COMPOSITIO MATHEMATICA

Rational points on hyperelliptic curves having a marked non-Weierstrass point

Arul Shankar and Xiaoheng Wang

Compositio Math. **154** (2018), 188–222.

doi:10.1112/S0010437X17007515

Compositio Math. 154 (2018) 188–222
doi:10.1112/S0010437X17007515

Rational points on hyperelliptic curves having a marked non-Weierstrass point

Arul Shankar and Xiaoheng Wang

Abstract

In this paper, we consider the family of hyperelliptic curves over $\mathbb{Q}$ having a fixed genus n and a marked rational non-Weierstrass point. We show that when $n \geqslant 9$, a positive proportion of these curves have exactly two rational points, and that this proportion tends to one as n tends to infinity. We study rational points on these curves by first obtaining results on the 2-Selmer groups of their Jacobians. In this direction, we prove that the average size of the 2-Selmer groups of the Jacobians of curves in our family is bounded above by 6, which implies a bound of 5/2 on the average rank of these Jacobians. Our results are natural extensions of Poonen and Stoll [*Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) **180** (2014), 1137–1166] and Bhargava and Gross [*The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, in *Automorphic representations and L-functions*, Tata Inst. Fundam. Res. Stud. Math., vol. 22 (Tata Institute of Fundamental Research, Mumbai, 2013), 23–91], where the analogous results are proved for the family of hyperelliptic curves with a marked rational Weierstrass point.

1. Introduction

In this paper, we prove that most monic even hyperelliptic curves have exactly two rational points. Consider the family of monic even hyperelliptic curves over $\mathbb{Q}$, namely complete genus-n curves given by the affine equation

$$C_f := y^2 = f(x) = x^{2n+2} + c_2x^{2n} + \cdots + c_{2n+2}, \tag{1}$$

where $n \geqslant 2$ and the c_i are elements of $\mathbb{Q}$ such that the polynomial $f(x)$ has distinct roots, or equivalently the discriminant $\Delta(f)$ of f is non-zero. We can realize C_f as a smooth curve in the weighted projective space $\mathbb{P}_{1,n+1,1}$ by homogenizing f to obtain $F(x,z)$, where $F(x,1) = f(x)$, and considering the projective curve given by $y^2 = F(x,z)$. Every curve in this family has a pair of non-Weierstrass points at infinity, denoted by $\infty = [1:1:0]$ and $\infty' = [1:-1:0]$, which are conjugate to each other by the hyperelliptic involution sending $[x:y:z]$ to $[x:-y:z]$. Scaling each c_i by λ^{2i} for $\lambda \in \mathbb{Q}^\times$ gives isomorphic curves. We then define a *height* on this family by setting

$$h(C_f) = \max_i\{|c_i|^{1/i}\},$$

where the c_i have been appropriately scaled so that $c_i \in \mathbb{Z}$ and there is no prime p such that $p^{2i} \mid c_i$ for all i. Throughout this paper, we order curves in our family by this height. The main result of our paper is the following theorem.

Received 16 August 2016, accepted in final form 8 June 2017, published online 9 October 2017.
2010 Mathematics Subject Classification 11G30 (primary).
Keywords: rational points on curves, hyperelliptic curves, ranks of abelian varieties, Selmer groups.

Theorem 1. *As n tends to infinity, a proportion approaching 100% of monic even hyperelliptic curves have exactly two rational points, namely ∞ and ∞'. More precisely, the proportion of monic even hyperelliptic curves having genus n that have exactly two rational points is at least $1-(24n+60)2^{-n}$.*

Note that the lower bound $1-(24n+60)2^{-n}$ is positive when $n \geqslant 9$. Theorem 1 adds to recent works on the study of rational points on curves as they vary across families. Bhargava [Bha13] uses geometry-of-numbers techniques to prove that most hyperelliptic curves have no rational points. Using Chabauty's method in conjunction with the results and techniques of [BG13], Poonen and Stoll [PS14] prove that most odd hyperelliptic curves have exactly one rational point. Our result adds evidence to the minimalist belief that when curves vary over a family, most of them have only the rational points that are forced on them. See [BMSW07] for a beautiful exposition on the implications of this belief for the distribution of ranks of elliptic curves.

There are three main steps in our proof of Theorem 1. First, we determine an upper bound on the average size of the 2-Selmer groups of Jacobians of curves in our family. More precisely, we prove the following theorem.

Theorem 2. *When all hyperelliptic curves of fixed genus $n \geqslant 2$ over $\mathbb{Q}$ having a marked rational non-Weierstrass point are ordered by height, the average size of the 2-Selmer groups of their Jacobians is at most 6.*

Theorem 2 is proved by constructing and counting locally soluble 2-covers of these Jacobians. Our proof naturally yields an equidistribution result (Theorem 34), which is important to our applications to rational points on these curves.

Next, we use these counting and equidistribution results in conjunction with Chabauty's method [Cha41, Col85], as refined by Poonen and Stoll [PS14], to prove that a positive proportion (the same proportion as in Theorem 1) of curves C in our family satisfy the following property: if $P \in C(\mathbb{Q})$, then $(P)-(\infty)$ is a rational multiple of $(\infty')-(\infty)$. Since our global results concern the 2-Selmer group, we need to work 2-adically in this step.

Finally, we use elimination theory over $\mathbb{Z}_p$, especially the theory of p-adic subanalytic sets, to prove that 0% of curves C in our family have rational points P such that $(P)-(\infty)$ is a rational multiple of $(\infty')-(\infty)$. This step is entirely local, and we work over large primes p.

In [BG13], Bhargava and Gross study odd hyperelliptic curves over $\mathbb{Q}$, and prove that the average size of the 2-Selmer groups of their Jacobians is bounded above by 3. We will show in Proposition 30 that the class $(\infty')-(\infty)$ is not divisible by 2 in $J(\mathbb{Q})$ for 100% of monic even hyperelliptic curves. Hence we expect the 2-Selmer groups of these Jacobians to have, on average, one extra generator compared to the Jacobians of monic odd hyperelliptic curves. This gives a heuristic reason for the ratio of these average values to be 2. In fact, we expect that these average values are indeed equal to 6 and 3.

For the 100% of curves where $(\infty')-(\infty)$ is not divisible by 2 in $J(\mathbb{Q})$, the average 2-rank of the 2-Selmer group minus 1 is at most 3/2. This is because $|\mathrm{Sel}_2(J)|/2$ is at least 1 and its average is at most 3. Therefore, we obtain the following immediate corollary to Theorem 2.

Corollary 3. *When all hyperelliptic curves of fixed genus $n \geqslant 2$ over $\mathbb{Q}$ having a marked rational non-Weierstrass point are ordered by height, the average rank of the 2-Selmer group of their Jacobians is at most 5/2. Thus the average rank of the Mordell–Weil groups of their Jacobians is at most 5/2.*

https://doi.org/10.1112/S0010437X17007515

To prove Theorem 2, we follow the same strategy as [BS15] and [BG13]: obtain first a bijection between Selmer elements and certain rational orbits of a representation V of a reductive group G; and then count these orbits using geometry-of-numbers methods. Let (U, Q) denote the split quadratic space of dimension $2n+2$ over $\mathbb{Q}$ and let V denote the space of operators T on U self-adjoint with respect to Q. For any monic separable polynomial $f(x)$ of degree $2n+2$, let J_f denote the Jacobian of the hyperelliptic curve defined by the affine equation $y^2 = f(x)$, and let V_f denote the subscheme of V consisting of self-adjoint operators T with characteristic polynomial $f(x)$. In § 2, we obtain a bijection between $\mathrm{Sel}_2(J_f)$ and locally soluble orbits of the conjugation action of $\mathrm{PSO}(U)(\mathbb{Q})$ on $V_f(\mathbb{Q})$. This parameterization step can be viewed as an example of arithmetic invariant theory. The various cohomological calculations are more complicated than in [BG13]. Although not strictly needed, we give in § 3 a very nice geometric interpretation of solubility using the arithmetic theory of pencils of quadrics as developed in [Wan13b]. More precisely, a self-adjoint operator $T \in V_f(\mathbb{Q})$ is soluble if and only if there exists a rational n-plane X that is isotropic with respect to the following two quadrics:

$$Q(v) = \langle v, v\rangle_Q,$$
$$Q_T(v) = \langle v, Tv\rangle_Q,$$

where $\langle\ ,\ \rangle_Q$ is the bilinear form associated to Q. A self-adjoint operator $T \in V_f(\mathbb{Q})$ is locally soluble if for every completion $\mathbb{Q}_v$ of $\mathbb{Q}$, there exists an n-plane X defined over $\mathbb{Q}_v$ that is isotropic with respect to the quadrics Q and Q_T.

In § 4, we count the number of locally soluble orbits using techniques of Bhargava developed in [Bha05] and prove Theorem 2. We count first the number of integral orbits soluble at $\mathbb{R}$ by counting the number of integral points inside a fundamental domain for the action of $\mathrm{PSO}(U)(\mathbb{Z})$ on $V(\mathbb{R})$. We break up this fundamental domain into a compact part and a cusp region where separate estimations are required. The compact part of the fundamental domain will contribute to, on average, four Selmer elements. The cusp region corresponds to the two 'obvious' classes: 0 and $(\infty') - (\infty)$. We then apply a sieve to the locally soluble orbits by imposing infinitely many congruence conditions. This gives an upper bound for the average size of the 2-Selmer groups. To show that the average size is in fact equal to 6, we would need a uniformity estimate on the number of $\mathrm{PSO}(U)(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ analogous to Proposition 25.

In § 5, we apply a refinement of Chabauty's method to study rational points on monic even hyperelliptic curves following the strategy of Poonen and Stoll [PS14]. The curve C embeds into its Jacobian J via the map sending a point P to the divisor class of $(P) - (\infty)$. The image of $C(\mathbb{Q}_2)$ is a one-dimensional 2-adic manifold in $J(\mathbb{Q}_2)$. On the other hand, $C(\mathbb{Q})$ also maps to the 2-Selmer group of its Jacobian which admits a natural map to $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$. The image of $C(\mathbb{Q}_2)$ in $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ is on average quite small compared to the size $2^n \# J(\mathbb{Q}_2)[2]$ of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$, once the genus n is large enough. Furthermore, the Selmer group has on average very few elements which, with the exception of 0 and the class of $(\infty') - (\infty)$, equidistribute onto $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$. However, these two sets, the image of $C(\mathbb{Q}_2)$ and the image of the 2-Selmer group in $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$, do always intersect at two points, namely the image of 0 and $(\infty') - (\infty)$. We thus modify the n-dimensional $\mathbb{F}_2$-vector space $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ as follows: we mod out by the line spanned by the (primitive part of the) image of $(\infty') - (\infty)$ and replace the remaining $(n-1)$-dimensional $\mathbb{F}_2$-vector space by its projectivization. We then prove that for a proportion at least $1 - O(n2^{-n})$ of curves C, these two sets do not intersect and that every rational point P of C is *bad*, that is, $(P) - (\infty)$ is a rational multiple of $(\infty') - (\infty)$.

Finally, in § 6, we use the theory of p-adic subanalytic sets to prove that the p-adic closure of the set of curves C over $\mathbb{Q}_p$ such that $C(\mathbb{Q}_p)\backslash\{\infty, \infty'\}$ contains a bad point has measure 0 in

https://doi.org/10.1112/S0010437X17007515

the corresponding moduli space. Combining this result with results from previous sections, we prove Theorem 1.

2. Orbit parameterization

Let k be a field of characteristic not equal to 2 and let (U, Q) be the (unique) split quadratic space over k of dimension $2n+2$ and discriminant 1. Recall that a $(2n+2)$-dimensional quadratic space over k is split if and only if there exists an isotropic subspace of dimension $n+1$ defined over k. Let $f(x)$ be a monic polynomial of degree $2n+2$ with no repeated roots and splitting completely over k^s, the separable closure of k. In this section, we study the action of $\mathrm{PSO}(U)$ on self-adjoint operators on U with characteristic polynomial $f(x)$ via conjugation. More precisely, let $\langle v, w\rangle_Q = Q(v+w) - Q(v) - Q(w)$ denote the bilinear form associated to Q. For any linear operator $T : U \to U$, its adjoint T^* is defined via the following equation:

$$\langle Tv, w\rangle_Q = \langle v, T^* w\rangle_Q, \quad \forall v, w \in U.$$

Let V denote the k-scheme

$$V = \{T : U \to U \mid T = T^*\},$$

and V_f the k-scheme

$$V_f = \{T : U \to U \mid T = T^*, \det(xI - T) = f(x)\}.$$

The group scheme

$$\mathrm{SO}(U) := \{g \in \mathrm{GL}(U) \mid g^* g = I, \det(g) = 1\}$$

acts on V_f via $g \cdot T = gTg^{-1}$. The center $\mu_2 \leqslant \mathrm{SO}(U)$ acts trivially. Hence we obtain a faithful action of

$$G = \mathrm{PSO}_{2n+2} := \mathrm{PSO}(U) = \mathrm{SO}(U)/\mu_2.$$

To study the orbits of these actions, we first work over the separable closure k^s of k in § 2.1 and show that $G(k^s)$ acts transitively on $V_f(k^s)$ for separable polynomials f. In § 2.2, we work over k and classify the $G(k)$-orbits on $V_f(k)$ using Galois cohomology. In § 2.3, we consider the Jacobian J of the hyperelliptic curve given by the equation $y^2 = f(x)$ and obtain a bijection between the set $G(k)\backslash V_f(k)$ of k-rational orbits with characteristic polynomial $f(x)$ and a subset of $H^1(k, J[2])$. The most difficult part of this section will be to show that this subset contains the image of $J(k)/2J(k)$ in $H^1(k, J[2])$. Finally, in § 2.4, we work over $\mathbb{Z}_p$ and describe the set $G(\mathbb{Z}_p)\backslash V(\mathbb{Z}_p)$ of integral orbits with characteristic polynomial $f(x)$.

2.1 Geometric orbits

Proposition 4. *Let $f(x) \in k[x]$ be a monic separable polynomial of degree $2n+2$ splitting completely over k^s. Then the group $G(k^s)$ acts transitively on $V_f(k^s)$. For any $T \in V_f(k)$, the stabilizer subscheme $\mathrm{Stab}_G(T)$ is isomorphic to $(\mathrm{Res}_{L/k}\,\mu_2)_{N=1}/\mu_2$, where $L = k[x]/f(x)$ is an étale k-algebra of dimension $2n+2$.*

Proof. Fix any T in $V_f(k)$. Since T has distinct eigenvalues, its stabilizer scheme in $\mathrm{GL}(U)$ is a maximal torus. It contains and hence is equal to the maximal torus $\mathrm{Res}_{L/k}\,\mathbb{G}_m$. For any k-algebra K, we have

$$\mathrm{Stab}_{\mathrm{O}(U)}(T)(K) = \{g \in (K[T]/f(T))^\times \mid g^* g = 1\}.$$

https://doi.org/10.1112/S0010437X17007515

Since $T = T^*$ and g is a polynomial in T, we have $g = g^*$. Thus,

$$\begin{aligned}\mathrm{Stab}_{\mathrm{O}(U)}(T) &\simeq \mathrm{Stab}_{\mathrm{GL}(U)}(T)[2] \simeq \mathrm{Res}_{L/k}\,\mu_2,\\ \mathrm{Stab}_{\mathrm{SO}(U)}(T) &\simeq (\mathrm{Res}_{L/k}\,\mu_2)_{N=1},\\ \mathrm{Stab}_{\mathrm{PSO}(U)}(T) &\simeq (\mathrm{Res}_{L/k}\,\mu_2)_{N=1}/\mu_2.\end{aligned}$$

Since T is self-adjoint, there is an orthonormal basis $\{u_1, \ldots, u_{2n+2}\}$ for U consisting of eigenvectors of T with eigenvalues $\lambda_1, \ldots, \lambda_{2n+2}$. If T' is another element of $V_f(k^s)$, then there is an orthonormal basis $\{u'_1, \ldots, u'_{2n+2}\}$ of U consisting of eigenvectors of T' with eigenvalues $\lambda_1, \ldots, \lambda_{2n+2}$. Let $g \in \mathrm{GL}(U)(k^s)$ be an operator sending u_i to $\pm u'_i$, where the signs are chosen so that $g \in \mathrm{SL}(U)(k^s)$. Then $g \in \mathrm{SO}(U)(k^s)$ and the image of g in $\mathrm{PSO}(U)(k^s)$ sends T to T'. □

2.2 Rational orbits via Galois cohomology

Our first aim is to show that $V_f(k)$ is non-empty. Indeed, one can view $L = k[x]/(f(x))$ as a $(2n+2)$-dimensional k-vector space with a power basis $\{1, \beta, \ldots, \beta^{2n+1}\}$ where $\beta \in k[x]/(f(x))$ is the image of x. We define the bilinear form $\langle\,,\rangle$ on L as follows:

$$\langle \lambda, \mu\rangle := \text{coefficient of } \beta^{2n+1} \quad \text{in } \lambda\mu = \mathrm{Tr}_{L/k}(\lambda\mu/f'(\beta)).$$

This form is split since the $(n+1)$-plane $Y = \mathrm{Span}\{1, \beta, \ldots, \beta^n\}$ is isotropic. Its discriminant is 1, as one can readily compute using the above power basis. By the uniqueness of split quadratic spaces of fixed dimension and discriminant 1, there exists an isometry between $(L, \langle\,,\rangle)$ and $(U, \langle\,,\rangle_Q)$, well defined up to post-composition by elements in $\mathrm{O}(U)(k)$. Let $\cdot\beta : L \to L$ denote the linear map on L given by multiplication by β. Then $\cdot\beta$ is self-adjoint with characteristic polynomial $f(x)$, and hence yields an element in $V_f(k)$ well defined up to $\mathrm{O}(U)(k)$ conjugation. In what follows, we fix an isometry $\iota : L \to U$, thus yielding a fixed element $T_f \in V_f(k)$.

Given $T \in V_f(k)$, there exists $g \in G(k^s)$ such that $T = gT_fg^{-1}$, since there is a unique geometric orbit by Proposition 4. For any $\sigma \in \mathrm{Gal}(k^s/k)$, the element ${}^\sigma g$ also conjugates T_f to T and hence $g^{-1}\,{}^\sigma g \in \mathrm{Stab}_G(T_f)(k^s)$. The 1-cochain c_T given by $(c_T)_\sigma = g^{-1}\,{}^\sigma g$ is a 1-cocycle whose image in $H^1(k, G)$ is trivial. This defines a bijection

$$G(k)\backslash V_f(k) \leftrightarrow \ker(H^1(k, \mathrm{Stab}_G(T_f)) \to H^1(k, G)) \tag{2}$$

$$T \mapsto c_T. \tag{3}$$

See [BG14, Proposition 1] for more details.

