TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 372, Number 1, 1 July 2019, Pages 267–304
https://doi.org/10.1090/tran/7546
Article electronically published on October 10, 2018

2-SELMER GROUPS OF HYPERELLIPTIC CURVES WITH MARKED POINTS

ANANTH N. SHANKAR

Abstract. We consider the family of hyperelliptic curves over $\mathbb{Q}$ of fixed genus along with a marked rational Weierstrass point and a marked rational non-Weierstrass point. When these curves are ordered by height, we prove that the average Mordell–Weil rank of their Jacobians is bounded above by 5/2, and that most such curves have only three rational points. We prove this by showing that the average rank of the 2-Selmer groups is bounded above by 6. We also consider another related family of curves and study the interplay between these two families. There is a family ϕ of isogenies between these two families, and we prove that the average size of the ϕ-Selmer groups is exactly 2.

1. Introduction

There has been a lot of recent progress while studying the statistics of Jacobians and rational points of families of curves. In [5], Bhargava and Gross prove that when all odd-degree hyperelliptic curves over $\mathbb{Q}$ are ordered by height, the average size of the 2-Selmer group of their Jacobians is bounded by 3, and the average rank of the Jacobians is bounded by 3/2. Using these results, Poonen and Stoll prove in [15] that a positive proportion of odd-degree hyperelliptic curves over $\mathbb{Q}$ have exactly one rational point (namely, the Weierstrass point at infinity), and that this proportion goes to 1 as the genus goes to infinity. In [16], Shankar and Wang prove results analogous to [5], [15] for the family of monic even-degree hyperelliptic curves. Thorne, in [19], studies the statistics of the 2-Selmer set in a family of nonhyperelliptic curves, which is a pointed subset of the 2-Selmer group. He proves that the average size of the 2-Selmer set is finite. He uses these statistics to prove that a positive proportion have integral points everywhere locally but have no global integral points.

In this work, we prove results about average Selmer sizes for different families of curves. We recall the definition of ϕ-Selmer groups, where $\phi : A \to B$ is an isogeny of abelian varieties over $\mathbb{Q}$. Let $A[\phi]$ denote its kernel. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the exact sequence

$$0 \to A[\phi](\overline{\mathbb{Q}}) \to A(\overline{\mathbb{Q}}) \to B(\overline{\mathbb{Q}}) \to 0$$

gives a long exact sequence of the Galois cohomology groups. In particular, there is an injective map $B(\mathbb{Q})/\phi A(\mathbb{Q}) \to H^1(\mathbb{Q}, A[\phi])$, where $H^1(\mathbb{Q}, A[\phi])$ is the Galois cohomology group of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with coefficients in $A[\phi](\overline{\mathbb{Q}})$. The ϕ-Selmer group Sel_ϕ over $\mathbb{Q}$ is a finite subgroup of $H^1(\mathbb{Q}, A[\phi])$ consisting of elements which locally lie in the images of $B(\mathbb{Q}_v)/\phi A(\mathbb{Q}_v)$ for all completions $\mathbb{Q}_v$ of $\mathbb{Q}$. This definition

Received by the editors December 15, 2017, and, in revised form, December 16, 2017, and February 21, 2018.

2010 *Mathematics Subject Classification.* Primary 11G10; Secondary 11G30, 14G05.

recovers the classical definitions of the n-Selmer groups by choosing the isogeny ϕ to be a multiplication by n.

Consider a smooth hyperelliptic curve C_1 of genus $m \geq 2$ over $\mathbb{Q}$, with a marked rational Weierstrass point that we denote by ∞_1, and a marked rational non-Weierstrass point that we denote by P_1. Let P_1' denote the conjugate of P_1 under the hyperelliptic involution. Without loss of generality, we may assume that under the natural map $C_1 \to \mathbb{P}^1$, ∞_1 maps to $\infty \in \mathbb{P}^1(\mathbb{Q})$, and P_1 maps to $0 \in \mathbb{P}^1(\mathbb{Q})$. Therefore, C_1 has an affine equation of the form

$$y^2 = x^{2m+1} + a_1 x^{2m} + \cdots + a_{2m} x + e^2 = f(x),$$

where $f(x) \in \mathbb{Q}[x]$ is separable over $\mathbb{Q}$, and $e \in \mathbb{Q}^\times$. If we assume that $f(x)$ has integral coefficients, and that there is no prime p, such that $p^{2i} | a_i$ for all i and $p^{2m+1} | e$, then the equation $y^2 = f(x)$ is unique. Denote the family of such polynomials by $\mathcal{B}$. We define the height of C_1 to be

$$\mathrm{ht}(C_1) := \mathrm{ht}(f) := \max\{|a_i|^{1/2i}, |e|^{1/2m+1}\}.$$

It follows from this definition that for a fixed $X \in \mathbb{R}$, there are finitely many curves with height bounded by X. Let J_1 denote the Jacobian of C_1. The first main result of the paper is as follows.

Theorem 1.1. *When all hyperelliptic curves of a fixed genus $m \geq 2$ having a marked rational Weierstrass point and a marked rational non-Weierstrass point are ordered by height, the average size of the 2-Selmer groups of their Jacobians is bounded above by 6.*

The family considered in [16] is the family of hyperelliptic curves with a marked non-Weierstrass point. The additional presence of the marked Weierstrass point ∞_1 in a curve C_1 of our family has the consequence of introducing a square root of the class of $(P_1) - (P_1')$ in $J_1(\mathbb{Q})$, where J_1 is the Jacobian of C_1. Indeed, $(P_1) - (P_1')$ is twice the class of $(P_1) - (\infty)$. We therefore expect that despite the existence of the extra marked Weierstrass point, the statistics of the 2-Selmer size for our family is the same as the statistics for the family of even hyperelliptic curves. This expectation is supported by the fact that our result agrees with [16, Theorem 2].

We prove that for 100% of the curves in our family, the class of $(P_1) - (\infty_1)$ in $J_1(\mathbb{Q})$ is not divisible by 2. Therefore, the average contribution of $(P_1) - (\infty_1)$ to the 2-rank of $\mathrm{Sel}_2(J_1)$ is 1. Denote the 2-rank by r_1. The following inequality holds 100% of the time:

$$2(r_1 - 1) \leq 2^{r_1 - 1} = \frac{\#\,\mathrm{Sel}_2(J_1)}{2}.$$

It follows that the average 2-rank of the 2-Selmer groups of Jacobians of curves in our family is at most 5/2. Because the 2-Selmer rank is an upper bound for the Mordell–Weil rank, we obtain the following corollary.

Corollary 1.2. *When all hyperelliptic curves of a fixed genus $m \geq 2$ having a marked rational Weierstrass point and a marked rational non-Weierstrass point are ordered by height, the average rank of the Mordell–Weil group of their Jacobians is bounded above by 5/2.*

To a curve C_1 corresponding to $f(x) \in \mathcal{B}$, we associate two other curves C_2 and C, where C_2 is defined by the equation $y^2 = xf(x)$, and C is defined by the equation $y^2 = f(x^2)$. We therefore obtain two other families of hyperelliptic

curves as f varies over $\mathcal{B}$. We have $J_1[2] \simeq J_2[2]$ as group schemes over $\mathbb{Q}$, where J_1 and J_2 are the Jacobians of C_1 and C_2, respectively. We denote this group scheme by Δ. There are canonical maps $C \to C_1$ $((x,y) \mapsto (x^2,y))$ and $C \to C_2$ $((x,y) \mapsto (x^2,xy))$. The Jacobians of these curves form the exact sequence

$$0 \longrightarrow \Delta \longrightarrow J_1 \times J_2 \xrightarrow{\phi} J \longrightarrow 0,$$

where J denotes the Jacobian of C.

Theorem 1.3. *Let the notation be as above. When $f \in \mathcal{B}$ is ordered by height, the average size of the ϕ-Selmer group is* 2.

We prove this theorem by studying the interplay between the 2-Selmer groups of J_1 and J_2 inside $H^1(\mathbb{Q},\Delta)$. Denote their intersection by $\mathrm{Sel}_{(1,2)}(f)$. Since the ϕ-Selmer group of $J_1 \times J_2 \to J$ equals $\mathrm{Sel}_{(1,2)}$, Theorem 1.3 follows from the following result.

Theorem 1.4. *The average size of* $\mathrm{Sel}_{(1,2)}(f)$*, as $f \in \mathcal{B}$ is ordered by height, is equal to* 2.

The group $\mathrm{Sel}_{(1,2)}$ always contains the identity of $H^1(\mathbb{Q},\Delta)$, and the image of $(P_1) - (\infty_1) \in J_1(\mathbb{Q})/2J_1(\mathbb{Q}) \subset H^1(\mathbb{Q},\Delta)$. Theorem 1.4 implies that 100% of the time, $\mathrm{Sel}_{(1,2)}$ contains nothing else.

Following [15], [16], we apply Theorem 1.1 to bound the number of rational points on C_1 and C.

Theorem 1.5. *Let $m \geq 4$. A proportion of at least $1 - (6m+19)2^{3-m}$ curves in the families C_1 and C have exactly* 3 *and* 4 *rational points, respectively.*

The structure of the paper follows [5]. In §2, we consider the representation $n \otimes n$ of the split semisimple group $\mathrm{SO}_n \times \mathrm{SO}_n$, where $n = 2m+1$ is an odd integer. This representation arises from Vinberg theory for the group SO_{2n}, i.e., groups of the form D_{odd}.[1] A vector in this representation can be viewed as a self-adjoint operator on a $2n$-dimensional vector space whose characteristic polynomial is of the form

$$f(x^2) = x^{2n} + a_1 x^{2(n-1)} + \cdots + a_{n-1}x^2 + e^2.$$

The functions $a_1, \ldots, a_{n-1}, e$ are invariant under the action of $\mathrm{SO}_n \times \mathrm{SO}_n$. In fact, these freely generate the ring of $\mathrm{SO}_n \times \mathrm{SO}_n$ invariants. A point in the invariant space is said to be regular semisimple if the corresponding polynomial $f(x^2)$ is separable. Using Thorne's work [18], we demonstrate the existence of two sections κ_1 and κ_2 from the space of invariants to $n \otimes n$. Further, we prove that the orbit of $\kappa_i(c)$ is *distinguished* (which we define in §2), where c is regular semisimple.

In §3, we prove that the regular semisimple invariants separate geometric $\mathrm{SO}_n \times \mathrm{SO}_n$ orbits. Using the language of [4], we describe in §4 how geometric orbits break up over arbitrary fields.

In §5, we associate two pencils of quadrics with each $\mathrm{SO}_n \times \mathrm{SO}_n$ orbits on $n \otimes n$. The theory developed in [23] realizes the Fano variety of these pencils as torsors for J_1 and J_2, where J_1 is the Jacobian of the curve $y^2 = f(x)$, and J_2 is the Jacobian of the curve $y^2 = xf(x)$. We prove that there is a bijection between the 2-Selmer group of $J_1[2]$, and rational orbits with these invariants such that the first Fano variety has points over $\mathbb{Q}_v$ for every place v. We call these orbits *locally soluble*

[1] Groups of the form D_{even} parameterize families of hyperelliptic curves with two sets of rational non-Weierstrass points.

orbits. Similarly, there is a bijection between the intersection of the 2-Selmer groups of J_1 and J_2 and rational orbits such that both of the Fano varieties have points over $\mathbb{Q}_v$ for all places v. We call these orbits *locally* $(1,2)$*-soluble orbits*. A crucial ingredient needed to prove Theorems 1.1 and 1.4 is to demonstrate the existence of integral representatives (with a minor technical condition at place 2) of locally soluble $\mathrm{SO}_n(\mathbb{Q}) \times \mathrm{SO}_n(\mathbb{Q})$ orbits, which have integral invariants. This is done in §6, and the result we prove is stated as Theorem 6.2.

Having parameterized the Selmer groups in terms of integral soluble and (1,2)-soluble orbits, we use Bhargava's geometry of numbers techniques [1] to estimate the number of these orbits. In order to do this, in §7, we count the number of points inside a fundamental domain for the action of $\mathrm{SO}_n(\mathbb{Z}) \times \mathrm{SO}_n(\mathbb{Z})$ on $\mathbb{R}^n \otimes \mathbb{R}^n$. This fundamental domain splits into two parts: the main body, which we prove contains a negligible number of distinguished orbits, and the cusp, which we prove contains predominantly distinguished orbits.

In §8, we impose appropriate congruence conditions to pass from integral orbits to locally soluble integral orbits, or to locally (1,2)-soluble integral orbits. In the first case, the main body will contribute on average at most four Selmer elements (based on some work in progress of Bhargava, Arul Shankar, and Wang, we expect that the contribution will be exactly four Selmer elements on average), and the cusp will correspond to the distinguished orbits, which are the marked elements in the Selmer group. This gives that the average size of the 2-Selmer group is bounded by 6, proving Theorem 1.1. In the second case, we prove that the product of the local densities diverges to 0 (Proposition 8.6), so the only contribution to the average comes from the cusp. This proves Theorem 1.4.

Finally, we sketch the arguments used in [15], [16, §§5 and 6] in §9 to prove Theorem 1.5.

2. A representation of $\mathrm{SO_n} \times \mathrm{SO_n}$

Let k be a field of characteristic other than 2. In this section, we consider the action of $\mathrm{SO_n} \times \mathrm{SO_n}$ on $n \otimes n$, where n denotes the standard representation of the split special orthogonal group $\mathrm{SO_n}$.

2.1. **Vinberg theory.** The above representation is in the Vinberg setting. Indeed, let (V_1, Q_1, ϵ_1) be an n-dimensional split orthogonal space with discriminant 1 with respect to the basis ϵ_1 of $\bigwedge^{\mathrm{top}}(V_1)$, and let (V_2, Q_2, ϵ_2) be an n-dimensional split orthogonal space of discriminant $(-1)^n$ (the discriminant is again relative to $\epsilon_2 \in \bigwedge^{\mathrm{top}}(V_2)$). Consider the $2n$-dimensional split orthogonal space $V = V_1 \oplus V_2, Q = Q_1 \oplus Q_2$, and the special orthogonal group $G = \mathrm{SO}(V)$ (the discriminant condition on (V_2, Q_2) is imposed so that the space (V, Q) is split).

We consider the involution θ of $\mathrm{SO}(V)$, given by conjugation by the element $(\mathrm{I}_n, -\mathrm{I}_n) \in \mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$. Let G^θ be the subgroup fixed by θ. It is the intersection of $\mathrm{O}(V_1) \times \mathrm{O}(V_2)$ with $\mathrm{SL}(V)$ inside $\mathrm{GL}(V)$. The involution θ also acts on the Lie algebra $\mathfrak{g}$. Let $\mathfrak{g}_1$ denote the -1 eigenspace. It consists of skew self-adjoint operators on V whose diagonal blocks (with respect to the decomposition $V = V_1 \oplus V_2$) are 0.

The action of G^θ on $\mathfrak{g}$ preserves the eigenspace $\mathfrak{g}_1$. As representations of G^θ, $\mathfrak{g}_1 \cong V_1 \otimes V_2$. The isomorphism can be described as follows: given an element $\alpha \in V_1 \otimes V_2$, we think of it as an operator $T_1 : V_1 \to V_2$ using the bilinear form on

V_1. Similarly, we get an operator $T_2 : V_2 \to V_1$. The operator $T_1 \oplus (-T_2) \in \mathfrak{g}_1$, i.e., is a skew self-adjoint operator on V with block diagonal 0.

Notice that the space W, consisting of self-adjoint operators on V with block diagonal 0, is also a representation of G^θ. This representation is also isomorphic to $V_1 \otimes V_2$, where α would map to $T_1 \oplus T_2$.

The G-invariant functions on $\mathfrak{g}$ restrict to G^θ-invariant functions on $\mathfrak{g}_1$. Let $T' \in \mathfrak{g}$. Since T' is skew self-adjoint, the coefficients of the odd powers of the characteristic polynomial will all be 0. Suppose that the characteristic polynomial of T' is $g_1(x) = f_1(x^2) = x^{2n} + b_1 x^{2n-2} + \cdots + b_{n-1}x^2 + b_n$. Because T' is skew self-adjoint, $b_n = (-1)^n e^2$, where e is the Pfaffian of T'. The functions $b_1, \ldots, b_{n-1}, e$ freely generate the ring of G-invariant functions on $\mathfrak{g}$. By Vinberg's theory, the ring of G^θ-invariant functions on $\mathfrak{g}_1$ is freely generated by $b_1, \ldots, b_{n-1}, e$ if the characteristic of k is 0 [13, Theorem 3.6].

If the characteristic polynomial of the associated skew self-adjoint operator is as above, the characteristic polynomial of the associated self-adjoint operator $T_1 \oplus T_2$ will just be $g(x) = f(x^2) = x^{2n} + a_1 x^{2n-2} + \cdots + a_{n-1}x^2 + a_n$, with $a_i = (-1)^i b_i$. Note that we now get $e^2 = a_n$. Henceforth, we will think of $\alpha \in V_1 \otimes V_2$ as a self-adjoint operator T on V with block diagonal 0. For notational reasons, we will use the symbol α when we want to talk of an element of $V_1 \otimes V_2$ in the abstract, and we will use the symbol T when we want to think of α as a self-adjoint operator on V. We call g the characteristic polynomial of α. We summarize this in the following definition.

Definition 1. Let $\alpha \in V_1 \otimes V_2$. We define $T' = T_1 \oplus (-T_2) \in \mathfrak{g}_1$ to be the associated skew self-adjoint linear transformation on V, and we define $T = T_1 \oplus T_2$ to be the associated self-adjoint transformation on V.

The invariants a_i, e are homogeneous functions, with the degree of a_i being $2i$, and the degree of e being n. Note that the sum of the degrees of the invariants is n^2, the dimension of $V_1 \otimes V_2$.

Define $\mathrm{Inv} = \operatorname{Spec} k[a_1, a_2, \ldots, a_{n-1}, e]$. If the characteristic of k is 0, then $\mathrm{Inv} \simeq V_1 \otimes V_2 /\!\!/ G^\theta$, the geometric invariant theory quotient of $V_1 \otimes V_2$ by G^θ. Even if k has a positive characteristic, there is still a G^θ-equivariant map from $V_1 \otimes V_2$ to Inv, where the action of G^θ on Inv is trivial. In either case, $\pi : V_1 \otimes V_2 \to \mathrm{Inv}$ denotes the G^θ-equivariant map.

Definition 2. We say that an element $\alpha \in V_1 \otimes V_2$ is regular semisimple if its characteristic polynomial splits into distinct linear factors over k^{sep}, i.e., if the discriminant of $g(x)$ is different from 0.

Note that α will be regular semisimple if and only if the polynomial f has a nonzero discriminant and $f(0) \neq 0$. In terms of the map π, the regular semisimple locus in $V_1 \otimes V_2$ equals $\pi^{-1}(\mathrm{Inv}^{\mathrm{rs}})$, where $\mathrm{Inv}^{\mathrm{rs}}$ is the locus where e and the discriminant of f are both nonzero.

Henceforth, we will assume that n is an odd integer. Let $n = 2m + 1$.

2.1.1. *Regular nilpotent orbits and Kostant sections.* In this paragraph, we assume that the characteristic of k is 0 because the paper [18] assumes that k has characteristic 0. We also think of $V_1 \otimes V_2$ as being $\mathfrak{g}_1$, i.e., as skew self-adjoint operators with block diagonal 0.

Definition 3. An element $x \in \mathfrak{g}$ is called regular nilpotent if it is nilpotent and its centralizer in $\mathfrak{g}$ has a dimension equal to the rank of $\mathfrak{g}$. We say that $x \in \mathfrak{g}_1$ is regular nilpotent if it is regular nilpotent when thought of as an element of $\mathfrak{g}$.

