An implementation of two-cover descent on plane quartic curves

by

Daniel Lewis

MMath, University of Warwick, 2014

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Summer 2019

Approval

Name:	**Daniel Lewis**
Degree:	**Master of Science (Mathematics)**
Title:	**An implementation of two-cover descent on plane quartic curves**
Examining Committee:	**Chair:** Stephen Choi Professor
	Nils Bruin Senior Supervisor Professor
	Nathan Ilten Supervisor Assistant Professor
	Imin Chen Internal Examiner Associate Professor
Date Defended:	**August 09, 2019**

Abstract

We gather experimental evidence related to the question of deciding whether a smooth plane quartic curve has a rational point. Smooth plane quartics describe curves in genus 3, the first genus in which non-hyperelliptic curves occur. We present an algorithm that determines a set of unramified covers of a given plane quartic curve, with the property that any rational point will lift to one of the covers. In particular, if the algorithm returns the empty set, then the curve has no rational points. We apply our algorithm to a total of 1000 isomorphism classes of randomly-generated plane quartic curves.

Keywords: rational points; bitangents; plane quartic curves; descent methods

Dedication

To Lita, Leon, Margaret and the dearly missed Eric.

Acknowledgements

First and foremost I would like to thank Professor Nils Bruin for suggesting this thesis, meeting with me each week, and guiding me through the process with sage advice and good humour.

Next I wish to thank Professor Nathan Ilten for his help and advice throughout my time at SFU. He has taught four of the courses I have taken, organised the NTAG seminar, and his door is seemingly always open.

Last I would like to thank my friends, family and colleagues. Special mentions go to Dr Avi Kulkarni, for his advice and technical expertise in arithmetic geometry and MAGMA programming; Dr Stefan Hannie and Brandon Elford, for helping me with coding difficulties; Sasha Zotine and Eugene Filatov for advice in algebraic geometry; Garrett Paluck and Dan Messenger for assistance with the Graduate Caucus; and many others whose names this margin is too small to contain. Most of all, many thanks to Gaby and Peter Eirew for putting me up when I first arrived in Vancouver, and Mohsen Seifi for putting up with me as housemate for two full years!

I would also like to thank all at the TSSU, Drs Elliott, Ng and Rosenfeld, Greg at Play Vancouver, and all at Richmond Olympic Parkrun and North Burnaby Runners.

Table of Contents

List of Figures

Chapter 1

Introduction

1.1 Historical motivation

Descent methods have been a part of number theory since the time of Pierre de Fermat. Fermat developed the method of *infinite descent* to prove that certain equations have no positive integral solutions. For instance, consider the following result:

Theorem 1.1. *There is no solution in positive integers to the equation*

$$y^2 = (2x^2 + 3)(11x^2 + 16). \tag{1.1}$$

Fermat's idea is to show that the existence of an integral solution would imply the existence of a smaller integral solution. In this way we can form an infinitely decreasing sequence of positive integers $n_1 > n_2 > \cdots > 0$, which is of course impossible.

This particular equation has no integral, or even rational solutions. In a way, that makes (1.1) even easier to prove. The proof still requires a non-trivial step, however: we need what we will name in Chapter 3 a *covering collection*. As a result, the proof is still deemed to be based on descent.

Definition 1.2. We say that a curve C over $\mathbb{Q}$ is *everywhere locally solvable* if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

An equation that describes a curve that is not everywhere locally solvable obviously has no solution (see Section 2.6). However, for (1.1), one can relatively straightforwardly prove that the curve $C : f(x) = 0$, where $f(x) = (2x^2+3)(11x^2+16) = f_1(x)f_2(x)$, is everywhere locally solvable.

Due to the Hasse–Weil bound (see Section 2.10), we need only consider the primes dividing the discriminant $16896 = 2^9 \cdot 3 \cdot 11$ of f. The bound gives that genus 1 curves over finite fields with at least 3 elements must have a point. If the curve is smooth, then Hensel-lifting gives that the reduction of C has a non-singular point, so by Hensel's Lemma $C(\mathbb{Q}_p)$ is non-empty.