2.2.1 *Distinguished orbits.* We call a self-adjoint operator $T \in V_f(k)$ *distinguished* if it is $\mathrm{PO}(U)(k)$-equivalent to T_f. Since the $\mathrm{PO}(U)(k)$-orbit of T_f might break up into two $\mathrm{PSO}(U)(k)$-orbits, there might exist two distinguished $\mathrm{PSO}(U)(k)$-orbits in contrast to the odd hyperelliptic case. As $\mathrm{Stab}_{\mathrm{PO}(U)}(T_f) \simeq \mathrm{Res}_{L/k}\,\mu_2/\mu_2$, we have the following diagram of exact rows.

$$\begin{array}{ccccccc}
\big(\mathrm{Res}_{L/k}\,\mu_2/\mu_2\big)(k) & \xrightarrow{N} & \mu_2(k) & \longrightarrow & H^1(k, \mathrm{Stab}_{\mathrm{PSO}(U)}(T_f)) & \longrightarrow & H^1(k, \mathrm{Stab}_{\mathrm{PO}(U)}(T_f))\\
 & & \downarrow\sim & & \downarrow & & \downarrow\\
\mathrm{PO}(U)(k) & \twoheadrightarrow & \mu_2(k) & \longrightarrow & H^1(k, \mathrm{PSO}(U)) & \longrightarrow & H^1(k, \mathrm{PO}(U))
\end{array}$$

Note that the second row consists of maps between pointed sets where the trivial classes in $H^1(k, \mathrm{PSO}(U))$ and $H^1(k, \mathrm{PO}(U))$ correspond to the split quadratic form (U, Q); and where

https://doi.org/10.1112/S0010437X17007515

exactness means that the preimages of the trivial classes equal the images of the previous maps. A self-adjoint operator $T \in V_f(k)$ is distinguished if and only if

$$c_T \in \ker(H^1(k, \mathrm{Stab}_{\mathrm{PSO}(U)}(T_f)) \to H^1(k, \mathrm{Stab}_{\mathrm{PO}(U)}(T_f))).$$

Since $H^1(k, \mathrm{PSO}(U)) \to H^1(k, \mathrm{PO}(U))$ is injective, every class in the above kernel corresponds to a $\mathrm{PSO}(U)(k)$-orbit.

Distinguished $\mathrm{PSO}(U)(k)$-orbits in $V_f(k)$ are unique if and only if the norm map $N : \mathrm{Res}_{L/k}\, \mu_2/\mu_2(k) \to \mu_2(k)$ is surjective. Therefore, [PS97, Lemma 11.2] immediately implies the following result.

PROPOSITION 5. *Let $f(x)$ be as in Proposition 4. Then the set of distinguished elements in $V_f(k)$ consists of a single $\mathrm{PSO}(U)(k)$-orbit if and only if one of the following conditions is satisfied:*

(i) *$f(x)$ has a factor of odd degree in $k[x]$;*
(ii) *n is even and $f(x)$ factors over some quadratic extension K of k as $h(x)\bar{h}(x)$, where $h(x) \in K[x]$ and $\bar{h}(x)$ is the $\mathrm{Gal}(K/k)$-conjugate of $h(x)$.*

Otherwise, the set of distinguished elements in $V_f(k)$ consists of two $\mathrm{PSO}(U)(k)$-orbits. Condition (ii) *is equivalent to saying that n is even, and L contains a quadratic extension K of k.*

To give a more explicit description of distinguished orbits, we have the following result, the proof of which is deferred to § 3.

PROPOSITION 6. *Let $f(x)$ be as in Proposition 4. Then a self-adjoint operator $T \in V_f(k)$ is distinguished if and only if there exists a k-rational n-plane $X \subset U$ such that $\mathrm{Span}\{X, TX\}$ is an isotropic $(n+1)$-plane.*

After a change of basis, we may take the matrix A with 1s on the anti-diagonal and 0s elsewhere as a Gram matrix for Q. We express this basis as

$$\{e_1, \ldots, e_{n+1}, f_{n+1}, \ldots, f_1\}$$

where

$$\langle e_i, f_j\rangle_Q = \delta_{ij}, \quad \langle e_i, e_j\rangle_Q = 0 = \langle f_i, f_j\rangle_Q. \tag{4}$$

We call this the standard basis. Then the above proposition yields the following explicit description of distinguished elements which will be useful in § 4.

PROPOSITION 7. *A self-adjoint operator in $V_f(k)$ is distinguished if and only if its $\mathrm{PSO}(U)(k)$-orbit contains an element T whose matrix M, with respect to the standard basis, satisfies*

$$AM = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & * & * \\ 0 & 0 & \cdots & 0 & * & * & * \\ \vdots & \vdots & \iddots & \iddots & \vdots & \vdots & \vdots \\ 0 & 0 & \iddots & \cdots & \vdots & \vdots & \vdots \\ 0 & * & \cdots & \cdots & * & * & * \\ * & * & \cdots & \cdots & * & * & * \\ * & * & \cdots & \cdots & * & * & * \end{pmatrix}. \tag{5}$$

https://doi.org/10.1112/S0010437X17007515

Proof. The forward direction follows from an argument identical to the proof of [BG13, Proposition 4.4]. For the backward direction, suppose AM has the form in (5). Then

$$Te_i \in \mathrm{Span}\{e_1, \dots, e_{n+1}\}^{\perp} = \mathrm{Span}\{e_1, \dots, e_{n+1}\}, \quad \text{for } i = 1, \dots, n. \tag{6}$$

Let X be the n-plane $\mathrm{Span}\{e_1, \dots, e_n\}$. Since T is self-adjoint, its eigenspaces are pairwise orthogonal. Since Q is non-degenerate, none of the eigenvectors of T is isotropic. As a result, no isotropic linear space is T-stable. Hence by (6),

$$\mathrm{Span}\{X, TX\} = \mathrm{Span}\{e_1, \dots, e_{n+1}\}.$$

By Proposition 6, T is distinguished. □

2.2.2 *Remaining orbits.* We start by describing the set of $\mathrm{O}(U)(k)$-orbits on $V_f(k)$. Recall that $\mathrm{Stab}_{\mathrm{O}(U)}(T_f) \simeq \mathrm{Res}_{L/k}\mu_2$. The set

$$\ker(H^1(k, \mathrm{Stab}_{\mathrm{O}(U)}(T_f)) \to H^1(k, O(U)))$$

consists of elements $\alpha \in H^1(k, \mathrm{Res}_{L/k}\mu_2) \simeq L^\times/L^{\times 2}$ whose image in $H^1(k, O(U))$ is trivial. For any $\alpha \in L^\times/L^{\times 2}$, lift it arbitrarily to $L^\times$ and consider the following bilinear form on L:

$$\langle \lambda, \mu \rangle_\alpha = \text{coefficient of } \beta^{2n+1} \quad \text{in } \alpha\lambda\mu = \mathrm{Tr}_{L/k}(\alpha\lambda\mu/f'(\beta)).$$

We claim that α maps to 0 in $H^1(k, \mathrm{O}(U))$ if and only if $\langle\,,\rangle_\alpha$ is split with discriminant 1. Indeed, let $\iota : (L, \langle\,,\rangle) \to (U, \langle\,,\rangle_Q)$ denote the isometry used to define T_f. Now $\langle\,,\rangle_\alpha$ is split with discriminant 1 if and only if there exists $g \in O(U)(k^s)$ such that the following composite map is defined over k:

$$(L, \langle\,,\rangle_\alpha) \xrightarrow{\sqrt{\alpha}}_{k^s} (L, \langle\,,\rangle) \xrightarrow{\iota}_{k} (U, \langle\,,\rangle_Q) \xrightarrow{g}_{k^s} (U, \langle\,,\rangle_Q), \tag{7}$$

where the subscripts below the arrows indicate the fields of definition and where the last map is the standard action of $g \in \mathrm{O}(U)(k^s)$. Unwinding the definitions [Wan13b, Proposition 2.13], we see that this is equivalent to the image of α mapping to 0 in $H^1(k, \mathrm{O}(U))$. We have therefore shown the following result.

Theorem 8. *Let $f(x)$ be as in Proposition 4. Then there is a bijection between $\mathrm{O}(U)(k)$-orbits on $V_f(k)$ and classes $\alpha \in (L^\times/L^{\times 2})_{N=1}$ such that $\langle\,,\rangle_\alpha$ is split.*

To study $\mathrm{SO}(U)(k)$- and $\mathrm{PO}(U)(k)$-orbits, we note that all the maps in the following diagram are injections.

$$\begin{array}{ccc} H^1(k, \mathrm{SO}(U)) & \longrightarrow & H^1(k, \mathrm{O}(U)) \\ \downarrow & & \downarrow \\ H^1(k, \mathrm{PSO}(U)) & \longrightarrow & H^1(k, \mathrm{PO}(U)) \end{array}$$

The horizontal maps are injective because the determinant map from $\mathrm{O}(U)(k)$ to $\mu_2(k)$ is surjective. The vertical maps are injective because the connecting homomorphism $\mathrm{PSO}(U)(k) \to k^\times/k^{\times 2}$ is surjective. Indeed, for any $c \in k^\times$, the element in $\mathrm{PSO}(U)(k)$ mapping to c is the operator

$$e_i \mapsto \sqrt{c}\, e_i, \quad f_i \mapsto \sqrt{c}^{-1} f_i, \quad \forall i = 1, \dots, n+1.$$

https://doi.org/10.1112/S0010437X17007515

Recall that $\mathrm{Stab}_{\mathrm{SO}(U)}(T_f) \simeq (\mathrm{Res}_{L/k}\mu_2)_{N=1}$. From the exact sequence

$$1 \to (\mathrm{Res}_{L/k}\mu_2)_{N=1} \to \mathrm{Res}_{L/k}\mu_2 \xrightarrow{N} \mu_2 \to 1,$$

we obtain the isomorphism

$$\ker\big(H^1(k, (\mathrm{Res}_{L/k}\mu_2)_{N=1}) \to H^1(k, \mathrm{Res}_{L/k}\mu_2)\big) \simeq \mathrm{coker}\big(\mu_2(L) \xrightarrow{N} \mu_2(k)\big).$$

We see that each $O(U)(k)$-orbit breaks up into one or two $\mathrm{SO}(U)(k)$-orbits depending on whether $f(x)$ has an odd degree factor or not, respectively.

We next describe the set of $\mathrm{PO}(U)(k)$-orbits on $V_f(k)$. Each such orbit breaks up into either one or two $\mathrm{PSO}(U)(k)$-orbits depending on whether the norm map $N : (\mathrm{Res}_{L/k}\,\mu_2/\mu_2)(k) \to \mu_2(k)$ is surjective or not, respectively (see Proposition 5 for a more descriptive criterion). As the stabilizer subscheme of T_f in $\mathrm{PO}(U)$ is $\mathrm{Res}_{L/k}\mu_2/\mu_2$, we have the following diagram of exact rows:

$$\begin{array}{ccccccc}
H^1(k,\mu_2) & \longrightarrow & H^1(k, \mathrm{Res}_{L/k}\mu_2) & \longrightarrow & H^1(k, \mathrm{Res}_{L/k}\mu_2/\mu_2) & \longrightarrow & H^2(k,\mu_2) \\
\downarrow{=} & & \downarrow & & \downarrow & & \downarrow{=} \\
H^1(k,\mu_2) & \longrightarrow & H^1(k, \mathrm{O}(U)) & \hookrightarrow & H^1(k, \mathrm{PO}(U)) & \longrightarrow & H^2(k,\mu_2)
\end{array}$$

Suppose

$$c'_T \in \ker(H^1(k, \mathrm{Res}_{L/k}\mu_2/\mu_2) \to H^1(k, \mathrm{PO}(U))).$$

Since c'_T maps to 0 in $H^2(k,\mu_2)$, it is the image of some $\alpha \in L^\times/L^{\times 2}$ well defined up to $k^\times/k^{\times 2}$. Since the map $H^1(k, \mathrm{O}(U)) \to H^1(k, \mathrm{PO}(U))$ is injective, the image of α in $H^1(k, \mathrm{O}(U))$ is trivial. By Theorem 8, this is equivalent to the form $\langle\,,\rangle_\alpha$ being split with discriminant 1. Therefore, we have the following characterization of $\mathrm{PO}(U)(k)$-orbits.

THEOREM 9. *There is a bijection between* $\mathrm{PO}(U)(k)$*-orbits and classes* $\alpha \in (L^\times/(L^{\times 2}k^\times))_{N=1}$ *such that* $\langle\,,\rangle_\alpha$ *is split. The distinguished orbit corresponds to* $\alpha = 1$*. Two* $\mathrm{O}(U)(k)$*-orbits corresponding to* $\alpha_1, \alpha_2 \in (L^\times/L^{\times 2})_{N=1}$ *are* $\mathrm{PO}(U)(k)$*-equivalent if and only if* α_1 *and* α_2 *have the same image in* $(L^\times/L^{\times 2}k^\times)_{N=1}$.

2.3 Connection to hyperelliptic curves

Let C be the monic even hyperelliptic curve of genus n given by the affine equation $y^2 = f(x)$, and let J denote its Jacobian. The curve C has two rational points above infinity, denoted by ∞ and ∞'. Let $P_1, \ldots, P_{2n+2}$ denote the Weierstrass points of C over k^s. These form the ramification locus of the map $x : C \to \mathbb{P}^1$. Let D_0 denote the hyperelliptic class obtained as the pullback of $\mathcal{O}_{\mathbb{P}^1}(1)$. Then the group $J[2](k^s)$ is generated by the divisor classes $(P_i) + (P_j) - D_0$ for $i \neq j$ subject only to the condition that

$$\sum_{i=1}^{2n+2} (P_i) - (n+1)D_0 \sim 0.$$

We have the following isomorphisms of group schemes over k:

$$J[2] \simeq (\mathrm{Res}_{L/k}\,\mu_2)_{N=1}/\mu_2 \simeq \mathrm{Stab}_G(T_f). \tag{8}$$

An explicit formula for this identification is given in [Wan13a, Remark 2.6].

https://doi.org/10.1112/S0010437X17007515

In conjunction with (2), this identification yields a bijection

$$G(k)\backslash V_f(k) \longrightarrow \ker(H^1(k, J[2]) \to H^1(k, G)).$$

Hence $G(k)$-orbits on $V_f(k)$ can be identified with a subset of $H^1(k, J[2])$. Recall that we have the following descent exact sequence:

$$1 \to J(k)/2J(k) \to H^1(k, J[2]) \to H^1(k, J)[2] \to 1. \tag{9}$$

A $G(k)$-orbit in $V_f(k)$ is said to be *soluble* if it corresponds to a class in $H^1(k, J[2])$ which is in the image of the map from $J(k)/2J(k)$. The following theorem states that there is a bijection between soluble $G(k)$-orbits in $V_f(k)$ and elements of $J(k)/2J(k)$.

Theorem 10. *The following composite map is trivial:*

$$J(k)/2J(k) \to H^1(k, J[2]) \to H^1(k, G). \tag{10}$$

Therefore, there is a bijection between soluble $G(k)$-orbits in $V_f(k)$ and elements of $J(k)/2J(k)$.

Proof. We prove Theorem 10 in the case when k is a local field. For a complete proof, see § 3. Combining the descent sequence (9) and the long exact sequence obtained by taking Galois cohomology of the short exact sequence

$$1 \to J[2] \to \mathrm{Res}_{L/k}\mu_2/\mu_2 \xrightarrow{N} \mu_2 \to 1,$$

we get the following commutative diagram.

$$\begin{array}{ccccccc} \langle(\infty') - (\infty)\rangle & \longrightarrow & J(k)/2J(k) & \xrightarrow{\delta'} & L^\times/(L^{\times 2}k^\times) & \xrightarrow{N} & k^\times/k^{\times 2} \\ \downarrow \sim & & \downarrow \delta & & \downarrow & & \downarrow \sim \\ \frac{\mu_2(k)}{N(\mathrm{Res}_{L/k}\mu_2/\mu_2(k))} & \longrightarrow & H^1(k, J[2]) & \longrightarrow & H^1(k, \mathrm{Res}_{L/k}\mu_2/\mu_2) & \xrightarrow{N} & H^1(k, \mu_2) \end{array} \tag{11}$$

The map δ' is defined in [PS97] by evaluating $(x - \beta)$ on a given divisor class. As shown in [PS97], the first row is not exact: the map δ' lands inside, generally not onto, $(L^\times/L^{\times 2}k^\times)_{N=1}$ with kernel the subgroup generated by the class $(\infty') - (\infty)$. Note that $(\infty') - (\infty) \in 2J(k)$ if and only if the norm map $N : \mathrm{Res}_{L/k}\,\mu_2/\mu_2(k) \to \mu_2(k)$ is surjective if and only if there is a unique distinguished orbit.

To prove Theorem 10, it suffices to show that if $\alpha \in (L^\times/L^{\times 2}k^\times)_{N=1}$ lies in the image of δ', then $\langle\,,\rangle_\alpha$ is split. We will prove this by explicitly writing down a k-rational $(n+1)$-dimensional isotropic subspace in the special case when k is a local field. For a complete and more conceptual proof using pencils of quadrics, see § 3. Suppose $\alpha = \delta'([D])$ for some $[D] \in J(k)/2J(k)$ of the form

$$[D] = (Q_1) + \cdots + (Q_m) - m(\infty) \mod 2J(k) \cdot \langle(\infty') - (\infty)\rangle,$$

where $Q_1, \ldots, Q_m \in C(k^s)$ are non-Weierstrass non-infinity points and $m \leqslant n+1$. When k is a local field, every $[D] \in J(k)/2J(k)$ can be written in this form [Wan13b, Lemma 3.8]. If we write $Q_i = (x_i, y_i)$, then $\alpha = (x_1 - \beta)\cdots(x_m - \beta)$ and

$$\langle\lambda, \mu\rangle_\alpha = \mathrm{Tr}_{L/k}((x_1 - \beta)\cdots(x_m - \beta)\lambda\mu/f'(\beta)).$$

https://doi.org/10.1112/S0010437X17007515

We may also assume that the x_i are all distinct since the sum of all the Q_i whose x-coordinates appear more than once lies in $2J(k)\cdot\langle(\infty')-(\infty)\rangle$. Write

$$\widetilde{V}=\prod_{1\leqslant i<j\leqslant m}(x_i-x_j)$$

for the Vandermonde polynomial, and, for each $i=1,\dots,m$, define

$$q_i:=\prod_{1\leqslant j\leqslant m, j\neq i}(x_j-x_i),\quad a_i:=\widetilde{V}/q_i,\quad h_i(t):=\frac{f(t)-f(x_i)}{t-x_i}.$$

For any $j\geqslant 0$, we define

$$g_j(t)=\sum_{i=1}^{m}x_i^j a_i\frac{h_i(t)}{y_i}.$$

Then the $(n+1)$-plane Y defined below is k-rational and isotropic [Wan13b, Lemma 2.44]:

$$Y:=\mathrm{Span}\{1,\beta,\dots,\beta^{n-m'},g_0(\beta),\dots,g_{m'-1}(\beta)\}\quad\text{if } m=2m' \text{ or } m=2m'+1.$$

This completes the proof of Theorem 10 when k is a local field. □

Suppose that k is a number field. Then the 2-Selmer group $\mathrm{Sel}_2(k,J)$ is the subgroup of $H^1(k,J[2])$ consisting of elements whose images in $H^1(k_\nu,J[2])$ lie in the images of $J(k_\nu)/2J(k_\nu)$ for all the local completions k_ν of k. Since the group $G=\mathrm{PSO}_{2n+2}$ is an adjoint group, it satisfies the Hasse principle (see [PR94, Theorem 6.22]), that is, the map

$$H^1(k,G)\to\prod_v H^1(k_v,G)$$

is injective, where the product is over all places v of k. Hence, Theorem 10 implies that the following composite is also trivial:

$$\mathrm{Sel}_2(k,J)\to H^1(k,J[2])\to H^1(k,G).$$

A self-adjoint operator $T\in V_f(k)$ is said to be *locally soluble* if T is soluble in $V_f(k_\nu)$ for all the local completions k_ν of k. Equivalently, T is locally soluble if and only if c_T lies in $\mathrm{Sel}_2(k,J)$. We have thus proven the following theorem.

