PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY, SERIES B
Volume 3, Pages 18–27 (December 6, 2016)
http://dx.doi.org/10.1090/bproc/24

MOST BINARY FORMS COME FROM A PENCIL OF QUADRICS

BRENDAN CREUTZ

(Communicated by Romyar T. Sharifi)

Abstract. A pair of symmetric bilinear forms A and B determine a binary form $f(x,y) := \operatorname{disc}(Ax - By)$. We prove that the question of whether a given binary form can be written in this way as a discriminant form generically satisfies a local-global principle and deduce from this that most binary forms over $\mathbb{Q}$ are discriminant forms. This is related to the arithmetic of the hyperelliptic curve $z^2 = f(x,y)$. Analogous results for nonhyperelliptic curves are also given.

1. Introduction

A pair of symmetric bilinear forms A and B in n variables over a field k of characteristic not equal to 2 determine a binary form

$$f(x,y) := \operatorname{disc}(Ax-By) = (-1)^{\frac{n(n-1)}{2}}\det(Ax-By) := f_0x^n+f_1x^{n-1}y+\cdots+f_ny^n$$

of degree n. The question of whether a given binary form can be written as a discriminant form in this way is studied in [BG13,Wan13,BGW15,BGW16]. We prove that the property of being a discriminant form generically satisfies a local-global principle and deduce from this that most binary forms over $\mathbb{Q}$ are discriminant forms.

It is easy to see that a binary form $f \in k[x,y]$ is a discriminant form if and only if the forms c^2f are too, for every $c \in k^\times$. When $k = \mathbb{Q}$, it thus suffices to consider integral binary forms, in which case we define the height of f to be $H(f) := \max\{|f_i|\}$ and consider the finite sets $N_n(X)$ of integral binary forms of degree n with $H(f) < X$. We prove:

Theorem 1. *For any $n \geq 3$,*

$$\liminf_{X\to\infty} \frac{\#\{f \in N_n(X) \ :\ f \text{ is a discriminant form over } \mathbb{Q}\}}{\#N_n(X)} > 75\%\,.$$

Moreover, these values tend to 100% *as $n \to \infty$.*

When n is even the corresponding lim sup is strictly less than 100%, as can been seen by local considerations. For example, a square free binary form over $\mathbb{R}$ is a discriminant form if and only if it is not negative definite (see [BGW16, Section 7.2]), a property which holds for a positive proportion of binary forms over $\mathbb{R}$. One is thus led to ask whether local obstructions are the only ones. This question was

Received by the editors January 24, 2016 and, in revised form, March 14, 2016; July 26, 2016; and August 16, 2016.

2010 *Mathematics Subject Classification.* Primary 11D09, 11G30; Secondary 14H25, 14L24.

©2016 by the author under Creative Commons Attribution-Noncommercial 3.0 License (CC BY NC 3.0)

posed in [BS09, Question 7.2], albeit using somewhat different language. When $n = 2$, the answer is yes and turns out to be equivalent to the Hasse principle for conics, and in this case the limit appearing in Theorem 1 is the probability that a random conic has a rational point, which is 0 (see [BCF15, Theorem 1.4]).

When k is a number field, define the height of f to be the height of the point $(f_0 : \cdots : f_n)$ in weighted projective space $\mathbb{P}^n(2 : \cdots : 2)$, and set $N_{n,k}(X)$ to be the finite set of degree n binary forms over k of height at most X. We prove the following:

Theorem 2. *Let k be a number field. For any $n \geq 1$,*

$$\lim_{X\to\infty} \frac{\#\{f \in N_{n,k}(X) \ :\ f \textit{ is a discriminant form over } k\}}{\#\{f \in N_{n,k}(X) \ :\ f \textit{ is a discriminant form everywhere locally}\}} = 100\%.$$

It is known that a square free binary form $f(x, y)$ is a discriminant form over k if the smooth projective hyperelliptic curve with affine model given by $z^2 = f(x, 1)$ has a rational point [BGW16, Theorem 28]. In particular binary forms of odd degree are discriminant forms. Results of Poonen and Stoll allow one to compute the proportion of hyperelliptic curves over $\mathbb{Q}$ of fixed genus that have points everywhere locally [PS99a, PS99b]. This gives lower bounds on the proportion of binary forms of fixed even degree that are locally discriminant forms. Computing these bounds and applying Theorem 2, one obtains Theorem 1.

Theorem 2 states that the property of being a discriminant form satisfies a local-global principle *generically.* This is rather surprising given that such a local-global principle does not hold *in general.* For example, there is a positive density set of positive square free integers c such that the binary form

$$f(x, y) = c(x^2 + y^2)(x^2 + 17y^2)(x^2 - 17y^2) \in \mathbb{Q}[x, y] \tag{1.1}$$

is a discriminant form locally, but not over $\mathbb{Q}$ (see [Cre13, Theorem 11]). Of course, the forms appearing in (1.1) are not generic. It is well known (as was first proved over $\mathbb{Q}$ by van der Waerden [vdW36]) that 100% of degree n univariate polynomials over a number field have Galois group S_n. Therefore Theorem 2 is a consequence of the following:

Theorem 3. *Suppose $f(x, y) \in k[x, y]$ is a binary form of degree n over a global field k of characteristic not equal to 2 and such that $f(x, 1)$ has Galois group S_n. If $f(x, y)$ is a discriminant form everywhere locally, then $f(x, y)$ is a discriminant form over k.*

A square free binary form $f(x, y)$ of even degree gives an affine model of a smooth hyperelliptic curve $C : z^2 = f(x, 1)$ with two points at infinity. As shown in [BGW16] the $\mathrm{SL}_n(k)$-orbits of pairs (A, B) with discriminant form $f(x, y)$ correspond to k-forms of the maximal abelian covering of C of exponent 2 unramified outside the pair of points at infinity. Geometrically these coverings arise as pullbacks of multiplication by 2 on the generalized Jacobian $J_{\mathfrak{m}}$ where $\mathfrak{m}$ is the modulus comprising the points at infinity. The Galois-descent obstruction to the existence of such coverings over k (and hence to the existence of a pencil of quadrics over k

with discriminant form $f(x,y)$) is an element of $\mathrm{H}^2(k, J_{\mathfrak{m}}[2])$ ([BGW16, Theorems 13 and 24]). The Galois action on $J_{\mathfrak{m}}[2]$ factors faithfully through the Galois group of $f(x,1)$, so Theorem 3 follows from:

Theorem 4. *Suppose C is a hyperelliptic curve of genus g over a global field k of characteristic not equal to 2 and that $\mathrm{Gal}(k(J_{\mathfrak{m}}[2])/k) = S_{2g+2}$. Then $\text{Ш}^2(k, J_{\mathfrak{m}}[2]) = 0$; i.e., an element of $\mathrm{H}^2(k, J_{\mathfrak{m}}[2])$ is trivial if it is everywhere locally trivial.*

This result is all the more surprising given that the analogous statement for the usual Jacobian is not true! There exist hyperelliptic curves of genus g with Jacobian J, generic Galois action on $J[2]$ and such that $\text{Ш}^1(k, J[2]) \simeq \text{Ш}^2(k, J[2]) \neq 0$. A concrete example is given in [PR11, Example 3.20]; see also Example 16 below. This leads one to suspect that there may exist locally solvable hyperelliptic curves whose maximal abelian unramified covering of exponent 2 does not descend to k (or, equivalently, that the torsor J^1 parameterizing divisor classes of degree 1 is not divisible by 2 in the group $\mathrm{H}^1(k, J)$). This can happen when the action of Galois on $J[2]$ is not generic; an example is given in [CV15, Theorem 6.7]. But Theorem 4 implies that it cannot happen when the Galois action is generic:

Theorem 5. *Suppose C is an everywhere locally soluble hyperelliptic curve satisfying the hypothesis of Theorem 4 and let $\overline{C}$ denote the base change to a separable closure of k. Then*

(a) the maximal unramified abelian covering of $\overline{C}$ of exponent 2 descends to k, and

(b) the maximal abelian covering of $\overline{C}$ of exponent 2 unramified outside $\mathfrak{m}$ descends to k.

Proof. The covering in (a) is the maximal unramified subcovering of that in (b), while (b) follows from Theorem 4 and the discussion preceding it. □

Theorem 4 generalizes to the context considered in [Cre16], which we now briefly summarize. Given a curve C, an integer m and a reduced base point free effective divisor $\mathfrak{m}$ on C, multiplication by m on the generalized Jacobian $J_{\mathfrak{m}}$ factors through an isogeny $\varphi : A_{\mathfrak{m}} \to J_{\mathfrak{m}}$ whose kernel is dual to the Galois module $\mathcal{J}[m] := (\mathrm{Pic}(C_{\overline{k}})/\langle\mathfrak{m}\rangle)[m]$. In the situation considered above $m = \deg(\mathfrak{m}) = 2$ and φ is multiplication by 2 on $J_{\mathfrak{m}}$ (in this case the duality is proved in [PS97, Section 6]). Via geometric class field theory the isogeny φ corresponds to an abelian covering of $C_{\overline{k}}$ of exponent m unramified outside $\mathfrak{m}$. The maximal unramified subcoverings of the k-forms of this ramified covering are the m-coverings of C parameterized by the explicit descents in [BS09, Cre14, BPS16]. The Galois-descent obstruction to the existence of such a covering over k is the class in $\mathrm{H}^2(k, A_{\mathfrak{m}}[\varphi])$ of the coboundary of $[J^1_{\mathfrak{m}}]$ from the exact sequence $0 \to A_{\mathfrak{m}}[\varphi] \to A_{\mathfrak{m}} \to J_{\mathfrak{m}} \to 0$.

The following theorem says that the group $\text{Ш}^2(k, A_{\mathfrak{m}}[\varphi])$ is trivial provided the action of Galois on the m-torsion of the Jacobian is sufficiently generic. Theorem 4 is case (1).

Theorem 6. *Suppose k is a global field of characteristic not dividing m, C is a smooth projective and geometrically integral curve of genus g over k, and $m, \mathfrak{m}$ and φ are as above. In all of the cases listed below, $\text{Ш}^2(k, A_{\mathfrak{m}}[\varphi]) = 0$.*

(1) $m = \deg(\mathfrak{m}) = h^0([\mathfrak{m}]) = 2$ and $\mathrm{Gal}(k(J_{\mathfrak{m}}[2])/k) \simeq S_{2g+2}$.

(2) $m = 2$, $\mathfrak{m}$ is a canonical divisor and $\mathrm{Gal}(k(J[2])/k) \simeq \mathrm{Sp}_{2g}(\mathbb{F}_2)$.

(3) $g = 1$ *and* $m = \deg(\mathfrak{m}) = 2$.

(4) $g = 1$, $m = \deg(\mathfrak{m}) = p^r$ *for some prime* p *and integer* $r \geq 1$ *and neither of the following holds:*

(a) The action of the absolute Galois group, Gal_k*, on* $J[p]$ *is reducible.*

(b) The action of Gal_k *on* $J[p]$ *factors through the symmetric group* S_3.

Remark 7. The statement and proof of the theorem depend only on the cohomology of the Gal_k-module $\mathcal{J}[m] := (\mathrm{Pic}(C_{\overline{k}})/\langle \mathfrak{m} \rangle)[m]$ and its dual $A_{\mathfrak{m}}[\varphi] = \mathcal{J}[m]^\vee$. If one likes, this can be taken as the definition of $A_{\mathfrak{m}}[\varphi]$, and the isogeny can be ignored.

In the case of genus one curves, the corresponding coverings can be described using the period-index obstruction map in [CFO$^+$08]. For example, a genus 1 hyperelliptic curve $C : z^2 = f(x, y)$ can be made into a 2-covering of its Jacobian. If $f(x, y)$ is the discriminant form of the pair (A, B), then the quadric intersection $C' : A = B = 0$ in $\mathbb{P}^3$ is a lift of C to a 4-covering of the Jacobian. This covering has trivial period-index obstruction in the sense described in [CFO$^+$08] and, conversely, any lift to a 4-covering with trivial period-index obstruction may be given by an intersection of quadrics which generate a pencil with discriminant form $f(x, y)$. The analogous statement holds for any $m \geq 2$ (see [Cre16]). Using this and Theorem 6 we obtain the following:

Theorem 8. *Fix* $m \geq 2$. *For* 100% *of locally solvable genus one curves* C *of degree* m *there exists a genus one curve* D *of period and index dividing* m^2 *such that* $m[D] = [C]$ *in the group* $\mathrm{H}^1(k, \mathrm{Jac}(C))$ *parameterizing isomorphism classes of torsors under the Jacobian of* C.

When $m = 2$ case (3) of Theorem 6 shows that we may replace "100%" with "all". This was first proved in the author's PhD thesis [Cre10, Theorem 2.5]. It would be interesting to determine if this is always true when m is prime. In this case it is known that there always exists D such that $m[D] = [C]$ [Cas62, Section 5] (but not for composite m [Cre13]). However, it is unknown whether D may be chosen to have index dividing m^2.

The proportion of locally solvable genus one curves of degree 3 has been computed by Bhargava-Cremona-Fisher [BCF16]. As 100% of cubic curves satisfy the hypothesis in case (4) of Theorem 6, this yields the following:

Theorem 9. *At least* 97% *of cubic curves* C *admit a lift to a genus one curve* D *of period and index* 9 *such that* $3[D] = [C]$ *in the Weil-Châtelet group of the Jacobian.*

2. Proof of Theorem 6

For a Gal_k-module M let

$$Ш^i(k, M) := \ker\left(\mathrm{H}^i(k, M) \overset{\prod \mathrm{res}_v}{\longrightarrow} \prod_v \mathrm{H}^i(k_v, M)\right),$$

the product running over all completions of k. For a finite group G and G-module M define

$$\mathrm{H}^i_*(G, M) := \ker\left(\mathrm{H}^i(G, M) \overset{\prod \mathrm{res}_g}{\longrightarrow} \prod_{g \in G} \mathrm{H}^i(\langle g \rangle, M)\right).$$

Lemma 10. *Suppose M is a finite Gal_k-module and let $G := \mathrm{Gal}(k(M)/k)$ be the Galois group of its splitting field over k. Then*

1. *$Ш^1(k,M)$ is contained in the image of $\mathrm{H}^1_*(G,M)$ under the inflation map,*
2. *if $\mathrm{H}^1_*(G,M) = 0$, then $Ш^1(k,M) = 0$, and*
3. *if $\mathrm{H}^1_*(G,M^\vee) = 0$, then $Ш^2(k,M) = 0$.*

Proof. (1) ⇒ (2) because the inflation map is injective, and (2) ⇒ (3) by Tate's global duality theorem. We prove (1) using Chebotarev's density theorem as follows.

Let $K = k(M)$ and for each place v of k, choose a place $\mathfrak{v}$ of K above v and let $G_{\mathfrak{v}} = \mathrm{Gal}(K_{\mathfrak{v}}/k_v)$ be the decomposition group. The inflation-restriction sequence gives the following commutative and exact diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(G,M) \arrow[r, "\inf"] \arrow[d, "a"] & \mathrm{H}^1(k,M) \arrow[r, "\mathrm{res}"] \arrow[d, "b"] & \mathrm{H}^1(K,M) \arrow[d, "c"] \\
0 \arrow[r] & \prod_v \mathrm{H}^1(G_v,M) \arrow[r] & \prod_v \mathrm{H}^1(k_v,M) \arrow[r] & \prod_v \mathrm{H}^1(K_{\mathfrak{v}},M)
\end{tikzcd}$$

Since M splits over K, we have $\mathrm{H}^1(K,M) = \mathrm{Hom}_{cont}(\mathrm{Gal}_K, M)$. The map c is therefore injective by Chebotarev's density theorem. Hence $\ker(b) = \inf(\ker(a))$. By a second application of Chebotarev's density theorem, the groups G_v range (up to conjugacy) over all cyclic subgroups of G. From this it follows that $\ker(a) \subset \mathrm{H}^1_*(G,M)$. □

Recall that $\mathcal{J}[m] := (\mathrm{Pic}(C_{\overline{k}})/\langle\mathfrak{m}\rangle)[m]$. Since $\mathcal{J}[m]^\vee = A_{\mathfrak{m}}[\varphi]$ (see [Cre16]) it suffices to prove, under the hypothesis of Theorem 6, that

$$\mathrm{H}^1_*(\mathrm{Gal}(k(\mathcal{J}[m])/k), \mathcal{J}[m]) = 0.$$

2.1. **Proof of Theorem 6 case (1).**

By assumption, the complete linear system associated to $\mathfrak{m}$ gives a double cover of $\pi : C \to \mathbb{P}^1$ which is not ramified at $\mathfrak{m}$. Changing coordinates if necessary, we may arrange that $\mathfrak{m}$ is the divisor above $\infty \in \mathbb{P}^1$. Then C is the hyperelliptic curve given by $z^2 = f(x,y)$, where $f(x,y)$ is a binary form of degree $n := 2g+2$ with nonzero discriminant. The ramification points of π form a finite étale subscheme $\Delta \subset C$ of size n which may be identified with the set of roots of $f(x,1)$.

As described in [PS97, Section 5] (see also [BGW16, Proposition 22]), we may identify $A_{\mathfrak{m}}[\varphi] = J_{\mathfrak{m}}[2] \simeq \mathrm{Res}^1_\Delta \mu_2$ with the subsets of Δ of even parity, while $\mathcal{J}[2] \simeq \mathrm{Res}_\Delta \mu_2/\mu_2$ corresponds to subsets modulo complements and $J[2] \simeq \mathrm{Res}^1_\Delta \mu_2/\mu_2$ corresponds to even subsets modulo complements. Parity of intersection defines a Galois equivariant and nondegenerate pairing,

$$e : J_{\mathfrak{m}}[2] \times \mathcal{J}[2] \to \mathbb{Z}/2\mathbb{Z}\,.$$

(See [PS97, Section 6] or [Cre16].) The induced pairing on $J[2] \times J[2]$ is the Weil pairing (written additively). Fixing an identification of the roots of $f(x,1)$ with the set $\{1,\dots,n\}$, the action of Gal_k on $\mathcal{J}[2]$ factors through the symmetric group S_n. The following lemma proves Theorem 6(1).

Lemma 11. $\mathrm{H}^1_*(S_n, \mathcal{J}[2]) = 0$.

Proof. For $t = 1,\dots,n-1$, let τ_t denote the transposition $\tau_t := (t, t+1) \in S_n$ and let $P_t := \{t, t+1\} \in J_{\mathfrak{m}}[2]$ (recall $J_{\mathfrak{m}}[2]$ is identified with the even subsets of

$\{1,\dots,n\}$). We use $\tilde{P}_t$ to denote the image of P_t in $J[2] \subset \mathcal{J}[2]$. We note that for any $Q \in \mathcal{J}[2]$,

$$\tau_t(Q) + Q = e(P_t, Q)\tilde{P}_t.$$

This is because τ_t is a transposition, addition is given by the symmetric difference, and the pairing e is given by parity of intersection.

Now suppose ξ is a 1-cocycle in $Z^1(S_n, \mathcal{J}[2])$ which represents a class in $\mathrm{H}^1_*(S_n, \mathcal{J}[2])$. By our assumption, the restriction of ξ to the subgroup $\langle \tau_t \rangle$ is a coboundary. Hence there is some $Q_t \in \mathcal{J}[2]$ such that $\xi_{\tau_t} = \tau_t(Q_t) + Q_t = e(P_t, Q)\tilde{P}_t$. Since $P_1, \dots, P_{n-1}$ form a basis for $J_{\mathfrak{m}}[2]$ and e is nondegenerate, we can find $Q \in \mathcal{J}[2]$ such that $e(P_t, Q) = e(P_t, Q_t)$ for all t. From this it follows that $\xi_{\tau_t} = \tau_t(Q) + Q$, for all t. In other words, Q simultaneously plays witness to the fact that ξ is a coboundary on each of the subgroups $\langle \tau_t \rangle$. But then ξ must be a coboundary, since the τ_t generate S_n. □

2.2. **A lemma.** Identifying $J[m]$ with $\mathrm{Pic}^0(C_{\overline{k}})[m]$ gives an exact sequence,

$$0 \to J[m] \xrightarrow{\iota} \mathcal{J}[m] \xrightarrow{\frac{1}{\ell}\deg} \mathbb{Z}/m\mathbb{Z} \to 0\,,$$

where the integer ℓ is $\deg(\mathfrak{m})/m$.

Lemma 12. *Let $G = \mathrm{Gal}(k(J[m])/k)$ and $G' = \mathrm{Gal}(k(\mathcal{J}[m])/k)$. The map $\iota_* \circ \mathrm{inf}$: $\mathrm{H}^1(G, J[m]) \to \mathrm{H}^1(G', \mathcal{J}[m])$ induces a surjection*

$$\ker\left(\mathrm{H}^1(G, J[m]) \to \bigoplus_{g \in G'} \mathrm{H}^1(\langle g \rangle, \mathcal{J}[m])\right) \longrightarrow \mathrm{H}^1_*(G', \mathcal{J}[m])\,.$$

Proof. Cohomology of G'-modules gives an exact sequence,

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\delta} \mathrm{H}^1(G', J[m]) \to \mathrm{H}^1(G', \mathcal{J}[m]) \to \mathrm{H}^1(G', \mathbb{Z}/m\mathbb{Z})\,.$$

Since $\mathrm{H}^1_*(G', \mathbb{Z}/m\mathbb{Z}) = 0$, we see that $\mathrm{H}^1_*(G', \mathcal{J}[m])$ is contained in the image of $\mathrm{H}^1(G', J[m])$. Hence, we may lift any $x \in \mathrm{H}^1_*(G', \mathcal{J}[m])$ to some $y \in \mathrm{H}^1(G', J[m])$. Now G' sits in an exact sequence $0 \to N \to G' \to G \to 1$. We must show it is possible to choose y such that $\mathrm{res}_N(y) = 0$, where res_N is as in the inflation-restriction sequence

$$0 \to \mathrm{H}^1(G, J[m]) \xrightarrow{\mathrm{inf}_N} \mathrm{H}^1(G', J[m]) \xrightarrow{\mathrm{res}_N} \mathrm{H}^1(N, J[m])^G\,.$$

To that end we will determine $\mathrm{res}_N \circ \delta(1)$. Since N acts trivially on $J[m]$ we have that $\mathrm{H}^1(N, J[m])^G = \mathrm{Hom}_G(N, J[m])$ (here G acts on the abelian group N by conjugation in G'). Let $\epsilon \in \mathcal{J}[m]$ be a lift of $1 \in \mathbb{Z}/m\mathbb{Z}$. By definition, $\mathrm{res}_N \circ \delta(1)$ is (represented by) the map $i : N \to J[m]$ given by $i(\sigma) = \sigma(\epsilon) - \epsilon$. It follows from the general theory that i is a morphism of G-modules. This is verified by the following computation:

$$\begin{aligned}
i({}^g\sigma) &= i(\tilde{g}\sigma\tilde{g}^{-1}) && \text{(where } \tilde{g} \text{ is a lift of } g \text{ to } G'\text{)}\\
&= \tilde{g}\left(\sigma(\tilde{g}^{-1}(\epsilon)) - \tilde{g}^{-1}(\epsilon)\right)\\
&= \tilde{g}\left(\sigma(\epsilon + a) - (\epsilon + a)\right) && \text{(where } \tilde{g}^{-1}(\epsilon) - \epsilon = a \in J[m]\text{)}\\
&= g\left(\sigma(\epsilon) - \epsilon\right) && \text{(since } N \text{ acts trivially on } J[m]\text{)}\\
&= g(i(\sigma)).
\end{aligned}$$

We claim moreover that i is injective. Indeed, if $\sigma \in N$ acts trivially on ϵ, then σ acts trivially on all of $\mathcal{J}[m]$ (because N acts trivially on $J[m]$, and $\mathcal{J}[m]$ is generated by $J[m]$ and ϵ).

By assumption on x, $\mathrm{res}_g(y)$ lies in the image of $\delta : \mathbb{Z}/m\mathbb{Z} \to \mathrm{H}^1(\langle g \rangle, J[m])$, for every $g \in G'$. It follows that $\mathrm{res}_N(y)$ lies in the subgroup

$$\mathrm{End}_G(N) = \mathrm{Hom}_G(N, i(N)) \subset \mathrm{Hom}_G(N, J[m])$$

and, moreover, that this endomorphism sends every element to some multiple of itself. Any such endomorphism is a multiple of the identity, in which case $\mathrm{res}_N(y)$ is a multiple of $\mathrm{res}_N \circ \delta(1)$. We may therefore adjust our lift y of x by a multiple $\delta(1)$ to arrange that $\mathrm{res}_N(y) = 0$. This proves the lemma. □

2.3. **Proof of Theorem 6 case (2).** Suppose C has genus $g \geq 2$, $m = 2$ and $\mathfrak{m}$ is a reduced and effective canonical divisor. Then $\deg(\mathfrak{m}) = 2g - 2$. Since the Weil pairing on $J[2] \times J[2]$ is alternating and Galois equivariant, the action of Gal_k on $J[2]$ factors through the symplectic group $\mathrm{Sp}(J[2]) \simeq \mathrm{Sp}_{2g}(\mathbb{F}_2)$. By [BPS16, Proposition 5.4] the action of Gal_k on $\mathcal{J}[2] = \mathrm{Pic}(C_{\overline{k}})/\langle [\mathfrak{m}] \rangle$ also factors through $\mathrm{Sp}(J[2])$. We will show that $\mathrm{H}^1_*(\mathrm{Sp}(J[2]), \mathcal{J}[2]) = 0$, after which the theorem follows from Lemma 10(3).

Let δ be the coboundary in $\mathrm{Sp}(J[2])$-cohomology of the exact sequence $0 \to J[2] \to \mathcal{J}[2] \to \mathbb{Z}/2\mathbb{Z} \to 0$. The sequence is not split, so $\delta(1)$ is nonzero. A direct (but rather involved) computation of group cohomology shows that $\mathrm{H}^1(\mathrm{Sp}(V), V)$ has $\mathbb{F}_2$-dimension 1 for any symplectic space V of dimension ≥ 4 over $\mathbb{F}_2$ (see [Pol71, Theorems 5.2, 4.8 and 4.1]). It follows that $\mathrm{H}^1(\mathrm{Sp}(J[2]), J[2]) = \langle \delta(1) \rangle$. Since the image of $\delta(1)$ in $\mathrm{H}^1(\mathrm{Sp}(J[2]), \mathcal{J}[2])$ is trivial, Lemma 12 shows that $\mathrm{H}^1_*(\mathrm{Sp}(J[2]), \mathcal{J}[2]) = 0$.

2.4. **Proof of Theorem 6 case (3).** We may assume $g = 1$. Let

$$G = \mathrm{Gal}(k(J[2])/k).$$

By Lemma 12 it is enough to show that $\mathrm{H}^1(G, J[2]) = 0$. Noting that $G \subset S_3$, let G_0 be the intersection of G with the unique index 2 subgroup of S_3. Then G_0 has odd order, so $\mathrm{H}^1(G_0, J[2]) = 0$. Also, the order of G/G_0 and the characteristic of $J[2]^{G_0}$ both divide 2, so $\mathrm{H}^1(G/G_0, J[2]^{G_0}) = 0$. (This follows easily from the computation of cohomology of cyclic groups, since the conditions imply that the kernel of the norm is equal to the image of the augmentation ideal.) The inflation-restriction sequence then gives that $\mathrm{H}^1(G, J[2]) = 0$ as desired.

2.5. **Proof of Theorem 6 case (4).** Suppose C is a genus one curve and $\deg(\mathfrak{m}) = m = p^r$ for some prime p and positive integer r. It suffices to show that $\text{Ш}^1(k, \mathcal{J}[m]) = 0$ except possibly when one of the following holds.

(a) The action of Gal_k on $J[p]$ is reducible, or

(b) $r > 1$ and the action of Gal_k on $J[p]$ factors through the symmetric group S_3.

So let us assume neither of these conditions holds. For $s \geq 1$ let $G_s = \mathrm{Gal}(k(J[p^s])/k)$. By Lemma 12 it suffices to show that $\mathrm{H}^1(G_r, J[p^r]) = 0$. The case $r = 1$ follows from Lemma 13 below. For $r > 1$, [ÇS15, Theorem 1] shows that the hypotheses ensure that the G_1-modules $J[p]$ and $\mathrm{End}(J[p])$ have no common irreducible subquotient. In this case the proof is completed by Lemma 14.

Lemma 13. *If G_1 acts on $J[p]$ irreducibly, then* $\mathrm{H}^1(G_1, J[p]) = 0$.

Proof. If $p \nmid \#G_1$, then $\mathrm{H}^1(G_1, J[p])$ is obviously trivial. If $p \mid \#G_1$, then a well known result of Serre [Ser72, Proposition 15] implies that either $\mathrm{SL}_2(\mathbb{F}_p) \subset G_1$ or G_1 is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. In the latter case the action is reducible, so we may assume $\mathrm{SL}_2(\mathbb{F}_p) \subset G_1$. As the case $p = 2$ has already been addressed in the proof of case (3) of the theorem, we may assume p is odd. In this case G_1 contains the normal subgroup μ_2 of order prime to p which has no fixed points. The corresponding inflation-restriction sequence

$$0 \to \mathrm{H}^1(G/\mu_2, J[p]^{\mu_2}) \to \mathrm{H}^1(G, J[p]) \to \mathrm{H}^1(\mu_2, J[p])$$

shows that $\mathrm{H}^1(G_1, J[p])$ must vanish. □

Lemma 14. *If* $\mathrm{H}^1(G_1, J[p]) = 0$ *and the G_1-modules $J[p]$ and* $\mathrm{End}(J[p])$ *have no common irreducible subquotient, then* $\mathrm{H}^1(G_r, J[p^r]) = 0$ *for all* $r \geq 1$.

Proof. We will prove below that the hypothesis of the lemma implies that $\mathrm{H}^1(G_r, J[p]) = 0$. Assuming this, induction on s and the exact sequence $0 \to J[p^s] \to J[p^{s+1}] \to J[p] \to 0$ prove that $\mathrm{H}^1(G_r, J[p^s]) = 0$ for every $1 \leq s \leq r$.

As we have assumed $\mathrm{H}^1(G_1, J[p]) = 0$, the inflation-restriction sequence gives an injective map $\mathrm{H}^1(G_r, J[p]) \hookrightarrow \mathrm{Hom}_{G_1}(H_r, J[p])$, where $H_r = \mathrm{Gal}(k(J[p^r])/k(J[p]))$ is the kernel of $G_r \to G_1$. The G_1-module H_r admits a filtration $0 \subset H_1 \subset \cdots \subset H_r$ whose successive quotients are G_1-submodules of $\ker\big(\mathrm{GL}(J[p^s]) \to \mathrm{GL}(J[p^{s-1}])\big) \cong \mathrm{End}(J[p])$. So the hypothesis of the lemma implies that $\mathrm{Hom}_{G_1}(H_r, J[p]) = 0$. □

3. Further remarks

The coboundary of 1 under the exact sequence of Gal_k-modules

$$0 \to J[m] \to \mathcal{J}[m] \to \mathbb{Z}/m\mathbb{Z} \to 0 \tag{3.1}$$

gives a class in $\mathrm{H}^1(k, J[m])$ which we denote by $[J^\ell_m]$. If either

(i) $m = \deg(\mathfrak{m}) = h^0([\mathfrak{m}]) = 2$ and g is even (i.e., C is a hyperelliptic curve of even genus) or

(ii) $m = 2$ and $\mathfrak{m}$ is a canonical divisor,

then $[J^\ell_m] \in \mathrm{H}^1(k, J[2])$ is the class of the theta characteristic torsor (cf. [PR11, Definition 3.15]).

Lemma 15. *The inclusion $J[m] \hookrightarrow \mathcal{J}[m]$ induces a map* $\mathrm{H}^1(k, J[m]) \to \mathrm{H}^1(k, \mathcal{J}[m])$ *for which the following hold.*

(1) $\text{Ш}^1(k, \mathcal{J}[m])$ *is contained in the image of* $\mathrm{H}^1(k, J[m])$.

(2) If $\text{Ш}^1(k, \mathcal{J}[m]) = 0$, *then* $\text{Ш}^1(k, J[m]) \subset \langle [J^\ell_m] \rangle$.

(3) If $[J^\ell_m] \in \text{Ш}^1(k, J[m])$, *then there is an exact sequence*

$$0 \to \langle [J^\ell_m] \rangle \subset \text{Ш}^1(k, J[m]) \to \text{Ш}^1(k, \mathcal{J}[m]) \to 0\,.$$

Proof. Take Galois cohomology of (3.1) and use the fact that $\text{Ш}^1(k, \mathbb{Z}/m\mathbb{Z}) = 0$. □

Example 16. Suppose $C : y^2 = x^6 + x + 6$. Theorem 6, Lemma 15 and [PR11, Example 3.20b] together show that $\text{Ш}^1(k, J[2]) = \langle [J^1_2] \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, while $\text{Ш}^1(k, \mathcal{J}[2]) = 0$.

In a sense this is the generic situation. Specifically one has the following.

Proposition 17. *Suppose that* $m = 2$ *and either*

(i) $\deg(\mathfrak{m}) = h^0([\mathfrak{m}]) = 2$ *and* $\mathrm{Gal}(k(J[2])/k) \simeq S_{2g+2}$ *or*

(ii) $\mathfrak{m}$ *is a canonical divisor and* $\mathrm{Gal}(k(J[2])/k) \simeq \mathrm{Sp}_{2g}(\mathbb{F}_2)$.

Let S *be any finite set of primes of* k *containing all archimedean primes, all primes above* 2*, and all primes where* $[J_2^\ell]$ *is ramified. Then*

$$Ш^1(k, S, J[2]) = \langle [J_2^\ell] \rangle \quad \textit{and} \quad Ш^1(k, S, \mathcal{J}[2]) = 0\,,$$

where $Ш^1(k, S, M) \subset \mathrm{H}^1(k, M)$ *denotes the subgroup that is locally trivial outside* S.

Proof. We first note that the assumptions in case (i) require that the genus be even, so that in both cases $[J_2^\ell]$ is the theta characteristic torsor. It follows from [PR11, Proposition 3.12] that $[J_2^\ell] \in Ш^1(k, S, J[2])$. On the other hand, Lemma 10 parts (1) and (2) and Lemma 15 all remain valid if we replace $Ш^1(k, M)$ with $Ш^1(k, S, M)$. □

References

[BCF16] Manjul Bhargava, John Cremona, and Tom Fisher, *The proportion of plane cubic curves over* $\mathbb{Q}$ *that everywhere locally have a point*, Int. J. Number Theory **12** (2016), no. 4, 1077–1092, DOI 10.1142/S1793042116500664. MR3484299

[BCF15] Manjul Bhargava, John E. Cremona, Tom Fisher, Nick G. Jones, and Jonathan P. Keating, *What is the Probability that a Random Integral Quadratic Form in n Variables has an Integral Zero?*, Int. Math. Res. Not. IMRN **12** (2016), 3828–3848, DOI 10.1093/imrn/rnv251. MR3544620

[BG13] Manjul Bhargava and Benedict H. Gross, *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, Automorphic representations and L-functions, Tata Inst. Fundam. Res. Stud. Math., vol. 22, Tata Inst. Fund. Res., Mumbai, 2013, pp. 23–91. MR3156850

[BGW16] Manjul Bhargava, Benedict Gross, and Xiaoheng Wang, *A positive proportion of locally soluble hyperelliptic curves over* $\mathbb{Q}$ *have no point over any odd degree extension*, J. Amer. Math. Soc., posted on July 27, 2016, DOI 10.1090/jams/863.

[BGW15] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang, *Arithmetic invariant theory II: Pure inner forms and obstructions to the existence of orbits*, Representations of reductive groups, Prog. Math. Phys., vol. 312, Birkhäuser/Springer, Cham, 2015, pp. 139–171. MR3495795

[BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum Math. Sigma **4** (2016), e6, 80, DOI 10.1017/fms.2016.1. MR3482281

[BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370, DOI 10.1090/S0025-5718-09-02255-8. MR2521292

[Cas62] J. W. S. Cassels, *Arithmetic on curves of genus* 1*. IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112. MR0163915

[ÇS15] Mirela Çiperiani and Jakob Stix, *Weil-Châtelet divisible elements in Tate-Shafarevich groups II: On a question of Cassels*, J. Reine Angew. Math. **700** (2015), 175–207, DOI 10.1515/crelle-2013-0013. MR3318515

[CFO$^+$08] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155, DOI 10.1515/CRELLE.2008.012. MR2384334

[Cre10] Brendan Creutz, *Explicit second p-descent on elliptic curves.* Ph.D. thesis, Jacobs University, 2010.

[Cre13] Brendan Creutz, *Locally trivial torsors that are not Weil-Châtelet divisible*, Bull. Lond. Math. Soc. **45** (2013), no. 5, 935–942, DOI 10.1112/blms/bdt019. MR3104985

[Cre14] Brendan Creutz, *Second p-descents on elliptic curves*, Math. Comp. **83** (2014), no. 285, 365–409, DOI 10.1090/S0025-5718-2013-02713-5. MR3120595

[Cre16] Brendan Creutz, *Generalized Jacobians and explicit descents* (2016), available at `arXiv:1601.06445`. Preprint.

[CV15] Brendan Creutz and Bianca Viray, *Two torsion in the Brauer group of a hyperelliptic curve*, Manuscripta Math. **147** (2015), no. 1-2, 139–167, DOI 10.1007/s00229-014-0721-7. MR3336942

[Pol71] Harriet Pollatsek, *First cohomology groups of some linear groups over fields of characteristic two*, Illinois J. Math. **15** (1971), 393–417. MR0280596

[PR11] Bjorn Poonen and Eric Rains, *Self cup products and the theta characteristic torsor*, Math. Res. Lett. **18** (2011), no. 6, 1305–1318, DOI 10.4310/MRL.2011.v18.n6.a18. MR2915483

[PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. MR1465369

[PS99a] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149, DOI 10.2307/121064. MR1740984

[PS99b] Bjorn Poonen and Michael Stoll, *A local-global principle for densities*, Topics in number theory (University Park, PA, 1997), Math. Appl., vol. 467, Kluwer Acad. Publ., Dordrecht, 1999, pp. 241–244. MR1691323

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* (French), Invent. Math. **15** (1972), no. 4, 259–331. MR0387283

[vdW36] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt* (German), Monatsh. Math. Phys. **43** (1936), no. 1, 133–147, DOI 10.1007/BF01707594. MR1550517

[Wan13] Xiaoheng Wang, *Pencils of quadrics and Jacobians of hyperelliptic curves*, ProQuest LLC, Ann Arbor, MI. Thesis (Ph.D.)–Harvard University, 2013. MR3167287

School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand

E-mail address: `brendan.creutz@canterbury.ac.nz`

URL: `http://www.math.canterbury.ac.nz/~bcreutz`