Inspection then allows us to find points in $C(\mathbb{Q}_p)$, for $p = 2, 3, 11$. We see also that $C(\mathbb{R}) \neq \emptyset$ since the leading coefficient of f is positive. So C is everywhere locally solvable, and the proof of Theorem 1.1 is necessarily a little more involved.

Proof of Theorem 1.1 (Sketch). Let C be defined as above. We show that $C(\mathbb{Q}) = \emptyset$; the result then follows a fortiori. The resultant $\mathrm{res}_x(f_1, f_2) = 1$, so any point in $C(\mathbb{Q})$ must come from a rational point on a curve

$$D_d : \begin{cases} 2x^2 + 3z^2 = dy_1^2, \\ 11x^2 + 16z^2 = dy_2^2, \end{cases} \tag{1.2}$$

for some $d \in \{\pm 1\}$, with $y = dy_1y_2$. To clarify, any rational-valued point (x, y) on C corresponds to a solution in coprime integers to (1.1), for some d. This means that x and z are coprime. Since the resultant $\mathrm{res}_x(f_1, f_2) = 1$, the two expressions $2x^2 + 3z^2$ and $11x^2 + 16z^2$ have no common factors. So each of these expressions must be a square, or the negative of a square.

Since $f_1(\xi) = f_2(\xi) > 0$ for all $\xi \in \mathbb{R}$, we have $D_{-1}(\mathbb{R}) = \emptyset$. For $d = 1$, we can show that $D_1(\mathbb{F}_3) = \emptyset$, so $D_1(\mathbb{Q}_3) = \emptyset$. So for all $d \in \{\pm 1\}$, D_d is not everywhere locally solvable. Therefore, $C(\mathbb{Q}) = \emptyset$. □

Descent methods were employed once again in the early 20th Century, as Louis Mordell proved what is now known as the Mordell–Weil theorem, in the case of elliptic curves defined over number fields.

Theorem 1.3 (Mordell, 1922)**.** *Let K be a number field and let E/K be an elliptic curve. Then the group $E(K)$ is finitely generated.*

Proof. See Silverman [30, ch. 8]. □

The key idea here was to split the proof into two parts, the "weak Mordell–Weil theorem" (see [30, ch. 8 §1]), and an infinite descent using so-called *height functions* (see [30, ch. 8 §§3-6]) satisfying various properties.

The following result, adapted from [30, ch. 10 Proposition 1.4], makes up a part of the proof of this case of the weak Mordell–Weil theorem.

Proposition 1.4 (2-Descent)**.** *Let E/K be an elliptic curve given by a Weierstrass equation*

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3) \tag{1.3}$$

for some $e_1, e_2, e_3 \in K$. Then there is a group homomorphism

$$\delta : E(K) \to (K^*/K^{*2})^2 \tag{1.4}$$

defined by

$$(x, y) \mapsto \begin{cases} (x - e_1, x - e_2) & x \neq e_1, e_2 \\ \left(\frac{e_1 - e_3}{e_1 - e_2}, e_1 - e_2\right) & x = e_1 \\ \left(e_2 - e_1, \frac{e_2 - e_3}{e_2 - e_1}\right) & x = e_2 \\ (1, 1) & x = \infty, \end{cases} \tag{1.5}$$

with $\ker \delta = 2E(K)$.

Proof. See Silverman [30, ch. 10 Theorem 1.1]. □

We shall provide an analogous setup in the case of a plane quartic curve C/K, and use this to obtain information about the rational points $C(K)$.