THEOREM 11. *Let k be a number field. Let $f(x)$ be a monic separable polynomial of degree $2n+2$ over k. Then there is a bijection between locally soluble $G(k)$-orbits on $V_f(k)$ and elements in $\mathrm{Sel}_2(k,J)$, where J is the Jacobian of the hyperelliptic curve given by the equation $y^2=f(x)$.*

2.4 Integral orbits

Let $f(x)\in\mathbb{Q}[x]$ be a monic separable polynomial of degree $2n+2$. Let C be the hyperelliptic curve defined by $y^2=f(x)$, and let J be its Jacobian. We have seen that elements in the 2-Selmer group of J are in bijection with locally soluble $G(\mathbb{Q})$-orbits in $V_f(\mathbb{Q})$. In this section, our aim is to show that when f has integral coefficients, every locally soluble $G(\mathbb{Q})$-orbit in $V_f(\mathbb{Q})$ contains an integral representative.

https://doi.org/10.1112/S0010437X17007515

We do this by working over the field $\mathbb{Q}_p$ and the ring $\mathbb{Z}_p$. Specifically, we prove the following result.

Proposition 12. *Let p be a prime and let $f(x) = x^{2n+2} + c_1x^{2n+1} + \cdots + c_{2n+2}$ be a monic separable polynomial in $\mathbb{Z}_p[x]$ such that $2^{4i}|c_i$ in $\mathbb{Z}_p$ for $i = 1, \ldots, 2n+2$. Then every soluble $G(\mathbb{Q}_p)$-orbit in $V_f(\mathbb{Q}_p)$ contains an integral representative.*

Recall that the class number of G over $\mathbb{Q}$ is the number of double cosets $G(\mathbb{A}(\infty))xG(\mathbb{Q})$ of the group $G(\mathbb{A})$, where $\mathbb{A}$ is the ring of adeles of $\mathbb{Q}$ and $\mathbb{A}(\infty)$ denotes the ring of integral adeles, that is, the product of $\mathbb{R}$ and $\mathbb{Z}_p$ over all primes p. For a quadratic space U, it is known (see [PR94, Proposition 8.4]) that the class number of $\mathrm{O}(U)$ over $\mathbb{Q}$ is the same as the number of classes in the genus of U. The number of classes in the genus of any space having determinant ± 1 is 1 [Ser73, ch. V, Theorem 6]. It then easily follows that the class number of G over $\mathbb{Q}$ is 1. We therefore immediately obtain the following corollary.

Corollary 13. *Let $f(x) = x^{2n+2} + c_1x^{2n+1} + \cdots + c_{2n+2}$ be a monic separable polynomial in $\mathbb{Z}[x]$ such that $2^{4i}|c_i$ for $i = 1, \ldots, 2n+2$. Then every locally soluble $G(\mathbb{Q})$-orbit in $V_f(\mathbb{Q})$ contains an integral representative.*

We will also prove the following result.

Proposition 14. *Let p be any odd prime, and let $f(x) \in \mathbb{Z}_p[x]$ be a monic separable polynomial of degree $2n+2$ such that $p^2 \nmid \Delta(f)$. Then the $G(\mathbb{Z}_p)$-orbits in $V_f(\mathbb{Z}_p)$ are in bijection with soluble $G(\mathbb{Q}_p)$-orbits in $V_f(\mathbb{Q}_p)$. Furthermore, if $T \in V_f(\mathbb{Z}_p)$, then $\mathrm{Stab}_{G(\mathbb{Z}_p)}(T) = \mathrm{Stab}_{G(\mathbb{Q}_p)}(T)$.*

Let p be a fixed prime. We start by considering the $\mathrm{O}(U)(\mathbb{Z}_p)$-orbits. A self-adjoint operator $T \in V_f(\mathbb{Q}_p)$ is *integral* if it stabilizes the self-dual lattice

$$M_0 = \mathrm{Span}_{\mathbb{Z}_p}\{e_1, \ldots, e_{n+1}, f_{n+1}, \ldots, f_1\}.$$

In other words, T is integral if and only if, when expressed in the standard basis (4), its entries are in $\mathbb{Z}_p$. In general, a lattice M is self-dual if the bilinear form restricts to a non-degenerate bilinear form: $M \times M \to \mathbb{Z}_p$. Since genus theory implies that any two self-dual lattices are $\mathrm{O}(U)(\mathbb{Q}_p)$-conjugate, the rational orbit of T contains an integral representative if and only if T stabilizes a self-dual lattice.

The action of T on U gives U the structure of a $\mathbb{Q}_p[x]$-module, where x acts via T. Since T is regular, we have an isomorphism of $\mathbb{Q}_p[x]$-modules: $U \simeq \mathbb{Q}_p[x]/(f(x)) = L$. Suppose T is integral, stabilizing the self-dual lattice M_0. The action of T on M_0 realizes M_0 as a $\mathbb{Z}_p[x]/(f(x))$-module. Write R for $\mathbb{Z}_p[x]/f(x)$. Since M_0 is a lattice, we see that after the identification $U \simeq L$, M_0 becomes a fractional ideal I for the order R. The split form Q on U gives a split form of discriminant 1 on L for which multiplication by β is self-adjoint. Any such form on L is of the form $\langle\, , \rangle_\alpha$ for some $\alpha \in L^\times$ with $N_{L/k}(\alpha) \in k^{\times 2}$. The condition that M_0 is self-dual translates to saying $\alpha \cdot I^2 \subset R$ and $N(I)^2 = N(\alpha^{-1})$.

The identification $U \simeq L$ is unique up to multiplication by some element $c \in L^\times$, which transforms the data (I, α) to $(c \cdot I, c^{-2}\alpha)$. We call two pairs (I, α), (I', α') equivalent if there exists $c \in L^\times$ such that $I' = c \cdot I$ and $\alpha' = c^{-2}\alpha$. Choosing a different integral representative T in an integral orbit amounts to pre-composing the map $U \simeq L$ by an element of $\mathrm{O}(U)(\mathbb{Z}_p)$ which does not change the equivalence class of the pair (I, α). Hence we have a well-defined map

$$\mathrm{O}(U)(\mathbb{Z}_p)\backslash V_f(\mathbb{Z}_p) \to \text{equivalence classes of pairs } (I, \alpha). \tag{12}$$

https://doi.org/10.1112/S0010437X17007515

THEOREM 15. *There is a bijection between $\mathrm{O}(U)(\mathbb{Z}_p)$-orbits and equivalence classes of pairs (I,α) such that $\langle\,,\rangle_\alpha$ is split, $\alpha\cdot I^2\subset R$, and $N(I)^2=N(\alpha^{-1})$. The image of α in $(L^\times/L^{\times 2})_{N=1}$ determines the rational orbit.*

Proof. Given a pair (I,α) such that $\langle\,,\rangle_\alpha$ is split, $\alpha I^2\subset R$ and $N(I)^2=N(\alpha^{-1})$, there exists an isometry over $\mathbb{Q}_p$ from $(L,\langle\,,\rangle_\alpha)$ to $(U,\langle\,,\rangle_Q)$ that sends I to the self-dual lattice M_0. The image of the multiplication by β operator lies in $V_f(\mathbb{Z}_p)$. Any two such isometries differ by an element in $\mathrm{O}(U)(\mathbb{Z}_p)$. Hence we get a well-defined $\mathrm{O}(U)(\mathbb{Z}_p)$-orbit in $V_f(\mathbb{Z}_p)$. Along with (12), we have proved the first statement.

For the second statement, from the sequence of isometries (7), we see that since $\langle\,,\rangle_\alpha$ is split, there exists $g\in\mathrm{O}(U)(\mathbb{Q}_p^s)$ such that

$$^\sigma\sqrt{\alpha}/\sqrt{\alpha}=g^{-1}\,{}^\sigma g\quad\forall\sigma\in\mathrm{Gal}(k^s/k).$$

Here, the left-hand side is viewed as an element of $\mathrm{Stab}_{\mathrm{O}(U)}(T_f)(k^s)$. The rational orbit corresponding the pair (I,α) is the rational orbit of $T=gT_fg^{-1}$. The rest follows formally from unwinding definitions. □

Suppose the $\mathrm{O}(U)(\mathbb{Z}_p)$-orbit of some $T\in V_f(\mathbb{Z}_p)$ corresponds to the equivalence class of the pair (I,α). Upon identifying R with $\mathbb{Z}_p[T]$, the stabilizer of T in $\mathrm{GL}(U)(\mathbb{Z}_p)$ is $\mathrm{End}_R(I)^\times$. Moreover, as in the proof of Proposition 4, we have

$$\begin{aligned}\mathrm{Stab}_{\mathrm{O}(U)}(T)(\mathbb{Z}_p)&=\mathrm{End}_R(I)^\times[2],\\ \mathrm{Stab}_{\mathrm{SO}(U)}(T)(\mathbb{Z}_p)&=(\mathrm{End}_R(I)^\times[2])_{N=1}.\end{aligned}$$

The stabilizer of T in the group $\mathrm{PO}(U)(\mathbb{Z}_p)$ (and $\mathrm{PSO}(U)(\mathbb{Z}_p)$) is slightly complicated because $\mathrm{PO}(U)(\mathbb{Z}_p)$ contains $\mathrm{O}(U)(\mathbb{Z}_p)/\mu_2$ as a subgroup with quotient $\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}$. We have the following exact sequences:

$$\begin{aligned}1\to\mathrm{End}_R(I)^\times[2]/\mu_2\to\mathrm{Stab}_{\mathrm{PO}(U)}(T)(\mathbb{Z}_p)\to(R^{\times 2}\cap\mathbb{Z}_p^\times)/\mathbb{Z}_p^{\times 2}\to 1,\\ 1\to(\mathrm{End}_R(I)^\times[2])_{N=1}/\mu_2\to\mathrm{Stab}_{\mathrm{PSO}(U)}(T)(\mathbb{Z}_p)\to(R^{\times 2}\cap\mathbb{Z}_p^\times)/\mathbb{Z}_p^{\times 2}\to 1.\end{aligned}\tag{13}$$

Proof of Proposition 12. First note that it suffices to show that the $\mathrm{PO}(U)(\mathbb{Q}_p)$-orbit of T contains an integral representative. Since T is soluble, there exists some $[D]\in J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ such that $\widetilde{\alpha}=\delta'([D])\in(L^\times/L^{\times 2}\mathbb{Q}_p^\times)_{N=1}$ corresponds to the $\mathrm{PO}(U)(\mathbb{Q}_p)$-orbit of T. By [Wan13b, Lemma 3.8], there exist non-Weierstrass non-infinity points $Q_1,\dots,Q_m\in C(\mathbb{Q}_p^s)$, with $m\leqslant n+1$, such that

$$[D]=(Q_1)+\cdots+(Q_m)-m(\infty)\mod 2J(\mathbb{Q}_p)\cdot\langle(\infty')-(\infty)\rangle.\tag{14}$$

Write each $Q_i=(x_i,y_i)\in C(\mathcal{O}_{\mathbb{Q}_p^s})$. Then $\alpha=(x_1-\beta)\cdots(x_m-\beta)$ is a lift of $\widetilde{\alpha}$ to $L^\times$. We claim that either the $\mathrm{O}(U)(\mathbb{Q}_p)$-orbit of T corresponding to the image of α in $L^\times/L^{\times 2}$ has an integral representative, or $[D]$ can be expressed in the form (14) with m replaced by $m-2$. Applying induction on m completes the proof.

The claim follows verbatim from the proof of [BG13, Proposition 8.5]. We give a quick sketch here. Let $r(x)\in\mathbb{Q}_p[x]$ be a polynomial of degree at most $m-1$ such that, for all i, $r(x_i)=y_i$, and let

$$p(x)=(x-x_1)\cdots(x-x_m)\in\mathbb{Z}_p[x].$$

Now $p(x)$ divides $r(x)^2-f(x)$ in $\mathbb{Q}_p[x]$ and we denote the quotient by $q(x)$. By definition, $\alpha=(-1)^mP(\beta)$. If the polynomial $r(x)\in\mathbb{Z}_p[x]$, then the ideal $I=(1,r(\beta)/\alpha)$ does the job.

https://doi.org/10.1112/S0010437X17007515

Note that $\alpha I^2 = (\alpha, r(\beta), q(\beta))$. The integrality assumption of $r(x)$ is used to show that $r(\beta), q(\beta) \in R$. A computation of ideal norms shows that $N(I)^2 = N(\alpha)^{-1}$.

When $r(x)$ is not integral, a Newton polygon analysis on $f(x) - r(x)^2$ shows that $\mathrm{div}(y - r(x)) - [D]$ has the form $D^* + E$ with D^*, $E \in J(\mathbb{Q}_p)$, where D^* can be expressed in (14) with m replaced by $m - 2$ and the x-coordinates of the non-infinity points in E have negative valuation. The condition of divisibility on the coefficients of $f(x)$ ensures that $E \in 2J(\mathbb{Q}_p) \cdot ((\infty') - (\infty))$, or equivalently $(x - \beta)(E) \in L^{\times 2}\mathbb{Q}_p^{\times}$. □

Proof of Proposition 14. Once again, it suffices to work with $\mathrm{PO}(U)$-orbits instead of $\mathrm{PSO}(U)$-orbits directly. The assumption on $\Delta(f)$ implies that R is the maximal order. Hence there is a bijection between $\mathrm{O}(U)(\mathbb{Z}_p)$-orbits and $(R^{\times}/R^{\times 2})_{N=1}$. Note that over non-archimedean local fields, the splitness of the quadratic form is automatic from the existence of a self-dual lattice. Taking flat cohomology over $\mathrm{Spec}(\mathbb{Z}_p)$ of the sequence

$$1 \to \mu_2 \to \mathrm{O}(U) \to \mathrm{PO}(U) \to 1$$

gives:

$$1 \to \mathrm{O}(U)(\mathbb{Z}_p)/\pm 1 \to \mathrm{PO}(U)(\mathbb{Z}_p) \to \mathbb{Z}_p^{\times}/\mathbb{Z}_p^{\times 2} \to 1.$$

Hence $\mathrm{PO}(U)(\mathbb{Z}_p)$-orbits correspond bijectively to $(R^{\times}/R^{\times 2}\mathbb{Z}_p^{\times})_{N=1}$.

On the other hand, the assumption on $\Delta(f)$ implies that the projective closure $\mathcal{C}$ (in weighted projective space) of the hyperelliptic curve C defined by affine equation $y^2 = f(x)$ over $\mathrm{Spec}(\mathbb{Z}_p)$ is regular. Since the special fiber of $\mathcal{C}$ is geometrically reduced and irreducible, the Neron model $\mathcal{J}$ of its Jacobian $J_{\mathbb{Q}_p}$ is fiberwise connected [BLR90, § 9.5, Theorem 1] and its 2-torsion $\mathcal{J}[2]$ is isomorphic to $(\mathrm{Res}_{R/\mathbb{Z}_p}\mu_2)_{N=1}/\mu_2$. Using diagram (11) after replacing L, k, J by $R, \mathbb{Z}_p, \mathcal{J}$, we see that the vertical maps are all isomorphisms and δ' maps $\mathcal{J}(\mathbb{Z}_p)/2\mathcal{J}(\mathbb{Z}_p)$ surjectively to $(R^{\times}/R^{\times 2}\mathbb{Z}_p^{\times})_{N=1}$. The Neron mapping property implies that $\mathcal{J}(\mathbb{Z}_p)/2\mathcal{J}(\mathbb{Z}_p) = J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$.

Suppose the $\mathrm{O}(U)(\mathbb{Z}_p)$-orbit of some $T \in V_f(\mathbb{Z}_p)$ corresponds to an equivalence class of pair (I, α). Since R is maximal, we have $\mathrm{End}_R(I) = R$. Since $R^{\times}[2] = L^{\times}[2]$, we see from (13) that it remains to compare $(R^{\times 2} \cap \mathbb{Z}_p^{\times})/\mathbb{Z}_p^{\times 2}$ with $(L^{\times 2} \cap \mathbb{Q}_p^{\times})/\mathbb{Q}_p^{\times 2}$. These two groups are only non-trivial when L contains a quadratic extension K' of $\mathbb{Q}_p$. The condition $p^2 \nmid \Delta(f)$ implies that $K' = \mathbb{Q}_p(\sqrt{u})$ can only be the unramified quadratic extension of $\mathbb{Q}_p$. In other words, u can be chosen to be a unit in $\mathbb{Z}_p^{\times}$. Hence in this case $(L^{\times 2} \cap \mathbb{Q}_p^{\times})/\mathbb{Q}_p^{\times 2}$ and $(R^{\times 2} \cap \mathbb{Z}_p^{\times})/\mathbb{Z}_p^{\times 2}$ are both equal to the group of order 2 generated by the class of u. □

3. Interpretation using pencils of quadrics

In this section, we give geometric meanings to the notions of distinguished and soluble. For the proof of all the statements below, see [Wan13a, § 2.2]. These geometric interpretations are not necessary if one wants only the average size of the 2-Selmer groups.

Let k be a field of characteristic not equal to 2 and let $f(x)$ be a monic separable polynomial of degree $2n + 2$. Let C denote the monic even hyperelliptic curve defined by $y^2 = f(x)$ and let ∞ and ∞' denote the two points above infinity. Let T be a self-adjoint operator in $V_f(k)$. One has a pencil of quadrics in U spanned by the following two quadrics:

$$Q(v) = \langle v, v \rangle_Q,$$
$$Q_T(v) = \langle v, Tv \rangle_Q.$$

This pencil is generic in the sense that there are precisely $2n + 2$ singular quadrics among $x_1 Q - x_2 Q_T$ for $[x_1, x_2] \in \mathbb{P}^1$, and that they are all simple cones. Its associated hyperelliptic

https://doi.org/10.1112/S0010437X17007515

curve C' is the curve parameterizing the rulings of the quadrics in the pencil. A ruling of a quadric Q_0 is a connected component of the Lagrangian variety of maximal isotropic subspaces. When Q_0 is a simple cone, there is only one ruling. When Q_0 is non-degenerate, there are two rulings defined over $k(\sqrt{\operatorname{disc}(Q_0)})$. To give a point on C' is the same as giving a quadric in the pencil along with a choice of ruling. Therefore, the curve C' is isomorphic over k to the hyperelliptic curve

$$y^2 = \operatorname{disc}(xQ - Q_T) = \operatorname{disc}(Q)\det(xI - T) = f(x),$$

canonical up to the hyperelliptic involution.

We fix an isomorphism between C' and C as follows. Recall the model space $(L, \langle\,,\rangle)$ defined in § 2.2 where $L = k[x]/(f(x)) = k[\beta]$ and $\langle\,,\rangle$ is the bilinear form on L defined by

$$\langle\lambda, \mu\rangle := \text{coefficient of } \beta^{2n+1} \quad \text{in } \lambda\mu = \operatorname{Tr}_{L/k}(\lambda\mu/f'(\beta)).$$

This form is split since the $(n+1)$-plane $Y = \operatorname{Span}\{1, \beta, \ldots, \beta^n\}$ is isotropic. We fix an isometry $\iota : (L, \langle\,,\rangle) \to (U, \langle\,,\rangle_Q)$. Let Y_0 denote ruling on Q containing the isotropic $(n+1)$-plane $\iota(Y)$. We fix an isomorphism $C' \simeq C$ so that the ruling Y_0 corresponds to $\infty \in C(k)$.

Since C has a rational point, the Fano variety F_T of n-planes isotropic with respect to both quadrics is a torsor of J of order dividing 2. In fact, it fits inside a disconnected algebraic group

$$J \dot\cup F_T \dot\cup \operatorname{Pic}^1(C) \dot\cup F_T'$$

where $F_T' \simeq F_T$ as varieties. Using the point ∞, one obtains a lift of F_T to a torsor of $J[2]$ by taking

$$\begin{aligned} F_T[2]_\infty &= \{X \in F_T \mid X + X = (\infty)\} \\ &= \{X \ n\text{-plane} \mid \operatorname{Span}\{X, TX\} \text{ is an isotropic } (n+1)\text{-plane in the ruling } Y_0\}. \end{aligned}$$

The second equality is [Wan13a, Proposition 2.32].

The group scheme $G = \operatorname{PSO}(U)$ acts on the k-scheme

$$W_f = \{(T, X) \mid T \in V_f, X \in F_T[2]_\infty\}$$

via $g \cdot (T, X) = (gTg^{-1}, gX)$. Let W_T denote the fiber above any fixed $T \in V_f(k)$. This action is simply transitive on k-points [Wan13a, Corollary 2.36]. Hence for any $T \in V_f(k)$, the above action induces a simply transitive action of $J[2] \simeq \operatorname{Stab}_G(T)$ on the fiber $W_T = F_T[2]_\infty$.

THEOREM 16 ([Wan13a, Proposition 2.38], [Wan13b, Lemma 2.19]). *These two actions of $J[2]$ coincide, and as elements of $H^1(k, J[2])$,*

$$[F_T[2]_\infty] = [W_T] = c_T, \tag{15}$$

where $c_T \in H^1(k, J[2])$ is defined in (2).

Theorem 16 gives a geometric realization of torsors of $J[2]$ using pencils of quadrics. For hyperelliptic curves with a rational Weierstrass point, one can obtain all torsors of $J[2]$ using pencils of quadrics [Wan13b, Proposition 2.11]. For hyperelliptic curves with no rational Weierstrass point but with a rational non-Weierstrass point, not all torsors of $J[2]$ arise as some $F_T[2]_\infty$ coming from a pencil of quadrics, but all of them that correspond to $\operatorname{PSO}(U)(k)$-orbits do.

https://doi.org/10.1112/S0010437X17007515

Suppose $T \in V_f(k)$. From (15), we see that there exists a k-rational n-plane X such that $\mathrm{Span}\{X, TX\}$ is an isotropic $(n+1)$-plane if and only if at least one of $[F_T[2]_\infty]$ and $[F_T[2]_{\infty'}]$ is trivial. Again by (15), this is equivalent to c_T being in the image of the subgroup generated by $(\infty') - (\infty) \in J(k)/2J(k)$ under the Kummer map $J(k)/2J(k) \hookrightarrow H^1(k, J[2])$. Commutativity of the top left square in (11) implies that this is in turn equivalent to c_T mapping to 0 in $H^1(k, \mathrm{Stab}_{\mathrm{PO}(U)}(T))$. Finally, this is equivalent to T being distinguished. We have therefore proved Proposition 6.

Since $[F_T[2]_\infty]$ maps to $[F_T]$ under the canonical map $H^1(k, J[2]) \to H^1(k, J)[2]$, we see that T is soluble if and only if $F_T(k) \neq \emptyset$. This equivalence of solubility and the existence of rational points is the main reason why the name 'soluble' is used. Likewise, T is locally soluble if and only if $F_T(k_\nu) \neq \emptyset$ at all places ν.

We now give a complete proof for the claim that if $\alpha \in (L^\times/L^{\times 2}k^\times)_{N=1}$ lies in the image of δ', then $\langle\,,\rangle_\alpha$ is split. Consider the pencil of quadrics in L spanned by the following two quadrics:

$$Q_\alpha(\lambda) = \langle \lambda, \lambda\rangle_\alpha,$$
$$Q'_\alpha(\lambda) = \langle \lambda, \beta\lambda\rangle_\alpha.$$

This pencil is once again generic, its associated hyperelliptic curve C_α is smooth of genus n isomorphic non-canonically to the hyperelliptic curve defined by affine equation

$$y^2 = \mathrm{disc}(xQ_\alpha - Q'_\alpha) = N_{L/k}(\alpha) f(x).$$

Since $N_{L/k}(\alpha) \in k^{\times 2}$, the curve C_α is isomorphic to C over k. Fix any isomorphism $C'_\alpha \simeq C$. The Fano variety F_α of n-planes isotropic with respect to both quadrics is a torsor of J of order dividing 2. There are two natural lifts of F_α to torsors of $J[2]$ by taking

$$F_\alpha[2]_\infty = \{X \in F \mid X + X = (\infty)\} \quad \text{or} \quad F_\alpha[2]_{\infty'} = \{X \in F \mid X + X = (\infty')\}.$$

As elements of $H^1(k, J[2])$, these two lifts map to the same class in $H^1(k, \mathrm{Res}_{L/k}\mu_2/\mu_2)$. The class α also maps to a class in $H^1(k, \mathrm{Res}_{L/k}\mu_2/\mu_2)$ as in (11). By [Wan13b, Proposition 2.27], these two classes coincide. Suppose $\alpha = \delta'([D])$ comes from $J(k)/2J(k)$. Then one of these two lifts recovers $[D]$ and hence $F_\alpha(k) \neq \emptyset$. Pick any $X \in F_\alpha(k)$. If $X + X = (\infty)$, then $[D] = 0$, $\alpha = 1$ and $\langle\,,\rangle$ is split. Otherwise, $\mathrm{Span}\{X, (\infty) - X\}$ is a k-rational $(n+1)$-plane isotropic with respect to $\langle\,,\rangle_\alpha$ implying again that $\langle\,,\rangle_\alpha$ is split.

4. Orbit counting

In this section, we let the polynomial $f(x)$ vary in the family of monic polynomials of degree $2n+2$ over $\mathbb{Z}$ whose x^{2n+1}-coefficient is 0 and count the average number of locally soluble orbits of the action of $G(\mathbb{Q})$ on $V_f(\mathbb{Q})$. We redefine V to be the following scheme over $\mathbb{Z}$:

$$V = \{B \in M_{(2n+2)\times(2n+2)} \mid B = B^t, B \text{ has anti-trace } 0\} \simeq \mathbb{A}^{2n^2+5n+2}_{\mathbb{Z}},$$

consisting of symmetric $(2n+2)\times(2n+2)$ matrices with anti-trace 0. Recall that the anti-trace is the sum of the entries on the anti-diagonal. We impose the extra condition on the anti-trace since the x^{2n+1}-coefficients of our polynomials are 0. One passes between self-adjoint operators T and symmetric matrices B via the relation $B = AT$. This change of perspective is only to simplify notation in what follows. We view elements of the group SO_{2n+2} also as $(2n+2)\times(2n+2)$ matrices using the standard basis defined in (4). The group $G = \mathrm{PSO}_{2n+2}$ acts on V by $g \cdot B := gBg^t$. The ring of polynomial invariants for this action is freely generated by the coefficients $c_2, \ldots, c_{2n+2}$

https://doi.org/10.1112/S0010437X17007515

of the *invariant polynomial* $\det(Ax - By)$. Indeed, Proposition 4 implies that there are no other independent polynomial invariants, and the existence of a self-adjoint operator T_f with any given characteristic polynomial $f(x)$ obtained in § 2.2 shows that there are no relations among these invariants. We define the scheme S to be

$$S = \operatorname{Spec} \mathbb{Z}[c_2, \dots, c_{2n+2}].$$

The map $\pi : V \to S$ is given by the coefficients of the invariant polynomial; we call $\pi(B)$ the invariant of B.

A point $c = (c_2, \dots, c_{2n+2}) \in S(\mathbb{R})$ corresponds to a monic polynomial

$$f_c(x) := x^{2n+2} + c_2 x^{2n} + \cdots + c_{2n+2}.$$

We define its height $H(f_c)$ by

$$H(f_c) := H(c) := \max\{|c_k|^{1/k}\}_{k=2}^{2n+2}.$$

The height of $B \in V(\mathbb{R})$ is defined to be the height of $\pi(B)$, and the height of the hyperelliptic curve $C(c)$ given by $y^2 = f_c(x)$ is defined to be $H(c)$.

For each prime p, let Σ_p be a closed subset of $S(\mathbb{Z}_p)\backslash\{\Delta = 0\}$ whose boundary has measure 0. Let Σ_∞ be the set of all $c \in S(\mathbb{R})\backslash\{\Delta = 0\}$ such that the corresponding polynomial f_c has m distinct pairs of complex conjugate roots, where m belongs to a fixed subset of $\{0, \dots, n+1\}$. To such a collection $(\Sigma_\nu)_\nu$ we associate the family $F = F_\Sigma$ of monic even hyperelliptic curves, where $C(c) \in F$ if and only if $c \in \Sigma_\nu$ for all places ν. Such a family is said to be *defined by congruence conditions*.

Given a family F of monic even hyperelliptic curves defined by congruence conditions, let $\mathrm{Inv}(F) \subset S(\mathbb{Z})$ denote the set of coefficients of the defining affine equations. We denote the p-adic closure of $\mathrm{Inv}(F)$ in $S(\mathbb{Z}_p)\backslash\{\Delta = 0\}$ by $\mathrm{Inv}_p(F)$. We say that a family F defined by congruence conditions is *large at* p if $\mathrm{Inv}_p(F)$ contains every element $c \in S(\mathbb{Z}_p)$ such that $p^2 \nmid \Delta(c)$. Finally, we say that F and $\mathrm{Inv}(F)$ are *large* if F is large at all but finitely many primes. An example of a large subset of $S(\mathbb{Z})$ is the set

$$F_0 = \{(c_2, \dots, c_{2n+2}) \in S(\mathbb{Z}) \mid p^{2k} \nmid c_k, \forall k = 2, \dots, 2n+2, \forall p, \text{prime}\}.$$

Another example is the set of elements in $S(\mathbb{Z})$ having squarefree discriminant.

In this section, our goal is to prove the following strengthening of Theorem 2.

THEOREM 17. *When all hyperelliptic curves over $\mathbb{Q}$ of genus n with a marked rational non-Weierstrass point in any large family are ordered by height, the average size of the 2-Selmer groups of their Jacobians is at most 6.*

In view of the correspondence (Theorem 11) between locally soluble orbits and 2-Selmer elements, the above result is an immediate consequence of the following theorem.

THEOREM 18. *The average number of locally soluble orbits for the action of $G(\mathbb{Q})$ on $V_f(\mathbb{Q})$ as f runs through any large subset of $S(\mathbb{Z})$, when ordered by height, is at most 6.*

This section is organized as follows. First, in § 4.1, we construct fundamental domains for the action of $G(\mathbb{Z})$ on the set of $\mathbb{R}$-soluble elements in $V(\mathbb{R})$. In § 4.2, we then use geometry-of-numbers techniques developed by Bhargava to determine the asymptotics for the number of $\mathbb{R}$-soluble $G(\mathbb{Z})$-orbits on non-distinguished elements in $V(\mathbb{Z})$ having non-zero discriminant and bounded height. In § 4.3, we bound the number of *weighted* $G(\mathbb{Z})$-orbits, where the weights are products of p-adic weights over all p. We also determine the number of monic even hyperelliptic curves having bounded height in any large family. Finally, in § 4.4, we deduce Theorem 18.

https://doi.org/10.1112/S0010437X17007515

4.1 Construction of fundamental domains

Let $V(\mathbb{R})^{\mathrm{sol}}$ denote the set of $\mathbb{R}$-soluble elements in $V(\mathbb{R})$ having non-zero discriminant. We partition $V(\mathbb{R})^{\mathrm{sol}}$ into $n+2$ sets,

$$V(\mathbb{R})^{\mathrm{sol}} = \bigcup_{m=0}^{n+1} V(\mathbb{R})^{(m)},$$

where $V(\mathbb{R})^{(m)}$ consists of elements $B \in V(\mathbb{R})^{\mathrm{sol}}$ such that the polynomial corresponding to $\pi(B)$ has m pairs of complex conjugate roots (and $2n+2-2m$ real roots). In this subsection, our goal is to describe convenient fundamental domains for the action of $G(\mathbb{Z})$ on $V(\mathbb{R})^{(m)}$ for $m \in \{0, \dots, n+1\}$.

4.1.1 *Fundamental sets for the action of $G(\mathbb{R})$ on $V(\mathbb{R})^{\mathrm{sol}}$.* First, we construct convenient fundamental sets for the action of $G(\mathbb{R})$ on $V(\mathbb{R})^{(m)}$. Let $S(\mathbb{R})^{(m)}$ denote the set of elements $c \in S(\mathbb{R})\backslash\{\Delta = 0\}$ such that the corresponding polynomial has m pairs of complex conjugate roots. There exists an algebraic section $\kappa : S \to V$ defined over $\mathbb{Z}[1/2]$ such that every element in the image of $S(\mathbb{R})\backslash\{\Delta = 0\}$ under κ is distinguished [Wan13b, § 3.1]. The number of $\mathbb{R}$-soluble $G(\mathbb{R})$-orbits in $V_{f_c}(\mathbb{R})$, for $c \in S(\mathbb{R})^{(m)}$, depends only on m. We denote it by τ_m. There exist elements $g_1, \dots, g_{\tau_m} \in \mathrm{GL}(U)(\mathbb{R})$ such that the set

$$R'^{(m)} := \bigcup_i g_i \kappa(S(\mathbb{R})^{(m)}) g_i^{-1} \tag{16}$$

is a fundamental set for $G(\mathbb{R})\backslash V(\mathbb{R})^{(m)}$. Indeed, since $L := \mathbb{R}[x]/(f_c(x))$ is independent of $c \in S(\mathbb{R})^{(m)}$, an element $g \in \mathrm{GL}(U)(\mathbb{R})$ that conjugates $\kappa(c_0)$, for any fixed $c_0 \in S(\mathbb{Q})^{(m)}$, to a $G(\mathbb{R})$-orbit corresponding to a class $\alpha \in (L^\times/L^{\times 2}\mathbb{R}^\times)_{N=1}$ does so for every $c \in S(\mathbb{R})^{(m)}$.

We now construct our fundamental set $R^{(m)}$ for $G(\mathbb{R})\backslash V(\mathbb{R})^{(m)}$ to be

$$R^{(m)} := \mathbb{R}_{>0} \cdot \{B \in R'^{(m)} : H(B) = 1\}. \tag{17}$$

The reason why we use the set $R^{(m)}$ instead of $R'^{(m)}$ is that the sizes of the coefficients of elements in $R^{(m)}$ having height X are bounded by $O(X^{1/d})$, where $d = (2n+2)(2n+1)$ is the degree of the height function. This follows because the elements in $R'^{(m)}$ having height 1 lie in a bounded subset of $V(\mathbb{R})$.

4.1.2 *Fundamental domains for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$.* We now describe Borel's construction [Bor62] of a fundamental domain $\mathcal{F}$ for the left action of $G(\mathbb{Z})$ on $G(\mathbb{R})$. Since $G(\mathbb{R}) = \mathrm{SO}(U)(\mathbb{R})/\{\pm 1\}$, and $\{\pm 1\} \subset \mathrm{SO}(U)(\mathbb{Z})$, the image in $G(\mathbb{R})$ of a fundamental domain for $\mathrm{SO}(U)(\mathbb{Z})\backslash \mathrm{SO}(U)(\mathbb{R})$ will map bijectively onto a fundamental domain for $G(\mathbb{Z})\backslash G(\mathbb{R})$. We will abuse notation and refer to both fundamental domains by $\mathcal{F}$. Let $\mathrm{SO}(U)(\mathbb{R}) = NTK$ be the Iwasawa decomposition of $\mathrm{SO}(U)(\mathbb{R})$. Here, N denotes the set of unipotent lower triangular matrices, T denotes the set of diagonal matrices, and K is a maximal compact subgroup. Then the fundamental domain $\mathcal{F}$ may be expressed in the form

$$\mathcal{F} := \{utk \mid u \in N'(t), t \in T', k \in K\} \subset N'T'K,$$

where $N' \subset N$ is a bounded set, $N'(t) \subset N'$ is a measurable set depending on $t \in T'$, and $T' \subset T$ is given by

$$T' := \{\mathrm{diag}(t_1^{-1}, t_2^{-1}, \dots, t_{n+1}^{-1}, t_{n+1}, \dots, t_1) \mid t_1/t_2 > c, \dots, t_n/t_{n+1} > c, t_n t_{n+1} > c\},$$

for some constant $c > 0$.

https://doi.org/10.1112/S0010437X17007515

4.1.3 *Fundamental domains for the action of $G(\mathbb{Z})$ on $V(\mathbb{R})^{\mathrm{sol}}$.* For $h \in G(\mathbb{R})$, we regard $\mathcal{F}h \cdot R^{(m)}$ as a multiset, where the multiplicity of B in $\mathcal{F}h \cdot R^{(m)}$ is given by $\#\{g \in \mathcal{F} \mid B \in gh \cdot R^{(m)}\}$. The $G(\mathbb{Z})$-orbit of any $B \in V(\mathbb{R})$ is represented $\#\mathrm{Stab}_{G(\mathbb{R})}(B)/\#\mathrm{Stab}_{G(\mathbb{Z})}(B)$ times in this multiset $\mathcal{F}h \cdot R^{(m)}$.

The group $\mathrm{Stab}_{G(\mathbb{Z})}(B)$ is non-trivial only for a set of measure 0 in $V(\mathbb{R})^{(m)}$. Indeed, $G(\mathbb{Z})$ is countable and every non-trivial element $g \in G(\mathbb{Z})$ only fixes a set of measure 0 in $V(\mathbb{R})$. (Later on, in Proposition 23, we will show that the number of $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ having a non-trivial stabilizer in $G(\mathbb{Z})$ is negligible.) The size $\#\mathrm{Stab}_{G(\mathbb{R})}(B)$ is constant over $B \in V(\mathbb{R})^{(m)}$. We denote it by $\#J^{(m)}[2](\mathbb{R})$. Therefore, the multiset $\mathcal{F}h \cdot R^{(m)}$ is a cover of a fundamental domain for $G(\mathbb{Z})$ on $V(\mathbb{R})^{(m)}$ (aside from a set of measure 0) of degree $\#J^{(m)}[2](\mathbb{R})$.

4.2 Averaging, cutting off the cusp, and estimation in the main body

An element $B \in V(\mathbb{Q})$ is said to be *irreducible* if it has non-zero discriminant and it is not distinguished. For any $G(\mathbb{Z})$-invariant set $\mathcal{L} \subset V(\mathbb{Z})^{(m)} := V(\mathbb{R})^{(m)} \cap V(\mathbb{Z})$, let $N(\mathcal{L}; X)$ denote the number of irreducible $G(\mathbb{Z})$-orbits of $\mathcal{L}$ that have height bounded by X, where each orbit $G(\mathbb{Z}) \cdot B$ is weighted by $1/\#\mathrm{Stab}_{G(\mathbb{Z})}(B)$. The result of the previous section shows that we have

$$N(\mathcal{L}; X) = \frac{1}{\#J^{(m)}[2](\mathbb{R})} \#\{\mathcal{F}hR^{(m)}(X) \cap \mathcal{L}^{\mathrm{irr}}\}$$

for any h in $G(\mathbb{R})$, where $R^{(m)}(X)$ denotes the elements in $R^{(m)}$ having height bounded by X and $\mathcal{L}^{\mathrm{irr}}$ denotes the set of irreducible elements in $\mathcal{L}$. Let G_0 be a bounded open K-invariant non-empty semialgebraic set in $G(\mathbb{R})$. Averaging the above equation over $h \in G_0$, we obtain

$$N(\mathcal{L}; X) = \frac{1}{\#J^{(m)}[2](\mathbb{R})\,\mathrm{Vol}(G_0)} \int_{h \in G_0} \#\{\mathcal{F}hR^{(m)}(X) \cap \mathcal{L}^{\mathrm{irr}}\}\, dh, \tag{18}$$

for any Haar measure dh on $G(\mathbb{R})$, and where the volume of G_0 is computed with respect to dh. Note that since G is reductive, every Haar measure is both left- and right-invariant. We may use (18) to define $N(\mathcal{L}; X)$ when $\mathcal{L}$ is not $G(\mathbb{Z})$-invariant. This could be useful to estimate the number of $G(\mathbb{Z})$-orbits having bounded height on a $G(\mathbb{Z})$-invariant set which is not a lattice, but which can be partitioned into a union of lattices each of which is not necessarily $G(\mathbb{Z})$-invariant. Note that if $\mathcal{L}$ is not $G(\mathbb{Z})$-invariant, then our definition of $N(\mathcal{L}; X)$ depends on G_0 and on the choice of the fundamental domain $\mathcal{F}$.

By an argument identical to the proof of [BS15, Theorem 2.5], we obtain

$$N(\mathcal{L}; X) = \frac{1}{\#J^{(m)}[2](\mathbb{R})\,\mathrm{Vol}(G_0)} \int_{h \in \mathcal{F}} \#\{hG_0R^{(m)}(X) \cap \mathcal{L}^{\mathrm{irr}}\}\, dh. \tag{19}$$

To estimate the number of integral points in the bounded region $hG_0R^{(m)}(X)$, we use the following result of Davenport [Dav51].

PROPOSITION 19. *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m and defined by at most k polynomial inequalities each having degree at most ℓ. Then the number of integral lattice points (counted with multiplicity) contained in the region $\mathcal{R}$ is*

$$\mathrm{Vol}(\mathcal{R}) + O(\max\{\mathrm{Vol}(\bar{\mathcal{R}}), 1\}),$$

https://doi.org/10.1112/S0010437X17007515

where $\mathrm{Vol}(\bar{\mathcal{R}})$ *denotes the greatest* d*-dimensional volume of any projection of* $\mathcal{R}$ *onto a coordinate subspace obtained by equating* $n-d$ *coordinates to zero, where* d *takes all values from* 1 *to* $n-1$*. The implied constant in the second summand depends only on* n*,* m*,* k*, and* ℓ*.*

The set $hG_0R^{(m)}(X)$ is a bounded region on which Proposition 19 may be applied. We can express any $h \in \mathcal{F}$ as $h = utk$, where $u \in N'$, $t \in T'$, and $k \in K$. As t grows in T', the estimates on the number of integral points in $hG_0R^{(m)}(X)$ obtained from Proposition 19 get worse and worse. Indeed, when t gets high enough (in the cusp of T'), the top left entry b_{11} of every element in $hG_0R^{(m)}(X)$ will be less than 1 in absolute value, at which point the error term in Proposition 19 dominates the main term. As t gets bigger, other entries start becoming less than 1 in absolute value and we get even worse estimates. To deal with this problem, we break $V(\mathbb{R})$ up into two pieces: the main body, which contains all elements $B \in V(\mathbb{R})$ with $|b_{11}| \geqslant 1$; and the cusp region, which contains all elements $B \in V(\mathbb{R})$ with $|b_{11}| < 1$. As t gets bigger, more and more coefficients of the integral elements of $hG_0R^{(m)}(X)$ will become 0. Using Proposition 7, we know that once enough entries of B are 0, it will become distinguished and thus reducible. In Proposition 21 we compute the number of irreducible integral points in the cusp region, and in Proposition 23 we compute the number of reducible integral points in the main body. They are both negligible when compared to the number of integral points in the main region, and as a result we will prove the following theorem.

Theorem 20. *We have for any* $m = 0, \dots, n+1$,

$$N(V(\mathbb{Z})^{(m)}; X) = \frac{1}{\#J^{(m)}[2](\mathbb{R})} \mathrm{Vol}(\mathcal{F} \cdot R^{(m)}(X)) + o(X^{(\dim V)/d}).$$

In § 4.4, we show that $\mathrm{Vol}(\mathcal{F} \cdot R^{(m)}(X))$ grows on the order of $X^{(\dim V)/d}$ so the error term is indeed smaller than the main term.

Let $V(\mathbb{Z})(b_{11} = 0)$ denote the set of points $B \in V(\mathbb{Z})$ such that $b_{11} = 0$. Then we have the following proposition.

Proposition 21. *With notation as above, we have* $N(V(\mathbb{Z})(b_{11} = 0); X) = O_\epsilon(X^{(\dim V - 1)/d + \epsilon})$.

Proof. It will be convenient to use the following parameters for T:

$$\begin{aligned} s_i &= t_i/t_{i+1} \quad \text{for } i = 1, \dots, n; \\ s_{n+1} &= t_n t_{n+1}. \end{aligned}$$

The condition for $t \in T'$ translates to $s_i > c$ for all i. We pick the following Haar measure dh on $G(\mathbb{R}) = NTK$:

$$\begin{aligned} dh &= du \prod_{j=1}^{n-1} s_j^{j(j-2n-1)} \cdot (s_n s_{n+1})^{-n(n+1)/2} d^\times s_j \, dk \\ &= du \delta(s) d^\times s \, dk, \end{aligned} \tag{20}$$

where du is a Haar measure on the unipotent group N, dk is the Haar measure on K normalized so that K has volume 1, $\delta(s)$ denotes $\prod_{j=1}^{n-1} s_j^{j(j-2n-1)} \cdot (s_n s_{n+1})^{-n(n+1)/2}$, and $d^\times s$ denotes $\prod_{j=1}^{n+1} d^\times s_j$ in which each $d^\times s_j = ds_j/s_j$ is the standard Haar measure on $\mathbb{R}^\times$. The conjugation action of T on N breaks up into a direct sum of characters of T. The Haar measure character $\delta(s)$ is the product of the inverses of all the characters of T arising in this decomposition, in order for the measure dh above to be left-invariant.

Then, since G_0 is K-invariant, (19) implies that

$$\begin{aligned} N(V(\mathbb{Z})(b_{11}=0);X) &= O\bigg(\int_{h\in\mathcal{F}} \#\{hG_0R^{(m)}(X)\cap V(\mathbb{Z})(b_{11}=0)\}\,dh\bigg)\\ &= O\bigg(\int_{u\in N'}\int_{t\in T'} \#\{utG_0R^{(m)}(X)\cap V(\mathbb{Z})(b_{11}=0)\}\,\delta(s)\,d^\times s\,du\bigg)\\ &= O\bigg(\int_{t\in T'} \#\{tG_0R^{(m)}(X)\cap V(\mathbb{Z})(b_{11}=0)\}\,\delta(s)\,d^\times s\bigg), \end{aligned} \tag{21}$$

where the final equality follows because N' has finite measure,

$$utG_0R^{(m)}(X) = t(t^{-1}ut)G_0R^{(m)}(X),$$

and the coefficients of $t^{-1}ut$ are bounded independent of $t\in T'$ and $u\in N'$.

Let b_{ij}, with $i\leqslant j$ and $(i,j)\neq(n+1,n+2)$, be the system of coordinates on $V(\mathbb{R})$, where b_{ij} is the (i,j)th entry of the symmetric matrix B. To each coordinate b_{ij} we associate the weight $w(i,j)$, which records how an element $s\in T$ scales b_{ij}. For example,

$$\begin{aligned} w(1,1) &= s_1^{-2}\cdots s_{n-1}^{-2}s_n^{-1}s_{n+1}^{-1}\\ w(i,2n+3-i) &= 1, \quad i=1,\dots,2n+2, \quad \text{coordinates on the anti-diagonal}\\ w(i,2n+2-i) &= s_i^{-1}, \quad i=1,\dots,2n+1, \quad \text{coordinates above the anti-diagonal}\\ w(n+1,n+1) &= s_ns_{n+1}^{-1}. \end{aligned}$$

Let C be an absolute constant such that $CX^{1/d}$ bounds the absolute value of all the coordinates of elements $B\in G_0R^{(m)}(X)$. If, for $(s_1,\dots,s_{n+1})\in T'$, we have $CX^{1/d}\,w(i_0,2n+2-i_0)<1$ for some $i_0\in\{1,\dots,n+1\}$, then $CX^{1/d}\,w(i,j)<1$ for all $i\leqslant i_0, j\leqslant 2n+2-i_0$. Hence the top left $i_0\times(2n+2-i_0)$ block of any integral $B\in tG_0R^{(m)}(X)$ is 0. Just as [BG13, Lemma 10.3] shows, any such B has zero discriminant. Hence, to prove Proposition 21, we may assume

$$s_i\leqslant CX^{1/d},\ i=1,\dots,n; \quad s_{n+1}\leqslant C^2X^{2/d}. \tag{22}$$

We use T_X to denote the set of $t=(s_1,\dots,s_{n+1})\in T'$ satisfying these bounds.

Let U denote the set of pairs of integers (i,j) with $1\leqslant i,j,\leqslant 2n+2$ and $i\leqslant j$. For any subset U_1 of U, let $V(\mathbb{R})(U_1)$ denote the subset of $V(\mathbb{R})$ consisting of elements B whose (i,j)th entry is less than 1 in absolute value when $(i,j)\in U_1$ and at least 1 in absolute value when $(i,j)\notin U_1$. Let $V(\mathbb{Z})(U_1)$ denote the set of integral points in $V(\mathbb{R})(U_1)$. Then to prove Proposition 21, it suffices to show that

$$N(V(\mathbb{Z})(U_1);X) = O_\epsilon(X^{(\dim V-1)/d+\epsilon}), \tag{23}$$

for every set U_1 containing $(1,1)$.

Proposition 19, in conjunction with the argument used to justify (21), implies

$$\begin{aligned} N(V(\mathbb{Z})(U_1);X) &= O\bigg(\int_{t\in T_X}\mathrm{Vol}(tG_0R^{(m)}(X)\cap V(\mathbb{R})(U_1))\,\delta(s)\,d^\times s\bigg)\\ &= O\bigg(X^{(\dim V-\#U_1)/d}\int_{t\in T_X}\prod_{(i,j)\notin U_1} w(i,j)\,\delta(s)\,d^\times s\bigg). \end{aligned}$$

Hence, to prove (23), we need to bound

$$\widetilde{I}(U_1,X) := X^{(\dim V-\#U_1)/d}\int_{t\in T_X}\prod_{(i,j)\notin U_1} w(i,j)\,\delta(s)\,d^\times s, \tag{24}$$

for every set U_1 containing $(1,1)$.

https://doi.org/10.1112/S0010437X17007515

Note that if $i' \leqslant i$ and $j' \leqslant j$, then $w(i', j')$ has smaller exponents in all the s_k than $w(i, j)$. Thus, if a set U_1 contains (i, j) but not (i', j'), then

$$\widetilde{I}(U_1 \backslash \{(i,j)\} \cup \{(i',j')\}, X) \geqslant \widetilde{I}(U_1, X).$$

Hence, for the purpose of obtaining an upper bound for $\widetilde{I}(U_1, X)$, we may assume that if $(i, j) \in U_1$, then $(i', j') \in U_1$ for all $i' \leqslant i$ and $j' \leqslant j$. We say that such a set U_1 is *closed*. If a closed set U_1 contains any element on, or to the right of, the off-anti-diagonal, then every element in $V(\mathbb{Z})(U_1)$ has discriminant 0 and, by definition, $N(V(\mathbb{Z})(U_1); X) = 0$. Let U_0 denote the set of coordinates (i, j) such that $i \leqslant j$ and $i + j \leqslant 2n + 1$. In other words, U_0 contains every coordinate to the left of the off-anti-diagonal. Since every element in $V(\mathbb{Z})(U_0)$ is distinguished (by Proposition 7), hence reducible, it suffices to consider $\widetilde{I}(U_1, X)$ for all $U_1 \subsetneq U_0$.

To this end, as the product of the weights over all coordinates is 1, we define

$$I(U_1, X) = X^{-\#U_1/d} \int_{s_1,\dots,s_n=c}^{CX^{1/d}} \int_{s_{n+1}=c}^{C^2X^{2/d}} \prod_{(i,j)\in U_1} w(i,j)^{-1} \prod_{k=1}^{n-1} s_k^{k(k-2n-1)} \cdot (s_n s_{n+1})^{-n(n+1)/2} \, d^\times s. \tag{25}$$

To complete the proof of Proposition 21, it suffices to prove the following lemma.

Lemma 22. *Let U_1 be non-empty proper closed subset of U_0. Then*

$$I(U_1, X) = O_\epsilon(X^{-1/d+\epsilon}).$$

If $U_1 = U_0$ or $U_1 = \emptyset$, then $I(U_1, X) = O(1)$.

Proof. The proof of this lemma is a combinatorial argument using induction on $n \geqslant 2$. We first compute

$$I(U_0, X) = X^{-n(n+1)/d} \int_{s_1,\dots,s_n=c}^{CX^{1/d}} \int_{s_{n+1}=c}^{C^2X^{2/d}} s_1 s_2^3 \cdots s_{n-1}^{2n-3} s_n^{n-1} s_{n+1}^n \, d^\times s = O(1). \tag{26}$$

This is expected since $V(\mathbb{Z})(U_0)$ contains all but negligibly few distinguished orbits (see Proposition 23). It is also easy to see that $I(\emptyset, X) = O(1)$. Let U_1' denote $U_0 \backslash U_1$, and define $I_n'(U_1', X)$ to equal $I(U_1, X)$. Combining (25) with (26), we obtain

$$\begin{aligned} I_n'(U_1', X) &= I(U_1, X) \\ &= X^{(\#U_1' - n(n+1))/d} \int_{s_1,\dots,s_n=c}^{CX^{1/d}} \int_{s_{n+1}=c}^{C^2X^{2/d}} \prod_{(i,j)\in U_1'} w(i,j) \cdot s_1 s_2^3 \cdots s_{n-1}^{2n-3} s_n^{n-1} s_{n+1}^n \, d^\times s. \end{aligned}$$

Even though we only need the result when $n \geqslant 2$, for the purpose of the induction it is also necessary to work out the case $n = 1$. When $n = 1$, we have $U_0 = \{(1, 1), (1, 2)\}$ and

$$\begin{aligned} I_1(\emptyset, X) &= O(1), \\ I_1(\{(1,1)\}, X) &= O_\epsilon(X^{-1/d+\epsilon}), \\ I_1(U_0, X) &= O_\epsilon(X^\epsilon). \end{aligned}$$

To establish the inductive step, we write $U_1' = U_2' \cup U_3'$ where U_2' is the set of coordinates $(1, j)$ in U_1' and $U_3' = U_1' \backslash U_2'$. Since we have

$$\int_c^{CX^{1/d}} s^k \, d^\times s \ll_{c,C} \int_c^{CX^{1/d}} s^{k_1} \, d^\times s \int_c^{CX^{1/d}} s^{k_2} \, d^\times s$$

https://doi.org/10.1112/S0010437X17007515

for every $k_1 + k_2 = k$, it follows that we may bound $I'_n(U'_1, X)$ by the product

$$I'_n(U'_1, X) \ll_{c,C} J_n(U'_2, X) K_n(U'_3, X),$$

where

$$J_n(U'_2, X) := X^{(\#U'_2 - 2n)/d} \int_{s_1=c}^{CX^{1/d}} \int_{s_2,\dots,s_n=c}^{CX^{1/d}} \int_{s_{n+1}=c}^{C^2X^{2/d}} \prod_{(1,j)\in U'_2} w(1,j)\, s_1 s_2^2 \cdots s_{n-1}^2 s_n s_{n+1}\, d^\times s,$$

$$K_n(U'_3, X) := X^{(\#U'_3 - (n-1)n)/d} \int_{s_2,\dots,s_n=c}^{CX^{1/d}} \int_{s_{n+1}=c}^{C^2X^{2/d}} \prod_{(i,j)\in U'_3} w(i,j)\, s_2 s_3^3 \cdots s_{n-1}^{2n-5} s_n^{n-2} s_{n+1}^{n-1}\, d^\times s.$$

Note that $K_n(U'_3, X) = I'_{n-1}(\{(i,j) : (i+1, j+1) \in U'_3\}, X)$ (which we denote by $I'_{n-1}(U'_3, X)$) and we may estimate it using induction. Since U_1 is closed and non-empty, the subset U'_2 is either empty or of the form $\{(1,k), (1,k+1), \dots, (1,2n)\}$ with $k \geqslant 2$. A direct calculation gives

$$J_n(U'_2, X) = \begin{cases} O(1) & \text{if } U'_2 = \emptyset, \\ O_\epsilon(X^{(-k+1)/d+\epsilon}) & \text{if } 2 \leqslant k \leqslant n+1, \\ O_\epsilon(X^{(k-2n-1)/d+\epsilon}) & \text{if } n+2 \leqslant k \leqslant 2n. \end{cases}$$

Hence we have

$$J_n(U'_2, X) = O_\epsilon(X^{-1/d+\epsilon}), \tag{27}$$

unless $U'_2 = \emptyset$, in which case it is $O(1)$.

Hence, if U'_2 is not empty, then the lemma follows by induction on n (used to bound $I'_{n-1}(U'_3, X)$ by $O_\epsilon(X^\epsilon)$). If U'_2 is empty, then U'_3 must be non-empty since U'_1 is non-empty. If, further, $U'_3 \neq U_0 \backslash \{(1,1), \dots, (1,2n)\}$, then by induction we have $I'_{n-1}(U'_3, X) = O_\epsilon(X^{-1/d+\epsilon})$. The only remaining case is when $U_1 = \{(1,1), \dots, (1,2n)\}$, for which a direct computation yields the result. □

This concludes the proof of Proposition 21. □

We now have the following proposition, whose proof follows that of [Bha10, Lemma 14].

PROPOSITION 23. *Let $V(\mathbb{Z})(\emptyset)^{\mathrm{red}}$ denote the set of elements in $V(\mathbb{Z})$ with $b_{11} \neq 0$ that are not irreducible, and let $V(\mathbb{Z})^{\mathrm{bigstab}}$ denote the set of elements in $V(\mathbb{Z})$ which have a non-trivial stabilizer in $G(\mathbb{Z})$. Then*

$$\int_{G_0} \#\{V(\mathbb{Z})(\emptyset)^{\mathrm{red}} \cap \mathcal{F} g \cdot R^{(m)}(X)\}\, dg = o(X^{(\dim V)/d}),$$

$$N(V(\mathbb{Z})^{\mathrm{bigstab}}; X) = o(X^{(\dim V)/d}).$$

Proof. Observe that if $B \in V(\mathbb{Z})$ is reducible over $\mathbb{Z}$, then the image of B in $V(\mathbb{F}_p)$ is reducible for all p. For any prime p, let ϕ_p denote the p-adic density of the set of elements of $V(\mathbb{Z}_p)$ that are reducible mod p. Then, to prove Proposition 23, it suffices to show

$$\prod_p \phi_p = 0.$$

We show this by proving that ϕ_p is bounded above by some constant less than 1 when p is large enough. For large enough p, there is a positive proportion r_n (depending only on n) of polynomials of degree $2n+2$ over $\mathbb{F}_p$ that factor into two linear terms and an irreducible

https://doi.org/10.1112/S0010437X17007515

polynomial of degree $2n$. Suppose $f(x) \in \mathbb{Z}_p[x]$ with this reduction type over $\mathbb{F}_p$. Since it has a linear factor, Proposition 5 implies that there is one distinguished orbit. Since $H^1(\mathbb{F}_p, J) = 0$ by Lang's theorem, every orbit is soluble. The number of orbits $\#J(\mathbb{F}_p)/2J(\mathbb{F}_p)$ is equal to the size of the stabilizer $\#J[2](\mathbb{F}_p)$. Since $f(x)$ has a factor of degree 2, $\#J[2](\mathbb{F}_p) \geqslant 2$. Therefore at least half of the elements in $V_f(\mathbb{F}_p)$ are not distinguished. Hence, for p large enough, $\phi_p \leqslant 1 - \frac{1}{2}r_n < 1$.

We use the same technique to prove the second claim in Proposition 23. For p large enough, there is a positive proportion r'_n (depending only on n) of polynomials of degree $2n+2$ over $\mathbb{F}_p$ that factors into a linear term and an irreducible polynomial of degree $2n+1$. If $B \in V_f(\mathbb{Z}_p)$ where $f(x)$ has this reduction type mod p, then p does not divide the discriminant of $f(x)$. As a consequence, the hyperelliptic curve $y^2 = f(x)$ is smooth over $\mathrm{Spec}(\mathbb{Z}_p)$ and the 2-torsion of its Jacobian $J[2]$ is a finite étale group scheme over $\mathrm{Spec}(\mathbb{Z}_p)$. From the reduction type of $f(x)$ over p, we see that $\#J[2](\mathbb{Q}_p) = \#J[2](\mathbb{F}_p) = 1$. Denote by ϕ_p the p-adic density of the set of elements of $V(\mathbb{Z}_p)$ with non-trivial stabilizer in $G(\mathbb{Q}_p)$. Then we have shown that $\phi_p \leqslant 1 - r'_n < 1$ for p sufficiently large. This completes the proof. □

We may now prove the main result of this section, which we state again for the convenience of the reader.

Theorem 24. *We have, for any $m = 0, \dots, n+1$,*

$$N(V(\mathbb{Z})^{(m)}; X) = \frac{1}{\#J^{(m)}[2](\mathbb{R})} \operatorname{Vol}(\mathcal{F} \cdot R^{(m)}(X)) + o(X^{(\dim V)/d}).$$

Proof. Let $\mathcal{F}' \subset \mathcal{F}$ be the set consisting of $h \in \mathcal{F}$ such that the b_{11}-coefficient of any $B \in hG_0R^{(m)}(X)$ is less than 1 in absolute value. From (19), we see that $N(V(\mathbb{Z})^{(m)}; X)$ is equal to

$$\begin{aligned}
&\frac{1}{\#J^{(m)}[2](\mathbb{R}) \operatorname{Vol}(G_0)} \int_{h \in \mathcal{F}} \#\{hG_0R^{(m)}(X) \cap V(\mathbb{Z})^{\mathrm{irr}}\}\, dh \\
&\quad = \frac{1}{\#J^{(m)}[2](\mathbb{R}) \operatorname{Vol}(G_0)} \Bigg(\int_{h \in \mathcal{F} \setminus \mathcal{F}'} \#\{hG_0R^{(m)}(X) \cap V(\mathbb{Z})^{\mathrm{irr}}\}\, dh \\
&\qquad + \int_{h \in \mathcal{F}'} \#\{hG_0R^{(m)}(X) \cap V(\mathbb{Z})^{\mathrm{irr}}\}\, dh \Bigg).
\end{aligned}$$

From Propositions 21 and 23, we obtain

$$N(V(\mathbb{Z})^{(m)}; X) = \frac{1}{\#J^{(m)}[2](\mathbb{R}) \operatorname{Vol}(G_0)} \int_{h \in \mathcal{F} \setminus \mathcal{F}'} \#\{hG_0R^{(m)}(X) \cap V(\mathbb{Z})\}\, dh + o(X^{(\dim V)/d}). \tag{28}$$

Note that b_{11} has minimal weight among all the b_{ij}, that is, the powers of the s_k in $w(1,1)/w(i,j)$ are non-negative for each i, j, k. Furthermore, the length of the projection of $hG_0R^{(m)}(X)$ onto the b_{11}-line is greater than 1 for any $h \in \mathcal{F} \setminus \mathcal{F}'$ (by the definition of $\mathcal{F}'$). Hence, for $h \in \mathcal{F} \setminus \mathcal{F}'$, the volumes of all smaller-dimensional projections of $hG_0R^{(m)}(X)$ are bounded by a constant times the volume of its projection onto the $b_{11} = 0$ hyperplane. Proposition 19 then implies that

$$\begin{aligned}
N(V(\mathbb{Z})^{(m)}; X) = \frac{1}{\#J^{(m)}[2](\mathbb{R}) \operatorname{Vol}(G_0)} &\int_{h \in \mathcal{F} \setminus \mathcal{F}'} \operatorname{Vol}(hG_0R^{(m)}(X)) \\
&+ O\left(\frac{\operatorname{Vol}(hG_0R^{(m)}(X))}{X^{1/d} w(1,1)} \right) dh + o(X^{(\dim V)/d}).
\end{aligned}$$

https://doi.org/10.1112/S0010437X17007515

Recall that $\mathcal{F}'$ is defined by the condition $CX^{1/d}w(1,1) < 1$. Hence, to be in $\mathcal{F}'$, one of the s_i must be at least $C^{1/2n}X^{1/2nd}$, which implies that the volume of $\mathcal{F}'$ is bounded by $o(1)$. Moreover, since $\int_{h\in\mathcal{F}\setminus\mathcal{F}'} 1/w(1,1)\,dh = O(1)$, we obtain

$$\begin{aligned} N(V(\mathbb{Z})^{(m)};X) &= \frac{1}{\#J^{(m)}[2](\mathbb{R})\operatorname{Vol}(G_0)}\int_{h\in\mathcal{F}}\operatorname{Vol}(hG_0R^{(m)}(X))\,dh + o(X^{(\dim V)/d}) \\ &= \frac{1}{\#J^{(m)}[2](\mathbb{R})\operatorname{Vol}(G_0)}\int_{h\in G_0}\operatorname{Vol}(\mathcal{F}h\cdot R^{(m)}(X))\,dh + o(X^{(\dim V)/d}) \\ &= \frac{\operatorname{Vol}(\mathcal{F}\cdot R^{(m)}(X))}{\#J^{(m)}[2](\mathbb{R})\operatorname{Vol}(G_0)}\int_{h\in G_0} dh + o(X^{(\dim V)/d}) \\ &= \frac{\operatorname{Vol}(\mathcal{F}\cdot R^{(m)}(X))}{\#J^{(m)}[2](\mathbb{R})} + o(X^{(\dim V)/d}), \end{aligned} \tag{29}$$

where the third equality follows because the volume of $\mathcal{F}h\cdot R^{(m)}(X)$ is independent of h. This concludes the proof of Theorem 24. □

4.3 A squarefree sieve

For any subset U of $S(\mathbb{Z})$, let $N(U;X)$ denote the number of elements in U having height bounded by X. Let $F = F_\Sigma$ be a large family of monic even hyperelliptic curves defined by congruence conditions. We assume without loss of generality that $\Sigma_\infty = S(\mathbb{R})^{(m)}$ for some fixed integer $m \in \{0,\dots,n+1\}$. We first determine asymptotics for $N(\operatorname{Inv}(F);X)$ as X goes to infinity. To this end, we have the following uniformity estimate, proved in [BSW16].

PROPOSITION 25. *For each prime p, let U_p denote the set of elements $c \in S(\mathbb{Z})$ such that $p^2 \mid \Delta(c)$. Then for any $M > 0$, we have*

$$\sum_{p>M} N(U_p;X) = O_\epsilon(X^{(\dim V)/d}/M^{1-\epsilon}) + o(X^{(\dim V)/d}),$$

where the implied constant is independent of X and M.

Then we have the following theorem which follows from Propositions 19 and 25 just as [BS15, Theorem 2.21] followed from [BS15, Theorems 2.12 and 2.13].

THEOREM 26. *Let $F = F_\Sigma$ be a large family of monic even hyperelliptic curves defined by congruence conditions such that $\Sigma_\infty = S(\mathbb{R})^{(m)}$ for some $m = 0,\dots,n+1$. Then the number of hyperelliptic curves in F having height bounded by X is*

$$\operatorname{Vol}(S(\mathbb{R})^{(m)}_{H<X})\prod_p \operatorname{Vol}(\operatorname{Inv}_p(F)) + o(X^{(\dim V)/d}).$$

The following weighted version of Theorem 20 follows immediately from the proof of Theorem 20.

THEOREM 27. *Fix some $m = 0,\dots,n+1$. Let $p_1,\dots,p_k$ be distinct prime numbers. For $j = 1,\dots,k$, let $\phi_{p_j} : V(\mathbb{Z}) \to \mathbb{R}$ be $G(\mathbb{Z})$-invariant functions on $V(\mathbb{Z})$ such that $\phi_{p_j}(B)$ depends only on the congruence class of B modulo some power $p_j^{a_j}$ of p_j. Let $N_\phi(V^{(m)}(\mathbb{Z});X)$ denote the number of irreducible $G(\mathbb{Z})$-orbits of $V^{(m)}(\mathbb{Z})$ having height bounded by X, where each orbit*

https://doi.org/10.1112/S0010437X17007515

$G(\mathbb{Z})\cdot B$ is counted with weight $\phi(B)/\#\mathrm{Stab}_{G(\mathbb{Z})}(B)$; here ϕ is defined by $\phi(B) := \prod_{j=1}^{k}\phi_{p_j}(B)$. Then we have

$$N_\phi(V^{(m)}(\mathbb{Z}); X) = N(V^{(m)}(\mathbb{Z}); X)\prod_{j=1}^{k}\int_{B\in V(\mathbb{Z}_{p_j})}\tilde{\phi}_{p_j}(B)\,dB + o(X^{(\dim V)/d}), \tag{30}$$

where $\tilde{\phi}_{p_j}$ is the natural extension of ϕ_{p_j} to $V(\mathbb{Z}_{p_j})$ and dB denotes the additive measure on $V(\mathbb{Z}_{p_j})$ normalized so that $\int_{B\in V(\mathbb{Z}_{p_j})} dB = 1$.

However, in order to prove Theorem 18, we shall need weights that are defined by certain infinite sets of congruence conditions. To describe which weight functions on $V(\mathbb{Z})$ are allowed, we need the following definition.

Definition 28. A function $\phi : V(\mathbb{Z}) \to [0,1]$ is said to be defined by congruence conditions if there exist local functions $\phi_p : V(\mathbb{Z}_p) \to [0,1]$ satisfying the following conditions:

(i) for all $B \in V(\mathbb{Z})$, the product $\prod_p \phi_p(B)$ converges to $\phi(B)$;
(ii) for each prime p, the function ϕ_p is locally constant outside some closed set S_p of measure 0.

Then we have the following theorem.

Theorem 29. *Let $\phi : V(\mathbb{Z}) \to [0,1]$ be a function defined by congruence conditions via local functions $\phi_p : V(\mathbb{Z}_p) \to [0,1]$. Then, with notation as in Theorem 27, we have*

$$N_\phi(V^{(m)}(\mathbb{Z}); X) \leqslant N(V^{(m)}; X)\prod_{p}\int_{B\in V(\mathbb{Z}_p)}\phi_p(B)\,dB + o(X^{(\dim V)/d}).$$

Theorem 29 follows from Theorem 27. The proof is identical to the first half of the proof of [BS15, Theorem 2.21].

4.4 Compatibility of measures and local computations

Let $F = F_\Sigma$ be a large family of monic even hyperelliptic curves defined by congruence conditions. We assume without loss of generality that $\Sigma_\infty = S(\mathbb{R})^{(m)}$ for some fixed integer $m \in \{0,\dots,n+1\}$. To prove Theorem 18 we need to weight each locally soluble element $B \in V(\mathbb{Z})$ (having invariant $\pi(B)$ in $\mathrm{Inv}(F)$) by the reciprocal of the number of $G(\mathbb{Z})$-orbits in $G(\mathbb{Q})\cdot B \cap V(\mathbb{Z})$. However, in order for our weight function to be defined by congruence conditions, we use instead the following weight function $w : V(\mathbb{Z}) \to [0,1]$:

$$w(B) := \begin{cases} \left(\displaystyle\sum_{B'} \frac{\#\mathrm{Stab}_{G(\mathbb{Q})}(B')}{\#\mathrm{Stab}_{G(\mathbb{Z})}(B')}\right)^{-1} & \text{if } B \text{ is locally soluble and } \pi(B)\in\mathrm{Inv}(F),\\ 0 & \text{otherwise,}\end{cases} \tag{31}$$

where the sum is over a complete set of representatives for the action of $G(\mathbb{Z})$ on $G(\mathbb{Q})\cdot B\cap V(\mathbb{Z})$.

We start with the following proposition proving that the class $(\infty') - (\infty)$ is not divisible by 2 in the Jacobians of most hyperelliptic curves in our family.

Proposition 30. *Let F be a large family of hyperelliptic curves. Then for 100% of elements $C \in F$, the class $(\infty') - (\infty)$ is not divisible by 2 in $J(\mathbb{Q})$.*

https://doi.org/10.1112/S0010437X17007515

Proof. By the proof of Theorem 10 and Proposition 5, for a monic even hyperelliptic curve C over $\mathbb{Q}$ defined by $y^2 = f(x)$, the element $(\infty') - (\infty)$ is divisible by 2 in $J(\mathbb{Q})$ if and only if the étale algebra $L = \mathbb{Q}[x]/(f(x))$ contains a quadratic extension of $\mathbb{Q}$. Proposition 30 then follows since for 100% of monic integral polynomials of degree $2n+2$, when ordered by height, the Galois group of the normal closure of $\mathbb{Q}[x]/(f(x))$ is S_n. □

We now have the following theorem.

THEOREM 31. *Let $F = F_\Sigma$ be a large family of monic even hyperelliptic curves defined by congruence conditions with $\Sigma_\infty = S(\mathbb{R})^{(m)}$ for some fixed integer $m \in \{0, \dots, n+1\}$. L Then*

$$\sum_{\substack{C \in F \\ H(C) \leqslant X}} (\#\mathrm{Sel}_2(J(C)) - 2) = N_w(V(\mathbb{Z})^{(m)}; X) + o(X^{(\dim V)/d}), \tag{32}$$

where $V(\mathbb{Z})^{(m)}$ is the set of all elements in $V(\mathbb{Z})$ whose invariants belong to $\Sigma_\infty = S(\mathbb{R})^{(m)}$.

Proof. It follows from Proposition 30 that for 100% of hyperelliptic curves $C(c) \in F$, the set $V_{f_c}(\mathbb{Q})$ has two distinguished orbits. Hence, Theorem 11 and Corollary 13 show that, up to an error of $o(X^{(\dim V)/d})$, the left-hand side of (32) is equal to the number of $G(\mathbb{Q})$-equivalence classes of elements in $V(\mathbb{Z})$ that are locally soluble, have invariants in $\mathrm{Inv}(F)$, and have height bounded by X.

Given a locally soluble element $B \in V(\mathbb{Z})$ such that $\pi(B) \in F$, let $B_1 \dots B_k$ denote a complete set of representatives for the action of $G(\mathbb{Z})$ on the $G(\mathbb{Q})$-equivalence class of B in $V(\mathbb{Z})$. Then

$$\begin{aligned}\sum_{i=1}^{k} \frac{w(B_i)}{\#\mathrm{Stab}_{G(\mathbb{Z})}(B_i)} &= \frac{1}{\#\mathrm{Stab}_{G(\mathbb{Q})}(B)} \left(\sum_{i=1}^{k} \frac{1}{\#\mathrm{Stab}_{G(\mathbb{Z})}(B_i)} \right)^{-1} \sum_{i=1}^{k} \frac{1}{\#\mathrm{Stab}_{G(\mathbb{Z})}(B_i)} \\ &= \frac{1}{\#\mathrm{Stab}_{G(\mathbb{Q})}(B)}. \end{aligned} \tag{33}$$

Hence the right-hand side of (32) counts the number of $G(\mathbb{Q})$-equivalence classes of elements in $V(\mathbb{Z})$ that are locally soluble, have invariants in F, and have height bounded by X, such that the $G(\mathbb{Q})$-orbit of B is weighted with $1/\#\mathrm{Stab}_{G(\mathbb{Q})}(B)$ for all orbits. The theorem now follows since $\mathrm{Stab}_{G(\mathbb{Q})}(B) = 1$ for all but negligibly few$B \in V(\mathbb{Z})$ by Proposition 23. □

In order to demonstrate that w is defined by congruence conditions, we need to express it as a local product of weight functions on $V(\mathbb{Z}_p)$. To this end, we define $w_p : V(\mathbb{Z}_p) \to [0, 1]$:

$$w_p(B) := \begin{cases} \left(\sum_{B'} \dfrac{\#\mathrm{Stab}_{G(\mathbb{Q}_p)}(B')}{\#\mathrm{Stab}_{G(\mathbb{Z}_p)}(B')} \right)^{-1} & \text{if } B \text{ is } \mathbb{Q}_p\text{-soluble and } \pi(B) \in \mathrm{Inv}_p(F), \\ 0 & \text{otherwise,} \end{cases} \tag{34}$$

where the sum is over a set of representatives for the action of $G(\mathbb{Z}_p)$ on the $G(\mathbb{Q}_p)$-equivalence class of B in $V(\mathbb{Z})$. We have the following result whose proof is identical to that of [BS15, Proposition 3.6], using the fact that G has class number 1 over $\mathbb{Q}$.

PROPOSITION 32. *If $B \in V(\mathbb{Z})$ has non-zero discriminant, then $w(B) = \prod_p w_p(B)$.*

https://doi.org/10.1112/S0010437X17007515

From Theorems 20 and 29, we have the equality

$$N_w(V(\mathbb{Z})^{(m)}; X) = \frac{1}{\#J^{(m)}[2](\mathbb{R})} \operatorname{Vol}(\mathcal{F} \cdot R^{(m)}(X)) \prod_p \int_{V(\mathbb{Z}_p)} w_p(B)\, dB + o(X^{(\dim V)/d}). \quad (35)$$

For the rest of the section, our aim is to express $\operatorname{Vol}(\mathcal{F} \cdot R^{(m)}(X))$ and $\int_{V(\mathbb{Z}_p)} w_p(B)\, dB$ in more convenient forms. To this end, we introduce the following notation. Recall that dB is Haar measure on V normalized so that $V(\mathbb{Z}_p)$ has volume 1 for each prime p, and such that $V(\mathbb{Z})$ has covolume 1 in $V(\mathbb{R})$. Let $d\mu(c)$ denote similarly normalized Euclidean measure on S. Finally, let ω be a differential which generates the rank-1 module of top-degree differentials of G over $\mathbb{Z}$. We denote the measure associated with ω by $d\tau(g)$. We now have the following result that allows us to compute volumes of multisets in $V(K)$, for $K = \mathbb{R}$ and $\mathbb{Z}_p$. This result follows from [BS15, Propositions 3.11 and 3.12].

Proposition 33. *Let K be $\mathbb{R}$ or $\mathbb{Z}_p$ for some prime p, let $|\cdot|$ denote the usual valuation on K, and let $s : S(K) \to V(K)$ be a continuous section. Then there exists a rational non-zero constant $\mathcal{J}$, independent of K and s, such that for any measurable function ϕ on $V(K)$, we have*

$$\int_{G(K)\cdot s(S(K))} \phi(B)\, dB = |\mathcal{J}| \int_{c\in S(K)} \int_{g\in G(K)} \phi(g \cdot s(c))\, d\tau(g)\, d\mu(c), \quad (36)$$

$$\int_{V(K)} \phi(B)\, dB = |\mathcal{J}| \int_{\substack{c\in S(K)\\ \Delta(c)\neq 0}} \left(\sum_{B\in (V_{f_c}(K)/G(K))} \frac{1}{\#\mathrm{Stab}_{G(K)}(B)} \int_{g\in G(K)} \phi(g \cdot B)\, d\tau(g) \right) d\mu(c), \quad (37)$$

where we regard $G(K) \cdot s(R)$ as a multiset, and $V_{f_c}(K)/G(K)$ denotes a set of representatives for the action of $G(K)$ on $V_{f_c}(K)$.

We use Proposition 33 to compute $\operatorname{Vol}(\mathcal{F} \cdot R^{(m)}(X))$. If $c \in R^{(m)}$ and J denotes the Jacobian of the corresponding hyperelliptic curve, then the number of $\mathbb{R}$-soluble $G(\mathbb{R})$-orbits of $V_{f_c}(\mathbb{R})$ is $\#(J(\mathbb{R})/2J(\mathbb{R}))$. This number is independent of $c \in V(\mathbb{R})^{(m)}$, and we denote it by $\#(J^{(m)}(\mathbb{R})/2J^{(m)}(\mathbb{R}))$. Hence, by (36), we have

$$\begin{aligned} \frac{1}{\#J^{(m)}[2](\mathbb{R})} \operatorname{Vol}(\mathcal{F} \cdot R^{(m)}(X)) &= |\mathcal{J}| \frac{\#(J^{(m)}(\mathbb{R})/2J^{(m)}(\mathbb{R}))}{\#J^{(m)}[2](\mathbb{R})} \operatorname{Vol}(\mathcal{F}) \operatorname{Vol}(S(\mathbb{R})^{(m)}) \\ &= |\mathcal{J}| a_\infty \operatorname{Vol}(\mathcal{F}) \operatorname{Vol}(S(\mathbb{R})^{(m)}), \end{aligned} \quad (38)$$

where

$$a_\infty = \frac{\#(J^{(m)}(\mathbb{R})/2J^{(m)}(\mathbb{R}))}{\#J^{(m)}[2](\mathbb{R})} = 2^{-n},$$

by [Sto01, Lemma 5.14].

Next we compute $\int_{V(\mathbb{Z}_p)} w_p(B)\, dB$. Note that since w_p is $G(\mathbb{Z}_p)$-invariant, we have

$$\begin{aligned} \int_{V(\mathbb{Z}_p)} w_p(B)\, dB &= |\mathcal{J}|_p \operatorname{Vol}(G(\mathbb{Z}_p)) \int_{c\in \mathrm{Inv}_p(F)} \left(\sum_{B\in (V_c(\mathbb{Z}_p)/G(\mathbb{Z}_p))} \frac{w_p(B)}{\#\mathrm{Stab}_{G(\mathbb{Z}_p)}(B)} \right) d\mu(c) \\ &= |\mathcal{J}|_p a_p \operatorname{Vol}(G(\mathbb{Z}_p)) \operatorname{Vol}(\mathrm{Inv}_p(F)). \end{aligned} \quad (39)$$

https://doi.org/10.1112/S0010437X17007515

The final equality follows from a computation similar to (33); namely, if J is the Jacobian of the monic even hyperelliptic curve c and B_c is any element in $V_{f_c}(\mathbb{Q}_p)$, we have by Proposition 12,

$$\sum_{B\in(V_{f_c}(\mathbb{Z}_p)/G(\mathbb{Z}_p))}\frac{w_p(B)}{\#\mathrm{Stab}_{G(\mathbb{Z}_p)}(B)}=\frac{\#(G(\mathbb{Q}_p)\backslash V_{f_c}^{\mathrm{sol}}(\mathbb{Q}_p))}{\#\mathrm{Stab}_{G(\mathbb{Q}_p)}(B_c)}=\frac{\#(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))}{\#J[2](\mathbb{Q}_p)}=:a_p.$$

Note that $a_p=1$ if $p\neq 2$ and $a_2=2^n$, by [Sto01, Lemma 5.7].

Combining Theorem 31 with (35), (38), and (39), we obtain

$$\begin{aligned}&\sum_{\substack{C\in F\\ H(C)\leqslant X}}(\#\mathrm{Sel}_2(J(C))-2)\\&\quad=|\mathcal{J}|\,a_\infty\,\mathrm{Vol}(\mathcal{F})\,\mathrm{Vol}(S(\mathbb{R})^{(m)})\prod_p|\mathcal{J}|_p\,a_p\,\mathrm{Vol}(G(\mathbb{Z}_p))\,\mathrm{Vol}(\mathrm{Inv}_p(F))+o(X^{(\dim V)/(\deg H)})\\&\quad=\mathrm{Vol}(\mathcal{F})\,\mathrm{Vol}(S(\mathbb{R})^{(m)})\prod_p\mathrm{Vol}(G(\mathbb{Z}_p))\,\mathrm{Vol}(\mathrm{Inv}_p(F))+o(X^{(\dim V)/(\deg H)}),\end{aligned}\tag{40}$$

since $a_\infty\prod_p a_p=1$ and $|\mathcal{J}|\prod_p|\mathcal{J}|_p=1$.

Theorem 26, Proposition 30 and (40) imply that

$$\begin{aligned}\lim_{X\to\infty}\frac{\sum_{\substack{C\in F\\ H(C)<X}}(\#\mathrm{Sel}_2(J(C))-2)}{\sum_{\substack{C\in F\\ H(C)<X}}1}&=\frac{\mathrm{Vol}(\mathcal{F})\,\mathrm{Vol}(S(\mathbb{R})^{(m)})\prod_p(\mathrm{Vol}(G(\mathbb{Z}_p))\,\mathrm{Vol}(\mathrm{Inv}_p(F)))}{\mathrm{Vol}(S(\mathbb{R})^{(m)})\prod_p\mathrm{Vol}(\mathrm{Inv}_p(F))}\\&=\tau_G,\end{aligned}\tag{41}$$

the Tamagawa number of G. Since the Tamagawa number of PSO is 4 [Lan66], Theorem 18 follows.

Finally, as a by-product of our proof of Theorem 18, we have the following analogue of [BG13, Theorem 12.4]; the proof is identical.

THEOREM 34. *Fix a place ν of $\mathbb{Q}$. Let F be a large family of hyperelliptic curves C over $\mathbb{Q}$ with a marked non-Weierstrass point such that:*

(a) *the cardinality of $J(C)(\mathbb{Q}_\nu)/2J(C)(\mathbb{Q}_\nu)$ is a constant k for all $C\in F$; and*
(b) *the set $U_\nu(F)\subset V(\mathbb{Z}_\nu)$, defined to be the set of soluble elements in $V(\mathbb{Z}_\nu)$ having invariants in $\mathrm{Inv}_\nu(F)$, can be partitioned into k open sets Ω_i such that:*
   (i) *for all i, if two elements in Ω_i have the same invariants, then they are $G(\mathbb{Q}_\nu)$-equivalent; and*
   (ii) *for all $i\neq j$, we have $G(\mathbb{Q}_\nu)\Omega_i\cap G(\mathbb{Q}_\nu)\Omega_j=\emptyset$.*

(In particular, the groups $J(C)(\mathbb{Q}_\nu)/2J(C)(\mathbb{Q}_\nu)$ are naturally identified for all $C\in F$.) Then when elements $C\in F$ are ordered by height, the images of the non-distinguished elements (i.e., elements that do not correspond to either the identity or the class of $(\infty')-(\infty)$ in $J(C)(\mathbb{Q})$) under the map

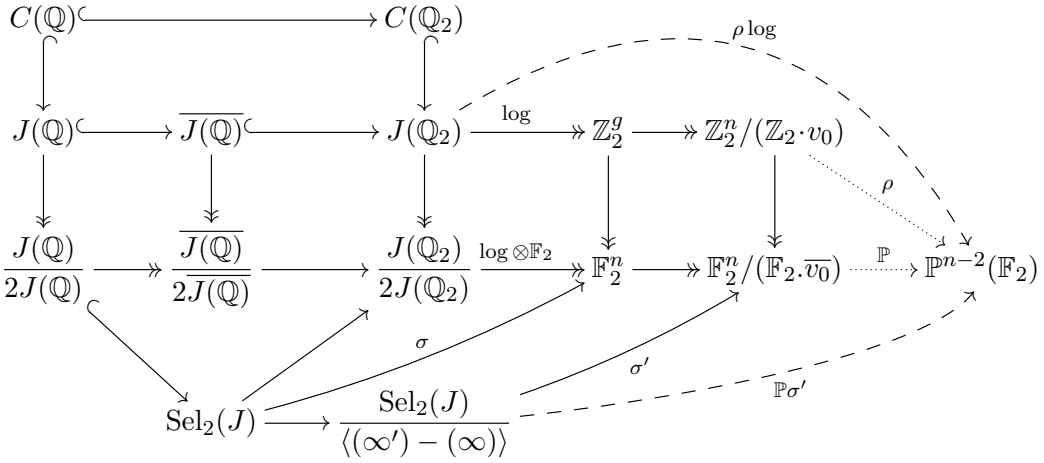
$$\mathrm{Sel}_2(J(C))\to J(C)(\mathbb{Q}_\nu)/2J(C)(\mathbb{Q}_\nu)$$

are equidistributed.

https://doi.org/10.1112/S0010437X17007515

5. An application of Chabauty's method

In this section, we apply Chabauty's method as refined by Poonen and Stoll [PS14]. Let C be a monic even hyperelliptic curve over $\mathbb{Q}$ with Jacobian J and two rational points, denoted by ∞ and ∞', at infinity. We embed $C(\mathbb{Q})$ and $C(\mathbb{Q}_2)$ into $J(\mathbb{Q})$ and $J(\mathbb{Q}_2)$ via the map $P \mapsto (P)-(\infty)$. Normalize the log map from $J(\mathbb{Q}_2)$ to $\mathbb{Z}_2^n$ to be surjective as in [PS14]. Let $v_0 \in \mathbb{Z}_2^n$ denote the primitive part of $\log((\infty)-(\infty'))$ and let $\overline{v_0}$ denote the reduction modulo 2 of v_0 in $\mathbb{F}_2^n$. For any $v \in \mathbb{Z}_2^n/(\mathbb{Z}_2 \cdot v_0) \simeq \mathbb{Z}_2^{n-1}$, $\rho(v)$ is defined by taking the reduction modulo 2 of the primitive part of v and then taking its image under $\mathbb{P}$, which takes a non-zero element in $\mathbb{F}_2^{n-1}$ and sends it to its projectivization in $\mathbb{P}^{n-2}(\mathbb{F}_2)$. Note that the maps ρ and $\mathbb{P}$ are only partially defined, since $\mathbb{P}$ is undefined on 0. Consider now the following diagram, which is commutative on elements where all the maps are defined:



A similar diagram is used in [PS14] to study rational points on hyperelliptic curves with a rational Weierstrass point. One major difference in our case is the extra generator $(\infty)'-(\infty)$ of $J(\mathbb{Q})$. Its class in $\mathrm{Sel}_2(J)$ does not equidistribute in $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$.

As in [PS14, Proposition 8.4], 100% of monic even hyperelliptic curves over $\mathbb{Q}$ have trivial torsion in their Jacobians. Hence in what follows, we consider only monic even hyperelliptic curves C such that $J(\mathbb{Q})_{\mathrm{tors}} = \{0\}$.

5.1 The image of $C(\mathbb{Q}_2)$ in $\mathbb{P}^{n-2}(\mathbb{F}_2)$ is locally constant and small on average

Break up the set of monic even hyperelliptic curves over $\mathbb{Q}$ of genus n with trivial torsion in their Jacobians into large families such that over each such large family F, the log map is normalized so that the image of $(\infty')-(\infty)$ in $\mathbb{Z}_2^n$ is locally constant and, as C varies in F, the image of $C(\mathbb{Q}_2)$ in $\mathbb{P}^{n-2}(\mathbb{F}_2)$ is constant. The analogous statement for odd hyperelliptic curves is proved in [PS14, §§ 8.1 and 8.2]. The same proofs carry through verbatim for monic even hyperelliptic curves.

Write $\rho\log(C(\mathbb{Q}_2))$ for the image of $C(\mathbb{Q}_2)$ in $\mathbb{P}^{n-2}(\mathbb{F}_2)$ (ignoring the points where ρ is not defined). For any prime p, associated to any $(2n+1)$-tuple $(c_2,\dots,c_{2n+2}) \in \mathbb{Z}_p^{2n+1}$ with $\Delta(x^{2n+2}+c_2x^{2n}+\cdots+c_{2n+2}) \neq 0$ is a monic even hyperelliptic curve over $\mathbb{Q}_p$ defined by $y^2 = x^{2n+2}+c_2x^{2n}+\cdots+c_{2n+2}$. We write $\mathbb{Z}_p^{2n+1}\backslash\{\Delta=0\}$ for this set of monic even hyperelliptic curves over $\mathbb{Q}_p$ of genus n. Then we have the following proposition.

Proposition 35. *Let C range over monic even hyperelliptic curves corresponding to elements in $\mathbb{Z}_2^{2n+1}\backslash\{\Delta=0\}$ such that $(\infty)-(\infty') \notin J(\mathbb{Q}_2)_{\mathrm{tors}}$. Then the average size of $\rho\log(C(\mathbb{Q}_2))$ is at most $6n+9$.*

https://doi.org/10.1112/S0010437X17007515

Proof. This result follows immediately from the proofs of [PS14, Proposition 5.4, Theorem 9.1] by breaking up $C(\mathbb{Q}_2)$ into residue disks in accordance with $\mathcal{C}^{\text{smooth}}(\mathbb{F}_2)$ where $\mathcal{C}$ denotes the minimal proper regular model of C and then counting the number of images coming from each residue disk. Denote by ρ' the scale and reduce map from $\mathbb{Z}_2^n$ to $\mathbb{P}^{n-1}(\mathbb{F}_2)$. Then we see that the average size of $\rho' \log(C(\mathbb{Q}_2))$ is at most $6n + 14$ using the upper bound of 4 for the average size of $\mathcal{C}^{\text{smooth}}(\mathbb{F}_2)$. Note that the definition of $\rho \log$ involves quotienting out by the $\mathbb{Z}_2$-line spanned by v_0. Hence the residue disk at ∞ and the residue disk at ∞' give the same image under $\rho \log$. Thus, following the proof of [PS14, Proposition 5.4], we obtain a bound of $6n+9$ for the average size of $\rho \log(C(\mathbb{Q}_2))$. □

5.2 The image of $J(\mathbb{Q})$ in $\mathbb{P}^{n-2}(\mathbb{F}_2)$ is contained in the image of $\text{Sel}_2(J)/\langle(\infty') - (\infty)\rangle$

Lemma 36. *Suppose C is a monic even-degree hyperelliptic curve over $\mathbb{Q}$ with $J(\mathbb{Q})_{\text{tors}} = \{0\}$. Write $d_0 = (\infty') - (\infty)$. Suppose the map σ' is injective. Then $\rho \log(\overline{J(\mathbb{Q})}) \subset \mathbb{P}\sigma'(\text{Sel}_2(J)/\langle d_0\rangle)$ where $\overline{J(\mathbb{Q})}$ denotes the p-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$. Furthermore, if $g \in J(\mathbb{Q})$ has no image under $\rho \log$, then there exist integers m and k such that $mg = kd_0$.*

Proof. Since $\rho \log$ is continuous and $\mathbb{P}^{n-2}(\mathbb{F}_2)$ is discrete, $\rho \log(\overline{J(\mathbb{Q})}) = \rho \log(J(\mathbb{Q}))$. Since $J(\mathbb{Q})_{\text{tors}} = 0$, we have $J(\mathbb{Q})/\mathbb{Z}d_0 \simeq F \oplus \mathbb{Z}^{r'}$, where r' is the rank of $J(\mathbb{Q})/\mathbb{Z}d_0$ and F is a finite abelian group such that any lift g to $J(\mathbb{Q})$ of an element in F satisfies $mg = kd_0$ for some integers m and k. This implies that such a g has no image under the partially defined map $\rho' \log$.

Let $h \in J(\mathbb{Q})$ be an element that does have an image under $\rho \log$. Write the image of h in $F \oplus \mathbb{Z}^{r'}$ as (t, h') with $t \in F$ and $h' \in \mathbb{Z}^{r'}$. Let h_0 denote the primitive part of h'. Then, viewing h_0 as an element of $J(\mathbb{Q})$, we have $\rho \log(h) = \rho \log(h_0)$. Since σ' is injective, the element h_0 has non-zero image under σ'. Therefore, we obtain $\rho \log(h) = \mathbb{P}\sigma'(h_0 + \langle d_0\rangle)$, which proves the first assertion of the lemma.

For the second statement, let $h \in J(\mathbb{Q})$ be an element that does not have an image under $\rho \log$. Let the image of h in $F \oplus \mathbb{Z}^{r'}$ be (t, h'), where $t \in F$ and $h' \in \mathbb{Z}^{r'}$. If $h' = 0$, then we are done. Suppose for a contradiction that h' is non-zero. Let h_0 denote the primitive part of h'. Since h has no image under $\rho \log$, neither does h_0, and we have $\log(h_0) \in \mathbb{Z}_2 \cdot v_0$. This implies that the class of h_0 in $\text{Sel}_2(J)/\langle d_0\rangle$ maps to 0 under σ', contradicting the injectivity of σ'. □

5.3 The equidistributed sets $\mathbb{P}\sigma'(\text{Sel}_2(J)/\langle(\infty') - (\infty)\rangle)$ rarely intersect the small sets $\rho \log(C(\mathbb{Q}_2))$

Let F be a large family of monic even hyperelliptic curves over $\mathbb{Q}$ satisfying the hypothesis of Theorem 34 such that the image of $\rho \log(C(\mathbb{Q}_2))$ in $\mathbb{P}^{n-2}(\mathbb{F}_2)$ is constant for $C \in F$. (We assume also that the log maps are normalized such that the image of $d_0 = (\infty') - (\infty)$ is constant throughout this family.) Denote this image by I.

On average over the curves in F, there are at most four non-distinguished elements in $\text{Sel}_2(J)$ by Theorem 18, and the images of these elements under σ equidistribute in $\mathbb{F}_2^n$ by Theorem 34. By Proposition 30, the class d_0 is not a multiple of 2 in the Jacobian for 100% of the curves in F. Hence, on average over F, there are at most two non-identity elements in $\text{Sel}_2(J)/\langle d_0\rangle$ and their images under σ' equidistribute in $\mathbb{F}_2^n/(\mathbb{F}_2 \cdot \overline{v_0})$. Hence a proportion of at least $1 - (\#I)2^{2-n}$ curves C in F satisfy

$$\rho \log(C(\mathbb{Q}_2)) \cap \mathbb{P}\sigma'(\text{Sel}_2(J)/\langle d_0\rangle) = \emptyset.$$

Furthermore, a proportion of at most 2^{2-n} curves in F fail to satisfy the conditions of Lemma 36 (corresponding to those curves C such that a non-identity element of $\text{Sel}_2(J)/\langle d_0\rangle$ maps to 0 under σ'). A point $P \in C(\mathbb{Q})\backslash\{\infty, \infty'\}$ is said to be *bad* if there exist integers m and k, not

https://doi.org/10.1112/S0010437X17007515

both zero, such that

$$m((P)-(\infty)) = k((\infty')-(\infty)). \tag{42}$$

Hence aside from a set of density at most $(1+\#I)2^{2-n}$, all curves $C \in F$ are such that every point $P \in C(\mathbb{Q})\backslash\{\infty,\infty'\}$ is bad.

We summarize the above discussion in the following theorem.

Theorem 37. *Suppose C is a monic even hyperelliptic curve of genus n over $\mathbb{Q}$ satisfying the following three conditions:*

(i) $J(\mathbb{Q})_{\mathrm{tors}} = \{0\}$;
(ii) $\ker \sigma' = \{0\}$;
(iii) $\rho\log(C(\mathbb{Q}_2)) \cap \mathbb{P}\sigma'(\mathrm{Sel}_2(J)/\langle d_0\rangle) = \emptyset$.

Then every point $P \in C(\mathbb{Q})\backslash\{\infty,\infty'\}$ is bad, that is, there exist integers m and k, not both 0, such that

$$m((P)-(\infty)) = k((\infty')-(\infty)).$$

Moreover, the proportion of monic even hyperelliptic curves of genus n over $\mathbb{Q}$ satisfying the above three conditions is at least $1-(24n+40)2^{-n}$.

6. Most monic even hyperelliptic curves have only two rational points

We say that a monic even hyperelliptic curve C over $\mathbb{Q}$ is *good* if $C(\mathbb{Q})$ has no bad points. Then, to prove Theorem 1, it remains to prove the following result.

Theorem 38. *All but 0% of monic even hyperelliptic curves over $\mathbb{Q}$ having fixed genus $n \geqslant 4$ are good.*

We work p-adically for some fixed prime p not dividing $2n+2$. Suppose C is a monic even-degree hyperelliptic curve with coefficients in $\mathbb{Z}_p$. Let $\ell : C(\mathbb{Q}_p) \to \mathbb{Z}_p^n$ denote the map sending $P \in C(\mathbb{Q}_p)$ to $\log((P)-(P^\tau))$ where τ denotes the hyperelliptic involution and log is computed with respect to the differentials

$$\{dx/y, x\,dx/y, \ldots, x^{n-1}\,dx/y\}.$$

We say that a point $P \in C(\mathbb{Q}_p)\backslash\{\infty,\infty'\}$ is *bad* if the $\mathbb{Z}_p$-lines spanned by $\ell(P)$ and $\ell(\infty)$ have non-zero intersections. Note that if $P \in C(\mathbb{Q})$ is bad, that is, satisfies (42), then P considered as a point in $C(\mathbb{Q}_p)$ is bad since we have

$$m((P)-(P^\tau)) = (m-2k)((\infty)-(\infty')).$$

We thank Jacob Tsimerman for several conversations which led to the proof of the following theorem, from which Theorem 38 will be shown to follow.

Theorem 39. *Suppose $n \geqslant 4$. The set U of elements in $\mathbb{Z}_p^{2n+1}\backslash\{\Delta = 0\}$ corresponding to monic even hyperelliptic curves C of genus n such that $C(\mathbb{Q}_p)\backslash\{\infty,\infty'\}$ contains no bad points is dense. Furthermore, the p-adic closure of its complement has measure 0.*

https://doi.org/10.1112/S0010437X17007515

Proof. Let C be a monic even hyperelliptic curve over $\mathbb{Q}_p$ corresponding to an element $v \in \mathbb{Z}_p^{2n+1}\backslash\{\Delta = 0\}$. Let $P \in C(\mathbb{Q}_p)$ be a non-Weierstrass point such that $P \notin \{\infty, \infty'\}$. Given such a point, we obtain elements $v' \in \mathbb{Z}_p^{2n+1}$ such that the curves C' corresponding to v' are isomorphic to C but the point $\infty \in C'(\mathbb{Q}_p)$ is P. Clearly it is possible to construct a sequence of points P_i tending to $\infty \in C(\mathbb{Q}_p)$ along with a corresponding sequence $v_i \in \mathbb{Z}_p^{2n+1}$ such that v_i tends to v. We say that a pair of points $(P, Q) \in C(\mathbb{Q}_p) \times C(\mathbb{Q}_p)$ is a *bad pair* if $P \notin \{Q, Q^\tau\}$, and the $\mathbb{Z}_p$-lines spanned by $\ell(P)$ and $\ell(Q)$ have a non-zero intersection. Note that even though the definition of ℓ depends on a choice of the marked point ∞ through the chosen basis of the differentials, the property of being a bad pair is independent of the choice of ∞. We will show in Lemma 40 below that the number of bad pairs $(P, Q) \in C(\mathbb{Q}_p) \times C(\mathbb{Q}_p)$ is finite for any monic even-degree hyperelliptic curve over $\mathbb{Q}_p$. From this it follows that, given (C, ∞) corresponding to $v \in \mathbb{Z}_p^{2n+1}\backslash\{\Delta = 0\}$, there exist points P arbitrarily close to ∞ such that P is not part of any bad pair. It then follows that there exist points $v' \in \mathbb{Z}_p^{2n+1}\backslash\{\Delta = 0\}$ (corresponding to (C, P)), arbitrarily close to v, that correspond to hyperelliptic curves containing no bad points. Hence U is dense.

Let V denote the complement of U in $M = \mathbb{Z}_p^{2n+1}\backslash\{\Delta = 0\}$. We claim that V is a p-adic subanalytic subset of M. The theory of subanalytic sets is studied in great detail in [DD88]. We do not repeat the definition of subanalytic sets and instead remark that subanalytic sets are stable under projections onto coordinate hyperplanes and that sets defined by the vanishing and non-vanishing of analytic functions are subanalytic. Moreover, being subanalytic is a (p-adic) local property. The *dimension* of a subanalytic set is defined to be the maximal dimension of a p-adic manifold contained in it [DD88, 3.15]. This notion of dimension behaves as expected: a zero-dimensional subanalytic set is finite; the dimension of the boundary $\bar{A}\backslash A$ of a subanalytic set A is less than the dimension of A [DD88, 3.26].

We now show that V is a p-adic subanalytic subset of M. It suffices to check this locally. Restrict to an open subset W of $\mathbb{Z}_p^{2n+1}\backslash\{\Delta = 0\}$ such that $\mathcal{C}^{\text{smooth}}(\mathbb{F}_p)$ is constant for curves C corresponding to elements in W where $\mathcal{C}$ denotes the minimal proper regular model of C. Then the moduli space of pairs (C, P), where C is a curve corresponding to an element in W and P is a point in $C(\mathbb{Q}_p)$, is isomorphic to $W \times \mathcal{C}^{\text{smooth}}(\mathbb{F}_p) \times \mathbb{Z}_p$. The set of pairs (C, P) corresponding to elements in this moduli space such that P is a bad point of $C(\mathbb{Q}_p)$ is a subanalytic set of $W \times \mathcal{C}^{\text{smooth}}(\mathbb{F}_p) \times \mathbb{Z}_p$ defined by $\ell(P) \neq 0$, $\ell(\infty) \neq 0$, and $\lambda_1\ell(P) = \lambda_2\ell(\infty)$ for some λ_1, $\lambda_2 \in \mathbb{Z}_p - \{0\}$ (a condition easily handled by projections). Since subanalytic sets are preserved by projections, this implies that $V \cap W$ is subanalytic in W, as desired. We have already proven that V does not contain any p-adic open ball of dimension $2n+1$ since its complement is dense. Hence its dimension as a subanalytic set [DD88, 3.15] is less than $\dim(\mathbb{Z}_p^{2n+1}\backslash\{\Delta = 0\}) = 2n+1$. Moreover, the dimension of $\bar{V}\backslash V$ is less than the dimension of V [DD88, 3.26], where $\bar{V}$ denotes the p-adic closure of V. Therefore, the p-adic closure of V has measure 0 as desired. □

We now prove the following result which was assumed in the proof of Theorem 39.

Lemma 40. *Let C be a monic even-degree hyperelliptic curve with coefficients in $\mathbb{Z}_p$, having genus $n \geqslant 4$. Then the set of bad pairs $(P, Q) \in C(\mathbb{Q}_p) \times C(\mathbb{Q}_p)$ is finite.*

Proof. Let Σ denote the subset of $C(\mathbb{Q}_p) \times C(\mathbb{Q}_p)$ consisting of bad pairs (P, Q). Then Σ is subanalytic as it is defined by $x(P) \neq x(Q)$, $\ell(P) \neq 0$, $\ell(Q) \neq 0$, and $\lambda_1\ell(P) = \lambda_2\ell(Q)$ for some $\lambda_1, \lambda_2 \in \mathbb{Z}_p - \{0\}$. We will show that the dimension of Σ as a subanalytic set is zero, which implies that Σ is finite by [DD88, 3.26].

https://doi.org/10.1112/S0010437X17007515

Let $P \in C(\mathbb{Q}_p)$ be any point. The main difficulty in proving Lemma 40 is that it is difficult to explicitly compute the function ℓ. However, for any P' in a small enough residue disk around P, $\ell(P')$ is the sum of $\ell(P)$ and a p-adic integral (multiplied by 2). Hence we can compute the derivative of ℓ with respect to x and obtain

$$\ell'(P') = \left(\frac{2}{y(P')}, \frac{2x(P')}{y(P')}, \ldots, \frac{2x(P')^{n-1}}{y(P')}\right) \quad \text{if } P' \notin \{\infty, \infty'\}. \tag{43}$$

One key fact to note is that two vectors $\ell'(P')$ and $\ell'(Q')$ are $\mathbb{Q}_p$-parallel if and only if $x(P') = x(Q')$. This observation is crucial in what follows.

Lemma 41. *For a fixed point $P \in C(\mathbb{Q}_p)$, the set of points $Q \in C(\mathbb{Q}_p)$ such that (P, Q) is a bad pair is finite.*

Proof. Indeed, the intersection of $\mathbb{Q}_p \cdot \ell(P)$ and $\ell(C(\mathbb{Z}_p))$ is a subanalytic set of dimension at most 1. Hence it either is finite or contains an open ball B. If it is finite, then we are done. Otherwise, the derivatives $\ell'(Q)$ are all parallel (to $\ell(P)$) for every $Q \in B$, which is a contradiction. □

We return to the proof of Lemma 40. Suppose for a contradiction that $\dim(\Sigma) \geqslant 1$. Then it contains a subset Σ_1 diffeomorphic to $\mathbb{Z}_p$. By shrinking Σ_1 if necessary, we may assume that Σ_1 is diffeomorphic to its images under the two coordinate projections by Lemma 41. That is, there exist an open subset W of $C(\mathbb{Q}_p)$ and an analytic map $s : W \to C(\mathbb{Q}_p)$ such that $(R, s(R)) \in \Sigma$ for any $R \in W$. Let $\alpha : W \to \mathbb{Q}_p^\times$ denote the analytic function such that

$$\ell(s(R)) = \alpha(R)\ell(R), \tag{44}$$

for any $R \in W$. The vanishing set of the derivative s' of s is analytic and hence either is finite or contains an open ball. In the latter case, s is constant on this open ball, which contradicts Lemma 41. By replacing W by an open ball inside it, we may assume that $s'(R) \neq 0$ for any $R \in W$. Differentiating (44) gives

$$\ell'(s(R)) = \alpha_1(R)\ell(R) + \alpha_2(R)\ell'(R), \tag{45}$$

with $\alpha_1 = \alpha'/s'$ and $\alpha_2 = \alpha/s'$. Differentiating (45) again shows that the vectors $\ell''(s(R))$, $\ell''(R)$, $\ell'(R)$, $\ell(R)$ are linearly dependent over $\mathbb{Q}_p$ for any $R \in W$. By the definition of bad pairs, we see that $x(R) \neq x(s(R))$ for any $R \in W$. Hence, for such R, the lines $\ell'(s(R))$ and $\ell'(R)$ are not parallel, which implies that $\ell(R)$ can be written as a linear combination of $\ell'(s(R))$ and $\ell'(R)$ by (45). It follows that the vectors $\ell''(s(R))$, $\ell'(s(R))$, $\ell''(R)$, $\ell'(R)$ are linearly dependent over $\mathbb{Q}_p$ for every $R \in W$. An elementary determinant computation (using the first four coordinates, which requires $n \geqslant 4$) shows that if $R, T \in C(\mathbb{Q}_p)\backslash\{\infty, \infty'\}$, then the vectors $\ell''(T)$, $\ell'(T)$, $\ell''(R)$, $\ell'(R)$ are linearly dependent if and only if $x(R) = x(T)$. This never happens if $R \in W$ and $T = s(R)$. We have obtained the desired contradiction, thus completing the proof of Lemma 40. □

Proof of Theorem 38. Let Ω denote the set of elements in $\mathbb{Z}_p^{2n+1}\backslash\{\Delta = 0\}$ corresponding to monic even hyperelliptic curves C such that $C(\mathbb{Q}_p)\backslash\{\infty, \infty'\}$ contains bad points. Let $\overline{\Omega}$ denote the closure of Ω, which by Theorem 39 has measure 0 in $\mathbb{Z}_p^{2n+1}$. Therefore, for every $\epsilon > 0$ there exists a subset $U(\epsilon)$ of $\mathbb{Z}_p^{2n+1}\backslash\{\Delta = 0\}$ such that $U(\epsilon)$ is defined by congruence conditions modulo some fixed power of p, the measure of $U(\epsilon)$ is at least $1 - \epsilon$, and every curve corresponding to a point in $U(\epsilon)$ has no bad points over $\mathbb{Q}_p$ apart from ∞ and ∞'. Therefore the proportion of hyperelliptic curves C over $\mathbb{Q}$ that are good is at least $1 - \epsilon$. Letting ϵ tend to 0, we obtain Theorem 38. □

Theorem 1 follows from Theorems 37 and 38.

https://doi.org/10.1112/S0010437X17007515

Acknowledgements

We are very grateful to Manjul Bhargava and Benedict Gross for suggesting this problem to us and for many helpful conversations. We are also very grateful to Bjorn Poonen for explaining Chabauty's method to us and for helpful comments on earlier versions of the argument. We are extremely grateful to Cheng-Chiang Tsai, Jacob Tsimerman, and Ila Varma for several helpful conversations. We are also very grateful for detailed and helpful comments from the annonymous referee. The first author is grateful for support from NSF grant DMS-1128155. The second author is grateful for support from a Simons Investigator Grant and NSF grant DMS-1001828.

References

BMSW07 B. Bektemirov, B. Mazur, W. Stein and M. Watkins, *Average ranks of elliptic curves: tension between data and conjecture*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), 233–254 (electronic).

Bha05 M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), 1031–1063.

Bha10 M. Bhargava, *The density of discriminants of quintic rings and fields*, Ann. of Math. (2) **172** (2010), 1559–1591.

Bha13 M. Bhargava, *Most hyperelliptic over $\mathbb{Q}$ curves have no rational points*, Preprint (2013), arXiv:1308.0395.

BG13 M. Bhargava and B. Gross, *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, in *Automorphic representations and L-functions*, Tata Inst. Fundam. Res. Stud. Math., vol. 22 (Tata Institute of Fundamental Research, Mumbai, 2013), 23–91.

BG14 M. Bhargava and B. Gross, *Arithmetic invariant theory*, in *Symmetry: representation theory and its applications*, Progress in Mathematics, vol. 257 (Birkhäuser, New York, 2014), 33–54.

BS15 M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), 191–242.

BSW16 M. Bhargava, A. Shankar and X. Wang, *Squarefree values of polynomial discriminants I*, Preprint (2016), arXiv:1611.09806.

Bor62 A. Borel, *Ensembles fondamentaux pour les groupes arithmétiques*, in *Colloque sur la Théorie des Groupes Algébriques, Bruxelles* (1962), 23–40.

BLR90 S. Bosch, W. Lutkebohmert and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21 (Springer, Berlin, 1990).

Cha41 C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.

Col85 R. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), 765–770.

Dav51 H. Davenport, *On a principle of Lipschitz*, J. Lond. Math. Soc. **26** (1951), 179–183. *Corrigendum: 'On a principle of Lipschitz'*, J. Lond. Math. Soc. **39** (1964), 580.

DD88 J. Denef and L. van den Dries, *p-adic and real subanalytic sets*, Ann. of Math. (2) **128** (1988), 79–138.

Lan66 R. P. Langlands, *The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups*, in *Algebraic groups and discontinuous subgroups*, Proceedings of Symposia in Pure Mathematics, vol. 9 (American Mathematical Society, Providence, RI, 1966), 143–148.

PR94 V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139 (Academic Press, Boston, MA, 1994). Translated from the 1991 Russian original by Rachel Rowen.

PS97 B. Poonen and E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188.

PS14 B. Poonen and M. Stoll, *Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) **180** (2014), 1137–1166.

Ser73 J. P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7 (Springer, New York, 1973).

Sto01 M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arithmetica **XCVIII.3** (2001), 245–277.

Wan13a X. Wang, *Maximal linear spaces contained in the base loci of pencils of quadrics*, Preprint (2013), arXiv:1302.2385.

Wan13b X. Wang, *Pencils of quadrics and Jacobians of hyperelliptic curves*, PhD thesis, Harvard University (2013).

Arul Shankar arul.shnkr@gmail.com
Department of Mathematics, University of Toronto, Toronto, Ontario, Canada

Xiaoheng Wang x46wang@uwaterloo.ca
Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada