Arithmetic statistics of isogeny Selmer groups associated to hyperelliptic curves

Martí Oller

September 15, 2025

Abstract

We determine an upper bound for the average size of the Selmer groups associated to certain self-dual isogenies related to Jacobians of hyperelliptic curves. This is one of the first results of this kind for isogenies that are not multiplication-by-n. The proof follows Bhargava's framework, and features a novel orbit parametrisation associated to the Dynkin diagram of type B_{2n}.

Contents

1 Introduction

1.1 Statement of results

Let $n \geq 2$, and consider the hyperelliptic curve $C\colon y^2 = xf(x)$, where $f(x) = x^{2n} + p_2x^{2n-1} + \cdots + p_{4n}$. Let $B = \operatorname{Spec} \mathbb{Z}[p_2, \ldots, p_{4n}]$, and for an element $b \in B(\mathbb{R})$ let us define its *height* as

$$\operatorname{ht}(b) = \sup_{i=1,\ldots,2n} \{|p_{2i}|^{1/(2i)}\}.$$

Let us consider the Jacobian $J_b = \operatorname{Jac}(C_b)$. The point $T = (0,0) \in C(\mathbb{Q})$ defines a rational 2-torsion point inside J_b: we will denote by M the group generated by T inside $J_b[2]$. Let $M^\perp$ be the orthogonal complement of M with respect to the Weil pairing. We note that $M \leqslant M^\perp$, and that both M and $M^\perp$ are stable under $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action. Therefore, there exists an abelian variety A_b with maps

$$J_b \xrightarrow{\phi_M} A_b \xrightarrow{\phi} A_b^\vee \to J_b, \tag{1}$$

such that if $\psi = \phi \circ \phi_M$, then $J_b[\phi] = M$, $J_b[\psi] = M^\perp$, $A_b[\phi] = M^\perp/M$ and the whole composition in (1) is the multiplication-by-2 isogeny. We will denote the isogenies by ϕ_b or ψ_b when we wish to emphasize the invariant $b \in B$.

Theorem 1.1. *When ordered by height, the average size of* $\operatorname{Sel}_\phi(A_b)$*, where* b *varies in* $B(\mathbb{Z})$*, is at most* 6*.*

In fact, Theorem 1.1 remains true even when finitely many congruence conditions are imposed on $B(\mathbb{Z})$: see Section 4 and Theorem 4.3.

1.2 Method of proof

Many results on the average size of Selmer groups of isogenies that are multiplication-by-n have appeared in the literature in the past years, helped mainly by Bhargava's striking new methods in geometry-of-numbers: as seen for instance in [BS15a; BS15b; Lag24], among many others.

The standard technique in "Bhargavology" is to parametrise the elements of the Selmer groups by integral orbits of a representation (G, V) of a reductive group G defined over $\mathbb{Z}$. Finding such parametrisations is one of the main obstacles in obtaining more of these results. Previous experience suggests that many representations used in arithmetic statistics actually arise from Vinberg theory, or in other words the study of graded Lie algebras. In [Tho13], Thorne connected the Vinberg representations associated to the $\mathbb{Z}/2\mathbb{Z}$-gradings of the simply laced Lie algebras (i.e. those of type A_n, D_n or E_n) with certain families of curves arising as deformations of simple surface singularities, in such a way that the orbits of the representation should give arithmetic information about the constructed families of curves. This perspective has been used, implicitly and explicitly, to obtain statistical results on the size of 2-Selmer groups in the past: all these results have been unified and reproved in Laga's thesis [Lag24], which gives a uniform proof of all such results.

Other Vinberg representations have appeared in the literature, either coming from either non-simply laced Dynkin diagrams or higher order gradings (or both). In [RT21], a $\mathbb{Z}/3\mathbb{Z}$-grading in E_8 is used to study the 3-Selmer group of odd genus 2 curves. In [BES20], a $\mathbb{Z}/3\mathbb{Z}$-grading of G_2 was used to study 3-isogeny Selmer groups of the elliptic curves $y^2 = x^3 + k$, a perspective that was later generalised in [Bha+19] for abelian varieties. In [Lag24], a $\mathbb{Z}/2\mathbb{Z}$-grading in F_4 is used to study 2-Selmer groups of a family of Prym varieties, in a manner that serves as a template for our results.

We now explain the structure of this paper. In Section 2, we will construct the representation (G, V) associated to the diagram B_{2n}, and we will describe its rational and integral orbits. We will also see how this representation is connected to the geometric picture of (1). We now explain this more precisely. First,

we will observe that the ring of invariants $\mathbb{Q}[V]^G$ is isomorphic to an affine space $\mathbb{Q}[p_2, \dots, p_{4n}]$, where p_{2i} has degree $2i$. Therefore, any element of $V(\mathbb{Q})$ can be associated to the hyperelliptic curve $C_b\colon y^2 = x(x^{2n} + p_2 x^{2n-1} + \cdots + p_{4n})$, and consequently to the isogenies described in (1). Then, we will find an embedding

$$\mathrm{Sel}_\psi J_b \hookrightarrow (G(\mathbb{Q})\backslash V_b(\mathbb{Q})) \bigcap \frac{1}{2}V(\mathbb{Z}),$$

where V_b denotes the subset of V of elements having invariants b. Later, in Section 3, we will consider a related representation (G^*, V^*), for which will have $V^* /\!\!/ G^* \simeq V /\!\!/ G$ and a commutative diagram

$$\begin{array}{ccc} \mathrm{Sel}_\psi J_b & \longrightarrow & \mathrm{Sel}_\phi A_b \\ \downarrow & & \downarrow \\ G(\mathbb{Q})\backslash V_b(\mathbb{Q}) & \longrightarrow & G^*(\mathbb{Q})\backslash V_b^*(\mathbb{Q}), \end{array}$$

where again the rightmost map is injective and every element in its image has a representative in $\frac{1}{2}V_b^*(\mathbb{Z})$. It turns out that the representation (G^*, V^*) is the Vinberg representation associated to the $\mathbb{Z}/2\mathbb{Z}$-grading on A_{2n-1}, which has already been studied in [SW18]. Therefore, in Section 4 we can use the counting results of *loc. cit.* to prove Theorem 1.1.

We can compare the result of Theorem 1.1 with the Poonen-Rains heuristics in [PR12]. These heuristics contain some predictions for Selmer groups of self-dual isogenies $\lambda\colon A \to A^\vee$ which come from some symmetric line sheaf $\mathcal{L}$ in A. This is the case for all of our isogenies $\phi\colon A_b \to A_b^\vee$: ϕ is self-dual by Lemma 3.3, and the obstruction for ϕ to come from a symmetric line bundle is measured by an element $c_\phi \in H^1(A_b[\phi])$, which is zero in our case by [PR11, Proposition 3.12(f)]. Then, [PR12, Theorem 4.14] identifies $\mathrm{Sel}_\phi J_b$[1] with an intersection of two maximal isotropic subspaces of an infinite-dimensional quadratic space over $\mathbb{F}_2$. Then, Theorem 1.1 appears to be consistent with the predictions of the Poonen-Rains heuristics: the upper bound for our average size coincides with that of 2-Selmer groups of even hyperelliptic curves, which in both cases account for the presence of a marked rational subgroup of the Selmer group.

We end by noting a limitation of our current methods. Namely, we cannot obtain an analogous result for the average of $\mathrm{Sel}_\psi J_b$ using the representation (G, V). This is explained in detail in Section 5, where we discuss the possibility that the average size of $\mathrm{Sel}_\psi J_b$ might be unbounded. We further elaborate how this compares with previous results in the literature in the elliptic curve case, and the reasons why such an average might be unbounded.

1.3 Acknowledgements

I wish to thank my PhD advisor Jack Thorne for many helpful comments and conversations. I also want to thank Jef Laga for his useful suggestions.

2 Orbit parametrisation in B_{2n}

2.1 The representation (G, V)

The representation (G, V) of interest will be the Vinberg representation associated to the stable 2-grading associated to the root system of type B_{2n}. We now construct it explicitly: the reader can consult [Vin76; Pan05; Ree+12] for more context on such representations.

[1]The cited [PR12, Theorem 4.14] only identifies a *quotient* of $\mathrm{Sel}_\phi J_b$ as an intersection, but that quotient is equal to $\mathrm{Sel}_\phi J_b$ 100% of the time by [PR12, Proposition 3.4], using the fact that $A_b[\phi]$ is isomorphic to the 2-torsion of the Jacobian of $y^2 = f(x)$.

Let J_m denote the $m \times m$ matrix with 1s in the antidiagonal and 0s elsewhere. Define $\mathrm{SO}(J_m) = \{A \in \mathrm{SL}_m \mid {}^tAJA = J\}$. Throughout this paper, we will simply denote $\mathrm{SO}_m := \mathrm{SO}(J_m)$. We will also fix a field K of characteristic 0.

Let $n \geq 1$, and define $G := \mathrm{SO}_{2n+1} \times \mathrm{SO}_{2n}$. This group acts on the vector space $V = (2n+1) \boxtimes (2n)$, whose elements can be seen as $(2n+1) \times (2n)$ matrices, by $(g,h) \cdot A = gAh^{-1}$ for any $g \in \mathrm{SO}_{2n+1}$, $h \in \mathrm{SO}_{2n}$ and $A \in V$. Given $A \in V$, define its adjoint to be $A^* = J_{2n}{}^tAJ_{2n+1}$. If the $(2n) \times (2n)$ matrix A^*A has characteristic polynomial $f(x) = x^{2n} + p_2x^{2n-1} + \cdots + p_{4n}$, then the $(2n+1) \times (2n+1)$ matrix AA^* has characteristic polynomial $xf(x)$. The coefficients $p_2, \ldots, p_{4n}$ are all invariants of the representation, satisfying $p_{2i}(\lambda v) = \lambda^{2i} p_{2i}(v)$ for all $i = 1, \ldots, n$. Let $B := V /\!\!/ G = \operatorname{Spec} K[V]^G$ be the GIT quotient: the following lemma holds by general facts of Vinberg theory (see [Pan05, Corollary 3.6]):

Proposition 2.1. *We have that $B \cong \operatorname{Spec} K[p_2, \ldots, p_{4n}]$.*

We will denote $\pi \colon V \to B$ for the invariant map, and we will write $V_b(K)$ for those elements in $V(K)$ with invariants $b \in B(K)$. We will also denote the *discriminant* Δ of an element $b \in B(K)$ corresponding to the polynomial $f(x) = x^{2n} + p_2x^{2n-1} + \cdots + p_{4n}$ as the discriminant of the polynomial $xf(x^2)$, and similarly define the discriminant of an element $v \in V(K)$ as the discriminant of $\pi(v)$. The following result is also well-known:

Proposition 2.2. *An element $v \in V(K)$ is regular semisimple if and only if $\Delta(v) \neq 0$.*

We will use the subscript V^{rs} to distinguish those elements that are regular semisimple, and we will also denote B^{rs} for $\pi(V^{rs})$, which is equivalently the set of elements of B with non-zero discriminant.

2.2 Rational orbits

In general, a $G(K^s)$-orbit of elements in $V(K^s)$ might break up into multiple $G(K)$-orbits in $V(K)$. We have the following general result from arithmetic invariant theory (see [BG14, Proposition 1]) indicating how this phenomenon can be studied with Galois cohomology groups:

Proposition 2.3. *Let $v \in V(K)$. The set of $G(K)$-orbits in $V(K)$ which are $G(K^s)$-conjugate to v are in bijection with the kernel of the map*

$$H^1(K, \mathrm{Stab}_G(v)) \to H^1(K, G)$$

of pointed sets.

We will now show how to construct all the rational orbits with given invariants from an element $\alpha \in \ker(H^1(K, \mathrm{Stab}_G(v)) \to H^1(K, G))$. We start by constructing a "distinguished" orbit, and then we will show how to obtain the rest from it.

2.2.1 A distinguished orbit

Let $b = (p_2, \ldots, p_{4n}) \in B(K)$, and consider the polynomial $f(x) = x^{2n} + p_2x^{2n-1} + \cdots + p_{4n}$. Define the K-vector space $M = K[x]/(xf(x^2)) = K[\beta]$, which is spanned by the K-linear combinations of $1, \beta, \ldots, \beta^{4n}$. Define the bilinear form $(\cdot,\cdot) \colon M \times M \to K$ by:

$$(\lambda, \mu) = \text{ coefficient of } \beta^{4n} \text{ in } \lambda\mu.$$

Let $L_1 = K[x]/(xf(x))$ and let $L_2 = K[x]/(f(x))$. Then, M is isomorphic to $L_1 \oplus \beta L_2$, where there is a natural inclusion $L_1 \hookrightarrow M$ by sending $x \mapsto x^2$. In other words, L_1 is the subspace spanned by $\{1, \beta^2, \ldots, \beta^{4n}\}$ and βL_2 is spanned by $\{\beta, \beta^3, \ldots, \beta^{4n-1}\}$. Then, the form $(\cdot,\cdot)$ splits as a direct sum of bilinear forms in

L_1 and βL_2. Using the explicit power bases, we can see that both quadratic forms on L_1 and L_2 have discriminant 1 and are in fact split, so we can isometrically identify L_1 with a quadratic space (W_1, J_{2n+1}) of dimension $2n+1$ and L_2 with a quadratic space (W_2, J_{2n}) of dimension $2n$.

Let W be the quadratic space given by $(W_1, J_{2n+1}) \oplus (W_2, J_{2n})$, and consider the multiplication-by-β map $T_\beta \colon M \to M$, which can also be seen as a map from W to W. Given that T_β is self-adjoint with respect to $(\cdot,\cdot)$, we get that the matrix of T_β on W is of the form

$$\left(\begin{array}{c|c} 0_{(2n+1)\times(2n+1)} & A \\ \hline A^* & 0_{2n\times 2n} \end{array}\right),$$

where $A \in \mathrm{Mat}_{(2n+1)\times(2n)}$. Thus, we get an element $v \in V(K)$ with invariants $b \in B(K)$ by construction. We also observe the following:

Proposition 2.4. *Let $v \in V(K)$ be the orbit previously constructed, and assume that $\Delta(v) \neq 0$. Then, the stabiliser $\mathrm{Stab}_G(v)$ is isomorphic to the kernel of the norm map $\mathrm{Res}_{L_2/K}\mu_2 \to \mu_2$.*

Proof. Given that v is regular semisimple by Proposition 2.2, the centraliser of T_β in $\mathrm{GL}(M)$ is $M^\times$. Since the centraliser actually lies inside $\mathrm{SO}(M)$, this forces elements $\lambda \in M^\times$ to satisfy $\lambda^2 = 1$. Moreover, because λ needs to preserve both L_1 and βL_2, we see that $\lambda \in L_1^\times$. Finally, the fact that $\lambda \in \mathrm{SO}(W) \times \mathrm{SO}(W_1)$ forces $N_{L_1/K}(\lambda) = 1$ and $N_{L_2/K}(\overline{\lambda}) = 1$, where $\overline{\lambda}$ is the image of λ in L_2.

The conclusion is that the stabiliser is in bijection with the elements of $\mathrm{Res}_{L_1/K}\mu_2$ whose norm is 1 and whose image in L_2 also has norm 1. This can be identified with $\ker(\mathrm{Res}_{L_2/K}\mu_2 \to \mu_2)$, and so we are done. □

We will denote the kernel of the map $\mathrm{Res}_{L_2/K}\mu_2 \to \mu_2$ by $(\mathrm{Res}_{L_2/K}\mu_2)_{N=1}$.

2.2.2 The other orbits

Let $G' = \mathrm{SO}_{2n+1} \times \mathrm{O}_{2n}$. We will start by explaining how to construct all the diferent $G'(K)$-orbits, and then we will specialise to $G(K)$-orbits. Note that given $v \in V(K)$ with $\Delta(v) \neq 0$, we have that $\mathrm{Stab}_{G'}(v) \cong \mathrm{Res}_{L_2/K}\mu_2$, and that $H^(K, \mathrm{Res}_{L_2/K}\mu_2) \cong L_2^\times / L_2^{\times 2}$. We also observe that the pointed set $H^1(K, \mathrm{SO}_m)$ parametrises non-degenerate quadratic spaces of dimension m and discriminant 1, and that the trivial element of $H^1(K, \mathrm{SO}_m)$ corresponds to the (unique) split orthogonal space of dimension m. Similarly, the pointed set $H^1(K, \mathrm{O}_m)$ classifies non-degenerate quadratic spaces of dimension m, with a similar trivial element. The map $H^1(K, \mathrm{SO}_m) \to H^1(K, \mathrm{O}_m)$ has trivial kernel as a map of pointed sets, as can be seen from the usual long exact sequence in group cohomology of

$$1 \longrightarrow \mathrm{SO}_m \longrightarrow \mathrm{O}_m \xrightarrow{det} \{\pm 1\} \longrightarrow 1.$$

In fact, $H^1(K, \mathrm{SO}_m) \to H^1(K, \mathrm{O}_m)$ is injective (cf. [Knu+98, §29.E]), but we will not need this fact.

Given $\alpha \in (L_2^\times / L_2^{\times 2})$ that maps to the trivial element in $H^1(K, G')$, we will show how to construct a rational orbit from it. An element $\alpha \in L_2^\times$ can be lifted to an element of $L_1^\times \cong K^\times \times L_2^\times$ by simply considering $(1, \alpha) \in L_1^\times$. Moreover, as in last section, we can naturally embed $L_1 \hookrightarrow M$, so given $\alpha \in (L_2^\times / L_2^{\times 2})$ we can naturally consider it as an element of M. Under this identification, consider the quadratic form $(\cdot,\cdot)_\alpha \colon M \times M \to K$ defined by

$$(\lambda, \mu)_\alpha = \text{ coefficient of } \beta^{4n} \text{ in } \alpha^{-1}\lambda\mu. \tag{2}$$

As before, this quadratic form splits as a direct sum of quadratic forms in L_1 and βL_2. If α has norm 1 (up to squares) in L_2, then both forms have discriminant 1, so they give a well-defined map to $H^1(K, G')$. Unwinding the definitions similarly to [BG14, §5], the condition that α lands in the kernel of $H^1(K, G')$ translates precisely to both forms $(\cdot,\cdot)_\alpha|_{L_1}$ and $(\cdot,\cdot)_\alpha|_{\beta L_2}$ being split of discriminant 1. Therefore, under

appropriate change of bases in L_1 and L_2, the map T_β given an element of $V(K)$ in the same way as in the distinguished case.

Thus, given $\alpha \in (L_2^\times/L_2^{\times 2})_{N\equiv 1}$ which maps to the trivial element of $H^1(K, G')$, we have constructed a rational $G'(K)$-orbit.

We now turn our attention to $G(K)$-orbits. Following [BGW15, §4.3], there is a map $H^1(K, (\mathrm{Res}_{L_2/K}\,\mu_2)_{N=1}) \to (L_2^\times/L_2^{\times 2})_{N\equiv 1}$ which is either bijective or 2-to-1, according to whether $f(x)$ has an odd degree factor over K or not, which in turn happens depending on whether $L_2^\times[2]$ has an element of norm -1 or not. Therefore, a $G'(K)$-orbit in $V(K)$ splits in either one or two $G(K)$-orbits. In the case where $f(x)$ does not have an odd degree factor over K, we note that the stabiliser over K of the constructed v over $\mathrm{SO}_{2n+1} \times \mathrm{SO}_{2n}$ is the same as the stabiliser over $\mathrm{SO}_{2n+1} \times \mathrm{O}_{2n}$. By choosing $h \in \mathrm{O}_{2n}(K) \setminus \mathrm{SO}_{2n}(K)$, we can obtain a new orbit by just considering the element $(1, h) \cdot v$. If $f(x)$ has an odd degree factor over K, the constructed orbits coincide. We summarise our results as follows:

Theorem 2.5. *Let $b \in B(K)$ with $\Delta(b) \neq 0$. Then, the set of $G(K)$-orbits in $V_b(K)$ are in bijection with the set of equivalence classes (α, s), where $\alpha \in (L_2^\times)_{N\equiv 1}$ maps to the trivial element in $H^1(K, G)$ and $s \in K^\times$ satisfies $N(\alpha) = s^2$. Two pairs (α, s) and (α', s') are equivalent if there exists $c \in L_2^\times$ such that $\alpha' = c^2\alpha$ and $s' = N(c)s$. The stabiliser of such an orbit is isomorphic to $(\mathrm{Res}_{L_2/K}\,\mu_2)_{N=1}$.*

It will be convenient for us later to introduce the notion of reducible and irreducible orbits:

Definition 2.6. Let $v \in V_b(K)$ with $b = \pi(v)$. We say that v is K-reducible if either $\Delta(b) = 0$ or if v maps to the trivial element in the composition

$$G(K)\backslash V_b(K) \to H^1(K, (\mathrm{Res}_{L_2/K}\,\mu_2)_{N=1}) \to \left(\frac{L_2}{L_2^{\times 2}}\right)_{N\equiv 1}.$$

We say that v is K-irreducible if it is not K-reducible.

Equivalently, $v \in V_b(K)$ is K-reducible if it is $(\mathrm{SO}_{2n+1} \times \mathrm{O}_{2n})(K)$-equivalent to the distinguished orbit constructed in Section 2.2.1. Note that the notion of reducibility depends on the base field. If K is algebraically closed, every element is K-reducible. We will typically refer to $\mathbb{Q}$-(ir)reducible elements simply as (ir)reducible. We also note that there might be one or two K-reducible $G(K)$-orbits with a given invariant $b \in B^{rs}(K)$.

We will now give an alternative, more explicit description of reducibility. Recall that an element $v \in V(K)$ corresponds to $(2n + 1) \times 2n$ matrix A, which can in turn be viewed as a linear map $A\colon L_2 \to L_1$. Under this convention, we can also view A^* as a linear map $A^*\colon L_1 \to L_2$.

Proposition 2.7. *Let $b \in B^{rs}(K)$. An orbit $v \in V_b(K)$ corresponding to a $(2n + 1) \times 2n$ matrix A is K-reducible if and only if there exists a K-rational space $X \subset L_1$ of dimension n such that $AA^*X \subset X^\perp$.*

Proof. Assume that b corresponds to the invariant polynomial $f(x)$. From $v \in V_b(K)$ and its corresponding matrix A, the matrix AA^* is a $(2n+1)\times(2n+1)$ matrix with characteristic polynomial $f(x)$, and the action of $(g, h) \in G(K)$ transforms AA^* as $(g, h) \cdot (AA^*) = gAA^*g^{-1}$ (noting that $g^{-1} = g^*$). Denoting $G' = \mathrm{SO}_{2n+1}$ and $V' = \mathrm{Sym}^2(2n + 1)$, we get a natural map $G(K)\backslash V_b(K) \to G'(K)\backslash V_b'(K)$. Note that (G', V') is the representation studied in [BG13]. In there, an operator $T\colon L_1 \to L_1 \in V_b'(K)$ is called *distinguished* if and only if there exists an n-dimensional isotropic subspace $X \subset L_1$ with $TX \subset X^\perp$. Furthermore, there is an injective map $G'(K)\backslash V_b'(K) \to (L_1^\times/L_1^{\times 2})_{N\equiv 1} \cong (L_2^\times/L_2^{\times 2})$ under which the (unique) distinguished $G'(K)$-orbit in $V_b'(K)$ maps to the trivial element. The proof concludes by observing that the diagram

$$\begin{array}{ccc} G(K)\backslash V_b(K) & \longrightarrow & G'(K)\backslash V_b'(K) \\ \downarrow & & \downarrow \\ (L_2^\times/L_2^{\times 2})_{N\equiv 1} & \longrightarrow & (L_2^\times/L_2^{\times 2}) \end{array}$$

is commutative, which follows from unpacking the definitions in [BG13]. □

2.3 Connection with hyperelliptic curves

Let $b \in B^{rs}(K)$ correspond to the polynomial $f(x) \in K[x]$ with $\deg f = 2n$. Consider the hyperelliptic curve $C_b\colon y^2 = xf(x)$ and its Jacobian $J_b := \mathrm{Jac}(C_b)$. If the discriminant of $xf(x)$ is non-zero, then the roots $x_0 = 0, x_1, \ldots, x_{2n}$ of $xf(x)$ over $\overline{K}$ are all different. If we denote $P_i = (x_i, 0)$ and ∞ is the point at infinity, then $J_b[2](\overline{K})$ is generated by the elements $(P_i) - (\infty)$, with the only relation that $\sum_{i=0}^{2n}((P_i) - (\infty)) = 0$.

Consider the order 2 subgroup $M \subset J_b[2]$ generated by $T = (0, 0)$, and consider its orthogonal complement $M^\perp$ under the Weil pairing. Note that $M \leq M^\perp$ and that $M^\perp(\overline{K})$ has size 2^{2n-1}. We can construct some isogenies as explained in the introduction, there are isogenies (see (1)).

$$J_b \xrightarrow{\phi_M} A_b \xrightarrow{\phi} A_b^\vee \xrightarrow{\hat{\psi}} J_b,$$

with $J_b[\phi_M] = M$, if $\psi = \phi \circ \phi_M$ then $J_b[\psi] = M^\perp$ and the whole composition is the multiplication-by-2 map.

Proposition 2.8. *Let $v \in V(K)$ with $\Delta(v) \neq 0$. Then,* $\mathrm{Stab}_G(v) \cong J_b[\psi]$.

Proof. It suffices to show that $J_b[\psi] \cong (\mathrm{Res}_{L_2/K}\, \mu_2)_{N=1}$, which is an elementary computation. □

Note that we also have that we have the injective descent map $A_b^\vee(K)/\psi(J_b(K)) \hookrightarrow H^1(K, J_b[\psi])$. It is then natural to ask whether the elements of $A_b^\vee(K)/\psi(J_b(K))$ actually correspond to $G_b(K)$-orbits in $V_b(K)$.

Theorem 2.9. *The natural composition*

$$A_b^\vee(K)/\psi(J_b(K)) \xrightarrow{\eta_b} H^1(K, J_b[\psi]) \to H^1(K, G)$$

is trivial.

Definition 2.10. We will say an element $v \in V^{rs}(K)$ is *K-soluble* if $v \in \eta_b(A_b^\vee(K)/\psi(J_b(K)))$.

It is not so obvious what an explicit description of the map $A_b^\vee(K)/\psi(J_b(K)) \to H^1(K, J_b[\psi])$ should be. However, we can try to simplify the situation by trying to relate it to the 2-descent map $J_b(K)/2J_b(K) \to H^1(K, J_b[2])$. Consider the group $G' = \mathrm{SO}_{2n+1} \times \mathrm{O}_{2n}$: similarly to Proposition 2.8, we can see that $\mathrm{Stab}_{G'}(v) \cong \mathrm{Res}_{L_1/K}(\mu_2) \cong J_b[2]$. We then have the following commutative diagram:

$$\begin{array}{ccc} A_b^\vee(K)/\psi(J_b(K)) & \longrightarrow & J_b(K)/2J_b(K) \\ \downarrow{\scriptstyle \delta_\psi} & & \downarrow{\scriptstyle \delta_2} \\ H^1(K, J_b[\psi]) & \xrightarrow{\iota} & H^1(K, J_b[2]) \\ \downarrow & & \downarrow \\ H^1(K, G) & \longrightarrow & H^1(K, G') \end{array} \tag{3}$$

The map $H^1(K, J_b[2]) \to H^1(K, G') \cong H^1(K, \mathrm{SO}_{2n+1}) \times H^1(K, \mathrm{O}_{2n})$ can be given using the same recipe as in Section 2.2.2. Explicitly, given $\alpha \in H^1(K, J_b[2])$, which can be viewed both as an element of $L_2^\times/L_2^{\times 2}$ and as an element of $(L_1^\times/L_1^{\times 2})_{N\equiv 1}$ via $\alpha \mapsto (N_{L_2/K}(\alpha), \alpha) \in K^\times \times L_2^\times \cong L_1^\times$, we obtain two quadratic spaces $(\cdot,\cdot)_\alpha^{(1)}\colon L_1 \times L_1 \to K$ and $(\cdot,\cdot)_\alpha^{(2)}\colon L_2 \times L_2 \to K$ given by

$$(\mu, \lambda)_\alpha^{(1)} = \text{ coefficient of } \beta_1^{2n} \text{ in } \alpha^{-1}\mu\lambda \text{ (inside } L_1)$$

and

$$(\mu, \lambda)_\alpha^{(2)} = \text{ coefficient of } \beta_2^{2n-1} \text{ in } \alpha^{-1}\mu\lambda \text{ (inside } L_2),$$

where we are writing $L_1 = K\langle 1, \beta, \dots, \beta^{2n}\rangle$ and $L_2 = K\langle 1, \beta, \dots, \beta^{2n-1}\rangle$. Alternatively, if we consider the codimension 1 vector subspace $\beta_1 L_1$ of L_1, we have that for $(\cdot,\cdot)_\alpha^{(2)}$ is equivalent to a form $(\cdot,\cdot)_\alpha^{(2')}\colon \beta_1 L_1 \times \beta_1 L_1 \to K$ given by $(\beta_1\mu, \beta_1\lambda)_\alpha^{(2')} := (\mu, \beta_1\lambda)_\alpha^{(1)}$ (we can check that this is well-defined).

The image of any given $\alpha \in H^1(K, J_b[2])$ in $H^1(K, \mathrm{SO}_{2n+1}) \times H^1(K, \mathrm{O}_{2n})$ is given by the quadratic spaces $(L_1, (\cdot,\cdot)_\alpha^{(1)})$ and $(L_2, (\cdot,\cdot)_\alpha^{(2)})$, and these quadratic spaces will correspond to the trivial element if and only if they are split of discriminant 1. We note that the discriminant of $(\cdot,\cdot)_\alpha^{(1)}$ is 1, while the discriminant of $(\cdot,\cdot)_\alpha^{(2)}$ is equal to $N_{L_2/K}(\alpha)$. Therefore, it is not necessarily the case that the composition $J_b(K)/2J_b(K) \xrightarrow{\delta_2} H^1(K, J_b[2]) \to H^1(K, G')$ is trivial: it is a necessary condition that $N_{L_2/K}(\alpha) \in K^{\times 2}$.

Recall that there is a surjective map $H^1(K, J_b[\psi]) \to (L_2^\times/L_2^{\times 2})_{N\equiv 1}$, which is either bijective or 2-to-1. Then, the map $\iota\colon H^1(K, J_b[\psi]) \to H^1(K, J_b[2]) \cong L_2^\times/L_2^{\times 2}$ is just given by the natural inclusion $H^1(K, J_b[\psi]) \to (L_2^\times/L_2^{\times 2})_{N\equiv 1} \to L_2^\times/L_2^{\times 2}$.

Lemma 2.11. *Let $[D] \in J_b(K)/2J_b(K)$, and suppose that $\delta_2([D]) \in \mathrm{Im}(\iota)$. Then, the image of $\delta_2([D])$ in $H^1(K, G')$ is trivial.*

Proof. We start by recounting the proof of [BG13, Proposition 5.2]. Consider the two quadrics in $L_1 \oplus K$ given by

$$Q_1(\lambda, a) = (\lambda,\lambda)_\alpha^{(1)}, \quad Q_2(\lambda, a) = (\lambda, \beta_1\lambda)_\alpha^{(1)} + a^2.$$

Then, it is shown in *loc. cit.* that there exists a rational n-dimensional subspace Y of $L_1 \oplus K$ which is isotropic with respect to both Q_1 and Q_2. In particular, given that the line $0 \oplus K$ is not contained in Y, we see that the projection of Y to L_1 is an n-dimensional isotropic subspace of Q_1, thus showing that $(\cdot,\cdot)_\alpha^{(1)}$ is split.

Now, consider the subspace $Y' = Y \cap (L_1 \oplus 0)$, of dimension at least $n-1$. We see that $Y' \cap f(\beta_1)L_1 = \{0\}$, as $(f(\beta_1), f(\beta_1))_\alpha^{(1)} = N_{L_2/K}(\alpha^{-1})N_{L_2/K}(\beta_1) \neq 0$. Therefore, the subspace $\beta_1 Y'$ of $\beta_1 L_1$ has dimension at least $n-1$, and it is also the case that for any $\beta_1\mu, \beta_1\lambda \in \beta_1 Y'$ we have that $(\beta_1\mu, \beta_1\lambda)_\alpha^{(2')} = (\mu, \beta_1\lambda)_\alpha^{(1)} = 0$ by construction. Therefore, $(\cdot,\cdot)_\alpha^{(2)}$ has a rational isotropic space of dimension $n-1$ and thus, as a quadratic space, we have that $(L_2, (\cdot,\cdot)_\alpha^{(2)}) \cong H^{n-1} \oplus V'$, where $H \sim \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$. But V' is a quadratic space of dimension 2 and discriminant 1 (by hypothesis), and therefore $V' \sim H$ as well, showing that $(\cdot,\cdot)_\alpha^{(2)}$ is split, as wanted. □

Proof of Theorem 2.9. First, note that the map $H^1(K, G) \to H^1(K, G')$ has a trivial pointed kernel, which is equivalent to $H^1(K, \mathrm{SO}_{2n}) \to H^1(K, \mathrm{O}_{2n})$ having a trivial pointed kernel, as noted in Section 2.2.2. Then, the proof follows from Lemma 2.11 and the commutativity of the diagram (3). □

Remark 2.12. Let $A_b^\vee[\hat{\psi}] = \{0, T_A\}$. Then, both 0 and T_A give distinguished orbits of $G(K)\backslash V_b(K)$. Whether or not these two orbits coincide depends on whether $T_A \in \psi(J_b(K))$.

Corollary 2.13. *Let K be a number field, and let $b \in B(K)$ with $\Delta(b) \neq 0$. Then, there is an embedding*

$$\mathrm{Sel}_\psi(J_b) \hookrightarrow G(K)\backslash V_b(K).$$

Proof. Consider the commutative diagram

$$\begin{array}{ccccc} A_b^\vee(K)/\psi(J_b(K)) & \longrightarrow & H^1(K, J_b[\psi]) & \longrightarrow & H^1(K, G) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_v A_b^\vee(K_v)/\psi(J_b(K_v)) & \xrightarrow{\delta_{\psi,v}} & \prod_v H^1(K_v, J_b[\psi]) & \longrightarrow & \prod_v H^1(K_v, G), \end{array}$$

where the product is taken over all finite places v of K. Recall that $\mathrm{Sel}_\psi(J_b)$ is defined as $\ker(H^1(K, J_b[\psi]) \to \prod_v H^1(K_v, J_b[\psi])/(\mathrm{Im}(\delta_{\psi,v})))$. Our statement then follows from the fact that the composition of maps in

the second row is trivial by Theorem 2.9, and the fact that the map $H^1(K,G) \to \prod_v H^1(K_v,G)$ has trivial kernel (see e.g. [Lag24, Proposition 6.8]). □

2.4 Integral orbits

To prove our main theorems, we will require an integral version of Corollary 2.13. We remark that even though we have originally constructed our representation over K, a field of characteristic zero, we could also have constructed (G,V) over $\mathbb{Z}$. In this case, we also have $B = \operatorname{Spec} \mathbb{Z}[p_2,\dots,p_{4n}]$.

Theorem 2.14. *The image of the map*

$$\mathrm{Sel}_\psi(J_b) \hookrightarrow G(\mathbb{Q})\backslash V_b(\mathbb{Q}).$$

falls inside $\frac{1}{2}V_b(\mathbb{Z})$.

Because G has class number 1 (cf. [Lag24, Proposition 7.2]), it will suffice to see that the map

$$A_b^\vee(\mathbb{Q}_p)/\psi(J(\mathbb{Q}_p)) \hookrightarrow G(\mathbb{Q}_p)\backslash V_b(\mathbb{Q}_p)$$

falls inside $\frac{1}{2}V(\mathbb{Z}_p)$ for all p. We start by giving an ideal parametrisation of integral orbits inside $\mathbb{Z}_p$, in an analogous way to other results in the literature, such as [Sha19, Proposition 6.7]. For the proof of Theorem 2.14, we will need to know when a $\mathbb{Z}_p$-lattice L of dimension m with a given symmetric bilinear form $L \times L \to \mathbb{Z}_p$ is isometric over $\mathbb{Z}_p$ to an m-dimensional lattice L_m with matrix J_m. We summarise known results on this next lemma:

Lemma 2.15. *Let I be a $\mathbb{Z}_p$-module of rank m equipped with a symmetric bilinear form $\varphi\colon I \times I \to \mathbb{Z}_p$ of discriminant 1.*

- *If $p \neq 2$, then I is isometric to L_m over $\mathbb{Z}_p$.*
- *If $p = 2$ and $m = 2m'+1$, then I is isometric to L_m over $\mathbb{Z}_2$ if $I \otimes \mathbb{Q}_2$ is a split orthogonal space.*
- *If $p = 2$ and $m = 2m'$, then I is isometric to L_m over $\mathbb{Z}_2$ if $I \otimes \mathbb{Q}_2$ is a split orthogonal space and I is an even lattice (i.e. $\varphi(x,x) \in 2\mathbb{Z}_2$ for all $x \in I$).*

In the last item, the condition that I is an even lattice is necessary, as (L_m, J_m) admits both an even and an odd lattice over $\mathbb{Z}_2$. These two lattices can be transformed to one another via an element of $\mathrm{O}_m(\mathbb{Q}_2)$ with coefficients in $\frac{1}{2}\mathbb{Z}_2$.

Proposition 2.16. *Let $b \in B(\mathbb{Z}_p)$ with $\Delta(b) \neq 0$. Then, the set of orbits $G(\mathbb{Z}_p)\backslash V_b(\mathbb{Z}_p)$ is in bijection with the equivalence classes of (I_1, I_2, α, s), where I_1 is a fractional ideal of R_1, I_2 is a fractional ideal of R_2, $\alpha \in (L_2^\times)_{N\equiv 1}$ and $s \in K^\times$; satisfying:*

1. *$I_1^2 \subset \alpha R_1$ and $N(I_1)^2 = N_{L_1/\mathbb{Q}_p}(\alpha)$, where α can be interpreted as an element of $L_1 \cong \mathbb{Q}_p \times L_2$ via $\alpha \mapsto (N_{L_2/\mathbb{Q}_p}(\alpha), \alpha)$.*
2. *$I_2^2 \subset \alpha R_2$ and $N(I_2)^2 = N_{L_2/\mathbb{Q}_p}(\alpha)$.*
3. *Let $\overline{I_1}$ denote the projection of I_1 in L_2, and let $\overline{I_1}' = \{\gamma \in L_2 \mid (0,\beta_1\gamma) \in I_1\}$. Then, $\overline{I_1} \subset I_2 \subset \overline{I_1}'$.*
4. *The forms $(\cdot,\cdot)_\alpha^{(1)}$ and $(\cdot,\cdot)_\alpha^{(2)}$ are split of discriminant 1 over $\mathbb{Q}_p$.*
5. *I_2 is even with respect to $(\cdot,\cdot)_\alpha^{(2)}$.*
6. *$N_{L_2/\mathbb{Q}_p}(\alpha) = s^2$.*

Two such tuples (I_1, I_2, α, s) and $(I_1', I_2', \alpha', s')$ are equivalent if and only if there exists an element $c \in L_2^\times$ such that $I_1 = cI_1'$, $I_2 = cI_2'$, $\alpha = c^2\alpha'$ and $s = N_{L_2/\mathbb{Q}_p}(c)s'$. An integral orbit (I_1, I_2, α, s) corresponds to the rational orbit given by (α, s).

Proof. First, we start with a tuple (I_1, I_2, α, s) and we construct an orbit in $G(\mathbb{Z}_p)\backslash V_b(\mathbb{Z}_p)$. First, we note that the forms $(\cdot,\cdot)_\alpha^{(1)}$ and $(\cdot,\cdot)_\alpha^{(2)}$, when restricted to I_1 and I_2 respectively, take integral values and are split of discriminant 1. Therefore, we can find $\mathbb{Z}_p$-bases for I_1 and I_2 such that the forms have Gram matrices J_{2n+1} and J_{2n} respecively. Then, also by construction we have that the matrix of T_β has values in $\mathbb{Z}_p$, so it gives an element of $V_b(\mathbb{Z}_p)$.

Now, suppose that we start with an orbit in $G(\mathbb{Z}_p)\backslash V_b(\mathbb{Z}_p)$. Theorem 2.5 gives (α, s) and hence properties 4 and 6. We recall that such an orbit can be constructed as the matrix of T_β in $M = \mathbb{Q}_p[x]/(xf(x^2))$. Given a basis $\{e_1, \dots, e_{4n+1}\}$ of M, the action of T_β realizes $J = \mathbb{Z}_p\langle e_1, \dots, e_{4n+1}\rangle$ as an $R = \mathbb{Z}_p[x]/(xf(x^2))$-submodule. Note that $R \cong R_1 \oplus \beta R_2$. The fact that T_β respects R_1 and R_2 implies that $J = I_1 + \beta I_2$ for some fractional ideals I_1 in R_1 and I_2 in R_2, which necessarily satisfy $\overline{I_1} \subset I_2 \subset \overline{I_1}'$. The fact that the forms $(\cdot,\cdot)_\alpha^{(1)}$ and $(\cdot,\cdot)_\alpha^{(2)}$ have to be self-dual with respect to I_1 and I_2 with matrices isometric to J_{2n+1} and J_{2n} over $\mathbb{Z}_p$, respectively, give the rest of the hypotheses.

These two constructions are inverse to each other, and so we are done. □

Proof of Theorem 2.14. It suffices to show that for every element of $\hat{A}_b(\mathbb{Q}_p)/\psi(J_b(\mathbb{Q}_p))$ there is a tuple (I_1, I_2, α, s) satisfying the conditions of Proposition 2.16. We note that splitness of the forms over $\mathbb{Q}_p$ follows from Theorem 2.9. Furthermore, by [LT24, Lemma 4.9] (cf. [BG13, Proposition 8.5]), there exists a fractional ideal I_1 in R_1 such that $I_1^2 \subset \alpha R_1$ with $N(I_1)^2 = N_{L_1/\mathbb{Q}_p}(\alpha)$.

We can observe that when reducing to R_2, the lattices $\overline{I_1}$ and $\overline{I_1}'$ are dual to each other with respect to the form $(\cdot,\cdot)_\alpha^{(2)}$. This follows from observing that for any $\mu, \lambda \in L_2$ with liftings $\mu', \lambda' \in L_1$ we have that

$$(\mu, \lambda)_\alpha^{(2)} = (\mu', \beta\lambda')_\alpha^{(1)}.$$

Then, the process of finding a fractional ideal I_2 with the required conditions reduces to finding a lattice $\overline{I_1} \subset \Lambda \subset \overline{I_1}'$ which is self-dual and is stable under multiplication by β_2, up to considerations at $p = 2$. We further observe that any lattice Λ satisfying $\overline{I_1} \subset \Lambda \subset \overline{I_1}'$ is automatically stable under $\times\beta_2$, so it automatically is a fractional ideal.

We split our the rest of our proof in the two cases $p \neq 2$ and $p = 2$, in a similar way to [Sha19, Propositions 6.9, 6.11].

- $p \neq 2$: By [Cas78, Lemma 3.4] we can find a basis (f_i) of $\overline{I_1}$ such that its Gram matrix with respect to $(\cdot,\cdot)_\alpha^{(2)}$ is

$$\begin{pmatrix} u_1 p^{a_1} & & & \\ & u_2 p^{a_2} & & \\ & & \ddots & \\ & & & u_{2n} p^{a_{2n}} \end{pmatrix}$$

  where the a_i are non-negative integers and $u_i \in \mathbb{Z}_p^\times$. By substituting f_i by $p^{-\lfloor \frac{a_i}{2} \rfloor} f_i$, we may assume that $a_i \in \{0, 1\}$, and the resulting lattice Λ still satisfies $\overline{I_1} \subset \Lambda \subset \overline{I_1}'$. Write $\Lambda = \Lambda_0 \oplus \Lambda_1$, where Λ_i is the span of those f_j with $b_j = i$ $(i = 0, 1)$. Given that the discriminant of the form is 1 modulo squares, the dimensions of both Λ_0 and Λ_1 have to be even. We will now see that both $\Lambda_0 \otimes \mathbb{Q}_p$ and $\Lambda_1 \otimes \mathbb{Q}_p$ are split quadratic spaces.

  Let Λ_0 be spanned by $(f_1, \dots, f_{2a})$ and let Λ_1 be spanned by $(f_{2a+1}, \dots, f_{2n})$. Then, the discriminant of $\Lambda_0 \otimes \mathbb{Q}_p$ is $(-1)^a \prod_{i=1}^{2a} u_i$ and the Hasse invariant is 1, as $(u_i, u_j)_p = 1$ for all $u_i, u_j \in \mathbb{Z}_p^\times$. On the other hand, the discriminant of $\Lambda_1 \otimes \mathbb{Q}_p$ is $(-1)^{n-a} \prod_{i=2a+1}^{2n} u_i$ and its Hasse invariant is

$(-1)^{(n-a)(p-1)/2}\prod_{i=2a+1}^{p}\left(\frac{u_i}{p}\right)$. A straightforward computation shows that the Hasse invariant of $(\Lambda_0 \oplus \Lambda_1) \otimes \mathbb{Q}_p$ is equal to the Hasse invariant of $\Lambda_1 \otimes \mathbb{Q}_p$, so both these invariants are equal to 1. Given that $(-1)^{(n-a)(p-1)/2}$ is equal to $(-1)^{n-a}$ up to squares (indeed, both these quantities are equal to $(-1)^{n-a}$ if $p \equiv 3 \pmod 4$ or equal to 1 modulo squares if $p \equiv 1 \pmod 4$), this forces the discriminant of $\Lambda_1 \otimes \mathbb{Q}_p$ to be equal to 1. Since the discriminant of $(\Lambda_0 \oplus \lambda_1) \otimes \mathbb{Q}_p$ is 1, and also the product of discriminants in Λ_0 and Λ_1, this implies that the discriminant of $\Lambda_0 \otimes \mathbb{Q}_p$ is also 1, proving our claim that both $\Lambda_0 \otimes \mathbb{Q}_p$ and $\Lambda_1 \otimes \mathbb{Q}_p$ are split quadratic spaces.

Thus, we can choose a basis of Λ_0 such that its Gram matrix is J_{2a}, and we can choose a basis of Λ_1 such that its basis is $pJ_{2(n-a)}$. By replacing $f_{2a+1}, \dots, f_{2n}$ by $f_{2a+1}/p, \dots, f_{a+n}/p, f_{a+n+1}, \dots, f_{2n}$, we get the matrix $J_{2(n-a)}$. Therefore, we obtain a self-dual lattice $\Lambda = \Lambda_0 \oplus \Lambda_1$ with the desired inclusion conditions.

- $p = 2$: In this situation, by [Cas78, Lemma 4.1] we can find a basis of $\overline{I_1}$ such that its Gram matrix with respect to $(\cdot,\cdot)_\alpha^{(2)}$ is
$$\begin{pmatrix} 2^{a_1}Q_1 & & & \\ & 2^{a_2}Q_2 & & \\ & & \ddots & \\ & & & 2^{a_k}Q_k \end{pmatrix},$$
where $a_i \geq 0$ and the Q_i are either 1×1 matrices with an entry in $\mathbb{Z}_p^\times$ or 2×2 matrices of the form
$$Q_i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{or} \quad Q_i = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$
As before, we may assume that $a_i \in \{0, 1\}$. For the 2×2 matrices, we may further assume that $a_i = 0$: if $a_i = 1$, we may substitute e_1 for $e_1/2$ to get a self-dual lattice. Therefore, we may assume that the Gram matrix is of the form
$$\begin{pmatrix} 2U & & & \\ & Q_2 & & \\ & & \ddots & \\ & & & Q_k \end{pmatrix},$$
where U is a diagonal matrix of size $2a \times 2a$ with unit entries, and the Q_i are either 1×1 or 2×2 matrices with unit determinant. Finally, we notice that for a matrix $\begin{pmatrix} 2u_1 & 0 \\ 0 & 2u_2 \end{pmatrix}$ with $u_1, u_2 \in \mathbb{Z}_p^\times$, the basis spanned by $(e_1 + e_2)/2$ and $(e_1 - e_2)/2$ gives a self-dual lattice. We can conclude that there exists a self-dual lattice $\overline{I_1} \subset \Lambda \subset \beta_2^{-1}\overline{I_1}$.

It is not necessarily the case that I_2 is even with respect to the form $(\cdot,\cdot)_\alpha^{(2)}$, so it might not the case that this lattice is isometric to (L_{2n}, J_{2n}) over $\mathbb{Z}_2$. However, it is the case that both lattices are isometric under a matrix in $\mathrm{O}_{2n}(\mathbb{Q}_2)$ with coefficients in $\frac{1}{2}\mathbb{Z}_2$. Thus, the given tuple (I_1, I_2, α, s) yields an orbit in $\frac{1}{2}V(\mathbb{Z})$.

□

3 The resolvent form

As before, let K be a field of characteristic zero. Consider an element $A \in V(K)$ as a $(2n+1) \times 2n$ matrix with entries in K and associated characteristic polynomial $f(x)$. Then, A^*A is a $2n \times 2n$ matrix that is symmetric along the antidiagonal and has characteristic polynomial $f(x)$. We get an action of $(g, h) \in \mathrm{SO}_{2n+1} \times \mathrm{SO}_{2n}$ act on A^*A by $(g, h) \cdot (A^*A) = hA^*Ah^*$.

Let $\mathrm{PSO}_{2n} = \mathrm{SO}_{2n}/\mu_2$. Then, we define the representation $(G^*, V^*) = (\mathrm{PSO}_{2n}, \mathrm{Sym}^2(2n))$, where $\mathrm{Sym}^2(2n)$ denotes the $2n \times 2n$ matrices that are symmetric along the antidiagonal, and G^* acts by conjugation on these

matrices. This is (up to a trace zero condition) the same representation that was studied in [SW18]. The ring of invariants of (G^*, V^*) is generated by the coefficients of the characteristic polynomials of the matrices of V^*, and hence we have an isomorphism between $B^* := V^* /\!\!/ G^*$ and B. We note, however, that the degrees of the elements of B^* are half the degrees of the corresponding invariants in B.

3.1 Rational orbits

We recall [SW18, Proposition 2.1].

Proposition 3.1. *Let $b \in B^{rs}(K)$ with $\Delta(b) \neq 0$. If the associated characteristic polynomial is $f(x)$, write $L = K[x]/(f(x))$. Then, if $v \in V_b^*(K)$, then $\mathrm{Stab}_{G^*}(v) \cong (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2$.*

Therefore, by Proposition 2.3, if $b \in B^{rs}(K)$ the $G^*(K)$-orbits in $V_b^*(K)$ are in bijection with the pointed kernel of

$$H^1(K, (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2) \to H^1(K, \mathrm{SO}_{2n}).$$

Similarly to (G, V), there is a map $H^1(K, (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2) \to (L^\times/K^\times L^{\times 2})_{N\equiv 1}$ which is bijective or 2-to-1 according to whether the norm map $N\colon (\mathrm{Res}_{L/K}\,\mu_2)\mu_2(K) \to \mu_2$ is surjective or not (see [SW18, Proposition 2.2] for a more explicit description).

Let β denote the image of x inside L, so that L has a K-basis $1, \beta, \ldots, \beta^{2n-1}$. Given $\alpha \in (L^\times/K^\times L^{\times 2})_{N\equiv 1}$, we can define the form $(\cdot,\cdot)_\alpha\colon L \times L \to K$ by

$$(\mu, \lambda)_\alpha = \text{coefficient of } \beta^{2n-1} \text{ in } \alpha^{-1}\mu\lambda.$$

This form has discriminant 1, up to squares. Then, we have (cf. [SW18, Theorem 2.6]):

Theorem 3.2. *There is a bijection between $\mathrm{PO}(K)$-orbits in $V_b^*(K)$ and elements $\alpha \in (L^\times/K^\times L^{\times 2})_{N\equiv 1}$ such that $(\cdot,\cdot)_\alpha$ is split. These $\mathrm{PO}(K)$-orbits split into one or two $\mathrm{PSO}(K)$-orbits according to whether the norm map on $(\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2$ is surjective or not, respectively.*

Let $b \in B^{rs}(K)$ correspond to the invariant polynomial $f(x)$, and consider the hyperelliptic curve $C_b\colon y^2 = xf(x)$ with Jacobian $J_b = \mathrm{Jac}(C_b)$. We recall the setup of (1):

$$J_b \xrightarrow{\phi_M} A_b \xrightarrow{\phi} A_b^\vee \to J_b$$

where $J_b[\phi_M] = M$, $J_b[\phi \circ \phi_M] = M^\perp$ and the whole composition $J_b \to J_b$ is multiplication-by-2. In particular, we have that $A_b[\phi]$ is isomorphic to $M^\perp/M$. First, we note the following fact:

Lemma 3.3. *The isogeny $\phi\colon A_b \to A_b^\vee$ is self-dual.*

Proof. As suggested by the notation, the abelian varieties A_b and $A_b^\vee$ are indeed dual to each other. It is a general fact of principally polarised abelian varieties that $(J/M)^\vee \simeq J/M^\perp$, which follows from the properties of the Weil pairing. Moreover, the finite group scheme $M^\perp/M$ is isomorphic to its own Cartier dual, so the dual isogeny $\phi^\vee\colon A_b \to A_b^\vee$ can be identified with ϕ. □

We also observe the following fact about the stabiliser:

Lemma 3.4. *Under the above notation, we have $(\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2 \cong M^\perp/M$.*

This follows immediately from Proposition 2.8. Therefore, we have a map

$$A_b^\vee(K)/\phi(A_b(K)) \hookrightarrow H^1(K, (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2).$$

Theorem 3.5. *The composition*

$$A_b^\vee(K)/\phi(A_b(K)) \hookrightarrow H^1(K, (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2) \to H^1(K, G)$$

is trivial.

Proof. Note there's a commutative diagram

$$\begin{array}{ccc} A_b^\vee(K)/\psi(J_b(K)) & \longrightarrow & A_b^\vee(K)/\phi(A_b(K)) \\ \downarrow & & \downarrow \\ H^1(K, J_b[\psi]) & \longrightarrow & H^1(K, A_b[\phi]) \\ \downarrow & & \downarrow \\ H^1(K, G) & \longrightarrow & H^1(K, G^*) \end{array}$$

Theorem 2.9 shows that the composition in the first column is trivial. The map in the first row is surjective, and the map in the last row is just the forgetful map $H^1(K, \mathrm{SO}_{2n+1} \times \mathrm{SO}_{2n}) \to H^1(K, \mathrm{SO}_{2n})$. The result follows. □

Therefore, for all $b \in B^{rs}(K)$ there is a map

$$A_b^\vee(K)/\phi(A_b(K)) \xhookrightarrow{\eta_b^*} G^*(K)\backslash V_b^*(K), \tag{4}$$

and similarly to the last section we will call a $G^*(K)$-orbit in $V_b^*(K)$ K-soluble if it intersects the image of η_b^*. If K is a number field, we say that an orbit is locally soluble if it is K_v soluble for all completions K_v. The same proof as in Corollary 2.13 yields

Corollary 3.6. *Let K be a number field. Then, for $b \in B^{rs}(K)$ we have*

$$\mathrm{Sel}_\phi(A_b) \hookrightarrow G^*(K)\backslash V_b^*(K).$$

In [SW18], a $G^*(K)$-orbit in $V_b^*(K)$ is called *reducible* (or distinguished) if it maps to the element $\alpha = 1$ in

$$H^1(K, (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2) \to (L^\times/K^\times L^{\times 2})_{N\equiv 1}.$$

More precisely, in [SW18, §2.2] a distinguished orbit v_b is constructed, and a $\mathrm{PSO}_{2n}(K)$-orbit is called distinguished if it is $\mathrm{PO}_{2n}(K)$-equivalent to the constructed orbit v_b. This corresponds precisely to the orbits that map to $1 \in (L^\times/K^\times L^{\times 2})_{N\equiv 1}$, of which there are at most two.

3.2 Integral representatives

We will prove the equivalent of Theorem 2.14. To do so, we will use the description of integral orbits in [SW18, §2.4]. We note, however, that there is an oversight in *loc. cit.* in the case $p = 2$; the amended statement should read like that:

Theorem 3.7. *Let $b \in B^{rs}(\mathbb{Z}_2)$ with invariant polynomial $f(x)$, and let $L = \mathbb{Q}_2[x]/(f(x))$ and $R = \mathbb{Z}_2[x]/(f(x))$. There is a bijection between $\mathrm{O}_{2n}(\mathbb{Z}_2)$-orbits in $V_b^*(\mathbb{Z}_2)$ and equivalence classes of (I, α), where $\alpha \in L^\times$ and I is a fractional ideal of R satisfying $I^2 \subset \alpha R$ and $N(I)^2 = N(\alpha)$, **which is even with respect to the form** $(\cdot,\cdot)_\alpha$. Two pairs (I_1, α_1) and (I_2, α_2) are equivalent if there exists $c \in L^\times$ such that $I_1 = cI_2$ and $\alpha_1 = c^2\alpha_2$.*

Remark 3.8. There's a small convention difference in [SW18], where they take α^{-1} where we take α.

The condition of I being even with respect to the form is necessary, and in some cases the constructed ideals in [SW18, §2.4] need not be even. In that case, it can only be guaranteed that the orbit will fall inside $\frac{1}{2}V^*(\mathbb{Z}_2)$.

Theorem 3.9. *Let $b \in B^{rs}(\mathbb{Z})$. Every locally soluble orbit in $V_b^*(\mathbb{Q})$ has a representative in $\frac{1}{2}V_b^*(\mathbb{Z})$.*

Proof. As in the proof of Theorem 2.14, it is enough to see that for all p, the map

$$A_b^\vee(\mathbb{Q}_p)/\phi(A_b(\mathbb{Q}_p)) \hookrightarrow G^*(\mathbb{Q}_p)\backslash V_b^*(\mathbb{Q}_p)$$

always intersects $\frac{1}{2}V_b^*(\mathbb{Z}_p)$. For $p \neq 2$, this is immediate; if a $(2n+1) \times 2n$ matrix A has entries in $\mathbb{Z}_p$, then A^*A also does. For $p = 2$, we note that by Theorem 2.14 and Proposition 2.16 there exists an ideal called I_2 in there satisfying the hypotheses of Theorem 3.7 with the corresponding α of the rational orbit. □

4 Proof of Theorem 1.1

To prove Theorem 1.1, we will use Theorem 3.9 in conjunction with the counting results of [SW18] (which are a particular case of [Lag24, §8]). We start by noting the following result from [Lag23, Lemma 7.1]:

Lemma 4.1. *Let $K = \mathbb{R}$ or $\mathbb{Q}_p$ for some prime p, and write $|\cdot|_K \colon K^\times \to \mathbb{R}_{>0}$ for the normalised absolute value of K. Let A be an abelian variety over K with dual abelian variety $A^\vee$, and let $\lambda \colon A \to A^\vee$ be a self-dual isogeny, which will have degree m^2 for some $m \in \mathbb{Z}_{\geq 1}$. Then, the quantity*

$$c(\lambda) := \frac{\#A^\vee(K)/\lambda(A(K))}{\#A[\lambda](K)}$$

satisfies $c(\lambda) = 1/|m|_K$.

In particular, for our map of interest $\phi \colon A_b \to A_b^\vee$, we will have that

$$c_p(\phi_b) = \begin{cases} 2^{-(n-1)} & \text{if } p = \infty, \\ 2^{(n-1)} & \text{if } p = 2, \\ 1 & \text{otherwise.} \end{cases}$$

We turn our interest into counting $G^*(\mathbb{Z})$-orbits in $V^*(\mathbb{Z})$. We will do so imposing infinitely many congruence conditions:

Definition 4.2. A map $w \colon V^*(\mathbb{Z}) \to [0,1]$ is said to be *defined by infinitely many congruence conditions* if for each prime p there exist functions $w_p \colon V^*(\mathbb{Z}_p) \to [0,1]$ such that

- w_p is $G(\mathbb{Z}_p)$-invariant;
- w_p is locally constant outside the subset $\{v \in V^*(\mathbb{Z}_p) \mid \Delta(v) = 0\}$;

which additionally satisfy $w = \prod_p w_p$.

Consider a $G^*(\mathbb{Z})$-invariant subset $A \subset V^*(\mathbb{Z})$, and let $w \colon V^*(\mathbb{Z}) \to \mathbb{R}$ be a function defined by infinitely many congruence conditions. We denote

$$N_w^*(A, X) = \sum_{v \in G^*(\mathbb{Z})\backslash A_{<X}} \frac{w(v)}{\#\operatorname{Stab}_{G^*(\mathbb{Z})}(v)}.$$

Recall that a $G^*(\mathbb{R})$-orbit in $V_b^*(\mathbb{R})$ is called $\mathbb{R}$-soluble if it falls in the image of η_b^* in (4). Observe that the number of $G^*(\mathbb{R})$-soluble orbits in $V_b^*(\mathbb{R})$ is $\#A_b^\vee(\mathbb{R})/\phi(A_b(\mathbb{R}))$. Then, analogously to [Lag24, Theorem 8.18] we get that

$$N_w^*(A,X) \leq \left(\prod_p \int_{v\in V(\mathbb{Z}_p)} w(v)dv\right) \frac{|W_1|}{2^{n-1}} \operatorname{vol}(G^*(\mathbb{Z})\backslash G^*(\mathbb{R})) \operatorname{vol}(B(\mathbb{R})_{<X}) + o(X^{\dim V^*}),$$

where $W_1 \in \mathbb{Q}^\times$ is a fixed scalar number, and where $w = \prod_p w_p$ are the congruence conditions defining w.

To estimate the size of $\mathrm{Sel}_\phi(A_b)$, we note that the non-trivial torsion point $T_b \in A_b^\vee[\hat{\psi}]$ generates a subgroup S_T in $\mathrm{Sel}_\phi(A_b)$ of order dividing 2. In the map

$$\mathrm{Sel}_\phi(A_b) \hookrightarrow G^*(K)\backslash V_b^*(K),$$

the elements of $\mathrm{Sel}_\phi(A_b)$ which intersect the reducible orbits correspond exactly to the subgroup S_T, and the complement of S_T falls entirely in the irreducible orbits. Given that $\#S_T \leq 2$, it suffices to bound $\mathrm{Sel}_\phi(A_b) \setminus S_T$ by looking at irreducible orbits.

We can prove our results in higher generality by imposing congruence conditions on B. We say that a set $\mathcal{B} \subset B(\mathbb{Z})^{rs}$ is *defined by finitely many congruence conditions* if it is the preimage of the reduction map $B(\mathbb{Z})^{rs} \to B(\mathbb{Z}/N\mathbb{Z})$ for some $N \geq 1$. We will prove the following:

Theorem 4.3. *Let $\mathcal{B} \subset B(\mathbb{Z})$ be defined by finitely many congruence conditions. Then,*

$$\lim_{X\to\infty} \frac{\sum_{b\in\mathcal{B},\, \mathrm{ht}(b)<X} \#(\mathrm{Sel}_\phi(A_b) \setminus S_T)}{\#\{b \in \mathcal{B} \mid \mathrm{ht}(b) < X\}} \leq 4.$$

Proof. Let $\mathcal{B}_p$ denote the closure of $\mathcal{B}$ inside $B^{rs}(\mathbb{Z}_p)$. For our counting result, it will suffice to count those irreducible $G*(\mathbb{Z})$-orbits in $V^*(\mathbb{Z})$ corresponding to Selmer elements, as given by Theorem 3.9. Given that we are only guaranteed to have orbits in $\frac{1}{2}V^*(\mathbb{Z})$, and that $\mathrm{Sel}_\phi(A_b) \simeq \mathrm{Sel}_\phi(A_{\lambda\cdot b})$ for any $\lambda \in \mathbb{Q}^\times$, it will suffice to look at orbits with invariants in $2\cdot\mathcal{B}$, for which Selmer elements will always have integral representatives. We choose the counting function

$$w(v) = \begin{cases} \left(\sum_{v'\in G^*(\mathbb{Z})\backslash(G^*(\mathbb{Q})\cdot v\cap V^*(\mathbb{Z}))} \frac{\#\operatorname{Stab}_{G^*(\mathbb{Q})}(v')}{\#\operatorname{Stab}_{G^*(\mathbb{Z})}(v')}\right)^{-1} & \text{if } \pi(v) \in 2\cdot\mathcal{B} \text{ and } v \text{ is locally soluble,} \\ 0 & \text{otherwise.} \end{cases}$$

This is defined by congruence conditions by the functions

$$w_p(v) = \begin{cases} \left(\sum_{v'\in G^*(\mathbb{Z}_p)\backslash(G^*(\mathbb{Q}_p)\cdot v\cap V^*(\mathbb{Z}_p))} \frac{\#\operatorname{Stab}_{G^*(\mathbb{Q}_p)}(v')}{\#\operatorname{Stab}_{G^*(\mathbb{Z}_p)}(v')}\right)^{-1} & \text{if } \pi(v) \in 2\cdot\mathcal{B}_p \text{ and } v \text{ is soluble,} \\ 0 & \text{otherwise,} \end{cases}$$

by an analogous argument to [BS15a, Proposition 3.6]. The last part of [Lag24, Lemma 8.5] gives

$$\begin{aligned} \int_{v\in V(\mathbb{Z}_p)} w(v)dv &= |W_1|_p \operatorname{vol}(G^*(\mathbb{Z}_p)) \int_{b\in 2\cdot\mathcal{B}_p} \frac{\#A_b^\vee(\mathbb{Q}_p)/\phi(A_b(\mathbb{Q}_p))}{\#A_b[\phi](\mathbb{Q}_p)} db \\ &= |W_1|_p \operatorname{vol}(G^*(\mathbb{Z}_p))|2^{-(n-1)}|_p |2^{n(2n+1)}|_p \operatorname{vol}(\mathcal{B}_p), \end{aligned}$$

using Lemma 4.1 in the last line. Under this counting function, we have that for any given locally soluble $v \in V^*(\mathbb{Z})$ with $\pi(v) \in \mathcal{B}$:

$$\sum_{v'\in G^*(\mathbb{Q})v\cap V^*(\mathbb{Z})} \frac{w(v')}{\#\operatorname{Stab}_{G^*(\mathbb{Z})}(v')} = \frac{1}{\#\operatorname{Stab}_{G^*(\mathbb{Q})}(v)}.$$

100% of the time, this quantity is equal to 1 by [SW18, Proposition 23]. Thus, we have that

$$\sum_{b\in\mathcal{B}_{<X}} \#(\mathrm{Sel}_\phi(A_b) \setminus S_T) = N_w^*(V^*(\mathbb{Z})^{irr} \cap V(\mathbb{R})^{sol}, 2X) + o(X^{n(2n+1)}).$$

With an elementary point-counting argument, we can see that

$$\lim_{X\to\infty} \frac{\prod_p \operatorname{vol}(\mathcal{B}_p)\operatorname{vol}(B(\mathbb{Z})_{<2X})}{\#\{b\in\mathcal{B} \mid \operatorname{ht}(b)<X\}} = 2^{n(2n-1)}.$$

Putting it all together, we have that

$$\frac{N_w^*(V^*(\mathbb{Z})^{irr}\cap V(\mathbb{R})^{sol}, 2X)}{\#\{b\in\mathcal{B} \mid \operatorname{ht}(b)<X\}} \leq \operatorname{vol}(G^*(\mathbb{Z})\backslash G^*(\mathbb{R}))\prod_p \operatorname{vol}(G^*(\mathbb{Z}_p)),$$

which equals the Tamagawa number of $G^* = \mathrm{PSO}_{2n}$, which is 4. This concludes the proof. □

Theorem 1.1 then follows from Theorem 4.3, since S_T has size at most 2.

5 Further heuristics

It seems natural that an analogous result to Theorem 1.1 should hold about the average size of $\mathrm{Sel}_\psi J_b$, using the representation (G,V) and Theorem 2.14. However, following the results in [KL14] for the analogous family in genus 1, there is a reasonable expectation that the average size of $\mathrm{Sel}_\psi J_b$ is unbounded, as long as one assumes that genus 1 phenomena generalises well to higher genus (as has been case with Sel_2 of the complete families, like in [BS15a] and [BG13]). We will now explain what can be said about $\mathrm{Sel}_\psi J_b$ with the tools we have at our disposal.

Using a standard diagram chase (cf. [Bha+19, Lemma 9.1]), we get the following exact sequence:

$$A_b[\phi](\mathbb{Q})/\phi_M(J_b[\psi](\mathbb{Q})) \longrightarrow \mathrm{Sel}_{\phi_M} J_b \longrightarrow \mathrm{Sel}_\psi J_b \longrightarrow \mathrm{Sel}_\phi A_b. \tag{5}$$

Moreover, we observe that $A_b[\phi](\mathbb{Q}) \simeq M^\perp/M$, and that the size of $M^\perp/M$ is bigger than 1 only if the corresponding polynomial $f(x)$ is reducible, something that should happen 0% of the time, asymptotically (cf. [BSW22, Proposition 4.3]). If $\mathrm{Sel}_\psi^\natural J_b$ denotes the subset of elements in $\mathrm{Sel}_\psi J_b$ having non-trivial image in $\mathrm{Sel}_\phi A_b$, then we have the bound

$$\#\,\mathrm{Sel}_\psi J_b \leq \#\,\mathrm{Sel}_{\phi_M} J_b + \#\,\mathrm{Sel}_\psi^\natural J_b,$$

We can obtain information about $\mathrm{Sel}_\psi^\natural J_b$ using the irreducible orbits of the representation (G,V), which we now define. Recall that there is a map $G(K)\backslash V_b(K) \to (L^\times/L^{\times 2})_{N=1}$.

Definition 5.1. Let $b\in B(K)$. We will say that a $G(K)$-orbit in $V_b(K)$ is *reducible* if $\Delta(b)=0$ or if it maps to 1 in the map

$$G(K)\backslash V_b(K) \to \left(\frac{L^\times}{K^\times L^{\times 2}}\right)_{N=1}.$$

Otherwise, we will say that the orbit is *irreducible*.

Alternatively, an orbit is reducible in (G,V) if and only if it maps to a reducible orbit in (G^*,V^*). Under these definitions, a $G(K)$-orbit corresponding to an element of $\mathrm{Sel}_\psi J_b$ is irreducible if and only if it corresponds to an element of $\mathrm{Sel}_\psi^\natural J_b$; and the orbit is reducible if and only if it is in the image of $\mathrm{Sel}_{\phi_M} J_b$ inside $\mathrm{Sel}_\psi J_b$ in (5). Therefore, if we want to determine the average size of $\mathrm{Sel}_\psi J_b$, it would suffice to understand both the reducible and irreducible orbits of (G,V).

Counting irreducible orbits can be done analogously to previous cases in the literature, following e.g. [Lag24, §8]. For instance, the analogue of [Lag24, Proposition 8.10] would hold: namely, if $w\colon V(\mathbb{Z})\to[0,1]$ is some function defined by congruence conditions $w=\prod_p w_p$, if we define

$$N_w(V(\mathbb{Z})^{irr}, X) = \sum_{v\in G(\mathbb{Z})\backslash V(\mathbb{Z})^{irr}_{<X}} \frac{w(v)}{\#\,\mathrm{Stab}_{G(\mathbb{Z})}(v)},$$

then we expect that

$$N_w(V(\mathbb{Z})^{irr}, X) \sim \left(\int_{v \in V(\mathbb{Z}_p)} w(v) dv \right) C X^{2n(2n+1)}, \tag{6}$$

for some constant $C > 0$ which can be made explicit. Equation 6 can indeed be proven with $\leq$ instead of an equality as in [Lag24, Theorem 8.18]. Analogously to Section 4, we can sieve the counting to Selmer elements by imposing congruence conditions. We note, however, two important differences with the arguments in that section:

- If $b \in B^{rs}(\mathbb{Z})$, then $\mathrm{Stab}_{G(\mathbb{Q})}(v)$ always has at least two elements.
- The Selmer ratio
$$c_p(\psi_b) = \frac{\# A_b^\vee(K)/\psi(J_b(K))}{\# J_b[\psi](K)}$$
for $K = \mathbb{Q}_p$ or $\mathbb{R}$ might not be constant like in Lemma 4.1, because ψ is not self-dual.

The end result is the following:

Theorem 5.2. *The average size of* $\mathrm{Sel}_\psi^\natural J_b$*, when* b *varies in* $B(\mathbb{Z})$*, is at most*

$$8 \frac{\int_{\substack{b \in B(\mathbb{R}) \\ \mathrm{ht}(b)<1}} c_\infty(\psi_b) db}{\int_{\substack{b \in B(\mathbb{R}) \\ \mathrm{ht}(b)<1}} db} \prod_p \frac{\int_{b \in B(\mathbb{Z}_p)} c_p(\psi_b) db}{\int_{b \in B(\mathbb{Z}_p)} db}.$$

The factor of 8 is a product of the Tamagawa number of G, which is 4, and the mentioned minimum size of the stabiliser, which is 2. We note that this result is similar to the main results in [BES20; Bha+19], and that similarly to *loc. cit.*, the average size of $\mathrm{Sel}_\psi^\natural J_b$ depends very much on the family in which $b \in B(\mathbb{Z})$, and that imposing congruence conditions on $B(\mathbb{Z})$ would yield different upper bounds.

To count reducible orbits, we can follow the methods of [Sha+24], generalised in [Oll25]. In there, for the Vinberg representations associated to the $\mathbb{Z}/2\mathbb{Z}$-gradings of type ADE, we observe that the number of reducible orbits is of the order of $X^{\dim V}$. In our B_{2n} case, the computations can be slightly reworked to show that $N(V(\mathbb{Z})^{red}, X) \sim C_{red} X^{2n(2n+1)} \log X$ for some constant $C_{red} > 0$. In particular, the representation (G, V) appears to answer [Sha+24, Question 2] in the negative, given that the number of reducible and irreducible orbits are of different orbits.

Following these computations, one may obtain the (rather weak) bound that the average size of $\mathrm{Sel}_\psi J_b$ is $\ll \log X$ as $X \to \infty$. Imposing congruence conditions to obtain a meaningful bound for the "reducible" part of $\mathrm{Sel}_\psi J_b$ seems hard to do using uniquely geometry-of-numbers methods. For instance, it is unclear whether the product of the p-adic densities in the classical squarefree sieve would diverge to 0 in this situation, which would require more advanced techniques. If $\mathrm{Sel}_\psi J_b$ is actually unbounded, it would be interesting to see whether the contribution of 5.2 would correspond to a second-order term in the counting.

In any case, the possible unboundedness of $\mathrm{Sel}_\psi J_b$ seems to come from the 2-isogeny $\mathrm{Sel}_{\phi_M} J_b$. In the case of elliptic curves (which we have excluded from our analysis), it is predicted by Kane and Klagsbrun (as mentioned in [KL14, §1]) that the average size of the 2-Selmer group of a 2-isogeny over the curves of the form $y^2 = x^3 + ax^2 + bx$ is of the order of $\sqrt{\log X}$ as $X \to \infty$. Similarly, in [CHL19] it is proven that the average size of the 2-Selmer group tends to infinity in the family of elliptic curves with full $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$-torsion. In both cases, these results are deduced from the unboundedness of the Tamagawa ratio, which for an isogeny $\lambda \colon A \to B$ of abelian varieties is defined as

$$\mathcal{T}(A/B) = \frac{\# \mathrm{Sel}_\lambda(A)}{\# \mathrm{Sel}_{\lambda^\vee}(B^\vee)}.$$

Both in [KL14] and [CHL19], they prove that the average of the Tamagawa ratio of an associated 2-isogeny is unbounded, from which the unboundedness of the corresponding ϕ-Selmer group (and therefore of the 2-Selmer group) follows. In our situation, for the isogeny $\phi_M\colon J_b \to A_b$, the Greenberg-Wiles formula [NSW08, Theorem 8.7.9] in our case states that

$$\mathcal{T}(J_b/A_b) = \prod_{p\leq\infty} c_p(\phi_{M,b}) = \prod_{p\leq\infty} \frac{\#A_b(\mathbb{Q}_p)/\phi_M(J_b(\mathbb{Q}_p))}{2},$$

and if $2 \neq p < \infty$, then by [Sch96, Lemma 3.8], we have that

$$c_p(\phi_{M,b}) = \frac{\#A_b(\mathbb{Q}_p)/A_{b,0}(\mathbb{Q}_p)}{\#J_b(\mathbb{Q}_p)/J_{b,0}(\mathbb{Q}_p)}.$$

If J_b has good reduction at an odd prime p, then $c_p(\phi_{M,b}) = 1$. However, given that $\phi_{M,b}$ is not self-dual, it could happen that $c_p(\phi_{M,b}) \neq 1$ if J_b does not have good reduction at p. Heuristically, let us assume the following:

- Over the $b \in B(\mathbb{Z}_p)$ with $p \mid \Delta(b)$, the expected value of $c_p(\phi_{M,b})$ tends to a constant $\alpha > 1$.
- The values of $c_p(\phi_{M,b})$ behave independently for each prime p.

It is not unreasonable to expect that the average value of $c_p(\phi_{M,b})$ over the b's of bad reduction is larger that 1: if, for instance, the proportion of b with $c_p(\phi_{M,b}) = 2^n$ was positive and equal to the proportion of $c_p(\phi_{M,b}) = 1/2^n$, that would be a contribution of $(2^{2n}+1)/2^{n+1} > 1$ to the expected value. The independence of different primes would give that

$$\mathbb{E}[\prod_p c_p(\phi_{M,b})] = \alpha^{\omega(\Delta(b))},$$

where $\omega(\Delta(b))$ denotes the number of distinct primes dividing $\Delta(b)$. As the height of b grows, we can expect the average of $\alpha^{\omega(\Delta(b))}$ to be unbounded, provided the heuristics are valid. More precisely, the expected value of $\alpha^{\omega(\Delta(b))}$ is $e^{2(\alpha-1)\log\log X}$, which recover the aforementioned predicted value of $\sqrt{\log X}$ if $\alpha = 5/4$. This phenomoenon is, very roughly, what happens in [KL14] and [CHL19].

The phenomenon in which the unboundedness of the average of Selmer groups comes from the unboundedness of the average of Tamagawa ratios has been widely observed: other than the aforementioned [KL14; CHL19], a similar phenomenon was noted by Smith in [Smi23, Proposition 2.5]. Smith has also asked to which extent the converse is true: whether the average of Selmer groups is unbounded if and only if the Tamagawa ratio of some related isogeny is unbounded. We wonder whether how the constructions in this article fit into this framework.

References

[BES20] Manjul Bhargava, Noam Elkies, and Ari Shnidman. "The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$". In: *J. Lond. Math. Soc. (2)* 101.1 (2020), pp. 299–327. ISSN: 0024-6107,1469-7750. DOI: 10.1112/jlms.12271. URL: https://doi.org/10.1112/jlms.12271.

[BG13] Manjul Bhargava and Benedict H. Gross. "The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point". In: *Automorphic representations and L-functions*. Vol. 22. Tata Inst. Fundam. Res. Stud. Math. Tata Inst. Fund. Res., Mumbai, 2013, pp. 23–91. ISBN: 978-93-80250-49-6.

[BG14] Manjul Bhargava and Benedict H. Gross. "Arithmetic invariant theory". In: *Symmetry: representation theory and its applications*. Vol. 257. Progr. Math. Birkhäuser/Springer, New York, 2014, pp. 33–54. ISBN: 978-1-4939-1589-7; 978-1-4939-1590-3. DOI: 10.1007/978-1-4939-1590-3_3. URL: https://doi.org/10.1007/978-1-4939-1590-3_3.

[BGW15] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang. "Arithmetic invariant theory II: Pure inner forms and obstructions to the existence of orbits". In: *Representations of reductive groups*. Vol. 312. Progr. Math. Birkhäuser/Springer, Cham, 2015, pp. 139–171. ISBN: 978-3-319-23442-7; 978-3-319-23443-4. DOI: 10.1007/978-3-319-23443-4_5. URL: https://doi.org/10.1007/978-3-319-23443-4_5.

[BS15a] Manjul Bhargava and Arul Shankar. "Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves". In: *Ann. of Math. (2)* 181.1 (2015), pp. 191–242. ISSN: 0003-486X,1939-8980. DOI: 10.4007/annals.2015.181.1.3. URL: https://doi.org/10.4007/annals.2015.181.1.3.

[BS15b] Manjul Bhargava and Arul Shankar. "Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0". In: *Ann. of Math. (2)* 181.2 (2015), pp. 587–621. ISSN: 0003-486X,1939-8980. DOI: 10.4007/annals.2015.181.2.4. URL: https://doi.org/10.4007/annals.2015.181.2.4.

[BSW22] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. "Squarefree values of polynomial discriminants I". In: *Invent. Math.* 228.3 (2022), pp. 1037–1073. ISSN: 0020-9910,1432-1297. DOI: 10.1007/s00222-022-01098-w. URL: https://doi.org/10.1007/s00222-022-01098-w.

[Bha+19] Manjul Bhargava et al. "3-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field". In: *Duke Math. J.* 168.15 (2019), pp. 2951–2989. ISSN: 0012-7094,1547-7398. DOI: 10.1215/00127094-2019-0031. URL: https://doi.org/10.1215/00127094-2019-0031.

[Cas78] J. W. S. Cassels. *Rational quadratic forms*. Vol. 13. London Mathematical Society Monographs. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978, pp. xvi+413. ISBN: 0-12-163260-1.

[CHL19] Stephanie Chan, Jeroen Hanselman, and Wanlin Li. "Ranks, 2-Selmer groups, and Tamagawa numbers of elliptic curves with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$-torsion". In: *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*. Vol. 2. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2019, pp. 173–189. ISBN: 978-1-935107-03-3; 978-1-935107-02-6.

[KL14] Zev Klagsbrun and Robert J. Lemke Oliver. "The distribution of the Tamagawa ratio in the family of elliptic curves with a two-torsion point". In: *Res. Math. Sci.* 1 (2014), Art. 15, 10. ISSN: 2522-0144,2197-9847. DOI: 10.1186/s40687-014-0015-4. URL: https://doi.org/10.1186/s40687-014-0015-4.

[Knu+98] Max-Albert Knus et al. *The book of involutions*. Vol. 44. American Mathematical Society Colloquium Publications. With a preface in French by J. Tits. American Mathematical Society, Providence, RI, 1998, pp. xxii+593. ISBN: 0-8218-0904-0. DOI: 10.1090/coll/044. URL: https://doi.org/10.1090/coll/044.

[Lag23] Jef Laga. "Arithmetic statistics of Prym surfaces". In: *Math. Ann.* 386.1-2 (2023), pp. 247–327. ISSN: 0025-5831,1432-1807. DOI: 10.1007/s00208-022-02398-5. URL: https://doi.org/10.1007/s00208-022-02398-5.

[Lag24] Jef Laga. "Graded Lie Algebras, Compactified Jacobians and Arithmetic Statistics". In: *J. Eur. Math. Soc.* (2024). Published online first. DOI: 10.4171/JEMS/1526.

[LT24] Jef Laga and Jack A. Thorne. *100% of odd hyperelliptic Jacobians have no rational points of small height*. 2024. arXiv: 2405.10224 [math.NT]. URL: https://arxiv.org/abs/2405.10224.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Second. Vol. 323. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2008, pp. xvi+825. ISBN: 978-3-540-37888-4. DOI: 10.1007/978-3-540-37889-1. URL: https://doi.org/10.1007/978-3-540-37889-1.

[Oll25] Martí Oller. *The density of ADE families of curves having squarefree discriminant*. 2025. arXiv: 2306.05961 [math.NT]. URL: https://arxiv.org/abs/2306.05961.

[Pan05] Dmitri I. Panyushev. "On invariant theory of θ-groups". In: *J. Algebra* 283.2 (2005), pp. 655–670. ISSN: 0021-8693,1090-266X. DOI: 10.1016/j.jalgebra.2004.03.032. URL: https://doi.org/10.1016/j.jalgebra.2004.03.032.

[PR11] Bjorn Poonen and Eric Rains. "Self cup products and the theta characteristic torsor". In: *Math. Res. Lett.* 18.6 (2011), pp. 1305–1318. ISSN: 1073-2780,1945-001X. DOI: 10.4310/MRL.2011.v18.n6.a18. URL: https://doi.org/10.4310/MRL.2011.v18.n6.a18.

[PR12] Bjorn Poonen and Eric Rains. "Random maximal isotropic subspaces and Selmer groups". In: *J. Amer. Math. Soc.* 25.1 (2012), pp. 245–269. ISSN: 0894-0347,1088-6834. DOI: 10.1090/S0894-0347-2011-00710-8. URL: https://doi.org/10.1090/S0894-0347-2011-00710-8.

[Ree+12] Mark Reeder et al. "Gradings of positive rank on simple Lie algebras". In: *Transform. Groups* 17.4 (2012), pp. 1123–1190. ISSN: 1083-4362,1531-586X. DOI: 10.1007/s00031-012-9196-3. URL: https://doi.org/10.1007/s00031-012-9196-3.

[RT21] Beth Romano and Jack A. Thorne. "E_8 and the average size of the 3-Selmer group of the Jacobian of a pointed genus-2 curve". In: *Proc. Lond. Math. Soc. (3)* 122.5 (2021), pp. 678–723. ISSN: 0024-6115,1460-244X. DOI: 10.1112/plms.12388. URL: https://doi.org/10.1112/plms.12388.

[Sch96] Edward F. Schaefer. "Class groups and Selmer groups". In: *J. Number Theory* 56.1 (1996), pp. 79–114. ISSN: 0022-314X,1096-1658. DOI: 10.1006/jnth.1996.0006. URL: https://doi.org/10.1006/jnth.1996.0006.

[Sha19] Ananth N. Shankar. "2-Selmer groups of hyperelliptic curves with marked points". In: *Trans. Amer. Math. Soc.* 372.1 (2019), pp. 267–304. ISSN: 0002-9947,1088-6850. DOI: 10.1090/tran/7546. URL: https://doi.org/10.1090/tran/7546.

[SW18] Arul Shankar and Xiaoheng Wang. "Rational points on hyperelliptic curves having a marked non-Weierstrass point". In: *Compos. Math.* 154.1 (2018), pp. 188–222. ISSN: 0010-437X,1570-5846. DOI: 10.1112/S0010437X17007515. URL: https://doi.org/10.1112/S0010437X17007515.

[Sha+24] Arul Shankar et al. *Geometry-of-numbers methods in the cusp*. 2024. arXiv: 2110.09466 [math.NT]. URL: https://arxiv.org/abs/2110.09466.

[Smi23] Alexander Smith. *The distribution of ℓ^∞-Selmer groups in degree ℓ twist families II*. 2023. arXiv: 2207.05143 [math.NT]. URL: https://arxiv.org/abs/2207.05143.

[Tho13] Jack A. Thorne. "Vinberg's representations and arithmetic invariant theory". In: *Algebra Number Theory* 7.9 (2013), pp. 2331–2368. ISSN: 1937-0652,1944-7833. DOI: 10.2140/ant.2013.7.2331. URL: https://doi.org/10.2140/ant.2013.7.2331.

[Vin76] È. B. Vinberg. "The Weyl group of a graded Lie algebra". In: *Izv. Akad. Nauk SSSR Ser. Mat.* 40.3 (1976), pp. 488–526, 709. ISSN: 0373-2436.