d = q + 1$, works for general d prime to p.

Proposition 7.1. *There is W-basis $\{e_a\}$ of H indexed by $a \in A'$ with the following properties*:

(1) $F(e_a) = c_a e_{pa}$ *where* $c_a \in W(k)$ *and*

$$\operatorname{ord}_p(c_a) = \begin{cases} 0 & \text{if } a \in A_0, \\ 1 & \text{if } a \in A_1. \end{cases}$$

(2) *For* $(\zeta_i) \in G$ *and* $a \in A'$,

$$(\zeta_i)e_a = a(\zeta_i)e_a = \zeta_0^{a_0}\zeta_1^{a_1}\zeta_2^{a_2}e_a$$

(*an equality in* $\overline{H}$).

7.2. ***A remark on twists.*** It is sometimes convenient to work with a different model of the Fermat curve, namely

$$F'_d : y_0^d + y_1^d = y_2^d.$$

This is a twist of F_d in the sense that they F_d and F'_d become isomorphic over $\bar{k}$ via

$$(x_0, x_1, x_2) \mapsto (y_0, y_1, \epsilon y_2)$$

where ϵ is a d-th root of -1. It follows that Proposition 7.1 holds for F'_d as well, with possibly different constants c_a which nevertheless continue to satisfy the valuation formula in part (1).

7.3. ***A remark on quotients.*** If $\mathcal{C}$ is the quotient of F_d by a subgroup of $G' \subset G$, then the crystalline cohomology of $\mathcal{C}$ can be identified with the W-submodule of H generated by the e_a whose indices a are trivial on G'.

For example, the hyperelliptic curve

$$\mathcal{C}_{2,d} : y^2 = x^d + 1$$

is the quotient of F'_{2d} by a subgroup of G isomorphic to $\mu_d \times \mu_2$. (If d is even, it is also a quotient of F'_d, but it is more convenient to have a uniform statement.)

More generally, the superelliptic curve

$$\mathcal{C}_{r,d} : y^r = x^d + 1$$

is the quotient of F'_{rd} by a subgroup of G isomorphic to $\mu_d \times \mu_r$.

The crystalline cohomology $H^1_{crys}(\mathcal{C}_{r,d}/W(k))$ can then be identified with the W-submodule of $H^1_{crys}(F'_{rd}/W(k))$ generated by the e_a where a has the form

$$a = (a_0, a_1, a_2) = (ir, -ir - jd, jd) \quad 0 < i < d, \quad 0 < j < r, \quad ir + jd \not\equiv 0 \pmod{rd}.$$

The set I of such indices has cardinality $(r-1)(d-1) - \gcd(r, d) + 1$, and it is the disjoint union $I = I_0 \cup I_1$ where

$$I_0 = I \cap A_0 \cong \{(i, j) \mid 0 < i < d,\ 0 < j < r,\ ir + jd > rd\}$$

and

$$I_1 = I \cap A_1 \cong \{(i, j) \mid 0 < i < d,\ 0 < j < r,\ ir + jd < rd\}.$$

In the case where $r = 2$ we may further simplify this to

$$I_0 \cong \left\{i \mid \tfrac{d}{2} < i < d\right\} \quad \text{and} \quad I_1 \cong \left\{i \mid 0 < i < \tfrac{d}{2}\right\}.$$

These sets, with their action of $\langle p\rangle$, will play a key role in the p-adic exercises that compute $\dim Ш$ for the Jacobians introduced in Section 6.

8. *p*-adic exercises

In this section, we carry out the exercises in semilinear algebra needed to compute the dimension of Ш for several families of abelian varieties.

Let p be a prime and let $\mathbb{F}_q$ be the field of cardinality q and characteristic p. Let $W = W(\mathbb{F}_q)$ be the Witt vectors over $\mathbb{F}_q$, and let $W_n = W/p^n$. Write σ for the p-power Witt-vector Frobenius. For a positive integer ν, we write $\mathbb{F}_{q^\nu}$ for the field of q^ν elements, $W_\nu = W(\mathbb{F}_{q^\nu})$ for the corresponding Witt ring, and $W_{n,\nu}$ for W_ν/p^n.

Let $A = W\{F, V\}$ be the Dieudonné ring of noncommutative polynomials in F and V with relations $FV = VF = p$, $F\alpha = \sigma(\alpha)F$, and $\alpha V = V\sigma(\alpha)$ for $\alpha \in W$. Also, let A_ν be the ring $W_\nu\{F, V\}$ with analogous relations.

Let $\langle p\rangle$ be the cyclic subgroup of $\mathbb{Q}^\times$ generated by p.

8.1. ***Data.*** Fix a finite set I equipped with an action of $\langle p\rangle$, which we write multiplicatively: $i \mapsto pi$. (In the applications below, I will typically be a subset of $\mathbb{Z}/d\mathbb{Z}$ for some d not divisible by p.) Let M be the free W-module with basis indexed by I:

$$M := \bigoplus_{i \in I} W e_i.$$

Write I as a disjoint union $I = I_0 \cup I_1$ and choose elements $c_i \in W$ such that

$$\operatorname{ord}(c_i) = \begin{cases} 0 & \text{if } i \in I_0, \\ 1 & \text{if } i \in I_1. \end{cases}$$

Define a σ-semilinear map $F : M \to M$ by setting

$$F(e_i) = c_i e_{pi}$$

and a σ^{-1}-semilinear map $V : M \to M$ by setting

$$V(e_i) = \frac{p}{\sigma^{-1}(c_{i/p})} e_{i/p}.$$

These definitions give M the structure of an A-module, and there is an induced A-module structure on $M_n := M \otimes_W W_n$. Parallel definitions make $M_\nu := M \otimes_W W_\nu$ and $M_{n,\nu} := M \otimes_W W_{n,\nu}$ into A_ν-modules.

Fix another finite set J equipped with an action of $\langle p \rangle$, write J as a disjoint union $J = J_0 \cup J_1$, and choose elements $d_j \in W$ with

$$\operatorname{ord}(d_j) = \begin{cases} 0 & \text{if } j \in J_0, \\ 1 & \text{if } j \in J_1. \end{cases}$$

Define

$$N := \bigoplus_{j \in J} W f_j,$$

with semilinear maps $F : N \to N$ and $V : N \to N$ defined by

$$F(f_j) = d_j f_{pj}$$

and

$$V(f_j) = \frac{p}{\sigma^{-1}(d_{j/p})} f_{j/p}.$$

Then N and $N_n := N \otimes_W W_n$ are A-modules, and parallel definitions make $N_\nu := N \otimes_W W_\nu$ and $N_{n,\nu} := N \otimes_W W_{n,\nu}$ into A_ν-modules.

Let $\langle p \rangle$ act on $I \times J$ diagonally, and let O be the set of orbits of this action. For an orbit $o \in O$, define

$$d(o) := \min(|((I_0 \times J_1) \cap o)|, |((I_1 \times J_0) \cap o)|).$$

Consider $\operatorname{Hom}_{W_\nu}(N_\nu, M_\nu)$, a free W_ν-module with basis φ_{ij} defined by

$$\varphi_{ij}(f_{j'}) = \begin{cases} e_i & \text{if } j' = j, \\ 0 & \text{if } j' \neq j. \end{cases}$$

These elements induce elements of

$$\operatorname{Hom}_{W_\nu}(N_{n,\nu}, M_{n,\nu}) = \operatorname{Hom}_{W_\nu}(N_\nu, M_\nu)/p^n$$

which form a basis over $W_{n,\nu}$ and which we abusively also denote φ_{ij}.

8.2. ***Statement.*** Our main objects of study in this section are the subgroups

$$H_\nu := \mathrm{Hom}_{A_\nu}(N_\nu, M_\nu) \subset \mathrm{Hom}_{W_\nu}(N_\nu, M_\nu)$$

and

$$H_{n,\nu} := \mathrm{Hom}_{A_\nu}(N_{n,\nu}, M_{n,\nu}) \subset \mathrm{Hom}_{W_\nu}(N_{n,\nu}, M_{n,\nu})$$

consisting of A_ν-module homomorphisms, i.e., homomorphisms φ such that $F\circ\varphi=\varphi\circ F$ and $V\circ\varphi=\varphi\circ V$.

To state the results, we first decompose the groups of interest into components indexed by the set of orbits O. For $o \in O$, let

$$\mathrm{Hom}_{W_\nu}(N_\nu, M_\nu)^o := \left\{\varphi = \sum_{i,j} \alpha_{i,j}\varphi_{i,j} \mid \alpha_{i,j} = 0 \text{ for all } (i, j) \notin o\right\}$$

and

$$\mathrm{Hom}_{W_\nu}(N_{n,\nu}, M_{n,\nu})^o := \left\{\varphi = \sum_{i,j} \alpha_{i,j}\varphi_{i,j} \mid \alpha_{i,j} = 0 \text{ for all } (i, j) \notin o\right\}.$$

We define

$$H_\nu^o := H_\nu \cap \mathrm{Hom}_{W_\nu}(N_\nu, M_\nu)^o \quad \text{and} \quad H_{n,\nu}^o := H_{n,\nu} \cap \mathrm{Hom}_{W_\nu}(N_{n,\nu}, M_{n,\nu})^o.$$

Here is the main result of this section:

Theorem 8.3. (1) *$H_\nu = \oplus_{o\in O} H_\nu^o$ and $H_{n,\nu} = \oplus_{o\in O} H_{n,\nu}^o$.*

(2) *$|H_\nu^o/p^n|$ is at most $p^{n|o|}$ and in particular is bounded independently of ν.*

(3) *For all sufficiently large n,*

$$\lim_{\nu\to\infty} \frac{\log|H_{n,\nu}^o|}{\log(q^\nu)} = d(o).$$

Proof. Let

$$\varphi = \sum_{(i,j)\in I\times J} \alpha_{i,j}\varphi_{i,j}$$

be a typical element of $\mathrm{Hom}_{W_\nu}(N_\nu, M_\nu)$ (with $\alpha_{i,j} \in W_\nu$) or $\mathrm{Hom}_{W_\nu}(N_{n,\nu}, M_{n,\nu})$ (with $\alpha_{i,j} \in W_{n,\nu}$). Then a straightforward calculation shows that $F \circ \varphi = \varphi \circ F$ if and only if

$$c_i\sigma(\alpha_{i,j}) = d_j\alpha_{p(i,j)} \quad \text{for all } (i, j) \in I \times J, \tag{8.3.1}$$

and $V \circ \varphi = \varphi \circ V$ if and only if

$$\left(\frac{p}{d_j}\right)\sigma(\alpha_{i,j}) = \left(\frac{p}{c_i}\right)\alpha_{p(i,j)} \quad \text{for all } (i, j) \in I \times J. \tag{8.3.2}$$

Defining

$$\varphi^o = \sum_{(i,j)\in o} \alpha_{i,j}\varphi_{i,j},$$

it is clear that $\varphi^o \in H_\nu^o$ or $H_{n,\nu}^o$ and that $\varphi = \sum_{o\in O} \varphi^o$. This shows that $H_\nu = \sum_{o\in O} H_\nu^o$ and $H_{n,\nu} = \sum_{o\in O} H_{n,\nu}^o$, and it is immediate that the sums are direct. This proves part (1) of the theorem.

For part (2), take a typical element $\varphi^o = \sum_{(i,j)\in o} \alpha_{i,j}\varphi_{i,j}$ of H_ν^o. Since W_ν is torsion-free, the conditions (8.3.1) and (8.3.2) are equivalent, so we focus on (8.3.1). Fix a base point $(i_0, j_0) \in o$ and note that α_{i_0,j_0} determines the other coefficients $\alpha_{i,j}$ with $(i, j) \in o$ by repeatedly using (8.3.1). Indeed, we have

$$c_{i_0}\sigma(\alpha_{i_0,j_0}) = d_{j_0}\alpha_{p(i_0,j_0)}$$
$$c_{pi_0}\sigma(c_{i_0})\sigma^2(\alpha_{i_0,j_0}) = d_{pj_0}\sigma(d_{j_0})\alpha_{p^2(i_0,j_0)}$$
$$\vdots$$
$$c_{p^{|o|-1}i_0}\sigma(c_{p^{|o|-2}i_0})\cdots\sigma^{|o|-1}(c_{i_0})\sigma^{|o|}(\alpha_{i_0,j_0}) = d_{p^{|o|-1}j_0}\sigma(d_{p^{|o|-2}j_0})\cdots\sigma^{|o|-1}(d_{j_0})\alpha_{i_0,j_0}$$

Here $|o|$ is the cardinality of o and in the last line we use that $p^{|o|}(i_0, j_0) = (i_0, j_0)$. Moreover, α_{i_0,j_0} determines a solution to (8.3.1) only if the last displayed line holds. (There may be other integrality conditions, but they are not important for our argument.) If the valuations of

$$c_{p^{|o|-1}i_0}\sigma(c_{p^{|o|-2}i_0})\cdots\sigma^{|o|-1}(c_{i_0}) \quad \text{and} \quad d_{p^{|o|-1}j_0}\sigma(d_{p^{|o|-2}j_0})\cdots\sigma^{|o|-1}(d_{j_0})$$

are distinct, then it is clear that the only solution is $\alpha_{i_0,j_0} = 0$. On the other hand, if the valuations are the same, the last equation is equivalent to one of the form $\sigma^{|o|}(\alpha_{i_0,j_0}) = \gamma\alpha_{i_0,j_0}$ where $\gamma \in W_\nu$ is a unit. Written in terms of Witt vector components, this last equation is a polynomial of degree $p^{|o|}$ in each component of α_{i_0,j_0} (with coefficients given by γ and the lower Witt components of α_{i_0,j_0}). Therefore, taking α_{i_0,j_0} modulo p^n, there are at most $p^{n|o|}$ solutions, and this proves part (2) of the theorem.

We now turn to part (3) of the theorem, which follows from a somewhat more elaborate version of the calculation of [Ulmer 2014c, §7, §10]. Namely, we fix an orbit o and consider (8.3.1) and (8.3.2) with $(i, j) \in o$ and $\alpha_{i,j} \in W_{n,\nu}$. These are the equations defining $H_{n,\nu}^o$ as a subset of $\mathrm{Hom}_{W_\nu}(N_{n,\nu}, M_{n,\nu})^o$, and analyzing them will allow us to estimate the size of $H_{n,\nu}^o$.

Fix an orbit $o \in O$ and a base point $(i_0, j_0) \in o$. We associate a word w on the alphabet $\{u, l, m\}$ to o as follows: $w = w_1w_2\cdots w_{|o|}$ where

$$w_\ell = \begin{cases} u & \text{if } p^{\ell-1}(i_0, j_0) \in I_1 \times J_0, \\ l & \text{if } p^{\ell-1}(i_0, j_0) \in I_0 \times J_1, \\ m & \text{if } p^{\ell-1}(i_0, j_0) \in (I_0 \times J_0) \cup (I_1 \times J_1). \end{cases}$$

Changing the base point changes w by a cyclic permutation. Note that $d(o)$ is the smaller of the number of appearances of l or u in w.

The motivation for these letters is as follows: If $w_\ell = u$, then in (8.3.1) and (8.3.2) for $(i, j) = p^{\ell-1}(i_0, j_0)$, d_j is a unit and p/c_j is a unit. It follows that the two equations are equivalent and either of them determines $\alpha_{p^\ell(i_o,j_0)}$ in terms of $\alpha_{p^{\ell-1}(i_o,j_0)}$. i.e., the "upper" $\alpha_{p^\ell(i_o,j_0)}$ is determined by the "lower" $\alpha_{p^{\ell-1}(i_o,j_0)}$. Similarly, if $w_\ell = l$, the "lower" $\alpha_{p^{\ell-1}(i_o,j_0)}$ is determined by the "upper" $\alpha_{p^\ell(i_o,j_0)}$. Finally, if $w_\ell = m$, then one of (8.3.1) and (8.3.2) implies other and shows that $\alpha_{p^{\ell-1}(i_o,j_0)}$ and $\alpha_{p^\ell(i_o,j_0)}$ determine each other. We will use these observations to eliminate most of the variables in the systems (8.3.1) and (8.3.2), and use the simplified system to estimate the size of $H^o_{n,\nu}$ and prove part (3) of the theorem.

We first deal with three degenerate cases, namely those where w is a power of m, or has no letters l, or has no letters u. In all three cases, $d(o)=0$, so it will suffice to prove that $|H^o_{n,\nu}|$ is bounded independently of ν. If $w=m^{|o|}$, then α_{i_0,j_0} determines all of the $\alpha_{p^\ell(i_0,j_0)}$, and the system ((8.3.1)–(8.3.2)) reduces to a single equation

$$\sigma^{|o|}\alpha_{i_0,j_0}=\gamma\alpha_{i_0,j_0}$$

where $\gamma\in W$ us a unit. This is easily seen to have at most $p^{n|o|}$ solutions for any ν, as desired. If w contains no letters l, then again α_{i_0,j_0} determines all of the $\alpha_{p^\ell(i_0,j_0)}$, and the system ((8.3.1)–(8.3.2)) reduces to a single equation

$$p^e\sigma^{|o|}\alpha_{i_0,j_0}=\gamma\alpha_{i_0,j_0}$$

where $e\geq 0$ and $\gamma\in W$ is a unit. (Here e is the number of appearances of u in w.) If $e=0$, we are in the previous case, and the equation has at most $p^{n|o|}$ solutions for any ν, whereas if $e>0$, then this equation is easily seen to have no solutions. Finally, if w has no letter u, then the system again reduces to a single equation of the form

$$\sigma^{|o|}\alpha_{i_0,j_0}=\gamma p^e\alpha_{i_0,j_0}$$

which has at most $p^{n|o|}$ solutions for any ν if $e=0$ and has no solutions if $e>0$.

For the rest of the argument, we may assume w contains at least one u and at least one l. Define a function $a:\{0,1,\dots,|o|\}\to\mathbb{Z}$ by setting $a(0)=0$ and

$$a(\ell)=a(\ell-1)+\begin{cases}1 & \text{if } w_\ell=u,\\ -1 & \text{if } w_\ell=l,\\ 0 & \text{if } w_\ell=m.\end{cases}$$

for $1\leq\ell\leq|o|$.

Define the *height* of o, denoted $ht(o)$, to be the maximum value of a minus the minimum value of a. Note that this is independent of the choice of a base point for o.

We divide into two cases depending on whether $a(|o|)\geq 0$ or $a(|o|)\leq 0$.

If $a(|o|)\geq 0$, we may change base point so that $0=a(0)$ is the minimum value of a (i.e., $a(\ell)\geq 0$ for $0\leq\ell\leq|o|$) and $a(|o|-1)>a(|o|)$. Indeed, start with any base point (i_0,j_0) and let ℓ_0 be such that $a(\ell_0)$ is minimum among the $a(\ell)$. Then replacing (i_0,j_0) with $(i_1,j_1)=p^{\ell_0}(i_0,j_0)$ ensures that $a(\ell)\geq 0$ for all $0\leq\ell\leq|o|$. If the new word w ends with m or u, we may replace (i_1,j_1) with $p^{-1}(i_1,j_1)$ without affecting the inequality $a(\ell)\geq 0$. Iterate until the last letter is l, thus yielding the desired base point. We fix such as base point and denote it (i_0,j_0).

Choose

$$0=\ell_0<\ell^0<\ell_1<\ell^1\cdots<\ell^{k-1}<\ell_k=|o|$$

such that a is nondecreasing on $\{\ell_\lambda, \dots, \ell^\lambda\}$ and nonincreasing on $\{\ell^\lambda, \dots, \ell_{\lambda+1}\}$ for $0 \le \lambda \le k-1$. In particular, the ℓ_λ are the arguments of local minima of a. Now let

$$\beta_\lambda = \alpha_{p^{\ell_\lambda}(i_0, j_0)} \quad 0 \le \lambda \le k.$$

(Note that $\beta_k = \beta_0$.) Then the motivating remarks above about the letters u, l, m show that the β_λ determine all the $\alpha_{i,j}$ with $(i, j) \in o$. The equations (8.3.1) and (8.3.2) hold if and only if the β_λ satisfy the system:

$$\begin{aligned} p^{e_1}\sigma^{\ell_1-\ell_0}\beta_0 &= \gamma_1 p^{e_2}\beta_1 \\ p^{e_3}\sigma^{\ell_2-\ell_1}\beta_1 &= \gamma_2 p^{e_4}\beta_2 \\ &\vdots \\ p^{e_{2k-1}}\sigma^{\ell_k-\ell_{k-1}}\beta_{k-1} &= \gamma_k p^{e_{2k}}\beta_k \end{aligned} \tag{8.3.3}$$

where

$$\begin{aligned} e_{2\lambda-1} &= \#\text{ of appearances of } u \text{ in the subword } w_{\ell_{\lambda-1}+1}\cdots w_{\ell_\lambda} \\ e_{2\lambda} &= \#\text{ of appearances of } l \text{ in the subword } w_{\ell_{\lambda-1}+1}\cdots w_{\ell_\lambda} \end{aligned}$$

and the units γ_λ are defined by

$$\gamma_\lambda = p^{e_{2\lambda-1}-e_{2\lambda}} \prod_{\ell=\ell_{\lambda-1}}^{\ell_\lambda - 1} \sigma^{\ell_\lambda-1-\ell}\left(\frac{d_{p^\ell j_0}}{c_{p^\ell i_0}}\right).$$

To recap, the assignment $\varphi \mapsto (\beta_\lambda)$ gives an injection $H^o_{n,\nu} \hookrightarrow W^k_{n,\nu}$ whose image is the set of solutions to equations (8.3.3). We will finish the proof of part (3) of the theorem by estimating the number of such solutions.

Since the theorem is an assertion about $H^o_{n,\nu}$ for sufficiently large n, we will assume for the rest of the proof that $n \ge ht(o)$. Then we have an exact sequence

$$0 \to p^{n-ht(o)}H^o_{n,\nu} \to H^o_{n,\nu} \to W_{n-ht(o),\nu}$$

where the right hand map sends a tuple (β_λ) to the reduction modulo $p^{n-ht(o)}$ of β_0. (Exactness in the middle follows from the fact that if $\mu \le n - ht(o)$, then we may recover the Witt components $\beta^{(\mu)}_\lambda$ from β_0 modulo $p^{n-ht(o)}$ using the equations (8.3.3) and the fact that $a(\ell) \ge a(0)$ for all ℓ.) Moreover, we have

$$\beta_0 \equiv (\gamma_1 \cdots \gamma_k)^{-1} p^{a(|o|)} \sigma^{|o|}\beta_0 \pmod{p^{n-ht(o)}}.$$

It follows that the image of $H^o_{n,\nu}$ in $W_{n-ht(o),\nu}$ has order at most $p^{|o|(n-ht(o))}$ independently of ν. (We may even conclude that it is 0 if $a(|o|) > 0$.) Thus this image does not contribute to the limit in the theorem, and it will suffice to bound $p^{n-ht(o)}H^o_{n,\nu}$.

Note also that if $n' > n \ge ht(o)$, then

$$p^{n-ht(o)}H^o_{n,\nu} \xrightarrow{\sim} p^{n'-ht(o)}H^o_{n',\nu}$$

via $(\beta_\lambda)\mapsto(p^{n'-n}\beta_\lambda)$. Thus we may assume that $n=ht(o)$ for the rest of the proof.

To finish the estimation, we "break" the circular system (8.3.3) into a triangular system, as in [Ulmer 2014c, §7.6]. To that end, choose λ so that $a(\ell^\lambda)$ is the maximum of a, and note that $ht(0)=a(\ell^\lambda)-a(0)=a(\ell^\lambda)$. Then we have

$$ht(o)=a(\ell^\lambda)=e_1-e_2+\cdots+e_{2\lambda+1}$$

and

$$0=p^{ht(o)}\beta_0=p^{e_1-e_2+\cdots+e_{2\lambda+1}}\beta_0=p^{e_3-e_4+\cdots+e_{2\lambda+1}}\sigma^{-\ell_1}(\gamma_1\beta_1)=\cdots=p^{e_{2\lambda+1}}\sigma^{-\ell_1}(\gamma_1)\cdots\sigma^{-\ell_\lambda}(\gamma_\lambda\beta_\lambda).$$

It follows that $p^{e_{2\lambda+1}}\beta_\lambda=0$. Using this in (8.3.3) and reordering, we obtain a lower-triangular system

$$\begin{aligned}
0&=\gamma_{\lambda+1}p^{e_{2\lambda+2}}\beta_{\lambda+1}\\
0&=-p^{e_{2\lambda+3}}\sigma^{\ell_{\lambda+2}-\ell_{\lambda+1}}\beta_{\lambda+1}+\gamma_{\lambda+2}p^{e_{2\lambda+4}}\beta_{\lambda+2}\\
&\ \ \vdots\\
0&=-p^{e_{2k-1}}\sigma^{\ell_k-\ell_{k-1}}\beta_{k-1}+\gamma_k p^{e_{2k}}\beta_k\\
0&=-p^{e_1}\sigma^{\ell_1-\ell_0}\beta_0+\gamma_1 p^{e_2}\beta_1\\
&\ \ \vdots\\
0&=-p^{e_{2\lambda-1}}\sigma^{\ell_\lambda-\ell_{\lambda-1}}\beta_{\lambda-1}+\gamma_\lambda p^{e_{2\lambda}}\beta_\lambda.
\end{aligned}$$

This system can be rewritten in the form

$$U_1BU_2\begin{pmatrix}\beta_{\lambda+1}\\ \vdots\\ \beta_k\\ \beta_1\\ \vdots\\ \beta_\lambda\end{pmatrix}=0$$

where U_1 and U_2 are diagonal with powers of σ and products of the units γ_i in the diagonal entries and where

$$B=\begin{pmatrix}
p^{e_{2\lambda+2}} &&&&&&\\
-p^{e_{2\lambda+3}} & p^{e_{2\lambda+4}} &&&&&\\
&&\ddots&&&&\\
&&-p^{e_{2k-1}} & p^{e_{2k}} &&&\\
&&& -p^{e_1} & p^{e_2} &&\\
&&&&&\ddots&\\
&&&&&-p^{e_{2\lambda-1}} & p^{e_{2\lambda}}
\end{pmatrix}.$$

It follows that the number of solutions to this system is

$$q^{\nu(e_2+e_4+\cdots+e_{2k})}.$$

On the other hand, $e_2+e_4+\cdots+e_{2k}$ is the total number of appearances of l in the word w, and since $a(|o|)\geq 0$, w has at least as many appearances of u as of l, so this sum is equal to $d(o)$. It follows that $|H^o_{ht(o),\nu}|=q^{\nu d(o)}$ and that

$$\lim_{\nu\to\infty}\frac{\log|H^o_{n,\nu}|}{\log(q^\nu)}=d(o)$$

for any $n\geq ht(o)$. This completes the proof of part (3) of the theorem under the hypothesis that $a(|o|)\geq 0$.

The proof when $a(|o|)\leq 0$ is very similar. Roughly speaking, one proceeds as above, but with a base point so that $a(|o|)$ is the minimum of a and with β_k playing the role of β_0. More precisely, assuming that w has at least one u and at least one l and that $a(|o|)\leq 0$, we may choose a base point for o such that $a(|o|)$ is the minimum value of a and $a(1)>a(0)=0$. Fix such a base point, denoted (i_0, j_0), for the rest of the argument.

As before, choose

$$0=\ell_0<\ell^0<\ell_1<\ell^1\cdots<\ell^{k-1}<\ell_k=|o|$$

such that a is nondecreasing on $\{\ell_\lambda,\dots,\ell^\lambda\}$ and nonincreasing on $\{\ell^\lambda,\dots,\ell_{\lambda+1}\}$ for $0\leq\lambda\leq k-1$. Let

$$\beta_\lambda=\alpha_{p^{\ell_\lambda}(i_0,j_0)}\quad 0\leq\lambda\leq k.$$

Then as before, the coefficients $\alpha_{i,j}$ satisfy equations (8.3.1) and (8.3.2) if and only if the β_λ satisfy (8.3.3).

The same dévissage as before shows that it suffices to estimate the order of $H^o_{n,\nu}$ in the case where $n=ht(o)$. We make the circular system (8.3.3) triangular as follows: Choose λ so that $a(\ell^\lambda)$ is the maximum of a. Then

$$ht(o)=a(\ell^\lambda)-a(|o|)=e_{2k}-e_{2k-1}+\cdots+e_{2\lambda+2}.$$

Therefore,

$$\begin{aligned}0=p^{ht(o)}\beta_k&=p^{e_{2k}-e_{2k-1}+\cdots+e_{2\lambda+2}}\beta_k\\&=p^{e_{2k-2}-e_{2k-3}+\cdots+e_{2\lambda+2}}\gamma_k^{-1}\sigma^{\ell_k-\ell_{k-1}}(\beta_{k-1})\\&\;\;\vdots\\&=p^{e_{2\lambda+2}}\gamma_k^{-1}\sigma^{\ell_k-\ell_{k-1}}(\gamma_{k-1}^{-1})\sigma^{\ell_k-\ell_{k-2}}(\gamma_{k-2}^{-1})\cdots\sigma^{\ell_k-\ell_{\lambda+1}}(\beta_{\lambda+1}).\end{aligned}$$

It follows that $p^{e_{2\lambda+2}}\beta_{\lambda+1}=0$. Using this in (8.3.3) and reordering, we obtain (up to units and powers of σ) an upper-triangular system whose diagonal entries are $p^{e_1}, p^{e_3},\dots,p^{e_{2k-1}}$.

It follows that the number of solutions to (8.3.3) with coefficients in $W_{n,\nu}$ (with $n=ht(o)$) is $q^{\nu(e_1+\cdots+e_{2k-1})}$. Observing that $a(|o|)\leq 0$ implies that $d(o)=e_1+\cdots+e_{2k-1}$, we find that $|H^o_{ht(o),\nu}|=q^{\nu d(o)}$

and that

$$\lim_{\nu\to\infty}\frac{\log|H^o_{n,\nu}|}{\log(q^\nu)}=d(o)$$

for any $n\geq ht(o)$. This completes the proof of part (3) of the theorem in the remaining case when $a(|o|)\leq 0$. □

9. Equidistribution

We record three equidistribution statements to be used to control the average behavior of the invariant $d(o)$ from the preceding section. The first is a consequence of what is proven in [Griffon 2018, Theorem 4.1]. The second is a straightforward "two-variable" generalization, and the third is a simple corollary of the first. We omit the proofs since they are orthogonal to our main concerns.

Proposition 9.1 (Helfgott, Hindry–Pacheco, Griffon). *Let $A\subset[0,1]$ be an interval of length α. Let p be a prime number and let d run through positive integers prime to p. Let $\langle p\rangle$ act on $\mathbb{Z}/d\mathbb{Z}$ by multiplication, and let O be the set of orbits. Then*

$$\lim_{d\to\infty}\frac{1}{d}\sum_{o\in O}\left|\frac{|\{a\in o\mid\langle a/d\rangle\in A\}|}{|o|}-\alpha\right|=0.$$

Proposition 9.2. *Let p be a prime number, let r be a fixed integer prime to p and let d run through integers prime to p. Let $\langle p\rangle$ act on $(\mathbb{Z}/r\mathbb{Z})\times(\mathbb{Z}/d\mathbb{Z})$ diagonally, and let O be the set of orbits. Then*

$$\lim_{d\to\infty}\frac{1}{d}\sum_{o\in O}\left|\frac{|\{(a,b)\in o\mid\langle a/r\rangle+\langle b/d\rangle<1\}|}{|o|}-\frac{1}{2}\right|=0.$$

Proposition 9.3. *Let p be a prime number, let $I=\mathbb{Z}/d\mathbb{Z}$ with d prime to p equipped with the multiplication action of $\langle p\rangle$, and let $J=\{0,1\}$ be a two-element set equipped with the nontrivial action of $\langle p\rangle$. Let $\langle p\rangle$ act on $I\times J$ diagonally, and let O be the set of orbits. Then*

$$\lim_{d\to\infty}\frac{1}{d}\sum_{o\in O}\left|\frac{|\{(a,b)\in o\mid\langle a/d\rangle<1/2,b=0\}|+|\{(a,b)\in o\mid\langle a/d\rangle>1/2,b=1\}|}{|o|}-\frac{1}{2}\right|=0.$$

10. Calculations for curves defined by four monomials

In this section we compute the limit of Brauer–Siegel ratios for a family of elliptic curves related to the constructions in [Shioda 1986; Ulmer 2002]. We then explain how the same can be done for families of Jacobians of every genus in every positive characteristic.

Throughout, let $k=\mathbb{F}_q$, the finite field of cardinality q and characteristic p, and let $K=k(t)$, the rational function field over k.

10.1. ***The curve of [Ulmer 2002].*** Let p be a prime number, let d be a positive integer prime to p, and let E_d be the elliptic curve over K defined by

$$y^2+xy=x^3-t^d \tag{10.1.1}$$

This family of curves was introduced in [Ulmer 2002] where it was shown that $\text{Ш}(E_d)$ is finite and the rank of $E_d(K)$ is unbounded as d varies. Hindry and Pacheco [2016] computed the Brauer–Siegel ratio of E_d as $d \to \infty$ by analytic means, i.e., by a careful study of the L-function of E_d. Here we compute it via algebraic means, more precisely, through a consideration of $\dim \text{Ш}(E_d)$.

Theorem 10.2. *We have*

$$\lim_{d\to\infty} \mathrm{BS}(E_d) = 1.$$

Proof. Because $E_{pd} = E_d^{(p)}$, Theorem 5.1 implies that it will suffice to compute the limit as d runs through positive integers relatively prime to p and tending to infinity.

We are going to bound $\mathrm{BS}(E_d)$ from below by estimating $\dim \text{Ш}(E_d)$. Since the latter is invariant under extension of the ground field, we are free to extend k as needed and will do so in the geometric argument below.

Let $\mathcal{E}_d$ be the smooth projective surface equipped with a relatively minimal morphism $\pi : \mathcal{E}_d \to \mathbb{P}^1$ whose generic fiber is E_d. The procedure for constructing a model $\mathcal{E}_d$ is explained in general in [Ulmer 2011, Lecture 3], and this particular example is carried out in detail in [Ulmer 2002, §3]. The important thing to know about $\mathcal{E}_d$ is that it is birational to the hypersurface in $\mathbb{A}^3_{(x,y,t)}$ defined by (10.1.1).

Using the method of [Shioda 1986], it is proven in [Ulmer 2002, §4] that $\mathcal{E}_d$ is birational to the quotient of the Fermat surface of degree d by a group of order d^2. It is proven in [Shioda and Katsura 1979] that the Fermat surface of degree d is birational to the quotient of the product of two Fermat curves of degree d by a group of order d. (Here we may need to extend k so that it contains the $2d$-th roots of unity.) Putting these together, we find that $\mathcal{E}_d$ is birational to the quotient of $F_d \times F_d$ by the group

$$\Delta \subset (\mu_d^3/\mu_d)^2 \subset \mathrm{Aut}(F_d) \times \mathrm{Aut}(F_d)$$

generated by

$$([\zeta^2, \zeta, 1], [1, 1, 1]),\ ([1, \zeta, 1], [\zeta^3, 1, 1]),\ \text{ and } ([1, 1, \zeta], [1, 1, \zeta])$$

where ζ is a primitive d-th root of unity in k.

It follows from Corollary 6.5 that

$$\dim \text{Ш}(E_d) = \dim \mathrm{Hom}_A(H^1(F_d)/p^n, H^1(F_d)/p^n)^{\Delta} \tag{10.2.1}$$

for all sufficiently large n. Section 7 and Proposition 7.1 describe the cohomology group $H^1(F_d)$ with its action of Frobenius. They show in particular that the dimension in the last display can be computed by the methods of Section 8.

To spell this out, recall that the cohomology of F_d splits into lines indexed by

$$A' = \left\{ (a_0, a_1, a_2) \mid a_i \neq 0, \sum a_i = 0 \right\} \subset (\mathbb{Z}/d\mathbb{Z})^3$$

and that A' is the disjoint union of A_0 and A_1 as in Section 7. The curves F_d and their cohomology furnish data $M = N = H^1_{crys}(F_d/W(k))$, $I = J = A'$, and (c_i, d_j) as in Section 8.1.

A short calculation reveals that the basis elements φ_{ij} which contribute to the right hand side of (10.2.1) are those indexed by (i, j) of the form

$$(i, j) = (a_0, a_1, a_2, b_0, b_1, b_2) = b_1(-3, 6, -3, 2, 1, -3)$$

where $b_1 \in d\mathbb{Z}$ is such that $6b_1 \neq 0$. In other words, projection to the b_1 coordinate allows us to identify the orbits of $\langle p\rangle$ on $I \times J$ which contribute to (10.2.1) with the orbits of $\langle p\rangle$ on

$$B = \{b \in \mathbb{Z}/d\mathbb{Z} \mid 6b \neq 0\}.$$

Under this identification, $(i, j) \in I_0 \times J_1$ if and only if

$$0 < \left\langle \frac{b}{d} \right\rangle < \frac{1}{6}$$

and $(i, j) \in I_1 \times J_0$ if and only if

$$\frac{5}{6} < \left\langle \frac{b}{d} \right\rangle < 1$$

where $\langle\cdot\rangle$ denotes the fractional part. Thus, the invariant $d(o)$ of Section 8.1 becomes the following invariant of orbits of $\langle p\rangle$ on B: Setting

$$B_0 = \left\{ b \in \mathbb{Z}/d\mathbb{Z} \mid 0 < \left\langle \frac{b}{d} \right\rangle < \frac{1}{6} \right\} \quad \text{and} \quad B_1 = \left\{ b \in \mathbb{Z}/d\mathbb{Z} \mid \frac{5}{6} < \left\langle \frac{b}{d} \right\rangle < 1 \right\},$$

we have

$$d(o) = \min(|o \cap B_0|, |o \cap B_1|).$$

Finally, the equidistribution result Proposition 9.1 yields that

$$\sum_{o \in O} d(o) = \tfrac{d}{6} + \epsilon$$

where $\epsilon/d \to 0$ as $d \to \infty$, and so

$$\dim Ш(E_d) = \tfrac{d}{6} + \epsilon.$$

It follows from [Ulmer 2002, §2] that $\deg \omega_{E_d} = \left\lceil \tfrac{d}{6} \right\rceil$, so by applying Corollary 4.7, we conclude that

$$\liminf_{d \to \infty} \mathrm{BS}(E_d) \geq 1.$$

Taking into account the upper bound (1.1) of Hindry and Pacheco, we finally conclude that

$$\lim_{d \to \infty} \mathrm{BS}(E_d) = 1. \qquad \square$$

10.3. ***Other elliptic curves.*** The methods employed in the previous subsection can be used to compute the limiting Brauer–Siegel ratio for several other families of elliptic curves, namely those defined by equations involving 4 monomials. This includes the Hessian family studied in [Griffon 2016, Chapter 5] and a closely related family introduced by Davis and Occhipinti [2016] and studied in [Griffon 2016, Chapter 7]. We will not give the details here, since no fundamentally new phenomena arise.

10.4. ***Higher genus Jacobians.*** For every prime p and every $g > 0$, there is a sequence of curves of genus g over $\mathbb{F}_p(t)$ whose Jacobians are absolutely simple, satisfy the Birch and Swinnerton-Dyer conjecture, and have unbounded analytic and algebraic ranks; see [Ulmer 2007, §7]. Since these curves are defined by four monomials, the methods of this paper suffice to compute the limit of their Brauer–Siegel ratios. In the rest of this subsection, we explain the details for the main case, namely when g is a positive integer and p is a prime such that $p \nmid (2g+2)(2g+1)$. The other cases are similar and we omit them in the interest of brevity.

Fix a positive integer g, a prime p such that $p \nmid (2g+2)(2g+1)$, and a positive integer d. Let X_d be the smooth, proper curve of genus g over $K = \mathbb{F}_p(t)$ defined by

$$y^2 = x^{2g+2} + x^{2g+1} + t^d \tag{10.4.1}$$

and let J_d be its Jacobian.

Theorem 10.5. $$\lim_{d\to\infty} \mathrm{BS}(J_d) = 1.$$

Proof. Once again, it suffices to restrict to d not divisible by p. We will bound $\mathrm{BS}(J_d)$ from below by estimating $\dim Ш(J_d)$ using that X_d has a model which is dominated by a product of Fermat curves. As usual, we are free to expand the ground field $\mathbb{F}_p$ and we do so as needed below.

Let $\mathcal{X}_d$ be the smooth projective surface equipped with a relatively minimal morphism $\pi : \mathcal{X}_d \to \mathbb{P}^1$ with generic fiber X_d. Again, what is most important is that $\mathcal{X}_d$ is birational to the hypersurface in $\mathbb{A}^3$ defined by (10.4.1).

Using the method of [Shioda 1986] (see also [Ulmer 2007]), one sees that $\mathcal{X}_d$ is birational to the quotient of the Fermat surface of degree $2d$ by a group of order $(2d)^2$, and therefore birational to the quotient of $F_{2d} \times F_{2d}$ by a group of order $(2d)^3$. (Here we enlarge $\mathbb{F}_p$ to a finite extension k that contains the $2d$-th roots of unity.) More precisely, carrying out the procedure of [Ulmer 2007, §6] and using [Shioda and Katsura 1979], one finds that $\mathcal{X}_d$ is birational to the quotient of $F_{2d} \times F_{2d}$ by the group

$$\Delta \subset (\mu_{2d}^3/\mu_{2d})^2 \subset \mathrm{Aut}(F_{2d}) \times \mathrm{Aut}(F_{2d})$$

generated by

$$([\zeta^2, 1, 1], [1, 1, 1]), \quad ([1, 1, 1], [1, \zeta^d, 1]), \quad ([1, 1, 1], [\zeta, \zeta^{2g+2}, 1]), \quad \text{and} \quad ([1, 1, \zeta], [1, 1, \zeta])$$

where ζ is a primitive $2d$-th root of unity in k.

It follows from Corollary 6.5 that

$$\dim Ш(E_d) = \dim \mathrm{Hom}_A(H^1(F_d)/p^n, H^1(F_d)/p^n)^\Delta \tag{10.5.1}$$

for all sufficiently large n.

As in the previous subsections, the curves F_{2d} and their cohomology furnish data $M = N = H^1_{crys}(F_{2d}/W(k))$, $I = J = A'$, and (c_i, d_j) as in Section 8.1.

A short calculation reveals that the basis elements φ_{ij} which contribute to the right hand side of (10.5.1) are those indexed by (i, j) of the form

$$(i, j) = (a_0, a_1, a_2, b_0, b_1, b_2) = (-(4g+4)b, 2b, (4g+2)b, d, d-(4g+2)b, (4g+2)b)$$

where $b \in \mathbb{Z}/d\mathbb{Z}$ is such that none of the coordinates $a_0, \ldots, b_2$ are zero in $\mathbb{Z}/2d\mathbb{Z}$. (Note that all of the coefficients of b above are even, so the display gives a well-defined element of $(\mathbb{Z}/2d\mathbb{Z})^6$ even though b lies in $\mathbb{Z}/d\mathbb{Z}$.) Thus the relevant orbits of $\langle p\rangle$ on $I \times J$ can be identified with the orbits of $\langle p\rangle$ on the subset B of $\mathbb{Z}/d\mathbb{Z}$ where none of the coordinates of (i, j) is 0.

Next we work out conditions on b for the corresponding (i, j) to lie in $I_0 \times J_1$ or $I_1 \times J_0$. One finds that

$$i = (a_0, a_1, a_2) = (-(4g+4)b, 2b, (4g+2)b)$$

lies in I_0 if and only if the fractional part $\langle b/d\rangle$ lies in one of the intervals

$$\left(\frac{k+1}{2g+2}, \frac{k+1}{2g+1}\right), \quad k = 0, \ldots, 2g$$

and i lies in I_1 if and only if the fractional part $\langle b/d\rangle$ lies in one of the intervals

$$\left(\frac{k}{2g+1}, \frac{k+1}{2g+2}\right), \quad k = 0, \ldots, 2g.$$

On the other hand,

$$j = (b_0, b_1, b_2) = (d, d-(4g+2)b, (4g+2)b)$$

lies in J_0 if and only if the fractional part $\langle b/d\rangle$ lies in one of the intervals

$$\left(\frac{2\ell+1}{4g+2}, \frac{2\ell+2}{4g+2}\right), \quad \ell = 0, \ldots, 2g$$

and j lies in J_1 if and only if the fractional part $\langle b/d\rangle$ lies in one of the intervals

$$\left(\frac{2\ell}{4g+2}, \frac{2\ell+1}{4g+2}\right), \quad \ell = 0, \ldots, 2g.$$

It follows that (i, j) lies in $I_0 \times J_1$ if and only if

$$\left\langle\frac{b}{d}\right\rangle \in \left(\frac{k+1}{2g+2}, \frac{2k+1}{4g+2}\right)$$

with $k = g+1, \ldots, 2g$ and it lies in $I_1 \times J_0$ if and only if

$$\left\langle\frac{b}{d}\right\rangle \in \left(\frac{2k+1}{4g+2}, \frac{k+1}{2g+2}\right)$$

with $k = 0, \ldots, g-1$.

The total length of the intervals corresponding to $I_0 \times J_1$ is

$$\sum_{k=g+1}^{2g}\left(\frac{2k+1}{4g+2}-\frac{k+1}{2g+2}\right)=\frac{g}{8g+4}$$

and the total length of the intervals corresponding to $I_1 \times J_0$ is

$$\sum_{k=0}^{g-1}\left(\frac{k+1}{2g+2}-\frac{2k+1}{4g+2}\right)=\frac{g}{8g+4}.$$

Transferring the definition of $d(o)$ to B and applying the equidistribution result Proposition 9.1, we find that

$$\dim Ш(J_d)=\sum_o d(o)=\frac{dg}{8g+4}+\epsilon$$

where $\epsilon/d \to 0$ as $d \to \infty$.

We pause briefly to consider the case $g = 1$. By [Weil 1954], the Jacobian of X_d is the elliptic curve

$$y^2 = x^3 - 4t^d x + t^d.$$

It is easy to see that the bundle ω_d attached to J_d has degree $\lceil \frac{d}{12} \rceil$. It then follows from our estimation of $\dim Ш(J_d)$ and Corollary 4.7 that $\liminf_{d\to\infty} \mathrm{BS}(J_d) \geq 1$ and thus, by the Hindry–Pacheco upper bound (1.1), that $\lim_{d\to\infty} \mathrm{BS}(J_d) = 1$.

To extend this to higher genus, we will give an upper bound on the degree of ω_d of the form $dg/(8g+4)+\epsilon$ where $\epsilon/d \to 0$ as $d \to \infty$. More precisely, we will show that $\deg(\omega_d) = dg/(8g+4)$ for all d divisible by $(2g+1)(2g+2)$. For a general d, we let

$$d' = \mathrm{lcm}(d, (2g+1)(2g+2))$$

and apply Lemma 2.7.1 to conclude that

$$\deg(\omega_d) \leq \frac{dg}{(8g+4)} + 2g((2g+1)(2g+2)-1)$$

which gives the desired estimate.

For $i = 1, \ldots, g$, let ω_i be the 1-form $x^{i-1}dx/y$ on X_d over K. These 1-forms are regular and give a basis of $H^0(X, \Omega^1_{X/K})$. We will consider their extensions to a suitable model $\pi : \mathcal{X} \to \mathbb{P}^1$ of X and use them to compute $\deg(\omega_d)$.

In [Ulmer 2007, §7.7], a model of X over $U = \mathbb{P}^1 \setminus \{0, \infty\}$ is constructed which is regular and a Lefschetz pencil, i.e., its singular fibers are irreducible with one ordinary node each. It is easy to see that the differentials ω_i extend to this model and

$$\sigma := \omega_1 \wedge \cdots \wedge \omega_g$$

defines a nowhere vanishing section of ω_d over U. To compute $\deg(\omega_d)$ it will thus suffice to compute the order of vanishing of σ at $t=0$ and $t=\infty$. This is where we use the hypothesis that d is a multiple of $(2g+1)(2g+2)$.

Indeed, if $d=2(2g+1)k$, then the change of coordinates $x\to t^{2k}x'$, $y\to t^{(2g+1)k}y'$ brings X into the form

$$y'^2=t^{2k}x'^{2g+2}+x'^{2g+1}+1$$

which has good reduction at $t=0$. Moreover, we see that $\omega_i=t^{(2i-2g-1)k}\omega_i'$ where $\omega_i'=(x'^{i-1}dx')/y'$, and that the ω_i' have linearly independent reductions at $t=0$. This shows that σ has a pole at $t=0$ of order

$$\sum_{i=1}^{g}\frac{(2g+1-2i)d}{2(2g+1)}.$$

Similarly, when $d=(2g+2)\ell$, the change of coordinates $x\to t^{2\ell}x$, $y\to t^{(2g+2)\ell}y$ brings X into the form

$$y^2=x^{2g+2}+t^{-\ell}x^{2g+1}+1,$$

which has good reduction at $t=\infty$. Moreover, we see that $\omega_i=t^{(i-g-1)\ell}\omega_i'$ where $\omega_i'=(x'^{i-1}dx')/y'$, and that the ω_i' have linearly independent reductions at $t=\infty$. This shows that σ has a zero at $t=\infty$ of order

$$\sum_{i=1}^{g}\frac{(g+1-i)d}{2g+2}.$$

A short computation then shows that $\deg(\omega_d)$ is $dg/(8g+4)$.

Note that these calculations also show that J_d has good reduction at $t=0$ and $t=\infty$ when d is divisible by $(2g+1)(2g+2)$. Using Section 2.6, these reduction results imply that $\tau(J_d)=O(H(J_d)^\epsilon)$ for all $\epsilon>0$. Then Proposition 4.6 shows that

$$\liminf_{d\to\infty}\mathrm{BS}(J_d)\geq\liminf_{d\to\infty}\frac{\dim(\text{Ш}(J_d))}{\deg(\omega_{J_d})}\geq 1.$$

Taking into account the upper bound (1.1) of Hindry and Pacheco, we finally conclude that

$$\lim_{d\to\infty}\mathrm{BS}(J_d)=1. \qquad \square$$

11. Calculations for Jacobians related to Berger's construction

In this section we compute the limiting Brauer–Siegel ratio for some families of curves related to the construction in [Berger 2008; Ulmer 2013].

Throughout, let $k=\mathbb{F}_q$, the finite field of cardinality q and characteristic p, and let $K=k(t)$, the rational function field over k.

11.1. ***The Legendre curve.*** Assume that $p > 2$, let d be a positive integer, and let E_d be the elliptic curve over K defined by

$$y^2 = x(x+1)(x+t^d). \tag{11.1.1}$$

This family of curves has been studied extensively, in particular in [Ulmer 2014b; Conceição et al. 2014; Ulmer 2014c; Griffon 2016, Chapter 4]. In the latter, the limit of the Brauer–Siegel ratio of E_d as $d \to \infty$ was computed by analytic means, i.e., by a careful study of the L-function of E_d. Here we compute it via algebraic means, more precisely, through a consideration of $\dim Ш(E_d)$.

Theorem 11.2. *We have*

$$\lim_{d\to\infty} \mathrm{BS}(E_d) = 1.$$

Proof. As usual, it suffices to consider values of d not divisible by p.

Let $\mathcal{E}_d$ be the smooth projective surface equipped with a relatively minimal morphism $\pi : \mathcal{E}_d \to \mathbb{P}^1$ whose generic fiber is E_d. This is constructed in [Ulmer 2014b] (under the simplifying hypothesis that d is even, but the odd case is similar). The main thing we need to know about $\mathcal{E}_d$ is that it is birational to the hypersurface in $\mathbb{A}^3_{(x,y,t)}$ defined by the (11.1.1).

Let $\mathcal{C}_d$ be the curve with affine equation

$$x^2 = z^d + 1$$

and let $\mathcal{D}_d$ be the curve with affine equation

$$y^2 = w^d + 1.$$

Both curves admit an evident action of $\Delta = \mu_2 \times \mu_d$ (over $\bar{k}$). Let Δ act "antidiagonally" on $\mathcal{C}_d \times \mathcal{D}_d$:

$$(\zeta_2, \zeta_d)(x, z, y, w) = (\zeta_2 x, \zeta_d z, \zeta_2^{-1} y, \zeta_d^{-1} w).$$

Our first main claim is that $\mathcal{E}_d$ is birational to the quotient $\mathcal{C}_d \times \mathcal{D}_d/\Delta$ via the map

$$(x, z, y, w) \mapsto (x = z^d, y = z^d xy, t = wz).$$

Indeed, it is evident that this defines a dominant rational map from $\mathcal{C}_d \times \mathcal{D}_d$ to $\mathcal{E}_d$ which factors through the quotient by Δ. Degree considerations then show that the induced map has degree 1, i.e., it is a birational isomorphism.

We are thus in position to apply the machinery of Section 6. In particular, it follows from Corollary 6.5 that

$$\dim Ш(E_d) = \dim \mathrm{Hom}_A(H^1(\mathcal{C}_d)/p^n, H^1(\mathcal{D}_d)/p^n)^{\Delta} \tag{11.2.1}$$

for all sufficiently large n. Section 7.3 and Proposition 7.1 describe the cohomology groups $H^1(\mathcal{C}_d)$ and $H^1(\mathcal{D}_d)$ with their actions of Frobenius. They show in particular, that the dimension in the last display can be computed by the methods of Section 8.

To spell this out, let

$$I = J = \mathbb{Z}/d\mathbb{Z} \setminus \{0, d/2 \text{ (if } d \text{ is even)}\},$$

decomposed as $I_0 = J_0 = \{i \mid d/2 < i < d\}$ and $I_1 = J_1 = \{i \mid 0 < i < d/2\}$. Section 7 shows that the crystalline cohomology groups $H^1(\mathcal{C}_d)$ and $H^1(\mathcal{D}_d)$ with their action of Frobenius furnish data (M, N, I, J, c_i, d_j) as in Section 8.1, as well as the invariant $d(o)$ for each orbit o of $\langle p\rangle$ on $I \times J$.

Since Δ acts antidiagonally, the orbits that contribute to the right hand side of (11.2.1) are those whose elements (i, j) satisfy $j = -i$. Write O^Δ for the set of such orbits. Applying Theorem 8.3, we conclude that

$$\dim Ш(E_d) = \sum_{o \in O^\Delta} d(o). \tag{11.2.2}$$

We may identify the orbits in O^Δ with the orbits of $\langle p\rangle$ on I via the projection $\pi_I : I \times J \to I$. Also, since $(i, -i) \in I_0 \times J_1$ if and only if $i \in I_0$, and $(i, -i) \in I_1 \times J_0$ if and only if $i \in I_1$, we have

$$d(o) = \min(|\pi_I(o) \cap I_0|, |\pi_I(o) \cap I_1|).$$

Thus the sum on the right hand side of (11.2.2) becomes a sum over orbits of $\langle p\rangle$ on I, and the invariant $d(o)$ is described "on average" in Section 9. In particular, the equidistribution result Proposition 9.1 implies that

$$\dim Ш(E_d) = \sum_{o \in O^\Delta} d(o) = \tfrac{d}{2} + \epsilon_d$$

where $\epsilon_d/d \to 0$ as $d \to \infty$.

Since $\deg(\omega_{E_d}) = \lceil \frac{d}{2} \rceil$ (e.g., by [Ulmer 2014b, Lemma 7.1]), Corollary 4.7 implies that

$$\liminf_{d\to\infty} \mathrm{BS}(E_d) \geq \liminf_{d\to\infty} \frac{\dim Ш(E_d)}{\deg(\omega_{E_d})} = 1.$$

Taking into account the upper bound (1.1) of Hindry and Pacheco, we conclude that

$$\lim_{d\to\infty} \mathrm{BS}(J_d) = 1. \qquad \square$$

11.3. ***Other elliptic curves.*** The methods employed in the previous subsection can be used to compute the limiting Brauer–Siegel ratio for several other families of elliptic curves, namely those coming from Berger's construction where the dominating curves are related to Fermat curves. This is the case in particular for the universal curve over $X_1(4)$ studied in [Griffon 2016, Chapter 6] and the curve "$B_{1/2,d}$" introduced in [Berger 2008, §4] and studied in [Griffon 2016, Chapter 8]. We will not give the details here, since no fundamentally new phenomena arise.

11.4. ***Higher dimensional Jacobians.*** Let p be a prime number, let q be a power of p, and let $k = \mathbb{F}_q$. Let r and d be integers relatively prime to p. Let $X = X_{r,d}$ be the smooth projective curve over $K = k(t)$ associated to the equation

$$y^r = x^{r-1}(x+1)(x+t^d). \tag{11.4.1}$$

This is a curve of genus $r-1$, and the case $r=2$ is the Legendre curve of Section 11.1. Let $J=J_{r,d}$ be the Jacobian of X. This family of Jacobians was studied in [Berger et al. 2015], where among other things it was proven that $Ш(J_{r,d})$ is finite for all p, q, r, and d as above. Here we will compute the limiting Brauer–Siegel ratio for fixed q and r as $d\to\infty$.

Theorem 11.5. *For all q and r as above*,

$$\lim_{\substack{d\to\infty\\(p,d)=1}} \mathrm{BS}(J_{r,d})=1.$$

Here the limit is through integers prime to p. It would be possible to include those d divisible by p using a straightforward generalization of the ideas in Section 5, but will not do that here.

Proof. Since r will be fixed throughout, we omit it from the notation. Let $\mathcal{X}_d$ be the smooth projective surface equipped with a relatively minimal morphism $\pi:\mathcal{X}_d\to\mathbb{P}^1$ whose generic fiber is X_d. This is constructed in [Berger et al. 2015, §3.1]. The important thing to know about $\mathcal{X}_d$ is that it is birational to the hypersurface in $\mathbb{A}^3_{(x,y,t)}$ defined by (11.4.1).

Let $\mathcal{C}_d$ be the curve with affine equation

$$x^r=z^d+1$$

and let $\mathcal{D}_d$ be the curve with affine equation

$$y^r=w^d+1.$$

Both curves admit an evident action of $\Delta=\mu_r\times\mu_d$ (over $\bar{k}$). Let Δ act "antidiagonally" on $\mathcal{C}_d\times\mathcal{D}_d$:

$$(\zeta_r,\zeta_d)(x,z,y,w)=(\zeta_r x,\zeta_d z,\zeta_r^{-1}y,\zeta_d^{-1}w).$$

It is proven in [Berger et al. 2015, §3.3] that $\mathcal{X}_d$ is birational to the quotient $\mathcal{C}_d\times\mathcal{D}_d/\Delta$ via the map

$$(x,z,y,w)\mapsto(x=z^d,\ y=z^d xy,\ t=wz).$$

We are thus in position to apply the machinery of Section 6. In particular, it follows from Corollary 6.5 that

$$\dim Ш(J_d)=\dim \mathrm{Hom}_A(H^1(\mathcal{C}_d)/p^n,H^1(\mathcal{D}_d)/p^n)^{\Delta} \tag{11.5.1}$$

for all sufficiently large n. Section 7.3 and Proposition 7.1 describe the cohomology groups $H^1(\mathcal{C}_d)$ and $H^1(\mathcal{D}_d)$ with their actions of Frobenius. They show in particular, that the dimension in the last display can be computed by the methods of Section 8.

To spell this out, let

$$I = J = \left\{(a,b) \in \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} \mid a \neq 0, b \neq 0, \left\langle \frac{a}{r} \right\rangle + \left\langle \frac{b}{d} \right\rangle \neq 1\right\},$$
$$I_0 = J_0 = \left\{(a,b) \in \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} \mid a \neq 0, b \neq 0, \left\langle \frac{a}{r} \right\rangle + \left\langle \frac{b}{d} \right\rangle > 1\right\}, \quad \text{and}$$
$$I_1 = J_1 = \left\{(a,b) \in \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} \mid a \neq 0, b \neq 0, \left\langle \frac{a}{r} \right\rangle + \left\langle \frac{b}{d} \right\rangle < 1\right\}.$$

Section 7 shows that the crystalline cohomology groups $H^1(\mathcal{C}_d)$ and $H^1(\mathcal{D}_d)$ with their action of Frobenius furnish data (M, N, I, J, c_i, d_j) as in Section 8.1, as well as the invariant $d(o)$ for each orbit o of $\langle p \rangle$ on $I \times J$.

Since Δ acts antidiagonally, the orbits that contribute to the right hand side of (11.5.1) are those whose elements $(i, j) = (a, b, a', b')$ satisfy $j = -i$, i.e., $a' = -a$ and $b' = -b$. Write O^Δ for the set of such orbits. Applying Theorem 8.3, we conclude that

$$\dim Ш(J_d) = \sum_{o \in O^\Delta} d(o). \tag{11.5.2}$$

We may identify the orbits in O^Δ with the orbits of $\langle p \rangle$ on I via the projection $\pi_I : I \times J \to I$. Also, since $(i, -i) \in I_0 \times J_1$ if and only if $i \in I_0$, and $(i, -i) \in I_1 \times J_0$ if and only if $i \in I_1$, we have

$$d(o) = \min(|\pi_I(o) \cap I_0|, |\pi_I(o) \cap I_1|).$$

We note that

$$|I_0| = |I_1| = \tfrac{1}{2}((r-1)(d-1) - (\gcd(r,d) - 1)),$$

which for fixed r is asymptotic to $d(r-1)/2$ as $d \to \infty$.

Thus the sum on the right hand side of (11.5.2) becomes a sum over orbits of $\langle p \rangle$ on I, and the invariant $d(o)$ is described "on average" in Section 9. In particular, the equidistribution result Proposition 9.2 implies that

$$\dim Ш(J_d) = \sum_{o \in O^\Delta} d(o) = \tfrac{1}{2} d(r-1) + \epsilon_d$$

where $\epsilon_d/d \to 0$ as $d \to \infty$.

To finish the proof, we will show that $\tau(J_d) = O(H(J_d)^\epsilon)$ for all $\epsilon > 0$ and that $\deg(\omega_{J_d}) \leq d(r-1)/2 + \epsilon_d$ where $\epsilon_d/d \to 0$ as $d \to \infty$. Once these claims are established, Proposition 4.6 implies that

$$\liminf_{d \to \infty} \mathrm{BS}(J_d) \geq \liminf_{d \to \infty} \frac{\dim Ш(J_d)}{\deg(\omega_{J_d})} \geq 1.$$

Taking into account the upper bound (1.1) of Hindry and Pacheco, we conclude that

$$\lim_{d \to \infty} \mathrm{BS}(J_d) = 1.$$

The assertion about $\tau(J_d)$ follows from the discussion of Section 2.6 and the fact (proven in [Berger et al. 2015, §3.1]) that X_d has semistable reduction at $t=0$ and $t=\infty$ whenever r divides d.

It is proven in [Berger et al. 2015, Proof of Proposition 7.5] that when r divides d, we have $\deg(\omega_{J_d}) = d(r-1)/2$. In general, if $d' = \operatorname{lcm}(d,r)$, we have $\deg(\omega_{J_{d'}}) = d'(r-1)/2$ and Lemma 2.7.1 shows that

$$\deg(\omega_{J_d}) \le \frac{d(r-1)}{2} + \frac{2(r-1)^2}{d'/d} = \frac{d(r-1)}{2} + \epsilon_d.$$

Since d'/d is an integer, ϵ_d is bounded independently of d, so $\epsilon_d/d \to 0$ as $d \to \infty$.

This completes the proof of the theorem. $\square$

12. Quadratic twists of constant curves

We conclude the paper with a study of Brauer–Siegel ratios of quadratic twists of constant elliptic curves. Throughout we let p be an odd prime number, $\mathbb{F}_q$ a finite field of characteristic p, and $K = \mathbb{F}_q(t)$.

12.1. ***Twists of a constant supersingular curve.*** Fix a supersingular elliptic curve E_0 over $\mathbb{F}_q$ and let $E = E_0 \times_{\mathbb{F}_q} K$. For a positive integer d relatively prime to p, let E_d be the twist of E by the quadratic extension $\mathbb{F}_q(t, \sqrt{t^d+1})$ of K. By results of Milne, the Tate–Shafarevich group of E_d is finite.

Theorem 12.2. *We have*

$$\lim_{\substack{d\to\infty \\ (p,d)=1}} \mathrm{BS}(E_d) = 1.$$

Proof. Let $\mathcal{E}_d \to \mathbb{P}^1$ be the Néron model of E_d/K, and let $\mathcal{C}_d$ be the smooth projective curve over $\mathbb{F}_q$ defined by $y^2 = x^d + 1$ and equipped with the action of μ_2 given by the hyperelliptic involution. It is easy to see that $\mathcal{E}_d$ is birational to the quotient of $\mathcal{C}_d \times_{\mathbb{F}_q} E_0$ by the (anti) diagonal action of μ_2, i.e., by μ_2 acting via the hyperelliptic involution on both factors.

We are thus in position to apply the machinery of Section 6. In particular, it follows from Corollary 6.5 that

$$\dim \text{Ш}(E_d) = \dim \operatorname{Hom}_A(H^1(\mathcal{C}_d)/p^n, H^1(E_0)/p^n)^{\mu_2} \tag{12.2.1}$$

for all sufficiently large n.

Section 7.3 and Proposition 7.1 describe the cohomology group $H^1(\mathcal{C}_d)$. We recall the well-known description of $H^1(E_0)$: It is a free W-module of rank 2 with a basis e_0, e_1 such that $F(e_0) = d_0 e_1$ and $F(e_1) = d_1 e_0$ where d_0 is a unit of W and d_1 is p times a unit. (See [Dummigan 1995, §5] for a detailed account.) To harmonize with earlier notation, let $J_0 = \{0\}$, $J_1 = \{1\}$, and $J = J_0 \cup J_1$, and equip J with the nontrivial action of $\langle p \rangle$.

Also, let

$$I = \mathbb{Z}/d\mathbb{Z} \setminus \left\{0, \tfrac{d}{2} \text{ (if } d \text{ is even)}\right\},$$

decomposed as $I_0 = \left\{i \mid \frac{d}{2} < i < d\right\}$ and $I_1 = \left\{i \mid 0 < i < \frac{d}{2}\right\}$. Section 7 and the preceding paragraph show that the crystalline cohomology groups $H^1(\mathcal{C}_d)$ and $H^1(E_0)$ with their actions of Frobenius furnish data (M, N, I, J, c_i, d_j) as in Section 8.1, as well as the invariant $d(o)$ for each orbit o of $\langle p\rangle$ on $I \times J$. We may thus compute the dimension in the last display by the methods of Section 8.

Since $\mathcal{C}_d$ and E_0 are hyperelliptic, the μ_2-invariant part of their cohomology is trivial, so

$$\mathrm{Hom}_A(H^1(\mathcal{C}_d)/p^n, H^1(E_0)/p^n)^{\mu_2} = \mathrm{Hom}_A(H^1(\mathcal{C}_d)/p^n, H^1(E_0)/p^n).$$

Applying Theorem 8.3, we conclude that

$$\dim Ш(E_d) = \sum_{o\in O} d(o) \tag{12.2.2}$$

where the sum is over all orbits of $\langle p\rangle$ on $I \times J$.

The equidistribution result Proposition 9.3 implies that

$$\sum_{o\in O} d(o) = \tfrac{d}{2} + \epsilon_d$$

where $\epsilon_d/d \to 0$ as $d \to \infty$.

Since $t^d + 1$ has distinct roots, it is easy to see that $\deg(\omega_{E_d}) = \lceil \frac{d}{2} \rceil$. Thus Corollary 4.7 implies that

$$\liminf_{d\to\infty} \mathrm{BS}(E_d) \geq \liminf_{d\to\infty} \frac{\dim Ш(E_d)}{\deg(\omega_{E_d})} = 1.$$

Taking into account the upper bound (1.1) of Hindry and Pacheco, we conclude that

$$\lim_{d\to\infty} \mathrm{BS}(E_d) = 1. \qquad \square$$

12.3. ***Twists of an constant ordinary curve.*** Now let E_0 be an ordinary elliptic curve over $\mathbb{F}_q$ and set $E = E_0 \times_{\mathbb{F}_q} K$. One could use methods similar to those in the last section to compute $\dim Ш(E_d)$ for the twist of E by $\mathbb{F}_q(t, \sqrt{t^d+1})$, but much more is easily deduced from results of Katz in p-adic cohomology.

Theorem 12.4. *Let E' be any quadratic twist of E. Then*

$$\dim Ш(E') = 0.$$

Proof. A variety X over a finite field is said to be *Hodge–Witt* if all of its deRham–Witt cohomology groups $H^i(X, W\Omega^j_X)$ are finitely generated. A curve is automatically Hodge–Witt, and a surface which satisfies the Tate conjecture is Hodge–Witt if and only if the dimension of its Brauer group (in the sense of Proposition/Definition 4.1) is 0 [Milne 1975, §1]. In other words, a surface X over $\mathbb{F}_q$ satisfying the Tate conjecture is Hodge–Witt if and only if

$$\lim_{n\to\infty} \frac{\log|H^2(X \times_{\mathbb{F}_q} \mathbb{F}_{q^n}, \mathrm{G}_m)[p^\infty]|}{\log(q^n)} = 0.$$

A theorem of Katz [1983] says that a product of varieties is Hodge–Witt if and only if one of the factors is ordinary and the other is Hodge–Witt.

Now let $\mathcal{C} \to \mathbb{P}^1$ be a double cover corresponding to a quadratic extension K'/K. Then the Néron model $\mathcal{E}' \to \mathbb{P}^1$ of E'/K is birational to the quotient of $\mathcal{C} \times_{\mathbb{F}_q} E_0$ by μ_2 acting diagonally by the hyperelliptic involutions. Since $p > 2$, the Brauer group of the quotient is the μ_2-invariant part of the Brauer group of $\mathcal{C} \times_{\mathbb{F}_q} E_0$, and the latter has dimension 0 since E_0 is ordinary. It follows that the Brauer group of $\mathcal{E}'$ has dimension 0 and so $\text{Ш}(E')$ has dimension zero. $\square$

Thus for a quadratic twist of a constant, ordinary elliptic curve, our p-adic methods do not give a nontrivial lower bound on the Brauer–Siegel ratio. This is compatible with Conjecture 1.7 of [Hindry and Pacheco 2016], which predicts that the $\liminf$ of $\mathrm{BS}(E')$ as E' runs over all quadratic twists is 0.

We finish by remarking that Griffon [2015] has shown that if E_d is the twist of a constant ordinary E/K by the quadratic extension $\mathbb{F}_q(t, \sqrt{t^d+1})$, then as d runs through "supersingular" integers, i.e., those that divide p^f+1 for some f, the limit of $\mathrm{BS}(E_d)$ is 1. In conjunction with Theorem 12.4, this shows that the Brauer–Siegel ratio of an elliptic curve E' may be large even when the dimension of $\text{Ш}(E')$ is zero.

References

[Artin 1974] M. Artin, "Supersingular $K3$ surfaces", *Ann. Sci. École Norm. Sup.* (4) **7** (1974), 543–567. MR Zbl

[Berger 2008] L. Berger, "Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields", *J. Number Theory* **128**:12 (2008), 3013–3030. MR Zbl

[Berger et al. 2015] L. Berger, C. Hall, R. Pannekoek, J. Park, R. Pries, S. Sharif, A. Silverberg, and D. Ulmer, "Explicit arithmetic of Jacobians of generalized Legendre curves over global function fields", 2015. arXiv

[Bosch et al. 1990] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)] **21**, Springer, 1990. MR Zbl

[Brauer 1950] R. Brauer, "On the zeta-functions of algebraic number fields, II", *Amer. J. Math.* **72** (1950), 739–746. MR Zbl

[Conceição et al. 2014] R. P. Conceição, C. Hall, and D. Ulmer, "Explicit points on the Legendre curve II", *Math. Res. Lett.* **21**:2 (2014), 261–280. MR Zbl

[Conrad 2006] B. Conrad, "Chow's K/k-image and K/k-trace, and the Lang–Néron theorem", *Enseign. Math.* (2) **52**:1-2 (2006), 37–108. MR Zbl

[Cossec and Dolgachev 1989] F. R. Cossec and I. V. Dolgachev, *Enriques surfaces, I*, Progress in Mathematics **76**, Birkhäuser, Boston, 1989. MR Zbl

[Davis and Occhipinti 2016] C. Davis and T. Occhipinti, "Explicit points on $y^2+xy-t^dy=x^3$ and related character sums", *J. Number Theory* **168** (2016), 13–38. MR Zbl

[Dummigan 1995] N. Dummigan, "The determinants of certain Mordell–Weil lattices", *Amer. J. Math.* **117**:6 (1995), 1409–1429. MR Zbl

[Griffon 2015] R. Griffon, "Analogue of the Brauer–Siegel theorem for some families of elliptic curves over function fields", poster, 2015. Presented at the *Silvermania* conference at Brown University.

[Griffon 2016] R. Griffon, *Analogues du théorème de Brauer–Siegel pour quelques familles de courbes elliptiques*, Ph.D. thesis, Université Paris Diderot, 2016, Available at http://math.richardgriffon.me/thesis/Griffon_thesis.pdf.

[Griffon 2018] R. Griffon, "A Brauer–Siegel theorem for Fermat surfaces over finite fields", *J. Lond. Math. Soc.* (2) **97**:3 (2018), 523–549. MR Zbl

[Grothendieck 1968] A. Grothendieck, "Le groupe de Brauer, III: Exemples et compléments", pp. 88–188 in *Dix exposés sur la cohomologie des schémas*, Adv. Stud. Pure Math. **3**, North-Holland, Amsterdam, 1968. MR Zbl

[Halle and Nicaise 2010] L. H. Halle and J. Nicaise, "The Néron component series of an abelian variety", *Math. Ann.* **348**:3 (2010), 749–778. MR Zbl

[Hindry 2007] M. Hindry, "Why is it difficult to compute the Mordell–Weil group?", pp. 197–219 in *Diophantine geometry*, edited by U. Zannier, CRM Series **4**, Ed. Norm., Pisa, 2007. MR Zbl

[Hindry and Pacheco 2016] M. Hindry and A. Pacheco, "An analogue of the Brauer–Siegel theorem for abelian varieties in positive characteristic", *Mosc. Math. J.* **16**:1 (2016), 45–93. MR Zbl

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

[Kato and Trihan 2003] K. Kato and F. Trihan, "On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$", *Invent. Math.* **153**:3 (2003), 537–592. MR Zbl

[Katz 1983] N. M. Katz, "On the ubiquity of "pathology" in products", pp. 139–153 in *Arithmetic and geometry, I*, edited by M. Artin and J. Tate, Progr. Math. **35**, Birkhäuser, Boston, 1983. MR Zbl

[Koblitz 1984] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd ed., Graduate Texts in Mathematics **58**, Springer, 1984. MR Zbl

[Lang and Néron 1959] S. Lang and A. Néron, "Rational points of abelian varieties over function fields", *Amer. J. Math.* **81** (1959), 95–118. MR Zbl

[Milne 1975] J. S. Milne, "On a conjecture of Artin and Tate", *Ann. of Math.* (2) **102**:3 (1975), 517–533. MR Zbl

[Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press, 1980. MR Zbl

[Moret-Bailly 1985] L. Moret-Bailly, "Pinceaux de variétés abéliennes", *Astérisque* 129 (1985), 266. MR Zbl

[Néron 1965] A. Néron, "Quasi-fonctions et hauteurs sur les variétés abéliennes", *Ann. of Math.* (2) **82** (1965), 249–331. MR Zbl

[Ogg 1967] A. P. Ogg, "Elliptic curves and wild ramification", *Amer. J. Math.* **89** (1967), 1–21. MR Zbl

[Saito 1988] T. Saito, "Conductor, discriminant, and the Noether formula of arithmetic surfaces", *Duke Math. J.* **57**:1 (1988), 151–173. MR Zbl

[Serre 1988] J.-P. Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics **117**, Springer, 1988. MR Zbl

[Shioda 1986] T. Shioda, "An explicit algorithm for computing the Picard number of certain algebraic surfaces", *Amer. J. Math.* **108**:2 (1986), 415–432. MR Zbl

[Shioda and Katsura 1979] T. Shioda and T. Katsura, "On Fermat varieties", *Tôhoku Math. J.* (2) **31**:1 (1979), 97–115. MR Zbl

[Tate 1966] J. Tate, "Endomorphisms of abelian varieties over finite fields", *Invent. Math.* **2** (1966), 134–144. MR Zbl

[Ulmer 1991] D. L. Ulmer, "p-descent in characteristic p", *Duke Math. J.* **62**:2 (1991), 237–265. MR Zbl

[Ulmer 2002] D. Ulmer, "Elliptic curves with large rank over function fields", *Ann. of Math.* (2) **155**:1 (2002), 295–315. MR Zbl

[Ulmer 2007] D. Ulmer, "L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields", *Invent. Math.* **167**:2 (2007), 379–408. MR Zbl

[Ulmer 2011] D. Ulmer, "Elliptic curves over function fields", pp. 211–280 in *Arithmetic of L-functions*, edited by C. Popescu et al., IAS/Park City Math. Ser. **18**, Amer. Math. Soc., Providence, RI, 2011. MR Zbl

[Ulmer 2013] D. Ulmer, "On Mordell–Weil groups of Jacobians over function fields", *J. Inst. Math. Jussieu* **12**:1 (2013), 1–29. MR Zbl

[Ulmer 2014a] D. Ulmer, "Curves and Jacobians over function fields", pp. 283–337 in *Arithmetic geometry over global function fields*, edited by F. Bars et al., Springer, 2014. MR Zbl

[Ulmer 2014b] D. Ulmer, "Explicit points on the Legendre curve", *J. Number Theory* **136** (2014), 165–194. MR Zbl

[Ulmer 2014c] D. Ulmer, "Explicit points on the Legendre curve III", *Algebra Number Theory* **8**:10 (2014), 2471–2522. MR Zbl

[Weil 1954] A. Weil, "Remarques sur un mémoire d'Hermite", *Arch. Math.* (*Basel*) **5** (1954), 197–202. MR Zbl

[Weil 1982] A. Weil, *Adeles and algebraic groups*, Progress in Mathematics **23**, Birkhäuser, Boston, 1982. MR Zbl

Communicated by Joseph H. Silverman
Received 2018-06-11 Revised 2019-02-27 Accepted 2019-04-02

ulmer@math.arizona.edu *Department of Mathematics, University of Arizona, Tucson, AZ, United States*

mathematical sciences publishers msp

Algebra & Number Theory

msp.org/ant

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

The subscription price for 2019 is US $/year for the electronic version, and $/year (+$, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

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

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

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 13 No. 5 2019

1937-0652(2019)13:5;1-8