1.2 Recent developments

In their joint paper [4] of 2008, Bruin and Stoll apply descent methods to the case of curves of genus 2 over $\mathbb{Q}$, given by equations of the form $y^2 = f(x)$ with f a square-free polynomial of degree 5 or 6, with integral coefficients of absolute value at most 3. They exhibit rational points on 70% of their sample size of almost 200000 isomorphism classes of curves, and descent methods allow them to prove the non-existence of rational points on all bar 1492 of the remaining 58681 curves. To these 1492 curves they apply a "Mordell–Weil sieve" computation, which rules out the existence of rational points on all but 42 curves. Assuming standard conjectures on L-series and the Birch and Swinnerton-Dyer conjecture, they are able to deduce the non-existence of rational points on these 42 curves as well.

In a second paper published the following year [5], the two authors provide further details of this so-called "two-cover descent" method in the context of hyperelliptic curves. They demonstrate how to determine a set of unramified covers of a given hyperelliptic curve,

such that any rational point will lift to one of the covers. We call such a set a *covering collection*. They discuss applications of their method to curves with known rational points, and to curves of genus one. They provide statistics on their experimental data, using these to provide heuristics on how frequently one can expect curves of genus two to have an everywhere locally solvable two-cover.

Bruin, Stoll and Poonen address the question of curves of genus three in their 2016 article [3]. This article provides unified description of explicit descent computations, subsuming all previous examples. It also gives the first examples of such computations applied to genus three curves without requiring special geometric properties.

1.3 Goal

In this thesis, we apply descent methods to a large collection of smooth plane quartic curves to prove, where possible, that they have no rational points. Smooth plane quartics describe curves in genus 3, the first genus in which non-hyperelliptic curves occur. Indeed, the numerical computations described in this thesis are the first larger-scale systematic investigation of the success rate of using descent methods to prove the non-existence of rational points on non-hyperelliptic curves.

We concentrate on curves that have all their bitangents defined over $\mathbb{Q}$. This situation is analogous to that of hyperelliptic curves with all their Weierstrass points defined over $\mathbb{Q}$. An interesting contrast is that such hyperelliptic curves automatically have rational points, so trying to prove otherwise is futile. On the contrary, only a small proportion of the non-hyperelliptic curves we consider have rational ponts, and two-cover descent as described in [2] is surprisingly often successful in proving so. Indeed, over a data set of 1000 isomorphism classes of plane quartic curves, we find rational points on 177 of the curves. Two-cover descent allows us to conclude that all of the remaining 823 curves do not have rational points. See Chapter 6 for further discussion of our findings.

1.4 Roadmap

In Chapter 2 we clarify our notation and provide the theoretical background necessary to present and explain our two-cover descent setup.

Chapter 3 is where we present our setup. We prove the results needed to ensure the success of our routines.

In order to carry out our experiments, we need some way to generate plane quartic curves together with their bitangents. In Chapter 4 we show how one can do this using classical algebraic-geometric constructions.

In Chapter 5 we explain the specific design choices we have made in implementing the procedures described in Chapters 3 and 4.

Finally, in Chapter 6 we provide our experimental results, and briefly describe the next steps we could take to further improve these results.

1.5 Electronic data

Please see the accompanying electronic resources at
`https://github.com/danlewis92/quartic-curves`
for a complete list of all curves considered together with the algorithms that should make it relatively easy to check the computations. The file `TestCurves.m` lists all the curves, represented by a sequence of 9 numbers in the interval $\{-20, \ldots, 20\}$. The file `Curves.m` provides a minimal model (see [32]) for each of these curves. In the file `routines.m` we include all our algorithms in machine-readable format for MAGMA [1].

Chapter 2

Background

In this chapter we briefly review some notions in algebraic number theory and algebraic geometry that are essential to the work in this thesis. For a more comprehensive treatment, we refer the reader to [21, chs. 1,2] and [13, chs. 2,3].

2.1 Notation

We write $k[x, y, z]$ for the multivariate polynomial ring over a field k in variables x, y, z. This polynomial ring naturally carries the structure of a k-vector space. We write $k[x, y, z]_n$ for the subspace consisting of homogeneous polynomials of total degree n.

Throughout this thesis, we let $\overline{k}$ denote an algebraic closure of a field k, and k^* denote the unit group of k.

We write $\mathbb{P}^2$ for projective 2-space over k (see Hartshorne [13, ch. 1 §2]). The set of k-rational points of $\mathbb{P}^2$, denoted $\mathbb{P}^2(k)$, is the set of 1-dimensional k-subvectorspaces of k^3, which can be represented as $(k^3 \setminus \{(0,0,0)\})/\equiv$, where $(x_0, y_0, z_0) \equiv (x_1, y_1, z_1)$ if the matrix $\begin{pmatrix} x_0 & y_0 & z_0 \\ x_1 & y_1 & z_1 \end{pmatrix}$ is of rank smaller than 2. See Hartshorne [13, ch. 2 §2] for further details of the Proj construction. Varieties in $\mathbb{P}^2$ are then irreducible subsets of the form

$$Z(T) = \{P \in \mathbb{P}^2 : f(P) = 0 \text{ for all } f \in T\},$$

for some set T of homogeneous elements of $k[x, y, z]$, equipped with the induced topology.

Thanks to Hilbert's Nullstellensatz we can distinguish varieties by looking at their $\overline{k}$-points, so in what follows we can avoid explicitly talking about schemes and define things in terms of point sets over $\overline{k}$.

2.2 Curves and rational points

Definition 2.1. A *projective plane curve* C is a projective variety of dimension one. The $\overline{k}$-rational points form a non-empty set

$$C(\overline{k}) = \left\{(x : y : z) \in \mathbb{P}^2(\overline{k}) \colon f(x, y, z) = 0\right\}, \tag{2.1}$$

defined by some non-constant polynomial $f \in \overline{k}[x, y, z]$. Typically, we will write

$$C \colon f(x, y, z) = 0, \tag{2.2}$$

for this leaves no ambiguity. The *degree* of C is simply the degree of f. A *smooth* curve is one whose points are all non-singular.

Definition 2.2. We say that a projective plane curve C is *defined over* k if its defining polynomial $f \in k[x, y, z]$. In this case the set of *k-rational points* of C, denoted $C(k)$, is defined as

$$C(k) = C(\overline{k}) \cap \mathbb{P}^2(k). \tag{2.3}$$

The simplest class of examples to consider is *conics*, those curves of degree two.

Example 2.3. Let C_1 be the projective plane curve with defining equation

$$C_1 \colon x^2 + y^2 = -z^2. \tag{2.4}$$

It is straightforward to see that $C_1(\mathbb{Q}) = \emptyset$, for indeed $C_1(\mathbb{Q}) \subseteq C_1(\mathbb{R}) = \emptyset$, since the squares of real numbers are non-negative.

Example 2.4. Let C_2 be the projective plane curve with defining equation

$$C_2 \colon x^2 + y^2 = 3z^2. \tag{2.5}$$

Again $C_2(\mathbb{Q}) = \emptyset$, but the proof take a little more work this time. First, note that every point $P \in \mathbb{P}^2(\mathbb{Q})$ can be represented by coordinates $P = (x : y : z)$, with $x, y, z \in \mathbb{Z}$ and $\gcd(x, y, z) = 1$. Now, the only squares modulo 3 are 0 and 1, so consideration of the cases forces $x \equiv y \equiv 0 \pmod 3$. But then looking modulo 9 we see that $z^2 \equiv 0 \pmod 3$, which implies that $z \equiv 0 \pmod 3$. So our coordinates x, y, z have a common factor of 3. This contradiction forces $C_2(\mathbb{Q}) = \emptyset$.

Perhaps these examples suggest that computation of rational points is a routine task, but they are somewhat contrived. For many curves, much more powerful arguments are needed to conclude anything about the set $C(\mathbb{Q})$. Two-cover descent methods provide one such means, and we will turn our focus to them in Chapter 3, but we should first turn our attention to the classical results of Hasse and Minkowski. For this, we follow Cohen [7, ch. 5].

