

Pencils of quadrics and the arithmetic of hyperelliptic curves

Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang
(with an appendix by Tim and Vladimir Dokchitser)

November 3, 2013

1 Introduction

In this article, for any fixed genus $g \geq 1$, we prove that a positive proportion of hyperelliptic curves over \mathbb{Q} of genus g have points over \mathbb{R} and over \mathbb{Q}_p for all p , but have no points globally over *any* extension of \mathbb{Q} of odd degree.

By a hyperelliptic curve over \mathbb{Q} , we mean a smooth, geometrically irreducible, complete curve C over \mathbb{Q} equipped with a fixed map of degree 2 to \mathbb{P}^1 defined over \mathbb{Q} . Thus any hyperelliptic curve C over \mathbb{Q} of genus g can be embedded in weighted projective space $\mathbb{P}(1, 1, g + 1)$ and expressed by an equation of the form

$$C : z^2 = f(x, y) = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n \quad (1)$$

where $n = 2g + 2$, the coefficients f_i lie in \mathbb{Z} , and f factors into distinct linear factors over $\bar{\mathbb{Q}}$. Define the height $H(C)$ of C by

$$H(C) := H(f) := \max\{|f_i|\}. \quad (2)$$

Then there are clearly only finitely many integral equations (1) of height less than X , and we use the height to enumerate the hyperelliptic curves of a fixed genus g over \mathbb{Q} .

We say that a variety over \mathbb{Q} is *locally soluble* if it has a point over \mathbb{Q}_ν for every place ν of \mathbb{Q} , and is *soluble* if it has a point over \mathbb{Q} . It is known that most hyperelliptic curves over \mathbb{Q} of any fixed genus $g \geq 1$ when ordered by height are locally soluble (cf. [26], where it is shown that more than 75% of hyperelliptic curves have this property).

We prove:

Theorem 1. *Fix any $g \geq 1$. Then a positive proportion of locally soluble hyperelliptic curves over \mathbb{Q} of genus g have no points over any odd degree extension of \mathbb{Q} .*

Let $J = \text{Pic}_{C/\mathbb{Q}}^0$ denote the Jacobian of C over \mathbb{Q} , which is an abelian variety of dimension g . The points of J over a finite extension K of \mathbb{Q} are the divisor classes of degree zero on C that are rational over K . (When C is locally soluble, we will see that every K -rational divisor class on C is represented by a K -rational divisor.) Let $J^1 = \text{Pic}_{C/\mathbb{Q}}^1$ denote the principal homogeneous space for J whose points correspond to the divisor classes of degree one on C . A point P on C defined over an extension field K/\mathbb{Q} of odd degree k gives a rational point on J^1 , by taking the class of the divisor of degree one that is the sum of the distinct conjugates of P minus $(k-1)/2$ times the hyperelliptic class d obtained by pulling back $\mathcal{O}(1)$ from \mathbb{P}^1 . Thus Theorem 1 is equivalent to the following:

Theorem 2. *Fix any $g \geq 1$. For a positive proportion of locally soluble hyperelliptic curves C over \mathbb{Q} of genus g , the variety J^1 has no rational points.*

We prove Theorems 1 and 2 by determining the average size of what we call the 2-Selmer set $\text{Sel}_2(J^1)$ of J^1 . Recall that the 2-Selmer group $\text{Sel}_2(J)$ of the Jacobian J of C is a finite subgroup of the Galois cohomology group $H^1(\mathbb{Q}, J[2])$, which is defined by certain local conditions. The 2-Selmer group fits into an exact sequence

$$0 \rightarrow J(\mathbb{Q})/2J(\mathbb{Q}) \rightarrow \text{Sel}_2(J) \rightarrow \text{III}_J[2] \rightarrow 0,$$

where III_J denotes the Tate-Shafarevich group of J over \mathbb{Q} . Geometrically, we may interpret elements in the 2-Selmer group $\text{Sel}_2(J)$ of the Jacobian J of C as isomorphism classes of locally soluble two-covers of J . A *two-cover* of a principal homogeneous space I of J is an unramified cover $\pi : Y \rightarrow I$ by a principal homogeneous space Y such that for all $y \in Y$ and $a \in J$, we have $\pi(y+a) = \pi(y) + 2a \in I$. The degree of such a covering is 2^{2g} . The simplest example of a two-cover of J is given by the isogeny $[2] : J \rightarrow J$. This two-cover corresponds to the identity element of $\text{Sel}_2(J)$.

Similarly, we define the 2-Selmer set $\text{Sel}_2(J^1)$ of J^1 as the set of isomorphism classes of locally soluble two-covers of J^1 . The 2-Selmer set can be empty, but when $\text{Sel}_2(J^1)$ is nonempty, it forms a principal homogeneous space for the finite abelian group $\text{Sel}_2(J)$. Note that a rational point P on $C(\mathbb{Q})$ determines a rational point e_P (= the class of the divisor (P)) on $J^1(\mathbb{Q})$. Furthermore, any rational point e on $J^1(\mathbb{Q})$ gives rise to a locally soluble (in fact soluble) two-cover of J^1 ; namely, after identifying J^1 with J by subtracting e , we pull back the multiplication-by-2 map on J . We say then that this two-cover of J^1 *comes from e* (or *from P* when $e = e_P$). Theorems 1 and 2 therefore immediately follow from:

Theorem 3. *Fix any $g \geq 1$. Then for a positive proportion of locally soluble hyperelliptic curves C over \mathbb{Q} , the 2-Selmer set $\text{Sel}_2(J^1)$ is empty.*

To prove this theorem, we compute the average size of $\text{Sel}_2(J^1)$ over all locally soluble hyperelliptic curves C over \mathbb{Q} of any fixed genus $g \geq 1$:

Theorem 4. *Fix any $g \geq 1$. Then the average size of the 2-Selmer set $\text{Sel}_2(J^1)$, taken over all locally soluble hyperelliptic curves C over \mathbb{Q} of genus g ordered by height, is equal to 2.*

Note that the average size of the 2-Selmer set $\text{Sel}_2(J^1)$ over all locally soluble hyperelliptic curves C over \mathbb{Q} of genus g is independent of g .

Our methods also allow us to count elements, on average, in more general 2-Selmer sets. For C a hyperelliptic curve over \mathbb{Q} having hyperelliptic class d , and $k > 0$ any odd integer, define the *2-Selmer set of order k* for C to be the subset of elements of $\text{Sel}_2(J^1)$ that locally come from \mathbb{Q}_ν -rational points on J^1 of the form $e_\nu - \frac{k-1}{2}d$, where e_ν is an effective divisor of odd degree k on C over \mathbb{Q}_ν , for all places ν . Then we show:

Theorem 5. *Fix any odd integer $k > 0$. Then the average size of the 2-Selmer set of order k , over all locally soluble hyperelliptic curves of genus g over \mathbb{Q} , is strictly less than 2 provided that $k < g$, and tends to 0 as $g \rightarrow \infty$.*

Theorem 5 implies that most hyperelliptic curves of large genus have no K -rational points over all extensions K of \mathbb{Q} having small odd degrees:

Corollary 6. *Fix any $m > 0$. Then as $g \rightarrow \infty$, a proportion approaching 100% of hyperelliptic curves C of genus g over \mathbb{Q} contain no points over all extensions of \mathbb{Q} of odd degree $\leq m$.*

Corollary 6 allows us to construct many smooth surfaces and varieties of higher degree, as symmetric powers of hyperelliptic curves, that fail the Hasse principle:

Corollary 7. *Fix any odd integer $k > 0$. Then as $g \rightarrow \infty$, the variety $\text{Sym}^k(C)$ fails the Hasse principle for a proportion approaching 100% of locally soluble hyperelliptic curves C over \mathbb{Q} of genus g .*

One may ask what is the obstruction to the Hasse principle for the varieties J^1 and $\text{Sym}^k(C)$ occurring in Theorem 2 and Corollary 7, respectively. In both cases, the obstruction arises from the non-existence of a locally soluble two-cover of J^1 . As shown by Skorobogotov [32, Theorem 6.1.1] (see also Stoll [33, Remark 6.5 & Theorem 7.1]), using the descent theory of Colliot-Thélène and Sansuc [14], this obstruction yields a case of the Brauer-Manin obstruction for both J^1 and $\text{Sym}^k(C)$. Therefore, we obtain:

Theorem 8. *Fix any $g \geq 1$. For a positive proportion of locally soluble hyperelliptic curves C over \mathbb{Q} of genus g , the variety J^1 of dimension g has a Brauer–Manin obstruction to having a rational point.*

Theorem 9. *Fix any odd integer $k > 0$. As $g \rightarrow \infty$, for a density approaching 100% of locally soluble hyperelliptic curves C over \mathbb{Q} of genus g , the variety $\text{Sym}^k(C)$ of dimension k has a Brauer–Manin obstruction to having a rational point.*

Recall that the index $I(C)$ of a curve C/\mathbb{Q} is the least positive degree of a \mathbb{Q} -rational divisor D on C . Equivalently, it is the greatest common divisor of all degrees $[K : \mathbb{Q}]$ of finite field extensions K/\mathbb{Q} such that C has a K -rational point. Then Theorems 1 and 2 are also equivalent to:

Theorem 10. *For any $g \geq 1$, a positive proportion of locally soluble hyperelliptic curves C of genus g over \mathbb{Q} have index 2.*

We will actually prove more general versions of all of these results, where for each $g \geq 1$ we range over any “admissible” congruence family of hyperelliptic curves C over \mathbb{Q} of genus g for which $\text{Div}^1(C)$ (but not necessarily C) is locally soluble; see Definition 42 for the definition of “admissible”.

We obtain Theorem 3 from Theorem 4 by combining it with a result of Dokchitser and Dokchitser (see Appendix A), which states that a positive proportion of locally soluble hyperelliptic curves over \mathbb{Q} of genus $g \geq 1$ have even (or odd) 2-Selmer rank. Indeed, suppose that C is a locally soluble hyperelliptic curve whose 2-Selmer set $\text{Sel}_2(J^1)$ is nonempty. Then the cardinality of $\text{Sel}_2(J^1)$ is equal to the order of the finite elementary abelian 2-group $\text{Sel}_2(J)$. Let $W[2]$ denote the torsor for $J[2]$ whose \mathbb{Q} -points consist of elements $P \in J^1(\mathbb{Q})$ such that $2P$ is the hyperelliptic class $d \in J^2(\mathbb{Q})$. Since C is locally soluble, the class of the torsor $W[2]$ in $H^1(\mathbb{Q}, J[2])$ lies in the subgroup $\text{Sel}_2(J)$. Indeed, its image in $H^1(\mathbb{Q}, J)[2]$ is the class of the principal homogeneous space J^1 of J .

The class of $W[2]$ is nontrivial for 100% of hyperelliptic curves; indeed, a rational point on $W[2]$ corresponds to an odd factorization of $f(x, y)$ that is rational over \mathbb{Q} . An *odd* (resp. *even*) *factorization* of $f(x, y)$ is a factorization of the form $f(x, y) = g(x, y)h(x, y)$ where g, h are odd (resp. even) degree binary forms that are either K -rational or are conjugate over some quadratic extension of K . Since such factorizations rarely exist, we see that, for 100% of locally soluble curves, the 2-Selmer group of J contains $\mathbb{Z}/2\mathbb{Z}$, and the 2-Selmer set of J^1 (when nonempty) has cardinality at least 2. Moreover, if the 2-Selmer rank of the Jacobian is even, then the set $\text{Sel}_2(J^1)$ (when nonempty) will have size at least 4. Therefore, Theorem 4 (and Appendix A) implies that for a positive proportion of locally soluble hyperelliptic curves, the Selmer set $\text{Sel}_2(J^1)$ is empty. This proves Theorem 3.

Remark 11. Another consequence of the fact that odd and even factorizations of a binary form $f(x, y)$ over \mathbb{Q} rarely exist is that for 100% of all locally soluble hyperelliptic curves C over \mathbb{Q} , the set $J^1(\mathbb{Q})$ is either empty or infinite. Indeed, if J^1 has a rational point, then the class of $W[2]$ in $H^1(\mathbb{Q}, J[2])$ lies in the image of the group $J(\mathbb{Q})/2J(\mathbb{Q})$. If $f(x, y)$ has no odd or even factorization over \mathbb{Q} , then $W[2]$ is nontrivial and $J(\mathbb{Q})[2] = 0$. Therefore, $J(\mathbb{Q})$ has positive rank and hence is infinite, and as a consequence $J^1(\mathbb{Q})$ is infinite.

We prove Theorem 4 by relating the problem to a purely algebraic one involving pencils of quadrics. Let A and B be two symmetric bilinear forms over \mathbb{Q} in $n = 2g + 2$ variables, and assume that the corresponding pencil of quadrics in \mathbb{P}^{n-1} is generic. Over the complex numbers, the Fano variety $F = F(A, B)$ of common maximal isotropic subspaces of A and B is isomorphic to the Jacobian J of the hyperelliptic curve given by $C : z^2 = \text{disc}(Ax - By) := (-1)^{g+1} \det(Ax - By)$ (cf. [28], [19], [16]); furthermore, all such pairs (A, B) with the same discriminant binary form are $\text{SL}_n(\mathbb{C})$ -equivalent.

However, as shown in [35], over \mathbb{Q} the situation is much different. Given A and B , the Fano variety $F = F(A, B)$ might not have any rational points. In general, F is a principal homogeneous space for J whose class $[F]$ in $H^1(\mathbb{Q}, J)$ has order dividing 4 and satisfies $2[F] = [J^1]$; hence F gives a two-cover of J^1 (see [35] or §4 for more details on the properties of the Fano variety). Moreover, given a hyperelliptic curve $C : z^2 = f(x, y)$ over \mathbb{Q} of genus g (equivalently, a binary form of degree $n = 2g + 2$ over \mathbb{Q} with nonzero discriminant), there might not exist *any* pair (A, B) of symmetric bilinear forms over \mathbb{Q} such that $f(x, y) = \text{disc}(Ax - By)$! This raises the natural question: for which binary forms $f(x, y)$ of degree $n = 2g + 2$ and nonzero discriminant over \mathbb{Q} does there exist a pair (A, B) of symmetric bilinear forms in n variables over \mathbb{Q} such that $f(x, y) = \text{disc}(Ax - By)$?

In this paper, we give a geometric answer to this question in terms of the generalized Jacobian $J_{\mathfrak{m}}$ of the hyperelliptic curve $C : z^2 = f(x, y)$. Assume for simplicity that $f(x, y) = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n$ has first coefficient $f_0 \neq 0$, so that the curve C has two distinct points P and P' above the point $\infty = (1, 0)$ on \mathbb{P}^1 . These points are rational and conjugate over the field $\mathbb{Q}(\sqrt{f_0})$. Let $\mathfrak{m} = P + P'$ be the corresponding modulus over \mathbb{Q} and let $C_{\mathfrak{m}}$ denote the singular curve associated to this modulus as in [29, Ch. IV, §4]. Then $C_{\mathfrak{m}}$ is given by the equation $z^2 = f(x, y)y^2$, and has an ordinary double point at infinity. The *generalized Jacobian* of C associated to the modulus \mathfrak{m} , denoted by $J_{\mathfrak{m}} = J_{\mathfrak{m}}(C)$, is the connected component of the identity of $\text{Pic}_{C_{\mathfrak{m}}/\mathbb{Q}}/\mathbb{Z} \cdot d$, while $J_{\mathfrak{m}}^1 = J_{\mathfrak{m}}^1(C)$ denotes the nonidentity component; here d denotes the hyperelliptic class of $C_{\mathfrak{m}}$ in $\text{Pic}_{C_{\mathfrak{m}}/\mathbb{Q}}^2(\mathbb{Q})$ obtained by pulling back $\mathcal{O}(1)$ from \mathbb{P}^1 . We prove:

Theorem 12. *Let $f(x, y)$ denote a binary form of even degree $n = 2g + 2$ over \mathbb{Q} , with nonzero discriminant and nonzero first coefficient. Then there exists a pair (A, B) of symmetric bilinear forms over \mathbb{Q} in n variables satisfying $f(x, y) = \text{disc}(Ax - By)$ if and only if there exists a two-cover of homogeneous spaces $F_{\mathfrak{m}} \rightarrow J_{\mathfrak{m}}^1$ for $J_{\mathfrak{m}}$ over \mathbb{Q} , or equivalently, if and only if the class of the homogeneous space $J_{\mathfrak{m}}^1$ is divisible by 2 in the group $H^1(\mathbb{Q}, J_{\mathfrak{m}})$.*

See Theorem 23 for a number of other equivalent conditions for the existence of A and B satisfying $f(x, y) = \text{disc}(Ax - By)$. It is of significance that the singular curve $C_{\mathfrak{m}}$ and the generalized Jacobian $J_{\mathfrak{m}}$ appear in Theorem 12. As noted in [27, Footnote 2], for the purpose of doing 2-descent on the Jacobians of hyperelliptic curves with no rational Weierstrass point, it is not always enough to study only unramified covers of C ; one needs also covers of C unramified away from the points above some fixed point on \mathbb{P}^1 .

The group $\mathrm{SL}_n(\mathbb{Q})$ acts on the space $\mathbb{Q}^2 \otimes \mathrm{Sym}_2 \mathbb{Q}^n$ of pairs (A, B) of symmetric bilinear forms on an n -dimensional vector space, and $\mu_2 \subset \mathrm{SL}_n$ acts trivially since $n = 2g + 2$ is even. The connection with Theorem 4 arises from the fact that we may parametrize elements of $\mathrm{Sel}_2(J^1)$ by certain orbits for the action of the group $(\mathrm{SL}_n / \mu_2)(\mathbb{Q})$ on the space $\mathbb{Q}^2 \otimes \mathrm{Sym}_2 \mathbb{Q}^n$. We say that an element $(A, B) \in \mathbb{Q}^2 \otimes \mathrm{Sym}_2 \mathbb{Q}^n$, or its $(\mathrm{SL}_n / \mu_2)(\mathbb{Q})$ -orbit, is *locally soluble* if the associated Fano variety $F(A, B)$ has a point locally over every place of \mathbb{Q} . Then we prove:

Theorem 13. *Let $f(x, y)$ denote a binary form of even degree $n = 2g + 2$ over \mathbb{Q} such that the hyperelliptic curve $C : z^2 = f(x, y)$ is locally soluble. Then the $(\mathrm{SL}_n / \mu_2)(\mathbb{Q})$ -orbits of locally soluble pairs (A, B) of symmetric bilinear forms in n variables over \mathbb{Q} such that $f(x, y) = \mathrm{disc}(Ax - By)$ are in bijection with the elements of the 2-Selmer set $\mathrm{Sel}_2(J^1)$.*

To obtain Theorem 4, we require a version of Theorem 13 for integral orbits. Let $\mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$ denote the space of pairs (A, B) of $n \times n$ symmetric bilinear forms over \mathbb{Z} . Then we show:

Theorem 14. *There exists a positive integer κ depending only on n such that, for any integral binary form $f(x, y)$ of even degree $n = 2g + 2$ with $C : z^2 = f(x, y)$ locally soluble over \mathbb{Q} , every $(\mathrm{SL}_n / \mu_2)(\mathbb{Q})$ -orbit of locally soluble pairs $(A, B) \in \mathbb{Q}^2 \otimes \mathrm{Sym}_2 \mathbb{Q}^n$ such that $\mathrm{disc}(Ax - By) = \kappa^2 f(x, y)$ contains an element in $\mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$. In other words, the $(\mathrm{SL}_n / \mu_2)(\mathbb{Q})$ -equivalence classes of locally soluble pairs $(A, B) \in \mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$ such that $\mathrm{disc}(Ax - By) = \kappa^2 f(x, y)$ are in bijection with the elements of $\mathrm{Sel}_2(J^1)$.*

We will prove Theorem 14 for $\kappa = 4^n$ but we expect this can be improved. We use Theorem 14, together with the results of [1] giving the number of $\mathrm{SL}_n(\mathbb{Z})$ -orbits on $\mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$ having bounded height, and a sieve, to deduce Theorem 4.

We note that the emptiness of $J^1(\mathbb{Q})$ for hyperelliptic curves C over \mathbb{Q} has been demonstrated previously for certain special algebraic families. In [13], Colliot-Thélène and Poonen constructed one-parameter algebraic families of curves $C = C_t$ of genus 1 and genus 2 for which the varieties J^1 have a Brauer-Manin obstruction to having a rational point for all $t \in \mathbb{Q}$. (We note that the family of genus 2 curves considered in [13] consists of hyperelliptic curves C over \mathbb{Q} with locally soluble $J^1(C)$ but not locally soluble $\mathrm{Div}^1(C)$.) For arbitrary genus $g > 5$ satisfying $4 \nmid g$, Dong Quan [20] constructed such one-parameter algebraic families of locally soluble hyperelliptic curves $C = C_t$ with empty $J^1(\mathbb{Q})$ for all $t \in \mathbb{Q}$.