Proposition 2.1. *There are exactly two distinct $G^\theta(k)$ orbits of regular nilpotent elements of $\mathfrak{g}_1$.*

Proof. Let Z and G_{ad} denote the center and the adjoint of G, respectively. Clearly, θ acts trivially on Z and hence descends to an involution of G_{ad}. Let $(G_{\mathrm{ad}})^\theta$ denote the subgroup of G_{ad} fixed by θ.

We have that $(G_{\mathrm{ad}})^\theta(\overline{k}) = \{g \in G(\overline{k}) | \theta(g) \in Z(\overline{k})g\}/Z(\overline{k})$. Clearly, G^θ/Z is a subgroup of $(G_{\mathrm{ad}})^\theta$, and the description of $\overline{k}$-points shows that the inclusion has index 2. The group G^θ/Z is isomorphic to $\mathrm{SO}(V_1) \times \mathrm{SO}(V_2)$ (this requires the assumption that n is odd) and is therefore the connected component of $(G_{\mathrm{ad}})^\theta$. Finally, it is easy to see that there always exists a $g \in G(k)$ with the property $\theta(g) = -g$. It follows that $(G^\theta/Z)(k)$ is always an index-2 subgroup of $G^\theta_{\mathrm{ad}}(k)$.

By [18, Lemma 2.13], $G^\theta_{\mathrm{ad}}(k)$ acts simply transitively on the set of regular nilpotent elements of $\mathfrak{g}_1(k)$. Therefore, the action of $(G^\theta/Z)(k)$ on the set of regular nilpotent elements has two orbits, as required. □

We now explicitly describe these two conjugacy classes of regular nilpotent elements. By the assumption on Q_1, there exists a basis $\{f_1, \ldots, f_{2m+1}\}$ of V_1, such that the Gram matrix of Q_1 is

$$B = \begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & 1 & & & \\ 1 & & & & \end{bmatrix}. \tag{1}$$

Similarly, there exists a basis $\{f'_1, \ldots, f'_{2m+1}\}$ of V_2 such that the Gram matrix of Q_2 is $-B$. Let $E_1 \in \mathfrak{g}_1$ be as follows:

$$f_1 \to f'_1,\ f'_1 \to f_2, \ldots, f'_{m-1} \to f_m,\ f_m \to f'_{m+1}, \ldots,$$
$$f'_{2m+1} \to f_{2m+1},\ f_{2m+1} \to 0; \quad f'_m \to 0.$$

Let E_2 be defined the same way, except with the f_i and f'_i swapped. Both the skew self-adjoint E_1 and E_2 are regular nilpotent elements of $V_1 \otimes V_2$. It is easy to see that E_1 and E_2 are in the same $G^\theta_{\mathrm{ad}}(k)$ orbit but in different $G^\theta(k)$ orbits.

By [18, Lemma 2.15], E_1 can be completed to an $\mathfrak{sl}_2$ triple (E_1, F_1, H_1) with $F_1 \in \mathfrak{g}_1$ and $H_1 \in \mathfrak{g}^{\theta=1}$ in a unique way. The same is true for E_2 (and we call the triple (E_2, F_2, H_2)). Let $\mathfrak{z}(F_1) = \{Z \in \mathfrak{g}_1 : [Z, F_1] = 0\}$ (and let $\mathfrak{z}(F_2)$ be defined analogously). By [18, Lemma 3.5], the two $\kappa'_i : E_i + \mathfrak{z}(F_i) \to \mathrm{Inv}$ (for $i = 1,\ 2$) are isomorphisms and thus give rise to two sections $\kappa_i : \mathrm{Inv} \to \mathfrak{g}_1$.

Definition 4. The sections κ_i are called Kostant sections.

Proposition 2.2. *Let $T' \in E_i + \mathfrak{z}(F_i)$ (where i is either 1 or 2) be a regular semisimple element. Then there exists $X \subset V_i$ a maximal isotropic subspace (for the quadratic form Q_i), with the property $T'^2 X \subset X^\perp$ ($^\perp$ is taken with respect to the quadratic form Q_i).*

Proof. It suffices to prove the result for $i = 1$. We will show that X can be chosen to be $\langle f_1, f_2, \ldots, f_m\rangle$, where $\langle\ \rangle$ denotes the span. We have $X^\perp = \langle X, f_{m+1}\rangle$. Notice that $\langle f_i\rangle$ and $\langle f_i'\rangle$ will be weight-spaces for H_1. Hence, we have F_1 acting as follows:

$$\langle f_1\rangle \leftarrow \langle f_1'\rangle,\ \langle f_1'\rangle \leftarrow \langle f_2\rangle,\ \ldots,\ \langle f_{m-1}'\rangle \leftarrow \langle f_m\rangle,$$
$$\langle f_m\rangle \leftarrow \langle f_{m+1}'\rangle,\ \ldots,\ \langle f_{2m+1}'\rangle \leftarrow \langle f_{2m+1}\rangle;$$
$$\langle f_1, f_m'\rangle \to 0.$$

The kernel of F_1^{2m} is $\langle f_1, \ldots, f_m, f_1', \ldots, f_{m+1}'\rangle$, and the kernel of F_1^{2m+1} is $\langle f_1, \ldots, f_{m+1}, f_1', \ldots, f_{m+1}'\rangle$. Thus, any $Z \in \mathfrak{z}(F_1)$ must preserve the above two subspaces. Therefore,

$$T'\langle f_1, \ldots, f_m, f_1', \ldots, f_m'\rangle \subset \langle f_1, \ldots, f_m, f_1', \ldots, f_{m+1}'\rangle,$$
$$T'\langle f_1, \ldots, f_m, f_1', \ldots, f_{m+1}'\rangle \subset \langle f_1, \ldots, f_{m+1}, f_1', \ldots, f_{m+1}'\rangle,$$

and consequently

$$T'^2\langle f_1, \ldots, f_m, f_1', \ldots, f_m'\rangle \subset \langle f_1, \ldots, f_{m+1}, f_1', \ldots, f_{m+1}'\rangle.$$

The proposition follows from the fact that T'^2 preserves V_1. □

Let T denote the self-adjoint operator defined in Definition 1 (which satisfies the relation $T^2 = -T'^2$). If $\alpha \in \kappa_i(\mathrm{Inv})$, T also satisfies the conclusions of Proposition 2.2. To that end, for k having a characteristic other than 2, we make the following definition.

Definition 5. We call $\alpha \in V_1 \otimes V_2$ and the associated self-adjoint operator T i distinguished (for $i = 1, 2$) if there exists a maximal isotropic subspace (with respect to the form Q_i) $X \subset V_i$ such that $T^2X \subset X^\perp$ ($^\perp$ is taken with respect to Q_i).

2.2. G_0^θ **from** G^θ**.** Let $G_0^\theta = \mathrm{SO}(V_1) \times \mathrm{SO}(V_2)$ be the connected component of G^θ containing the identity. Note that it has index 2 in G^θ. As n is odd, $-\mathrm{I}_n \in \mathrm{GL}(V)$ is an element of G^θ, but not of G_0^θ. The element $-\mathrm{I}_n$ acts trivially on $V_1 \otimes V_2$, so $V_1 \otimes V_2 /\!\!/ G^\theta = V_1 \otimes V_2 /\!\!/ G_0^\theta$. Further, for any field k, we have that $V_1 \otimes V_2(k)/G_0^\theta(k) = V_1 \otimes V_2(k)/G^\theta(k)$.

Henceforth, we define G_i to be $\mathrm{SO}(V_i)$ for $i = 1, 2$. For ease of notation, let $H = G_1 \times G_2$. We will henceforth use the notation W for $V_1 \otimes V_2$.

3. Orbits over a separably closed field

Recall that we have assumed that $n = 2m + 1$ is an odd integer. In this section, we prove that over a separably closed field k, regular semisimple elements having the same invariants lie in the same $H(k)$ orbit.

Proposition 3.1. *Let S and T be regular semisimple elements in W with block diagonal 0. Suppose that S and T have the same invariants. Then there exists a $g \in H(k)$ such that $gSg^{-1} = T$.*

Proof. Suppose that the common characteristic polynomial is $g(x) = f(x^2)$. If λ is an eigenvalue, then so is $-\lambda$. Let $w_{\pm 1}$, $w_{\pm 2}$, …, $w_{\pm n}$ and $w'_{\pm 1}$, $w'_{\pm 2}$, …, $w'_{\pm n}$ be the eigenvectors of S and T, respectively, with eigenvalues $\pm\lambda_1 \cdots \pm \lambda_n$. By considering S^2, we see that for any i, the span of the two vectors $w_{\pm i}$ intersected with V_1 (and V_2) is one dimensional. Of course, the same reasoning applies to the span of the two vectors $w'_{\pm i}$. Note that w_i (and w_i') form a basis orthogonal for the form on V, since S and T are self-adjoint and the eigenvalues $\pm\lambda_i$ are distinct.

Without loss of generality, assume that $w_i + w_{-i}$ (and the same with w') lies in V_1 for every i. As S maps V_1 to V_2, $\lambda_i(w_i - w_{-i})$, and therefore $w_i - w_{-i}$ has to lie in V_2. We have $(w_i + w_{-i}, w_i - w_{-i}) = 0$ where $(\ ,\ )$ is the bilinear form associated with Q, whence $Q(w_i) = Q(w_{-i})$. Clearly, the same happens with $w'_{\pm i}$. By scaling $w'_{\pm i}$ appropriately, we may assume that $Q(w_{\pm i}) = Q(w'_{\pm i})$.

Therefore, the transformation g taking $w_{\pm i}$ to $w'_{\pm i}$ is orthogonal (the bases w_i and w'_i being orthogonal for the form), and conjugation by g takes T to S. Finally, the fact that the $(w_i + w_{-i})$ (resp., $(w_i - w_{-i})$) span V_1 (resp., V_2) implies that g preserves V_1 (resp., V_2). Therefore, g lies in the subgroup $\mathrm{O}(V_1) \times \mathrm{O}(V_2)$. Conjugating by g multiplies the Pfaffian by the determinant of g. The fact is that the two operators S and T have the same Pfaffian forces g to lie in $\mathrm{SL}(V)$, which means that $g \in G^\theta$. As remarked at the end of the previous section, we can choose g be an element of $H(k)$. □

The corollary below follows directly from Proposition 3.1.

Corollary 3.2. *For k as a separably closed field, two regular semisimple elements α_1 and α_2 lie in the same $H(k)$ orbit if and only if they have the same invariants.*

4. Orbits over an arbitrary field

In this section, we first demonstrate the existence of rational orbits with a given set of invariants, and we describe using the theory developed in [4] how a geometric orbit decomposes into rational orbits.

4.1. **Existence of orbits with a given set of invariants.** Fix a set of invariants $c = (a_1, a_2, a_3, \ldots, a_{n-1}, e) \in \mathrm{Inv}^{\mathrm{rs}}(k)$. Recall that we have associated to c two polynomials, $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + e^2$ and $g(x) = f(x^2)$. The existence of the Kostant sections proves that when the characteristic of k is 0, the set of k-rational orbits with invariants c is nonempty, i.e., $\pi^{-1}(c)(\overline{k})$ contains a k-rational point. We construct an explicit $T \in W(k)$ with invariants c. The construction holds for k having a characteristic other than 2.

Let $L = k[x]/(f(x))$, and let $M = k[x]/(g(x))$. There is an embedding of k-algebras $L \hookrightarrow M$ such that $x \mapsto x^2$. Let σ be the nontrivial automorphism of M which leaves L fixed. Let β and γ be the images of x in M and L, respectively. By definition, $\gamma = \beta^2$ and σ sends β to $-\beta$. Define a symmetric bilinear form $(\ ,\ )$ on M by setting

$$(\lambda, \mu) = \mathrm{Trace}_{M/k}(f'(\gamma)\lambda\mu).$$

For $\mu \in L$, we have $\mathrm{Trace}_{M/k}\, \beta\mu = 0$. Therefore, $(\ ,\ )$ breaks up into a direct sum of split bilinear forms on L and $L\beta$. An easy computation shows that these spaces have the discriminants 1 and $(-1)^n = (-1)$, respectively. Isometrically identifying L and $L\beta$ with V_1 and V_2, respectively, the self-adjoint operator T_β on M (given by multiplication by β) pulls back to a self-adjoint operator T on V. Clearly, T is self-adjoint, maps V_1 to V_2 and V_2 to V_1, and therefore corresponds to an orbit of $\alpha_1 \in W(k)$ of our representation. The invariants of T are c by construction, up to the sign of the Pfaffian. To obtain an operator with the same invariants except for the sign of the Pfaffian being reversed, replace β with $-\beta$.

For $c \in \mathrm{Inv}^{\mathrm{rs}}(k)$, let $\alpha_1(c) \in W(k)$ denote the orbit just constructed.

Proposition 4.1. *The stabilizer Δ_c of $\alpha_1(c)$ is isomorphic to the kernel of the norm map $\mathrm{Res}_{L/k}(\mu_2) \to \mu_2$.*

Proof. The stabilizer Δ_c of this orbit is the space of orthogonal linear transformations on M which preserve L and $L\beta$, commute with T_β, and have determinant 1 when restricted to L and $L\beta$.

As the orbit is regular semisimple, the centralizer of T_β in $\mathrm{GL}(M)$ (with M thought of as a k-vector space) is $M^\times$ (acting on M by multiplication). That Δ_c is a subgroup of $\mathrm{SO}(M)$ implies that only elements $\lambda \in M^\times$ of the form $\lambda^2 = 1$ are allowed. We have $M^\times \cap \mathrm{GL}(V_1) \times \mathrm{GL}(V_2) = L^\times$, and therefore $\lambda \in L^\times$. Finally, the determinant condition forces $N_{L/k}(\lambda) = 1$. The proposition follows. □

Corollary 4.2. *We have $\Delta_c(k) \neq \{1\}$ precisely when the polynomial f is not irreducible.*

Proof. The étale algebra L is a field precisely when f is irreducible. Applying Proposition 4.1 finishes the proof. □

Note that the intersection of $L^\times$ (and therefore Δ_c) with $\mathrm{GL}(V_1) \times \{1\}$, and with $\{1\} \times \mathrm{GL}(V_2)$, is just the identity. This implies that either projection restricted to $L^\times$ (and therefore to Δ_c) is an isomorphism onto its image.

Corollary 4.3. *For $c \in \mathrm{Inv}^{\mathrm{rs}}(k)$, Δ_c is isomorphic to the stabilizer of any other $\alpha \in W(k)$ with the same invariants.*

Proof. Let T be the operator corresponding to α. By Proposition 3.2, there exists a $g \in H(k^{\mathrm{sep}})$ such that gT is the operator associated with $\alpha_1(c)$, which for ease we denote by S. Conjugation by g provides an isomorphism between the stabilizers of S and T, a priori defined only over k^{sep}. Clearly, conjugation by $\sigma(g)$ is the isomorphism between the stabilizers obtained by applying σ to the previous isomorphism, where $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

We claim that the two maps are the same. Indeed, S and T are k-rational, so $\sigma(g)T = gT$, thereby forcing $g^{-1}\sigma(g) \in \Delta_c$. Therefore, the two maps differ by conjugation by an element of Δ_c. The fact that Δ_c is abelian forces the two maps to be the same. Therefore, the isomorphism between the two stabilizers is defined over k, proving the result. □

4.2. **Distinguished orbits.**

Proposition 4.4. *Fix $c \in \mathrm{Inv}^{\mathrm{rs}}(k)$. Then $H(k)$ acts simply transitively on the set of pairs (T, X), where $T \in W(k)$ and $\pi(T) = c$, and $X \subset V_1$ is a maximal isotropic subspace, with the property that $T^2X \subset X^\perp$.*

Proof. We first show that the stabilizer of such pairs is just the identity. Let $g = (g_1, g_2) \in \mathrm{SO}(V_1) \times \mathrm{SO}(V_2)(k)$ be an element in the stabilizer. Then g_1, thought of as an element of $\mathrm{SO}(V_1)$, commutes with the self-adjoint operator T^2 restricted to V_1 and also preserves the subspace X. By [5, Proposition 4.1], $g_1 = \mathrm{I}_n$. As remarked above, this forces $g_2 = \mathrm{I}_n$, as required. Because this stabilizer is trivial, an easy descent argument shows that it suffices to prove the statement over k^{sep}.

By Proposition 3.2, it suffices to prove that (T, X') and (T, X) are in the same orbit, where X' is a subspace with the same properties as X. By [5, Proposition 4.1], there exists a $g_1 \in \mathrm{SO}(V_1)$ which commutes with T^2 such that $g_1 X' = X$. It suffices to demonstrate the existence of $g_2 \in \mathrm{SO}(V_2)$ such that $g = (g_1, g_2) \in \Delta_c$. By [5, Proposition 4.1], the centralizer Δ_{V_1} of T^2 in $\mathrm{SO}(V_1)$ is an abelian 2-group of order 2^{n-1}, which is the same as the order of Δ_c. Therefore, the projection map

(having a trivial kernel) from Δ_c to Δ_{V_1} must be a bijection, whence we deduce the existence of the required g_2. □

It is easy to see that $\alpha_1 \in W(k)$ is 1-distinguished. Similarly, in the next subsection, we will explicitly construct a corresponding α_2 which is 2-distinguished. Over a separably closed field, these two operators will lie in the same H-orbit.

4.3. **The remaining orbits.** We again fix $c \in \mathrm{Inv}^{\mathrm{rs}}(k)$. Let W_c denote the fiber of π over c. Proposition 3.2 can be rephrased as stating that $H(k^{\mathrm{sep}})$ acts transitively on $W_c(k^{\mathrm{sep}})$. Once one particular $H(k)$-orbit is fixed, by [4, Proposition 1], the set $W_c(k)/H(k)$ is in bijection with the kernel of a map of pointed sets $\delta : H^1(k, \Delta_c) \to H^1(k, H)$ (the notation used in [4] is γ, not δ). We use $\alpha_1(v)$ (the 1-distinguished orbit) as our fixed orbit and explicitly describe the map δ.

The Kummer exact sequence gives $H^1(k, \Delta_c) = (L^\times/L^{\times 2})_{N=1}$. To an element ν in $L^\times_{N=1}$, we associate the orthogonal space M with the bilinear form $\langle\ ,\ \rangle_\nu$, with $\langle \lambda, \mu\rangle_\nu = \mathrm{Trace}_{M/k}(f'(\gamma)\nu\lambda\mu)$. This orthogonal space corresponds to an element in $H^1(k, \mathrm{SO}(V))$. Clearly, the new form breaks up into a direct sum of forms on L and $L\beta$, so our cocycle actually lies in $H^1(k, H)$ (recall that $H = G_1 \times G_2$). Let $(\ ,\ )_\nu$ denote the bilinear form on L given by $(\lambda, \mu)_\nu = \mathrm{Trace}_{L/k}(f'(\gamma)\nu\lambda\mu)$. It is easy to see that $\langle\ ,\ \rangle_\nu = (\ ,\ )_\nu \oplus (\ ,\ )_{\text{-}\nu\gamma}$. The map δ maps the class ν to the element of $H^1(k, H)$ just described [4, Lemma 3]. The class of ν will be in the kernel precisely when the spaces L and $L\beta$ are both split. Note that this is the same as saying that the forms on L given by ν and $\nu\gamma$ are both split.

