TWO-COVER DESCENT ON PLANE QUARTICS WITH RATIONAL BITANGENTS

NILS BRUIN AND DANIEL LEWIS

Abstract. We implement two-cover descent for plane quartics over $\mathbb{Q}$ with all 28 bitangents rational and show that on a significant collection of test cases, it resolves the existence of rational points. We also review a classical description of the relevant moduli space and use it to generate examples. We observe that local obstructions are quite rare for such curves and only seem to occur in practice at primes of good reduction. In particular, having good reduction at 11 implies having no rational points. We also gather numerical data on two-Selmer ranks of Jacobians of these curves, providing evidence these behave differently from those of general abelian varieties due to the frequent presence of an everywhere locally trivial torsor.

1. Introduction

A central problem in arithmetic geometry is to determine if a variety C over a number field k, for instance a nonsingular projective curve, has any k-rational points. The most elementary way of showing that $C(k)$ is empty is by showing that $C(k_v) = \emptyset$ for some completion k_v of k. In that case, we say C has a *local obstruction* to having rational points.

We consider a more refined *descent obstruction* here. Our construction can be read in elementary terms, but the theoretical motivation is enlightening. Suppose we have an unramified cover $\pi\colon D \to C$ of nonsingular proper varieties over k with geometric automorphism group $\Gamma = \mathrm{Aut}_{k^{\mathrm{alg}}}(D/C)$ satisfying $\#\Gamma = \deg(\pi)$. The *twisting principle* [Mil80, III.4.3(a)] gives us that the Galois cohomology set $\mathrm{H}^1(k,\Gamma)$ parametrizes *twists* $\pi_\gamma\colon D_\gamma \to C$, as well as a map $\boldsymbol{\gamma}\colon C(k) \to \mathrm{H}^1(k,\Gamma)$ such that for $P \in C(k)$ and $\gamma = \boldsymbol{\gamma}(P)$, we have $Q \in D_\gamma(k)$ such that $\pi_\gamma(Q) = P$. This leads us to consider the associated Selmer set

$$\mathrm{Sel}^{(\pi)}(C/k) = \{\gamma \in \mathrm{H}^1(k,\Gamma) : D_\gamma(k_v) \neq \emptyset \text{ for all completions } k_v \text{ of } k\}.$$

Since the map $\boldsymbol{\gamma}$ takes values in $\mathrm{Sel}^{(\pi)}(C/k)$, we see that if the latter is empty then $C(k)$ is empty too. In that case we say that C has a *π-cover obstruction* to having rational points: C has no rational points because a collection of covering varieties all have local obstructions.

The proof of the Chevalley-Weil theorem [CW32] implies that $\mathrm{Sel}^{(\pi)}(C/k) \subset \mathrm{H}^1(k,\Gamma;S)$, where the latter denotes the classes that are unramified outside the set

---

Date: May 20, 2020.

2010 *Mathematics Subject Classification.* Primary 11G30, 14H30; Secondary 11D41, 14H50.

Key words and phrases. Plane quartics, rational points, local-to-global obstructions, bitangents, descent obstructions, two-covers.

The first author acknowledges the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), funding reference number RGPIN-2018-04191.

S of bad places for the cover $\pi\colon D \to C$. The set $\mathrm{H}^1(k,\Gamma;S)$ is finite and explicitly computable. This means that to compute $\mathrm{Sel}^{(\pi)}(C/k)$ one only needs to check the local solvability of finitely many D_γ. Hence, $\mathrm{Sel}^{(\pi)}(C/k)$ is explicitly computable, although not necessarily efficiently.

For hyperelliptic curves, there is a well-developed theory of *two-covers* [BS09], where $\Gamma = \mathrm{Jac}_C[2]$. Their associated Selmer sets are relatively practical to compute and, as is described there, many genus two curves over $\mathbb{Q}$ have no local obstruction, but can be shown to have $\mathrm{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset$. In fact it has since been shown [BGW17] that in a precise way, *most* hyperelliptic curves have a two-cover obstruction.

Results beyond hyperelliptic curves are sparse. The general descent theory is available in [BPS16], which also provides some genus three examples, but in its full generality, the need to compute class group information of degree 28 extensions limits large-scale experiments significantly. There is also some progress on creating an appropriate setting for arithmetic statistical techniques [Tho16] to two-descent on Jacobians of curves of genus three, but it is presently not clear how to generalize the Bhargava–Gross–Wang approach to this setting.

In this article we endeavour to start a more systematic study by considering plane quartics C with a restricted 2-level structure; in particular $\mathrm{Jac}_C[2](\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^6$. This forces the 28 bitangents of C to be defined over $\mathbb{Q}$ and has the computational and expository advantage that all required data can be expressed over $\mathbb{Q}$; no algebraic number theory is required.

Remark 1.1. For a hyperelliptic curve C of genus g, having $\mathrm{Jac}_C[2](k) = (\mathbb{Z}/2\mathbb{Z})^{2g}$ implies that all $2g+2$ Weierstrass points on C are rational, making two-cover descent rather uninteresting. In this sense, two-cover descent on plane quartics has simpler non-trivial applications than on hyperelliptic curves.

In Section 3 we review an explicit description of the moduli space of smooth plane quartics with labelled bitangents as the space of seven labelled points in general position in $\mathbb{P}^2$. For small fields we prove

Proposition 1.2. *For $p = 3, 5, 7$, there exist no nonsingular plane quartics over $\mathbb{F}_p$ with all bitangents defined over $\mathbb{F}_p$. Over $\mathbb{F}_9$, there is only one isomorphism class, represented by the Fermat quartic*

$$C_9\colon x^4 + y^4 + z^4 = 0, \text{ with } \#C_9(\mathbb{F}_9) = 28.$$

Over $\mathbb{F}_{11}$, there is only one isomorphism class, represented by:

$$C_{11}\colon x^4 + y^4 + z^4 + x^2y^2 + x^2z^2 + y^2z^2 = 0, \text{ and } C_{11}(\mathbb{F}_{11}) = \emptyset.$$

In particular, a plane quartic C over $\mathbb{Q}$ with rational bitangents has bad reduction at 3, 5, and 7. If it has good reduction at 11, then it has a local obstruction there. The curve C_9 attains the maximum number of rational points for a genus three curve over $\mathbb{F}_9$. Its rational points are contacts of the 28 hyperflexes. Both C_9 and C_{11} are reductions of the Klein quartic $x^4+y^4+z^4-\frac{3}{2}(1+\sqrt{-7})(x^2y^2+x^2z^2+y^2z^2)$.

Section 4 describes, given a smooth plane quartic C with rational bitangents, an explicit model for a two-cover $\pi_\gamma\colon D_\gamma \to C$, with $\Gamma = (\mathbb{Z}/2\mathbb{Z})^6$ as a Galois-module. This directly establishes a description of two-covers and their twists, without appealing to étale cohomology.

In Section 5 we describe an algorithm to compute, with reasonable efficiency, sets $\mathrm{Sel}^{(2)}(C/k,N) \supset \mathrm{Sel}^{(2)}(C/k)$, for integers $N \geq 1$, with equality holding for $N \geq 66569$, and, in practice, for much smaller values of N already.

In Section 6 we describe a numerical experiment, where we tabulate the behaviour of $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$ for various quartics C. We consider a systematic collection of 81070 moduli points with coordinates from $\{-6,\dots,6\}$, as well as a collection of 70000 randomly selected points with coordinates from $\{-40,\dots,40\}$.

Observation 1.3. *For all curves C in our collections with $\mathrm{Sel}^{(2)}(C/\mathbb{Q}) \neq \emptyset$, we can find a point $P \in C(\mathbb{Q})$.*

This leaves the following question, which we fully expect to have an affirmative answer, but remains open for now.

Question 1.4. *Is it possible to construct a smooth plane quartic C over $\mathbb{Q}$ with rational bitangents such that $\mathrm{Sel}^{(2)}(C/\mathbb{Q}) \neq \emptyset$ but $C(\mathbb{Q}) = \emptyset$?*

Remark 1.5. For a considerable number of curves in our collections we also get information on the 2-Selmer groups of their Jacobians. The data matches the distribution conjectured in [PR12, Conjecture 1.1] quite closely, but only after taking into account that the Jac_C-torsor representing Pic^1 is very frequently everywhere locally trivial. Since non-hyperelliptic curves often have points everywhere locally, this phenomenon should be general: one should expect Jacobians to exhibit special arithmetic behaviour.

This work is based on the master's thesis [Lew19] of the second author.

2. Plane quartics and their bitangents

In this section we collect the classical combinatorics and geometry of bitangents and theta characteristics on non-hyperelliptic curves of genus three. See [Dol12, Chapter 6] or [GH04] for a more comprehensive modern treatment.

Let k be a field of characteristic different from 2 and let C be a curve of genus three over k. Then $\mathrm{Jac}(C)[2]$ is a 0-dimensional separated group scheme of degree 64 and exponent 2, equipped with a non-degenerate alternating bilinear pairing. Indeed, the automorphism group of $\mathrm{Jac}(C)[2]$ is $\mathrm{Sp}_6(\mathbb{F}_2)$.

Definition 2.1. A *theta characteristic* on a curve C of genus g is a divisor class $\theta \in \mathrm{Pic}^{g-1}(C)$ such that 2θ is the canonical class. The *parity* of θ is determined by the parity of the dimension of the Riemann-Roch space $\mathrm{H}^0(C,\theta)$.

It is a classical result [GH04, Proposition 1.11] that a curve of genus g has $2^{g-1}(2^g+1)$ even and $2^{g-1}(2^g-1)$ odd theta characteristics. For $g=3$ and C non-hyperelliptic it is easily checked that $h^0(C,\theta) \leq 1$, so the odd theta characteristics are exactly the ones that admit a (unique) effective representative.

The canonical model of a non-hyperelliptic genus three curve C is a quartic in $\mathbb{P}^2$:

$$C\colon f(x,y,z) = 0, \text{ with } f \in k[x,y,z] \text{ homogeneous of degree four.}$$

Since canonical classes are exactly line sections $C \cdot l$, we see there are 28 lines l such that $C \cdot l = 2\theta$, where θ is a degree two effective divisor representing a theta characteristic: we recover the 28 bitangents of a smooth plane quartic. Fix for each bitangent line l, a linear form ℓ describing the line.

Lemma 2.2. *Let C be a smooth plane quartic. Then no seven distinct bitangents pass through a single point.*

Proof. Suppose $l_1, \dots, l_7$ intersect in P_0. If P_0 were to lie on C it would be singular, so it does not. Hence projecting away from P_0 gives a degree four map $C \to \mathbb{P}^1$. Since $l_i \cdot C$ is a fiber of this projection, the ramification divisor has degree at least $2 \cdot 7$. But that exceeds the degree 12 given by Riemann-Hurwitz. □

Let θ_1, θ_2 be two odd theta-characteristics. Then $2(\theta_1 - \theta_2) = \mathrm{div}(\ell_1/\ell_2)$, where we regard the quotient of linear forms as a rational function on C. We see that $[\theta_2 - \theta_1] \in \mathrm{Pic}^0(C)[2]$. As it turns out, all nonzero 2-torsion classes admit such a representative, in fact, $\binom{28}{2}/63 = 6$ of them. We see that $\theta_1 - \theta_2$ and $\theta_3 - \theta_4$ are linearly equivalent precisely when $\theta_1 + \cdots + \theta_4$ is twice canonical. For bitangent forms, this leads to the following concept.

Definition 2.3. We say a quadruple of bitangent forms $\mathfrak{q} = \{\ell_1, \dots, \ell_4\}$ is a *syzygetic quadruple* if their contact points with C lie on a conic. This means there are constants $\delta_{\mathfrak{q}}, c_{\mathfrak{q}} \in k^*$ and a quadratic form $Q_{\mathfrak{q}} \in k[x, y, z]$ such that

$$\ell_1\ell_2\ell_3\ell_4 = \delta_{\mathfrak{q}} Q_{\mathfrak{q}}^2 + c_{\mathfrak{q}} f. \tag{2.1}$$

There are 315 syzygetic quadruples. We say a triple of bitangents is *syzygetic* if it is part of a syzygetic quadruple. If it is, then it is part of only one.

Definition 2.4. We say that a set of seven bitangent forms $\{\ell_1, \dots, \ell_7\}$ is an *Aronhold set* if none of its triples are syzygetic.

There are 288 Aronhold sets. For an Aronhold set, write $\{\theta_1, \dots, \theta_7\}$ for the corresponding theta characteristics. Then $\theta_1 + \cdots + \theta_7 - 3\kappa_C$ is again a theta characteristic: an even one. We see that each even theta characteristic has $288/36 = 8$ Aronhold sets associated with it. Additionally, one can check that $\{\theta_1 - \theta_7, \dots, \theta_6 - \theta_7\}$ forms a basis for $\mathrm{Pic}(C)[2]$.

It follows that specifying a labelled Aronhold set on a smooth plane quartic amounts to marking a 2-level structure on its Jacobian. The converse holds too.

Proposition 2.5 ([GH04]). *The following two moduli spaces are naturally isomorphic.*

- *non-hyperelliptic genus three curves with a labelled Aronhold set*
- *non-hyperellipic genus three curves with full* 2*-level structure.*

There is a unique conjugacy class $\mathrm{Sym}(8) \subset \mathrm{Sp}_6(\mathbb{F}_2)$. It is of length 36 and it corresponds to the stabilizer of an even theta characteristic. The action can be made explicit by labelling the bitangents by

$$\{\ell_{ij} = \ell_{\{i,j\}} : i \in \{0, \dots, 7\}, j \in \{i+1, \dots, 7\}\}, \tag{2.2}$$

with Sym(8) acting in the obvious way on the subscripts. This labelling can be chosen in such a way that the syzygetic quadruples come in two Sym(8)-orbits: one of length 210 and one of length 105, represented by, respectively,

$$\{\ell_{01}, \ell_{12}, \ell_{23}, \ell_{03}\} \text{ and } \{\ell_{01}, \ell_{23}, \ell_{45}, \ell_{67}\}. \tag{2.3}$$

We see that for $i = 0, \dots, 7$, we have the Aronhold sets $\{\ell_{ij} : j \neq i\}$. We sometimes suppress $i = 0$ in our indices, so $\ell_{0j} = \ell_j$.

Proposition 2.6. *Let $\ell_1, \dots, \ell_7$ be an Aronhold set of bitangent forms on a smooth plane quartic $C\colon f(x, y, z) = 0$. Then the square class of each of the other bitangents*

ℓ_{ij} is determined in the sense that there is a constant $\delta_{ij} \in k^\times$ and a cubic form $g_{ij} \in k[x, y, z]$ such that

$$\Big(\prod_{n \notin \{i,j\}} \ell_n\Big)\ell_{ij} \equiv \delta_{ij} g_{ij}^2 \pmod{fk[x, y, z]}.$$

Proof. To ease notation, set $\{i, j\} = \{6, 7\}$. By combining the syzygetic quadruples

$$\{\ell_1, \ell_{23}, \ell_{45}, \ell_{67}\}, \{\ell_2, \ell_7, \ell_{23}, \ell_{37}\}, \{\ell_4, \ell_7, \ell_{45}, \ell_{57}\}, \{\ell_3, \ell_5, \ell_{37}, \ell_{57}\}$$

we get that the left hand side has a divisor with even multiplicities. The existence of g_{ij} follows from the projective normality of C. □

3. Generating plane quartics with rational bitangents

We use del Pezzo surfaces of degree two (see [Dol12, 6.3.3] or [GH04]) to describe a classical link between non-hyperelliptic genus three curves with 2-level structure and point configurations in the plane.

Definition 3.1. We say seven points $p_1, \ldots, p_7 \in \mathbb{P}^2$ lie in *general position* if no three are collinear and no six lie on a conic.

Given seven points $p_1, \ldots, p_7 \in \mathbb{P}^2$ in general position, we obtain a del Pezzo surface X of degree two by blowing up the seven points. In fact we obtain a labelling of the 56 exceptional curves on X:

- Seven exceptional components E'_i above the blown-up points p_i
- Seven proper transforms E_i of cubics $\tilde{E}_i$ through the seven points with a nodal singularity at p_i
- 21 proper transforms E_{ij} of lines $\tilde{E}_{ij}$ connecting p_i and p_j.
- 21 proper transforms E'_{ij} of conics $\tilde{E}'_{ij}$ through $\{p_1, \ldots, p_7\} \setminus \{p_i, p_j\}$.

A del Pezzo surface X of degree 2 comes equipped with a $2 : 1$ map $X \to \mathbb{P}^2$, given by the anticanonical system $|-\kappa_X|$ on X. The branch locus C in $\mathbb{P}^2$ is a smooth plane quartic.

If X is obtained as the blow-up of $p_1, \ldots, p_7 \in \mathbb{P}^2$ then there is an induced rational map ϕ making the following diagram commute.

$$\begin{array}{ccc} & X & \\ {}^{\mathrm{bl}}\swarrow & & \searrow^{2:1} \\ \mathbb{P}^2 & \overset{\phi}{\dashrightarrow} & \mathbb{P}^2 \end{array}$$

Let ϕ_1, ϕ_2, ϕ_3 generate the space of cubics passing through $p_1, \ldots, p_7$. It is straightforward to check that the $\mathrm{bl}^*\phi_i$ generate $|-\kappa_X|$, so $\phi = (\phi_1 : \phi_2 : \phi_3)$. The branch locus of ϕ is contained in the plane sextic curve

$$C' \colon \det \left(\frac{\partial \phi_i}{\partial x_j}\right)_{ij} = 0 \tag{3.1}$$

and indeed, $C = \phi(C')$ turns out to be a plane quartic.

Since $\tilde{E}_i$ and $\tilde{E}_{ij} \cup \tilde{E}'_{ij}$ are loci described by cubics in the span of ϕ_1, ϕ_2, ϕ_3, they map to lines, whose defining forms we denote by ℓ_i and ℓ_{ij} respectively.

Lemma 3.2. *The labelling described above is compatible with* (2.2)*, so $\{\ell_1, \ldots, \ell_7\}$ is an Aronhold set and* (2.3) *describes the syzygetic quadruples.*

Proof. The deeper reason is that the configuration of seven points in $\mathbb{P}^2$ has the same moduli as seven points in $\mathbb{P}^3$ by *association* of point sets [Cob22]. The sextic model C' actually arises as the projection from a linear system $|\theta_{\text{even}} + \kappa_C|$ (see [GH04]), so the labelling is indeed directly linked to the choice of an even theta characteristic on C. However, it is also sufficient to just verify the statement for a particular case and then argue via connectedness of the moduli space. □

The construction above provides a very explicit description of the moduli space of non-hyperelliptic genus three curves with full 2-level structure. For explicitly parametrizing it, we lose no generality by setting p_1, p_2, p_3, p_4 to be the standard simplex and choosing $p_5, p_6, p_7 = (u_1 : v_1 : 1), (u_2 : v_2 : 1), (u_3 : v_3 : 1)$. General position means the 3×3, respectively 6×6 minors of

$$\begin{pmatrix} 1 & 0 & 0 & 1 & u_1 & u_2 & u_3 \\ 0 & 1 & 0 & 1 & v_1 & v_2 & v_3 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 & 1 & u_1^2 & u_2^2 & u_3^2 \\ 0 & 1 & 0 & 1 & v_1^2 & v_2^2 & v_3^2 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & u_1 v_1 & u_2 v_2 & u_3 v_3 \\ 0 & 0 & 0 & 1 & u_1 & u_2 & u_3 \\ 0 & 0 & 0 & 1 & v_1 & v_2 & v_3 \end{pmatrix},$$

do not vanish.

Proof of Proposition 1.2. With the description given above, it is a finite amount of work to check all the possibilities for $p = 3, 5, 7, 11$. For $p = 3, 5, 7$ there are no 7 points over $\mathbb{F}_p$ in general position (see also [BFL19, Proposition 4.4]). For $\mathbb{F}_9$ there are 40 triples $\{(u_1 : v_1 : 1), (u_2 : v_2 : 1), (u_3 : v_3 : 1)\}$ that complement the standard simplex to 7 points in general position. The construction (3.1) requires lifting to characteristic 0, but the rest of the construction remains valid. We find all resulting curves are isomorphic to C_9. For $\mathbb{F}_{11}$ there are 1440 triples, all giving curves isomorphic to C_{11}. □

4. Two-covers of smooth plane quartics with rational bitangents

Let $C\colon f(x, y, z) = 0$ be a smooth plane quartic with an Aronhold set $\ell_1, \dots, \ell_7$. We adopt the notation of Proposition 2.6. For $\gamma = (\gamma_1, \dots, \gamma_7) \in (k^\times)^7$ we define the following curve in weighted projective space $\mathbb{P}[2^3, 1^{28}]$ with coordinates x, y, z of weight 2 and $w_1, \dots, w_7, w_{12}, \dots, w_{67}$ of weight 1.

$$D'_\gamma\colon \begin{cases} f(x, y, z) = 0, & \\ \ell_i(x, y, z) = \gamma_i w_i^2 & \text{for } i = 1, \dots, 7, \\ \ell_{ij}(x, y, z) = \dfrac{\delta_{ij}}{\prod_{n \neq i,j} \gamma_n} w_{ij}^2 & \text{for } 1 \leq i < j \leq 7, \\ g_{ij}(x, y, z) = w_{ij} \prod_{n \neq i,j} w_n & \text{for } 0 \leq i < j \leq 7. \end{cases}$$

Thanks to the relations from Proposition 2.6 we have a well-defined projection $D'_\gamma \to C$. In fact, from the sign changes on $w_1, \dots, w_7$ we see that $\operatorname{Aut}(D'_\gamma/C) = (\mathbb{Z}/2\mathbb{Z})^7$. Furthermore, from the fact that the representation of the automorphism group on $w_{12}, w_{23}, \dots, w_{67}, w_{17}$ is faithful and for any fiber of $D'_\gamma \to C$ at most one of w_i or w_{ij} is zero, it follows the cover is unramified and that D'_γ is not geometrically connected. Indeed the involution on D'_γ that swaps the signs of all of $w_1, \dots, w_7$ interchanges geometric components. We consider the projection $\mathbb{P}[2^3, 1^{28}] \to \mathbb{P}^{27}$ away from the weight 2 part and consider the image D_γ of D'_γ.

Lemma 2.2 yields three linearly independent linear forms ℓ_i, ℓ_j, ℓ_n, so that we can express x, y, z as linear forms in w_i^2, w_j^2, w_k^2. Eliminating x, y, z from the equations gives us D_γ as an intersection of an octic equation, 25 quadratic equations, and 28 sextic equations. Alternatively we derive quartic relations from the syzygetic quadruples and their described relations (see Definition 2.3).

We introduce notation for a group naturally isomorphic to $(k^\times/k^{\times 2})^6$, but presented in a way more natural for our purposes.

Definition 4.1. We define $L'(2,k) \simeq (k^\times/k^{\times 2})^6$ by the exact sequence

$$1 \to (k^\times/k^{\times 2}) \xrightarrow{\text{diagonal}} (k^\times/k^{\times 2})^7 \to L'(2,k) \to 1.$$

and we usually represent elements in $L'(2,k)$ by $(\gamma_1, \ldots, \gamma_7) \in (k^\times)^7$.

Proposition 4.2. *The two-covers of C are exactly*

$$\{\pi_\gamma \colon D_\gamma \to C, \text{ where } \gamma \in L'(2,k)\}.$$

Proof. The projection of D_γ onto the coordinates $(w_1 : \cdots : w_7)$ gives a birational map to an intersection $\tilde{D}_\gamma$ of four quadrics and an octic hypersurface. Its singular locus is the pull-back along π_γ of the contact locus of the bitangents $\ell_1, \ldots, \ell_7$. We see that $\tilde{\pi} w \colon \tilde{D}_\gamma \to C$ is a finite rational cover of degree 2^6 and that $\tilde{\pi}^*(\ell_i/\ell_7) = (\gamma_i/\gamma_7)(w_i/w_7)^2$. This shows that a basis for $\mathrm{Pic}^0(C)[2]$ pulls back to principal divisors, and hence that $\tilde{D}_\gamma$ is a birational model of a two-cover, and therefore so is D_γ. To see that D_γ is nonsingular, we use that for $P \in D_\gamma(k^{\mathrm{alg}})$ we can find an Aronhold set of bitangents that do not meet $\pi_\gamma(P)$.

In order to show that all 2-covers arise as D_γ, we observe that $\mathrm{Pic}(C/k)[2] = (\mu_2)^6$, where we write μ_2 for the Galois module $\{-1, 1\}$. By the Kummer sequence we have

$$\mathrm{H}^1(k, \mathrm{Pic}(C/k)[2]) = (k^\times/k^{\times 2})^6 \simeq L'(2,k).$$

For $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$ we define the cocycle

$$\xi_\gamma(\sigma) \colon (w_1 : \ldots : w_7) \mapsto \left(\frac{\sqrt{\gamma_1}^\sigma}{\sqrt{\gamma_1}} w_1 : \cdots : \frac{\sqrt{\gamma_7}^\sigma}{\sqrt{\gamma_7}} w_7 \right).$$

This gives an isomorphism $L'(2,k) \simeq \mathrm{H}^1(k, \mathrm{Aut}(D_1, C)) \simeq \mathrm{H}^1(k, \mathrm{Pic}^0(C)[2])$, and D_γ is the twist of D_1 by the Galois cocycle ξ_γ. □

We define a partial map

$$\boldsymbol{\gamma} \colon C(k) \dashrightarrow L'(2,k);\ P \mapsto (\ell_1(P), \ldots, \ell_7(P))$$

and extend it to a full map by observing that by Definition 2.3, for any syzygetic quadruple $\mathfrak{q} = \{\ell_i, \ell_a, \ell_b, \ell_c\}$ we have that

$$\ell_i(P) \equiv \delta_{\mathfrak{q}} \ell_a(P) \ell_b(P) \ell_c(P) \pmod{\text{squares}}$$

whenever both sides are nonzero, so if $\ell_i(P) = 0$, we assign the appropriate value by taking the right hand side for a suitable quadruple $\mathfrak{q}$. We obtain

Proposition 4.3. *The map $\boldsymbol{\gamma} \colon C(k) \to L'(2,k)$ assigns to $P \in C(k)$ the cover $D_{\boldsymbol{\gamma}(P)}$ for which there is a point $Q \in D_{\boldsymbol{\gamma}(P)}(k)$ such that $\pi_{\boldsymbol{\gamma}(P)}(Q) = P$.*

5. Selmer sets

We restrict to the case where k is a number field, but our method applies to any global field of characteristic different from 2. We write $\mathcal{O}$ for its ring of integers, Ω for the set of places of k and write k_v for the completion of k at $v \in \Omega$. For non-archimedean v we write $\mathcal{O}_v \subset k_v$ for its ring of integers, $\mathfrak{p}_v$ for its maximal ideal, and $\mathcal{O}_v/\mathfrak{p}_v$ for its residue field.

The map $\boldsymbol{\gamma}$ from Proposition 4.3 and its local variant $\boldsymbol{\gamma}_v$ fit in the commutative diagram

$$\begin{array}{ccc} C(k) & \xrightarrow{\boldsymbol{\gamma}} & L'(2,k) \\ \big\downarrow & & \big\downarrow \rho_v \\ C(k_v) & \xrightarrow{\boldsymbol{\gamma}_v} & L'(2,k_v)\,. \end{array}$$

We define

$$\mathrm{Sel}^{(2)}(C/k) = \{\gamma \in L'(2,k) : \rho_v(\gamma) \in \boldsymbol{\gamma}_v(C(k_v)) \text{ for all } v \in \Omega_k\}.$$

Clearly we have $\boldsymbol{\gamma}(C(k)) \subset \mathrm{Sel}^{(2)}(C/k)$ and in particular, if $\mathrm{Sel}^{(2)}(C/k) = \emptyset$ then $C(k) = \emptyset$.

Let us now fix an integral model $C\colon f(x,y,z) = 0$ with $f \in \mathcal{O}[x,y,z]$, as well as 28 bitangent forms $\ell_{ij} \in \mathcal{O}[x,y,z]$. The *discriminant* $D_{27}(f)$ of a quartic (see [GKZ08, Chapter 13, Proposition 1.7]) is an integer form of degree 27 in the coefficients of f that vanishes precisely when f describes a singular curve. Thus, if we take

$$S = \{v \in \Omega_k : \mathrm{ord}_v(2D_{27}(f)) > 0, \text{ or } \ell_{ij} \in \mathfrak{p}_v[x,y,z], \text{ or } v \text{ is archimedean}\}$$

then C has good reduction at all v not in S, meaning that the coefficient-wise reductions of f and ℓ_{ij} describe a nonsingular plane quartic and its bitangents over $\mathcal{O}_v/\mathfrak{p}_v$. We consider the *unramified part*

$$L'(2,k_v)^{\mathrm{unr}} = \{\gamma \in L'(2,k_v) : \mathrm{ord}_v(\gamma_i) \equiv \mathrm{ord}_v(\gamma_j) \pmod 2 \text{ for all } i,j\}.$$

Proposition 5.1. *If C/k_v has good reduction as a plane quartic and the residue characteristic of k_v is odd, then $\boldsymbol{\gamma}_v(C(k_v)) \subset L'(2,k_v)^{\mathrm{unr}}$. If furthermore $\#\mathcal{O}_v/\mathfrak{p}_v \geq 66562$ then $\boldsymbol{\gamma}_v(C(k_v)) = L'(2,k_v)^{\mathrm{unr}}$.*

Proof. Let $\overline{C}$ be the reduction of C. Any point $P \in C(k_v)$ reduces to a point $\overline{P} \in \overline{C}(\mathcal{O}_v/\mathfrak{p}_v)$. Since the bitangents do not share contact points, we have $\mathrm{ord}_v(\ell_i(P)) > 0$ for at most one i. Let $\mathfrak{q} = \{\ell_i, \ell_a, \ell_b, \ell_c\}$ be a syzygetic quadruple. The good reduction properties imply that $\mathrm{ord}_v(\delta_{\mathfrak{q}}) = 0$, in the notation of Definition 2.3. We see that $\ell_i(P)\ell_a(P)\ell_b(P)\ell_c(P)$ must have even valuation, but that implies that $\mathrm{ord}_v(\ell_i(P))$ is even.

For the second part, we observe that for $\gamma \in L'(2,k_v)^{\mathrm{unr}}$, the curve D_γ has good reduction as well. This curve has genus 129 and, writing $q = \#\mathcal{O}_v/\mathfrak{p}_v$, the Hasse-Weil bounds give

$$\#\overline{D}_\gamma(\mathcal{O}_v/\mathfrak{p}_v) \geq q + 1 - 2\cdot 129\sqrt{q},$$

so if $q \geq 66562$, then there is a (necessarily smooth) point on $\overline{D}_\gamma$, so Hensel lifting gives a point in $D_\gamma(k_v)$. The image of that point on C maps to γ. □

We define

$$L'(2,k;S) = \{\gamma \in L'(2,k) : \rho_v(\gamma) \in L'(2,k_v)^{\mathrm{unr}} \text{ for all } v \in \Omega_k \setminus S\}.$$

Let $\mathcal{O}_S$ be the ring obtained by inverting the primes of the finite places in S. If $\mathcal{O}_S$ has odd ideal class number then $L'(2,k;S)$ is generated by $(\mathcal{O}_S^\times/\mathcal{O}_S^{\times 2})^7$, so it is a finite group. Note that by enlarging S, we can ensure that $\mathcal{O}_S$ has odd class number.

It follows from Proposition 5.1 that $\mathrm{Sel}^{(2)}(C/k) \subset L'(2,k;S)$. Furthermore, if we set

$$T = S \cup \{v \in \Omega_k : \#\mathcal{O}_v/\mathfrak{p}_v < 66562\},$$

then we obtain

$$\mathrm{Sel}^{(2)}(C/k) = \{\gamma \in L'(2,k;S) : \rho_v(\gamma) \in \boldsymbol{\gamma}_v(C(k_v)) \text{ for } v \in T\}. \qquad (5.1)$$

Hence, if we can compute generators for $\mathcal{O}_S^\times$, which is a standard task in algebraic number theory, and compute $\boldsymbol{\gamma}_v(C(k_v))$ for finite and real v, then we can compute the Selmer set.

5.1. **Computing the local image for archimedean places.** For $k_v = \mathbb{C}$ we have that $\mathbb{C}^\times = \mathbb{C}^{\times 2}$ and $C(\mathbb{C}) \neq \emptyset$, so there is nothing to compute: the local image is the whole (trivial) group $L'(2,\mathbb{C})$.

For $k = \mathbb{R}$ we have that $\mathbb{R}^\times/\mathbb{R}^{\times 2}$ is represented by $\{\pm 1\}$. Furthermore, a smooth plane quartic $C/\mathbb{R}$ with all bitangents defined over $\mathbb{R}$ has four components [Har76], and the map $\boldsymbol{\gamma}\colon C(\mathbb{R}) \to L'(2,\mathbb{R}) \simeq \mathbb{F}_2^6$ is continuous and therefore constant on components. In order to find $\boldsymbol{\gamma}(C(\mathbb{R}))$ we only need to find points on each component and evaluate $\boldsymbol{\gamma}$ there. Each pair of components has four bitangents touching each, so these contact points must be real. The remaining four bitangents might have complex conjugate contact points. Each pair of components is separated by a bitangent, so $\boldsymbol{\gamma}$ actually takes different values on the components: we know that $\#\boldsymbol{\gamma}(C(\mathbb{R})) = 4$.

Since we need to compute the bitangents anyway, we can use the real contact points to evaluate $\boldsymbol{\gamma}$. Once we have found four different images, we know we have determined the entire image.

5.2. **Computing the local image for finite places.** In this section, we take k to be a local field with ring of integers $\mathcal{O}$, uniformizer π with $\mathfrak{p} = \pi\mathcal{O}$, and a set D of representatives of $\mathcal{O}/\mathfrak{p}$.

We have $k^\times \simeq \mathbb{Z} \oplus \mathcal{O}^\times$. The map $\mu\colon k^\times \to k^\times/k^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathcal{O}^\times/\mathcal{O}^{\times 2})$ is constant on sets of the form $x_0 + \mathfrak{p}^{\mathrm{ord}(4)+1}$, with $x_0 \in \mathcal{O}^\times$, as can easily be checked from the fact that Newton iteration for finding the roots of $y^2 - x_0$ amounts to iterating the map $y \mapsto \frac{1}{2}(y + \frac{x}{y})$, which converges for $y \in 1 + 2\mathfrak{p}$ if $\mathrm{ord}((x_0-1)/4) > 1$.

We assume we have $f, \ell_{ij} \in \mathcal{O}[x,y,z]$ representing a quartic curve $C\colon f(x,y,z) = 0$ and its bitangents. Furthermore, we assume we have the $\delta_\mathfrak{q}$ from Definition 2.3 for all syzygetic quadruples $\mathfrak{q}$, or at least the 210 that involve $\ell_1, \ldots, \ell_7$.

Note that any $P \in C(k)$ admits a representative of one of the forms $(x_0 : y_0 : 1), (x_0 : 1 : \pi y_0), (1 : \pi x_0 : \pi y_0)$, with $x_0, y_0 \in \mathcal{O}$, so it is sufficient to restrict ourselves to $\mathcal{O}$-valued points on affine plane quartics.

We say a set of the form $\mathcal{B} = (x_0 + \mathfrak{p}^e) \times (y_0 + \mathfrak{p}^e)$ is a *Hensel-liftable ball* for $f(x,y) = 0$ if $0 \in f(\mathcal{B})$ and $(0,0) \notin \nabla_{xy} f(\mathcal{B})$, with ∇_{xy} denoting the gradient. In that case, applying Newton iteration to any point in $\mathcal{B}$ converges to an $\mathcal{O}$-valued point of $f(x,y) = 0$. It is a standard result that the $\mathcal{O}$-valued points on a nonsingular curve can be covered with finitely many Hensel-liftable balls (see Algorithm 2 in the Appendix).

In addition, we require that $\boldsymbol{\gamma}$ is constant on $\mathcal{B}\cap C(k)$. For this we use that the component $\boldsymbol{\gamma}_i(P)$ can be computed via either $\mu(\ell_i(P))$ or, for a syzygetic quadruple $\mathfrak{q}=\{\ell_i,\ell_a,\ell_b,\ell_c\}$, by $\mu(\delta_{\mathfrak{q}}\ell_a(P)\ell_b(P)\ell_c(P))$. Since bitangents do not share contact points, we see that for sufficiently small balls, at least one of the descriptions will be constant. We can then evaluate the map at a single representative. We start with a covering of Hensel-liftable balls and refine it as required. With Algorithm 3 (see Appendix) we find

$$\begin{aligned}\boldsymbol{\gamma}(C(k)) = &\textsc{LocalImage}(f(x,y,1)) \cup \textsc{LocalImage}(f(x,1,\pi y))\\ &\cup \textsc{LocalImage}(f(1,\pi x,\pi y)).\end{aligned}$$

Remark 5.2. The additional condition that $\boldsymbol{\gamma}$ be constant on our Hensel-liftable balls $\mathcal{B}$ is surprisingly easily satisfied. In experiments with $\mathcal{O}=\mathbb{Z}_p$, including for $p=2$, we find that refinement is only rarely required.

This happens because there are many syzygetic quadruples: each ℓ_i is involved in 45. Hence, if P lies close to a zero of ℓ_i, then there is likely a quadruple $\mathfrak{q}$ such that P lies far away from the contact points of the other three bitangents.

This is in stark contrast with the hyperelliptic case, where the role of the bitangent contact points is played by the Weierstrass points. They are fewer in number, but there are also fewer relations between them, necessitating higher lifting.

5.3. **Overcoming combinatorial explosion.** If k is a number field, then we can compute $L'(2,k;S)$ and the algorithms from Sections 5.1 and 5.2 allow us to compute the local images, so using (5.1) we can compute $\mathrm{Sel}^{(2)}(C/k)$. However, as an $\mathbb{F}_2$-vector space, we have $\dim_2 L'(2,k;S)=6(\#S)$, and S tends to have considerable size. For instance, if $k=\mathbb{Q}$ and C has points everywhere locally, then Proposition 1.2 yields that $\{2,3,5,7,11,\infty\}\subset S$, so $\#L'(\mathbb{Q},2;S)\geq 2^{36}$. Consequently, the point-wise iteration over $L'(k,2;S)$ that (5.1) suggests, is usually practically infeasible. We use some linear algebra first.

We extend $\boldsymbol{\gamma}$ linearly to divisors, while also keeping track of the parity of the degree,

$$\tilde{\boldsymbol{\gamma}}\colon \mathrm{Div}(C)\to\mathbb{F}_2\times L'(2,k);\quad \tilde{\boldsymbol{\gamma}}\Big(\sum n_P P\Big)=\Big(\sum n_P,\prod \boldsymbol{\gamma}(P)^{n_P}\Big),$$

(see [BPS16, §6]). One finds that principal divisors lie in the kernel, so $\tilde{\boldsymbol{\gamma}}$ descends to a map on $\mathrm{Pic}(C/k)$. We write $W_v=\langle\tilde{\boldsymbol{\gamma}}(C(k_v))\rangle$ for the $\mathbb{F}_2$-span. We write W_v^0 for the kernel of the projection $W_v\to\mathbb{F}_2$ on the first coordinate, and W_v^1 for its complement.

Given explicit representations for $L'(2,k;S)$ and $L'(2,k_v)$ as $\mathbb{F}_2$-vector spaces, it is straightforward to find a description of $\tilde{\rho}_v\colon \mathbb{F}_2\times L'(2,k;S)\to\mathbb{F}_2\times L'(2,k_v)$ as a linear transformation. We immediately obtain

$$\mathrm{Sel}^{(2)}(C/k)\subset W_C^1 := \bigcap_{v\in S}\tilde{\rho}_v^{-1}(W_v^1), \tag{5.2}$$

where the intersection on the right hand side is easily computed as an affine subset using standard linear algebra tools, even if $\#S\sim 100$.

On $\mathrm{Pic}^0(C/k_v)$ the kernel of $\tilde{\boldsymbol{\gamma}}_v$ is exactly $2\,\mathrm{Pic}^0(C/k_v)$. Furthermore, with the presence of a point $P_0\in C(k_v)$ we have that $\mathrm{Pic}^0(C/k_v)=\mathrm{Jac}_C(k_v)$, and since the latter is a compact k_v-Lie group we have

$$\#(\mathrm{Jac}_C(k_v)/2\,\mathrm{Jac}_C(k_v)) = (\#\,\mathrm{Jac}_C[2](k_v))/|2|_v^3, \tag{5.3}$$

where we normalize

$$|2|_v = \begin{cases} 2 & \text{if } v \text{ is a real place,} \\ 4 & \text{if } v \text{ is a complex place,} \\ (\#\mathcal{O}_v/\mathfrak{p}_v)^{-\operatorname{ord}_v(2)} & \text{if } v \text{ is a finite place.} \end{cases}$$

Lemma 5.3. *Suppose that C is defined over a completion $\mathbb{Q}_v$ of $\mathbb{Q}$. If $\{P_0, \dots, P_r\} \subset C(\mathbb{Q}_v)$ are such that*

$$\dim_2\langle \boldsymbol{\gamma}_v(P_i) - \boldsymbol{\gamma}_v(P_0) : i = 1, \dots, r\rangle = \begin{cases} 3 & \text{if } \mathbb{Q}_v = \mathbb{R}, \\ 9 & \text{if } \mathbb{Q}_v = \mathbb{Q}_2, \\ 6 & \text{otherwise,} \end{cases}$$

then $\tilde{\boldsymbol{\gamma}}_v(\operatorname{Pic}^0(C/\mathbb{Q}_v)) = W_v^0$ and $W_v = \langle \tilde{\boldsymbol{\gamma}}(P_0), \dots, \tilde{\boldsymbol{\gamma}}(P_r)\rangle$.

Proof. We have $\# \operatorname{Jac}_C[2](\mathbb{Q}_v) = 64$, so the dimension bound is just (5.3). Thus the condition is that the divisor classes $[P_1 - P_0], \dots, [P_r - P_0]$ generate $\operatorname{Pic}^0(C/\mathbb{Q}_v)/2\operatorname{Pic}^0(C/\mathbb{Q}_v)$. The second statement follows simply from $W_v = W_v^0 + \tilde{\boldsymbol{\gamma}}(P_0)$. □

This lemma provides us in many cases with a way to compute W_v directly and quickly. An alternative is to determine $\tilde{\boldsymbol{\gamma}}_v(C(k_v))$ using the algorithm sketched in Section 5.2. This has a complexity proportional to the size of the residue field $\mathcal{O}_v/\mathfrak{p}_v$, which is rather bad.

In many cases the k_v-valued contact points of the bitangents are already sufficient to generate W_v. In fact for real places this is always the case by the argument in Section 5.1.

It may be the case that $\operatorname{Pic}^0(C/k_v)/2\operatorname{Pic}^0(C/k_v)$ really does need divisors with higher degree places in their support. In that case, if the residue field is small enough, we can compute W_v via Section 5.2 or we can search for these higher degree places and use $\langle\tilde{\boldsymbol{\gamma}}_v(P_0)\rangle + \tilde{\boldsymbol{\gamma}}_v(\operatorname{Pic}^0(C/k_v))$ as an upper bound for W_v in (5.2).

Remark 5.4. If Lemma 5.3 applies to all $v \in S$ then we compute the 2-Selmer group of Jac_C as well, via

$$\operatorname{Sel}^{(2)}(\operatorname{Jac}_C/\mathbb{Q}) = \bigcap_{v\in S} \tilde{\rho}_v(W_v^0),$$

and in any case the right hand side gives a subgroup of the Selmer group, so we get a lower bound in all cases. See Section 6.2.

5.4. **Information at good primes.** Let k_v be a local field of odd residue characteristic, with $q = \#(\mathcal{O}_v/\mathfrak{p}_v)$. Then

$$\#L'(2, k_v)^{\mathrm{unr}} = 64.$$

If C/k_v has good reduction $\overline{C}$, then $\boldsymbol{\gamma}_v(P)$ is already determined by the reduction of P, so using the Hasse-Weil bounds, we obtain

$$\#\boldsymbol{\gamma}_v(C(k_v)) \le \#\overline{C}(\mathcal{O}_v/\mathfrak{p}_v) \le q + 1 + 6\sqrt{q}.$$

If $q \le 29$ then $\boldsymbol{\gamma}_v(C(k_v)) \subsetneq L'(2, k_v)^{\mathrm{unr}}$, and even if q is larger, it is quite likely that the local image is not the entire unramified set. Hence, for small residue class field, many of the two-covers D_γ fail to have points locally, even at primes of good reduction. We see that in the intersection (5.1), the primes of small norm actually impose significant conditions.

Algorithm 1: TwoCoverDescent

Input : Quartic $f \in \mathcal{O}[x, y, z]$ describing a nonsingular plane quartic C with bitangent forms $\{\ell_{ij} \in \mathcal{O}[x, y, z] : 0 \leq i < j \leq 7\}$ and the $\delta_{\mathfrak{q}}$ according to Definition 2.3, and a norm bound N.

Output: $\mathrm{Sel}^{(2)}(C/k; N)$

1 $S \leftarrow \{v \in \Omega_k : v$ archimedean or $\mathrm{ord}_v(D_{27}(f)) > 0\}$
2 $W \leftarrow \mathbb{F}_2 \times L'(2, k; S)$
3 **for** $v \in S$**:**
4 $\quad \mathcal{P} \leftarrow \{\tilde{\boldsymbol{\gamma}}_v(P) \in C(k_v) : \ell_{ij}(P) = 0$ for some $i, j\}$
5 $\quad$ **if** $\dim_2\langle P - Q : P, Q \in \mathcal{P}\rangle$ equals the bound in Lemma 5.3**:**
6 $\qquad W_v \leftarrow \langle \mathcal{P} \rangle$
7 $\quad$ **else:**
8 $\qquad W_v \leftarrow \langle \tilde{\boldsymbol{\gamma}}_v(C(k_v))\rangle$ as computed in Sections 5.1 and 5.2.
9 $\quad W \leftarrow W \cap \rho_v^{-1}(W_v)$
10 $W^1 \leftarrow \{w \in W : w_1 = 1\}$, where w_1 is the image of w in $\mathbb{F}_2$ from Line 2
11 **for** $v \in \Omega_k : v$ is finite and $\#(\mathcal{O}_v/\mathfrak{p}_v) \leq N$**:**
12 $\quad W^1 \leftarrow \{w \in W^1 : \tilde{\rho}_v(w) \in \tilde{\boldsymbol{\gamma}}_v(C(k_v))\}$.
13 **return** W

Because computing local images for primes of larger norm is expensive, we define a more easily computed set that contains $\mathrm{Sel}^{(2)}(C/k)$, by

$$\mathrm{Sel}^{(2)}(C/k; N) = \{\gamma \in L'(2, k; S) : (1, \gamma) \in W_C^1 \text{ for } v \in S \text{ and } \rho_v(\gamma) \in \boldsymbol{\gamma}_v(C(k_v)) \text{ for } v \text{ such that } \#(\mathcal{O}_v/\mathfrak{p}_v) \leq N\}.$$

We compute this set using Algorithm 1. If the resulting set is empty, then $C(k)$ is empty.

6. Results

We implemented Algorithm 1 for $k = \mathbb{Q}$ in Magma [BCP97] and tested it on two sample sets:

A. Curves parameterized by

$$\{(u_1, \ldots, v_3) \in \{-6, \ldots, 6\} : u_1 < u_2 < u_3 \text{ and } u_1 < v_1\}.$$

The inequalities normalize some of the permutations possible on the points that lead to isomorphic curves. We found 81070 configurations in general position. However, because of the small values of the coefficients, there are many configurations with extra symmetries, so we find many isomorphic curves in the configurations. We find 33471 distinct values for D_{27}, indicating that the collection contains many non-isomorphic curves as well.

B. 70000 curves with $u_1, \ldots, v_3$ chosen uniformly randomly from $\{-40, \ldots, 40\}$, while discarding configurations that are not in general position. We originally found two quartics with matching D_{27}. Their configurations differed by a permutation, so the curves were isomorphic. We replaced one of them.

In each case, we used Magma's `MinimizeReducePlaneQuartic` to find a nicer plane model, with smaller discriminant. Since isomorphisms change D_{27} by a 27^{th} power, it is easy to tell from discriminants when curves are not isomorphic.

	$C(\mathbb{Q}_v)=\emptyset$	$\mathrm{Sel}^{(2)}(C/\mathbb{Q})=\emptyset$	rational bitangent contact point	other rational point	total
A	3654	42477	34025	4568	81070
	4.5%	52%	42%	5.6%	100%
B	521	63926	4830	1244	70000
	0.7%	91%	6.9%	1.8%	100%

TABLE 6.1. Two-cover descent results

Typical examples take less than 2 seconds to execute, with the quartic reduction step being one of the more expensive and less predictable steps. Occasional anomalies arise, where computation of a local image at a large prime is required. The whole experiment represents about 126 CPU hours of work.

Example 6.1. As a small, typical, example, take

$$\begin{pmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{pmatrix} = \begin{pmatrix} 17 & -7 & -9 \\ 35 & 3 & 9 \end{pmatrix}.$$

We find

$$\begin{aligned} C\colon 9x^4 - 60x^3y + 357x^2y^2 + 246xy^3 + 16y^4 - 42x^3z + 259x^2yz - 168xy^2z \\ - 141y^3z + 31x^2z^2 - 492xyz^2 + 207y^2z^2 + 42xz^3 - 27yz^3 + 9z^4 = 0 \end{aligned}$$

and $D_{27}(C) = 2^{34}\cdot 3^{20}\cdot 5^{10}\cdot 7^8\cdot 11^2\cdot 13^6\cdot 17^4\cdot 19^4\cdot 29^2\cdot 37^2\cdot 41^2$. The curve C has points everywhere locally. We have $\dim_2 L'(2,\mathbb{Q};S) = 72$ and $W_C = \bigcap_{v\in S} \tilde{\rho}_v^{-1}(W_v)$ has $\dim_2 W_C = 10$. We find that W_C^1 is non-empty, so it has 2^9 elements. Computing $W_{C,T}^1 = \{w \in W_C^1 : \tilde{\rho}_v(w) \in \tilde{\gamma}_v(C(k_v)) \text{ for } v \in T\}$ is quite doable, for various sets T. We conclude that $C(\mathbb{Q}) = \emptyset$ from, for example,

$$\mathrm{Sel}^{(2)}(C/\mathbb{Q}) \subset W_{C,T}^1 = \emptyset \text{ for } T = \{2,3,5\} \text{ or } \{31,43,47,53,71,83\}.$$

Furthermore, from the data computed we can conclude that

$$\dim_2 \mathrm{Sel}^{(2)}(\mathrm{Jac}_C/\mathbb{Q}) = \dim_2 W_C^0 = 9,$$

so either $\mathrm{Jac}_C(\mathbb{Q})$ has free rank 3 or $Ш(\mathrm{Jac}_C/\mathbb{Q})[2]$ is non-trivial.

6.1. **Results of two-cover descent.** We executed Algorithm 1 on our samples, with $N = 50$. This allowed us to determine the existence of rational points on each of the curves. We summarize our findings in Table 6.1.

When $\mathrm{Sel}^{(2)}(C/\mathbb{Q}) \neq \emptyset$ and C has no rational bitangent contact points (possibly a hyperflex), we search for a low-height nonsingular point using `PointSearch` on either the sextic model (3.1) or the plane quartic model we construct from it. These are the curves reported in the “other rational point” column. For two curves we needed to search up to a height bound of 10^7.

Another interesting fact is that local obstructions are quite rare (having a local obstruction implies $\mathrm{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset$). Furthermore we only found $C(\mathbb{Q}_p) = \emptyset$ for $p = 2, 11, 23$, and only when C has good reduction at those places. Proposition 1.2 gives a partial explanation of this fact. This is quite contrary to the case of hyperelliptic curves, where local obstructions do tend to occur at primes of bad reduction.

	6	7	8	9	10	11	12	13	
A	0.05%	18.7%	39.4%	29.1%	10.1%	2.28%	0.29%	0.006%	$(n = 31990)$
B	0	20.2%	41.8%	27.9%	8.71%	1.27%	0.10%	0.006%	$(n = 51685)$

TABLE 6.2. Distribution of $\dim_2 \mathrm{Sel}^{(2)}(\mathrm{Jac}_C/\mathbb{Q})$ where our data allowed its computation

6.2. **Information on rank and Ш.** We have

$$\mathrm{Sel}^{(2)}(\mathrm{Jac}_C/\mathbb{Q}) = L'(\mathbb{Q}, 2; S) \cap \bigcap_{v \in S} \rho_v^{-1} \boldsymbol{\gamma}_v(\mathrm{Pic}^0(C/\mathbb{Q}_v)).$$

Lemma 5.3 gives a condition for when the sets on the right hand side are generated by differences of degree 1 points. For a reasonable proportion of our curves, our data allows us to compute $\mathrm{Sel}^{(2)}(\mathrm{Jac}_C/\mathbb{Q})$. We list the results in Table 6.2. In the rest of this section, we only consider these examples.

With $\mathrm{Jac}_C[2](\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^6$, we must have that the Selmer rank is at least 6, but as one can see, the distribution has an average significantly higher than that. Part of that is explained by the fact that C, and hence the class $J^1 \in H^1(k, \mathrm{Jac}_C)$ representing $\mathrm{Pic}^1(C/\mathbb{Q})$ is trivial everywhere locally. Since C has quadratic points, we can pull the class back under the homomorphism $\mathrm{Sel}^{(2)}(\mathrm{Jac}_C/\mathbb{Q}) \to H^1(k, \mathrm{Jac}_C)[2]$ and the preimage is likely independent of the image of $\mathrm{Jac}_C[2](\mathbb{Q})$.

If $W_C^1 = \emptyset$ in (5.2) then it follows by [Cre20, Theorem 5.3] that J^1 is not divisible by two in $Ш(\mathrm{Jac}_C/\mathbb{Q})$, and therefore is nontrivial. This happens in about half the examples.

Once we take into account that we expect that $\dim_2 \mathrm{Sel}^{(2)}(\mathrm{Jac}_C/\mathbb{Q}) \geq 7$, we find that the distributions in Table 6.2, particularly for collection **B**, match [PR12, Conjecture 1.1] rather well. This does require us to account for the fact that J^1 almost always has points everywhere locally.

Generally, non-hyperelliptic curves tend to have points everywhere locally. Therefore, one actually should expect that Selmer groups of Jacobians of curves behave a little differently from those of general abelian varieties, because they tend to come equipped with an everywhere locally trivial torsor.

ACKNOWLEDGMENTS

We thank Michael Stoll for interesting discussions and suggestions on how to interpret the rank results in light of [PR12], and an anonymous referee for helpful comments.

REFERENCES

[BCP97] The MAGMA computer algebra system is described in Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265. ↑6

[BFL19] Barinder Banwait, Francesc Fité, and Daniel Loughran, *Del Pezzo surfaces over finite fields and their Frobenius traces*, Math. Proc. Cambridge Philos. Soc. **167** (2019), no. 1, 35–60. ↑3

[BGW17] Manjul Bhargava, Benedict H. 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. **30** (2017), no. 2, 451–493. With an appendix by Tim Dokchitser and Vladimir Dokchitser. ↑1

[Bru06] Nils Bruin, *Some ternary Diophantine equations of signature* $(n, n, 2)$, Discovering mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 63–91. ↑A

[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. ↑1, 5.3

[BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370. ↑1, A

[CW32] C. Chevalley and A. Weil, *Un théorème d'arithmétique sur les courbes algébriques*, C. R. Acad. Sci. Paris **195** (1932), 570–572. ↑1

[Cre20] Brendan Creutz, *Generalized Jacobians and explicit descents*, Math. Comp. **89** (2020), no. 323, 1365–1394, DOI 10.1090/mcom/3491. MR4063321 ↑6.2

[Cob22] Arthur B. Coble, *Associated sets of points*, Trans. Amer. Math. Soc. **24** (1922), no. 1, 1–20. ↑3

[Dol12] Igor V. Dolgachev, *Classical algebraic geometry*, Cambridge University Press, Cambridge, 2012. A modern view. ↑2, 3

[GKZ08] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants, resultants and multidimensional determinants*, Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2008. Reprint of the 1994 edition. ↑5

[GH04] Benedict H. Gross and Joe Harris, *On some geometric constructions related to theta characteristics*, Contributions to automorphic forms, geometry, and number theory, Johns Hopkins Univ. Press, Baltimore, MD, 2004, pp. 279–311. ↑2, 2, 2.5, 3, 3

[Har76] Axel Harnack, *Ueber die Vieltheiligkeit der ebenen algebraischen Curven*, Math. Ann. **10** (1876), no. 2, 189–198 (German). ↑5.1

[Lew19] Daniel Lewis, *An implementation of two-cover descent on plane quartic curves*, Simon Fraser University, 2019, `https://summit.sfu.ca/identifier/etd20482`. (M.Sc. thesis). ↑1

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. ↑1

[PR12] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269. ↑1.5, 6.2, 6.2

[Tho16] Jack A. Thorne, *Arithmetic invariant theory and 2-descent for plane quartic curves*, Algebra Number Theory **10** (2016), no. 7, 1373–1413. With an appendix by Tasho Kaletha. ↑1

Appendix A. Local algorithms

We use the notation from Section 5.2. The algorithms here are in the spirit of [Bru06, §5] and [BS09, §4].

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6

Email address: `nbruin@cecm.sfu.ca`

URL: `http://www.cecm.sfu.ca/~nbruin`

Department of Mathematics, The University of Arizona, 617 N. Santa Rita Ave, Tucson, AZ 85721, USA

Email address: `dlewis3@math.arizona.edu`

URL: `https://sites.google.com/view/dan-lewis-mathematics/`

Algorithm 2: HenselBalls

Input : $f \in \mathcal{O}[x,y]$, describing a smooth curve.
Output: A finite set $\{(x_t, y_t, e_t)\}_t$ of Hensel-liftable balls covering the $\mathcal{O}$-valued solutions of $f(x,y)=0$.

for $(x_0,y_0) \in \{(x_0,y_0) \in D^2 : f(x_0,y_0) \equiv 0 \pmod{\mathfrak{p}}\}$**:**
    $R \leftarrow \emptyset$
    if $\frac{\partial f}{\partial x}(x_0,y_0) \not\equiv 0 \pmod{\mathfrak{p}}$ or $\frac{\partial f}{\partial y}(x_0,y_0) \not\equiv 0 \pmod{\mathfrak{p}}$**:**
        $R \leftarrow R \cup \{(x_0,y_0,1)\}$.
    else:
        $g \leftarrow f(x_0 + \pi x, y_0 + \pi y)$
        $T \leftarrow$ HenselBalls$(g/\text{content}(g))$
        $R \leftarrow R \cup \{(x_0 + \pi x_1, y_0 + \pi y_1, e+1) : (x_1, y_1, e) \in T\}$.
    return R

Algorithm 3: LocalImage

Input : $f \in \mathcal{O}[x,y]$ describing a smooth plane quartic, together with its bitangent forms $\{\ell_{ij} \in \mathcal{O}[x,y] : 0 \le i < j \le 7\}$ and syzygetic data $\delta_{\mathfrak{q}}$ as in Definition 2.3.
Output: Local image of $\boldsymbol{\gamma}_v$ on the given affine patch

Denote the mod-squares map by $\mu\colon \mathcal{O} \setminus \{0\} \to k^\times / k^{\times 2}$.
$T \leftarrow$ HenselBalls(f)
$R \leftarrow \emptyset$
while $T \neq \emptyset$**:**
    Take (x_0, y_0, e) from T,
    $L \leftarrow [\ell_{ij}(x_0,y_0) : 0 \le i < j \le 7]$
    for $i = 1, \ldots, 7$**:**
        if $\text{ord}(L_i) < e - \text{ord}(4)$**:**
            $\gamma_i \leftarrow \mu(L_i)$
        else if there is a syzygetic quadruple $\mathfrak{q} = \{\ell_i, \ell_a, \ell_b, \ell_c\}$ such that $\max(\text{ord}(\ell_a(x_0,y_0)), \text{ord}(\ell_b(x_0,y_0)), \text{ord}(\ell_c(x_0,y_0))) < e - \text{ord}(4)$**:**
            $\gamma_i \leftarrow \mu(\delta_{\mathfrak{q}} \ell_a(x_0,y_0) \ell_b(x_0,y_0) \ell_c(x_0,y_0))$
        else: [**Remark:** we refine the covering]
            $g \leftarrow f(x_0 + \pi^e x, y_0 + \pi^e y)$
            $h \leftarrow g/\text{content}(g)$ [**Remark:** $h \pmod{\mathfrak{p}}$ will be linear]
            for $(x_1, y_1) \in \{(x_1, y_1) \in D : h(x_1, y_1) \equiv 0 \pmod{\mathfrak{p}}\}$**:**
                $T \leftarrow T \cup (x_0 + \pi^e x_1, y_0 + \pi^e y_1, e+1)$
            break to while
    Add $(\gamma_1, \ldots, \gamma_7)$ to R.
return R.