This paper is organized as follows. In Section 2, we introduce the key representation $2 \otimes \mathrm{Sym}_2(n)$ of SL_n on pairs of symmetric bilinear forms that we will use to study the arithmetic of hyperelliptic curves. We adapt the results of Wood [38] to study the orbits of this representation over a general Dedekind domain D whose characteristic is not equal to 2. In Section 3, we introduce hyperelliptic curves and some of the relevant properties of their generalized Jacobians. In Section 4, we then relate hyperelliptic curves to generic pencils of quadrics over a field K of characteristic not equal to 2, and we review the results that we will need from [35]. In Section 5, we then study *regular* pencils of quadrics, which allows us to determine which binary n -ic forms over K arise as the discriminant of a pencil of quadrics over K ; in particular, we prove Theorem 12.

In Section 6, we describe how the K -soluble orbits (i.e., orbits of those (A, B) over K such that $F(A, B)$ has a K -rational point), having associated hyperelliptic curve C over K , are parametrized by elements of the set $J^1(K)/2J(K)$. We study the orbits over some arithmetic fields in more detail in Section 7 and then we focus on global fields and discuss *locally soluble* orbits in Section 8. We show that the locally soluble orbits over \mathbb{Q} , having associated hyperelliptic curve C over \mathbb{Q} are parametrized

by the elements of the finite set $\text{Sel}_2(J^1)$, proving Theorem 13. The existence of integral orbits (Theorem 14) is demonstrated in Section 9. We then discuss the counting results from [1] that we need in Section 10, and discuss the details of the required sieve in Section 11. Finally, we complete the proofs of Theorems 4 and 5 in the final Section 12.

2 Orbits of pairs of symmetric bilinear forms over a Dedekind domain

In this section, we study the orbits of our key representation $2 \otimes \text{Sym}_2(n)$ over a Dedekind domain. In later sections, we will relate these orbits to the arithmetic of hyperelliptic curves.

Let D be a Dedekind domain, with quotient field K . We assume throughout this paper that the characteristic of D is not equal to 2. Let $n \geq 2$ be an integer. The group $\text{SL}_n(D)$ acts on the D -module of pairs (A, B) of symmetric bilinear forms on a free D -module W of rank n . After a choice of basis for W , this is the representation $D^2 \otimes \text{Sym}_2 D^n = \text{Sym}_2 D^n \oplus \text{Sym}_2 D^n$.

The coefficients of the binary n -ic form

$$f(x, y) = \text{disc}(xA - yB) := (-1)^{n(n-1)/2} \det(xA - yB) = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n,$$

which we call the *invariant binary n -ic form* of the element $(A, B) \in D^2 \otimes \text{Sym}_2 D^n$, give $n + 1$ polynomial invariants of degree n which freely generate the ring of invariant polynomials over D . We also have the invariant *discriminant* polynomial $\Delta(f) = \Delta(f_0, f_1, \dots, f_n)$ given by the discriminant of the binary form f , which has degree $2n(n - 1)$ in the entries of A and B .

In Wood's work [38], the orbits of $\text{SL}_2^\pm(T) = \{g \in \text{GL}_2(T) : \det(g) = \pm 1\}$ on $T^2 \otimes \text{Sym}_2 T^n$ were classified for general rings (and in fact even for general base schemes) T in terms of ideal classes of rings of rank n over T . In this section, we translate these results into a form that we will require later on, in the important special case where $T = D$ is a Dedekind domain with quotient field K . In particular, we will need to use the actions by the groups $\text{SL}_n(D)$ and $(\text{SL}_n/\mu_2)(D)$ rather than $\text{SL}_n^\pm(D)$, which causes some key changes in the parametrization data and will indeed be important for us in our later discussion and connection with hyperelliptic curves.

Let us assume that $f_0 \neq 0$ and write $f(x, 1) = f_0g(x)$, where $g(x)$ has coefficients in the quotient field K and has n distinct roots in a separable closure K^s of K . Let $L = L_f := K[x]/g(x)$ be the corresponding étale algebra of rank n over K , and let θ be the image of x in the algebra L . Then $g(\theta) = 0$ in L . Let $g'(x)$ be the derivative of $g(x)$ in $K[x]$; since $g(x)$ is separable, the value $g'(\theta)$ must be an invertible element of L . We define $f'(\theta) = f_0g'(\theta)$ in L^\times .

For $k = 1, 2, \dots, n - 1$, define the integral elements

$$\zeta_k = f_0\theta^k + f_1\theta^{k-1} + \cdots + f_{k-1}\theta$$

in L , and let $R = R_f$ be the free D -submodule of L having D -basis $\{1, \zeta_1, \zeta_2, \dots, \zeta_{n-1}\}$. For $k = 0, 1, \dots, n - 1$, let $I(k)$ be the free D -submodule of L with basis $\{1, \theta, \theta^2, \dots, \theta^k, \zeta_{k+1}, \dots, \zeta_{n-1}\}$. Then $I(k) = I(1)^k$, and $I(0) = R \subset I(1) \subset \cdots \subset I(n - 1)$. Note that $I(n - 1)$ has the power basis $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$, but that the elements of $I(n - 1)$ need not be integral when f_0 is not a unit in D .

A remarkable fact (cf. [8], [24, Proposition 1.1], [37, §2.1]) is that R is a D -order in L of discriminant $\Delta(f)$, and the free D -modules $I(k)$ are all fractional ideals of R . The fractional ideal $(1/f'(\theta))I(n - 2)$ is the dual of R under the trace pairing on L , and the fractional ideal $I(n - 3)$ will play a crucial role in the parametrization of orbits in our representation.

We then have the following translation of [38, Theorem 1.3] in the case of the action of $\mathrm{SL}_n(D)$ on $D^2 \otimes \mathrm{Sym}_2 D^n$, where D is a Dedekind domain:

Theorem 15. *Assume that $f(x, y)$ is a binary form of degree n over D with $\Delta(f) \neq 0$ and $f_0 \neq 0$. Then there is a bijection (to be described below) between the set of orbits for $\mathrm{SL}_n(D)$ on $D^2 \otimes \mathrm{Sym}_2 D^n$ with invariant form f and the set of equivalence classes of triples (I, α, s) , where I is a fractional ideal for R , $\alpha \in L^\times$, and $s \in K^\times$, that satisfy the relations $I^2 \subset \alpha I(n-3)$, $N(I)$ is the principal fractional ideal sD in K , and $N(\alpha) = s^2 f_0^{n-3}$ in K^\times . The triple (I, α, s) is equivalent to the triple $(cI, c^2\alpha, N(c)s)$ for any $c \in L^\times$. The stabilizer of a triple (I, α, s) is $S^\times[2]_{N=1}$ where $S = \mathrm{End}_R(I) \subset L$.*

From a triple (I, α, s) , we construct an orbit as follows. Since $N(I)$ is the principal D -ideal sD , the projective D -module I of rank n is free. Since $I^2 \subset \alpha I(n-3)$, we obtain two symmetric bilinear forms on the free module I by defining $\langle \lambda, \mu \rangle_A$ and $\langle \lambda, \mu \rangle_B$ as the respective coefficients of ζ_{n-1} and ζ_{n-2} in the basis expansion of the product $\lambda\mu/\alpha$ in $I(n-3)$. We obtain an $\mathrm{SL}_n(D)$ -orbit of two symmetric $n \times n$ matrices (A, B) over D by taking the Gram matrices of these forms with respect to any ordered basis of I that gives rise to the basis element $s(1 \wedge \zeta_1 \wedge \zeta_2 \wedge \cdots \wedge \zeta_{n-1})$ of the top exterior power of I over D . This normalization deals with the difference between $\mathrm{SL}_n(D)$ - and $\mathrm{GL}_n(D)$ -orbits. The stabilizer statement follows because elements in $S^\times[2]_{N=1}$ are precisely the elements of $L_{N=1}^\times$ that preserve the map $\frac{1}{\alpha} \times : I \times I \rightarrow I(n-3)$.

Conversely, given an element $(A, B) \in D^2 \otimes \mathrm{Sym}_2 D^n$, we construct the ring $R = R_f$ from f as described above, where $f(x, y) = \mathrm{disc}(xA - yB)$. The R -module I is then constructed by letting $\theta \in L$ act on K^n by the matrix $A^{-1}B$. Then $\zeta_1 = f_0\theta \in R$ preserves the lattice D^n . Similarly, formulas for the action of each $\zeta_i \in R$ on D^n , in terms of integral polynomials in the entries of A and B , can be worked out when A is assumed to be invertible; these same formulas can then be used to show that D^n is an R -module, even when A is not invertible. See [38, §3.1] for the details.

When $n = 2m$ is even, the larger group $(\mathrm{SL}_n/\mu_2)(D)$ acts on the representation $D^2 \otimes \mathrm{Sym}_2 D^n$, and distinct orbits for the subgroup $\mathrm{SL}_n(D)/\mu_2(D)$ may become identified as a single orbit for the larger group. Since $H^1(D, \mathrm{SL}_n) = 1$, we have an exact sequence of groups

$$1 \rightarrow \mathrm{SL}_n(D)/\mu_2(D) \rightarrow (\mathrm{SL}_n/\mu_2)(D) \rightarrow H^1(D, \mu_2) \rightarrow 1.$$

By Kummer theory, the quotient group $H^1(D, \mu_2)$ lies in an exact sequence

$$1 \rightarrow D^\times/D^{\times 2} \rightarrow H^1(D, \mu_2) \rightarrow \mathrm{Pic}(D)[2] \rightarrow 1.$$

The image of the group $H^1(D, \mu_2)$ in $H^1(K, \mu_2) = K^\times/K^{\times 2}$ is the subgroup $K^{\times(2)}/K^{\times 2}$ of elements t such that the principal ideal $tD = M^2$ is a square, and the map to $\mathrm{Pic}(D)[2]$ is given by mapping such an element t to the class of M .

With this identification of the quotient, the action of elements t in the group $K^{\times(2)}/K^{\times 2}$ on the equivalence class of triples (I, α, s) giving the orbits for $\mathrm{SL}_n(D)$ with invariant form f in the Theorem 15 is given by

$$t \cdot (I, \alpha, s) = (MI, t\alpha, t^m s)$$

where $m = n/2$ and $tD = M^2$. The equivalence classes of triples for this additional action give the orbits of $(\mathrm{SL}_n/\mu_2)(D)$ with invariant form f . The stabilizer of the triple (I, α, s) contains the finite group $S^\times[2]_{N=1}/D^\times[2]$ where $S = \mathrm{End}_R(I) \subset L$, as that is the image of the stabilizer from $\mathrm{SL}_n(D)$.

Theorem 16. *Assume that $f(x, y)$ is a binary form of degree n over D with $\Delta(f) \neq 0$ and $f_0 \neq 0$. Then there is a bijection between the set of orbits for $(\mathrm{SL}_n / \mu_2)(D)$ on $D^2 \otimes \mathrm{Sym}_2 D^n$ with invariant form f and the set of equivalence classes of triples (I, α, s) , where I is a fractional ideal for R , $\alpha \in L^\times$, and $s \in K^\times$, that satisfy the relations $I^2 \subset \alpha I(n-3)$, $N(I)$ is the principal fractional ideal sD in K , and $N(\alpha) = s^2 f_0^{n-3}$ in K^\times . The triple (I, α, s) is equivalent to the triple $(cMI, c^2 t \alpha, N(c)t^m s)$ for any $c \in L^\times$ and $t \in K^{\times(2)}$, where $m = n/2$ and $tD = M^2$. The stabilizer of the triple (I, α, s) is an elementary abelian 2-group which contains $S^\times[2]_{N=1}/D^\times[2]$ where $S = \mathrm{End}_R(I) \subset L$.*

Remark 17. We can simplify the statement of Theorem 16 when the domain D is a PID and every fractional ideal for the order R is principal, generated by an element of L . In that case, the fractional ideal I of R is completely determined by the pair (α, s) and the identities $I^2 \subset (\alpha)I(n-3)$, $N(I) = (s)$, and $N(\alpha) = s^2 f_0^{n-3}$. Indeed, together these force $I^2 = (\alpha)I(n-3)$. There is a bijection from the set of equivalence classes of α to the set $(R^\times / R^{\times 2} D^\times)_{N=f_0}$. Moreover, we have $S = \mathrm{End}_R(I) = R$ and $K^{\times(2)} = D^\times K^{\times 2}$. The stabilizer in $(\mathrm{SL}_n / \mu_2)(D)$ of a triple (I, α, s) then fits into the exact sequence

$$1 \rightarrow (R^\times[2])_{N=1}/D^\times[2] \rightarrow \mathrm{Stab}_{(\mathrm{SL}_n / \mu_2)(D)}(I, \alpha, s) \rightarrow (R^{\times 2} \cap D^\times)/D^{\times 2} \rightarrow 1. \quad (3)$$

When L is not an algebra over a quadratic extension of K , the quotient $(R^{\times 2} \cap D^\times)/D^{\times 2}$ is trivial.

In particular, when $D = K$ is a field, we recover [5, Theorems 7 and 8]. These versions of Theorems 15 and 16 over a field K will also be important in the sequel. For convenience, we restate them below.

Corollary 18. *Assume that $f(x, y)$ is a binary form of degree n over K with $\Delta(f) \neq 0$ and $f_0 \neq 0$. Then there is a bijection between the set of orbits for $\mathrm{SL}_n(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant form f and the set of equivalence classes of pairs (α, s) with $N(\alpha) = s^2 f_0^{n-3}$ in K^\times . The pair (α, s) is equivalent to the pair $(c^2 \alpha, N(c)s)$ for any $c \in L^\times$. The stabilizer of the orbit corresponding to a pair (α, s) is the finite commutative group scheme $(\mathrm{Res}_{L/K} \mu_2)_{N=1}$ over K .*

It follows from Corollary 18 that the set of $\mathrm{SL}_n(K)$ -orbits is either in bijection with or has a 2-to-1 map to $(L^\times / L^{\times 2})_{N=f_0}$, depending on whether $f(x, y)$ has an odd degree factor over K or not, respectively. Indeed, the pair (α, s) is equivalent to the pair $(\alpha, -s)$ if and only if there is an element $c \in L^\times$ with $c^2 = 1$ and $N(c) = -1$.

Corollary 19. *Assume that $f(x, y)$ is a binary form of degree n over K with $\Delta(f) \neq 0$ and $f_0 \neq 0$. Then there is a bijection between the set of orbits for $(\mathrm{SL}_n / \mu_2)(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$ with invariant form f and the set of equivalence classes of pairs (α, s) with $N(\alpha) = s^2 f_0^{n-3}$ in K^\times . The pair (α, s) is equivalent to the pair $(c^2 t \alpha, N(c)t^{n/2} s)$ for any $c \in L^\times$ and $t \in K^{\times(2)} = K^\times$. The stabilizer of the orbit corresponding to a pair (α, s) is the finite commutative group scheme $(\mathrm{Res}_{L/K} \mu_2)_{N=1}/\mu_2$ over K .*

It follows from Corollary 19 that the set of $(\mathrm{SL}_n / \mu_2)(K)$ -orbits is either in bijection with or has a 2-to-1 map to $(L^\times / L^{\times 2} K^\times)_{N=f_0}$, depending on whether $f(x, y)$ has an odd factorization or not, respectively. Here an *odd factorization* of $f(x, y)$ is a factorization of the form $f(x, y) = g(x, y)h(x, y)$, where g and h are odd degree binary forms that are either K -rational or are conjugate over some quadratic extension of K .

3 Hyperelliptic curves, divisor classes, and generalized Jacobians

Assume from now on that $n \geq 2$ is even and write $n = 2g + 2$. Fix a field K of characteristic not 2. In order to interpret the orbits for $\mathrm{SL}_n(K)$ and $(\mathrm{SL}_n/\mu_2)(K)$ having a fixed invariant binary form, we first review some of the arithmetic and geometry of hyperelliptic curves of genus g over K . As in [21], we define a hyperelliptic curve over K as a smooth, projective curve over K with a 2-to-1 map to the projective line over K , although now we treat the general case (without any fixed K -rational points at infinity.)

Let $f(x, y) = f_0x^{2g+2} + \cdots + f_{2g+2}y^{2g+2}$ be a binary form of degree $2g + 2$ over K , with $\Delta \neq 0$ and $f_0 \neq 0$. We associate to $f(x, y)$ the hyperelliptic curve C over K with equation

$$z^2 = f(x, y).$$

This defines a smooth curve of genus g , as a hypersurface of degree $2g + 2$ in the weighted projective plane $\mathbb{P}(1, 1, g + 1)$. The weighted projective plane embeds as a surface in \mathbb{P}^{g+2} via the map $(x, y, z) \rightarrow (x^{g+1}, x^gy, \dots, y^{g+1}, z)$. The image is a cone over the rational normal curve in \mathbb{P}^{g+1} , which has a singularity at the vertex $(0, 0, \dots, 1)$ when $g \geq 1$. The curve C is the intersection of this surface with a quadric hypersurface that does not pass through the vertex of the cone. Finally, the linear series on C of projective dimension $g + 2$ and degree $2g + 2$ that gives this embedding is the sum of the all the Weierstrass points (i.e., points with $z = 0$).

There are two points $P = (1, 0, z_0)$ and $P' = (1, 0, -z_0)$ at infinity, where $z_0^2 = f_0$. If f_0 is a square in K^\times , then these points are rational over K . If not, then they are rational over the quadratic extension $K' = K(\sqrt{f_0})$. Let w be the rational function z/y^{g+1} on C , and let t be the rational function x/y on C . Both are regular outside of the two points P and P' with $y = 0$, where they have poles of order $g + 1$ and 1 respectively. The field of rational functions on C is given by $K(C) = K(t, w)$, with $w^2 = f(t, 1) = f_0t^{2g+2} + \cdots + f_{2g+2}$, and the subring of functions that are regular outside of P and P' is $K[t, w] = K[t, \sqrt{f(t, 1)}]$ [21].

Let \mathfrak{m} be the modulus $\mathfrak{m} = P + P'$ on C and let $C_{\mathfrak{m}}$ be the singular curve constructed from C and this modulus in [29, Ch. IV, no. 4]. Then $C_{\mathfrak{m}}$ has equation

$$z^2 = f(x, y)y^2$$

of degree $2g + 4$ in $\mathbb{P}(1, 1, g + 2)$. This defines a singular, projective curve of arithmetic genus $g + 1$ whose normalization is C . There is now a single point $Q = (1, 0, 0)$ at infinity, which is an ordinary double point whose tangents are rational over the quadratic extension field K .

Let $\mathrm{Pic}_{C/K}$ and $\mathrm{Pic}_{C_{\mathfrak{m}}/K}$ denote the Picard functors of the projective curves C and $C_{\mathfrak{m}}$ respectively. These are represented by commutative group schemes over K , whose component groups are both isomorphic to \mathbb{Z} . Let K^s be a fixed separable closure of K and let E be any extension of K contained in K^s . The E -rational points of $\mathrm{Pic}_{C/K}$ correspond bijectively to the divisor classes on C over the separable closure K^s that are fixed by the Galois group $\mathrm{Gal}(K^s/E)$. When the curve C has no E -rational points, an E -rational divisor class on C may not be represented by an E -rational divisor. The subgroup of classes in $\mathrm{Pic}_{C/K}(E)$ that are represented by E -rational divisors is just the image of $\mathrm{Pic}(C/E) = H^1(C/E, \mathbb{G}_m)$ in $H^0(E, H^1(C/K^s, \mathbb{G}_m))$, under the map induced by the spectral sequence for the morphism $C/E \rightarrow \mathrm{Spec} E$. From this spectral sequence, we also obtain an injection from the quotient group to the Brauer group of K (cf. [32, §2.3], [9, Ch. 8]):

$$\mathrm{Pic}_{C/K}(K)/\mathrm{Pic}(C/K) \rightarrow H^2(K, \mathbb{G}_m) = \mathrm{Br}(K).$$

Since C has a rational point over the quadratic extension $K' = K(\sqrt{f_0})$, the image of this injection is contained in the subgroup $\text{Br}(K'/K) = K^\times/N(K'^\times)$. Every class in $\text{Br}(K'/K)$ corresponds to a quaternion algebra D over K that is split by K' , or equivalently, to a curve of genus zero over K with two conjugate points rational over K' .

Proposition 20. *If a hyperelliptic curve C over K has a rational divisor of odd degree, or equivalently a rational point over an extension of K of odd degree, then every K -rational divisor class is represented by a K -rational divisor. If K is a global field and $\text{Div}^1(C)$ is locally soluble, then every K -rational divisor class is represented by a K -rational divisor.*

Indeed, a quaternion algebra split by an odd degree extension of K is already split over K . Similarly, a quaternion algebra over a global field that splits locally everywhere is split globally.

The distinction between K -rational divisor classes and K -rational divisors does not arise for the curve C_m , which always has the K -rational singular point Q . Hence the points of $\text{Pic}_{C_m/K}$ over E correspond to the classes of divisors that are rational over E and are prime to \mathfrak{m} , modulo the divisors of functions with $f \equiv 1$ modulo \mathfrak{m} . We have an exact sequence of smooth group schemes over K :

$$0 \rightarrow T \rightarrow \text{Pic}_{C_m/K} \rightarrow \text{Pic}_{C/K} \rightarrow 0, \quad (4)$$

where T is the one-dimensional torus that is split by K' . Taking the long exact sequence in Galois cohomology, and noting that the image of $\text{Pic}_{C_m/K}(K)$ in $\text{Pic}_{C/K}(K)$ is precisely the subgroup $\text{Pic}(C/K) = H^1(C/K, \mathbb{G}_m)$ represented by K -rational divisors, we recover the injection

$$\text{Pic}_{C/K}(K)/\text{Pic}(C/K) \rightarrow H^1(K, T) = K^\times/N(K'^\times) = \text{Br}(K'/K).$$

To see this geometrically, note that the fiber over a K -rational point P of $\text{Pic}_{C/K}$ is a principal homogeneous space for T over K , which is a curve of genus zero with two conjugate points over K' removed. This curve of genus zero determines the image of P in $\text{Br}(K'/K)$.

The connected components of the identity of the Picard schemes $J = \text{Pic}_{C/K}^0$ and $J_m = \text{Pic}_{C_m/K}^0$ are the Jacobian and generalized Jacobian of [29, Ch. V]. They correspond to the divisor classes of degree zero on these curves. The exact sequence in (4) restricts to the following exact sequence [29, Ch. V, §3]

$$0 \rightarrow T \rightarrow J_m \rightarrow J \rightarrow 0. \quad (5)$$

There is a line bundle of degree 2 on C_m (and hence on C) which is the pull-back of the line bundle $\mathcal{O}(1)$ from the projective line under the map $(x, y, z) \rightarrow (x, y)$. This is represented by the K -rational divisor $d = (R) + (R')$ prime to \mathfrak{m} consisting of the two points above a point (x_0, y_0) on the projective line, whenever y_0 is nonzero. The quotient groups $\text{Pic}_{C/K}/\mathbb{Z} \cdot d = J \sqcup J^1$ and $\text{Pic}_{C_m/K}/\mathbb{Z} \cdot d = J_m \sqcup J_m^1$ both have two connected components, represented by the divisor classes of degree 0 and 1. There are morphisms

$$\begin{aligned} C &\longrightarrow J^1 \\ C - \{P, P'\} = C_m - \{Q\} &\longrightarrow J_m^1 \end{aligned}$$

defined over K , which take a point to the corresponding divisor class of degree 1 [29, Ch V, §4].

Proposition 21. *Let $f(x, y) = f_0x^{2g+2} + \dots + f_{2g+2}y^{2g+2}$ be a binary form with nonzero discriminant and nonzero f_0 . Let $C : z^2 = f(x, y)$ and $C_m : z^2 = f(x, y)y^2$ denote the associated hyperelliptic curve and singular curve with Jacobian J and generalized Jacobian J_m . Let $L = K[x]/f(x, 1)$ denote the corresponding étale algebra of rank $2g + 2$. Then:*

1. The 2-torsion subgroup $J_m[2]$ of J_m is isomorphic to the group scheme $(\text{Res}_{L/K}\mu_2)_{N=1}$. Its K -rational points correspond to the even degree factors of $f(x, y)$ over K .
2. The 2-torsion subgroup $J[2]$ of J is isomorphic to the group scheme $(\text{Res}_{L/K}\mu_2)_{N=1}/\mu_2$. Its K -rational points correspond to the even factorizations of $f(x, y)$ over K .
3. The 2-torsion $W_m[2]$ in the component J_m^1 of $\text{Pic}_{C_m/K}/\mathbb{Z} \cdot d = J_m \sqcup J_m^1$, is a torsor for $J_m[2]$ whose K -rational points correspond to the odd degree factors of $f(x, y)$ over K .
4. The 2-torsion $W[2]$ in the component J^1 of $\text{Pic}_{C/K}/\mathbb{Z} \cdot d = J \sqcup J^1$ is a torsor for $J[2]$ whose K -rational points correspond to the odd factorizations of $f(x, y)$ over K .

Here an odd (resp. even) factorization of $f(x, y)$ over K is a factorization of the form $f = gh$, where g and h are either odd (resp. even) degree binary forms over K or are conjugate over some quadratic extension of K .

Proof. To prove the proposition, we observe that the 2-torsion points of J_m over the separable closure K^s are represented by the classes of divisors of the form $(P_1) + (P_2) + \cdots + (P_{2m}) - md$, where each $P_i = (x_i, 1, 0)$ comes from a distinct root x_i of $f(x, 1)$ [22, §4]. Hence the points of $J_m[2]$ over K^s correspond bijectively to the factors of even degree of $f(x, y)$. Since the Galois group acts by permutation of the roots, we have a canonical isomorphism $J_m[2] \simeq (\text{Res}_{L/K}\mu_2)_{N=1}$. On the quotient J , there is a single relation: $(P_1) + \cdots + (P_{2g+2}) - (g+1)d = \text{div}(y) \equiv 0$, so $J[2] \simeq (\text{Res}_{L/K}\mu_2)_{N=1}/\mu_2$. The last two statements of Proposition 21 follow similarly. \square

Finally, we note that the Weil pairing $J[2] \times J[2] \rightarrow \mu_2$ gives the self-duality of the finite group scheme $(\text{Res}_{L/K}\mu_2)_{N=1}/\mu_2$, and the connecting homomorphism $H^1(K, J[2]) \rightarrow H^2(K, \mu_2)$ whose kernel is the image of $H^1(K, J_m[2])$ is cup product with the class of $W[2]$ (see [27, Proposition 10.3]).

4 Generic pencils of quadrics

In this section, we relate hyperelliptic curves to pencils of quadrics. In particular, we will see how pencils of quadrics yield two-covers of J^1 for certain hyperelliptic curves.

Let $W = K^n$ be a vector space of dimension $n \geq 3$ over K and let A and B be two symmetric bilinear forms on W . Let Q_A and Q_B be the corresponding quadric hypersurfaces in $\mathbb{P}(W)$, so Q_A is defined by the equation $\langle w, w \rangle_A = 0$ and Q_B is defined by the equation $\langle w, w \rangle_B = 0$. Let Y be the base locus of the pencil spanned by A and B , which is defined by the equations $\langle w, w \rangle_A = \langle w, w \rangle_B = 0$ in $\mathbb{P}(W)$. Then Y has dimension $n - 3$ and is a smooth complete intersection if and only if the discriminant of the pencil $\text{disc}(xA - yB) = f(x, y)$ has $\Delta(f) \neq 0$. In this case we say that the pencil spanned by A and B is generic. In this section, we will only consider generic pencils. The Fano scheme $F = F(A, B)$ is the Hilbert scheme of maximal linear subspaces of $\mathbb{P}(W)$ that are contained in Y .

When $n = 2g + 1$ is odd, the Fano scheme has dimension zero and is a principal homogeneous space for the finite group scheme $\text{Res}_{L/K}\mu_2/\mu_2 \simeq (\text{Res}_{L/K}\mu_2)_{N=1}$. Here L is the étale algebra of rank $2g + 1$ determined by the separable binary form $f(x, y)$. The 2^{2g} points of F over the separable closure of K correspond to the subspaces Z of W of g that are isotropic for all the quadrics in the pencil, and the scheme F depends only on the $\text{SL}_n(K)$ -orbit of the pair (A, B) .

When $n = 2g + 2$ is even, the Fano scheme F is smooth and geometrically connected of dimension g , and is a principal homogeneous space for the Jacobian J of the smooth hyperelliptic curve C with equation $z^2 = f(x, y)$. A point of F corresponds to a subspace Z of W of dimension g that is isotropic for all of the quadrics in the pencil, whereas a point of C corresponds to a quadric in the pencil plus a choice of one of the two rulings of that quadric. This interpretation can be used to define a morphism $C \times F \rightarrow F$ over K , which in turn gives a fixed point free action of J on F . In this case, the Fano variety F depends only on the $(\mathrm{SL}_n / \mu_2)(K)$ -orbit of the pair (A, B) . Proofs of all assertions on the Fano scheme can be found in [35].

Theorem 22. ([35, Theorem 2.7]) *Let F be the Fano variety of maximal linear subspaces contained in the base locus of a generic pencil of quadrics generated by symmetric bilinear forms $(A, B) \in K^2 \otimes \mathrm{Sym}_2 K^n$. Let $f(x, y)$ denote the invariant binary form of (A, B) . Let $C : z^2 = f(x, y)$ denote the corresponding hyperelliptic curve with Jacobian J . Then the disconnected variety*

$$X := J \sqcup F \sqcup J^1 \sqcup F \tag{6}$$

has a commutative algebraic group structure over K . In particular, $[F]$ as a class in $H^1(K, J)$ is 4-torsion and $2[F] = [J^1]$.

The group X contains the subgroup $\mathrm{Pic}_{C/K} / \mathbb{Z} \cdot d = J \sqcup J^1$ with index two. Let $F[4]$ be the principal homogeneous space for $J[4]$ consisting of the points of F of (minimal) order 4 in the group X . Multiplication by 2 in X gives finite étale coverings

$$F \rightarrow J^1$$

$$F[4] \rightarrow W[2]$$

of degree 2^{2g} with an action of the group scheme $J[2]$. This shows that the class $[F]$ of the principal homogeneous space F satisfies $2[F] = [J^1]$ in the group $H^1(K, J)$. Similarly, the class of $W[2]$ in $H^1(K, J[2])$ is the image of the class $F[4]$ in $H^1(K, J[4])$ under the map $2 : H^1(K, J[4]) \rightarrow H^1(K, J[2])$.

Consequently, a necessary condition on the existence of a pencil (A, B) over K with discriminant curve C is that the class of J^1 and the class of $W[2]$ should be divisible by 2 in $H^1(K, J)$ and $H^1(K, J[4])$ respectively. However, this condition is not sufficient. Consider the curve C of genus zero with equation $z^2 = -x^2 - y^2$ over \mathbb{R} . In this case, both J and $J[2]$ reduce to a single point, so any homogeneous space for J or $J[2]$ is trivial, and hence divisible by 2. On the other hand, since $L = \mathbb{C}$ and $f_0 = -1$ is not a norm, by Corollary 18 (or 19) there are no pencils over \mathbb{R} with discriminant $f(x, y) = -x^2 - y^2$. To obtain a geometric condition that is both necessary and sufficient for the existence of a pencil, we will have to consider non-generic pencils whose invariant binary form defines the singular curve C_m . This is the object of the next section.

5 Regular pencils of quadrics

In this section, we give a list of equivalent conditions for the existence of a pencil over K whose discriminant is some given binary form $f(x, y)$. In particular, we prove Theorem 12.

Let (A, B) generate a generic pencil of bilinear forms on a vector space W of even dimension $n = 2g + 2$ over K , and let $f(x, y) = \mathrm{disc}(xA - yB)$ be the associated binary form of degree $2g + 2$ and

discriminant $\Delta(f) \neq 0$. We continue to assume that $f_0 = \text{disc}(A)$ is also nonzero in K . Let (A', B') be a pair of bilinear forms on the vector space $W' = W \oplus K^2$ of dimension $n + 2 = 2g + 4$, where A' is the direct sum of A and the rank one form $\langle (a, b), (a', b') \rangle = aa'$ on K^2 and B' is the direct sum of B and the split form $\langle (a, b), (a', b') \rangle = ab' + a'b$ of rank 2. The invariant binary form of this pencil

$$\text{disc}(xA' - yB') = f(x, y)y^2$$

then has a double zero at $(x, y) = (1, 0)$, and the pencil is not generic. The base locus defined by the equations $Q_{A'} = Q_{B'} = 0$ in $\mathbb{P}(W \oplus K^2)$ has an ordinary double point at the unique singular point $R = (0_W; 0, 1)$ of the quadric $Q_{A'}$. There are exactly $2g + 3$ singular quadrics in the pencil and all of them are simple cones. The K -algebra L' associated to the pencil is not étale, but is isomorphic to $L \oplus K[y]/y^2$. Even though L' is not étale, the vector space W' is a free L' -module of rank 1, so the pencil is regular in the sense of [35, §3]. Since the norms from $K[y]/y^2$ to K are precisely the squares in K , we have an equality of quotient groups $K^\times / K^{\times 2} N(L^\times) = K^\times / K^{\times 2} N(L'^\times)$.

The Fano scheme F_m of this pencil consists of the subspaces Z of dimension $g + 1$ in $W \oplus K^2$ that are isotropic for all of the quadrics in the pencil and do not contain the unique line that is the radical of the form A' (so the projective space $\mathbb{P}(Z)$, which is contained in the base locus, does not meet the unique double point R). The Fano scheme is a smooth variety of dimension $g + 1$. However, in this case F_m is not projective. It is a principal homogeneous space for the generalized Jacobian J_m associated to the singular curve C_m of arithmetic genus $g + 1$ and equation $z^2 = f(x, y)y^2$ in weighted projective space.

For example, when $g = 0$, the curve C is the non-singular quadric $z^2 = ax^2 + bxy + cy^2$ in \mathbb{P}^2 , with $a = f_0$ and $b^2 - 4ac = \Delta(f)$ both nonzero in K . The pencil (A', B') has discriminant $f'(x, y) = ax^2y^2 + bxy^3 + cy^4$. Its base locus D in \mathbb{P}^3 is isomorphic to a singular curve of arithmetic genus one, with a single node R whose tangents are rational over the quadratic extension $K' = K(\sqrt{f_0})$. The Fano variety F_m in this case is just the affine curve $D - \{R\}$, and J_m^1 is the affine curve $C_m - \{Q\} = C - \{P, P'\}$. Both are principal homogeneous spaces for the one-dimensional torus $T = J_m$ which is split by K' . We shall see that there is an unramified double cover $F_m \rightarrow J_m^1$ that extends to a double cover of complete curves of genus zero $M \rightarrow C$ which is ramified at P and P' .

Since the pencil is regular and its associated hyperelliptic curve has only nodal singularities, we again obtain a commutative algebraic group

$$X_m = J_m \sqcup F_m \sqcup J_m^1 \sqcup F_m \quad (7)$$

over K with connected component J_m and component group $\mathbb{Z}/4$, which contains the algebraic group $\text{Pic}_{C_m/K} / \mathbb{Z} \cdot d = J_m \sqcup J_m^1$ with index two [35, §3.2]. Just as in the generic case, multiplication by 2 in the group X_m gives an unramified cover

$$F_m \rightarrow J_m^1$$

of degree 2^{2g+1} with an action of $J_m[2]$, and shows that $2[F_m] = [J_m^1]$ in the group $H^1(K, J_m)$ of principal homogeneous spaces for J_m . Hence a necessary condition for the existence of such a pencil (A', B') is that the class of J_m^1 is divisible by 2. In this case, the necessary condition is also sufficient.

Theorem 23. *Let $f(x, y) = f_0x^{2g+2} + \dots + f_{2g+2}y^{2g+2}$ be a binary form of degree $2g + 2$ over K with f_0 and $\Delta(f)$ both nonzero in K . Write $f(x, 1) = f_0g(x)$ with $g(x)$ monic and separable. Let L be the étale algebra $K[x]/g(x)$ of degree n over K and let β denote the image of x in L . Let C be the smooth hyperelliptic curve of genus g with equation $z^2 = f(x, y)$ and let C_m be the singular hyperelliptic*

curve of arithmetic genus $g + 1$ with equation $z^2 = f(x, y)y^2$. Then the following conditions are all equivalent.

- a. There is a generic pencil (A, B) over K with $\text{disc}(xA - yB) = f(x, y)$.
- b. There is a regular pencil (A', B') over K with $\text{disc}(xA' - yB') = f(x, y)y^2$.
- c. The coefficient f_0 lies in the subgroup $K^{\times 2}N(L^\times)$ of K^\times .
- d. The class of the homogeneous space J_m^1 is divisible by 2 in the group $H^1(K, J_m)$.
- e. The class of the homogeneous space $W_m[2]$ is in the image of the multiplication-by-2 map $H^1(K, J_m[4]) \rightarrow H^1(K, J_m[2])$.
- f. There is an unramified two-cover of homogeneous spaces $F_m \rightarrow J_m^1$ for J_m over K .
- g. The maximal unramified abelian cover $U \rightarrow C - \{P, P'\}$ of exponent 2 over K^s descends to K .
- h. The maximal abelian cover $M \rightarrow C$ of exponent 2 over K^s that is ramified only at the points $\{P, P'\}$ descends to K .

Note the maximal abelian covers above all have degree 2^{2g+1} . The equivalence of conditions a, d, and f proves Theorem 12.

Proof. $a \Leftrightarrow b \Leftrightarrow c$. We have already seen that the existence of orbits in both cases is equivalent to condition c, that the class of f_0 in $K^\times/K^{\times 2}$ is in the image of the norm map from $L^\times/L^{\times 2}$.

$b \Rightarrow d \Leftrightarrow e \Rightarrow f$. When a regular orbit (A', B') exists in b, the Fano variety F_m of the base locus of the pencil provides a homogenous space for J_m whose class is a square-root of the class of J_m^1 in the group $H^1(K, J_m)$. The equivalence of conditions d, e and f is clear.

$f \Rightarrow g \Rightarrow h$. Assuming that an unramified covering $F \rightarrow J_m^1$ exists over K , we obtain the unramified covering of $C - \{P, P'\}$ by taking the fiber product with the morphism $C - \{P, P'\} \rightarrow J_m^1$, and the ramified covering of C by completing the unramified cover of $C - \{P, P'\}$.

$h \Rightarrow c$. Finally, assuming the existence of the ramified covering $M \rightarrow C$ over K , we show that f_0 lies in the subgroup $K^{\times 2}N(L^\times)$ of K^\times , which will complete the proof of Theorem 23. The covering $M \rightarrow C$ corresponds to an inclusion of function fields $K(C) \rightarrow K(M)$. Over K^s , the function field $K^s(M)$ is obtained from $K^s(C)$ by adjoining the square-roots of all rational functions on C whose divisors have the form $2d_1$ or $2d_1 + (P) + (P')$ for some divisor d_1 on C . Since the characteristic of K is not equal to 2, these square-roots either give unramified extensions of C or extensions that are ramified only at the two points P and P' , where the ramification is tame. More precisely, there are $2^{2g+1} - 1$ distinct quadratic extensions of $K^s(C)$ of this form that are contained in $K^s(M)$, and their composition is equal to $K^s(M)$.

Indeed, by Galois theory, these quadratic extensions correspond to the subgroups of index 2 in $J_m[2](K^s)$, or equivalently to nontrivial K^s -points in the Cartier dual $\text{Res}_{L/K}\mu_2/\mu_2$. Let w be the rational function z/y^{g+1} on C , and let t be the rational function x/y on C , so $w^2 = f_0g(t)$. The nontrivial points in $(\text{Res}_{L/K}\mu_2/\mu_2)(K^s)$ correspond bijectively to the nontrivial monic factorizations $g(x) = h(x)j(x)$ over K^s , and the corresponding quadratic extension of $K^s(C)$ is given by $K^s(C)(\sqrt{h(t)}) = K^s(C)(\sqrt{j(t)})$. When both $h(x)$ and $j(x)$ have even degree, the divisors of the rational functions $h(t)$ and $j(t)$ are of the form $2d_1$ and the corresponding quadratic cover of the curve C is unramified. When the factors both have odd degree, these divisors are of the form $2d_1 + (P) + (P')$ and the quadratic cover is ramified at the points P and P' .

Since there might be no nontrivial factorizations of $g(x)$ over K , there might be no nontrivial K -rational points of $\text{Res}_{L/K}\mu_2/\mu_2$ and hence no quadratic field extensions of $K(C)$ contained in $K(M)$. However, over L we have the factorization $g(x) = (x - \beta)j(x) = h(x)j(x)$, so the algebra $L(M)$ must contain a square-root u of some constant multiple of the function $h(t) = (t - \beta)$. (The need to adjoin a square-root of $t - \beta$ whose divisor has the form $2d_1 + (P) + (P')$ is the main reason for the appearance of the generalized Jacobian J_m (cf. [27, Footnote 2]).) Write $u^2 = \alpha(t - \beta)$ with α in L^\times and take the norm to $K(M)$ to obtain the equation $N(u)^2 = N(\alpha)g(t)$. Then the two rational functions $N(u)$ and w in $K(M)^\times$ have the same divisor, so they are equal up to a constant factor in K^\times . Writing $bN(u) = w$ with b in K^\times , we find $w^2 = b^2N(u)^2 = b^2N(\alpha)g(t)$. However, $w^2 = f_0g(t)$, so $f_0 = b^2N(\alpha)$ is in the subgroup $K^{\times 2}N(L^\times)$ of K^\times . This completes the proof of Theorem 23. \square

In fact, the obstruction classes for the eight conditions in Theorem 23 are all equal. More precisely, the obstruction class for conditions a, b, c is the class of f_0 in $K^\times/K^{\times 2}(NL^\times)$. This group can be viewed as a subgroup of $H^2(K, J_m[2])$ via

$$\text{coker}(N : H^1(K, \text{Res}_{L/K}\mu_2) \rightarrow H^1(K, \mu_2)) \hookrightarrow H^2(K, (\text{Res}_{L/K}\mu_2)_{N=1}).$$

We denote the image of f_0 in $H^2(K, J_m[2])$ by $[f_0]$. This is the cohomological class d_f whose non-vanishing obstructs the existence of rational orbits with invariant f for (all pure inner forms of) SL_n ; see [5, §2.4 and Theorem 9].

The obstruction class for conditions d, e is the class $\delta[J_m^1]$ in $H^2(K, J_m[2])$ where δ is the connecting homomorphism $H^1(K, J_m) \rightarrow H^2(K, J_m[2])$ arising from the exact sequence $1 \rightarrow J_m[2] \rightarrow J_m \xrightarrow{2} J_m \rightarrow 1$.

The obstruction class for conditions f, g, h comes from Galois descent. There is an unramified two-cover $\pi : J_m^1 \rightarrow J_m^1$ over K^s obtained by identifying J_m^1 with J_m using a K^s point of J_m^1 , then taking the multiplication-by-2 map on J_m . The descent obstruction of this cover to K is the image in $H^2(K, J_m[2])$ of the class $[\pi : J_m^1 \rightarrow J_m^1]$ under the following map from the Hochschild-Serre spectral sequence:

$$H^0(K, H^1(C \times_K K^s - \{P, P'\}, J_m[2])) \longrightarrow H^2(K, J_m[2]).$$

This obstruction class equals $\delta[J_m^1]$ for formal reasons (cf. [32, Lemma 2.4.5]). We have the following strengthening of Theorem 23.

Theorem 24. *Let $f(x, y) = f_0x^{2g+2} + \dots + f_{2g+2}y^{2g+2}$ be a binary form of degree $2g + 2$ over K with f_0 and $\Delta(f)$ both nonzero in K . Let C be the smooth hyperelliptic curve of genus g with equation $z^2 = f(x, y)$ and let J_m denote its generalized Jacobian. Then the obstruction classes for conditions a through h in Theorem 23 are all equal in $H^2(K, J_m[2])$, i.e., $[f_0] = \delta[J_m^1]$.*

Proof. Consider the following commutative diagram:

$$\begin{array}{ccccccc} 1 & \longrightarrow & J_m[2] & \longrightarrow & J_m & \xrightarrow{2} & J_m \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow = \\ 1 & \longrightarrow & J_m \sqcup J_m^1[2] & \longrightarrow & J_m \sqcup J_m^1 & \xrightarrow{2} & J_m \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \\ & & \mu_2 & \xrightarrow{=} & \mu_2 & & \end{array} .$$

Here the map $J_m \sqcup J_m^1 \xrightarrow{2} J_m$ is given by $[D] \mapsto 2[D] - \deg([D]) \cdot d$. Theorem 24 follows from the following two results.

Proposition 25. *For any $a \in K$, there exists a class $[J_a^{1/2}] \in H^1(K, J_m \sqcup J_m^1)$ such that $2[J_a^{1/2}] = [J_m^1]$ in $H^1(K, J_m)$ and such that the image of $[J_a^{1/2}]$ in $H^1(K, \mu_2) = K^\times / K^{\times 2}$ equals $f_0 g(a) = f_0 N_{L/K}(a - \beta)$.*

Lemma 26. *Let $1 \rightarrow A_1 \rightarrow B_1 \rightarrow C \rightarrow 1$ and $1 \rightarrow A_2 \rightarrow B_2 \rightarrow C \rightarrow 1$ be central extensions of algebraic groups over K such that the following diagram commutes:*

$$\begin{array}{ccccccc} 1 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow = \\ 1 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \\ & & D & \xrightarrow{=} & D & & \end{array}$$

Then the following diagram commutes up to sign:

$$\begin{array}{ccc} H^1(K, B_2) & \longrightarrow & H^1(K, C) \\ \downarrow & & \downarrow \\ H^1(K, D) & \longrightarrow & H^2(K, A_1) \end{array}$$

Lemma 26 follows from a direct cocycle computation. We now prove Proposition 25. Fix $a \in K$, let $P_a \in C(K(\sqrt{\alpha}))$ be a point with x -coordinate a where $\alpha = f_0 g(a)$, and let P'_a be the conjugate of P_a under the hyperelliptic involution. The class $[J_m^1] \in H^1(K, J_m)$ is given by the 1-cocycle $\sigma \mapsto \sigma(P'_a) - (P'_a)$. In other words,

$$[J_m^1]_\sigma = \begin{cases} 0 & \text{if } \sigma(\sqrt{\alpha}) = \sqrt{\alpha} \\ (P_a) - (P'_a) & \text{if } \sigma(\sqrt{\alpha}) = -\sqrt{\alpha}. \end{cases}$$

Let $[J_a^{1/2}]$ denote the following 1-cochain with values in $(J_m \sqcup J_m^1)(K^s)$:

$$[J_a^{1/2}]_\sigma = \begin{cases} 0 & \text{if } \sigma(\sqrt{\alpha}) = \sqrt{\alpha} \\ (P_a) & \text{if } \sigma(\sqrt{\alpha}) = -\sqrt{\alpha}. \end{cases}$$

Since $2(P_a) - d = 2(P_a) - ((P_a) + (P'_a)) = (P_a) - (P'_a)$, we see that $2[J_a^{1/2}]_\sigma = [J_m^1]_\sigma$ for all $\sigma \in \text{Gal}(K^s/K)$. Moreover, a direct computation shows that $[J_a^{1/2}]$ is a 1-cocycle and its image in $H^1(K, \mu_2)$ is the 1-cocycle $\sigma \mapsto \sigma\sqrt{\alpha}/\sqrt{\alpha}$. This completes the proof of Proposition 25, and thus Theorem 24. \square

6 Soluble orbits

In the previous section, we gave necessary and sufficient conditions for the existence of pencils of bilinear forms $(A, B) \in K^2 \otimes \text{Sym}_2 K^n$ having a given invariant binary form. In this section, we

consider *soluble* pencils of bilinear forms (A, B) , i.e., those for which the associated Fano variety $F = F(A, B)$ has a K -rational point.

Fix a binary form $f(x, y)$ of degree $n = 2g + 2$ over K with $\Delta(f)$ and f_0 nonzero in K , and let C be the smooth hyperelliptic curve with equation $z^2 = f(x, y)$. Suppose that (A, B) is a generic pencil of bilinear forms on W over K with invariant binary form $f(x, y) = \text{disc}(Ax - By)$ and let (A', B') be the regular pencil of bilinear forms on $W \oplus K^2$ having invariant binary form $f(x, y)y^2$ constructed above. We say that (A, B) lies in a *soluble* orbit for SL_n if the Fano variety F_m of the base locus of (A', B') has a K -rational point. Similarly, we say that the pencil (A, B) lies in a *soluble* orbit for SL_n/μ_2 if the Fano variety F of the base locus of (A, B) has a K -rational point. In this section, we classify the soluble orbits for SL_n and SL_n/μ_2 .

Since we have constructed an unramified two-cover $F_m \rightarrow J_m^1$, a necessary condition for the existence of soluble orbits for SL_n is that $J_m^1(K)$ is nonempty. (Recall that every K -rational point in J_m^1 is represented by an odd degree K -rational divisor on the curve C that is relatively prime to the divisor $\mathfrak{m} = (P) + (P')$.) In this case, the group $J_m(K)$ acts simply transitively on the set of points $J_m^1(K)$.

Theorem 27. *Let $f(x, y)$ be a binary form of degree $n = 2g + 2$ over K with $\Delta(f)$ and f_0 nonzero in K . Then soluble orbits for the action of $\text{SL}_n(K)$ on $K^2 \otimes \text{Sym}_2 K^n$ having invariant binary form $f(x, y)$ exist if and only if there is a K -rational divisor of odd degree on the curve $C : z^2 = f(x, y)$. In that case, they are in bijection with the elements of $J_m^1(K)/2J_m(K)$.*

Proof. Suppose first that soluble orbits with invariant binary form $f(x, y)$ exist. Let (A, B) be in $K^2 \otimes \text{Sym}_2 K^n$ with invariant binary form $f(x, y)$ such that the Fano variety $F(A, B)_m$ of the associated regular pencil (A', B') in $W \oplus K^2$ has a rational point. The stabilizer of (A, B) in SL_n is isomorphic to $J_m[2]$ by Corollary 18 and Proposition 21. Since $H^1(K, \text{SL}_n) = 1$, we see that the rational orbits with invariant binary form $f(x, y)$ are in bijection with the elements in the Galois cohomology group $H^1(K, J_m[2])$. This bijection depends on the choice of the initial soluble orbit (A, B) which maps to the trivial class in $H^1(K, J_m[2])$.

Explicitly, suppose the pair $(A_1, B_1) \in K^2 \otimes \text{Sym}_2 K^n$ has invariant binary form $f(x, y)$ and corresponds to the class $c \in H^1(K, J_m[2])$. Let (A'_1, B'_1) be the associated regular pencil with Fano variety $F(A_1, B_1)_m$. Then as elements of $H^1(K, J_m)[4]$, we have, up to sign¹, the formula

$$[F(A_1, B_1)_m] = [F(A, B)_m] + c. \quad (8)$$

Hence we see that $F(A_1, B_1)_m$ is the trivial torsor of J_m if and only if c is in the Kummer image of $J_m(K)/2J_m(K)$. Therefore, the set of soluble orbits with invariant binary form $f(x, y)$ is in bijection with the elements of the quotient group $J_m(K)/2J_m(K)$, once the fixed soluble orbit (A, B) has been chosen.

On the other hand, if $x \in F(A, B)_m(K)$ is any rational point, then the sum $x + x = 2x$ in the algebraic group X_m in (7) gives a rational point of J_m^1 well-defined up to hyperelliptic conjugation (cf. Footnote 1). Hence $J_m^1(K)$ is nonempty. Therefore, the set $J_m^1(K)/2J_m(K)$ is also in bijection with $J_m(K)/2J_m(K)$.

To complete the proof of Theorem 27, it remains to show that if $J_m^1(K)$ is nonempty, then soluble orbits with invariant binary form $f(x, y)$ exist. We show this first in the special case where the

¹The ambiguity of sign comes from the fact that we cannot distinguish between $[F_m]$ and $-[F_m]$ in $H^1(K, J_m)$. In other words, we cannot distinguish the two copies of F_m in the group X_m defined in (7).

curve C_m has a non-singular K -rational point $Q = (x_0, 1, z_0)$. Let $L = K[x]/f(x, 1)$ denote as usual the étale algebra of rank n associated to $f(x, y)$ and let β denote the image of x in L . The rational orbit corresponding to (Q) is given by the equivalence class of a pair (α, s) (see Corollary 18) where $\alpha = (x - T)(Q)$. Here “ $x - T$ ” is the descent map introduced by Cassels [12]:

$$J_m^1(K)/2J_m(K) \rightarrow (L^\times/L^{\times 2})_{N \equiv f_0}.$$

We note that s is not uniquely determined when $W_m[2]$ is a nontrivial torsor of $J_m[2]$. In this case, the fibers of the above $x - T$ map also have size 2. From the definition of the bijection between the set of rational orbits and the set of equivalence classes of pairs (α, s) in Section 2, we see that if the orbit corresponding to a pair (α, s) is soluble, then the orbit corresponding to any pair (α', s') with $\alpha' = \alpha$ is also soluble.

Consider the two binary forms (A', B') on $L \oplus K^2$ given by

$$\begin{aligned} \langle (\lambda, a, b), (\mu, a', b') \rangle_{A'} &= (\text{coefficient of } \beta^{n-1} \text{ in } \alpha\lambda\mu) + aa', \\ \langle (\lambda, a, b), (\mu, a', b') \rangle_{B'} &= (\text{coefficient of } \beta^{n-1} \text{ in } \alpha\beta\lambda\mu) + ab' + a'b. \end{aligned}$$

We show that for $\alpha = (x - T)(Q)$, there is a rational $(g + 1)$ -plane x' isotropic with respect to both bilinear forms.

When $z_0 \neq 0$, we have $\alpha = (x - T)(Q) = x_0 - \beta$. Set $h_1(t) = (f(t, 1) - f(x_0, 1))/(t - x_0)$.

Then

$$x' = \text{Span}\left\{(1, 0, 0), (\beta, 0, 0), \dots, (\beta^{g-1}, 0, 0), (\beta^g, 1, -\frac{1}{2}(x_0 + \frac{f_1}{f_0}))\right\}$$

is isotropic with respect to both bilinear forms. To check this, we note that $(x_0 - \beta)\beta^{2g+1}$ has leading coefficient $x_0 + f_1/f_0$.

When $z_0 = 0$, we set $h_0(t) = t - x_0$ and $h_1(t) = f(t, 1)/(t - x_0)$. Then $\alpha = (x - T)(Q) = h_1(\beta) - h_0(\beta)$ and the following $(g + 1)$ -plane is isotropic with respect to both bilinear forms:

$$x' = \text{Span}\left\{(h_1(\beta) - h_1(x_0), 0, 0), (\beta - x_0, 0, 0), \dots, ((\beta - x_0)^{g-1}, 0, 0), ((\beta - x_0)^g, 1, -\frac{1}{2}((2g+1)x_0 + \frac{f_1}{f_0}))\right\}.$$

This can be checked by a simple calculation noting that $h_1(\beta)h_1(x_0)(h_1(\beta) - h_1(x_0)) = h_0(\beta)h_1(x_0)$.

Before moving on to the general case, we make an important observation. Using this pencil with $\alpha = (x - T)(Q)$ as the base point, we obtain a bijection between the set of the rational orbits with invariant binary form $f(x, y)$ and $H^1(K, J_m[2])$ as described above. If (A_1, B_1) is an element of $K^2 \otimes \text{Sym}_2 K^n$ with invariant binary form $f(x, y)$ and such that its associated α equals to $(x - T)(D)$ for some $D \in J_m^1(K)/2J_m(K)$, then the orbit of (A_1, B_1) corresponds to the class $D - (Q)$ or $D - (Q')$ in $J_m(K)/2J_m(K)$ where Q' denote the hyperelliptic conjugate of Q . Hence the orbit of (A_1, B_1) is soluble.

We now treat the general case, assuming only that $J_m^1(K)$ is nonempty. Now C_m has a non-singular point Q defined over some extension K' of K of odd degree k . Let $D \in J_m^1(K)$ denote the divisor class of degree 1 obtained by taking the sum of the conjugates of Q and subtracting $\frac{k-1}{2}$ times the hyperelliptic class. We claim that the orbits correspond to D are soluble thereby completing the proof of Theorem 27. Let (A, B) is an element of $K^2 \otimes \text{Sym}_2 K^n$ with invariant binary form $f(x, y)$ and such that its associated α equals to $(x - T)(D)$ and let $F(A, B)_m$ denote the Fano variety of the associated regular pencil. Since C has a point over K' , we have seen that the K' -rational orbits (α, s) with $\alpha = (x - T)(Q)$ and hence with $\alpha = (x - T)(D)$ are soluble over K' . In other words,

$F(A, B)_m(K')$ is nonempty. Thus, as an element of $H^1(K, J_m)$, the class of $F(A, B)_m$ becomes trivial when restricted to $H^1(K', J_m)$. A standard argument using the corestriction map shows that this class is killed by the degree k of K' over K . Since $F(A, B)_m$ is a torsor of J_m of order dividing 4 and k is odd, we see that $F(A, B)_m$ must be the trivial torsor. \square

The same argument also classifies the soluble orbits for SL_n/μ_2 , provided that C has a K -rational divisor of odd degree. The descent map “ $x - T$ ” gives a map of sets

$$J^1(K)/2J(K) \rightarrow (L^\times/L^{\times 2}K^\times)_{N \equiv f_0}$$

and is either 2-to-1 or injective (depending on the triviality of the class $W[2]$ in $H^1(K, J[2])$). To see that there are no soluble orbits when C has no divisors of odd degree, we use the exact sequence of commutative algebraic groups [35, Corollary 3.22]:

$$1 \rightarrow T \rightarrow X_m \rightarrow X \rightarrow 1.$$

If $J_m^1(K)$ is empty but both $J^1(K)$ and $F(K)$ are nonempty, then the quotient of $X(K)$ by the image of $X_m(K)$ maps onto the component group $\mathbb{Z}/4\mathbb{Z}$ of X . On the other hand, this quotient injects into $H^1(K, T)$, which has exponent 2, a contradiction. Hence we have proved the following:

Theorem 28. *Let $f(x, y)$ be a binary form of degree $n = 2g + 2$ over K with $\Delta(f)$ and f_0 nonzero in K . Then soluble orbits for the action of $(\mathrm{SL}_n/\mu_2)(K)$ with invariant binary form $f(x, y)$ exist if and only if there is a K -rational divisor of odd degree on the curve $C : z^2 = f(x, y)$. In that case, they are in bijection with the cosets of $J^1(K)/2J(K)$ and the group $J(K)/2J(K)$ acts simply transitively on the set of soluble orbits.*

7 Finite and archimedean local fields

In this section we consider the orbits for the action of $(\mathrm{SL}_n/\mu_2)(K)$ on $K^2 \otimes \mathrm{Sym}_2 K^n$ when the base field K is a finite field or an archimedean local field. In particular, we compute the number of these orbits with a fixed invariant binary form $f(x, y)$.

7.1 Finite fields

Let K be a finite field of odd cardinality q . Let $f(x, y)$ be a binary form of even degree n over K with nonzero first coefficient f_0 and nonzero discriminant Δ and write $f(x, 1) = f_0 g(x)$. We factor

$$g(x) = \prod_{i=1}^m g_i(x)$$

where $g_i(x)$ has degree d_i . Then L is the product of m finite fields L_i of cardinality q^{d_i} . Since finite fields have unique extensions of any degree, we see that either one of L_i has odd degree over K or all of the L_i contain the unique quadratic extension of K . Therefore, $f(x, y)$ always has either an odd or an even factorization over K .

Since the norm map $L^\times \rightarrow K^\times$ is surjective, f_0 is always a norm. Therefore, by Corollary 19, the number of $(\mathrm{SL}_n/\mu_2)(K)$ -orbits with binary form $f(x, y)$ is 2^m if all L_i have even degree and n is

congruent to 0 (mod 4); 2^{m-1} if all L_i have even degree and n is congruent to 2 (mod 4); and 2^{m-2} if some L_i has odd degree over K . The size of the stabilizer equals to the number of even factorization of $f(x, y)$. Hence each stabilizer has size 2^m if all L_i have even degree and n is congruent to 0 (mod 4); 2^{m-1} if all L_i have even degree and n is congruent to 2 (mod 4); and 2^{m-2} if some L_i has odd degree over K . Therefore, the number of pairs $(A, B) \in K^2 \otimes \text{Sym}_2 K^n$ with invariant binary form $f(x, y)$ is $|(\text{SL}_n / \mu_2)(K)| = |\text{SL}_n(K)|$. This agrees with [1, §3.3]. Note for the purpose of application in Section 12, the main ingredients that we need are the number of orbits and the fact that all the orbits with the same invariant binary form have the same number of elements.

By Lang's theorem, we have $H^1(K, J) = H^1(K, J_m) = 0$. Then the Fano varieties F and F_m associated to an orbit always have a K -rational point, and every orbit is soluble.

7.2 \mathbb{R} and \mathbb{C}

We now classify the orbits over $K = \mathbb{R}$ and $K = \mathbb{C}$. Let $f(x, y)$ be a binary form of degree n over K with nonzero first coefficient f_0 and nonzero discriminant Δ , and write $f(x, 1) = f_0 g(x)$. Over \mathbb{C} there is a single orbit with binary form $f(x, y)$.

In the case when $K = \mathbb{R}$, we factor

$$g(x) = \prod_{i=1}^{r_1} g_i(x) \prod_{j=1}^{r_2} h_j(x)$$

where each $g_i(x)$ has degree one and each $h_j(x)$ has degree two. Then the algebra L is the product of r_1 copies of \mathbb{R} and r_2 copies of \mathbb{C} , with $r_1 + 2r_2 = n$. Note that r_1 has the same parity as n . The quotient group $\mathbb{R}^\times / \mathbb{R}^{\times 2} N(L^\times)$ is trivial unless $r_1 = 0$, in which case it has order 2. Just as in the case of finite fields, $f(x, y)$ always has either an odd or an even factorization over K .

If the form f is negative definite, then there are no orbits having invariant binary form $f(x, y)$. Indeed, in this case $r_1 = 0$ and the leading coefficient f_0 is negative. In this case, the hyperelliptic curve C with equation $z^2 = f(x, y)$ has no real points, and the map $\text{Pic}_{C/\mathbb{R}}(\mathbb{R}) \rightarrow \text{Br}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ is surjective. The real divisor classes that are not represented by real divisors have degrees congruent to $g - 1$ modulo 2. When g is even, the Jacobian $J(\mathbb{R})$ is connected and every principal homogeneous space for J is trivial. In particular, J^1 has real points (which are not represented by real divisors of odd degree). When g is odd, the real points of the Jacobian $J(\mathbb{R})$ have two connected components, and J^1 is the unique nontrivial principal homogeneous space for J . The points in the connected component of $J(\mathbb{R})$ are the real divisor classes of degree zero that are represented by real divisors.

If f is not negative definite, then the element f_0 is a norm from L^\times to \mathbb{R}^\times . Hence rational orbits exist. When $r_1 = 0$, so f is positive definite, there are two orbits if n is congruent to 0 (mod 4) and there is only one orbit if n is congruent to 2 (mod 4). In both cases, the real points of the hyperelliptic curve $C(\mathbb{R})$ and its Jacobian $J(\mathbb{R})$ are both connected and the orbits are all soluble. If $r_1 > 0$ and the form f takes both signs, then the number of orbits is 2^{r_1-2} . The hyperelliptic curve C with equation $z^2 = f(x, y)$ has $m = r_1/2$ connected components in its real locus, and $J(\mathbb{R})$ has 2^{m-1} connected components. Since the subgroup $2J(\mathbb{R})$ is equal to the connected component of $J(\mathbb{R})$, 2^{m-1} of these orbits are soluble.

The computation for the sizes of the stabilizers is similar to the finite field case. If $r_1 = 0$, then the size of the stabilizer is $2^{n/2}$ if n is congruent to 0 (mod 4) and is $2^{n/2-1}$ if n is congruent to 2 (mod 4). If $r_1 > 0$, then the size of the stabilizer is $2^{n/2+m-2}$ where $m = r_1/2$.

8 Global fields and locally soluble orbits

In this section, we assume that K is a global field of characteristic not 2. Let $f(x, y)$ be a binary form of degree $n = 2g + 2$ over K with nonzero discriminant. Let $C : z^2 = f(x, y)$ denote the associated hyperelliptic curve. Recall that an element (A, B) of $K^2 \otimes \text{Sym}_2 K^n$ (or its $(\text{SL}_n / \mu_2)(K)$ -orbit) with invariant binary form $f(x, y)$ is *locally soluble* if the associated Fano variety $F(A, B)$ over K has points over every completion K_ν . We wish to determine when rational orbits and locally soluble orbits for the action of $(\text{SL}_n / \mu_2)(K)$ on $K^2 \otimes \text{Sym}_2 K^n$ exist. Theorem 23 gives a list of necessary and sufficient conditions for the existence of rational orbits over general fields. In this section, we assume that there exists a locally soluble two-cover of J^1 over K and that $\text{Div}^1(C)$ is locally soluble. The main result is that these two conditions are sufficient for the existence of a global orbit and a locally soluble orbit.

Recall the torsor $W[2]$ of $J[2]$ which consists of points $P \in J^1$ such that $2P = d$ where d is the hyperelliptic class of C . The class of $W[2]$ in $H^1(K, J[2])$ maps to the class of J^1 in $H^1(K, J)[2]$. Since $J^1(K_\nu)$ is nonempty for all ν , we see that a priori $W[2]$ lies in the 2-Selmer subgroup $\text{Sel}_2(J/K)$ of $H^1(K, J[2])$. Let $\pi : F_0 \rightarrow J^1$ denote a locally soluble two-cover of J^1 over K . Let $F_0[4]$ denote the torsor of $J[4]$ consisting of points $x \in F_0$ such that $\pi(x) \in W[2]$. Then the class of $W[2]$ is twice the class of $F_0[4]$ in $H^1(K, J[4])$. Since $F_0(K_\nu)$ is nonempty for all ν , the class of $F_0[4]$ is in the 4-Selmer subgroup $\text{Sel}_4(J/K)$ of $H^1(K, J[4])$.

Conversely if C is any hyperelliptic curve over K with locally soluble $\text{Div}^1(C)$. If $W[2]$ is divisible by 2 in $\text{Sel}_4(J/K)$, then a locally soluble two-cover of J^1 over K exists. Indeed, suppose $W[2] = 2F[4]$ for some $F[4] \in \text{Sel}_4(J/K)$. Let F denote the principle homogeneous space of J whose class in $H^1(K, J)$ is the image of $F[4]$ in $H^1(K, J)[4]$. Then $2F = [J^1]$ and hence there exists a map $F \rightarrow J^1$ realizing F as a two-cover of J^1 .

Theorem 29. *Suppose $C : z^2 = f(x, y)$ is a hyperelliptic curve over a global field K of characteristic not 2 such that $\text{Div}^1(C)(K_\nu) \neq \emptyset$ for all places ν of K and such that J^1 admits a locally soluble two-cover over K (equivalently, $W[2]$ is divisible by 2 in $\text{Sel}_4(J/K)$). Then orbits for the action of $(\text{SL}_n / \mu_2)(K)$ on $K^2 \otimes \text{Sym}_2 K^n$ with invariant binary form $f(x, y)$ exist.*

Proof. Let $T = (\text{Res}_{K'/K} \mathbb{G}_m)_{N=1}$ be the kernel of $J_m \rightarrow J$ as in (5) where $K' = K(\sqrt{f_0})$. Let ϕ, i_2, i_4 be defined by the following diagram arising as part of the long exact sequence in Galois cohomology:

$$\begin{array}{ccccc} H^1(K, T[4]) & \xrightarrow{i_4} & H^1(K, J_m[4]) & \xrightarrow{\phi} & H^1(K, J[4]) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(K, T[2]) & \xrightarrow{i_2} & H^1(K, J_m[2]) & \longrightarrow & H^1(K, J[2]) \end{array}$$

Let $F[4]$ be a class in $\text{Sel}_4(J/K)$ such that $2F[4] = W[2]$. By Theorem 23, it suffices to show that the class of the torsor $W_m[2]$ of $J_m[2]$ is in the image of the map $H^1(K, J_m[4]) \rightarrow H^1(K, J_m[2])$ induced by multiplication by 2. We break up the proof of Proposition 29 into three steps.

Step 1: There exists a class $F_m[4]$ in $H^1(K, J_m[4])$ such that $\phi(F_m[4]) = F[4]$.

For any place ν of K , let $\phi_\nu : H^1(K_\nu, J_m[4]) \rightarrow H^1(K_\nu, J[4])$ denote the ν -adic restriction of ϕ , and let $F[4]_\nu$ denote the ν -adic restriction of $F[4]$. Since $F[4]$ is in $\text{Sel}_4(J/K)$, the restriction $F[4]_\nu$ comes from a K_ν -rational point on the Jacobian for every place ν of K . Since Div^1 is locally soluble, every K_ν -rational divisor class is representable by a K_ν -rational divisor (Proposition 20). Therefore,

$F[4]_\nu$ is in the image of ϕ_ν for every place ν of K . To show that $F[4]$ is in the image of the global ϕ , note that the cokernel of ϕ maps injectively to $H^2(K, T[4])$. Hence it suffices to show that $H^2(K, T[4])$ satisfies the local-global principle. Since $T[4] = (\text{Res}_{K'/K} \mu_4)_{N=1}$, we have the exact sequence

$$1 \rightarrow K^\times / N(K'^\times) K^{\times 4} \rightarrow H^2(K, T[4]) \rightarrow \text{Br}(K')[4]_{N=1} \rightarrow 1.$$

Now $\text{Br}(K')$ satisfies the local-global principle with respect to the places of K , and $K^\times / N(K'^\times) K^{\times 4} = K^\times / N(K'^\times)$ also satisfies the local-global principle since K'/K is cyclic.

Step 2: The class $2F_m[4]$ in $H^1(K, J_m[2])$ is in the 2-Selmer group. That is, its image in $H^1(K, J_m)$ is locally trivial.

Let F_m denote the image of $F_m[4]$ in $H^1(K, J_m)$. Fix any place ν of K and denote by $F_{m,\nu}$ and F_ν the ν -adic restrictions of F_m and F , respectively. Since $F_{m,\nu}$ maps to F_ν under the map $H^1(K_\nu, J_m) \rightarrow H^1(K_\nu, J)$ and F is locally soluble, we see that $F_{m,\nu}$ is in the image of $H^1(K_\nu, T) \rightarrow H^1(K_\nu, J_m)$. Therefore, $2F_{m,\nu}$ is the trivial torsor since $H^1(K_\nu, T)$ has exponent 2.

Step 3: There exists $c' \in H^1(K, T[4])$ such that $2(F_m[4] + i_4(c')) = W_m[2]$. This will complete the proof of Theorem 29.

Since $\phi(F_m[4]) = F[4]$, we see that $W_m[2] - 2F_m[4] = i_2(c)$ for some c in $H^1(K, T[2])$. By Step 2, the image of c under the composite map $H^1(K, T[2]) \rightarrow H^1(K, J_m[2]) \rightarrow H^1(K, J_m)$ is locally trivial. Since Div^1 is locally soluble, the map $H^1(k', T) \rightarrow H^1(k', J_m)$ is injective for $k' = K$ or K_ν for any place ν of K . Therefore, the image of c under the map $H^1(K, T[2]) \rightarrow H^1(K, T)$ is locally trivial. Since $H^1(K, T) = K^\times / N(K'^\times)$ has the local-global principle, the image of c in $H^1(K, T)$ is in fact 0. Therefore, c is in the image of the Kummer map $T(K)/2T(K) \rightarrow H^1(K, T[2])$. Hence it is also in the image of $H^1(K, T[4]) \rightarrow H^1(K, T[2])$ induced by multiplication by 2. Write $c = 2c'$ for some $c' \in H^1(K, T[4])$. Then $2(F_m[4] + i_4(c')) = W_m[2]$. \square

If we assume that $\text{Div}^1(C)$ is locally soluble, then the existence of a locally soluble two-cover of J^1 is in fact equivalent to the existence of a locally soluble orbit for the action of $(\text{SL}_n / \mu_2)(K)$ on $K^2 \otimes \text{Sym}_2 K^n$. We will see that $\text{Sel}_2(J/K)$ acts simply transitively on the set of locally soluble orbits. Therefore, we see that every locally soluble two-cover of J^1 is isomorphic to the Fano variety $F(A, B)$ associated to the pencil of quadrics determined by some $(A, B) \in K^2 \otimes \text{Sym}_2 K^n$. This also proves Theorem 13.

Theorem 30. *Suppose $C : z^2 = f(x, y)$ is a hyperelliptic curve over a global field K of characteristic not 2 such that $\text{Div}^1(C)(K_\nu) \neq \emptyset$ for all places ν of K . Then locally soluble orbits for the action of $(\text{SL}_n / \mu_2)(K)$ on $K^2 \otimes \text{Sym}_2 K^n$ exist with invariant binary form $f(x, y)$ if and only if $W[2]$ is divisible by 2 in $\text{Sel}_4(J/K)$, or equivalently that J^1 admits a locally soluble two-cover over K . Furthermore, when these conditions are satisfied, the group $\text{Sel}_2(J/K)$ acts simply transitively on the set of locally soluble orbits and this set is finite.*

Before proving Theorem 30, we note that the notion of locally soluble orbit is a tricky one. There could exist an integral binary quartic form $f(x, y)$ that has locally soluble orbits but no soluble orbits over \mathbb{Q} . For a specific example (suggested by John Cremona, see also [32, §8.1]), consider the elliptic curve E defined by the equation $y^2 = x^3 - 1221$. This curve has trivial Mordell-Weil group $E(\mathbb{Q}) = 0$ and Tate-Shafarevich group isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$. The binary quartic form $f(x, y) = 3x^4 - 12x^3y + 11xy^3 - 11y^4$ of discriminant $\Delta = -40252707 = -3^5 11^2 37^2$ corresponds to a class b in the Tate-Shafarevich group of E that is divisible by 2. Any of the elements c of order 4 in the

Tate-Shafarevich group with $2c = b$ gives a locally soluble orbit with invariant binary form $f(x, y)$. The hyperelliptic curve $z^2 = f(x, y)$ is locally soluble but has no global points; hence, by Theorem 28, there is no soluble orbit having invariant binary form $f(x, y)$.

There are also examples where rational orbits exist but there are no locally soluble orbits. For example, consider the binary quartic form $f(x, y) = -1x^4 + 2x^3y + 104x^2y^2 - 104xy^3 - 2764y^4$ of discriminant $\Delta = -2^8 571$. The associated quartic field L has discriminant $-2^4 571 = -9136$ and ring of integers $\mathbb{Z}[\theta]$, where θ is a root of the polynomial $F(t) = t^4 - 2t^2 + 2t - 3$. Since $F(1) = -2$, $F(0) = -3$, and $F(-1) = -6$, the element $\theta^3 - \theta$ in L^\times has norm $-6^2 \equiv -1 = f_0$. So there are orbits over \mathbb{Q} with this invariant quartic form. On the other hand, the hyperelliptic curve $C : z^2 = f(x, y)$ of genus one is a principal homogeneous space of order 2 for its Jacobian E , which is an elliptic curve with equation $y^2 + xy = x^3 - x^2 - 929x - 10595$ and prime conductor 571. This curve has trivial Mordell-Weil group $E(\mathbb{Q}) = 0$ and Tate-Shafarevich group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. Hence $\text{Sel}_2(E/\mathbb{Q})$ and $\text{Sel}_4(E/\mathbb{Q})$ are both isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. The curve C represents one of the nontrivial locally trivial principal homogeneous spaces for E . Since its class is not in the image of multiplication by 2 from $\text{Sel}_4(E/\mathbb{Q})$, there are no locally soluble orbits. (Thanks to John Cremona and Noam Elkies for help with computation in this example.)

Proof of Theorem 30: Suppose locally soluble orbits with invariant binary form $f(x, y)$ exist. We prove first that $\text{Sel}_2(J/K)$ acts simply transitively on the set of locally soluble orbits with invariant binary form $f(x, y)$. Indeed, suppose that (A, B) is a rational pencil with Fano variety $F(A, B)$ and invariant binary form $f(x, y)$. Any other rational pencil (A_1, B_1) with the same binary form corresponds to a class $[c]$ in $H^1(K, J[2])$ that is in the kernel of the composite map $\gamma : H^1(K, J[2]) \rightarrow H^1(K, \text{SL}_n/\mu_2) \hookrightarrow H^2(K, \mu_2)$ ([3, Proposition 1]). The map γ is cup product with the class $W[2] \in H^1(K, J[2])$ ([27, Proposition 10.3]). Let $F(A_1, B_1)$ denote the Fano variety associated to the pencil (A_1, B_1) . Then one has, up to sign (cf. Footnote 1),

$$[F(A_1, B_1)] = [F(A, B)] + [c] \tag{9}$$

in $H^1(K, J)[4]$. Since the subgroup $J(K_v)/2J(K_v)$ of $H^1(K_v, J[2])$ maps to the trivial class in $H^1(K_v, \text{SL}_n/\mu_2)$ for all places v , the Hasse principle for the cohomology of the group SL_n/μ_2 shows that the subgroup $\text{Sel}_2(J/K)$ of $H^1(K, J[2])$ also lies in $\ker \gamma$. It is then clear from (9) that if (A, B) is locally soluble, then $[c] \in \text{Sel}_2(J/K)$ if and only if (A', B') is locally soluble. Hence $\text{Sel}_2(J/K)$ acts simply transitively on the set of locally soluble orbits with invariant binary form $f(x, y)$. Since the 2-Selmer group is finite, the set of locally soluble orbits with invariant binary form $f(x, y)$ is also finite. Moreover, if (A, B) is locally soluble, then $F(A, B)$ gives a locally soluble two-cover of J^1 over K .

We now consider the sufficiency of the above two conditions for the existence of locally soluble orbits. Let F denote the Fano variety corresponding to one rational orbit with invariant binary form $f(x, y)$. The existence of this rational orbit follows from Theorem 29. Let $F[4] = F[4]_0$ denote the lift of F to a torsor of $J[4]$ consisting of elements $x \in F$ such that $x + x + x + x = 0$ in the group X of four components defined in Theorem 22. We need to show that there exists a class $c \in H^1(K, J[2])$ such that $c \cup W[2] = 0$ and $F[4] + c \in \text{Sel}_4(J/K)$. Let d_0 be a class in $\text{Sel}_4(J/K)$ such that $W[2] = 2d_0$. It suffices to show that

$$(F[4] - d_0) \cup W[2] = 0. \tag{10}$$

For ease of notation, we denote the above cup product by $e_2(F[4] - d_0, W[2])$ since the cup product is induced from the Weil pairing e_2 on $J[2]$. Since $d_0 \in \text{Sel}_4(J/K)$ is isotropic with respect to e_4 , we

have

$$e_2(F[4] - d_0, W[2]) = e_4(F[4] - d_0, d_0) = e_4(F[4], d_0).$$

Fix a place ν and denote by $F[4]_\nu, d_{0,\nu}, e_{4,\nu}$ the ν -adic restrictions. Pick any $D_\nu \in J^1(K_\nu)$. Since F arises from a pencil of quadrics, we define

$$F[2]_{D_\nu} = \{x \in F : x + x = D_\nu\}.$$

The image of this torsor of $J[2]$ in $H^1(K_\nu, J[4])$ is the following torsor:

$$F[4]_{2D_\nu - d} = \{x \in F : x + x + x + x = 2D_\nu - d\},$$

where d denotes the hyperelliptic class as before. Therefore, as elements of $H^1(K_\nu, J[4])$, we have

$$F[4]_\nu - F[2]_{D_\nu} = \delta_{4,\nu}(2D_\nu - d),$$

where $\delta_{4,\nu}$ is the Kummer map $J(K_\nu)/4J(K_\nu) \rightarrow H^1(K_\nu, J[4])$. Since $d_0 \in \text{Sel}_4(K, J)$, we see that $d_{0,\nu}$ is in the image of $\delta_{4,\nu}$. Since $J(K_\nu)/4J(K_\nu)$ is isotropic with respect to $e_{4,\nu}$, we have

$$e_{4,\nu}(F[4]_\nu, d_{0,\nu}) = e_{4,\nu}(F[2]_{D_\nu}, d_{0,\nu}) = e_{2,\nu}(F[2]_{D_\nu}, W[2]_\nu). \quad (11)$$

Choosing a different $D_\nu \in J^1(K_\nu)$ changes $F[2]_{D_\nu}$ by an element of $J(K_\nu)/2J(K_\nu)$. As $J(K_\nu)/2J(K_\nu)$ is isotropic with respect to e_2 , the last term in (11) does not depend on the choice of D_ν . Theorem 30 then follows from the following general lemma.

Lemma 31. *Suppose K is any local field of characteristic not 2. Let $f(x, y)$ be a binary form of degree $2g + 2$ with nonzero discriminant such that the associated hyperelliptic curve $C : z^2 = f(x, y)$ satisfies $\text{Div}^1(C)(K) \neq \emptyset$. Suppose there is a rational orbit for the action of $(\text{SL}_n / \mu_2)(K)$ on $K^2 \otimes \text{Sym}_2 K^n$ with invariant binary form $f(x, y)$ and let F denote the associated Fano variety. Then*

$$e_2(F[2], W[2]) = 0, \quad (12)$$

where $F[2]$ denotes any lift of F to a torsor of $J[2]$ using a point of $J^1(K)$.

Proof. The first key point is that if (12) holds for one rational orbit, then it holds for any rational orbit with the same invariant binary form. Indeed, if F' denotes the torsor of J coming from a different orbit, then $F' - F \in \ker \gamma$, where $\gamma : H^1(K, J[2]) \rightarrow H^2(K, \mu_2)$ is cup product with $W[2]$. In other words, $e_2(F' - F, W[2]) = 0$. Hence $e_2(F[2], W[2]) = e_2(F'[2], W[2])$.

The second key point is that since $\text{Div}^1(C)(K) \neq \emptyset$, there exists a soluble orbit by Theorem 28. Let F denote the corresponding torsor arising from this soluble pencil. Then $F[2] \in J(K)/2J(K)$ and hence $e_2(F[2], W[2]) = 0$. \square

This completes the proof of Theorem 30. \square

We conclude by remarking that the natural generalization of the *fake 2-Selmer set* $\text{Sel}_{2, \text{fake}}(C)$ of C ([10]), namely the *fake 2-Selmer set* $\text{Sel}_{2, \text{fake}}(J^1)$ of J^1 , is in natural bijection with the set of locally soluble orbits for the group SL_n^\pm / μ_2 , where SL_n^\pm denotes as before the subgroup of elements of GL_n with determinant ± 1 . Using the group SL_n instead of SL_n^\pm allows us to “unfake” this fake Selmer set (cf. [34]).

9 Existence of integral orbits

The purpose of this section is to prove Theorem 14. More precisely, we prove:

Theorem 32. *Assume that $n \geq 2$ is even. Let $f(x, y)$ be a binary form of degree $n = 2g + 2$ with coefficients in $16^n\mathbb{Z}$ such that the hyperelliptic curve $C : z^2 = f(x, y)$ has locally soluble Div^1 . Then every locally soluble orbit for the action of $(\text{SL}_n / \mu_2)(\mathbb{Q})$ on $\mathbb{Q}^2 \otimes \text{Sym}_2 \mathbb{Q}^n$ with invariant binary form $f(x, y)$ has an integral representative, i.e., a representative in $\mathbb{Z}^2 \otimes \text{Sym}_2 \mathbb{Z}^n$.*

By Theorem 16 with $D = \mathbb{Z}$ and \mathbb{Z}_p , it suffices to find a representative over \mathbb{Z}_p for every soluble orbit over \mathbb{Q}_p with $f(x, y) \in \mathbb{Z}_p[x, y]$. We begin by recalling from [1, §2] the construction of an integral orbit associated to a rational point on C , or a p -adically integral orbit associated to a p -adic point on C . For this we recall some of the notations in Section 2. Without loss of generality, we may assume $f_0 \neq 0$. (By our convention, C being a hyperelliptic curve is equivalent to $\Delta(f) \neq 0$.) Write $f(x, 1) = f_0 g(x)$ and let $L = \mathbb{Q}_p[x]/g(x)$ be the corresponding étale algebra of rank n over \mathbb{Q}_p . For $k = 1, 2, \dots, n-1$, there are integral elements

$$\zeta_k = f_0 \theta^k + f_1 \theta^{k-1} + \dots + f_{k-1} \theta$$

in L . Let R_f be the free \mathbb{Z}_p -submodule of L having \mathbb{Z}_p -basis $\{1, \zeta_1, \zeta_2, \dots, \zeta_{n-1}\}$. For $k = 0, 1, \dots, n-1$, let $I_f(k)$ be the free \mathbb{Z}_p -submodule of L with basis $\{1, \theta, \theta^2, \dots, \theta^k, \zeta_{k+1}, \dots, \zeta_{n-1}\}$. By Theorem 16, an integral orbit is an equivalence class of triples (I, α, s) where I is an ideal of R_f , $\alpha \in L^\times$, $s \in K^\times$ such that $I^2 \subset \alpha I_f(n-3)$, $N(I) = s\mathbb{Z}_p$ and $N(\alpha) = s^2 f_0^{n-3}$. The rational orbit is given by the equivalence class of the pair (α, s) .

Via a scaling and change of variable, we may assume that we have an integral point $P = (0, 1, c)$ on the curve $z^2 = f(x, y)$, so that the coefficient $f_n = c^2$ is a square. Then set $\alpha = \theta$, and note that

$$\theta I_f(n-3) = \text{Span}_{\mathbb{Z}_p} \{c^2, \theta, \theta^2, \dots, \theta^{n-2}, f_0 \theta^{n-1}\}. \quad (13)$$

Let $I = \text{Span}_{\mathbb{Z}_p} \{c, \theta, \theta^2, \dots, \theta^{(n-2)/2}, \zeta_{n/2}, \dots, \zeta_{n-1}\}$. Then it is easy to check that I is an ideal of R_f and that $I^2 \subseteq \alpha I_f(n-3)$ and

$$N(I)^2 = N(\theta)N(I_f(n-3)) = [c/f_0^{(n-2)/2}]^2 \mathbb{Z}_p.$$

Let $s = \pm c/f_0^{(n-2)/2}$ be such that (α, s) corresponds to the rational orbit determined by P . The triple (I, α, s) gives an integral orbit representing the soluble orbit given by P in $J^1(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$. We note that this association of an integral orbit to a \mathbb{Q} -rational point, and the paucity of integral orbits, is the key to the arguments of [1] which show that rational points are rare.

Given one such $f(x, y) = f_0 x^n + \dots + f_n y^n$ with coefficients in $16^n\mathbb{Z}$, we put $\tilde{f}(x, y) = \tilde{f}_0 x^n + \dots + \tilde{f}_n y^n$ where $\tilde{f}_i = f_i/16^{n-i}$. If $(A, B) \in \mathbb{Z}^2 \otimes \text{Sym}_2 \mathbb{Z}^n$ has invariant binary form $\tilde{f}(x, y)$, then $(4A, B)$ has invariant binary form $f(x, y)$. Therefore, Theorem 32 follows from the following proposition where the assumption on the coefficients is asymmetrical in contrast to Theorem 32.

Proposition 33. *Assume that $n \geq 2$ is even. Let $f(x, y) = f_0 x^n + \dots + f_n y^n$ be a binary form of degree $n = 2g + 2$ satisfying $f_0 \neq 0$ and $2^{4i} \mid f_i/f_0$ for $i = 1, \dots, n$, such that the hyperelliptic curve $C : z^2 = f(x, y)$ has locally soluble Div^1 . Then every locally soluble rational orbit for the action of $(\text{SL}_n / \mu_2)(\mathbb{Q})$ on $\mathbb{Q}^2 \otimes \text{Sym}_2 \mathbb{Q}^n$ with invariant binary form $f(x, y)$ has an integral representative.*

Proof. We work over \mathbb{Z}_p and give an explicit construction of the ideal I , in a manner similar to the one-point case shown above (cf. [1, §2]) and the corresponding statements in [4, Proposition 8.2] and [30, Proposition 2.9]. We begin by noting that the condition $2^{4i} \mid f_i/f_0$, which is nontrivial only when $p = 2$, implies that if $a \in \mathbb{Q}_p$ is non-integral, then $a - \theta \in L^\times$ in fact lies in $L^{\times 2}\mathbb{Q}_p^\times$. Since $\text{Div}^1(C)(\mathbb{Q}_p) \neq \emptyset$, every \mathbb{Q}_p -rational divisor class can be represented by a rational divisor by Proposition 20. Therefore, by [36, Lemma 3.8], we can represent any class in $J^1(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ by a Galois-invariant divisor of degree $m \leq g + 1$, say

$$D = (P_1) + (P_2) + \cdots + (P_m) - D^*, \quad (14)$$

where each $P_i = (a_i, b_i, c_i)$ is defined over some finite Galois extension K of \mathbb{Q}_p with $c_i \neq 0$ and D^* is a divisor supported on points above ∞ . We may assume that m is odd, for otherwise f_0 is a square in \mathbb{Q}_p^\times and we are reduced to the case of [30, Proposition 2.9]. By Theorem 16, if $D_1, D_2 \in J^1(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ have the same image in $(L^\times/L^{\times 2}\mathbb{Q}_p^\times)_{N=f_0}$ under the “ $x - T$ ” map, then a triple (I, α, s) exist for D_1 if and only if it exists for D_2 . We may assume that the coordinates of all the P_i 's lie in the ring of integers of K with $b_i = 1$, and that the a_i 's are all distinct. Indeed, the sum of all the points P_i with a_i non-integral is rational and maps to 1 in $L^\times/L^{\times 2}\mathbb{Q}_p^\times$.

Define the monic polynomial

$$P(x) = (x - a_1)(x - a_2) \cdots (x - a_m)$$

of degree m over \mathbb{Q}_p . Let $R(x)$ be the polynomial of degree $\leq m - 1$ over \mathbb{Q}_p obtained from Lagrange interpolation with the property that

$$R(a_i) = c_i, \quad 1 \leq i \leq m.$$

Then $R(x)^2 - f(x, 1) = h(x)P(x)$ in $\mathbb{Q}_p[x]$ for some $h(x) \in \mathbb{Q}_p[x]$.

The polynomial $P(x)$ clearly has coefficients in the ring \mathbb{Z}_p . When $R(x)$ also has coefficients in \mathbb{Z}_p , we define the ideal I_D of R_f as the R_f -submodule of $L = K_f$ given by

$$\langle R(\theta), P(\theta)I_f((n - 3 - m)/2) \rangle.$$

For example, when $m = 1$, the divisor D has the form (P) with $P = (a, b, c)$, and the ideal I_D is given by

$$I_D = \text{Span}_{\mathbb{Z}_p} \{c, \theta - a, (\theta - a)^2, \dots, (\theta - a)^{(n-2)/2}, \zeta_{n/2}, \dots, \zeta_{n-1}\}.$$

We claim that I_D^2 is contained in the ideal $\alpha I_f(n - 3)$ where $\alpha = P(\theta)$, and that $N(I_D)^2 = N(P(\theta))N(I_f(n - 3))$. Let s be the square root of $N(\alpha)$ such that (α, s) corresponds to the rational orbit determined by D . Thus we obtain an integral orbit mapping to the rational orbit corresponding to D . Since the case $m = 1$ has been dealt with already, we assume that $m \geq 3$.

The fact that the ideal $I_D^2 = \langle R(\theta)^2, P(\theta)R(\theta)I_f((n - 3 - m)/2), P(\theta)^2I_f(n - 3 - m) \rangle$ is contained in $P(\theta)I_f(n - 3)$ follows by observing that $f(\theta, 1) = 0$, so $R(\theta)^2 = h(\theta)P(\theta)$. It therefore suffices to show that $\langle h(\theta), R(\theta)I_f((n - 3 - m)/2), P(\theta)I_f(n - 3 - m) \rangle$ is contained in $I_f(n - 3)$, and this follows from the fact that P has degree m , $R(x)$ has degree less than m and hence degree at most $(n - 3 + m)/2$, and h has degree at most $n - m$ and thus at most $n - 3$. (Note that the leading coefficient of h is f_0 . Therefore, even when $m = 1$, one still has $h(\theta) \in I_f(n - 3)$.)

To compute the norm of I_D , we use a specialization argument. Let \mathcal{R} denote the ring

$$\mathcal{R} = \mathbb{Z}_p[f_0, \dots, f_n, a_1, \dots, a_m][\sqrt{f(a_1, 1)}, \dots, \sqrt{f(a_m, 1)}],$$

where $f(x, 1) = f_0x^n + \cdots + f_n$. Write $c_i = \sqrt{f(a_i, 1)}$ for each $i = 1, \dots, m$. Inside $\mathcal{R}[x]/f(x, 1)$, we define $\zeta_1, \dots, \zeta_{n-1}$ as before and denote the corresponding R_f, I_f, I_D by $\mathcal{R}_f, \mathcal{I}_f, \mathcal{I}_D$. One has the notion of $N\mathcal{I}_D$ as an \mathcal{R} -submodule of the fraction field of \mathcal{R} .

We claim that $N\mathcal{I}_D$ is the principal ideal generated by $s = c_1 \cdots c_m / f_0^{(n-3+m)/2}$. Specializing to particular $f_0, \dots, f_n, a_1, \dots, a_m$ then completes the proof. We prove this claim by first inverting f_0 . In this case, the result follows from [3, Proposition 8.5]. Next we localize at (f_0) to check that the correct power of f_0 is attained. Since every ideal is invertible now, it suffices to show that $\mathcal{I}_D^2 = P(\theta)\mathcal{I}_f^{n-3}$ which follows from the statements

$$(\theta - a_i)(\mathcal{R}_f)_{(f_0)} = (\mathcal{I}_f)_{(f_0)} \quad (15)$$

for $i = 1, \dots, m$. To see that (15) is sufficient, we note that $P(\theta)(\mathcal{R}_f)_{(f_0)} = (\mathcal{I}_f(m))_{(f_0)}$ since $P(\theta)$ is the product of all $\theta - a_i$. Therefore,

$$P(\theta)(\mathcal{I}_f(n-3))_{(f_0)} = P(\theta)^2(\mathcal{I}_f(n-3-m))_{(f_0)} \subset (\mathcal{I}_D)_{(f_0)}^2 \subset P(\theta)(\mathcal{I}_f(n-3))_{(f_0)}.$$

To prove (15), note that the containment \subset is clear since $\theta - a_i \in \mathcal{I}_f$; equality follows because they have the same norm. We now give another more explicit proof. Note that it remains to show that $1 \in (\theta - a_i)(\mathcal{R}_f)_{(f_0)}$. Consider the polynomial $h_i(t) = (f(t, 1) - c_i^2)/(t - a_i)$. By definition $h_i(\theta)(\theta - a_i) = -c_i^2$. Moreover, writing out $h_i(t)$ explicitly, one sees that

$$h_i(\theta) = \zeta_{n-1} + a_i\zeta_{n-2} + a_i^2\zeta_{n-3} + \cdots + a_i^{n-2}\zeta_1 + h_i(0) \in \mathcal{R}_f.$$

This shows that $c_i^2 \in (\theta - a_i)(\mathcal{R}_f)_{(f_0)}$, and hence $1 \in (\theta - a_i)(\mathcal{R}_f)_{(f_0)}$ since c_i is a unit in $(\mathcal{R}_f)_{(f_0)}$.

Suppose now that $R(x)$ is not integral. Let $z^2 = f(x, 1)$ denote an affine model for the given hyperelliptic curve. A Newton polygon analysis on $f(x, 1) - R(x)^2$ shows that $\text{div}(z - R(x)) - [D]$ has the form $D^* + E$ with $D^* \in J^1(\mathbb{Q}_p)$ and $E \in J(\mathbb{Q}_p)$, where D^* can be expressed in (14) with m replaced by $m - 2$ and the x -coordinates of the non-infinity points in E have negative valuation. The condition of divisibility on the coefficients of $f(x, y)$ ensures that $(x - \theta)(E) \in L^{\times 2}\mathbb{Q}_p^{\times}$. The proof now concludes by induction on the number m of points in D . Once $m \leq 1$ the polynomials $P(x)$ and $R(x)$ are both integral. \square

The following result will be important to us in Section 11.

Proposition 34. *Let p be any odd prime, and let $f(x, y) \in \mathbb{Z}_p[x, y]$ be a binary form of even degree n such that $p^2 \nmid \Delta(f)$ and $f_0 \neq 0$. Let C denote the hyperelliptic curve $z^2 = f(x, y)$. Suppose that $\text{Div}^1(C)(\mathbb{Q}_p) \neq \emptyset$. Then the $(\text{SL}_n / \mu_2)(\mathbb{Z}_p)$ -orbits on $\mathbb{Z}_p^2 \otimes \text{Sym}_2 \mathbb{Z}_p^n$ with invariant binary form $f(x, y)$ are in bijection with soluble $(\text{SL}_n / \mu_2)(\mathbb{Q}_p)$ -orbits on $\mathbb{Q}_p^2 \otimes \text{Sym}_2 \mathbb{Q}_p^n$ with invariant binary form $f(x, y)$. Furthermore, if $(A, B) \in \mathbb{Z}_p^2 \otimes \text{Sym}_2 \mathbb{Z}_p^n$ with invariant binary form $f(x, y)$, then $\text{Stab}_{(\text{SL}_n / \mu_2)(\mathbb{Z}_p)}(A, B) = \text{Stab}_{(\text{SL}_n / \mu_2)(\mathbb{Q}_p)}(A, B)$.*

Proof. As noted earlier, we only need to focus on the pair (I, α) . The condition $p^2 \nmid \Delta(f)$ implies that the order R_f is maximal and that the projective closure \mathcal{C} of C over $\text{Spec}(\mathbb{Z}_p)$ is regular. By Theorem 28, the assumption that $\text{Div}^1(C)(\mathbb{Q}_p) \neq \emptyset$ implies that soluble \mathbb{Q}_p -orbits with invariant binary form $f(x, y)$ exist. Since p is odd, the p -adic version of Proposition 33 implies that \mathbb{Z}_p -orbits with invariant binary form $f(x, y)$ exist. Therefore, by Remark 17, the set of equivalence classes of pairs (I, α) is nonempty and is in bijection with $(R_f^{\times} / R_f^{\times 2} \mathbb{Z}_p^{\times})_{N \equiv 1}$. Let \mathcal{J} denote the Néron model of J

over $\text{Spec}(\mathbb{Z}_p)$. Since \mathcal{C} is regular, \mathcal{J} is connected and we have via flat cohomology ([30, Proposition 2.11]) that

$$\mathcal{J}(\mathbb{Z}_p)/2\mathcal{J}(\mathbb{Z}_p) \simeq (R_f^\times/R_f^{\times 2}\mathbb{Z}_p^\times)_{N \equiv 1}.$$

The Néron mapping property implies that $\mathcal{J}(\mathbb{Z}_p)/2\mathcal{J}(\mathbb{Z}_p) = J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$. For the stabilizer statement, consider the exact sequence (3). Since $L^\times[2] = R_f^\times[2]$, it remains to compare $(L^{\times 2} \cap \mathbb{Q}_p^\times)/\mathbb{Q}_p^{\times 2}$ and $(R_f^{\times 2} \cap \mathbb{Z}_p^\times)/\mathbb{Z}_p^{\times 2}$. These two sets are only nonempty when L contains a quadratic extension K' of \mathbb{Q}_p . The condition $p^2 \nmid \Delta(f)$ implies that $K' = \mathbb{Q}_p(\sqrt{u})$ can only be the unramified quadratic extension of \mathbb{Q}_p . In other words, $u \in \mathbb{Z}_p^\times$. Hence in this case $(L^{\times 2} \cap \mathbb{Q}_p^\times)/\mathbb{Q}_p^{\times 2}$ and $(R_f^{\times 2} \cap \mathbb{Z}_p^\times)/\mathbb{Z}_p^{\times 2}$ both are equal to the group of order 2 generated by the class of u . \square

10 The number of irreducible integral orbits of bounded height

Let $V = \text{Sym}_2(W^*) \oplus \text{Sym}_2(W^*)$ be the scheme of pairs of symmetric bilinear forms on W . Define the height of an element $v \in V_{\mathbb{Z}}$ by $H(v) := H(f_v)$. In [1, §4], the asymptotic number of irreducible $\text{SL}_n^{\pm 1}(\mathbb{Z})$ -orbits on $V(\mathbb{Z})$ having height less than X was determined, and also the number of such orbits whose invariant binary forms $f(x, y)$ satisfy any finite set of congruences. The same computation applies also with $G = \text{SL}_n/\mu_2$ in place of $\text{SL}_n^{\pm 1}$. We assume henceforth that n is even.

To state this counting result precisely, recall ([1, §4.1.1]) that we may naturally partition the set of elements in $V(\mathbb{R})$ with $\Delta \neq 0$ and nonnegative definite invariant binary n -ic form into $\sum_{m=0}^{n/2} \tau(m)$ components, which we denote by $V^{(m, \tau)}$ for $m = 0, \dots, n/2$ and $\tau = 1, \dots, \tau(m)$ where $\tau(m) = 2^{2m-2}$ if $m > 1$; $\tau(0) = 2$ if n is congruent to 0 (mod 4); and $\tau(0) = 1$ if n is congruent to 2 (mod 4). In [1, §4.1.1], when $m > 0$, there are 2^{2m-1} choices for the parameter τ as it runs over all assignments of signs \pm to the $2m$ real linear factors of $f(x, y)$ subject to the condition that the product of the signs matches the sign of leading coefficient of $f(x, y)$. When using the group $(\text{SL}_n/\mu_2)(\mathbb{R})$, two such τ_1, τ_2 are equivalent if and only if the sign assignments associated to τ_1 are exactly the negatives of those associated to τ_2 .

For a given value of m , the component $V^{(m, \tau)}$ in $V(\mathbb{R})$ maps to the component $I(m)$ of nonnegative definite binary n -ic forms in \mathbb{R}^{n+1} having nonzero discriminant and $2m$ real linear factors. Let $F^{(m, \tau)}$ denote a fundamental domain for the action of $G(\mathbb{Z})$ on $V^{(m, \tau)}$, and set

$$c_{m, \tau} = \text{Vol}(F^{(m, \tau)} \cap \{v \in V(\mathbb{R}) : H(v) < 1\}).$$

The number of τ 's that correspond to orbits soluble at \mathbb{R} is $\#(J^1(\mathbb{R})/2J(\mathbb{R}))$ where J denotes the Jacobian of a hyperelliptic curve $z^2 = f(x, y)$ with $f(x, y) \in I(m)$. The size of this quotient does not depend on the choice of $f(x, y) \in I(m)$. Then from [1, Theorems 9 and 17], we obtain:

Theorem 35. *Fix m, τ . For any $G(\mathbb{Z})$ -invariant set $S \subset V(\mathbb{Z})^{(m, \tau)} := V(\mathbb{Z}) \cap V^{(m, \tau)}$ defined by finitely many congruence conditions, let $N(S; X)$ denote the number of $G(\mathbb{Z})$ -equivalence classes of elements $v \in S$ satisfying $H(v) < X$. Then*

$$N(S; X) = c_{m, \tau} \cdot \prod_p \mu_p(S) \cdot X^{n+1} + o(X^{n+1}),$$

where $\mu_p(S)$ denotes the p -adic density of S in $V(\mathbb{Z})$.

11 Sieving to locally soluble orbits

Since local solubility is defined by infinitely many congruence conditions, we need a weighted version of Theorem 35 in which we allow weights to be defined by certain infinite sets of congruence conditions. The technique for proving such a result involves using Theorem 35 to impose more and more congruence conditions. While doing so, we need to uniformly bound the error term. To this end, we have the following proposition proven in [2].

Proposition 36. *For each prime p , let W_p denote the set of elements $v = (A, B) \in V(\mathbb{Z})$ such that $p^2 \mid \Delta(\text{disc}(Ax - By))$. Then there exists $\delta > 0$ such that, for any $M > 0$, we have*

$$\sum_{p > M} N(W_p; X) = O(X^{n+1}/M^\delta),$$

where the implied constant is independent of X and M .

To describe which weight functions on $V(\mathbb{Z})$ are allowed, we need the following definition motivated by the above proposition:

Definition 37. Suppose $W = \mathbb{A}^M$ is some affine space. A function $\phi : W(\mathbb{Z}) \rightarrow [0, 1]$ is said to be *defined by congruence conditions* if there exist local functions $\phi_p : W(\mathbb{Z}_p) \rightarrow [0, 1]$ satisfying the following conditions:

1. For all $v \in W(\mathbb{Z})$, the product $\prod_p \phi_p(v)$ converges to $\phi(v)$.
2. For each prime p , the function ϕ_p is locally constant outside some (p -adically) closed subset of $W(\mathbb{Z}_p)$ of measure 0.
3. The p -adic integral $\int_{W(\mathbb{Z}_p)} \phi_p(v) dv$ is nonzero.

A subset W' of $W(\mathbb{Z})$ is said to be *defined by congruence conditions* if its characteristic function is defined by congruence conditions.

A function $\phi : V(\mathbb{Z}) \rightarrow [0, 1]$ is said to be *acceptable* if, for all sufficiently large p , we have $\phi_p(v) = 1$ whenever $p^2 \nmid \Delta(\text{disc}(Ax - By))$.

Then we have the following theorem.

Theorem 38. *Let $\phi : V(\mathbb{Z}) \rightarrow [0, 1]$ be a function that is defined by congruence conditions via local functions $\phi_p : V(\mathbb{Z}_p) \rightarrow [0, 1]$. Fix m, τ . Let S be an $G(\mathbb{Z})$ -invariant subset of $V(\mathbb{Z})^{(m, \tau)}$ defined by congruence conditions. Let $N_\phi(S; X)$ denote the number of $G(\mathbb{Z})$ -equivalence classes of irreducible elements $v \in S$ having height bounded by X , where each equivalence class $G(\mathbb{Z})v$ is counted with weight $\phi(v)$. If ϕ is acceptable, then*

$$N_\phi(S; X) = c_{m, \tau} \prod_p \int_{v \in V(\mathbb{Z}_p)} \phi_p(v) dv + o(X^{n+1}).$$

Theorem 38 follows from Theorem 35 and Proposition 36 just as [6, Theorem 2.20] followed from [6, Theorems 2.12 and 2.13].

Let F_0 denote the set of all integral binary forms $f(x, y)$ of degree n . Identify the scheme of all binary n -ic forms over \mathbb{Z} with $\mathbb{A}_{\mathbb{Z}}^{n+1}$. If F is a subset of F_0 , denote by $F(\mathbb{F}_p)$ the reduction modulo p of the p -adic closure of F in $\mathbb{A}_{\mathbb{Z}}^{n+1}(\mathbb{Z}_p)$.

Definition 39. A subset F of F_0 is *large* if the following conditions are satisfied:

1. It is defined by congruence conditions,
2. There exists a subscheme S_0 of $\mathbb{A}_{\mathbb{Z}}^{n+1}$ of codimension at least 2 such that for all but finitely many p , we have $F_0(\mathbb{F}_p) \setminus F(\mathbb{F}_p) \subset S_0(\mathbb{F}_p)$.

We identify hyperelliptic curves with their associated binary forms. Thus, we say that a family of hyperelliptic curves $z^2 = f(x, y)$ is *large* if the set of binary forms $f(x, y)$ appearing is large.

As an example, the subset F_1 of F_0 consisting of binary n -ic forms $f(x, y)$ such that the corresponding hyperelliptic curves C given by $z^2 = f(x, y)$ have locally soluble Div^1 is large. The set $F_2 \subset F_1$ of integral binary n -ic forms such that the corresponding hyperelliptic curve C is locally soluble is also large. These two statements follow from [25, Lemma 15]. Our aim is to prove Theorem 4 for large families of hyperelliptic curves whose associated binary forms are contained in F_1 .

Let F be a large subset of F_0 contained in F_1 . Since the curves $z^2 = f(x, y)$ and $z^2 = \kappa^2 f(x, y)$ are isomorphic over \mathbb{Q} where κ is the constant in Theorem 14, we assume without loss of generality that the coefficients of every $f(x, y)$ in $\text{Inv}(F)$ lie in $\kappa^2 \mathbb{Z}$. To prove Theorem 4, we need to weight each locally soluble element $v \in V(\mathbb{Z})$ having invariants in $\text{Inv}(F)$ by the reciprocal of the number of $G(\mathbb{Z})$ -orbits in the $G(\mathbb{Q})$ -equivalence class of v in $V(\mathbb{Z})$. However, in order for our weight function to be defined by congruence conditions, we instead define the following weight function $w : V(\mathbb{Z}) \rightarrow [0, 1]$:

$$w(v) := \begin{cases} \left(\sum_{v'} \frac{\# \text{Stab}_{G(\mathbb{Q})}(v')}{\# \text{Stab}_{G(\mathbb{Z})}(v')} \right)^{-1} & \text{if } v \text{ is locally soluble with invariant in } \text{Inv}(F), \\ 0 & \text{otherwise,} \end{cases} \quad (16)$$

where the sum is over a complete set of representatives for the action of $G(\mathbb{Z})$ on the $G(\mathbb{Q})$ -equivalence class of v in $V(\mathbb{Z})$. We then have the following theorem:

Theorem 40. *Let F be a large subset of F_0 contained in F_1 . Moreover, suppose that the coefficients of every $f(x, y)$ in $\text{Inv}(F)$ lie in $16^n \mathbb{Z}$. Then*

$$\sum_{\substack{C \in F \\ H(C) < X}} \# \text{Sel}_2(J^1) = \sum_{m=0}^{n/2} \sum_{\tau \text{ soluble}} N_w(V(\mathbb{Z})_F^{(m, \tau)}; X) + o(X^{n+1}). \quad (17)$$

where $V(\mathbb{Z})_F^{(m, \tau)}$ is the set of all elements in $V(\mathbb{Z})^{(m, \tau)}$ with invariant binary forms in $\text{Inv}(F)$.

Proof. By Theorems 30 and 32, the left hand side is equal to the number of $G(\mathbb{Q})$ -equivalence classes of elements in $V(\mathbb{Z})$ that are locally soluble, have invariants in $\text{Inv}(F)$, and have height bounded by X . Given a locally soluble element $v \in V(\mathbb{Z})$ with invariant in $\text{Inv}(F)$, let v_1, \dots, v_k denote a complete set of representatives for the action of $G(\mathbb{Z})$ on the $G(\mathbb{Q})$ -equivalence class of v in $V(\mathbb{Z})$. Then

$$\sum_{i=1}^k \frac{w(v_i)}{\# \text{Stab}_{G(\mathbb{Z})}(v_i)} = \left(\sum_{i=1}^k \frac{\# \text{Stab}_{G(\mathbb{Q})}(v)}{\# \text{Stab}_{G(\mathbb{Z})}(v_i)} \right)^{-1} \sum_{i=1}^k \frac{1}{\# \text{Stab}_{G(\mathbb{Z})}(v_i)} = \frac{1}{\# \text{Stab}_{G(\mathbb{Q})}(v)}. \quad (18)$$

When $\text{Stab}_{G(\mathbb{Q})}(v)$ is trivial, which happens for all but negligibly many $v \in V(\mathbb{Z})$ by [1, Proposition 14], (18) simplifies to

$$\sum_{i=1}^k w(v_i) = 1. \quad (19)$$

Since the size of $\text{Stab}_{G(\mathbb{Q})}(v)$ is bounded above by 2^{2g} , (19) always holds up to an absolutely bounded factor. Therefore, the right hand side of (17) counts the number of $G(\mathbb{Q})$ -equivalence classes of elements in $V(\mathbb{Z})$ that are locally soluble, have invariants in F , and have height bounded by X . \square

In order to apply Theorem 38 to compute $N_w(V(\mathbb{Z})^{(m,\tau)}; X)$, we need to know that w is an acceptable function defined by congruence conditions. The proof that w is a product $\prod_p w_p$ of local weight functions is identical to the proof of [6, Proposition 3.6]. To prove that w is acceptable, it remains to show that for p sufficiently large, $w(v) = 1$ whenever $p^2 \nmid \Delta(\text{disc}(Ax - By))$. This follows from Proposition 34. Therefore, to compute $N_w(V(\mathbb{Z})^{(m,\tau)}; X)$, it remains to compute $c_{m,\tau}$ and the p -adic integrals $\int w_p(v)dv$. For these, we have the following results:

$$\begin{aligned} c_{m,\tau} &= \frac{|\mathcal{J}|\text{Vol}(G(\mathbb{Z})\backslash G(\mathbb{R}))}{\#J^{(m)}[2](\mathbb{R})}\text{Vol}(\{f \in I(m) \mid H(f) < X\}); \\ \int_{v \in V(\mathbb{Z}_p)} w_p(v)dv &= |\mathcal{J}|_p \text{Vol}(G(\mathbb{Z}_p))\text{Vol}(\text{Inv}_p(F)) \frac{\#(J^1(\mathbb{Q}_p)/2J(\mathbb{Q}_p))}{\#J[2](\mathbb{Q}_p)}. \end{aligned}$$

Here \mathcal{J} is a nonzero rational constant; $J^{(m)}$ denotes the Jacobian of any hyperelliptic curve defined by $z^2 = f(x, y)$ where $f(x, y) \in \mathbb{Z}[x, y] \cap I(m)$; and J denotes the Jacobian of any hyperelliptic curve defined by $z^2 = f(x, y)$ where $f(x, y) \in \text{Inv}(F)$; and $\text{Inv}_p(F)$ is the p -adic closure of $\text{Inv}(F)$. The first equation is proved in [1, §4.4]. The second equation follows from the identical computation as in [30, §4.5].

For every place ν of \mathbb{Q} , we let a_ν denote the following quotient:

$$a_\nu = \frac{\#(J^1(\mathbb{Q}_\nu)/2J(\mathbb{Q}_\nu))}{\#J[2](\mathbb{Q}_\nu)}.$$

Because of the assumption that $J^1(\mathbb{Q}_\nu) \neq \emptyset$, this quotient depends only on ν, g . Indeed, it is equal to 2^{-g} for $\nu = \infty$, 2^g for $\nu = 2$, and 1 for all other primes (see, e.g., [3, Lemma 12.3]). The a_ν 's satisfy the product formula $\prod_\nu a_\nu = 1$.

We now combine Theorem 38, Theorem 40, and the product formula $\prod_\nu |\mathcal{J}|_\nu = 1$ to obtain:

Theorem 41. *Let F be a large subset of F_0 contained in F_1 . Moreover, suppose that the coefficients of every $f(x, y)$ in $\text{Inv}(F)$ lie in $16^n\mathbb{Z}$. Then*

$$\sum_{\substack{C \in F \\ H(C) < X}} \# \text{Sel}_2(J^1) = \tau(G)\text{Vol}(\{f \in I(m) \mid H(f) < X\}) \prod_p \text{Vol}(\text{Inv}_p(F)) + o(X^{n+1}), \quad (20)$$

where $\tau(G) = 2$ denotes the Tamagawa number of G .

12 Proofs of main theorems

All the results stated in the introduction, with the exception of Theorems 1–3, hold even if for each $g \geq 1$ we range over any large congruence family of hyperelliptic curves C over \mathbb{Q} of genus g for which $\text{Div}^1(C)$ is locally soluble. (See Definition 39 for the definition of “large”.)

We prove Theorems 4 and 5 in this generality.

Proof of Theorem 4: Let F be a large family of hyperelliptic curves with locally soluble Div^1 . Since Condition 2 in Definition 39 is a mod p condition, a similar uniformity estimate as in Proposition 36 counting the number of hyperelliptic curves in F with bounded height is given by [26]. Theorem 38 then gives

$$\sum_{\substack{C \in F \\ H(C) < X}} 1 = \text{Vol}(\{f \in I(m) \mid H(f) < X\}) \prod_p \text{Vol}(\text{Inv}_p(F)) + o(X^{n+1}), \quad (21)$$

and dividing (20) by (21) gives Theorem 4. \square

Proof of Theorem 5: Let F be a large family of hyperelliptic curves C with locally soluble Div^1 . Let $k > 0$ be an odd integer. Recall that the 2-Selmer set of order k is defined to be the subset of elements of $\text{Sel}_2(J^1)$ that locally everywhere come from points in $J^1(\mathbb{Q}_\nu)$ of the form $d_1 - \frac{k-1}{2}d$ where d_1 is an effective divisor of degree k and d is the hyperelliptic class. To obtain the average size of this 2-Selmer set of order k , we need to perform a further sieve from the whole 2-Selmer set to this subset. Let $\varphi_\nu \leq 1$ denote the local sieving factor at a place ν of \mathbb{Q} . Therefore, to prove that the average size of the 2-Selmer set of order k is less than 2, it suffices to show that $\varphi_\nu < 1$ for some ν .

We use the archimedean place. Suppose $f(x, y)$ is a degree $2g + 2$ binary form having $2m$ real linear factors and let C be its associated hyperelliptic curve with $m > 0$. Then $C(\mathbb{R})$ has m connected components and $J(\mathbb{R})/2J(\mathbb{R})$ has size 2^{m-1} . Let σ denote complex conjugation. Then for any $P \in C(\mathbb{C})$ with x -coordinate $t \in \mathbb{C}^\times$, we have that $(t - \beta)(\sigma t - \beta) = N_{\mathbb{C}/\mathbb{R}}(t - \beta) \in \mathbb{R}^{\times 2}$ for any $\beta \in \mathbb{R}$. Hence the descent “ $x - T$ ” map sends the class of $(P) + (\sigma P) - d$ to 1 in $L^\times/L^{\times 2}\mathbb{R}$ where L denotes the étale algebra of rank n associated to $f(x, y)$. Thus $(P) + (\sigma P) - d \in 2J(\mathbb{R})$. Therefore, the image of $(\text{Sym}^k(C))(\mathbb{R})$ in $J^1(\mathbb{R})/2J(\mathbb{R})$ is equal to the image of $\text{Sym}^k(C(\mathbb{R}))$ in $J^1(\mathbb{R})/2J(\mathbb{R})$. Since m is positive, C has a rational Weierstrass point over \mathbb{R} . Hence if $P \in C(\mathbb{R})$, then $2(P) - d \in 2J(\mathbb{R})$. Since $C(\mathbb{R})$ has m connected components, we see that the image of $\text{Sym}^k(C(\mathbb{R}))$ in $J^1(\mathbb{R})/2J(\mathbb{R})$ has size at most

$$S_m(k) = \binom{m}{1} + \binom{m}{3} + \cdots + \binom{m}{k}.$$

There is a positive proportion of hyperelliptic curves $C : z^2 = f(x, y)$ in F such that $f(x, y)$ splits completely over \mathbb{R} . For any odd integer $k < g$, we have $S_{g+1}(k) < 2^g = |J^1(\mathbb{R})/2J(\mathbb{R})|$. Therefore, $\varphi_\infty < 1$.

Consider now the second statement that the average size of the 2-Selmer set of order k goes to 0 as g approaches ∞ . We may use the archimedean place again. Suppose $f(x, y)$ is a degree $n = 2g + 2$ binary form having $2m$ real linear factors and let C be its associated hyperelliptic curve. For a fixed odd integer $k > 0$, we have

$$\lim_{m \rightarrow \infty} \frac{S_m(k)}{2^{m-1}} = 0. \quad (22)$$

On the other hand, [15, Theorem 1.2] states that the density of real polynomials of degree n having

fewer than $\log n / \log \log n$ real roots is $O(n^{-b+o(1)})$ for some $b > 0$. Therefore, the result now follows from this and (22) since $2^{m-1} = |J^1(\mathbb{R})/2J(\mathbb{R})|$. \square

Our approach to Theorem 3 (which in turn implies Theorems 1 and 2) using a result of Dokchitser and Dokchitser (Appendix A) does not work in the generality of large families, but does work for “admissible” families as defined below.

Definition 42. A subset F of the set F_0 of all integral binary forms of degree n is *admissible* if the following conditions are satisfied:

1. It is defined by congruence conditions;
2. For large enough primes p , the p -adic closure of F contains all binary forms $f(x, y)$ of degree n over \mathbb{Z}_p such that the hyperelliptic curve $z^2 = f(x, y)$ has a \mathbb{Q}_p -rational point.

We say that a family of hyperelliptic curves $z^2 = f(x, y)$ is *admissible* if the set of binary forms $f(x, y)$ appearing is admissible.

To prove Theorem 3 where we range over any admissible family of hyperelliptic curves over \mathbb{Q} of genus $g \geq 1$ with locally soluble Div^1 , we note that the result of Dokchitser and Dokchitser holds for admissible families (Theorem A.2). The rest of the proof is identical to that given in the introduction.

We conclude by giving a version of Theorem 1 in the most general setting that our methods allow.

Theorem 43. *Suppose F is a large congruence family of integral binary forms of degree $n = 2g + 2$ for which there exist two primes p, q neither of which is a quadratic residue modulo the other such that the following conditions hold for a positive proportion of $f(x, y)$ in F :*

1. *The four integral binary forms $f(x, y)$, $pf(x, y)$, $qf(x, y)$, $pqf(x, y)$ all lie inside F and the corresponding hyperelliptic curves have points over \mathbb{Q}_p and \mathbb{Q}_q .*
2. *If J denotes the Jacobian of the hyperelliptic curve $z^2 = f(x, y)$, then J has split semistable reduction of toric dimension 1 at p and good reduction at q .*

Then for a positive proportion of binary forms $f(x, y)$ in F , the corresponding hyperelliptic curve $C : z^2 = f(x, y)$ has no points over any odd degree extension of \mathbb{Q} (i.e., the variety J^1 has no rational points), and moreover the 2-Selmer set $\text{Sel}_2(J^1)$ is empty.

Appendix A: A positive proportion of hyperelliptic curves have odd/even 2-Selmer rank

by Tim and Vladimir Dokchitser

In this appendix we show that both odd and even 2-Selmer ranks occur a positive proportion of the time among hyperelliptic curves of a given genus.

For an abelian variety A defined over a number field K , write $\text{rk}_2(A/K) = \dim_{\mathbb{F}_2} \text{Sel}_2(A/K)$ for the 2-Selmer rank, and $\text{rk}_{2^\infty}(A/K)$ for the 2^∞ -Selmer rank². We will say ‘rank of a curve’ meaning ‘rank of its Jacobian’.

² Mordell–Weil rank + number of copies of $\mathbb{Q}_2/\mathbb{Z}_2$ in $\text{III}_{A/K}$; if III is finite, this is just the Mordell–Weil rank.

Theorem A.1. *The proportion of both odd and even 2^∞ -Selmer ranks in the family of hyperelliptic curves over \mathbb{Q} ,*

$$y^2 = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \quad (n \geq 3),$$

ordered by height as in (2) is at least 2^{-4n-4} . In particular, assuming finiteness of the 2-part of III, at least these proportions of curves have Jacobians of odd and of even Mordell–Weil rank.

Theorem A.2. *Let K be a number field with ring of integers \mathcal{O} . Fix $n \geq 3$. Consider the family of all hyperelliptic curves*

$$y^2 = a_n x^n + \cdots + a_0, \quad a_i \in \mathcal{O},$$

or any other “admissible” family (see Definition 42). Then a positive proportion of the hyperelliptic curves in the family, when ordered by height, have even 2-Selmer rank and a positive proportion have odd 2-Selmer rank. The same conclusion holds for the 2^∞ -Selmer rank.

The proofs resemble that of [7, §4.1] for elliptic curves over \mathbb{Q} . Recall that the conjecture of Birch and Swinnerton-Dyer implies, in particular, that the parity of the rank of an elliptic curve E is determined by whether its root number — that is, the sign of the functional equation of the L -function $L(E, s)$ of E — is $+1$ or -1 . The proof in [7] uses that twisting by -1 does not affect the height of the curve but often changes the root number, and that the parity of the Selmer rank is (unconjecturally) compatible with the root number.

This compatibility is not known for hyperelliptic curves (but see the forthcoming work of A. Morgan for 2-Selmer ranks for quadratic twists). Instead, we tweak the argument to use Brauer relations in biquadratic extensions, where it is known in enough cases. To illustrate the method, consider an elliptic curve E/\mathbb{Q} with split multiplicative reduction at 2. Then it has root number -1 over $F = \mathbb{Q}(i, \sqrt{2})$, since the unique place above 2 in F contributes -1 , while every other rational place splits into an even number of places in F and so contributes $+1$. In other words, the sum of the Mordell–Weil ranks for the four quadratic twists

$$\mathrm{rk}(E/F) = \mathrm{rk}(E/\mathbb{Q}) + \mathrm{rk}(E_{-1}/\mathbb{Q}) + \mathrm{rk}(E_2/\mathbb{Q}) + \mathrm{rk}(E_{-2}/\mathbb{Q}) \quad (*)$$

should be odd, and so both odd and even rank should occur among the 4 twists. The point is that for the 2^∞ -Selmer rank, the parity in $(*)$ can be computed unconditionally, using a Brauer relation in $\mathrm{Gal}(F/\mathbb{Q}) \cong C_2 \times C_2$. Moreover, this works for general abelian varieties and over a general number field K , replacing $\mathbb{Q}(i, \sqrt{2})$ by a suitable biquadratic extension of K . The fact that most of the decomposition groups are cyclic allows us to avoid all the hard local computations and restrictions on the reduction types, and varying the curve in the family gives the required positive proportions.

The exact result we will use is:

Theorem A.3. *Let $F = K(\sqrt{\alpha}, \sqrt{\beta})$ be a biquadratic extension of number fields. Suppose that some prime \mathfrak{p}_0 of K has a unique prime above it in F . Let C/K be a curve with Jacobian J , such that*

1. $C(K_{\mathfrak{p}_0}) \neq \emptyset$ and J has split semistable reduction of toric dimension 1 at \mathfrak{p}_0 ;
2. $C(K_{\mathfrak{p}}) \neq \emptyset$ and J has good reduction at \mathfrak{p} for every $\mathfrak{p} \neq \mathfrak{p}_0$ that has a unique prime above it in F/K .

Then

$$\mathrm{rk}_{2^\infty}(J/K) + \mathrm{rk}_{2^\infty}(J_\alpha/K) + \mathrm{rk}_{2^\infty}(J_\beta/K) + \mathrm{rk}_{2^\infty}(J_{\alpha\beta}/K) \equiv 1 \pmod{2}.$$

If, in addition, $C_\alpha(K_{\mathfrak{p}})$, $C_\beta(K_{\mathfrak{p}})$ and $C_{\alpha\beta}(K_{\mathfrak{p}})$ are non-empty for all primes \mathfrak{p} of K that have a unique prime above them in F , then the same conclusion holds for the 2-Selmer rank as well.

Postponing the proof of this theorem, we first explain how it implies Theorems A.1 and A.2.

Proof of Theorem A.1

For Theorem A.1, it suffices to prove the following:

Proposition A.4. *Consider a squarefree polynomial $f(x) \in \mathbb{Q}[x]$,*

$$f(x) = a_n x^n + \cdots + a_0 \quad (n \geq 3, \quad n = 2g + 1 \text{ or } 2g + 2),$$

whose coefficients satisfy $a_2 \equiv 1 \pmod{8}$, $a_{2g+1} \equiv 4 \pmod{8}$ and all other $a_i \equiv 0 \pmod{8}$. Then among the four hyperelliptic curves

$$y^2 = f(x), \quad y^2 = -f(x), \quad y^2 = 2f(x), \quad y^2 = -2f(x)$$

at least one has even and at least one has odd 2^∞ -Selmer rank.

Proof. Replacing $y \mapsto 2y + x$ in $C : y^2 = f(x)$ and dividing the equation by 4, yields a curve with reduction

$$\bar{C}/\mathbb{F}_2 : y^2 + xy = x^{2g+1}.$$

This equation has a split node at $(0, 0)$ and no other singularities, so $\text{Jac}(C)$ has split semistable reduction at 2 of toric dimension 1. Hensel lifting the non-singular point at ∞ on \bar{C} we find that $C(\mathbb{Q}_2) \neq \emptyset$. Now apply Theorem A.3 with $K = \mathbb{Q}$, $F = \mathbb{Q}(i, \sqrt{2})$ and $\mathfrak{p}_0 = 2$. (Note that all odd primes split in F/\mathbb{Q} , and that $\text{Jac}(C_\alpha) = (\text{Jac}(C))_\alpha$.) \square

Proof of Theorem A.2

Lemma A.5. *Let K be a finite extension of \mathbb{Q}_p (p odd), with residue field \mathbb{F}_q . Take a hyperelliptic curve*

$$C : y^2 = a_n x^n + \cdots + a_0, \quad a_i \in \mathcal{O}_K,$$

and let $f(x) \in \mathbb{F}_q[x]$ be the reduction of the right-hand side.

1. *If f is squarefree of degree n and has an \mathbb{F}_q -rational root, then $\text{Jac}(C)$ has good reduction, and $C_\alpha(K) \neq \emptyset$ for every $\alpha \in K^\times$.*
2. *If $f(x) = (x - a)^2 h(x)$ for some $a \in \mathbb{F}_q$ and some squarefree polynomial $h(x)$ of degree $n - 2$ that possesses an \mathbb{F}_q -rational root and satisfies $h(a) \in \mathbb{F}_q^{\times 2}$, then $\text{Jac}(C)$ has split semistable reduction of toric dimension 1, and $C_\alpha(K) \neq \emptyset$ for every $\alpha \in K^\times$.*
3. *If $f(x)$ is not of the form $\lambda h(x)^2$, $\lambda \in \mathbb{F}_q$, and $q > 4n^2$, then $C(K) \neq \emptyset$.*

Proof. In the first case, C has good reduction, and therefore so does $\text{Jac}(C)$. In the second case, C has one split node and no other singular points, and so its Jacobian has split semistable reduction of toric dimension 1. In both cases, $f(x)$ has a simple root $b \in \mathbb{F}_q$, by assumption. Lifting it by Hensel's lemma, we get a point $(B, 0)$ on C/K . This point gives a K -rational point on every quadratic twist of C .

For (3), this is the argument in [25, Lemma 15]: write $f(x) = l(x)h(x)^2$ with l and h coprime and l non-constant and squarefree. By the Weil conjectures, the curve $y^2 = l(x)$ has at least $q + 1 - n\sqrt{q} > n$ rational points over \mathbb{F}_q . So there is at least one whose x -coordinate is not a root of f . It is non-singular on $y^2 = f(x)$, and by Hensel's lemma it lifts to a point in $C(K)$. \square

Proof of Theorem A.2. Write O for the ring of integers of K , and \mathbb{F}_p for the residue field at p .

Suppose we are given an admissible family \mathcal{F} of hyperelliptic curves. In other words, for every prime p the curves lie in some open set \mathcal{F}_p of p -adic curves C/O_p , defined by congruence conditions modulo \mathfrak{p}^{m_p} , and outside a finite set of primes Σ of O these sets include all curves with $C(O_p) \neq \emptyset$. Enlarge Σ to include all primes $p|2$, with m_p chosen so that units of the form $1 + p^{m_p}$ are squares in O_p , and all primes of norm $\leq 4n^2$.

Take a prime $\mathfrak{p}_0 \notin \Sigma$. Pick $\alpha, \beta \in O$ with $\alpha \equiv \beta \equiv 1 \pmod{\prod_{p \in \Sigma} \mathfrak{p}^{m_p}}$, and such that α has valuation 1 at \mathfrak{p}_0 and β is a non-square unit modulo \mathfrak{p}_0 . Then \mathfrak{p}_0 ramifies in $K(\sqrt{\alpha})$ and is inert in $K(\sqrt{\beta})$, so $F = K(\sqrt{\alpha}, \sqrt{\beta})$ is a biquadratic extension with a unique prime above \mathfrak{p}_0 . There is a finite set of primes U of K that have a unique prime above them in F , and $U \cap \Sigma = \emptyset$. (The set is finite since such primes must ramify in F/K .)

Within our family \mathcal{F} consider those curves $C : y^2 = f(x)$ whose reductions are as in Lemma A.5(2) at \mathfrak{p}_0 , as in Lemma A.5(1) at all $\mathfrak{p} \in U \setminus \{\mathfrak{p}_0\}$, and such that $f \pmod{\mathfrak{p}}$ is not a unit times the square of a polynomial at any $\mathfrak{p} \notin \Sigma \cup U$. (This is a positive proportion of curves in \mathcal{F} by [26].) For each such curve C , Theorem A.3 implies that both odd and even 2-Selmer ranks occur among the twists of $\text{Jac}(C)$ by $1, \alpha, \beta$ and $\alpha\beta$, in other words the Jacobians of C, C_α, C_β and $C_{\alpha\beta}$. Note that these twists are in \mathcal{F} , since for $\mathfrak{p} \in \Sigma$ this twisting does not change the class modulo \mathfrak{p}^{m_p} , while for $\mathfrak{p} \notin \Sigma$ these twists are all locally soluble by Lemma A.5(3).

Because quadratic twists by α, β and $\alpha\beta$ only change the height by at most $N_{K/\mathbb{Q}}(\alpha\beta)^n$, we get the asserted positive proportion. \square

Proof of Theorem A.3

We refer the reader to [18, §2] for the theory of Brauer relations and their regulator constants.

Notation A.6. Let F/K be a Galois extension of number fields with Galois group G , and A/K an abelian variety. Fix a global invariant exterior form ω on A/K . For $K \subset L \subset F$ and a prime p , we write

$$\begin{aligned} \text{III}_{A/L}^{[p]} & \quad p\text{-primary part of } \text{III}_{A/L} \text{ modulo divisible elements (a finite abelian } p\text{-group).} \\ \tilde{c}_{A/L} & \quad \prod c_v |\omega/\omega_v^o|_v, \text{ where the product is taken over all primes of } L, c_v \text{ is the Tamagawa number} \\ & \quad \text{of } A/L \text{ at } v, \omega_v^o \text{ the Néron exterior form and } |\cdot|_v \text{ the normalised absolute value at } v. \end{aligned}$$

In the theorem below we write

$$\begin{aligned} \mathcal{S} & \quad \text{the set of self-dual irreducible } \mathbb{Q}_p G\text{-representations.} \\ \Theta & \quad = \sum n_i H_i \text{ a Brauer relation in } G \text{ (i.e. } \sum_i n_i \text{Ind}_{H_i}^G \mathbf{1} = 0). \\ \mathcal{C}(\Theta, \rho) & \quad \text{the regulator constant } \prod_i \det\left(\frac{1}{|H_i|} \langle \cdot, \cdot \rangle | \rho^{H_i}\right)^{n_i} \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}, \\ & \quad \text{where } \langle \cdot, \cdot \rangle \text{ is some non-degenerate } G\text{-invariant pairing on } \rho. \end{aligned}$$

Finally, as in [17] we let³

$$\mathcal{S}_\Theta = \{\rho \in \mathcal{S} \mid \text{ord}_p \mathcal{C}(\Theta, \rho) \equiv 1 \pmod{2}\}.$$

Theorem A.7. *Suppose A/K is a principally polarised abelian variety. For $\rho \in \mathcal{S}$ write m_ρ for its multiplicity in the dual p^∞ -Selmer group of A/F . Then*

$$\sum_{\rho \in \mathcal{S}_\Theta} m_\rho \equiv \text{ord}_p \prod_i \tilde{c}_{A/F^{H_i}} \text{III}_{A/F^{H_i}}^{[p]} \pmod{2}.$$

³[17] also includes representations of the form $T \oplus T^*$ for some irreducible $T \not\cong T^*$ (T^* is the contragredient of T), but these have trivial regulator constants by [18, Cor. 2.25].

Proof. This is essentially [17, Thm. 1.6], except for the $\text{III}^{[p]}$ term in the right-hand side. For odd p , this term is a square and does not contribute to the formula. For $p = 2$, this is the formula that comes out of the proof of [17, Thm. 1.6]. There the main step of the proof ([17, Thm. 3.1]) assumes that A/K has a principal polarisation induced by a K -rational divisor to get rid of the $\text{III}^{[2]}$ term coming from [17, Thm. 2.2]. \square

Corollary A.8. *Let $F = K(\sqrt{\alpha}, \sqrt{\beta})$ be a biquadratic extension of number fields. For every principally polarised abelian variety A/K ,*

$$\begin{aligned}
& \text{rk}_{2^\infty}(A/K) + \text{rk}_{2^\infty}(A_\alpha/K) + \text{rk}_{2^\infty}(A_\beta/K) + \text{rk}_{2^\infty}(A_{\alpha\beta}/K) \equiv \\
(\dagger) \quad & \equiv \text{ord}_2 \frac{\tilde{c}_{A/K(\sqrt{\alpha})} \tilde{c}_{A/K(\sqrt{\beta})} \tilde{c}_{A/K(\sqrt{\alpha\beta})}}{\tilde{c}_{A/F} (\tilde{c}_{A/K})^2} \\
& + \text{ord}_2 \frac{|\text{III}_{A/K(\sqrt{\alpha})}^{[2]}| |\text{III}_{A/K(\sqrt{\beta})}^{[2]}| |\text{III}_{A/K(\sqrt{\alpha\beta})}^{[2]}|}{|\text{III}_{A/F}^{[2]}| |\text{III}_{A/K}^{[2]}|^2} \pmod{2}.
\end{aligned}$$

Proof. Write $1, C_2^a, C_2^b, C_2^c$ for the proper subgroups of $G = \text{Gal}(F/K)$, and $\mathbf{1}, \epsilon_a, \epsilon_b, \epsilon_c$ for its 1-dimensional representations (so $\mathbb{C}[G/C_2^\bullet] \cong \mathbb{1} \oplus \epsilon^\bullet$ for $\bullet = a, b, c$). Thus the four 2^∞ -Selmer ranks in question are the multiplicities of these four representations in the dual 2^∞ -Selmer group of A/F . Now apply the theorem to the Brauer relation

$$\Theta = \{\mathbf{1}\} - C_2^a - C_2^b - C_2^c + 2G. \quad (23)$$

Its regulator constants are (see [18, 2.3 and 2.14])

$$\mathcal{C}_\Theta(\mathbf{1}) = \mathcal{C}_\Theta(\epsilon^a) = \mathcal{C}_\Theta(\epsilon^b) = \mathcal{C}_\Theta(\epsilon^c) = 2 \in \mathbb{Q}^\times / \mathbb{Q}^{\times 2},$$

and so $S_\Theta = \{\mathbf{1}, \epsilon_a, \epsilon_b, \epsilon_c\}$ in this case. \square

Proof of Theorem A.3. We write the two expressions in $\text{ord}_2(\dots)$ on the right-hand side of Corollary A.8 as a product of local terms. The modified Tamagawa numbers $\tilde{c}_{J/K}, \tilde{c}_{J/K(\sqrt{\alpha})}, \dots$ are, by definition, products over primes of $K, K(\sqrt{\alpha}), \dots$, and we group all terms by primes of K . Similarly, as shown by Poonen and Stoll in [25, §8], the parity of $\text{ord}_2 \text{III}^{[2]}$ is a sum of local terms that are 1 or 0 depending on whether $\text{Pic}^{g-1}(C)$ is empty or not over the corresponding completion, and again we group them by primes \mathfrak{p} of K . This results in an expression

$$\text{rk}_{2^\infty}(J/K) + \text{rk}_{2^\infty}(J_\alpha/K) + \text{rk}_{2^\infty}(J_\beta/K) + \text{rk}_{2^\infty}(J_{\alpha\beta}/K) \equiv \sum_{\mathfrak{p}} t_{\mathfrak{p}} \pmod{2}.$$

There are three cases to consider for \mathfrak{p} :

If there are several primes $q_i | \mathfrak{p}$ in F , then the decomposition groups of q_i are cyclic, and this forces $t_{\mathfrak{p}} = 0$. This is a general fact about Brauer relations and functions of number fields that are products of local terms, see [18, 2.31, 2.33, 2.36(1)].

If there is a unique prime $q | \mathfrak{p}$ in F , then $C(K_{\mathfrak{p}}) \neq \emptyset$ by assumption. So $\text{Pic}^{g-1}(C)$ is non-empty in every extension of $K_{\mathfrak{p}}$, and all the local terms for $\text{III}^{[2]}$ above \mathfrak{p} vanish. Also J has semistable reduction, again by assumption, so its Néron minimal model stays minimal in all extensions. The term $|\omega/\omega_v^g|_v$ always cancels in Brauer relations in this case, see e.g. [18, 2.29]. So the only contribution to $t_{\mathfrak{p}}$ comes from Tamagawa numbers.

When $\mathfrak{p} \neq \mathfrak{p}_0$, the Jacobian J has good reduction and the Tamagawa numbers are trivial, so $t_{\mathfrak{p}} = 0$. Finally, if $\mathfrak{p} = \mathfrak{p}_0$, then J has split semistable reduction at \mathfrak{p} of toric dimension 1. In this case, the Tamagawa number term at \mathfrak{p} multiplies to $2 \in \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$, in other words $t_{\mathfrak{p}} = 1$. This follows e.g. from [18, 3.3, 3.23] for the Brauer relation (23). This proves the claim for the 2^∞ -Selmer rank.

It remains to deduce the formula for rk_2 from the one for rk_{2^∞} . The difference between rk_2 and rk_{2^∞} comes from $\text{III}^{[2]}$ and the 2-torsion in the Mordell–Weil group on J , J_α , J_β , and $J_{\alpha\beta}$. Two-torsion is the same for all four twists, and so gives an even contribution. As for $\text{III}^{[2]}$, the local terms that define its parity give an even contribution at every prime of K that splits in F , as the twists then come in isomorphic pairs. At the non-split primes, all four twists have local points by assumption, and so the local terms are 0. \square

Acknowledgments

We thank Jean-Louis Colliot-Thélène, John Cremona, Noam Elkies, Tom Fisher, Bjorn Poonen, Peter Sarnak, Arul Shankar, and Michael Stoll for many helpful conversations. The first and third authors were supported by a Simons Investigator Grant and NSF grant DMS-1001828. The second author was supported by NSF grant DMS-0901102.

References

- [1] M. Bhargava, Most hyperelliptic over \mathbb{Q} curves have no rational points, <http://arxiv.org/abs/1308.0395>.
- [2] M. Bhargava, The geometric sieve and the density of squarefree values of polynomial discriminants and other invariant polynomials, in progress.
- [3] M. Bhargava and B. Gross, Arithmetic invariant theory, <http://arxiv.org/abs/1208.1007>.
- [4] M. Bhargava and B. Gross, The average size of the 2 Selmer group of the Jacobians of hyperelliptic curves with a rational Weierstrass point, <http://arxiv.org/abs/1208.1007>.
- [5] M. Bhargava, B. Gross, and X. Wang, Arithmetic invariant theory II, preprint.
- [6] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, <http://arxiv.org/abs/1006.1002>, to appear in *Ann. of Math.*
- [7] M. Bhargava and A. Shankar, Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0, to appear in *Ann. of Math.*
- [8] B. J. Birch and J. R. Merriman, Finiteness theorems for binary forms, *Proc. London Math. Soc.* **s3-24** (1972), 385–394.
- [9] S. Bosch, W. Lutkebohmert, and M. Raynaud, *Néron models*, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*, **21**, Berlin, New York: Springer-Verlag, 1990.

- [10] N. Bruin and M. Stoll, Two-cover descent on hyperelliptic curves, *Math. Comp.* **78** (2009), no. 268, 2347–2370.
- [11] M. Car, Factorisation dans $\mathbb{F}_q[x]$, *C.R. Acad. Sci. Paris. Ser. I*, **294** (1982), 147–150.
- [12] J. W. S. Cassels, The Mordell-Weil group of curves of genus 2, in: *Arithmetic and Geometry I*, Birkhäuser, Boston (1983), 27–60.
- [13] J.-L. Colliot-Thélène and B. Poonen, Algebraic families of nonzero elements of Shafarevich–Tate groups, *J. Amer. Math. Soc.* **13** (2000), no. 1, 83–99.
- [14] J.-L. Colliot-Thélène and J. J. Sansuc, La descente sur les variétés rationnelles, II, *Duke Math. J.* **54** (1987), 375 – 492
- [15] A. Dembo, B. Poonen, Q.-M. Shao, and O. Zeitouni, Random polynomials having few or no real zeros, *J. Amer. Math. Soc.* **15** (2002), 857–892.
- [16] U.V. Desale and S. Ramanan, Classification of vector bundles of rank 2 on hyperelliptic curves, *Invent. Math.* **38** (1976), 161–185.
- [17] T. Dokchitser and V. Dokchitser, Self-duality of Selmer groups, *Math. Proc. Cam. Phil. Soc.* **146** (2009), 257–267.
- [18] T. Dokchitser and V. Dokchitser, Regulator constants and the parity conjecture, *Invent. Math.* **178**, no. 1 (2009), 23–71.
- [19] R. Donagi, Group law on the intersection of two quadrics, *Annali della Scuola Normale Superiore di Pisa* **7** (1980), 217–239.
- [20] N. N. Dong Quan, Algebraic families of hyperelliptic curves violating the Hasse principle. Available at <http://www.math.ubc.ca/~dongquan/JTNB-algebraic-families.pdf>.
- [21] B. Gross, Hanoi lectures on the arithmetic of hyperelliptic curves, *Acta mathematica vietnamica* **37** (2012), 579–588.
- [22] B. Gross, On Bhargava’s representations and Vinberg’s invariant theory, In: *Frontiers of Mathematical Sciences*, International Press (2011), 317–321.
- [23] S. Lichtenbaum, Duality theorems for curves over p -adic fields, *Invent. Math.* **7**, (1969), 120–136.
- [24] J. Nakagawa, Binary forms and orders of algebraic number fields, *Invent. Math.* **97** (1989), 219–235.
- [25] B. Poonen and M. Stoll, The Cassels–Tate pairing on polarized abelian varieties, *Ann. of Math.* **150** (1999), 1109–1149.
- [26] B. Poonen and M. Stoll, A local-global principle for densities, *Topics in number theory* (University Park, PA, 1997), 241–244, *Math. Appl.* **467**, Kluwer Acad. Publ., Dordrecht, 1999.
- [27] B. Poonen and E. F. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line, *J. reine angew. Math.* **488** (1997), 141–188.

- [28] M. Reid, The complete intersection of two or more quadrics, PhD Thesis, Trinity College, Cambridge (1972).
- [29] J-P. Serre, *Groupes algébriques et corps de classes*, Hermann, 1959.
- [30] A. Shankar and X. Wang, Average size of the 2-Selmer group for monic even hyperelliptic curves, <http://arxiv.org/abs/1307.3531>.
- [31] S. Siksek, Chabauty for symmetric powers of curves, *Algebra & Number Theory* **3** (no. 2), 209–236.
- [32] A. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics **114**, 2001.
- [33] M. Stoll, Finite descent obstructions and rational points on curves, *Algebra and Number Theory* **1** (1997), 349–391.
- [34] M. Stoll and R. van Luijk, Unfaking the fake Selmer group, www.math.leidenuniv.nl/~rvl/ps/unfaking.pdf.
- [35] X. Wang, Maximal linear spaces contained in the base loci of pencils of quadrics, <http://arxiv.org/abs/1302.2385>.
- [36] X. Wang, *Pencils of quadrics and Jacobians of hyperelliptic curves*, Ph. D. thesis, Harvard University, 2013.
- [37] M. Wood, Rings and ideals parametrized by binary n -ic forms, *J. London Math. Soc. (2)* **83** (2011), 208–231.
- [38] M. Wood, Parametrization of ideal classes in rings associated to binary forms, *J. reine angew. Math.*, to appear.