It is easy to see that the element $\nu = (-\gamma) \in H^1(k, \Delta_c)$ does lie in the kernel of δ. Therefore, $(-\gamma)$ gives rise to $\alpha_2 \in W_c(k)$, and its class in $H^1(k, \Delta_c)$ gives a k-rational orbit in $W_c(k)/H(k)$. In fact, the orbit of α_2 is 2-distinguished. Indeed, by [5, Equation 4.2], the bilinear form $(\ ,\ )_{\gamma^2}$ (which corresponds to the bilinear form on V_2 for the orbit α_2) can be described as

$$(\lambda, \nu) \mapsto \text{the coefficient of } \gamma^{2m} \text{ in the product } \gamma^2 f'(\gamma)^2 \lambda\nu.$$

Here, we mean the coefficient with respect to the basis $\{1, \gamma, \gamma^2, \ldots, \gamma^{2m}\}$. It follows that X, the span of $1/\gamma f'(\gamma), \gamma/\gamma f'(\gamma), \ldots, \gamma^{m-1}/\gamma f'(\gamma)$, is a maximal isotropic subspace satisfying the conditions laid out in Definition 5 for $i = 2$.

Summarizing, we have the following proposition.

Proposition 4.5. *For each $c \in \mathrm{Inv}^{\mathrm{rs}}(k)$, the $H(k)$ orbit of $\alpha_1(v) \in W(k)$ is 1-distinguished. The stabilizer of α_1, Δ_c, is isomorphic to $\mathrm{Res}_{L/k}(\mu_2)_{N=1}$. All of the other k-rational orbits with the same invariants have the same stabilizer, lie in the $H(k^{\mathrm{sep}})$-orbit of α_1, and correspond bijectively to the nonidentity classes in the kernel of $\delta : H^1(k, \Delta_c) \to H^1(k, H)$. The class of $\nu \in L^\times_{N=1}$ in $H^1(k, \Delta_c)$ corresponds to the space M along with the operator T_β and the bilinear form $\langle\ ,\ \rangle_\nu = (\ ,\ )_\nu \oplus (\ ,\ )_{\text{-}\nu\gamma}$, and it is in the kernel of δ exactly when $(\ ,\ )_\nu$ and $(\ ,\ )_{\text{-}\nu\gamma}$ are split. The class of $(-\gamma)$ is the 2-distinguished orbit, corresponding to the $H(k)$ orbit of α_2.*

An immediate corollary is the following.

Corollary 4.6. *Fix $c \in \mathrm{Inv}^{\mathrm{rs}}(k)$. The two distinguished orbits lie in the same $H(k)$-orbit if and only if $(-\gamma)$ is a perfect square in $L^\times$.*

5. Connection with hyperelliptic curves

In this section, we associate hyperelliptic curves and some torsors to rational orbits of our representation. Recall that we have assumed that $n = 2m + 1$ is odd. Given that $c \in \mathrm{Inv}^{\mathrm{rs}}(k)$, we associate the curves $C_{1,c}, C_{2,c}$ given by $y^2 = f(x)$ and $y^2 = xf(x)$. As usual, $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + e^2$, where $c = (a_1, \ldots, a_{n-1}, e)$.

The curves have marked points (rational over k). $C_{1,c}$ has a rational Weierstrass point which we call ∞_1, which lies above the point at infinity in $\mathbb{P}^1$. The points $(0, \pm e)$ are also k-rational and are conjugate for the hyperelliptic involution on $C_{1,c}$. We call these points P_1, P_1'. Similarly, the point of $C_{2,c}$ above 0 is a rational Weierstrass point, which we call P_2. There is also a pair of k-rational points above the point at infinity, ∞_2, ∞_2', which are conjugate for the hyperelliptic involution on $C_{2,c}$. Let $J_{i,c}$ be the Jacobians of $C_{i,c}$. Note that $J_{1,c}[2] \cong J_{2,c}[2] \cong \mathrm{Res}_{L/k}(\mu_2)_{N=1}$.

5.1. **Pencils of quadrics.** Suppose that $\alpha \in W_c^{\mathrm{rs}}(k)$, i.e., has invariants c. The 2-torsions of $J_{1,c}$ and $J_{2,c}$ are related to the stabilizer of α as follows.

Proposition 5.1. *The stabilizer Δ_c is isomorphic (as group schemes over k) to $J_{i,c}[2]$.*

Proof. The same proof as in [5, Proposition 5.1] applies. □

Recall that the $H(k)$-orbit of $\alpha_1(c)$ is 1-distinguished, and that the map δ (based at the orbit of α_1) described in the previous section gives a map from $W_c(k)/H(k) \to H^1(k, \Delta_c)$. The inclusion $A[2] \hookrightarrow A$ for any group scheme over k gives the natural map $H^1(k, A[2]) \to H^1(k, A)$. Therefore, for $i = 1, 2$, we have maps $W_c(k)/H(k) \to H^1(k, J_{i,c})$, by identifying Δ_c with $J_i[2]$. We recall the theory developed in [23] (also see [4], [22]), which describes these maps.

Recall that the vector spaces V_1 and V_2 are equipped with quadratic forms Q_1 and Q_2. Let B_1 and B_2 denote the associated bilinear forms. Let $\alpha \in W_c(k)$, and let $T = T_1 \oplus T_2$ be the associated self-adjoint matrix with block diagonal 0. Define $B_{1,T^2}(v_1, w_1) = B_1(v_1, T^2w_1)$ for $v_1, w_1 \in V_1$. Note that B_{1,T^2} is B_2 pulled back from V_2 by T_1. Denote by Q_1 and Q_{1,T^2} the corresponding quadratic forms on V_1.

Define P_α^1 to be the pencil of quadrics on the space $\mathbb{P}(V_1 \oplus k)$ spanned by Q_1' and Q_{1,T^2}', where $Q_1'((v_1, \lambda)) = Q_1(v_1)$ and $Q_{1,T^2}'((v_1, \lambda)) = Q_{1,T^2}(v_1, v_1) + \lambda^2$. Define F_α^1 to be the Fano variety of the base locus of P_α^1. The theory developed in [23] demonstrates F_α^1 as being a torsor for J_1. In fact, if the orbit of α corresponds to $\nu \in H^1(k, \Delta_c)$, then it is proved in [23, Corollary 2.23] that F_α^1 is the image of ν in $H^1(k, J_{1,c})$.

The same construction with the order of Q_1 and Q_{1,T^2} reversed gives a pencil of quadrics P_α^2. The associated Fano variety F_α^2 gives a torsor of the Jacobian of the curve $y^2 = x^n + \frac{a_{n-1}}{e^2}x^{n-1} + \cdots + \frac{a_1}{e^2}x + \frac{1}{e^2}$. But this curve is isomorphic to C_2 via the isomorphism $(x, y) \mapsto (1/x, ey/x^{\frac{n+1}{2}})$. Again, F_α^2 is the image of ν in $H^1(k, J_2)$, where Δ_c is identified with $J_{2,c}[2]$.

For $i = 1, 2$, $\delta(\alpha)$ will be in the image of $J_{i,c}/2J_{i,c}$ precisely when F_α^i has a k-rational point. Also, changing only the sign of the Pfaffian but leaving the other invariants fixed does not change P_α^1 or P_α^2. This is because changing the Pfaffian is the same is replacing T by $-T$, and this does not change T^2. Therefore, the 2-cover that we get stays the same. We will ignore the sign of the Pfaffian while associating pencils with rational orbits.

5.2. **Soluble orbits.** Any element of $J_{i,c}(k)$ can be mapped to $H^1(J_{i,c}[2])$ and, through the identification with $H^1(k, \Delta_c)$, to $H^1(k, H)$. We have also identified the set of $H(k)$ orbits with invariants c with a subset of $H^1(k, \Delta_c)$, under which the 1-distinguished orbit corresponds to the trivial element of $H^1(k, \Delta_c)$.

Proposition 5.2. *The class of the 2-distinguished orbit in $H^1(k, \Delta_c)$ is in the image of $J_{i,c}$ for both i.*

Proof. Stoll in [17] explicitly computes the 2-descent map from $J_{i,c}(k)$ to $H^1(k, J_{i,c}[2])$. With this in hand, an easy computation in which $(-\gamma)$, the class of the 2-distinguished orbit, is the image of $P_1 - \infty_1 \in J_{1,c}(k)$, and also the image of $P_2 - \infty_2 \in J_{2,c}(k)$. We carry this out for the case $i = 1$, leaving the reader to verify the case of $i = 2$ for themselves.

By [5, §5.1], $H^1(k, \Delta_c) = (L^\times / L^{\times^2})_{N=1}$. Then by Stoll's computation (for an exact reference, see [5, §5.1]), we have the image of $(0, e) - \infty_1$ in $H^1(k, \Delta_c)$ being $0 - \gamma = (-\gamma)$, which is the class of the 2-distinguished orbit α_2, as required. □

Having seen that the marked points of both curves give rise to the 2-distinguished orbit, we now prove that the composite maps from $J_{i,c}(k)$ to $H^1(k, H)$ are trivial, which tells us that rational points in either Jacobian give us rational orbits.

Proposition 5.3. *Let ν be an element of $H^1(k, \Delta_c)$ which lies in one of the subgroups $J_{i,c}/2J_{i,c}$. Then ν lies in the kernel of δ.*

Proof. By Proposition 4.5, it suffices to prove that $(\ ,\ )_\nu$ and $(\ ,\ )_{-\nu\gamma}$ are both split.

By [4, Proposition 6] (see [20, Theorem 4.6] for a proof which does not use pencils of quadrics), $(\ ,\ )_\lambda$ is split for any $\lambda \in J_{1,c}(k)/2J_{1,c}(k) \subset H^1(k, \Delta_c)$. If $\nu \in J_{1,c}(k)/2J_{1,c}(k)$, we apply Proposition 5.2 to conclude that the same holds for $-\nu\gamma$. Therefore, the required spaces are split if ν lies in the subgroup $J_{1,c}(k)/2J_{1,c}(k)$.

Exactly the same argument works if ν is in the image of $J_{2,c}/2J_{2,c}$: notice that $C_{2,c}$ is isomorphic to the curve given by the Weierstrass equation $y^2 = x^n + \frac{a_{n-1}}{e^2}x^{n-1} + \cdots + \frac{a_1}{e^2}x + \frac{1}{e^2}$, and we apply the same result from [4] (or [20]) and Proposition 5.2 to finish the proof of the result. □

Definition 6. Suppose that an orbit under $H(k)$ corresponds to a $\nu \in H^1(\Delta_c)$ in the image of $J_{i,c}(k)/2J_{i,c}(k)$ for $i = 1, 2$. We then say that the orbit is i soluble. If an orbit lies in the image of both $J_{1,c}(k)$ and $J_{2,c}(k)$, we say that the orbit is $(1, 2)$ soluble.

Note that an orbit is $(1, 2)$-soluble if and only if it is both 1 soluble and 2-soluble. Further, there is a geometric description of when an orbit is i-soluble or $(1, 2)$-soluble. Indeed, as mentioned above, the orbit of α is i soluble if the corresponding Fano variety F^i_α has a k-rational point. The distinguished orbits are i-soluble for both $i = 1$ and $i = 2$.

We will not work with 2-soluble orbits, and we have defined what they are only for the sake of completion.

6. Orbits over arithmetic bases

Suppose now that k is a number field, and that $c \in \mathrm{Inv}^{\mathrm{rs}}(k)$. Define $\mathrm{Sel}_{(1,2)}(c)$ to be the intersection of $\mathrm{Sel}_2(J_{i,c})$ (for $i = 1, 2$) in $H^1(k, \Delta_c)$.

We show that all elements in $\mathrm{Sel}_2(J_{i,c}) \subset H^1(k, J_i[2])$ give rise to orbits.

Proposition 6.1. *Let $\nu \in \mathrm{Sel}_2(J_{i,c})$ for $i = 1$ or 2. Then $\delta(\nu)$ is the trivial element in $H^1(k, H)$.*

Proof. The exact same proof as in [4] works. We prove the result for $k = \mathbb{Q}$, for the same proof applies in general. We need to show that the bilinear forms $(\ ,\ )_\nu$ and $(\ ,\ )_{-\nu\gamma}$ are split. Because $\nu \in \mathrm{Sel}_2(J_{i,c})$, Proposition 5.3 tells us that $B_\nu \otimes \mathbb{Q}_p$ and $B_\nu \otimes \mathbb{R}$ are split (for all p). The same is true for $(\ ,\ )_{-\nu\gamma}$. Therefore, by the Hasse–Minkowski theorem, the two forms must be split over $\mathbb{Q}$, as required. □

We say that the $H(k)$-orbit of $\alpha \in W(k)$ is locally 1-soluble (or locally $(1,2)$-soluble) if $\alpha \in W(k_\nu)$ is soluble for every place ν of k. We henceforth work predominantly over the bases $\mathbb{Z}$ and $\mathbb{Q}$, and their completions. The main goal in this section is to prove that rational $H(\mathbb{Q})$-orbits on $W(\mathbb{Q})$ which are locally 1-soluble, and whose invariants are integral, have representatives in $W(\mathbb{Z})$.

To that end, let D_1 and D_2 be self-dual $\mathbb{Z}$-lattices inside V_1 and V_2, respectively. When we work with the rings $\mathbb{Z}_p$, we will (for sake of brevity) use the same notation D_i to denote the completions of the lattices inside $V_i \otimes \mathbb{Q}_p$. Further, we will use the notation $W(\mathbb{Z})$ (resp., $V_1(\mathbb{Z}), V_2(\mathbb{Z})$) for $D_1 \otimes D_2$ (resp., D_1, D_2). The same holds for $\mathbb{Z}_p$.

Recall that there exist bases of $V_1(\mathbb{Z})$ and $V_2(\mathbb{Z})$, with respect to which the Gram matricies are $\pm B$, with B as in equation (1).

The group H is defined over $\mathbb{Z}$ and is a reductive group scheme over $\operatorname{Spec}\mathbb{Z}[1/2]$. Given that $\alpha \in W(R)$, define $\Delta_\alpha(R) = \{g \in H(R) | g \cdot \alpha = \alpha\}$, where R stands for $\mathbb{Z}$ or $\mathbb{Z}_p$. Clearly, $\Delta_\alpha(R) \subset \Delta_\alpha(R \otimes_{\mathbb{Z}} \mathbb{Q})$.

Definition 7. Let $\pi : W \to \mathrm{Inv}$ be the map described in §2.

(1) Define $\mathrm{Inv}(\mathbb{Z}) \subset \mathrm{Inv}(\mathbb{Q})$ to be $\pi(W(\mathbb{Z}))$.
(2) Define $\mathrm{Inv}^{\mathrm{rs}}(\mathbb{Z}) \subset \mathrm{Inv}(\mathbb{Z})$ to be $\pi(W(\mathbb{Z}) \cap W^{\mathrm{rs}}(\mathbb{Q}))$.
(3) Define $\mathrm{Inv}(\mathbb{Z}_p) \subset \mathrm{Inv}(\mathbb{Q}_p)$ to be $\pi(W(\mathbb{Z}_p))$.
(4) Define $\mathrm{Inv}^{\mathrm{rs}}(\mathbb{Z}_p) \subset \mathrm{Inv}(\mathbb{Z}_p)$ to be $\pi(W(\mathbb{Z}_p) \cap W^{\mathrm{rs}}(\mathbb{Q}_p))$.

Notice that there is a reduction map from $\mathrm{Inv}(\mathbb{Z})$ to $\mathrm{Inv}(\mathbb{F}_p)$ for $p > 2$. An element of $\mathrm{Inv}^{\mathrm{rs}}(\mathbb{Z})$ maps to an element of $\mathrm{Inv}^{\mathrm{rs}}(\mathbb{F}_p)$ exactly when p does not divide the discriminant of $g(x)$; i.e., p does not divide e and p does not divide the discriminant of $f(x)$.

We have already seen that Selmer group elements always give rise to $H(\mathbb{Q})$ orbits—the locally soluble ones. The main theorem of this section is the following.

Theorem 6.2. *Suppose that $c = (a_1, \ldots, a_{n-1}, e) \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{Z})$ such that $2^{4i} | a_i$ and $2^{2n} | e$. Then every $H(\mathbb{Q})$-orbit which has invariants c and is locally 1-soluble has an integral representative.*

The local versions of Theorem 6.2 are as follows.

Theorem 6.3. *Let $c = (a_1, \ldots, a_{n-1}, e) \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{Z}_p)$, where $p \neq 2$. Then every $H(\mathbb{Q}_p)$-orbit which has invariants c and is 1-soluble has an integral representative.*

Proposition 6.4. *Let $c = (a_1, \ldots, a_{n-1}, e) \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{Z}_2)$ such that $2^{4i} | a_i$ and $2^{2n} | e$. Then, every soluble $\mathbb{Q}_2$-orbit with invariants c has an integral representative.*

We spend the bulk of this section proving Theorem 6.3 and Proposition 6.4. We also describe how H-orbits behave over arithmetic fields.

6.1. **Finite fields of odd characteristic.** For this subsection, let $k = \mathbb{F}_q$, a finite field with q elements where q is odd. Lang's theorem implies that $H^1(k, H)$ is trivial. Therefore, for $c \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{F}_q)$, the number of $\mathbb{F}_q$-orbits with invariants c equals the cardinality of $H^1(k, \Delta_c)$.

Similarly, $H^1(k, J_{i,c})$ also equals 0. Therefore, the map from $J_{i,c}(k)/2J_{i,c}(k)$ to $H^1(k, J_{i,c}[2])$ is an isomorphism. Hence, every $H(k)$-orbit is soluble when k is a finite field.

6.2. **The p-adics for $p \neq 2$.** Let $k = \mathbb{Q}_p$, where $p \neq 2$. Let $c \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{Q}_p)$. We have the following well-known result about soluble orbits (for instance, see [17]).

Proposition 6.5. *Let J be the Jacobian of a hyperelliptic curve over $\mathbb{Q}_p$. The quantity $b_p = \#\dfrac{J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)}{J[2](\mathbb{Q}_p)}$ is 1, independent of J.*

We now give an ideal-theoretic description of integral orbits. We first cite a result of [5] which we will need.

Lemma 6.6 ([5, Lemma 8.1])**.** *Let I be a $\mathbb{Z}_p$-module of rank n equipped with a symmetric binear form $I \times I \to \mathbb{Z}_p$. Suppose that $I \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is split. If the discriminant of I is 1, then I is isometric to D_1, and if the discriminant is -1, then I is isometric to D_2.*

The condition that the form be split is unnecessary. However, we have added it because then the result holds even for $\mathbb{Z}_2$.

Using this result, we will give an ideal-theoretic description of $\mathbb{Z}_p$-orbits of $H(\mathbb{Z}_p)$. An element α in $D_1 \otimes D_2$ corresponds to an operator T from $D_1 \oplus D_2$ to $D_2 \oplus D_1$, just as in the case of fields. Let f and g be as above. We identify $V_1 \oplus V_2$ with M (the étale $\mathbb{Q}_p$-algebra $\mathbb{Q}_p[x]/(f(x^2))$ as defined in §4). Since T is integral, the lattice $D_1 \oplus D_2$, is realized as a $\mathbb{Z}_p[x]/(f(x^2))$ submodule of M, which we call a fractional ideal J of $\mathbb{Z}_p[x]/(f(x^2))$. We can in fact say more—that T^2 stabilizing each of the D_i forces the fractional ideal J to be of the form $J = I_1 + \beta I_2$, with I_1 and I_2 being fractional ideals of the ring $\mathbb{Z}_p[x]/(f(x))$. Here, we identify I_i with D_i. Since T maps D_1 to D_2, we have $I_1 \subset I_2$. Similarly, we must have $\gamma I_2 \subset I_1$.

The bilinear form on M is of the form $(\ ,\ )_\nu$ for $\nu \in L^\times_{N=1}$. The conditions that the lattices D_i are self-dual translate to $\nu I_1^2 \subset \mathbb{Z}_p[x]/f(x)$, and $N(I_1)^2 = N(\nu)^{-1}$, $\nu\gamma I_2^2 \subset \mathbb{Z}_p[x]/f(x)$, and $N(I_2)^2 = N(-\gamma\nu)^{-1}$. In sum, we have just proved the following proposition.

Proposition 6.7. *Assume that f, e, with $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_0$, $e^2 = a_0 \neq 0$, is a polynomial with coefficients in $\mathbb{Z}_p$ with nonzero discriminant. Then the integral orbits of $H(\mathbb{Z}_p)$ on $D_1 \otimes D_2$ with invariants a_i, e correspond to equivalence classes of triples (I_1, I_2, ν). Further, $\nu \in L^\times/L^{\times 2}_{N=1}$, and the I_i are fractional ideals for the order $R = \mathbb{Z}_p[x]/(f(x))$ satisfying $I_1 \subset I_2 \subset \gamma^{-1}I_1$. The element ν has the properties that the bilinear forms $(\ ,\ )_\nu$, $(\ ,\ )_{-\nu\gamma}$ are split forms over $\mathbb{Q}_p$, that $\nu I_1^2 \subset \mathbb{Z}_p[x]/f(x)$, $\nu\gamma I_2^2 \subset \mathbb{Z}_p[x]/f(x)$, and that $N(I_1)^2 = N(\nu)^{-1}$, $N(I_2)^2 = N(-\gamma\nu)^{-1}$. The triple (I_1, I_2, ν) is equivalent to (I_1', I_2', ν') if $I_i = \lambda I_i'$ and $\nu' = \lambda^2\nu$ for some $\lambda \in L^\times$. The integral orbit corresponding to the triple (I_1, I_2, ν) maps to the rational orbit of $H(\mathbb{Q}_p)$ on $W(\mathbb{Q}_p)$ corresponding to the class of ν in $(L^\times/L^{\times 2})_{N=1}$.*

The condition that the forms $(\ ,\ )_\nu$ and $(\ ,\ )_{-\gamma\nu}$ are split is unnecessary. However, we have added it because it makes the result hold even for $\mathbb{Z}_2$.

In case $R = \mathbb{Z}_p[x]/(f(x))$ happens to be of maximal order, we see that the integral orbits are in bijection with $(R^\times/R^{\times 2})_{N\equiv 1}$. This is always true when p does not divide $\mathrm{Disc}(f(x))$. In this case, the 1-soluble $H(\mathbb{Q}_p)$ orbits have a particularly nice form.

Proposition 6.8. *If p does not divide the discriminant of $f(x)$, then the integral orbits with invariants c are in bijection with 1-soluble orbits.*

Proof. The argument immediately preceding [5, Corollary 8.4] applies verbatim. □

If c modulo p is actually regular semisimple, then both the J_i have good reduction. In this case, we have the following strengthening of Proposition 6.8.

Proposition 6.9. *If c modulo p is regular semisimple, then the image of $J_1(\mathbb{Q}_p)$ in $H^1(k, \Delta_c)$ is the same as the image of $J_2(\mathbb{Q}_p)$ (i.e., the 1-soluble orbits are the same as the $(1,2)$-soluble orbits). Further, the integral orbits with invariants c are in bijection with 1-soluble orbits (and $(1,2)$-soluble orbits).*

We omit the proof, as it mimics that of Proposition 6.8. We now turn to the proof of Theorem 6.3.

Proof of Theorem 6.3. Suppose that $\nu \in (L^\times/L^{\times 2})_{N=1}$ corresponds to a 1-soluble $H(\mathbb{Q}_p)$-orbit. As both ν and $-\nu\gamma$ are 1-soluble, by [5, Proposition 8.5], there exist ideals I_1 and I_2 which satisfy all of the properties of the previous proposition, except perhaps for the conditions $I_1 \subset I_2 \subset \gamma^{-1}I_1$. We will work with I_1 and deduce the existence of I_2 from it, where I_2 satisfies the inclusion conditions.

A fractional ideal of R corresponds to a full-rank $\mathbb{Z}_p$ module contained in L, which is stable by multiplication by γ. Clearly, any lattice Λ with $I_1 \subset \Lambda \subset \gamma^{-1}I_1$ is stable under multiplication by γ and hence must be a fractional ideal. Therefore, we just need to find a Λ satisfying the above inclusion relations, and one which is self-dual for the bilinear form $(\ ,\ )_{\nu\gamma}$.

Note that by choice I_1 is self-dual for the bilinear form $(\ ,\ )_\nu$; therefore, I_1 and $\gamma^{-1}I_1$ are dual to each other for the form $(\ ,\ )_{\nu\gamma}$. By a result of Cassels [8, Lemma 3.4], there exists a $\mathbb{Z}_p$ basis (f_i) of I_1 such that the Gram matrix for $(\ ,\ )_{\nu\gamma}$ is

$$\begin{pmatrix} u_1 p^{b_1} & & & \\ & u_2 p^{b_2} & & \\ & & \ddots & \\ & & & u_n p^{b_n} \end{pmatrix},$$

where the u_i are units in $\mathbb{Z}_p$.

By replacing f_i by $p^{-[b_i/2]} f_i$, we may assume that the b_i are all 1 or 0. It is clear that the lattice Λ spanned by f_i is still sandwiched between I_1 and $\gamma^{-1}I_1$. Suppose that $\Lambda = \Lambda_0 \oplus \Lambda_1$, where Λ_j is the $\mathbb{Z}_p$-span of those f_i with $b_i = j$ $(j = 0, 1)$. Since the discriminant of B_2 is 1 modulo squares (and therefore has to have even p-adic valuation), the dimension of Λ_1 is forced to be even (hence, the dimension of Λ_0 is odd). Let the dimension of Λ_1 be $2a$. Without any loss of generality, assume that Λ_1 is spanned by $f_1, \ldots, f_{2a}$.

In particular, Λ_0 is a quadratic space of odd dimension, with the form being nondegenerate modulo p. Therefore, $\Lambda_0 \otimes \mathbb{Q}_p$ is a split quadratic space. Suppose that $\Lambda_1 \otimes \mathbb{Q}_p$ were also a split space. Then, by choosing a different basis $f_1' \cdots f_{2a}'$ of Λ_1, we may assume that the Gram matrix of $\frac{1}{p}B_2$ restricted to Λ_1 is B.

By replacing Λ_1 by the span of $f_1'/p, \ldots, f_a'/p, f_{a+1}', \ldots, f_{2a}'$, we see that $\Lambda = \Lambda_0 \oplus \Lambda_1$ is now self-dual for B_2, and that $I_1 \subset \Lambda \subset \gamma^{-1} I_1$.

Therefore, it remains for us to show that Λ_1 is split, i.e., the Hasse invariant and the discriminant are both 1. As $(\Lambda_0 \oplus \Lambda_1) \otimes \mathbb{Q}_p$ with B_2 is also split, this means that the Hasse invariant B_2 is 1. Computing the Hasse invariant using the Gram matrix of B_2 in the basis f_i, it is clear that it equals the Hasse invariant of B_2 restricted to Λ_1, which therefore has to have Hasse invariant 1. In terms of the u_i and m, the Hasse invariant equals $(-1)^{\epsilon(p)m} \prod_{i=1}^{2a} \left(\frac{u_i}{p}\right)$, where $\epsilon(p) = (p-1)/2$. The discriminant of Λ_1 equals $(-1)^m \prod_{i=1}^{2a} u_i$ modulo squares. By definition, u_i modulo squares in $\mathbb{Z}_p^\times$ equals $\left(\dfrac{u_i}{p}\right)$ (this is after identifying $\mathbb{Z}_p^\times$ modulo squares with the group $\{\pm 1\}$). Further, modulo squares $(-1)^m = (-1)^{\epsilon(p)m}$: they both equal $(-1)^m$ if p is not 1 modulo 4, and both equal 1 if p is 1 modulo 4. Therefore, the Hasse invariant being 1 forces the discriminant of Λ_1 to be 1, thereby proving the theorem. □

In fact, we have just proved the following corollary.

Corollary 6.10. *Let V be a split quadratic space over $\mathbb{Q}_p$ with an odd dimension. Let $\Lambda \subset V$ denote a $\mathbb{Z}_p$ lattice such that $\Lambda \subset \Lambda^*$, where Λ^* denotes its dual with respect to the quadratic form. Then there exists a self-dual lattice Λ' such that $\Lambda \subset \Lambda' \subset \Lambda^*$.*

6.3. **The 2-adics.** Let $k = \mathbb{Q}_2$. We state the 2-adic analogue of Proposition 6.5 (again, see [17]).

Proposition 6.11. *Let J be the Jacobian of a genus g hyperelliptic curve. Then the quantity $2^g = b_2 = \#\dfrac{J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)}{J[2](\mathbb{Q}_2)}$ depends only on g, not on J.*

We now prove Proposition 6.4. As in the proof of Theorem 6.3, we will use the existence of the ideal I_1 as proved in [5] (the argument just preceding Proposition 8.8), and we will deduce the existence of I_2. We need the divisibility condition because Bhargava and Gross need them to deduce the existence of I_1 (we would not need these conditions to deduce the existence of I_2 if we were guaranteed the existence of I_1).

Proof of Proposition 6.4. Suppose that $\alpha \in (L^\times/L^{\times 2})_{N=1}$ corresponds to a 1-soluble $\mathbb{Q}_2$ orbit. The first part of the proof proceeds along exactly the same lines. We still have I_1 is self-dual for the bilinear form $B_1 = (\ ,\ )_\alpha$, and therefore I_1 and $\gamma^{-1} I_1$ are dual to each other for the form $B_2 = (\ ,\ )_{\gamma\alpha}$. We apply the corresponding result of Cassels [8, Lemma 4.1] to $\mathbb{Z}_2$ to find a suitable basis (f_i) to express the Gram matrix $B_2(f_i, f_j)$ of B_2 in a suitable form. Cassels's result is in terms of the quadratic form associated with B_2; translating this in terms of the bilinear form B_2, we have

$$B_2(f_i, f_j) = \begin{pmatrix} 2^{b_1} Q_1' & & & \\ & 2^{b_2} Q_2' & & \\ & & \ddots & \\ & & & 2^{b_n} Q_{k'}' \end{pmatrix},$$

where each $b_i \geq 0$ and Q_i' is either a 1×1 block consisting of $u_i \in \mathbb{Z}_2^\times$ or

$$Q_i' = H = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$$

or

$$Q_i' = H_0 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

By construction, we know that the bilinear forms B_1 and B_2 are split. Therefore, by Proposition 6.7, it suffices to find a lattice containing the $\mathbb{Z}_2$-span of the f_i which is self-dual for B_2. By multiplying the basis vectors f_i by appropriate negative powers of 2 we may assume that all of the b_i are either 0 or 1. In fact, we may assume that $b_i = 0$ if $Q' = H$ or H_0. Indeed, if a two-dimensional vector space with basis e_1, e_2 has a bilinear form with Gram matrix $2H$ or $2H_0$, by replacing e_1 with $e_1/2$ (and leaving e_2 unchanged), we are left with a lattice that is self-dual. In the first case, the Gram matrix with respect to the new basis would be H. In the second case, the Gram matrix with respect to the new basis will be

$$\begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix}.$$

The Gram matrix now has the form

$$\begin{pmatrix} 2U_1 & & & \\ & Q_2 & & \\ & & \ddots & \\ & & & Q_k \end{pmatrix},$$

where U_1 is a diagonal matrix of size $2a \times 2a$ consisting solely of units, and where the Q_i are either 1×1 or 2×2 matrices with a unit determinant. The claim on the parity of the size of U_1 holds because the discriminant of B_2 in $\mathbb{Q}_2^\times$ is -1 modulo squares and hence has even 2-adic valuation. The proposition follows from Lemma 6.12. □

Lemma 6.12. *Let $\Lambda = \mathbb{Z}_2 f_1 \oplus \mathbb{Z}_2 f_2$ be equipped with a bilinear form whose Gram matrix in the basis (f_1, f_2) is*

$$\begin{pmatrix} 2u_1 & 0 \\ 0 & 2u_2 \end{pmatrix},$$

where u_1 and u_2 are units in $\mathbb{Z}_2$. Then there exists a lattice $\Lambda' \supset \Lambda$ which is self-dual for B.

Proof. The lattice Λ' spanned by $(f_1 + f_2)/2$ and $(f_1 - f_2)/2$ has the required properties. □

6.4. **Archimedean fields.**

6.4.1. *The complex numbers.* In the case $k = \mathbb{C}$, we work over an algebraically closed field, so for every $c \in \mathrm{Inv}^{\mathrm{rs}}$, there is precisely one $H(\mathbb{C})$ orbit with invariants c.

6.4.2. *The real numbers.* We have the archimedean version of Propositions 6.5 and 6.11 (again, see [17]).

Proposition 6.13. *Let J be the Jacobian of a genus g hyperelliptic curve. Then the quantity $2^{-g} = b_\infty = \#\dfrac{J(\mathbb{R})/2J(\mathbb{R})}{J[2](\mathbb{R})}$ depends only on g, not on J.*

Let $c \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{R})$, and let f_c denote the corresponding polynomial. Define $\mathrm{Inv}^{\mathrm{rs}}(\mathbb{R})^{(a,b)}$ to be the set of $c \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{R})$ such that f_c has a pairs of complex conjugate roots, b positive real roots, and $n - 2a + b$ negative real roots. The stabilizer Δ_c (as a group scheme over $\mathbb{R}$) depends only on the (a, b) such that $c \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{R})^{(a,b)}$. We call this $\Delta^{(a,b)}$. Let $\eta^{(a,b)}$ denote the size of this group.

Further, computing with the descent map for the Jacobians J_1 and J_2 shows that the number of 1-soluble orbits with invariants c depends only on (a, b). The same holds for $(1, 2)$-soluble orbits.

6.5. **Orbits over $\mathbb{Q}$ and $\mathbb{Z}$.** For the Jacobian J of a hyperelliptic curve over $\mathbb{Q}$, the local constants b_ν clearly multiply to yield 1. We conclude this section by demonstrating the existence of $\mathbb{Z}$-representatives of locally soluble $\mathbb{Q}$-orbits.

Proof of Theorem 6.2. The split groups SO_n have class number 1. Therefore, $H = \mathrm{SO}(V_1) \times \mathrm{SO}(V_2)$ also has class number 1. The same proof as in [6] applies. □

7. Counting integral orbits

In this section, we use Bhargava's averaging technique to count the number of $H(\mathbb{Z})$-orbits on $W(\mathbb{Z})$ of height bounded by X, as in [6]. Toward that end, we first define a height function on $W(\mathbb{R})$. Recall that Inv is the categorical quotient of W by H; i.e., functions on Inv are H-invariant functions on W. The scheme Inv is defined over $\mathbb{Z}$ and equals $\mathrm{Spec}(\mathbb{Z}[a_1, \ldots, a_{n-1}, e])$. A point $c = (a_1, \ldots, a_{n-1}, e)$ corresponds to the polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + e^2$. We define a height function on $\mathrm{Inv}(\mathbb{R})$ as follows:

$$\mathrm{ht}(c) = \mathrm{ht}(f) = \max\{|a_i|^{1/2i}, |e|^{1/n}\}.$$

The canonical map $\pi : W \to \mathrm{Inv}$ is given by sending the operator T to the nonconstant coefficients of its characteristic polynomial, and to the Pfaffian. The height function $\mathrm{ht} : W(\mathbb{R}) \to \mathbb{R}$ (we use the same symbol as for the height function on $\mathrm{Inv}(\mathbb{R})$) is defined to be the composition of π and $\mathrm{ht} : \mathrm{Inv}(\mathbb{R}) \to \mathbb{R}$.

Notice that ht is homogeneous of degree 1 on W, i.e., $\mathrm{ht}(\lambda T) = \lambda\,\mathrm{ht}(T)$, for $\lambda \in \mathbb{R}$ positive, $T \in W(\mathbb{R})$.

7.1. **Fundamental domains.** Let $W(\mathbb{R})_{\mathrm{sol}}$ denote the subset of $W^{\mathrm{rs}}(\mathbb{R})$ consisting of elements which the property sol, where sol stands for either 1-soluble or $(1, 2)$-soluble. Depending on whether we want to count 1-soluble orbits or $(1, 2)$-soluble orbits, we will choose sol to be 1-soluble or $(1, 2)$-soluble, respectively.

We partition $W(\mathbb{R})_{\mathrm{sol}}$ into sets indexed by (a, b) with $2a + b \leq n$ as in §6.4:

$$W(\mathbb{R})_{\mathrm{sol}} = \bigcup_{(a,b)} W(\mathbb{R})^{(a,b)}_{\mathrm{sol}}.$$

Here, $W(\mathbb{R})^{(a,b)}_{\mathrm{sol}}$ consists of $T \in W(R)_{\mathrm{sol}}$ such that $\pi(T) \in \mathrm{Inv}(\mathbb{R})^{(a,b)}$.

Similarly, let $W(\mathbb{Z})^{(a,b)} = W(\mathbb{Z}) \cap W(\mathbb{R})^{(a,b)}_{\mathrm{sol}}$ (we have suppressed the subscript "sol"). If we are working in the case where sol means 1-soluble, then we will

acknowledge this with the notation $W(\mathbb{Z})_1^{(a,b)}$. Similarly, if sol stands for $(1,2)$-soluble, we will use the notation $W(\mathbb{Z})_{(1,2)}^{(a,b)}$.

7.1.1. *Fundamental sets for the action of $H(\mathbb{R})$ on $W(\mathbb{R})_{\mathrm{sol}}$.* We use a Kostant section (recall that there are two distinguished orbits, and therefore two different Kostant sections) $\kappa : \mathrm{Inv}(\mathbb{R}) \to W(\mathbb{R})$ to define a fundamental set for the action of $H(\mathbb{R})$ on $W(\mathbb{R})_{\mathrm{sol}}^{(a,b)}$. Let $\mathrm{Inv}^{\mathrm{rs}}(\mathbb{R})^{(a,b)}$ denote the intersection of $\pi(W(\mathbb{R})^{(a,b)})$ and $\mathrm{Inv}^{\mathrm{rs}}(\mathbb{R})$. The number of $H(\mathbb{R})$ orbits having the property sol depends only on (a,b). Denote this number by $\tau_{\mathrm{sol}}^{(a,b)}$. Just as in [5, §9.1], there exist elements $h_1, \ldots, h_{\tau_{\mathrm{sol}}^{(a,b)}} \in \mathrm{GL}(V_1 \oplus V_2)$ such that $\mathcal{D}_{\mathrm{sol}}^{\prime(a,b)} = \bigcup_i h_i \kappa(\mathrm{Inv}(\mathbb{R})^{(a,b)}) h_i^{-1}$ is a fundamental set for the action of $H(\mathbb{R})$ on $W(\mathbb{R})^{(a,b)}$. We work with the fundamental set $\mathcal{D}_{\mathrm{sol}}^{(a,b)}$ where

$$\mathcal{D}_{\mathrm{sol}}^{(a,b)} = \mathbb{R}_{>0}\{T \in \mathcal{D}_{\mathrm{sol}}^{\prime(a,b)} : \mathrm{ht}(T) = 1\}.$$

Notice that the size of the entries of any $T \in \mathcal{D}_{\mathrm{sol}}^{(a,b)}$ having height X is bounded by $O(X)$. This is because $\{T \in \mathcal{D}_{\mathrm{sol}}^{\prime(a,b)} : \mathrm{ht}(T) = 1\}$ is a bounded set. Let $\mathcal{D}_{\mathrm{sol}}^{(a,b)}(X)$ denote the subset of $\mathcal{D}_{\mathrm{sol}}^{(a,b)}$ consisting of elements having height bounded by X.

For ease of notation, we will suppress the subscript sol while referring to $\mathcal{D}_{\mathrm{sol}}^{(a,b)}(X)$. For the better part of what follows, the results stay the same whether sol stands for 1-soluble or $(1,2)$-soluble. We will revert to using the subscript only when it matters what sol stands for. We will then refer to $\mathcal{D}_{\mathrm{sol}}^{(a,b)}(X)$ as $\mathcal{D}_1^{(a,b)}(X)$ if we are working with 1-soluble orbits, and to $\mathcal{D}_{\mathrm{sol}}^{(a,b)}(X)$ as $\mathcal{D}_{1,2}^{(a,b)}(X)$ if we are working with $(1,2)$-soluble orbits.

7.1.2. *A fundamental domain for the action of $(H\mathbb{Z})$ on $H(\mathbb{R})$.* We describe a fundamental domain $\mathcal{F}$ for the left action of $H(\mathbb{Z})$ on $H(\mathbb{R})$ as constructed by Borel in [7].

The set $\mathcal{F}$ may be expressed in the form $\mathcal{F}_1 \times \mathcal{F}_2$, where $\mathcal{F}_i$ is the fundamental domain for the action of $\mathrm{SO}(V_i)(\mathbb{Z})$ on $\mathrm{SO}(V_i)(\mathbb{R})$, $i \in \{1,2\}$. $\mathcal{F}_1$ may be expressed as

$$\mathcal{F}_1 = \{ur'\theta : u \in N_1'(r'),\ r' \in R',\ \theta \in K_1\},$$

where $N_1'(r')$ is an absolutely bounded measurable set—which depends on $r' \in R$—of unipotent lower triangular matricies; R' is the subset of the torus of diagonal matrices with positive entries

$$\begin{bmatrix} r_1'^{-1} & & & & & & \\ & \ddots & & & & & \\ & & r_m'^{-1} & & & & \\ & & & 1 & & & \\ & & & & r_m' & & \\ & & & & & \ddots & \\ & & & & & & r_1' \end{bmatrix}$$

constrained by the relations $r_1'/r_2' > c, \ldots, r_{m-1}'/r_m' > c$, $r_m' > c$, and K_1 is a maximal compact of $\mathrm{SO}(V_1)(\mathbb{R})$. We will parameterize R' differently. Indeed, for $i = 1, \ldots, m$, we define $r_i = r_i'/r_{i+1}'$ (where we set $r_{m+1}' = 1$). Then $r = (r_1, \ldots, r_m)$ belongs to R' exactly when $r_i > c$. We define $\mathcal{F}_2$ similarly, and we denote by S the

diagonal torus, and by s_i the analogous coordinates. Let $N'(t)$ denote the product of $N_1'(r) \times N_2'(s)$, and let K denote the maximal compact subgroup of $H(\mathbb{R})$ given by the products of the K_i. We fix a Haar measure dh on $H(\mathbb{R})$ by setting

$$dh = \prod_{i=1}^{k} (r_i s_i)^{i^2-2im} \cdot du \cdot d^\times t \cdot d\theta,$$

where du is an invariant measure on N, the group of unipotent lower triangular real matrices, $d\theta$ is the unique Haar measure on K giving it unit volume, and $d^\times t = d^\times r d^\times s = \frac{dr}{r}\frac{ds}{s}$ is a Haar measure on $R \times S$. To simplify notation, we make the following definition.

Definition 8. Let $\delta(t) = \delta(r,s)$ denote the quantity $= \prod_{i=1}^{k} (r_i s_i)^{i^2-2im}$.

7.1.3. *A fundamental domain for the action of $H(\mathbb{Z})$ on $W(\mathbb{R})_{\mathrm{sol}}$.* For $h \in H(\mathbb{R})$, we regard $\mathcal{F}h \cdot \mathcal{D}^{(a,b)}(X)$ as a multiset, where the multiplicity of $T \in \mathcal{F}h \cdot \mathcal{D}^{(a,b)}(X)$ is given by $\#\{h' \in \mathcal{F} : T \in h'h \cdot \mathcal{D}^{(a,b)}(X)\}$. The $H(\mathbb{Z})$ orbit of T is counted with multiplicity $\dfrac{\#\,\Delta_T(\mathbb{R})}{\#(\Delta_T(\mathbb{R}) \cap H(\mathbb{Z}))}$. Let $\Delta_T(\mathbb{Z})$ denote the group $\Delta_T(\mathbb{R}) \cap H(\mathbb{Z})$.

The same argument as in [16, §4.2] applies to conclude that $(\Delta_T(\mathbb{R}) \cap H(\mathbb{Z}))$ is nontrivial only for a measure-0 set of $W(\mathbb{R})$. Recall that the group scheme Δ_T is constant over $T \in W^{(a,b)}$, and $\eta^{(a,b)}$ denotes the cardinality of $\Delta_T(\mathbb{R})$. Therefore, the multiset $\mathcal{F}h \cdot \mathcal{D}^{(a,b)}(X)$ is a cover of a fundamental domain for $H(\mathbb{Z})$ on $W(\mathbb{R})^{(a,b)}$ of degree $\eta^{(a,b)}$.

7.2. **Counting the number of integral orbits.**

Definition 9. An element $\alpha \in W(\mathbb{Q})$ is called irreducible if $\pi(\alpha) \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{Q})$ and if α is not distinguished.

Note that every α whose invariants are not in $\mathrm{Inv}^{\mathrm{rs}}(\mathbb{Q})$ is automatically reducible. In particular, elements with discriminant 0 are reducible. For an $H(\mathbb{Z})$-invariant set $S \subset W(\mathbb{Z})^{(a,b)}$, define $N(S,X)$ to be the number of irreducible $H(\mathbb{Z})$ orbits of S that have height bounded by X, where each orbit $H(\mathbb{Z}) \cdot T$ is weighted by $1/\#\,\Delta_T(\mathbb{Z})$.

Theorem 7.1.

$$N(W(\mathbb{Z})^{(a,b)}, X) = \frac{1}{\eta^{(a,b)}} \mathrm{Vol}(\mathcal{F} \cdot \mathcal{D}^{(a,b)}(X)) + o(X^{n^2}).$$

We will spend most of this section proving Theorem 7.1. By our construction of the fundamental domain, we have

$$N(S,X) = \frac{1}{\eta^{(a,b)}} \#\{\mathcal{F}h \cdot \mathcal{D}^{(a,b)}(X) \cap S^{\mathrm{irr}}\}$$

for any $h \in H(\mathbb{R})$. Let A_0 be a bounded open $(K_1 \times K_2)$-invariant ball in $H(\mathbb{R})$. Averaging the above equation over A_0 we have

$$N(S,X) = \frac{1}{\eta^{(a,b)} \mathrm{Vol}(A_0)} \int_{h \in A_0} \#\{\mathcal{F}h \cdot \mathcal{D}^{(a,b)}(X) \cap S^{\mathrm{irr}}\} dh. \tag{2}$$

We use equation (2) to define $N(S,X)$ even if S is not $H(\mathbb{Z})$-invariant. Using an argument entirely analogous to the proof of [6, Theorem 2.5] (Bhargava's averaging

technique), we obtain

$$N(S,X) = \frac{1}{\eta^{(a,b)}\,\mathrm{Vol}(A_0)} \int_{h\in\mathcal{F}} \#\{hA_0 \cdot \mathcal{D}^{(a,b)}(X) \cap S^{\mathrm{irr}}\}dh. \tag{3}$$

We now state a result of Davenport [9] which we will use extensively in what follows.

Proposition 7.2 (Davenport)**.** *Let A be a bounded, semialgebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m that is defined by at most k polynomial inequalities, with each having a degree of at most ℓ. Then the number of lattice points (counted with multiplicity) contained in the region A is*

$$\mathrm{Vol}(A) + O(\max\{\mathrm{Vol}(\overline{A}), 1\}),$$

where $\mathrm{Vol}(\overline{A})$ denotes the greatest d-dimensional volume of any projection of A onto a coordinate subspace obtained by equating $n-d$ coordinates to 0, 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.

Here is a sketch of how we prove Theorem 7.1. We divide $\mathcal{F}$ (the region of integration in equation (3)) into two parts: the main body and the cuspidal region. We will prove that the integral of $\#\{hA_0 \cdot \mathcal{D}^{(a,b)}(X) \cap S^{\mathrm{irr}}\}$ over the main body is $o(X^{n^2})$ (Proposition 7.12), and that the integral of $\#\{hA_0 \cdot \mathcal{D}^{(a,b)}(X) \cap S^{\mathrm{irr}}\}$ over the cuspidal region is $o(X^{n^2})$ (Proposition 7.6). The result will then follow from an application of Proposition 7.2.

7.2.1. *The number of irreducible points in the cusp is negligible.* Recall that we have fixed bases for V_1 and V_2 with respect to which the bilinear forms B_i have Gram matricies $\pm B$ (equation (1)).

We pick a set of coordinates on W as follows. An element T corresponds to

$$T = \left[\begin{array}{c|c} 0 & A \\ \hline A^* & 0 \end{array}\right],$$

where A is some $n \times n$ matrix and $A^* = (-BAB^{-1})^{\mathrm{t}}$ (where the superscript refers to taking the transpose). The matrix A^* is the unique matrix which makes T self-adjoint. To pick coordinates on W, it suffices to pick coordinates on the set of all matrices A, which we do as follows:

$$\begin{bmatrix} a_{m\,-m} & a_{m\,1-m} & \cdots & a_{m\,m} \\ a_{m-1\,-m} & a_{m-1\,1-m} & \cdots & a_{m-1\,m} \\ \vdots & & \ddots & \vdots \\ a_{-m\,-m} & a_{-m\,1-m} & \cdots & a_{-m\,m} \end{bmatrix}.$$

The a_{ij} are scaled by the action of the torus $R \times S$. Define w_{ij} as the weight according to which $R \times S$ scales a_{ij}. For instance, if i and j are positive, $w_{ij} = r_1^{-1} \cdots r_i^{-1} s_1^{-1} \cdots s_j^{-1}$, and $w_{-i\,-j} = w_{ij}^{-1}$. We define a partial order $\preceq$ on the set of variables: $a_{ij} \preceq a_{i'j'}$ if $i' \le i$ and $j' \le j$. Further, $a_{ij} \preceq a_{i'j'}$ precisely when $\frac{w_{ij}}{w_{i'j'}}$ consists of nonpositive powers of r and s. With respect to this order, a_{mm} is the unique minimal element.

We now prove some results on reducibility of elements in $W(\mathbb{Z})$, which we will need to prove Proposition 7.6.

Lemma 7.3. *If for some i the top-right $i \times (2m+2-i)$ block of A is identically 0, then the corresponding T has discriminant 0.*

Proof. If such a block is identically 0, then the determinant of A is 0. Therefore, the operator T has the eigenvalue 0 with multiplicity 2, rendering it impossible for T to be regular semisimple. □

Lemma 7.4. *If the top-right $m \times (m+1)$ or $(m+1) \times m$ block of A is 0, then T is reducible.*

Proof. We will show that in the first case, the orbit will be 1-distinguished, and in the second case, the orbit will be 2-distinguished. Indeed, it is easy to check that

$$T^2 = \left[\begin{array}{c|c} AA^* & 0 \\ \hline 0 & A^*A \end{array}\right].$$

If the top-right $m \times (m+1)$ block of A is identically 0, then an easy computation shows that the top-right $m \times m$ block of AA^* will also be 0. Consequently, the isotropic space X spanned by the last m basis vectors of V_1 has the property that $T^2X \subset X^\perp$, so the orbit is 1-distinguished. The same proof (except that we use A^*A instead) shows that in the second case, the orbit would be 2-distinguished. Therefore, T is reducible. □

Lemma 7.5. *Suppose that $i+j = 2m+1$. If the top-right $i \times j$ and $j \times i$ blocks of A are 0, then T has discriminant 0.*

Proof. Without any loss of generality, we assume that $i < j$. If A has the property that the top-right blocks of size $i \times j$ and $j \times i$ are identically 0, then so does A^*, and therefore so do AA^* and A^*A. We will show that AA^* (and, similarly, A^*A) has repeated eigenvalues. For brevity, let Y denote the matrix AA^*. It will be of the form

$$Y = \left[\begin{array}{c|c|c} Y_{11} & \mathbf{0} & \mathbf{0} \\ \hline * & Y_{22} & \mathbf{0} \\ \hline * & * & Y_{33} \end{array}\right],$$

where Y_{11} and Y_{33} are of the size $i \times i$ and Y_{22} is of the size $(j-i) \times (j-i)$. The determinant of Y equals the product of the determinants of Y_{11}, Y_{22}, and Y_{33}. Note that the determinant of Y_{11} equals the determinant of Y_{33}. This is so because Y is self-adjoint for the bilinear form on V_1. The same conclusions hold with the characteristic polynomial replacing the determinant because the same argument applies to $Y - xI$. Let P_M denote the characteristic polynomial of any square matrix M. We have shown that $P_Y = P_{Y_{22}} P_{Y_{11}}^2$, so $AA^* = Y$ must have repeated eigenvalues, as claimed. Therefore, T has discriminant 0 and is reducible. □

Define the cusp, or cuspidal region, to be the set of all elements of $W(\mathbb{R})$ such that $|a_{mm}| < 1$, and define the main body to be the complement of the cuspidal region. We say that $h \in \mathcal{F}$ is cuspidal if $hA_0\mathcal{D}^{(a,b)}(X)$ lies fully in the cusp. Clearly, an integral element will lie in the cusp only if $a_{mm} = 0$. We have the following proposition.

Proposition 7.6.

$$\int_{h \in \mathcal{F}} \#\{hA_0\mathcal{D}^{(a,b)}(X) \cap W(\mathbb{Z})^{\mathrm{irr}}_{a_{mm}=0}\} dh = o(X^{n^2}).$$

Proof. To lighten the notation, we drop the superscript "(a,b)" while proving this result. The strategy is to use Proposition 7.2 to replace the number of integral points with a volume. The same argument as in [16, Proposition 21] shows that it suffices to prove[2]

$$\int_{t\in R\times S} \#\{tA_0\mathcal{D}(X)\cap W(\mathbb{Z})^{\mathrm{irr}}_{a_{mm}=0}\}\delta(t)d^\times t = o(X^{n^2}).$$

If $t=(r,s)\in R\times S$ has the property that $tA_0\mathcal{D}(X)\subset W(\mathbb{R})_{|a_{ij}|<1}$, then $tA_0\mathcal{D}(X)\subset W(\mathbb{R})_{|a_{i'j'}|<0}$ for all $a_{i'j'}\preceq a_{ij}$. This is true because $\frac{w_{i'j'}}{w_{ij}}$ consists of nonpositive powers of r and s, so t would act with a higher negative weight on $a_{i'j'}$.

Let U denote a subset of the coordinates a_{ij}, with the property that if $a_{i_0j_0}\in U$, then U also contains a_{ij} with $a_{ij}\preceq a_{i_0j_0}$; i.e., U contains all variables a_{ij} to the top right of $a_{i_0j_0}$. Define $W(U)$ to be the subspace of W given by $a_{ij}=0$, $a_{ij}\in U$. Define $W(U)(\mathbb{Z})^{\mathrm{irr}}_0$ to be $\alpha\in W(U)(\mathbb{Z})^{\mathrm{irr}}$ such that $a_{ij}\neq 0$ for $a_{ij}\notin U$. It suffices to prove that

$$\int_{t\in R\times S} \#\{tA_0\mathcal{D}(X)\cap W(U)(\mathbb{Z})^{\mathrm{irr}}_0\}\delta(t)d^\times t = o(X^{n^2}).$$

By Lemmas 7.3 and 7.4, if U contains a_{ij} with $i+j\le 0$ or with $\{i,j\}=\{0,1\}$, then every element of $W(U)(\mathbb{Z})$ is reducible. Similarly, by Lemma 7.5, if U contains a_{ij} and a_{ji} for some pair (i,j) such that $i+j=1$, then every element of $W(U)(\mathbb{Z})$ is reducible. We may assume that U does not contain any such a_{ij}. We now prove two results which we will need to finish this proof.

Claim 7.7. For any $w_{ij}\notin U$, we may assume that $Xw_{ij}(t)\ge 1$.

Proof. If $Xw_{ij}(t)<1$, then $a_{ij}(\alpha)=0$ for $\alpha\in W(U)(\mathbb{Z})$, so $\alpha\notin W(U)(\mathbb{Z})_0$. □

It is an easy consequence of Claim 7.7 that $Xs_m^{-1}>1$ and $Xr_m^{-1}>1$, and for all k, $X^2s_k^{-1}>1$ and $X^2r_k^{-1}>1$.

Claim 7.8. We have

$$\#\{tA_0\mathcal{D}(X)\cap W(U)(\mathbb{Z})^{\mathrm{irr}}_0\} = O\Big(\prod_{a_{ij}\in U} w_{ij}^{-1}(t)X^{n^2-|U|}\Big).$$

Proof. By Proposition 7.2,

$$\#\{tA_0\mathcal{D}(X)\cap W(U)(\mathbb{Z})^{\mathrm{irr}}_0\} = O(\mathrm{Vol})+E,$$

where Vol is the volume of the projection of $tA_0\mathcal{D}(X)$ onto $W(U)$, and E is an error term mentioned in Proposition 7.2. If the projection of $tA_0\mathcal{D}(X)$ onto some line spanned by a_{ij} for some $a_{ij}\notin U$ has a volume less than 1, then $tA_0\mathcal{D}(X)\cap W(U)(\mathbb{Z})^{\mathrm{irr}}_0=\emptyset$. Therefore, the volume of the projection of $tA_0\mathcal{D}(X)$ onto any coordinate subspace of $W(U)$ is bounded by Vol. We therefore have the bound

$$\#\{tA_0\mathcal{D}(X)\cap W(U)(\mathbb{Z})^{\mathrm{irr}}_0\} = O(\mathrm{Vol}).$$

The claim follows from the fact that $\mathrm{Vol}=O\Big(\prod_{a_{ij}\in U} w_{ij}^{-1}(t)X^{n^2-|U|}\Big)$. □

[2] $\delta(t)$ was defined in Definition 8.

By Claim 7.8, we have

$$\int_{t\in R\times S} \#\{tA_0\mathcal{D}(X)\cap W(U)(\mathbb{Z})_0^{\mathrm{irr}}\}\delta(t)d^\times t$$
$$= O\Big(X^{n^2-|U|}\int_{t\in R\times S}\prod_{a_{ij}\in U} w_{ij}^{-1}\prod(r_is_i)^{i^2-2im}d^\times t\Big).$$

It remains to prove that $\int_{t\in R\times S}\prod_{a_{ij}\in U} w_{ij}^{-1}\prod(r_is_i)^{i^2-2im}d^\times t = o\big(X^{|U|}\big)$. Suppose, first, that U is contained in the top-right $m\times m$ block. We then have $\prod_{i,j>0} w_{ij}^{-1} = \prod(r_is_i)^{im}$. If U is strictly contained in the top-right $m\times m$ block, all of the exponents in the r_i and s_i (in the integrand) are strictly negative, so the integral is bounded by $O(1)$. If U equals the top-right $m\times m$ block, the exponents of r_m and s_m are 0, and the other exponents are strictly negative. By Claim 7.7, $Xw_{10}\geq 1$ and $Xw_{01}\geq 1$. We make the exponents of r_m and s_m negative as well, by multiplying the entire expression by $X^2w_{10}w_{01}$, thus bounding the integral by $o(X^2)$.

Let us therefore assume that U is not contained in the top-right $m\times m$ block. It follows that U either contains a variable of the form a_{mj} with $j\leq 0$, or a_{im} with $i\leq 0$. We will induct on m to prove the proposition. We deal with the problem in two cases. Case 1 will be when U contains variables of both forms, i.e., a_{mj} and a_{im} with $i,j\leq 0$; and Case 2 will be when U contains variables of only one of the two kinds. The proof of the first case is strictly harder than the second case, so we will be content with simply proving the first case.

Case 1. Let the topmost row U_R of U have size $1\times(m+b_s)$, and the rightmost column U_C have size $(m+b_r)\times 1$, with $b_s\geq b_r$. As mentioned above, using Lemma 7.5, we assume that $b_r<m$. In order to apply induction, we have to show that

$$\delta_m(r,s)\delta_{m-1}(r,s)^{-1}\prod_{w\in U_R\cup U_C} w^{-1}(r,s) = o(X^{2m+b_s+b_r-1}).$$

For ease of notation, let $a=b_s-b_r$, $k_s=m-b_s$, and $k_r=m-b_r$. The left-hand side of the above equation is going to be a product of a term s_u consisting of the parameters s_k and a term r_u consisting of the parameters r_k.

A calculation shows that

$$s_u = s_m^{1-a}\cdots s_{k_s+1}^{1-a}s_{k_s}^{-a}\cdots s_1^{k_s-1+1}$$

and

$$r_u = r_m^{1+a}\cdots r_{k_s+a+1}^{1+a}r_{k_s+a}^{a}\cdots r_{k_s+1}r_{k_s}^{0}\cdots r_1^{-k_s+1}.$$

Recall that $Xw>1$ for any $w\notin U$. Let $w_0=(r_1\cdots r_m)^{-1}(s_{k_s+1}\cdots s_m)$ be the weight of the variable a_{m-b_s}. We have $w_0^a s_u r_u$ being equal to $s_m s_{m-1}\cdots s_{k_s+1}r_m\cdots r_{k_s+a+1}$ multiplied by nonpositive powers of s_k and r_k. Recall that we have $X^2s_k^{-1}>1$ and $X^2r_k>1$. Further, $Xr_m^{-1}>1$ and $Xs_m^{-1}>1$.

Multiplying s_ur_u by $X^{a+2b_s+2(b_s-a)-2}w_0^a(s_m\cdots s_{k_s+2})^{-1}(r_m\cdots r_{k_s+a+1})^{-1}$ gives us a product of nonpositive powers of r_k and s_k. Further, it is easy to see that the exponent of X is at most $2m+b_s+b_r-2$. Finally, we again use the fact that $X^4r_k^{-1}s_k^{-1}<1$ to multiply by a small power of X to make the exponents of r_k and s_k negative. This concludes the first case.

As we mentioned above, the proof of the second case is simpler and runs along the same lines. We have thus proved Proposition 7.6. □

7.2.2. *Proof of Theorem* 7.1. We largely follow the exposition in [16, Theorem 24]. Let $\mathcal{F}' \subset \mathcal{F}$ be the set of cuspidal elements of $\mathcal{F}$. By Proposition 7.6, we have

$$\begin{aligned} &N(W(\mathbb{Z})^{(a,b)}, X) \\ &= \frac{1}{\eta^{(a,b)} \operatorname{Vol}(A_0)} \int_{h\in\mathcal{F}} \#\{hA_0\mathcal{D}^{(a,b)}(X) \cap W(\mathbb{Z})^{\mathrm{irr}}\} dh \\ &= \frac{1}{\eta^{(a,b)} \operatorname{Vol}(A_0)} \int_{h\in\mathcal{F}\setminus\mathcal{F}'} \#\{hA_0\mathcal{D}^{(a,b)}(X) \cap W(\mathbb{Z})^{\mathrm{irr}}\} dh \ + o(X^{n^2}). \end{aligned}$$

By Proposition 7.12, we may replace W^{irr} with W. We use Proposition 7.2 to approximate $\#\{hA_0\mathcal{D}^{(a,b)}(X) \cap W(\mathbb{Z})\}$.

By construction of $\mathcal{F}'$, the length of the projection of $hA_o\mathcal{D}(X)$ onto the coordinate a_{mm} for all h in $\mathcal{F}\setminus\mathcal{F}'$ is at least 1. Further, the weight of a_{mm} being minimal, the volume of all smaller dimensional projections of $hA_o\mathcal{D}(X)$ are bounded by the volume of the projection onto the hyperplane $a_{mm} = 0$. Therefore, $N(W(\mathbb{Z})^{(a,b)}, X)$ equals

$$\frac{1}{\eta^{(a,b)} \operatorname{Vol}(A_0)} \int_{h\in\mathcal{F}\setminus\mathcal{F}'} \left[\operatorname{Vol}(hA_0\mathcal{D}^{(a,b)}(X)) + O\left(\frac{\operatorname{Vol}(hA_0\mathcal{D}^{(a,b)}(X))}{Xw_{mm}} \right) \right] dh + o(X^{n^2}).$$

We see that $\int_{h\in\mathcal{F}\setminus\mathcal{F}'} \frac{1}{w_{mm}} dh$ is bounded by $O(1)$. Further, by the same argument used in [16], the volume of the cuspidal region $\mathcal{F}'$ is also bounded by $o(1)$. Therefore, we have

$$\begin{aligned} N(W(\mathbb{Z})^{(a,b)}, X) &= \frac{1}{\eta^{(a,b)} \operatorname{Vol}(A_0)} \int_{h\in\mathcal{F}} \operatorname{Vol}(hA_0\mathcal{D}^{(a,b)}(X)) dh + o(X^{n^2}) \\ &= \frac{1}{\eta^{(a,b)} \operatorname{Vol}(A_0)} \int_{h\in A_o} \operatorname{Vol}(\mathcal{F}h\mathcal{D}^{(a,b)}(X)) dh + o(X^{n^2}). \end{aligned}$$

The set $\mathcal{F}h\mathcal{D}^{(a,b)}(X)$ does not depend on h, so the integrand equals $\operatorname{Vol}(\mathcal{F}\mathcal{D}^{(a,b)}(X))$. Substituting this in the final equality, we see that

$$N(W(\mathbb{Z})^{(a,b)}, X) = \frac{1}{\eta^{(a,b)}} \operatorname{Vol}(\mathcal{F}\mathcal{D}^{(a,b)}(X)) + o(X^{n^2}),$$

as required.

7.3. **Congruence conditions.** Let $\mathcal{L} \subset W(\mathbb{Z})$ be a subset defined by congruence conditions modulo finitely many prime powers. We want to count irreducible $H(\mathbb{Z})$-orbits in $\mathcal{L}$, and the main result in this subsection is as follows.

Theorem 7.9. *We have*

$$N(\mathcal{L}^{(a,b)}, X) = N(W(\mathbb{Z})^{(a.b)}, X) \prod_p \mu_p(\mathcal{L}) + o(X^{n^2}),$$

where $\mathcal{L}^{(a,b)} = \mathcal{L} \cap W(\mathbb{Z})^{(a,b)}$*, and* μ_p *is the p-adic density of* $\mathcal{L}$ *in* $W(\mathbb{Z})$*.*

The structure of our proof shall be thus: we will first prove Lemma 7.10, and using it, we will prove Proposition 7.12. We will see that Theorem 7.9 follows immediately. We remark that the proofs of Lemma 7.10 and Proposition 7.12 are independent of Theorem 7.1.

Lemma 7.10. *Notation is as above. We then have*

$$\int_{h\in\mathcal{F}\backslash\mathcal{F}'} \#\{hA_0\mathcal{D}^{(a,b)}(X)\cap\mathcal{L}\}dh$$
$$= \prod_p \mu_p(\mathcal{L}) \int_{h\in\mathcal{F}\backslash\mathcal{F}'} \#\{hA_0\mathcal{D}^{(a,b)}(X)\cap W(\mathbb{Z})\}dh + o(X^{n^2}).$$

Proof. We follow the proof of [5, Theorem 10.11]. Suppose that $\mathcal{L}$ is defined by congruences modulo some integer m. Then $\mathcal{L}$ may be viewed as a disjoint union of translates $\mathcal{L}_1\cdots\mathcal{L}_k$ of the lattice $mW(\mathbb{Z})$. To estimate $\#\{hA_0\mathcal{D}^{(a,b)}(X)\cap\mathcal{L}\}$, we again use Proposition 7.2 and see that $\#\{hA_0\mathcal{D}^{(a,b)}(X)\cap\mathcal{L}_i\} = 1/m^{n^2}\,\mathrm{Vol}(hA_0\mathcal{D}^{(a,b)}(X))$, up to an error of $o(X^{n^2})$. Summing over i, we obtain

$$\int_{h\in\mathcal{F}\backslash\mathcal{F}'} \#\{hA_0\mathcal{D}^{(a,b)}(X)\cap\mathcal{L}\}dh = k/m^{n^2}\int_{h\in\mathcal{F}\backslash\mathcal{F}'} \mathrm{Vol}(hA_0\mathcal{D}^{(a,b)}(X))dh + o(X^{n^2}).$$

The lemma follows from the observation that the product of the p-adic densities of $\mathcal{L}\subset W(\mathbb{Z})$ equals k/m^{n^2}. □

The proof of Theorem 7.9 runs along the same lines as the proof of Theorem 7.1. The only additional input is Lemma 7.10, which has to be applied at the obvious point.

7.3.1. *Computations modulo p and consequences.*

Lemma 7.11. *The ratio of the number of reducible elements in $W(\mathbb{F}_p)$ to the total number of elements in $W(\mathbb{F}_p)$ is bounded away from 1 independent of p.*

Proof. It suffices to show that the ratio of irreducible elements in $W(\mathbb{F}_p)$ to the total number of elements is bounded away from 0.

The total number of invariants modulo p is p^n. The cardinality of $H(\mathbb{F}_p)$ is at least $p^{n^2-n}/2$ for a large enough p. The stabilizer of any regular semisimple element has at most 2^n elements. The cardinality of $W(\mathbb{F}_p)$ is p^{n^2}. We define a set of invariants a_i, e to be "good" if there exists an orbit with these invariants which is regular semisimple. It suffices to prove that the ratio of the number of good invariants to the total number of invariants is bounded away from 0. Indeed, if there were N good invariants, then there would be at least $Np^{n^2-n}/2^{n+1}$ irreducible elements in $W(\mathbb{F}_p)$. If $\frac{N}{p^n} > r_n$, then $\frac{Np^{n^2-n}/2^{n+1}}{p^{n^2}} > r_n/2^{n+1}$.

The proportion of polynomials $f(x)$ of degree n which have at least three irreducible factors, which also have a nonzero discriminant, and whose constant term a nonzero square is positive and bounded away from 0 independent of p. Let r_n be some positive lower bound for the above proportion for all p. For invariants giving such polynomials, the number of $\mathbb{F}_p$-orbits is at least 4. This is because $L = \mathbb{F}_p[x]/(f(x))$ will be a product of at least three fields, so $|(L^\times/L^{\times 2})_{N=1}| \geq 4$. Such invariants have to be good because there have to be at least two irreducible $\mathbb{F}_p$ orbits. The lemma follows. □

Proposition 7.12. *We have*

$$\int_{h\in\mathcal{F}\backslash\mathcal{F}'} \#\{hA_0\mathcal{D}(X)\cap W(\mathbb{Z})^{\mathrm{irr}}\}dh = \int_{h\in\mathcal{F}\backslash\mathcal{F}'} \#\{hA_0\mathcal{D}(X)\cap W(\mathbb{Z})\}dh + o(X^{n^2}).$$

Proof. It suffices to prove

$$\int_{h\in\mathcal{F}\setminus\mathcal{F}'} \#\{hA_0\mathcal{D}(X)\cap W(\mathbb{Z})^{\mathrm{red}}\}dh = o\Big(\int_{h\in\mathcal{F}\setminus\mathcal{F}'} \#\{hA_0\mathcal{D}(X)\cap W(\mathbb{Z})\}dh\Big).$$

To that end, fix $Y\in\mathbb{N}$, some positive number, and let $\mathcal{L}_Y\subset W(\mathbb{Z})$ be the set of all elements whose reduction modulo p is reducible in $W(\mathbb{F}_p)$ for $p\le Y$. For every $Y\in\mathbb{N}$, the set $\mathcal{L}_Y$ is defined by congruence conditions and contains $W(\mathbb{Z})^{\mathrm{red}}$.

By Lemma 7.10, we have

$$\int_{h\in\mathcal{F}\setminus\mathcal{F}'} \#\{hA_0\mathcal{D}(X)\cap\mathcal{L}_Y\}dh = \prod_{p<Y}\mu_p(\mathcal{L}_Y)\int_{h\in\mathcal{F}\setminus\mathcal{F}'} \#\{hA_0\mathcal{D}(X)\cap W(\mathbb{Z})\}dh.$$

By Lemma 7.11, each $\mu_p(\mathcal{L}_Y)$ is bounded away from 1 independent of p. Therefore, we have $\lim_{Y\to\infty}\prod_{p<Y}\mu_p(\mathcal{L}_Y)=0$.

The proposition follows because $W(\mathbb{Z})^{\mathrm{red}}\subset\mathcal{L}_Y$ for all Y. □

Lemma 7.13. *The proportion of elements in $W(\mathbb{F}_p)$ having a nontrivial stabilizer in $H(\mathbb{F}_p)$ is bounded away from* 1 *independent of p.*

Proof. Using the same argument as in Lemma 7.11, it suffices to show that the proportion of invariants having the required property is bounded away from 1 independent of p. To that end, we remark that the proportion of degree n polynomials which are irreducible with a constant term to a nonzero perfect square is bounded away from 0 independent of p. The proposition follows. □

Proposition 7.14. *Let $S\subset W(\mathbb{Z})$ consist of those T with the property that $\Delta_T(\mathbb{Q})$ is nontrivial. Then $N(S,X)=o(X^{n^2})$.*

Proof. Let $f\in\mathbb{Z}[x]$ be the polynomial associated with T. By Corollary 4.2, the stabilizer in $H(\mathbb{Q})$ is nontrivial if and only if f is not irreducible. Clearly, f is irreducible in $\mathbb{Q}[x]$ only if its reduction modulo p is irreducible for every prime p, and by applying Corollary 4.2 again, we see that this happens precisely when the stabilizer of T modulo p is trivial. However, by Lemma 7.13, the proportion of elements in $W(\mathbb{F}_p)$ having a nontrivial stabilizer is bounded away from 1 independent of p. The product of this ratio over all primes converges to 0. Therefore, the same argument as in the proof of Proposition 7.12 applies to prove our result. □

Lemma 7.15. *For a large enough p, the proportion of invariants over $\mathbb{F}_p$ either which are not regular semisimple or which satisfy the condition that the distinguished orbits are in the same $H(\mathbb{F}_p)$-orbit is bounded away from* 1 *independent of p.*

Proof. It suffices to show that the proportion of invariants over $\mathbb{F}_p$ which are regular semisimple, and such that the distinguished orbits are in different $H(\mathbb{F}_p)$-orbits, is bounded away from 0 independent of p. The proportion of invariants such that the corresponding polynomial f has n distinct nonzero roots over $\mathbb{F}_p$ is bounded away from 0 independent of p. The proportion of such an f, with the properties that at least one root is a perfect square in $\mathbb{F}_p^\times$ and at least one root is *not* a perfect square, is again bounded away from 0 independent of p. Therefore, the proportion of invariants with the property that γ is not a perfect square in $L^\times$ is bounded away from 0 independent of p (here, $L=\mathbb{F}_p[x]/(f(x))$ is the étale algebra associated to

regular semisimple invariants). If (-1) is a square in $\mathbb{F}_p^\times$, then $(-\gamma)$ is clearly not a perfect square either. If (-1) is not a perfect square, then because one of the components of γ is a perfect square, that component of $(-\gamma)$ would now cease to be a square. In either case, $(-\gamma)$ is *not* a perfect square.

The result follows from Corollary 4.6, which states that the two distinguished orbits lie in the same $H(\mathbb{F}_p)$-orbit if and only if $-\gamma$ is a perfect square in $L^\times$. □

Proposition 7.16. *Let N_X denote the number of invariants $c \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{Z})$ with height bounded by X such that the two distinguished orbits in $W(\mathbb{Q})$ with invariants c lie in the same $H(\mathbb{Q})$-orbit. Then $N_X = o(X^{n^2})$; i.e., the proportion of N_X to the number of invariants with height bounded by X goes to 0.*

Proof. Fix $c \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{Z}) \subset \mathrm{Inv}^{\mathrm{rs}}(\mathbb{Q})$, and let L denote the corresponding étale algebra of dimension n. By Corollary 4.6, the two distinguished orbits lie in the same $H(\mathbb{Q})$-orbit, precisely when $-\gamma$ is a perfect square in $L^\times$. As $c \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{Z})$, all the data can be reduced modulo all primes p.

If $(-\gamma)$ is a perfect square, then either c modulo p is no longer regular semisimple or the corresponding $(-\gamma) \in L_p^\times$ stays a square (here, L_p is the étale $\mathbb{F}_p$ algebra corresponding to the reduction of c modulo p).

Therefore, if the two distinguished orbits lie in the same $H(\mathbb{Q})$-orbit, then either the reduction of c modulo p is not regular semisimple or the two $\mathbb{F}_p$ distinguished orbits lie in the same $H(\mathbb{F}_p)$-orbit. The set whose cardinality is N_X is cut out by infinitely many congruence conditions, whose local densities (by Lemma 7.15) are bounded away from 1. The proposition follows. □

We conclude this paragraph with a lemma which we will need to prove Theorem 1.4.

Lemma 7.17. *Consider the proportion r_p of $c = (a_1, a_2, \ldots, a_{n-1}, e) \in \mathrm{Inv}(\mathbb{F}_p)$ with the following properties:*

1. *The associated polynomial f satisfies $f(0) = 0$, i.e., $e = 0$.*
2. *f has distinct roots $u_1,\ u_2, \ldots, u_{n-1},\ u_n = 0$ over $\mathbb{F}_p$*
3. *The product of the nonzero roots is a perfect square.*

Then for a large enough p there exists some $r > 0$ independent of p such that $r_p > r/p$.

Proof. The number of invariants such that the corresponding f has distinct roots over $\mathbb{F}_p$, one of which is 0, is $\prod_{i=1}^{n-1}(p-i)/(n-1)!$. Adding the condition that the product of the nonzero roots is a square is the same as scaling this by a factor of $1/2$. The ratio $p\prod_{i=1}^{n-1}(p-i)/(n-1)!p^n$ is clearly bounded away from 0 independent of p. The lemma follows. □

7.3.2. *Infinitely many congruence conditions.* In this section, we count elements having bounded height in subsets of $\mathrm{Inv}(\mathbb{Z})$ and $W(\mathbb{Z})$ that are defined by certain infinite sets of congruence conditions.

Definition 10. Let $\Sigma \subset \mathrm{Inv}(\mathbb{Z})$ be a set defined by (possibly infinitely many) congruence conditions. For a prime p, let Σ_p denote the closure of Σ in $\mathrm{Inv}(\mathbb{Z}_p)$. We say that Σ is *large at p* if Σ_p contains every c such that the reduction of f_c modulo p has no triple root. The set $\Sigma \subset \mathrm{Inv}(\mathbb{Z})$ is then said to be *large* if it is large at all but finitely many primes.

We now have the following theorem counting the number of elements having bounded height in large sets.

Theorem 7.18. *Let $\Sigma \subset \mathrm{Inv}(\mathbb{Z})$ be large. Then*

$$\#\{c \in \Sigma \cap \mathrm{Inv}(\mathbb{R})^{(a,b)} \,|\, \mathrm{ht}(c) < X\} \sim \prod_p \mathrm{Vol}(\Sigma_p)\,\mathrm{Vol}(\mathrm{Inv}(\mathbb{R})^{(a,b)}_{\mathrm{ht}<X}).$$

Here, $\sim$ denotes asymptotic equality.

Proof. Let $Z \subset \mathrm{Inv}$ denote the variety of elements c such that f_c has a triple root. Then Z has codimension 2. Let $Y_p \subset \mathrm{Inv}(\mathbb{Z})$ denote the set of elements c whose reduction modulo p lie in $Z(\mathbb{F}_p)$. An argument identical to the proof of [3, Theorem 3.5] yields the estimate

$$\#\bigcup_{p>M}\{c \in Y_p : \mathrm{ht}(c) < X\} = O\Big(\frac{X^{n^2}\log X}{M}\Big).$$

The theorem now follows from the above "tail estimate" using standard sieving arguments (see, for example, the proof of [6, Theorem 2.21]). □

Next, we need a weighted version of Theorem 7.9 that allows for infinitely many congruence conditions. Let $\phi : W(\mathbb{Z}) \to [0,1]$ be a $H(\mathbb{Z})$-invariant function. Then let $N_\phi(W(\mathbb{Z}), X)$ denote the number of irreducible $H(\mathbb{Z})$-orbits of $W(\mathbb{Z})$ having height bounded by X, where each orbit $H(\mathbb{Z})\cdot T$ is weighted by $\dfrac{\phi(T)}{\#\,\Delta_T(\mathbb{Z})}$.

Definition 11. A function $\phi : W(\mathbb{Z}) \to [0,1]$ is said to be defined by congruence conditions if there exist local functions $\phi_p : W(\mathbb{Z}_p) \to [0,1]$ satisfying the following conditions:

(1) For all $T \in W(\mathbb{Z})$, $\prod_p(\phi_p(T))$ converges to $\phi(T)$.
(2) For each prime p, ϕ_p is locally constant outside a closed set of measure 0.

Theorem 7.19. *Suppose that $\phi : W(\mathbb{Z}) \to [0,1]$ is defined by congruence conditions, and that the ϕ_p are $H(\mathbb{Z}_p)$-invariant. Then*

$$N_\phi(W(\mathbb{Z}), X) \le N(W(\mathbb{Z}), X)\prod_p \int_{T\in W(\mathbb{Z})} \phi_p(T)dT + o(X^{n^2}).$$

If the function ϕ were nice enough, we would expect the upper bound to be an equality. We will not make precise in this paper what "nice" means (see [16, §4] for the precise definition) and will content ourselves by saying that a function which were to pick out locally 1-soluble orbits would be nice.

Proof. For $N \in \mathbb{N}$, define $\phi_{p,N} : W(\mathbb{Z}_p) \to [0,1]$ to be $\phi_{p,N}(T) = \max_{T'\in Z}\phi_p(T')$, where $Z = \{T' : T' \equiv T \mod p^N\}$. Because ϕ_p is $H(\mathbb{Z}_p)$ invariant, so is $\phi_{p,N}$. Further, as ϕ_p is locally constant (outside a set of measure 0), $\phi_{p,N}$ converges to ϕ_p as N goes to infinity. For $Y \in \mathbb{N}$, define ψ_Y as $\prod_{p<Y}\phi_p$, and define $\psi_{Y,N}$ as $\prod_{p<Y}\phi_{p,N}$.

The same method used to prove Theorem 7.9 applies to prove this result (with equality instead of an upper bound) for the function $\psi_{Y,N}$. Therefore, we have

$$\begin{aligned} N_\phi(W(\mathbb{Z}), X) &\le N_{\psi_{Y,N}}(W(\mathbb{Z}), X) \\ &= N(W(\mathbb{Z}), X)\prod_{p<Y}\int_{T\in W(\mathbb{Z})}\psi_{p,N}(T)dT + o(X^{n^2}). \end{aligned}$$

The theorem follows by allowing N, and then Y, to go to infinity. □

8. Selmer groups

In this section, we prove a strengthening of Theorems 1.1 and 1.4. Recall that for $c = (a_1, \dots, a_{n-1}, e) \in \mathrm{Inv}$, we have associated a polynomial $f_c(x)$ and hyperelliptic curves whose affine equations are $y^2 = f_c(x)$ and $y^2 = xf_c(x)$.

Theorem 8.1. *Let $\Sigma \subset \mathrm{Inv}(\mathbb{Z})$ be any large family with the property that Σ_2 is contained in the subset of $\mathrm{Inv}(\mathbb{Z}_2)$ consisting of all $c = (a_1, \dots, a_{n-1}, e)$ such that $2^{4i}|a_i$ and $2^{2n}|e$. Then the average size over Σ of $\mathrm{Sel}_2(J_{1,c})$ is bounded above by 6, and the average size of $\mathrm{Sel}_{(1,2)}(c)$ equals 2.*

Theorems 1.1 and 1.4 follow from applying Theorem 8.1 to the large family Σ^0, chosen as follows.

For $p \neq 2$, let $\Sigma_p \subset \mathrm{Inv}(\mathbb{Z}_p)$ consist of all $c = (a_1, \dots, a_{n-1}, e)$ such that either $p^2 i \nmid a_i$ for some i or $p^n \nmid e$. Let Σ_2 consist of all $c = (a_1, \dots, a_{n-1}, e)$ such that $2^{4i}|a_i$, $2^{2n}|e$, and let either $2^{6i} \nmid a_i$ for some i or $2^{3n} \nmid e$. Let $\Sigma^0 \subset \mathrm{Inv}(\mathbb{Z})$ be the subset defined by the local condition Σ_p, i.e., $\Sigma^0 = \{c \in \mathrm{Inv}(\mathbb{Z}) |\ \forall p,\ c \in \Sigma_p\}$.

We spend the rest of the section proving Theorem 8.1. Henceforth, by soluble we will mean 1-soluble. Let $\phi : W(\mathbb{Z}) \to [0, 1]$ be the function

(4)
$$\phi(T) = \begin{cases} \Big(\sum\limits_{T'} \dfrac{\#\,\Delta_{T'}(\mathbb{Q})}{\#\,\Delta_{T'}(\mathbb{Z})}\Big)^{-1} & \text{if } T \text{ is locally soluble and } T \text{ has invariants in } \Sigma, \\ 0 & \text{otherwise,} \end{cases}$$

where the sum is over a complete set of representatives for the action of $H(\mathbb{Z})$ on the $H(\mathbb{Q})$-equivalence class of T in $W(\mathbb{Z})$. Similarly, let $\phi_{12} : W(\mathbb{Z}) \to [0, 1]$ be defined as follows:

(5)
$$\phi_{12}(T) = \begin{cases} \Big(\sum\limits_{T'} \dfrac{\#\,\Delta_{T'}(\mathbb{Q})}{\#\,\Delta_{T'}(\mathbb{Z})}\Big)^{-1} & \text{if } T \text{ is locally } (1,2)\text{-soluble and } T \text{ has invariants} \\ & \text{in } \Sigma, \\ 0 & \text{otherwise.} \end{cases}$$

The sum is again over a complete set of representatives for the action of $H(\mathbb{Z})$ on the $H(\mathbb{Q})$-equivalence class of Y in $W(\mathbb{Z})$.

Proposition 8.2. *Let $\Sigma^{(a,b)} = \Sigma \cap \mathrm{Inv}(\mathbb{R})^{(a,b)}$. Then*

$$\sum_{\substack{c \in \Sigma^{(a,b)} \\ \mathrm{ht}(c) \leq X}} (\#\,\mathrm{Sel}_2(J_{1,c}) - 2) = N_\phi(W(\mathbb{Z})^{(a,b)}, X) + o(X^{n^2}),$$

$$\sum_{\substack{c \in \Sigma^{(a,b)} \\ \mathrm{ht}(c) \leq X}} (\#(\mathrm{Sel}_2(J_{1,c}) \cap \mathrm{Sel}_2(J_{2,c})) - 2) = N_{\phi_{12}}(W(\mathbb{Z})^{(a,b)}, X) + o(X^{n^2}).$$

Proof. The proof in the $(1, 2)$-soluble case is identical to the proof of the soluble case; hence, we will demonstrate only the first proof. By Proposition 7.16, the set of $c \in \mathrm{Inv}(\mathbb{Z})^{(a,b)}$ with $\mathrm{ht}(c) \leq X$ and which satisfy the condition that the two distinguished elements lie in the same $H(\mathbb{Q})$ orbit is $o(X^{n^2})$. Further, by

Theorem 6.2, every element in $\mathrm{Sel}_2(J_{1,c}) \subset H^1(J_{1,c}[2])$ gives rise to integral orbits, which by definition are locally soluble. Therefore,

$$\sum_{\substack{c\in\Sigma^{(a,b)}\\ \mathrm{ht}(c)\le X}} (\#\,\mathrm{Sel}_2(J_{1,c}) - 2) = \#(H(\mathbb{Q})\backslash W(\mathbb{Z})^{\mathrm{irr},\phi\neq 0}_{\mathrm{ht}\le X}) + o(X^{n^2}).$$

Recall that in the definition of $N(S,X)$ for sets S, the $H(\mathbb{Z})$-orbit of $T\in S$ was weighted by $\frac{1}{\#\,\Delta_T(\mathbb{Z})}$. Let $c\in \mathrm{Inv}$ be the invariants of $T\in W(\mathbb{Z})^{(a,b),\phi\neq 0}$. Suppose that $T = T_1\cdots T_k$ are a set of representatives for the action of $H(\mathbb{Z})$ on the $H(\mathbb{Q})$-equivalence class of T in $W(\mathbb{Z})$. Each T_i would be counted on the right-hand side with a weight of $\frac{\phi(T_i)}{\#\,\Delta_{T_i}(\mathbb{Z})}$. The term $\phi(T_i)$ is independent of i and equals $\left(\sum_{i=0}^k \frac{\#\,\Delta_{T_i}(\mathbb{Q})}{\#\,\Delta_{T_i}(\mathbb{Z})}\right)^{-1}$. We now sum over i:

$$\sum_{i=0}^{k} \frac{\phi(T_i)}{\#\,\Delta_{T_i}(\mathbb{Z})} = \phi(T)\sum_{i=0}^{k}\frac{1}{\#\,\Delta_{T_i}(\mathbb{Z})} = \frac{1}{\#\,\Delta_T(\mathbb{Q})}.$$

Therefore, $N_\phi(W(\mathbb{Z})^{(a,b)},X)$ counts each locally soluble $H(\mathbb{Q})$-orbit having invariants in Σ, with a representative T in $W(\mathbb{Z})$ with a weight of $\frac{1}{\#\,\Delta_T(\mathbb{Q})}$. By Proposition 7.14, the number of orbits having nontrivial stabilizer over $\mathbb{Q}$ is $o(X^{n^2})$. The proposition follows. □

We define the local analogues ϕ_p and $\phi_{12,p}$, functions from $W(\mathbb{Z}_p)\to[0,1]$.

$$\phi_p(T) = \begin{cases} \left(\sum_{T'} \frac{\#\,\Delta_{T'}(\mathbb{Q}_p)}{\#\,\Delta_{T'}(\mathbb{Z}_p)}\right)^{-1} & \text{if } T \text{ is soluble and } T \text{ has invariants in } \Sigma,\\ 0 & \text{otherwise,}\end{cases} \tag{6}$$

$$\phi_{12,p}(T) = \begin{cases} \left(\sum_{T'} \frac{\#\,\Delta_{T'}(\mathbb{Q}_p)}{\#\,\Delta_{T'}(\mathbb{Z}_p)}\right)^{-1} & \text{if } T \text{ is } (1,2)\text{-soluble, and } T \text{ has invariants in } \Sigma,\\ 0 & \text{otherwise,}\end{cases} \tag{7}$$

where, in both cases, the sum is over a complete set of representatives of $H(\mathbb{Z}_p)$ on the $H(\mathbb{Q}_p)$-equivalence class of Y in $W(\mathbb{Z}_p)$. The local weight functions are related to the global ones in the following way.

Proposition 8.3. *Let w denote either ϕ or ϕ_{12}. Then $w(T) = \prod_p w_p(T)$.*

Proof. The class numbers of $\mathrm{SO}(V_1)$ and $\mathrm{SO}(V_2)$ are 1, and therefore the class number of $H = \mathrm{SO}(V_1)\times\mathrm{SO}(V_2)$ is also 1. This being the case, the same proof as in [6] applies. □

Recall that for $c\in\mathrm{Inv}(\mathbb{Q}_p)$, W_c is the fiber in W over c. In order to compute $N_\phi(W(\mathbb{Z}),X)$ and $N_{\phi_{12}}(W(\mathbb{Z}),X)$, we will need to compute the p-adic integrals listed in Theorem 7.19. To that end, let dT and dc denote Euclidean measures on W and Inv, so that $W(\mathbb{Z})$ and $\mathrm{Inv}(\mathbb{Z})$ have covolume 1. Pick ω, an algebraic differential form that generates the rank 1 module of the top-degree left invariant differential forms on $H = \mathrm{SO}(V_1)\times\mathrm{SO}(V_2)$. We cite the following result from [6, Proposition 3.11].

Proposition 8.4. *Let $|\cdot|$ denote the p-adic valuation on $\mathbb{Z}_p$. There then exists a rational nonzero constant $\mathcal{J}$, independent of p, such that for any $H(\mathbb{Z}_p)$-invariant function w_p on $W(\mathbb{Z}_p)$, we have*

$$\int_{W(\mathbb{Z}_p)} w(T)dT = \mathrm{Vol}(H(\mathbb{Z}_p))|\mathcal{J}| \int_{c\in \mathrm{Inv}(\mathbb{Z}_p)} \Big(\sum_{T\in \frac{W_c(\mathbb{Z}_p)}{H(\mathbb{Z}_p)}} \frac{w_p(T)}{\#\,\Delta_T(\mathbb{Z}_p)}\Big) dc,$$

where $\frac{W_c(\mathbb{Z}_p)}{H(\mathbb{Z}_p)}$ denotes a set of representatives for the action of $H(\mathbb{Z}_p)$ on $W_c(\mathbb{Z}_p)$.

We will also want to express the volume of $\mathcal{FD}^{(a,b)}(X)$ in terms of the volume on $H(\mathbb{R})$ and $\mathrm{Inv}(\mathbb{R})$. The proof of the following proposition is the same as in [6, Proposition 3.12].

Proposition 8.5. *The volume of the multiset $\mathcal{FD}^{(a,b)}_{\mathrm{sol}}(X)$ is given by*

$$\mathrm{Vol}(\mathcal{FD}^{(a,b)}_{\mathrm{sol}}(X)) = \tau^{(a,b)}_{\mathrm{sol}}|\mathcal{J}|\,\mathrm{Vol}(\mathcal{F})\,\mathrm{Vol}(\mathrm{Inv}(\mathbb{R})^{(a,b)}_{\mathrm{ht}<X}).$$

Here, $\mathcal{J}$ is the same constant that appears in Proposition 8.4*, and the numbers $\tau^{(a,b)}_{\mathrm{sol}}$ are as in* §7.1.

The proofs of [6, Propositions 3.11 and 3.12] apply because the action of H on W satisfy the conditions in [6, Remark 3.14]. Indeed, the ring of invariants is freely generated; the stabilizer of a regular semisimple element is a finite group scheme of order 2^{n-1} and is therefore uniformly bounded (outside the discriminant-0 locus); the sum of the degrees of the invariants equals n^2, the dimension of W; and there exist Kostant sections $\kappa : \mathrm{Inv} \to W$.

We need to simplify the expression

$$\int_{c\in\Sigma_p} \Big(\sum_{T\in \frac{W_c(\mathbb{Z}_p)}{H(\mathbb{Z}_p)}} \frac{w_p(T)}{\#\,\Delta_T(\mathbb{Z}_p)}\Big) dc,$$

where w stands for either ϕ_p or $\phi_{12,p}$. We have

$$\sum_{T\in \frac{W_c(\mathbb{Z}_p)}{H(\mathbb{Z}_p)}} \frac{w_p(T)}{\#\,\Delta_T(\mathbb{Z}_p)} = \frac{\#(W_c(\mathbb{Q}_p)_{\mathrm{sol}}/H(\mathbb{Q}_p))}{\#\,\Delta_T(\mathbb{Q}_p)},$$

where the subscript sol is as in §7.1. Depending on whether sol stands for 1 soluble or $(1,2)$-soluble, we have

$$\#(W_c(\mathbb{Q}_p)_1/H(\mathbb{Q}_p)) = \#\frac{J_{1,c}(\mathbb{Q}_p)}{2J_{1,c}(\mathbb{Q}_p)}$$

and

$$\#(W_c(\mathbb{Q}_p)_{(1,2)}/H(\mathbb{Q}_p)) = \#\left(\frac{J_{1,c}(\mathbb{Q}_p)}{2J_{1,c}(\mathbb{Q}_p)} \cap \frac{J_{2,c}(\mathbb{Q}_p)}{2J_{2,c}(\mathbb{Q}_p)}\right),$$

where the intersection happens in $H^1(\mathbb{Q}_p, \Delta_c)$.

8.1. **Average size of the 2-Selmer group.** We now bound the average size of the 2-Selmer group of our family of hyperelliptic curves. Recall that the set of hyperelliptic curve with the extra marked points is in bijection with $\Sigma \subset \mathrm{Inv}(\mathbb{Z})$. Without any loss of generality, we restrict ourselves to the family over $\Sigma^{(a,b)}$ for a fixed pair (a,b). Using Propositions 6.5 and 6.11, if $c \in \Sigma_p$, the integrand in

Proposition 8.4 is constant and equals b_p. The integrand is 0 if $c \notin \Sigma_p$. Substituting this into Proposition 8.4, we obtain

$$\sum_{\substack{c\in\Sigma^{(a,b)}\\ \mathrm{ht}(c)\le X}} (\#\operatorname{Sel}_2(J_{1,c})-2) \le N(W(\mathbb{Z})^{(a,b)},X) \times \prod_p \left(b_p|\mathcal{J}|_p \operatorname{Vol}(H(\mathbb{Z}_p))\operatorname{Vol}(\Sigma_p)\right) + o(X^{n^2}).$$

Further, by Proposition 8.5 and Theorem 7.1,

$$N(W(\mathbb{Z})^{(a,b)},X) = |\mathcal{J}|\frac{\tau_1^{(a,b)}}{\eta^{(a,b)}}\operatorname{Vol}(\mathcal{F})\operatorname{Vol}(\mathrm{Inv}(\mathbb{R})^{(a,b)}_{\mathrm{ht}<X}) + o(X^{n^2}).$$

Clearly, $b_\infty = \frac{\tau_1^{(a,b)}}{\eta^{(a,b)}}$ because the numerator equals the number of real soluble orbits. Therefore, by using the fact that the b_ν all multiply by 1, we see that the main term simplifies to

$$\operatorname{Vol}(\mathrm{Inv}(\mathbb{R})^{(a,b)}_{\mathrm{ht}<X})\operatorname{Vol}(\mathcal{F})\prod_p \operatorname{Vol}(H(\mathbb{Z}_p)).$$

The product of the local volumes along with $\operatorname{Vol}(\mathcal{F})$ is the Tamagawa number of H, which equals 4 [11]. Therefore, we have

$$\sum_{\substack{c\in\Sigma^{(a,b)}\\ \mathrm{ht}(c)\le X}} (\#\operatorname{Sel}_2(J_{1,c})-2) \le 4\operatorname{Vol}(\mathrm{Inv}(\mathbb{R})^{(a,b)}_{\mathrm{ht}<X})\prod_p \operatorname{Vol}(\Sigma_p).$$

The number of hyperelliptic curves in our family with height less than X is $\sum_{\substack{c\in\Sigma^{(a,b)}\\ \mathrm{ht}(c)\le X}} 1$, which by Theorem 7.18 is $\operatorname{Vol}(\mathrm{Inv}(\mathbb{R})^{(a,b)}_{\mathrm{ht}<X})\prod_p \operatorname{Vol}(\Sigma_p)$ up to an error of $o(X^{n^2})$. Putting all of this together, we have

$$\lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{c\in\Sigma^{(a,b)}\\ \mathrm{ht}(c)\le X}} (\#\operatorname{Sel}_2(J_{1,c})-2)}{\displaystyle\sum_{\substack{c\in\Sigma^{(a,b)}\\ \mathrm{ht}(c)\le X}} 1} \le 4.$$

Therefore, we have the average size of the 2-Selmer group is bounded above by 6.

8.2. **The (1,2)-Selmer group.**

Proposition 8.6. *Let $p > 2$ be a large enough prime. We have*

$$\int_{\mathrm{Inv}(\mathbb{Z}_p)} \frac{\#(J_{1,c}(\mathbb{Q}_p)/2J_{1,c}(\mathbb{Q}_p)\cap J_{2,c}(\mathbb{Q}_p)/2J_{2,c}(\mathbb{Q}_p))dh}{\#\,\Delta_c(\mathbb{Q}_p)}dc \le (1-a/p)\operatorname{Vol}(\mathrm{Inv}(\mathbb{Z}_p)),$$

where the intersection happens inside $H^1(\mathbb{Q}_p,\Delta_c)$, and a is some positive constant independent of p.

Proof. For ease of notation, we will drop the subscript c. We had remarked earlier (Proposition 6.5) that $\dfrac{\#J_1(\mathbb{Q}_p)/2J_1(\mathbb{Q}_p)}{\#\Delta(\mathbb{Q}_p)} = 1$. The same holds true with J_2 in place of J_1. Therefore, 1 is a trivial upper bound for the integral. We note that for some c, if the images of $J_1(\mathbb{Q}_p)/2J_1(\mathbb{Q}_p)$ and $J_2(\mathbb{Q}_p)/2J_2(\mathbb{Q}_p)$ do not coincide,

then the integrand will be at most $1/2$. We will show that there exists $S \subset \mathrm{Inv}(\mathbb{Z}_p)$ of volume greater than r/p, such that for $c \in S$, the images of J_1 and J_2 do not coincide. Here, r is the constant alluded to in Lemma 7.17. The proposition follows from the existence of S. Indeed,

$$\int_{\mathrm{Inv}(\mathbb{Z}_p)} \frac{\#(J_{1,c}(\mathbb{Q}_p)/2J_{1,c}(\mathbb{Q}_p) \cap J_{2,c}(\mathbb{Q}_p)/2J_{2,c}(\mathbb{Q}_p))dh}{\#\,\Delta_c(\mathbb{Q}_p)}dc$$
$$\leq \int_{\mathrm{Inv}(\mathbb{Z}_p)\setminus S} 1dc + \int_{c\in S} 1/2dc \leq (1-r/p)\,\mathrm{Vol}(\mathrm{Inv}_p(F)) + (r/2p)\,\mathrm{Vol}(\mathrm{Inv}_p(F)).$$

Setting $a = r/2$ gives the proposition.

Let $S_p \subset \mathrm{Inv}(\mathbb{F}_p)$ be the subset defined by the conditions in Lemma 7.17. Let $S' \subset \mathrm{Inv}(\mathbb{Z}_p)$ be the set of all points reducing to S_p. For $c \in S'$, the polynomial f_c factors into distinct linear factors over $\mathbb{Z}_p$ (Hensel's lemma), so the discriminant of f_c is not 0. In fact, it is a unit. For such c, exactly one of the roots of f_c is a multiple of p. Indeed, its p-adic valuation has to equal $2b$ for some positive integer b (this is because $f_c(0) = e_c^2$). Let S'' denote the set of all $c \in S'$ such that $e_c = 0$. Clearly, S'' is a measure-0 set. Let $S = S' \setminus S''$. The set S has a volume of at least r/p.

We therefore are left with showing that for $c \in S$, the images of $J_1(\mathbb{Q}_p)$ and $J_2(\mathbb{Q}_p)$ in $H^1(\mathbb{Q}_p, \Delta_c)$ do not coincide. By construction, f_c splits into linear factors which are pairwise unequal modulo p over $\mathbb{Z}_p$. We therefore have $\Delta_c = \mathrm{Res}_{\mathbb{Q}_p^n/\mathbb{Q}_p}(\mu_2)_{N=1}$, and $H^1(\mathbb{Q}_p, \Delta_c) = ((\mathbb{Q}_p^\times)^n/(\mathbb{Q}_p^{\times 2})^n)_{N=1}$. Because the discriminant of f_c is a p-adic unit, by Proposition 6.8, the image of $J_1(\mathbb{Q}_p)$ equals $((\mathbb{Z}_p^\times)^n/(\mathbb{Z}_p^{\times 2})^n)_{N=1}$. In order to show that the image of $J_2(\mathbb{Q}_p)$ is not the same, it suffices to show the existence of an element in $H^1(\mathbb{Q}_p, \Delta_c)$ with odd p-adic valuation in at least one of its components. We will show that $pf_c(p)$ is a perfect square in $\mathbb{Q}_p$, thereby demonstrating the existence of a $\mathbb{Q}_p$-rational point Q of $y^2 = xf_c(x)$ with an x coordinate having p-adic valuation 1 (indeed, the x coordinate by construction would equal p). It is then easy to see, using the explicit descent map described in [17], that the image of $Q - \infty_1$ in $H_1(\mathbb{Q}_p, \Delta_c)$ has the property that at least one of its components has odd p-adic valuation, thereby completing the proof.

Thus, it suffices to show that $pf_c(p)$ is a perfect square in $\mathbb{Q}_p$. Suppose that $u_i' \in \mathbb{Z}_p^\times$, which lift $u_i \in \mathbb{F}_p^\times$, are the roots of f_c. Suppose that $p^{2b}u_e' \neq 0$ is the final root (which as mentioned above has p-adic valuation equaling $2b$). Then $f_c(p) = (p - p^{2b}u_e')\prod_{i=1}^{n-1}(p-u_i') = p(1-p^{2b-1}u_e')\prod_{i=1}^{n-1}(p-u_i')$. Since n is odd,

$$\prod_{i=1}^{n-1}(p-u_i') = \prod_{i=1}^{n-1}(u_i'-p) \equiv \prod_{i=1}^{n-1} u_i' \mod p.$$

By construction, $\prod_{i=1}^{n-1}(p-u_i')$ is a nonzero square modulo p and is therefore a square in $\mathbb{Z}_p^\times$. Similarly, $1-p^{2b-1}u_e'$ is also a square in $\mathbb{Z}_p^\times$. Therefore, $f_c(p)$ is p multiplied by a square, so $pf_c(p)$ must be a square in $\mathbb{Q}_p^\times$. We have proved our result. □

We now prove that the average size of $\mathrm{Sel}_2(J_1) \cap \mathrm{Sel}_2(J_2)$ is 2. Again, it suffices to restrict ourselves to the family over $\Sigma^{(a,b)} = \Sigma \cap \mathrm{Inv}(\mathbb{R})^{(a,b)}$ for a fixed pair (a,b).

It suffices to prove that

$$\lim_{X\to\infty} \frac{\sum\limits_{\substack{c\in\Sigma^{(a,b)}\\ \mathrm{ht}(c)\le X}} (\#(\mathrm{Sel}_2(J_{1,c})\cap \mathrm{Sel}_2(J_{2,c})) - 2)}{\sum\limits_{\substack{c\in\Sigma^{(a,b)}\\ \mathrm{ht}(c)\le X}} 1} = 0.$$

The denominator (up to an error of $o(X^{n^2})$) is a fixed constant multiple of X^{n^2}. We will prove that the numerator is $o(X^2)$. Indeed, we have

$$\sum_{\substack{c\in\Sigma^{(a,b)}\\ \mathrm{ht}(c)\le X}} (\#(\mathrm{Sel}_2(J_1(C))\cap \mathrm{Sel}_2(J_2(C))) - 2) = N_{\phi_{12}}(W(\mathbb{Z})^{(a,b)}_{(1,2)}, X) + o(X^{n^2}).$$

By Theorem 7.19, we have

$$N_{\phi_{12}}(W(\mathbb{Z})^{(a,b)}_{(1,2)}, X) \le N(W(\mathbb{Z})^{(a,b)}_{(1,2)}, X) \prod_p \int_{W(\mathbb{Z}_p)} \phi_{12,p}(T)dT + o(X^{n^2}).$$

The above proposition shows that the product of the local weights converges to 0. We have thus shown that the expression is dominated by the error term $o(X^{n^2})$. Therefore, the above limit equals 0, and we have proved Theorem 8.1.

9. Rational points

We will now apply Poonen and Stoll's refinement of Chabauty's method, as used in [15], [16], to prove Theorem 1.5. Note that it suffices to prove the result for the family $C_{1,c}$: there is a degree 2 map $C_c \to C_{1,c}$ which is ramified over P_1 and P_1'. Therefore, the inverse image of the marked points of $C_{1,c}$ is the four marked points of C_c. Any other rational point of C_c would necessarily map to some nonmarked rational point of $C_{1,c}$, whence it follows that the result for $C_{1,c}$ implies the result for C_c.

The techniques used in [15], [16, §5, §6] apply in our situation, so we content ourselves with merely sketching the overall arguments and referring to [15], [16, §§5 and 6] for proofs.

Recall that $C_{1,c}$ has a marked rational Weierstrass point denoted by ∞_1 and a pair of marked non-Weierstrass points P_1, P_1'. We embed $C_{1,c}$ in $J_{1,c}$ via the Abel–Jacobi map, i.e., by mapping a point P to the class of $(P) - (\infty_1)$. Note that $(P_1) - (\infty_1) = (\infty_1) - (P_1')$.

9.1. **Definition of the maps.** We consider the same diagram as in [16, page 26]. We define a normalized logarithm $J_{1,c}(\mathbb{Q}_2) \to \mathbb{Z}_2^m$ which is surjective and whose kernel is the torsion of $J(\mathbb{Q}_p)$. Let $u \in \mathbb{Z}_2^m$ be nonzero, and suppose that $u \in 2^a\mathbb{Z}_2^m \setminus 2^{a+1}\mathbb{Z}_2^m$. Following [16], we define the primitive part of u to be $u/2^a$. We define v to be the primitive part of the image of P_1 under the Abel–Jacobi map composed with the logarithm, and define $\overline{v}$ to be the reduction of v . For some $u \in \mathbb{Z}_2^m/\mathbb{Z}_2\langle v\rangle$, we define $r(u) \in \mathbb{P}^{m-2}(\mathbb{F}_2)$ to be the projectivization of the mod 2 reduction of the primitive part of u in $\mathbb{F}_2^{m-1}$. Note that r is defined only away from 0. For $P \in C_{1,c}(\mathbb{Q}_2)$, we define $\rho_C(P)$ to equal $r(u)$, where u is the image of P in $\mathbb{Z}_2^m/\mathbb{Z}_2\langle v\rangle$.

The map ρ_C is defined away from the union of the torsion of $C_{1,c}(\mathbb{Q}_2)$ and the intersection of $C_{1,c}(\mathbb{Q}_2)$ and $\mathbb{Z}_2\langle v\rangle$ inside $\mathbb{Z}_2^m$, the image of the logarithm from $J_{1,c}(\mathbb{Q}_p)$. Following [16], we make the following definition.

Definition 12. A point $P \in C_{1,c}(\mathbb{Q}) \setminus \{P_1, P_1', \infty_1\}$ is said to be "bad" if there exist integers a and k such that $a((P) - (\infty_1)) = k((P_1) - (\infty_1))$. A point is said to be good if it is not bad.

The map ρ_C is defined precisely on the set of good points of $C_{1,c}(\mathbb{Q})$ (note that torsion points are bad).

We now define a map $\mathrm{Sel}_2(J_{1,c}) \to \mathbb{P}^{m-2}(\mathbb{F}_2)$ which is defined away from a submodule. There is a natural map (induced by the logarithm) $\rho_A : \mathrm{Sel}_2(J_{1,c}) \to \mathbb{F}_2^m/\mathbb{F}_2\langle\overline{v}\rangle$. Projectivizing yields the map $\rho_S : \mathrm{Sel}_2(J_{1,c}) \to \mathbb{P}^{m-2}$ which is defined away from the kernel of ρ_A.

Following [15], [16], the proof of Theorem 1.5 consists of the steps below.

9.2. **Bounding the size of the image of ρ_C.** The set$\rho_C(C_{1,c}(\mathbb{Q}_2))$ is locally constant and small on average. In other words, the family of hyperelliptic curves we consider can be broken up into large families such that for each family, $\rho_C(C_{1,c}(\mathbb{Q}_p)) \subset \mathbb{P}^{m-2}(\mathbb{F}_2)$ is constant. Further, the average size of $\rho_C(C_{1,c}(\mathbb{Q}_p))$ is small. The precise statement follows.

Proposition 9.1. *Consider the family $C_{1,c}$ for all $c \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{Z}_2)$. The average size of $\rho_C(C_{1,c}(\mathbb{Q}_2))$ is at most $6m + 19$.*

This is the analogue of [15, Corollary 9.10] and [16, Proposition 35], and the proof goes along the same lines. The only difference is that we have three marked points, and this changes the average from $6m + 9$ in [15] to $6m + 19$.

9.3. **Equidistribution of Selmer elements.** The proof of the following statement goes along the same lines of [5, Theorem 12.4].

Proposition 9.2. *When the curves $C_{1,c}$ are ordered by height, the image of the nontrivial and nondistinguished elements of $\mathrm{Sel}_2(J_{1,c})$ under ρ_A equidistribute in $\mathbb{F}_2^{m-1}$.*

As there are four such elements on average, the proportion of $c \in \mathrm{Inv}^{\mathrm{rs}}(\mathbb{Q})$ such that the kernel of ρ_A contains more than the distinguished elements is at most 2^{3-m}. We now restrict ourselves to some large family such that the image of ρ_C is constant and has size I. The proportion of curves such that the image of ρ_S intersects the image of ρ_C is at most $I2^{3-m}$. The corollary below follows immediately.

Corollary 9.3. *For a proportion of at least $1 - (1 + I)2^{3-m}$ curves in our large family, the kernel of ρ_A contains only the distinguished elements, and the images of ρ_S and ρ_C are disjoint.*

9.4. **The image of ρ_C is contained in the image of ρ_S and deals with good points.** Recall that we have assumed that the kernel of ρ_A contains only the distinguished elements.

Proposition 9.4. *For every $P \in C_{1,c}(\mathbb{Q})$ which is good, $\rho_C(P)$ is contained in the image of ρ_S.*

We refer to [16, Lemma 36] for a proof. Restricting ourselves to a large family as above (where the image of ρ_C is constant and has size I), it follows that a proportion of at least $1-(1+I)2^{3-m}$ curves have only three good rational points, namely, the marked points P_1, P_1', ∞_1. As a corollary, we obtain the following result.

Corollary 9.5. *It follows that over the entire family, a proportion of at least* $1-(1+6m+19)2^{3-m}$ *curves have only three good rational points.*

9.5. **Dealing with bad points.** The following result completes the proof of Theorem 1.5.

Proposition 9.6. 0% *of curves have bad points.*

This is the analogue of [16, Theorem 38], and the proof is exactly the same.

Acknowledgments

I am very grateful to Benedict Gross for suggesting that I work on this project, and also for numerous useful conversations. I also thank Manjul Bhargava, Chao Li, Arul Shankar, Jack Thorne, Cheng-Chiang Tsai, and Xiaoheng Wang for helpful discussions. It is a pleasure to thank Arul Shankar and Xiaoheng Wang for very helpful comments on previous versions of this paper. Finally, I thank the referee for greatly helping to improve the exposition of this work.

References

[1] Manjul Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063, DOI 10.4007/annals.2005.162.1031. MR2183288

[2] K. Belabas and C. Delaunay, *Manjul Bhargava, anneaux de petit rang et courbes elliptiques* (French, with French summary), Gaz. Math. **143** (2015), 6–15. MR3338935

[3] M. Bhargava, *The geometric sieve and the density of squarefree values of invariant polynomials*, arXiv:1402.0031 (2014).

[4] Manjul Bhargava and Benedict H. Gross, *Arithmetic invariant theory*, Symmetry: Representation theory and its applications, Progr. Math., vol. 257, Birkhäuser/Springer, New York, 2014, pp. 33–54, DOI 10.1007/978-1-4939-1590-3_3. MR3363006

[5] Manjul Bhargava and Benedict H. Gross, *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, Automorphic representations and L-functions, Tata Inst. Fundam. Res. Stud. Math., vol. 22, Tata Inst. Fund. Res., Mumbai, 2013, pp. 23–91. MR3156850

[6] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242, DOI 10.4007/annals.2015.181.1.3. MR3272925

[7] Armand Borel, *Ensembles fondamentaux pour les groupes arithmétiques* (French), Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962), Librairie Universitaire, Louvain; Gauthier-Villars, Paris, 1962, pp. 23–40. MR0148666

[8] J. W. S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, vol. 13, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978. MR522835

[9] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183, DOI 10.1112/jlms/s1-26.3.179. MR0043821

[10] Benedict H. Gross, *Hanoi lectures on the arithmetic of hyperelliptic curves*, Acta Math. Vietnam. **37** (2012), no. 4, 579–588. MR3058664

[11] R. P. Langlands, *The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups*, Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), Amer. Math. Soc., Providence, R.I., 1966, pp. 143–148. MR0213362

[12] Paul Levy, *Vinberg's θ-groups in positive characteristic and Kostant-Weierstrass slices*, Transform. Groups **14** (2009), no. 2, 417–461, DOI 10.1007/s00031-009-9056-y. MR2504929

[13] Dmitri I. Panyushev, *On invariant theory of θ-groups*, J. Algebra **283** (2005), no. 2, 655–670, DOI 10.1016/j.jalgebra.2004.03.032. MR2111215

[14] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen. MR1278263

[15] Bjorn Poonen and Michael Stoll, *Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) **180** (2014), no. 3, 1137–1166, DOI 10.4007/annals.2014.180.3.7. MR3245014

[16] A. Shankar and X. Wang, *Average size of the* 2*-Selmer group of Jacobians of monic even hyperelliptic curves*, Compositio Math. (to appear).

[17] Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277, DOI 10.4064/aa98-3-4. MR1829626

[18] Jack A. Thorne, *Vinberg's representations and arithmetic invariant theory*, Algebra Number Theory **7** (2013), no. 9, 2331–2368, DOI 10.2140/ant.2013.7.2331. MR3152016

[19] Jack A. Thorne, *E_6 and the arithmetic of a family of non-hyperelliptic curves of genus 3*, Forum Math. Pi **3** (2015), e1, 41, DOI 10.1017/fmp.2014.2. MR3298319

[20] Jack A. Thorne, *A remark on the arithmetic invariant theory of hyperelliptic curves*, Math. Res. Lett. **21** (2014), no. 6, 1451–1464, DOI 10.4310/MRL.2014.v21.n6.a13. MR3335856

[21] È. B. Vinberg, *The Weyl group of a graded Lie algebra* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **40** (1976), no. 3, 488–526, 709. MR0430168

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

[23] Xiaoheng Wang, *Pencils of quadrics and Jacobians of hyperelliptic curves*, ProQuest LLC, Ann Arbor, MI, 2013. Thesis (Ph.D.)–Harvard University. MR3167287

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts