2-Selmer groups of hyperelliptic curves with two marked points

Ananth N. Shankar

October 16, 2018

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. We prove this by showing that the average rank of the 2-Selmer groups is bounded above by 6. We also prove that the average size of the \( \phi \)-Selmer groups of a family of isogenies associated to this family is exactly 2.

1 Introduction

There has been a lot of recent progress on studying the statistics of Jacobians and rational points of families of curves. In [5], Manjul Bhargava and Benedict 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, Bjorn Poonen and Michael Stoll in [15] prove 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 one as the genus goes to infinity. In [16], Arul Shankar and Xiaoheng Wang prove results analogous to [5] and [15] for the family of monic even-degree hyperelliptic curves. Jack Thorne, in [19], studies the statistics of the 2-Selmer set in a family of non-hyperelliptic 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 \( \phi \)-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 \( \text{Gal}(\overline{\mathbb{Q}}^{\text{sep}}/\mathbb{Q}) \) 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 \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) with coefficients in \( A[\phi](\overline{\mathbb{Q}}) \). The \( \phi \)-Selmer group \( \text{Sel}_\phi \) 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 recovers the classical definitions of the \( n \)-Selmer groups, by choosing the isogeny \( \phi \) to be 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 \( \infty_1 \), 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 \( C_1 \to \mathbb{P}^1, \infty_1 \) 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

\[
y^2 = x^{2m+1} + a_1 x^{2m} + \ldots + a_{2m} x + c^2 = f(x)
\]
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

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

It follows from this definition that for 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

**Theorem 1.1.** When all hyperelliptic curves of a fixed genus \( m \geq 2 \) having a marked rational Weirstrass point and a marked rational non-Weirstrass 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-Weirstrass point. The additional presence of the marked Weirstrass point \( \infty_1 \) in a curve \( C_1 \) of our family has the consequence of introducing a square-root of the class of \((1,0)\), where \( \mathbb{Q} \) is the Jacobian of \( C_1 \). Indeed, \((1,0) - (\infty_1)\) is unique. We therefore expect that despite the existence of the extra marked Weirstrass 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 1.2.

We prove that for 100% of curves in our family, the class of \((1,0) - (\infty_1)\) in \( J_1(\mathbb{Q}) \) is not divisible by 2. Therefore, the average contribution of \((1,0) - (\infty_1)\) to the \( 2 \)-rank of \( \text{Sel}_2(J_1) \) is 1. Denote the \( 2 \)-rank by \( r_1 \). The following inequality holds 100% of the time:

\[
2(r_1 - 1) \leq 2^{n-1} = \frac{\# \text{Sel}_2(J_1)}{2}.
\]

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

**Corollary 1.2.** When all hyperelliptic curves of a fixed genus \( m \geq 2 \) having a marked rational Weirstrass point and a marked rational non-Weirstrass 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 given by the equation \( y^2 = xf(x) \), and \( C \) is given 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 \( \Delta \). Therefore, the \( 2 \)-Selmer groups of \( J_1 \) and \( J_2 \) are subgroups of the same group, \( H^1(\mathbb{Q}, \Delta) \). Denote their intersection by \( \text{Sel}_{(1,2)}(f) \).

**Theorem 1.3.** The average size of \( \text{Sel}_{(1,2)}(f) \), as \( f \in \mathcal{B} \) is ordered by height, is equal to 2.

The group \( \text{Sel}_{(1,2)} \) always contains the identity of \( H^1(\mathbb{Q}, \Delta) \), and the image of \((1,0) \in J_1(\mathbb{Q})/2J_1(\mathbb{Q}) \subset H^1(\mathbb{Q}, \Delta) \). Theorem 1.3 implies that 100% of the time, \( \text{Sel}_{(1,2)} \) contains nothing else.

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

\[
0 \to \Delta \to J_1 \times J_2 \xrightarrow{\phi} J \to 0
\]

where \( J \) denotes the Jacobian of \( C \). Since the \( \phi \)-Selmer group of \( J_1 \times J_2 \to J \) equals \( \text{Sel}_{(1,2)} \), we obtain the following corollary to Theorem 1.3

**Corollary 1.4.** Let notation be as above. When \( f \in \mathcal{B} \) is ordered by height, the average size of the \( \phi \)-Selmer group is 2.
The structure of the paper follows [5]. In §2, we consider the representation $n \otimes n$ of the split semisimple group $SO_n \times SO_n$, where $n = 2m + 1$ is an odd integer. By viewing this representation in the Vinberg setting, 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

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

The functions $a_1, \ldots, a_{n-1}, e$ are invariant under the action of $SO_n \times SO_n$. In fact, these freely generate the ring of $SO_n \times SO_n$-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 [13], we demonstrate the existence of two sections $\kappa_1$ and $\kappa_2$ 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 $SO \times SO$ 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 to each $SO_n \times SO_n$-orbits on $n \otimes n$. The theory developed in [23] realises 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 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 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 1.3 is to demonstrate the existence of integral representatives (with a minor technical condition at the place 2) of locally soluble $SO_n(\mathbb{Q}) \times SO_n(\mathbb{Q})$ orbits, which have integral invariants. This is done in §6, and the result we prove is stated as Theorem 6.2.

Having parameterised the Selmer groups in terms of integral soluble and $(1,2)$-soluble orbits, we use Bhargava’s geometry of numbers techniques ([11]) 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 $SO_n(\mathbb{Z}) \times SO_n(\mathbb{Z})$ 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 work in progress of Manjul Bhargava, Arul Shankar and Xiaoheng 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 zero (Proposition 8.6), and so the only contribution to the average comes from the cusp. This proves Theorem 1.3.

In future work, we will use these results to bound the number of rational points of curves in these families.

Acknowledgements

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. Finally, I would like to thank Arul Shankar and Xiaoheng Wang for very helpful comments on previous versions of this paper.
2 A representation of $SO_n \times SO_n$

Let $k$ be a field of characteristic different from 2. In this section, we consider the action of $SO_n \times SO_n$ on $n \otimes n$.

2.1 Vinberg theory

The above representation is in the Vinberg setting. Indeed, let $(V_1, Q_1, e_1)$ be an $n$-dimensional split orthogonal space, with discriminant 1 with respect to the basis $e_1$ of $\Lambda^{top}(V_1)$, and $(V_2, Q_2, e_2)$ be an $n$-dimensional split orthogonal space of discriminant $(-1)^n$ (the discriminant is again relative to $e_2 \in \Lambda^{top}(V_2)$). Consider the $2n-$dimensional split orthogonal space $V = V_1 \oplus V_2$, $Q = Q_1 \oplus Q_2$, and the special orthogonal group $G = SO(V)$ (the discriminant condition on $(V_2, Q_2)$ is imposed so that the space $(V, Q)$ is split).

We consider the involution $\theta$ of $SO(V)$, given by conjugation by the element $(I_n, -I_n) \in GL(V_1) \times GL(V_2)$. Let $G^{\theta}$ be the subgroup fixed by $\theta$. It is the intersection of $O(V_1) \times O(V_2)$ with $SL(V)$, inside $GL(V)$. The involution $\theta$ 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 $G^{\theta}$ on $\mathfrak{g}$ preserves the eigenspace $\mathfrak{g}_1$. As representations of $G^{\theta}$, $\mathfrak{g}_1 \cong V_1 \otimes V_2$.

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 also 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 diagonals zero.

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

The $G$-invariant functions on $\mathfrak{g}$ restrict to $G^{\theta}$-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 zero. Suppose that the characteristic polynomial of $T'$ is $g_1(x) = f_1(x^2) = x^{2n} + b_1x^{2n-2} + \ldots + b_{n-1}x^2 + b_n$. Because $T'$ is skew self-adjoint, $b_n = (-1)^ne^2$, 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 $G^{\theta}$-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 $g(x) = f(x^2) = x^{2n} + a_1x^{2n-2} + \ldots + a_{n-1}x^2 + a_n$ with $a_i = (-1)^ib_i$. 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 zero. For notational reasons, we will use the symbol $\alpha$ 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 $\alpha$ as a self-adjoint operator on $V$.

We call $g$ the characteristic polynomial of $\alpha$.

The invariants $a_i, e$ are homogenous 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 $\text{Inv} = \text{Spec} \{a_1, a_2, \ldots, a_{n-1}, e\}$. If the characteristic of $k$ is 0, then $\text{Inv} \cong V_1 \otimes V_2 / G^{\theta}$, the GIT quotient of $V_1 \otimes V_2$ by $G^{\theta}$. Even if $k$ has positive characteristic, there is still a $G^{\theta}$-equivariant map from $V_1 \otimes V_2$ to $\text{Inv}$, where the action of $G^{\theta}$ on $\text{Inv}$ is trivial. In either case, $\pi : V_1 \otimes V_2 \to \text{Inv}$ denote the $G^{\theta}$-equivariant map.

Definition 1. 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 zero.

Note that $\alpha$ will be regular semisimple if and only if the polynomial $f$ has non-zero discriminant and $f(0) \neq 0$. In terms of the map $\pi$, the regular semisimple locus in $V_1 \otimes V_2$ equals $\pi^{-1}(\text{Inv}^{ns})$, where $\text{Inv}^{ns}$ is the locus where $e$ and the discriminant of $f$ are both non-zero.
Henceforth, we assume that $n$ is an odd integer. Let $n = 2m + 1$.

**Regular nilpotent orbits and Kostant sections**

For this paragraph, we assume that the characteristic of $k$ is zero. We also think of $V_1 \otimes V_2$ as being $\mathfrak{g}_1$, i.e. as skew self-adjoint operators with block diagonal zero.

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

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

By [18, Lemma 2.13], $G^\theta_{ad}(k)$ 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

$$B = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 1 \end{bmatrix}.$$  \hspace{1cm} (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:

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

Let $E_2$ be defined the same way, except with the $f_i$ and $f'_i$ swapped. Both $E_1$ and $E_2$ are regular nilpotent elements of $V_1 \otimes V_2$ (thought of as symmetric operators with block diagonal zero). It is easy to see that $E_1$ and $E_2$ are in the same $G^\theta_{ad}(k)$ orbit, but are 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 $\kappa'_i : E_i + \mathfrak{z}(F_i) \to \text{Inv}$ (for $i = 1, 2$) are isomorphisms, and thus give rise to two sections $\kappa_i : \text{Inv} \to \mathfrak{g}_1$.

**Definition 2.** The sections $\kappa_i$ 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 $T'^2X \subset X^\perp$ ($^\perp$ 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 the $\langle f_i \rangle$ and $\langle f'_i \rangle$ will be weight-spaces for $H_1$. Hence, we have that $F_1$ acts as follows:

$$\langle f_1 \rangle \leftarrow \langle f'_1 \rangle \leftarrow \langle f_2 \rangle, \quad \ldots \quad \langle f'_{m-1} \rangle \leftarrow \langle f_m \rangle, \quad \langle f_m \rangle \leftarrow \langle f'_{m+1} \rangle, \quad \ldots \quad \langle f'_{2m+1} \rangle \leftarrow \langle f_{2m+1} \rangle;$$
Thus, any such that \( T_i \) element that it has index 2 in \( G \). Let \( G \) the same \( H \). Recall that we have assumed that 3. Orbits over a separably closed field \( V \) with \( W \). 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 \( T^2 X \subset X^\perp \) (\( \perp \) is taken with respect to \( Q_i \)).

\[ \langle f_1, f'_m \rangle \to 0. \]

The kernel of \( F^m_1 \) is \( \langle f_1, \ldots f_m, f'_1 \ldots f'_{m+1} \rangle \), and the kernel of \( F^{m+1}_1 \) is \( \langle f_1, \ldots f_{m+1}, f'_1 \ldots f'_{m+1} \rangle \). Thus, any \( Z \in \mathfrak{g}(F_1) \) 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 \( V \).

Recall that we associated a self-adjoint operator \( T \) to each \( T' \in \mathfrak{g}_1 \), and that \( T \) and \( T' \) satisfy the relation \( T^2 = -T'^2 \). Therefore, if \( \alpha \in \kappa_\alpha(\text{Inv}) \), the corresponding (self-adjoint) \( T \) satisfies the conclusions of Proposition 2.2. To that end, for \( k \) having characteristic different from two, we make the following definition.

**Definition 3.** 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 \( T^2 X \subset X^\perp \) (\( \perp \) is taken with respect to \( Q_i \)).

### 2.2 \( G_0^\theta \) from \( G^\theta \)

Let \( G_0^\theta = \text{SO}(V_1) \times \text{SO}(V_2) \) be the connected component of \( G^\theta \) containing the identity. Note that it has index 2 in \( G^\theta \). As \( n \) is odd, \( -I_n \in \text{GL}(V) \) is an element of \( G^\theta \), but not of \( G_0^\theta \). The element \( -I_n \) acts trivially on \( V_1 \otimes V_2 \), and 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 \( \text{SO}(V_i) \) for \( i = 1, 2 \). For ease of notation, let \( H = G_1 \times G_2 \).

Recall that we have identified \( W \), the space of self-adjoint operators with block diagonal zero, with \( V_1 \otimes V_2 \) as \( H \) representations. 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 zero. Suppose that \( S \) and \( T \) have the same invariants. Then, there exists \( g \in H(k) \) such that \( gSg^{-1} = T \).

**Proof.** Suppose that the common characteristic polynomial is \( g(x) = f(x^2) \). If \( \lambda \) is an eigenvalue, then so is \(-\lambda \). Let \( w \pm_1, w \pm_2, \ldots, w \pm_n, \) and \( w' \pm_1, w' \pm_2, \ldots, w' \pm_n \) be the eigenvectors of \( S \) and \( T \) respectively, with eigenvalues \( \pm \lambda_1, \ldots, \pm \lambda_n \). 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 the \( w_i \) (and the \( w'_i \)) form a basis orthogonal for the form on \( V_i \), 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 \( w'_i \)) 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 that \( (w_i + w_{-i}, w_i - w_{-i}) = 0 \) where \( (, ) \) is the bilinear form associated with \( Q \), whence \( Q(w_i) = Q(w_{-i}) \). Clearly, the same happens with the \( w' \pm_i \). By scaling \( w' \pm_i \) appropriately, we may assume that \( Q(w \pm_i) = Q(w' \pm_i) \).
Therefore, the transformation $g$ taking the $w_{\pm i}$ to the $w'_{\pm i}$ 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 $O(V_1) \times O(V_2)$. Conjugating by $g$ multiplies the pfaffian by the determinant of $g$. The fact that the two operators $S$ and $T$ have the same pfaffian forces $g$ to lie in $SL(V)$, 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 the above proposition.

**Corollary 3.2.** For $k$ a separably closed field, two regular semisimple elements $\alpha_1$ and $\alpha_2$ 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 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 $c = (a_1, a_2, a_3, \ldots, a_{n-1}, e) \in Inv^n(k)$. Recall that we have associated to $c$, two polynomials $f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + e^2$, and $g(x) = f(x^2)$. The existence of the Kostant sections prove that when the characteristic of $k$ is zero, the set of $k$-rational orbits with invariants $c$ is non-empty, 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 characteristic different from two.

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 $\sigma$ be the non-trivial automorphism of $M$ which leaves $L$ fixed. Let $\beta$ and $\gamma$ be the images of $x$ in $M$ and $L$ respectively. By definition, $\beta = \gamma^2$ and $\sigma$ sends $\beta$ to $-\beta$.

Define a symmetric bilinear form $(\ , \ )$ on $M$ by setting

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

For $\mu \in L$, we have that $\text{Trace}_{M/k} \beta \mu = 0$. Therefore $(\ , \ )$ breaks up into a direct sum of split bilinear forms on $L$ and $L\beta$. An easy computation shows that these spaces have discriminants 1 and $(-1)^n = (-1)$ respectively. Isometrically identifying $L$ and $L\beta$ with $V_1$ and $V_2$ respectively, the self-adjoint operator $T_\beta$ on $M$ (given by multiplication by $\beta$) 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 $\beta$ by $-\beta$.

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

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

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

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

7
Corollary 4.2. We have $\Delta_c(k) \neq \{1\}$ precisely when the polynomial $f$ is not irreducible.

Proof. The etale 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 $\Delta_c$) with $\text{GL}(V_1) \times \{1\}$, and with $\{1\} \times \text{GL}(V_2)$ is just the identity. This implies that either projection restricted to $L^\times$ (and therefore to $\Delta_c$) is an isomorphism onto its image.

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

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

We claim that the two maps are the same. Indeed, $S$ and $T$ are $k$-rational, so that $\sigma(g)T = gT$, thereby forcing $g^{-1}\sigma(g) \in \Delta_c$. Therefore, the two maps differ by conjugation by an element of $\Delta_c$. That $\Delta_c$ 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 $c \in \text{Inv}^v(k)$. 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 $g = (g_1, g_2) \in \text{SO}(V_1) \times \text{SO}(V_2)(k)$ be an element in the stabilizer. Then $g_1$, thought of as an element of $\text{SO}(V_1)$ commutes with the self adjoint operator $T^2$ restricted to $V_1$ and also preserves the subspace $X$. By [5], $g_1 = I_n$. As remarked above, this forces $g_2 = I_n$, as required. Because this stabilizer is trivial, an easy descent argument shows that it suffices to prove the statement over $k^{\text{sep}}$.

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 6], there exists $g_1 \in \text{SO}(V_1)$ which commutes with $T^2$, such that $g_1X' = X$. It suffices to demonstrate the existence of $g_2 \in \text{SO}(V_2)$ such that $g = (g_1, g_2) \in \Delta_c$. By [5], the centralizer of $g_1$ of $T^2$ in $\text{SO}(V_1)$ is an abelian 2-group of order $2^{n-1}$, which is the same as the order of $\Delta_c$. Therefore, the projection map (having trivial kernel) from $\Delta_c$ to $\Delta_{V_1}$ 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 $\alpha_2$ 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 $c \in \text{Inv}^v(k)$. Let $W_c$ denote the fiber of $\pi$ over $c$. Proposition 3.2 can be rephrased as stating that $H(k^{\text{sep}})$ acts transitively on $W_c(k^{\text{sep}})$. 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 $\delta : H^1(k, \Delta_c) \rightarrow H^1(k, H)$ (the notation used in [4] is $\gamma$, not $\delta$). We use $\alpha_1(v)$ (the 1-distinguished orbit) as our fixed orbit, and explicitly describe the map $\delta$.

The Kummer exact sequence gives that $H^1(k, \Delta_c) = (L^\times/L^\times)^{2N-1}$. To an element $\nu$ in $L^\times_{N=1}$, we associate the orthogonal space $M$ with the bilinear form $\langle , \rangle_\nu$, with $\langle \lambda, \mu \rangle_\nu = \lambda(\nu) \cdot \mu(\nu)$.
Suppose that \(5.1\) Pencils of quadrics

Proposition 5.1.

The point of \(H\) and are conjugate for the hyperelliptic involution on \(\nu\). Therefore, for \(\delta\) associated self-adjoint matrix with block diagonal zero. Define \(\chi\).

We recall the theory developed in \([23]\), (also see \([4]\), \([22]\)) which describes these maps.

Fix \(\alpha\) and \(V\) in \(H\). In fact, the orbit of \(\alpha\) for \(V\) is two-distinguished. Summarizing, we have the

\[\text{Proposition 4.5.}\quad \text{For each } c \in \text{Inv}^\ast(k), \text{the } H(k)\text{-orbit of } \alpha_1(v) \in W(k) \text{ is } 1\text{-distinguished.}
\]

The stabilizer of \(\alpha_1, \Delta_c\) is isomorphic to \(\text{Res}_{L/k}(\mu_2)^N=1\). All the other \(k\)-rational orbits with the same invariants have the same stabilizer, lie in the \(H(k^{sep})\text{-orbit of } \alpha_1\) and correspond bijectively to the non-identity 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 \(T_{\beta}\) and the bilinear form \((\ , \ )_{\nu}\). The class of \((-\gamma)\) is the 2-distinguished orbit, corresponding to the \(H(k)\) orbit of \(\alpha_2\).

An immediate corollary is

\[\text{Corollary 4.6.}\quad \text{Fix } c \in \text{Inv}^\ast(k). \text{ The two distinguished orbits lie in the same } H(k)\text{-orbit if and only if } (-\gamma) \text{ is a perfect square in } L^\times.\]

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 \(c \in \text{Inv}^\ast(k),\) we associate the curves \(C_{1,c}, C_{2,c}\) given by \(y^2 = f(x)\) and \(y^2 = xf(x)\). As usual, \(f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + e^2,\) 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 \(\infty_1,\) 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, \(\infty_2, \infty_2',\) which are conjugate for the hyperelliptic involution on \(C_{2,c}.\) Let \(J_{1,c}\) be the Jacobians of \(C_{1,c}.\) Note that \(J_{1,c}[2] \cong J_{2,c}[2] \cong \text{Res}_{L/k}(\mu_2)^N=1.\)

5.1 Pencils of quadrics

Suppose that \(\alpha \in W^r_c(k),\) i.e. has invariants \(c.\) The 2-torsions of \(J_{1,c}\) and \(J_{2,c}\) are related to the stabilizer of \(\alpha\) as follows:

\[\text{Proposition 5.1.}\quad \text{The stabilizer } \Delta_c \text{ is isomorphic (as group schemes over } k) \text{ to } J_{1,c}[2].\]

Recall that \(H(k)\)-orbit of \(\alpha_1(c)\) is 1-distinguished, and that the map \(\delta\) (based at the orbit of \(\alpha_1\)) 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 \(\Delta_c\) 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 zero. 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 \(V_1.\)
Proposition 5.3. The image of both $J$-elements gives us rational orbits.

The same construction with the order of $Q_1$ and $Q_{1,T^2}$ reversed gives a pencil of quadrics $P_2^\alpha$. The associated Fano variety $F_2^\alpha$ gives a torsor of the Jacobian of the curve $y^2 = x^n + \frac{a_0}{2x^2} + \frac{a_1}{x} + \ldots + \frac{a_n}{x^{n-1}} + \frac{1}{x^2}$. But this curve is isomorphic to $C_2$ via the isomorphism $(x, y) \mapsto \left(1/x, ey/x^{n-1}\right)$. Again, $P_2^\alpha$ is the image of $\nu$ in $H^1(k, J_2)$, where $\Delta_c$ is identified with $J_{2,c}$.

For $i = 1, 2$, $\delta(\alpha)$ will be in the image of $J_{i,c}/2J_{i,c}$ precisely when $F_2^\alpha$ has a $k$-rational point. Also, changing only the sign of the pfaffian but leaving the other invariants fixed doesn’t change $P_1^\alpha$ or $P_2^\alpha$. This is because, changing the pfaffian is the same as replacing $T$ by $-T$, and this doesn’t change $T^2$. Therefore the 2-cover that we get stay the same. We will ignore the sign of the pfaffian while associating pencils to rational orbits.

5.2 Soluble orbits

Any element of $J_{1,c}(k)$ can be mapped to $H^1(J_{1,c}[2])$, 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, it is easy to see that $(-\gamma)$, the class of the 2-distinguished orbit, is the image of $P_1 - \infty \in J_{1,c}(k)$, and also the image of $P_2 - \infty \in J_{2,c}(k)$.

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 rational points in either Jacobian give us rational orbits.

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

Proof. The element $\delta(\nu) \in H^1(G_1 \times G_2)$ corresponds to the quadratic spaces isomorphic to $L$ with forms $(\ , \ )_\nu$ and $(\ , \ )_{-\nu\gamma}$. The element $\delta(\nu)$ is trivial precisely when $(\ , \ )_\nu$ and $(\ , \ )_{-\nu\gamma}$ are both split.

By [4] Proposition 6] (see [20] Theorem 4.6] for proof which doesn’t 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 $\nu$ lies in the subgroup $J_{1,c}(k)/2J_{1,c}(k)$.

Exactly the same argument works if $\nu$ is in the image of $J_{2,c}/2J_{2,c}$ - notice that $C_{2,c}$ is isomorphic to the curve given by the Weirstrass equation $y^2 = x^n + \frac{a_0}{2x^2} + \frac{a_1}{x} + \ldots + \frac{a_n}{x^{n-1}} + \frac{1}{x^2}$, and we apply the same result of [4] (or [20]) and Proposition 5.2 to finish the proof of the result.

Definition 4. Suppose that an orbit under $H(k)$ corresponds to an $\nu \in H^1(\Delta_c)$ 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 $\alpha$ is $i$-soluble if the corresponding Fano variety $F^i_\alpha$ has a $k$--rational point. The distinguished orbits are $i$-soluble for both $i = 1$ and $2$.

We will not work with $2$-soluble orbits, and 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 $c \in \text{Inv}^{rs}(k)$. Define $\text{Sel}_{(1,2)}(c)$ to be the intersection of the $\text{Sel}_2(J_{i,c})$ (for $i = 1, 2$) in $H^1(k, \Delta_c)$.

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

**Proposition 6.1.** Let $\nu \in \text{Sel}_2(J_{i,c})$ 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 $\nu \in \text{Sel}_2(J_{i,c})$, Proposition 6.3 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 $1$-soluble (or locally $(1,2)$-soluble) if $\alpha \in W(k_v)$ is soluble for every place $v$ 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 matrices are $\pm B$, with $B$ as in Equation (1).

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

**Definition 5.** Let $\pi : W \to \text{Inv}$ be the map described in §2.

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

Notice that there is a reduction map from $\text{Inv}(\mathbb{Z})$ to $\text{Inv}(\mathbb{F}_p)$ for $p > 2$. An element of $\text{Inv}^{rs}(\mathbb{Z})$ maps to an element of $\text{Inv}^{rs}(\mathbb{F}_p)$ exactly when $p$ doesn’t divide the discriminant of $g(x)$, i.e. $p$ doesn’t divide $c$ and $p$ doesn’t 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 $c = (a_1, \ldots, a_{n-1}, e) \in \text{Inv}^{rs}(\mathbb{Z})$, such that $2^k|a_i$, and $2^n|e$. 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:

**Theorem 6.3.** Let $c = (a_1, \ldots, a_{n-1}, e) \in \text{Inv}^{rs}(\mathbb{Z}_p)$, 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 \( c = (a_1, \ldots, a_{n-1}, e) \in \text{Inv}^\nu(\mathbb{Z}_2) \), such that \( 2^{|e|} |a_i| \) and \( 2^{|e|} |c| \). 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 6.3. 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 \( H^1(k, H) \) is trivial. Therefore, for \( c \in \text{Inv}^\nu(\mathbb{F}_q) \), 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 zero. 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 \( c \in \text{Inv}^\nu(\mathbb{Q}_p) \). 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 \( b_p = \frac{J(Q_p)/2J(Q_p)}{J(\mathbb{Q}_p)} \) 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 15] Let \( I \) be a \( \mathbb{Z}_p \)-module of rank \( n \) equipped with a symmetric binary 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 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 \( \alpha \) 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 etale \( \mathbb{Q}_p \)-algebra \( \mathbb{Q}_p[x]/(f(x^2)) \) as defined in [4]). Since \( T \) is integral, the lattice \( D_1 \oplus D_2 \) is realised 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 \( T^2 \) stabilizes each of the \( D_i \) forces the fractional ideal \( J \) to be of the form \( J = I_1 + \beta I_2 \), \( I_1 \) and \( I_2 \) being fractional ideals of the ring \( \mathbb{Z}_p[x]/(f(x)) \). Here, we identify \( I_1 \) with \( D_1 \). 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 \( \nu \in L^\nu_{N=1} \). The conditions that the lattices \( D_i \) are self dual translate to \( \nu I_1^2 \subset \mathbb{Z}_p[x]/(f(x)) \), and \( N(I_1)^2 = N(\nu)^{-1}, \nu_1 I_2^2 \subset \mathbb{Z}_p[x]/(f(x)) \), 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 \( f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_0 = e \neq 0 \), 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 \( a_1, e \) correspond to equivalence classes of triples \( (I_1, I_2, \nu) \). Further, \( \nu \in L^\lambda \), and the \( I_i \) are fractional ideals for the order \( R = \mathbb{Z}[x]/(f(x)) \) satisfying \( I_1 \subset I_2 \subset \gamma^{-1} I_1 \). The element \( \nu \) has the properties that the bilinear forms \( ( , )_\nu \) is \( ( , )_{\nu^2} \) are split forms over \( \mathbb{Q}_p \), that \( \nu I_1^2 \subset \mathbb{Z}_p[x]/(f(x)) \), \( \nu_1 I_2^2 \subset \mathbb{Z}_p[x]/(f(x)) \), and that \( N(I_1)^2 = N(\nu)^{-1}, N(I_2)^2 = N(-\gamma \nu)^{-1} \). The triple \( (I_1, I_2, \nu) \) is equivalent to \( (I_1', I_2', \nu') \) if \( I_1 = \lambda I_1' \) and \( \nu' = \lambda^2 \nu \), for some \( \lambda \in L^\lambda \). The integral orbit corresponding to the triple \( (I_1, I_2, \nu) \) maps to the rational orbit of \( H(\mathbb{Q}_p) \) on \( W(\mathbb{Q}_p) \) corresponding to the class of \( \nu \) in \( (L^\lambda/L^\lambda)^{N=1} \).

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 the maximal order, we see that the integral orbits are in bijection with $(R^\times/R^\times)^{N=1}$. This is always true when $p$ does not divide $\text{Disc}(f(x))$ (equivalently, when $J_1$ has good reduction). 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 18] applies verbatim. \qed

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 $\nu \in (L^\times/L_2^\times)^{N=1}$ corresponds to a 1-soluble $H(\mathbb{Q}_p)$-orbit. As both $\nu$ and $-\nu\gamma$ are 1-soluble, by [5, Proposition 19], there exist ideals $I_1$ and $I_2$ which satisfy all the properties of the previous proposition, except perhaps for the conditions $f_1 \subset I_2 \subset \gamma^{-1}I_1$. 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 $\gamma$. Clearly, any lattice $\Lambda$, with $I_1 \subset \Lambda \subset \gamma^{-1}I_1$ is stable under multiplication by $\gamma$, and hence must be a fractional ideal. Therefore, we just need to find a $\Lambda$ satisfying the above inclusion relations, and which is self dual for the bilinear form $(\cdot, \cdot)_{\nu\gamma}$.

Note that by choice $I_1$ is self dual for the bilinear form $(\cdot, \cdot)_\nu$, therefore $I_1$ and $\gamma^{-1}I_1$ are dual to each other for the form $(\cdot, \cdot)_{\nu\gamma}$. By a result of Cassels [3, Lemma 3.4], there exists a $\mathbb{Z}_p$ basis $(f_i)$ of $I_1$ such that the Gram matrix for $(\cdot, \cdot)_{\nu\gamma}$ is

$$
\begin{pmatrix}
    u_1p^{b_1} & u_2p^{b_2} & \cdots & u_np^{b_n}
\end{pmatrix}
$$

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 $\Lambda$ spanned by $f_i$ is still sandwiched between $I_1$ and $\gamma^{-1}I_1$. Suppose that $\Lambda = \Lambda_0 \oplus \Lambda_1$, where $\Lambda_j$ 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 $\Lambda_1$ is forced to be even (hence, the dimension of $\Lambda_0$ is odd). Let the dimension of $\Lambda_1$ be $2n$. Without any loss of generality, assume that $\Lambda_1$ is spanned by $f_1, \ldots, f_{2n}$.

In particular, $\Lambda_0$ is a quadratic space of odd dimension, with the form being non-degenerate 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 $f_1, \ldots, f_{2n}$ of $\Lambda_1$, we may assume that the Gram matrix of $\Lambda_1$ restricted to $\Lambda_1$ is $B$.

By replacing $\Lambda_1$ by the span of $f_1, \ldots, f_{2n}$, 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 to show that $\Lambda_1$ 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 $\Lambda_1$, 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 $A_1$ equals $(-1)^{m} \prod_{i=1}^{2a} u_i$ modulo squares. By definition, $u_i$ modulo squares in $\mathbb{Z}_p^\times$ equals $\left( \frac{u_i}{p} \right)$ (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 $A_1$ to be 1, thereby proving the theorem.

\[ \blacksquare \]

6.3 The 2-adics

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

**Proposition 6.10.** Let $J$ be the Jacobian of a genus $g$ hyperelliptic curve. Then the quantity $2^g = b_2 = \frac{J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)}{J[2](\mathbb{Q}_2)}$ depends only on $g$, and not on $J$.

We now prove Proposition 6.10. As in the proof of Theorem 6.3, we will use the existence of the ideal $I_1$, as proved in [5], and 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 $I_1$, if we were guaranteed the existence of $I_1$).

**Proof of Proposition 6.10.** Suppose that $\alpha \in (L^\times/L^\times)^{N=1}$ corresponds to a 1-soluble $\mathbb{Q}_2$ orbit. The first part of the proof proceeds along exactly the same lines - we will still use [5] for the existence of $I_1$. We still have $I_1$ is self dual for the bilinear form $B_1 = (\ , \ )_\alpha$, and therefore $I_1$ and $\gamma I_1$ 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’ result is in terms of the quadratic form associated to $B_2$ - translating this in terms of the bilinear form $B_2$ we have

$$B_2(f_i, f_j) = \begin{pmatrix} 2^{b_1}Q'_1 & 2^{b_2}Q'_2 & \cdots & 2^{b_{k'}}Q'_{k'} \\ \vdots & \vdots & \ddots & \vdots \\ 2^{b_1}Q'_1 & 2^{b_2}Q'_2 & \cdots & 2^{b_{k'}}Q'_{k'} \end{pmatrix}$$

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

$$Q'_i = H = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},$$

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 the $b_i$ are either 0 or 1. In fact, we may assume that $b_i = 0$ if $Q'_i = H$ or $H_0$. Indeed, if a 2-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

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

where $U_1$ is a diagonal matrix of size $2a \times 2a$ consisting solely of units, and the $Q_i$ are either $1 \times 1$ or $2 \times 2$ matrices with 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 6.11 below.

**Lemma 6.11.** 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 $\Lambda'$ spanned by $(f_1 + f_2)/2$ and $(f_1 - f_2)/2$ has the required properties. $\square$

### 6.4 Archimedean fields

#### The complex numbers

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

#### The real numbers

We have the archimedean version of Propositions 6.5 and 6.10 (again, see [17]):

**Proposition 6.12.** Let $J$ be the Jacobian of a genus $g$ hyperelliptic curve. Then the quantity $2^{-g} = b_\infty = \frac{J(\mathbb{R})/2J(\mathbb{R})}{J(\mathbb{R})/2J(\mathbb{R})}$ depends only on $g$, and not on $J$.

Let $c \in \text{Inv}^{rs}(\mathbb{R})$, and let $f_c$ denote the corresponding polynomial. Define $\text{Inv}^{rs}(\mathbb{R})^{(a,b)}$ to be the set of $c \in \text{Inv}^{rs}(\mathbb{R})$ such that $f_c$ has $a$ pairs of complex conjugate roots, $b$ positive real roots, and $n - 2a + b$ negative real roots. The stabilizer $\Delta_c$ (as a group scheme over $\mathbb{R}$) depends only on the $(a, b)$ such that $c \in \text{Inv}^{rs}(\mathbb{R})^{(a,b)}$. 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 \( b_v \) 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 \( \text{SO}_n \) have class number 1. Therefore, \( H = \text{SO}(V_1) \times \text{SO}(V_2) \) also has class number one. The same proof as in [6] applies. \( \square \)

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]. Towards that end, we first define a height function on \( W(\mathbb{R}) \). Recall that \( \text{Inv} \) is the categorical quotient of \( W \) by \( H \), i.e. functions on \( \text{Inv} \) are \( H \) invariant functions on \( W \). The scheme \( \text{Inv} \) is defined over \( \mathbb{Z} \), and equals \( \text{Spec}(\mathbb{Z}[a_1, \ldots, a_n, e]) \). A point \( c = (a_1, \ldots, a_n, e) \) corresponds to the polynomial \( f(x) = x^n + a_1 x^{n-1} + \ldots + a_n x + e^2 \). We define a height function on \( \text{Inv}(\mathbb{R}) \) as follows:

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

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

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

7.1 Fundamental domains

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

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

\[
W(\mathbb{R})_{\text{sol}} = \bigcup_{(a, b)} W(\mathbb{R})_{\text{sol}}^{(a, b)}.
\]

Here \( W(\mathbb{R})_{\text{sol}}^{(a, b)} \) consists of \( T \in W(\mathbb{R})_{\text{sol}} \) such that \( \pi(T) \in \text{Inv}(\mathbb{R})^{(a, b)} \). Recall that the stabilizer of \( T \in W(\mathbb{R})^{(a, b)}_{\text{sol}} \) is independent of \( T \). We have defined this group to be \( \Delta^{(a, b)} \), and its size to be \( g^{(a, b)} \).

Similarly, let \( W(\mathbb{Z})^{(a, b)} = W(\mathbb{Z}) \cap W(\mathbb{R})_{\text{sol}}^{(a, b)} \) (we have supressed the subscript \( \text{sol} \)). If we are working in the case where \( \text{sol} \) means 1-soluble, then we will acknowledge this with the notation \( W(\mathbb{Z})_{1}^{(a, b)} \). Similarly, if \( \text{sol} \) stands for (1,2)-soluble, we will use the notation \( W(\mathbb{Z})_{(1,2)}^{(a, b)} \).

**Fundamental sets for the action of** \( H(\mathbb{R}) \) **on** \( W(\mathbb{R})_{\text{sol}} \)

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

\[
D_{sol}^{(a,b)} = \mathbb{R}_{>0} \{ T \in D_{sol}^{(a,b)} : \text{ht}(T) = 1 \}.
\]

Notice that the size of the entries of any Borel in \( \mathbb{R} \).

A fundamental domain for the action of \( H(\mathbb{Z}) \) on \( H(R) \)

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

The set \( F \) may be expressed in the form \( F_1 \times F_2 \), where \( F_i \) is the fundamental domain for the action of \( \text{SO}(V_i)(\mathbb{Z}) \) on \( \text{SO}(V_i)(\mathbb{R}) \), \( i \in \{1,2\} \). \( F_1 \) may be expressed as

\[
F_1 = \{ ur^t \theta : u \in N_1'(r'), r' \in R', \theta \in K_1 \}
\]

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

\[
\begin{bmatrix}
    r'_{-1} & & \\
    & \ddots & \\
    & & r'_{m-1} \\
    & & & 1 \\
    & & & & r'_{m} \\
    & & & & & \ddots \\
    & & & & & & r'_{1}
\end{bmatrix}
\]

constrained by the relations \( r'_1/r'_2 > c, \ldots, r'_{m-1}/r'_m > c, r'_{m} > c \); and \( K_1 \) a maximal compact of \( \text{SO}(V_1)(\mathbb{R}) \). We will parameterize \( R' \) differently. Indeed, for \( i = 1, \ldots, m \) let \( r_i = r'_1 \ldots r'_i \). Then \( r = (r_1, \ldots, r_m) \) belongs to \( R' \) exactly when \( r_i > c \). We define \( F_2 \) similarly, and we denote by \( S \) the diagonal torus, and by \( s_i \), the analogous coordinates. Let \( N'(r) \) denote the product of \( N'_1(r) \times N'_2(s) \), and let \( K \) denote the maximal compact subgroup of \( H(R) \) given by the products of the \( K_i \). We fix a Haar measure \( dh \) on \( H(R) \) by setting

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

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 \( d^x t = d^x r d^x s = \frac{dr}{r} \frac{ds}{s} \) is a Haar measure on \( R \times S \).

A fundamental domain for the action of \( H(\mathbb{Z}) \) on \( W(R)^{sol} \)

For \( h \in H(R) \), we regard \( Fh \cdot D^{(a,b)}(X) \) as a multiset, where the multiplicity of \( T \in Fh \cdot D^{(a,b)}(X) \) is given by \( \frac{\#(h' \in F : T \in h' h \cdot D^{(a,b)}(X))}{\Delta_T(R)} \). The \( H(\mathbb{Z}) \) orbit of \( T \) is counted with multiplicity \( \frac{\Delta_T(R)}{\#(\Delta_T(R) \cap H(\mathbb{Z}))} \). Let \( \Delta_T(\mathbb{Z}) \) denote the denominator in the previous expression.
The same argument as in \cite{16} §4.2 applies to conclude that \((\Delta_T(\mathbb{R}) \cap H(\mathbb{Z}))\) is non-trivial only for a measure-zero set of \(W(\mathbb{R})\). Recall that the group scheme \(\Delta_T\) 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 6.** An element \(\alpha \in W(\mathbb{Q})\) is called irreducible if \(\pi(\alpha) \in \text{Inv}^{\text{rs}}(\mathbb{Q})\) and if \(\alpha\) is not distinguished.

For a \(H(\mathbb{Z})\)-invariant set \(S \subseteq W(\mathbb{Z})^{(a,b)}\), 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.**

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

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

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

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:

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

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 \cite{6} Theorem 2.5 (Bhargava’s averaging technique), we obtain

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

We now state a result of Davenport \cite{9} which we will use extensively in what follows.

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

\[
\text{Vol}(A) + O(\max \{ \text{Vol}(\overline{A}), 1 \})
\]

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

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 \(\# \{ \mathcal{F}h \mathcal{D}(X) \cap S^{\text{red}} \}\) over the main body is \(o(X^{n^2})\) (Proposition 7.12), and that the integral of \(\# \{ \mathcal{F}h \mathcal{D}(X) \cap S^{\text{irr}} \}\) over the cuspidal region is \(o(X^{n^2})\) (Proposition 7.3). 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 matrices $\pm B$ (Equation (1) in §2).

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

$$T = \begin{bmatrix} 0 & A \\ A^* & 0 \end{bmatrix}$$

where $A$ is some $n \times n$ matrix, and $A^* = (-BAB^{-1})^t$ (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:

$$\begin{bmatrix} \alpha_{m-m} & \alpha_{m-1-m} & \cdots & \alpha_{m-m} \\ \alpha_{m-1-m} & \alpha_{m-1-1-m} & \cdots & \alpha_{m-1-m} \\ \vdots & \ddots & \vdots \\ \alpha_{m-m} & \alpha_{m-1-m} & \cdots & \alpha_{m-m} \end{bmatrix}$$

The $a_{ij}$ are scaled by the action of the torus $R \times S$. Define $w_{ij}$ to be the weight according to which $R \times S$ scales $a_{ij}$. For instance, if $i$ and $j$ are positive, $w_{ij} = r_1^{i'} \cdots r_s^{i'} s_1^{j'} \cdots s_s^{j'}$, 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 $i' \leq i$ and $j' \leq j$. Further, $a_{ij} \preceq a_{i'j'}$ precisely when $w_{ij}^{r_s \cdots r_1}$ consists of non-positive 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 zero, then the corresponding $T$ has discriminant zero.

**Proof.** If such a block is identically zero, then the determinant of $A$ is zero. Therefore, the operator $T$ has the eigenvalue 0 with multiplicity two, rendering it impossible for $T$ to be regular semisimple. \hfill $\square$

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

$$T^2 = \begin{bmatrix} AA^* & 0 \\ 0 & A^*A \end{bmatrix}$$

If the top-right $m \times (m + 1)$ block of $A$ is identically zero, then an easy computation shows that the top-right $m \times m$ block of $AA^*$ will also be zero. Consequently, the isotropic space $X$ spanned by the last $m$ basis vectors of $V_1$ has the property that $T^2X \subset X^\perp$, and 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. \hfill $\square$

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

**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 zero, 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

$$Y = \begin{bmatrix} Y_{11} & 0 & 0 \\ * & Y_{22} & 0 \\ * & * & Y_{33} \end{bmatrix}$$

where $Y_{11}$ and $Y_{33}$ are of size $i \times i$ and $Y_{22}$ is of 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 $V$. 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 $P_Y = P_{Y_{11}} P_{Y_{33}}^2$, and so $AA^* = Y$ must have repeated eigenvalues, as claimed. Therefore, $T$ has discriminant zero 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 $hA_0 D^{(a,b)}(X)$ lies fully in in the cusp. Clearly, an integral element will lie in the cusp only if $a_{mm} = 0$. We have:

**Proposition 7.6.**

$$\int_{h \in \mathcal{F}} \# \{ hA_0 D^{(a,b)}(X) \cap W(\mathbb{Z})_{a_{mm}=0} \} \, dh = o(X^{1/2})$$

**Proof.** To lighten 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 [10] Proposition 4.5], shows that it suffices to prove

$$\int_{t \in R \times S} \# \{ tA_0 D(X) \cap W(\mathbb{Z})_{a_{mm}=0} \} \delta(t) \, d^\times t = o(X^{3/2})$$

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

Let $U$ denote a subset of the coordinates $a_{ij}$, with the property that if $a_{ij,j'} \in U$ then $U$ also contains $a_{ij}$ with $a_{ij} \leq a_{i0,j0}$, i.e. $U$ contains all variables $a_{ij}$ to the top-right of $a_{i0,j0}$. Define $W(U)$ to be the subspace of $W$ given by $a_{ij} = 0$, $a_{ij} \in U$. Define $W(U)(\mathbb{Z})_{a_{mm}}$ to be $\alpha \in W(U)(\mathbb{Z})_{a_{mm}}$ such that $a_{ij} \neq 0$ for $a_{ij} \notin U$. It suffices to prove that

$$\int_{t \in R \times S} \# \{ tA_0 D(X) \cap W(U)(\mathbb{Z})_{a_{mm}=0} \} \delta(t) \, d^\times t = o(X^{3/2})$$

By Lemmas 7.3 and 7.4 if $U$ contains $a_{ij}$ with $i+j \leq 0$ or with $\{i,j\} = \{0,1\}$, then every element of $W(U)(\mathbb{Z})_{a_{mm}}$ is reducible. Similarly, by Lemma 7.3 if $U$ contains $a_{ij}$ and $a_{ji}$ for some pair $(i,j)$ such that $i+j = 1$, then every element of $W(U)(\mathbb{Z})_{a_{mm}}$ is reducible. We may assume that $U$ doesn’t 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 $X w_{ij}(t) \geq 1$.

**Proof.** If $X w_{ij}(t) < 1$, then $a_{ij}(\alpha) = 0$ for $\alpha \in W(U)(\mathbb{Z})_{a_{mm}}$, and so $\alpha \notin W(U)(\mathbb{Z})_{a_{mm}}$.

It is an easy consequence of Claim 7.4 that $X s_m^{-1} > 1$ and $X r_m^{-1} > 1$, and for all $k$, $X^2 s_k^{-1} > 1$ and $X^2 r_k^{-1} > 1$. 

20
Claim 7.8. We have

$$\#\{tA_0D(X) \cap W(U)(\mathbb{Z})_{10}^\text{irr}\} = O\left(\prod_{a_{ij} \in U} w_{ij}^{-1}(t)X^{n^2-|U|}\right).$$

Proof. By Proposition \ref{prop:bound},

$$\#\{tA_0D(X) \cap W(U)(\mathbb{Z})_{10}^\text{irr}\} = O(\text{Vol}) + E,$$

where Vol is the volume of the projection of $tA_0D(X)$ onto $W(U)$, and $E$ is error term mentioned in Proposition \ref{prop:bound}. If the projection of $tA_0D(X)$ onto some line spanned by $a_{ij}$, for some $a_{ij} \notin U$ has volume less than 1, then $tA_0D(X) \cap W(U)(\mathbb{Z})_{10}^\text{irr} = \emptyset$. Therefore, the volume of the projection of $tA_0D(X)$ onto any coordinate subspace of $W(U)$ is bounded by Vol. We therefore have the bound

$$\#\{tA_0D(X) \cap W(U)(\mathbb{Z})_{10}^\text{irr}\} = O(\text{Vol}).$$

The claim follows from the fact that $\text{Vol} = O\left(\prod_{a_{ij} \in U} w_{ij}^{-1}(t)X^{n^2-|U|}\right).$ \hfill \qed

By Claim \ref{claim:bound} we have

$$\int_{t \in R \times S} \#\{tA_0D(X) \cap W(U)(\mathbb{Z})_{10}^\text{irr}\} \delta(t) d^x t = O\left(X^{n^2-|U|} \int_{t \in R \times S} \prod_{a_{ij} \in U} w_{ij}^{-1} \prod (r_i s_i)^{2-2im} d^x t\right).$$

It remains to prove that

$$\int_{t \in R \times S} \prod_{a_{ij} \in U} w_{ij}^{-1} \prod (r_i s_i)^{2-2im} d^x t = o\left(X^{|U|}\right).$$

Suppose first, that $U$ is contained in the top-right $m \times m$ block. We then have $\prod_{i,j>0} w_{ij}^{-1} = \prod (r_i s_i)^{im}$. If $U$ is strictly contained in the top-right $m \times m$ block, all the exponents in the $r_i$ and $s_i$ (in the integrand) are strictly negative, and 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 zero, and the other exponents are strictly negative. By Claim \ref{claim:bound}, $X w_{10} \geq 1$ and $X w_{01} \geq 1$. We make the exponents of $r_m$ and $s_m$ negative as well, by multiplying the entire expression by $X^2 w_{10} w_{01}$, 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 $j \leq 0$ of $a_{im}$, $i \leq 0$. 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 is 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 \ref{lemma:induction} we assume that, $b_r < m$. In order to apply induction, we have to show that

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

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

$$s_u = s_{m-1} \ldots s_{k_r+1} s_{k_s} \ldots s_1^{k_s-1+1}$$
and
\[ r_u = x_1^{1+a} \cdots x_{k_1+a+1}^{r_1} \cdots x_{k_r+a+1}^{r_r} \cdots x_{k_2+a+1}^{r_{k_2}} \cdots x_{k_2}^{-k_2+1}. \]

Recall that \( Xw > 1 \) for any \( w \notin U \). Let \( w_0 = (r_1 \ldots r_m)^{-1}(s_{k_1+1} \ldots s_{m}) \), be the weight of the variable \( a_{m} \cdot b_{s} \). We have that \( w_0^g s_0 r_u \) equals \( s_m s_{m-1} \ldots s_{k_1+1} r_m \ldots r_{k_2+a+1} \) multiplied by non-positive powers of the \( s_k \) and \( r_k \). Recall that we have \( X^2 s_k^{-1} > 1 \) and \( X^2 r_k > 1 \). Further, \( Xr_m^{-1} > 1 \) and \( Xs_m^{-1} > 1 \).

Multiplying \( s_0 r_u \) by \( X^{a+2b_1+(b_s-a)-2} w_0^g (s_m \ldots s_{k_2+2})^{-1}(r_m \ldots r_{k_2+a+1})^{-1} \) gives us a product of non-positive powers of the \( r_k \) 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 that \( X^4 r_k^{-1} s_k^{-1} < 1 \) 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 4.9. Let \( \mathcal{F}' \subset \mathcal{F} \) be the set of cuspidal elements of \( \mathcal{F} \). By Proposition 7.6, we have

\[
\frac{N(W(Z)^{(a,b)}, X)}{\eta(a,b)} \cdot \frac{1}{\text{Vol}(A_0)} \int_{h \in \mathcal{F}} d h \# \{ hA_0 D^{(a,b)}(X) \cap W(Z)^{\text{irr}} \} = \frac{1}{\eta(a,b)} \cdot \frac{1}{\text{Vol}(A_0)} \int_{h \in \mathcal{F} \setminus \mathcal{F}'} d h \# \{ hA_0 D^{(a,b)}(X) \cap W(Z)^{\text{irr}} \} + \text{o}(X^n^2).
\]

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

By construction of \( \mathcal{F}' \), the length of the projection of \( hA_0 D(X) \) onto the coordinate \( a_m = 0 \) for all \( h \) in \( \mathcal{F} \setminus \mathcal{F}' \) is at least 1. Further, the weight of \( a_m \) being minimal, the volume of all smaller dimensional projections of \( hA_0 D(X) \) are bounded by the volume of the projection onto the hyperplane \( a_m = 0 \). Therefore, \( N(W(Z)^{(a,b)}, X) \) equals

\[
\frac{1}{\eta(a,b) \text{Vol}(A_0)} \int_{h \in \mathcal{F} \setminus \mathcal{F}'} \left[ \text{Vol}(hA_0 D^{(a,b)}(X)) + \text{o}(\frac{\text{Vol}(hA_0 D^{(a,b)}(X))}{X w_{mm}}) \right] d h + \text{o}(X^n^2)
\]

We have that \( \int_{h \in \mathcal{F} \setminus \mathcal{F}'} \frac{1}{w_{mm}} d h \) 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

\[
N(W(Z)^{(a,b)}, X) = \frac{1}{\eta(a,b) \text{Vol}(A_0)} \int_{h \in \mathcal{F}} \text{Vol}(hA_0 D^{(a,b)}(X)) d h + \text{o}(X^n^2)
\]

= \[
\frac{1}{\eta(a,b) \text{Vol}(A_0)} \int_{h \in A_0} \text{Vol}(F h D^{(a,b)}(X)) d h + \text{o}(X^n^2)
\]

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

\[
N(W(Z)^{(a,b)}, X) = \frac{1}{\eta(a,b)} \text{Vol}(F D^{(a,b)}(X)) + \text{o}(X^n^2)
\]

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:

**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 \( \mu_p \) is the \( p \)-adic density of \( \mathcal{L} \) in \( W(\mathbb{Z}) \).

The structure of our proof will be as follows: 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 as above. We then have

\[
\int_{h \in \mathcal{X} \setminus \mathcal{F}} \# \{ hA_0D^{(a,b)}(X) \cap \mathcal{L} \} dh = \prod_p \mu_p(\mathcal{L}) \int_{h \in \mathcal{Y} \setminus \mathcal{F}} \# \{ hA_0D^{(a,b)}(X) \cap W(\mathbb{Z}) \} dh + o(X^{n^2})
\]

**Proof.** We follow the proof of [5, Theorem 35]. Suppose that \( \mathcal{L} \) is defined by congruences modulo some integer \( m \). Then \( \mathcal{L} \) may be viewed as a disjoint union of translates \( \mathcal{L}_1 \ldots \mathcal{L}_k \) of the lattice \( mW(\mathbb{Z}) \). To estimate \( \# \{ hA_0D^{(a,b)}(X) \cap \mathcal{L}_i \} \), we again use Proposition 7.2 and see that \( \# \{ hA_0D^{(a,b)}(X) \cap \mathcal{L}_i \} = 1/mn^2 \text{Vol}(hA_0D^{(a,b)}(X)) \), up to an error of \( o(X^{n^2}) \). Summing over \( \mathcal{L}_i \), we obtain

\[
\int_{h \in \mathcal{X} \setminus \mathcal{F}} \# \{ hA_0D^{(a,b)}(X) \cap \mathcal{L} \} dh = \frac{1}{m} \sum_{i=1}^k \text{Vol}(hA_0D^{(a,b)}(X)) dh + o(X^{n^2}).
\]

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

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.

**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 large enough \( p \). The stabilizer of any regular semisimple element has at most \( 2^n \) elements. The cardinality of \( W(\mathbb{F}_p) \) is \( p^n \). 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 zero. 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 \( \frac{Np^{n^2-n}/2^{n+1}}{p^{n^2}} > r_n \), 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, and which also have non-zero discriminant, and whose constant term a non-zero 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, and so \( |(L^x/L^{x^2})|_{N=1} \geq 4 \). Such invariants have to be good, because there have to be at least 2 irreducible \( \mathbb{F}_p \)-orbits. The lemma follows.
Proposition 7.12. We have
\[ \int_{h \in \mathcal{F} \setminus \mathcal{F}'} \# \{ hA_0D(x) \cap W(\mathbb{Z}) \} dh = \int_{h \in \mathcal{F} \setminus \mathcal{F}'} \# \{ hA_0D(x) \cap W(\mathbb{Z}) \} dh + o(X^n) \]

Proof. It suffices to show that the proportion of invariants over \( \mathbb{F}_p \) having non-trivial stabilizer in \( H(\mathbb{F}_p) \) is bounded away from 1 independent of \( p \). 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 \( p \leq Y \). For every \( Y \in \mathbb{N} \), the set \( \mathcal{L}_Y \) is defined by congruence conditions and contains \( W(\mathbb{Z})^{\text{red}} \).

By Lemma 7.11, we have
\[ \int_{h \in \mathcal{F} \setminus \mathcal{F}'} \# \{ hA_0D(x) \cap \mathcal{L}_Y \} dh = \prod_{p < Y} \mu_p(\mathcal{L}_Y) \int_{h \in \mathcal{F} \setminus \mathcal{F}'} \# \{ hA_0D(x) \cap W(\mathbb{Z}) \} dh. \]

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 \( W(\mathbb{Z})^{\text{red}} \subset \mathcal{L}_Y \) for all \( Y \).

Lemma 7.13. The proportion of elements in \( W(\mathbb{F}_p) \) having non-trivial 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 constant term a non-zero perfect square, is bounded away from zero 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 non-trivial. Then \( N(S, X) = o(X^n) \).

Proof. Let \( f \in \mathbb{Z}[x] \) be the polynomial associated to \( T \). By Corollary 4.2, the stabilizer in \( H(\mathbb{Q}) \) is non-trivial 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 non-trivial stabilizer is bounded away from 1 independent of \( p \). The product of this ratio over all primes diverges to 0. Therefore, the same argument as in the proof of Proposition 7.12 applies to prove our result.

Lemma 7.15. The proportion of invariants over \( \mathbb{F}_p \) which are either 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 zero independent of \( p \). The proportion of invariants such that the corresponding polynomial \( f \) has \( n \) distinct non-zero roots over \( \mathbb{F}_p \) is bounded away from zero independent of \( p \). The proportion of such \( f \) 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 zero, independent of \( p \). Therefore, the proportion of invariants with the property that \( \gamma \) is not a perfect square in \( L^\times \) is bounded away from zero, independent of \( p \) (here, \( L = \mathbb{F}_p[x]/(f(x)) \) is the étale algebra associated to regular
roots is a square is the same as scaling this by a factor of $\frac{1}{p}$
is clearly bounded away from zero independent of
of which is zero, is
The number of invariants such that the corresponding
Proof. Then there exists some
in large sets.
Divisions. For a prime $p$
Definition 7.
In this section, we count elements having bounded height in subsets of $\text{Inv}(\mathbb{Z})$ and $W(\mathbb{Z})$ that are defined by certain infinite sets of congruence conditions.

**Definition 7.** Let $\Sigma \subset \text{Inv}(\mathbb{Z})$ be a set defined by (possibly infinitely many) congruence conditions. For a prime $p$, let $\Sigma_p$ denote the closure of $\Sigma$ in $\text{Inv}(\mathbb{Z}_p)$. We say that $\Sigma$ is large at $p$ if $\Sigma_p$ contains every $c$ such that the reduction of $f_c$ modulo $p$ has no triple root. The set $\Sigma \subset \text{Inv}(\mathbb{Z})$ 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.

**Proposition 7.16.** Let $N_X$ denote the number of invariants $c \in \text{Inv}^{rs}(\mathbb{Z})$ 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 $N_X = o(X^n)$, i.e. the proportion of $N_X$ to the number of invariants with height bounded by $X$ goes to zero.

**Proof.** Fix $c \in \text{Inv}^{rs}(\mathbb{Z}) \subset \text{Inv}^{rs}(\mathbb{Q})$, and let $L$ denote the corresponding etale 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 $c \in \text{Inv}^{rs}(\mathbb{Z})$, 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 etale $\mathbb{F}_p$ algebra corresponding to the reduction of $c$ modulo $p$).

Therefore, if the two distinguished orbits lie in the same $H(\mathbb{Q})$ orbit, then the reduction of $c$ modulo $p$ is either 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 congruence conditions, whose local densities (by Lemma 7.15) are bounded away from 1. The proposition follows. \qed

We conclude this paragraph with a lemma which we will need to prove Theorem 1.3.

**Lemma 7.17.** Consider the proportion $r_p$ of $c = (a_1, a_2, \ldots, a_n, e) \in \text{Inv}(\mathbb{F}_p)$ 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 non-zero roots is a perfect square.

Then 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 zero, is $\prod_{i=1}^{n-1} (p - i)/(n - 1)!$. Adding the condition that the product of the non-zero 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 zero independent of $p$. The lemma follows. \qed

**Infinitely many congruence conditions**

In this section, we count elements having bounded height in subsets of $\text{Inv}(\mathbb{Z})$ and $W(\mathbb{Z})$ that are defined by certain infinite sets of congruence conditions.
Theorem 7.18. Let $\Sigma \subseteq \text{Inv}(\mathbb{Z})$ be large. Then
\[
\# \{ c \in \Sigma \cap \text{Inv}(\mathbb{R})^{(a,b)} | \text{ht}(c) < X \} = \prod_p \text{Vol}(\Sigma_p) \text{Vol}(\text{Inv}(\mathbb{R})^{(a,b)}_{\text{ht} < X})
\]

Proof. Let $Z \subseteq \text{Inv}$ denote the variety of elements $c$ such that $f_c$ has a triple root. Then $Z$ has codimension 2. Let $Y_p \subseteq \text{Inv}(\mathbb{Z})$ denote the set of elements $c$ whose reduction modulo $p$ lie in $Z(\bar{\mathbb{F}}_p)$. An argument identical to the proof of [3, Theorem 3.5] yields the estimate
\[
\# \bigcup_{p > M} \{ c \in Y_p : \text{ht}(c) < X \} = O\left( \frac{X^{n^2} \log X}{M} \right).
\]
The theorem now follows from the above “tail estimate” using standard sieving arguments (see, for example, the proof of [6, Theorem 2.21]). \hfill \Box

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 is weighted by $\phi(T) / \# \Delta_{\Gamma}(\mathbb{Z})$.

Definition 8. 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 $p$, $\phi_p$ is locally constant outside a closed set of measure zero.

Theorem 7.19. Suppose $\phi : W(\mathbb{Z}) \to [0, 1]$ is defined by congruence conditions, and that the $\phi_p$ are $H(\mathbb{Z}_p)$ invariant. Then
\[
N_{\phi}(W(\mathbb{Z}), X) \leq N(W(\mathbb{Z}), X) \prod_p \int_{T \in W(\mathbb{Z})} \phi_p(T) dT + o(X^{n^2})
\]

If the function $\phi$ were nice enough, we expect that the upper bound is 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 $\phi_p$ is $H(\mathbb{Z}_p)$ invariant, so is $\phi_{p,N}$. Further, as $\phi_p$ is locally constant (outside a set of measure zero), $\phi_{p,N}$ converges to $\phi_p$ as $N$ goes to infinity. For $Y \subseteq \mathbb{N}$, define $\psi_Y$ to be $\prod_{p \in Y} \phi_p$, and $\psi_{Y,N}$ to be $\prod_{p \in Y} \phi_{p,N}$.

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
\[
N_{\phi}(W(\mathbb{Z}), X) \leq N_{\psi_{Y,N}}(W(\mathbb{Z}), X) = N(W(\mathbb{Z}), X) \prod_{p \in Y} \int_{T \in W(\mathbb{Z})} \psi_{p,N}(T) dT + o(X^{n^2}).
\]
The theorem follows by allowing $N$, and then $Y$, to go to infinity. \hfill \Box

26
8 Selmer Groups

In this section, we prove a strengthening of Theorems 1.1 and 1.3. Recall that for \( c = (a_1, \ldots, a_{n-1}, e) \in \text{Inv} \), 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 \( \Sigma \subset \text{Inv}(\mathbb{Z}) \) be any large family with the property that \( \Sigma_2 \) is contained in the subset of \( \text{Inv}(\mathbb{Z}) \) consisting of all \( c = (a_1, \ldots, a_{n-1}, e) \) such that \( 2^{2i} | a_i \) and \( 2^{2n} | e \). Then the average size over \( \Sigma \) of \( \text{Sel}_2(J_1,c) \) is bounded above by 6, and the average size of \( \text{Sel}_{1,2}(c) \) equals 2.

Theorems 1.1 and 1.3 follow from by applying Theorem 8.1 to the large family \( \Sigma_0 \) chosen as follows:

For \( p \neq 2 \), let \( \Sigma_p \subset \text{Inv}(\mathbb{Z}_p) \) consist of all \( c = (a_1, \ldots, a_{n-1}, e) \) such that either \( p^2i \not| a_i \) for some \( i \), or \( p^n \not| e \). Let \( \Sigma_2 \) consist of all \( c = (a_1, \ldots, a_{n-1}, e) \) such that \( 2^{2i} | a_i \) and \( 2^{2n} | e \), and either \( 2^{6i} \not| a_i \) for some \( i \), or \( 2^{3n} \not| e \). Let \( \Sigma_0 \subset \text{Inv}(\mathbb{Z}) \) be the subset defined by the local condition \( \Sigma_p \), i.e. \( \Sigma_0 = \{ c \in \text{Inv}(\mathbb{Z}) \mid \forall p, c \in \Sigma_p \} \).

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

\[
\phi(T) = \begin{cases} 
\left( \frac{\sum_{T' \in \Sigma} \# \Delta_{T'}(Q)}{\# \Delta_{T'}(Z)} \right)^{-1} & \text{if } T \text{ is locally soluble, and } T \text{ has invariants in } \Sigma, \\
0, & \text{otherwise}
\end{cases}
\]

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

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

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

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

\[
\sum_{c \in \Sigma^{(a,b)}, \text{ht}(c) \leq X} (\# \text{Sel}_2(J_1,c) - 2) = N_\phi(W(\mathbb{Z})^{(a,b)}, X) + o(X^{n^2}),
\]

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

**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 7.18 the set of \( c \in \text{Inv}(\mathbb{Z})^{(a,b)} \) with \( \text{ht}(c) \leq X \) 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 8.2 every element in \( \text{Sel}_2(J_{1,c}) \subset H^1(J_{1,c}[2]) \) gives rise to integral orbits, which by definition are locally soluble. Therefore,

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

Recall that in the definition of \( N(S, X) \) for sets \( S \), the \( H(\mathbb{Z}) \)-orbit of \( T \in S \) was weighted by \( \frac{1}{\# \Delta_{T}(Z)} \). Let \( c \in \text{Inv} \) be the invariants of \( T \in W(\mathbb{Z})^{(a,b), \phi \neq 0} \). Suppose that \( T = T_1 \ldots T_k \) 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 \(\Sigma\), with a representative \(T\) in \(W(\mathbb{Z})\) with a weight of \(\frac{1}{\# \Delta T(\mathbb{Q})}\). By Proposition\[?[7.13]\], the number of orbits having non-trivial stabilizer over \(\mathbb{Q}\) is \(o(X^{n^2})\). The proposition follows. \(\square\)

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

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

\(\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}
\]

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 \(\phi\) or \(\phi_{12}\). Then \(w(T) = \prod_p w_p(T)\).

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

Recall that for \(c \in \text{Inv}(\mathbb{Q}_p)\), \(W_c\) 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 Inv(\(\mathbb{Z}\)) have covolume 1. Pick \(\omega\), an algebraic differential form that generates the rank 1 module of top-degree left invariant differential forms on \(H = SO(V_1) \otimes SO(V_2)\). 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

\[
\int_{W(\mathbb{Z}_p)} w(T) dT = \text{Vol}(H(\mathbb{Z}_p)) |\mathcal{J}| \int_{\text{Inv}(\mathbb{Z}_p)} \left(\sum_{c \in \text{Inv}(\mathbb{Z}_p)} \frac{w_p(T)}{\# \Delta T(\mathbb{Z}_p)}\right) dc
\]

where \(\frac{W(\mathbb{Z}_p)}{H(\mathbb{Z}_p)}\) 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 \(\text{Inv}(\mathbb{R})\). The proof of the following proposition is the same as in \([6]\) Proposition 3.12.

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

\[
\text{Vol}(\mathcal{FD}^{(a,b)}_{\text{sol}}(X)) = \tau_{\text{sol}}^{(a,b)} |\mathcal{J}| \text{Vol}(\mathcal{FD}^{(a,b)}_{\text{ht,}}) \text{Vol}(\text{Inv}(\mathbb{R})^{(a,b)}_{\text{ht,<}}).
\]

Here, \(\mathcal{J}\) is the same constant that appears in Proposition\[?[8.4]\], and the numbers \(\tau_{\text{sol}}^{(a,b)}\) are as in \(\S 7.1\).
The proofs of [6] Propositions 3.11, 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-zero locus); the sum of the degrees of the invariants equals $n^2$, the dimension of $W$; and there exist Kostant sections $\kappa: \text{Inv} \to W$.

We need to simplify the expression

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

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

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

where the subscript $\text{sol}$ is as in §7.1. Depending on whether $\text{sol}$ 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 $\Sigma \subset \text{Inv}(\mathbb{Z})$. Without any loss of generality, we restrict ourselves to the family over $\Sigma$ and $F$. The product of the local volumes along with $\text{Vol}(\Sigma_p)$ is bounded (outside the discriminant-zero locus); the sum of the degrees of the invariants equals $n^2$, the dimension of $W$; and there exist Kostant sections $\kappa: \text{Inv} \to W$.

Further, by Proposition 8.5 and Theorem 7.1

$$N(\mathbb{W}(\mathbb{Z}), X) = |\mathcal{J}| \tau(\mathbb{Z})(\mathbb{R}) \text{Vol}(\mathbb{F}) \text{Vol}(\Sigma_p) + o(X^{n^2}).$$

Clearly, $b_\infty = \frac{\tau(\mathbb{Z})(\mathbb{R})}{\eta(\mathbb{R})}$, because the numerator equals the number of real soluble orbits. Therefore, by using the fact that the $b_\nu$ all multiply to 1, we see that the main term simplifies to

$$\text{Vol}(\Sigma_p) \prod_p \text{Vol}(\mathbb{Z}_p).$$

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

$$\sum_{c \in \Sigma^{(a,b)}(\mathbb{Z})} \#(\text{Sel}^2(J_{1,c}) - 2) \leq 4 \text{Vol}(\Sigma_p) \prod_p \text{Vol}(\Sigma_p).$$
The number of hyperelliptic curves in our family with height less than \( X \) is \( \sum_{n \in \Sigma^{(a,b)}_{\text{ht}(c) \leq X}} 1 \), which by Theorem \ref{thm:selmer-volume} is \( \text{Vol}(\text{Inv}(\mathbb{P}))^{(a,b)} \prod_p \text{Vol}(\Sigma_p) \) up to an error of \( o(X^{n^2}) \). Putting all this together, we have

\[
\lim_{X \to \infty} \frac{\sum_{\substack{c \in \Sigma^{(a,b)} \\text{ht}(c) \leq X}} (# \text{Sel}_2(J_{1,c}) - 2)}{\sum_{\substack{c \in \Sigma^{(a,b)} \\text{ht}(c) \leq X}} 1} \leq 4.
\]

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

### 8.2 The (1,2)-Selmer

**Proposition 8.6.** Let \( p > 2 \) be a large enough prime. We have

\[
\int_{\text{Inv}(\mathbb{Z}_p)} \frac{\#(J_{1,c}(\mathbb{Q}_p)/2J_{1,c}(\mathbb{Q}_p) \cap J_{2,c}(\mathbb{Q}_p)/2J_{2,c}(\mathbb{Q}_p))dh}{\# \Delta_c(\mathbb{Q}_p)} \leq (1 - a/p) \text{Vol}(\text{Inv}(\mathbb{Z}_p))
\]

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 \ref{prop:selmer-volume}) that \( \frac{\#J_1(\mathbb{Q}_p)/2J_1(\mathbb{Q}_p) - \#\Delta(\mathbb{Q}_p)}{\#\Delta(\mathbb{Q}_p)} = 1 \). 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 \( J_2(\mathbb{Q}_p)/2J_2(\mathbb{Q}_p) \) don’t coincide, then the integrand will be at least 1/2. We will show that there exists \( S \subset \text{Inv}(\mathbb{Z}_p) \) of volume greater than \( r/p \), such that for \( c \in S \), the images of \( J_1 \) and \( J_2 \) don’t coincide. Here, \( r \) is the constant alluded to in Lemma \ref{lem:selmer-volume}. The proposition follows from the existence of \( S \). Indeed,

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

Setting \( a = r/2 \) gives the proposition.

Let \( S_p \subset \text{Inv}(\mathbb{F}_p) \) be the subset defined by the conditions in Lemma \ref{lem:selmer-volume}. Let \( S' \subset \text{Inv}(\mathbb{Z}_p) \) 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), and so the discriminant of \( f_c \) is not zero. 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 \( f_c(0) = c_p^2 \)). Let \( S'' \) denote the set of all \( c \in S' \) such that \( e_c = 0 \). Clearly, \( S'' \) a measure-zero set. Let \( S = S' \setminus S'' \). The set \( S \) has volume 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 that \( \Delta_c = \text{Res}_{\mathbb{Q}_p/\mathbb{Q}_p}(\mu_2)_{N=1} \), and \( H^1(\mathbb{Q}_p, \Delta_c) = ((\mathbb{Z}_p^\times)^n,((\mathbb{Z}_p^\times)^2)^n)_{N=1} \). Because the discriminant of \( f_c \) is a \( p \)-adic unit, by Proposition \ref{prop:selmer-volume} 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 \( J_2(\mathbb{Q}_p) \) isn’t 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 \( y^2 = x f_c(x) \) with \( x \)-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 \( Q - \infty \) 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 \( u'_i \in \mathbb{Z}^x_p \), which lift \( u_i \in \mathbb{F}_p^x \), are the roots of \( f_c \). Suppose that \( p^{2b} u'_c \neq 0 \) is the final root (which as mentioned above has \( p \)-adic valuation equaling \( 2b \)). Then, \( f_c(p) = (p - p^{2b} u'_c) \prod_{i=1}^{n-1} (p - u'_i) = p(1 - p^{2b-1} u'_c) \prod_{i=1}^{n-1} (p - u'_i) \). Since \( n \) is odd,

\[
\prod_{i=1}^{n-1} (p - u'_i) = \prod_{i=1}^{n-1} (u'_i - p) \equiv \prod_{i=1}^{n-1} u'_i \bmod p.
\]

By construction, \( \prod_{i=1}^{n-1} (p - u'_i) \) is a non-zero square modulo \( p \), and is therefore a square in \( \mathbb{Z}^x_p \).

Similarly, \( 1 - p^{2b-1} u'_c \) is also a square in \( \mathbb{Z}^x_p \). Therefore, \( f_c(p) \) is \( p \) multiplied by a square, and so \( pf_c(p) \) must be a square in \( \mathbb{Q}_p^x \). We have proved our result.

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

\[
\lim_{X \to \infty} \frac{\sum_{c \in \Sigma^{(a,b)}} \left( \#(\text{Sel}_2(J_{1,c}) \cap \text{Sel}_2(J_{2,c})) - 2 \right)}{\sum_{c \in \Sigma^{(a,b)}} \frac{1}{\text{ht}(c) \leq X}} = 0.
\]

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 that

\[
\sum_{c \in \Sigma^{(a,b)}} \left( \#(\text{Sel}_2(J_1(C)) \cap \text{Sel}_2(J_2(C))) - 2 \right) = N_{\phi_{12}}(W(\mathbb{Z})^{(a,b)}_{(1,2)}, X) + o(X^{n^2}).
\]

By Theorem [7.19] we have

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

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 zero and we have proved Theorem [8.7]

References

[1] M. Bhargava, The density of quartic rings and fields, *Ann. of Math.* **162**, 1031–1063.
[2] M. Bhargava, Most hyperelliptic over \( \mathbb{Q} \) curves have no rational points, [http://arxiv.org/abs/1308.0395](http://arxiv.org/abs/1308.0395).
[3] M. Bhargava, The geometric sieve and the density of squarefree values of invariant polynomials (2014), arXiv/1402.0031
[4] M. Bhargava and B. Gross, Arithmetic invariant theory (2012), arXiv/1206.4774.
[5] M. Bhargava and B. Gross, The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point (2012), arXiv/1208.1007.

[6] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, arXiv/1006.1002.

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

[8] J. W. S. Cassels, Rational quadratic forms, London Mathematical Society Monographs, 13. *Academic Press, Inc [Harcourt Brace Janovich, Publishers], London-New York*, 1978. ISBN: 0-12-163260-1

[9] H. Davenport, On a principle of Lipschitz, *J. London Math. Soc.* 26 (1951), 179–183. Corrigendum: “On a principle of Lipschitz ”, *J. London Math. Soc.* 39 (1964), 580.

[10] B. Gross, Hanoi lectures on the arithmetic of hyperelliptic curves, *Acta Mathematica Vietnamica* 37 (2012), 579–588.

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

[12] P. Levy, Vinberg’s θ-groups in positive characteristic and Kostant-Weierstrass slices, *Transform. Groups* 14 (2009), 2 417 – 461.

[13] D. Panyushev, On invariant theory of θ-groups, *J. Algebra* 283, (2005) 2, 255–270.

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

[15] B. Poonen and M. Stoll, Most odd degree hyperelliptic curves have only one rational point (2013), arXiv/1302.0061.

[16] A. Shankar and X. Wang, Average size of the 2-Selmer group of Jacobians of monic even hyperelliptic curves (2014), arxiv/1307.3531.

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

[18] J. Thorne, Vinberg’s representation and arithmetic invariant theory, *Algebra Number Theory* 7 (2013), 9, 2231 –2368.

[19] J. Thorne, *E*6 and the arithmetic of a family of non-hyperelliptic curves of genus 3, *Forum Math. Pi* 3 (2014).

[20] J. Thorne, A remark on the arithmetic invariant theory of hyperelliptic curves, *Math. Res. Lett.* 21 (2014), 6, 1451 –1464.

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

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

[23] X. Wang, Pencils of quadrics and Jacobians of hyperelliptic curves, Ph.D thesis, Harvard (2013).

E-mail address, ashankar@math.harvard.edu
Department of Mathematics, Harvard University, Cambridge, MA 02138, USA