2.3 Ostrowski's theorem

Recall (from e.g. [21, p.116]) that an *absolute value* on a field k is a map

$$|\cdot|\colon k \to \mathbb{R}_{\geq 0} \tag{2.6}$$

satisfying each of the following three properties:

- $|x| = 0 \iff x = 0$,
- $|xy| = |x||y|$,
- $|x + y| \leq |x| + |y|$.

Example 2.5.

- The *trivial absolute value* on k is that for which $|x|_{\text{triv}} = 1$ for all $x \neq 0$.
- For each prime $p \in \mathbb{Z}_{>0}$, we have a *p-adic absolute value* on $\mathbb{Q}$:

$$\left|p^n \frac{a}{b}\right|_p = \begin{cases} 0 & \text{if } a = 0, \\ p^{-n} & \text{if } a, b \neq 0,\ a, b \in \mathbb{Z},\ p \nmid a,\ p \nmid b. \end{cases} \tag{2.7}$$

  We write $v_p\left(p^n \frac{a}{b}\right) = n$. This v_p is the *p-adic valuation.*

- We also have the *standard absolute value* on $\mathbb{Q}$, denoted $|\cdot|$ or $|\cdot|_\infty$, for it corresponds to the infinite place ∞:

$$|x|_\infty = \max\{x, -x\}. \tag{2.8}$$

For simplicity, we shall define two valuations to be equivalent via an algebraic criterion, and follow this with a topological remark. Neukirch [21, pp.116-117] argues in the opposite direction.

Definition 2.6. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on k are *equivalent* if and only if there exists a real number $s > 0$ such that

$$|x|_1 = |x|_2^s \tag{2.9}$$

for all $x \in k$.

Remark 2.7. If we define the distance between two points $x, y \in k$ by

$$d(x, y) = |x - y|, \tag{2.10}$$

then we make k into a metric space and a fortiori a topological space. It then follows that two absolute values are equivalent if they define the same topology on k; see [21, p. 117].

We may now present one formulation of Ostrowski's theorem, which motivates why in Section 2.6 we only consider the completions $\mathbb{Q}_p$ (for primes p) and $\mathbb{R}$ of $\mathbb{Q}$.

Theorem 2.8 (Ostrowski)**.** *Every non-trivial absolute value $|\cdot|$ on $\mathbb{Q}$ is equivalent to either $|\cdot|_p$ for some prime $p \in \mathbb{Z}_{>0}$, or $|\cdot|_\infty$.*

Proof. Neukirch proves a stronger statement [21, pp. 124-125], from which the above theorem follows as an immediate corollary. □

2.4 Invariants of plane quartic curves

In his 1987 paper [8], Jacques Dixmier classified seven algebraic invariants of projective plane quartic curves. More recently, Toshiaki Ohno completed the classification [22], defining six further invariants, for a total of 13. Lercier et al. have since then implemented these invariants in MAGMA [18]. We make use of their code to distinguish isomorphism classes of the curves we generate, and thereby ensure we are considering sufficiently many non-isomorphic curves.

Of the Dixmier–Ohno invariants, the one we shall make the most use of is the *discriminant*, which was known to Salmon [27]. We denote the discriminant I_{27}, in keeping with Dixmier's notation. Note that I_{27} is defined for any plane quartic curve, and $I_{27}(f) \neq 0$ if and only if f describes a smooth plane quartic curve.

The *genus* g of a smooth plane curve of degree d is given by the genus–degree formula

$$g = \frac{1}{2}(d-1)(d-2). \tag{2.11}$$

In particular, smooth plane quartic curves all have genus 3.

2.5 The reduction of an equation for a curve

In this section we define what it means for primes to be of good/bad reduction for a given curve. See Silverman [30, §VII.2] for a more detailed treatment, restricted to the case of elliptic curves.

Let D be a smooth projective curve, defined over $\mathbb{Q}$, with defining equation

$$D : G(x, y, z) = 0, \tag{2.12}$$

for some non-constant polynomial $G \in \mathbb{Q}[x, y, z]$. As we saw in Example 2.4, we may scale (2.12) such that D is defined by a polynomial with integer coefficients. The resulting equation can be considered over $\mathbb{F}_p$. We denote this variety by $\tilde{D}$, so

$$\tilde{D} : g(x, y, z) = 0, \tag{2.13}$$

for some non-constant polynomial $g \in \mathbb{F}_p[x, y, z]$. If $\tilde{D}$ is a non-singular variety over $\mathbb{F}_p$, then we say D has good reduction at the prime p.

Remark 2.9. If $\tilde{D}$ describes a singular variety over $\mathbb{F}_p$, it may still be the case that there exists another equation of the form (2.13) that describes a curve D' that is isomorphic to D over $\mathbb{Q}$ and has good reduction at p. In that case the *curve* D over $\mathbb{Q}$ can still be considered to have good reduction. In the rest of this thesis, we will consider only a single defining equation for any particular curve and restrict our notion of good reduction to that of the equation given.

Proposition 2.10. *Let $f \in \mathbb{Z}[x, y, z]$ be a defining polynomial for a smooth plane quartic curve C over $\mathbb{Q}$. Then $I_{27}(f) \in \mathbb{Z}$, and for any prime p that does not divide $I_{27}(f)$, we have that C has good reduction at p.*

Proof. First, note that $I_{27}(f)$ is an integer polynomial expression in the coefficients of f, so it follows that $I_{27}(f)$ is an integer as well.

Let $\tilde{f} \in \mathbb{F}_p[x, y, z]$ be the coefficient-wise reduction of f modulo p. Since $I_{27}(f)$ is just a polynomial combination of coefficients, we have that $I_{27}(\tilde{f}) \equiv I_{27}(f) \pmod{p}$. If p does not divide $I_{27}(f)$ then $I_{27}(\tilde{f}) \neq 0$, so it describes a smooth curve over $\mathbb{F}_p$. It follows that C has good reduction at p. □

For polynomials f as in Proposition 2.10, we refer to primes p that divide $I_{27}(f)$ as *primes of bad reduction*. As we saw in Remark 2.9, it is only our chosen equation that has bad reduction at p.

2.6 The local–global principle

Ostrowski's theorem classifies all the completions of $\mathbb{Q}$: they are $\mathbb{R}$ and $\mathbb{Q}_p$, for all primes p. Our principal concern is whether a projective plane curve C has rational points. It is immediately true that

$$C(k) \neq \emptyset \implies C(k_v) \neq \emptyset, \tag{2.14}$$

for any place v of k. The contrapostive implication, therefore, says that if at any place v of k we have $C(k_v) = \emptyset$, then $C(k) = \emptyset$.

Definition 2.11. If for some place v of k we have $C(k_v) = \emptyset$, then we say that C has a *local obstruction* at v to having rational points.

There are certain varieties for which the converse of (2.14) holds:

Definition 2.12. We say that a quadratic form q *represents* 0 *in* k if there exists a nonzero $x \in k^n$ such that $q(x) = 0$,

Theorem 2.13 (Hasse–Minkowski)**.** *Let q be a quadratic form in n variables with coefficients in $\mathbb{Q}$. Then q represents 0 in $\mathbb{Q}$ if and only if it represents 0 in every completion of $\mathbb{Q}$.*

Proof. See Cohen [7, §5.3]. □

Remark 2.14. The theorem also holds true in the more general case of quadratic forms on a number field k, as Hasse showed in a series of papers in 1924 [14, 15].

Definition 2.15. We say that *the Hasse principle holds* for a certain collection $\mathscr{C}$ of varieties if for all $X \in \mathscr{C}$ we have that if $X(k_v) \neq \emptyset$ for all places v of k, then $X(k) \neq \emptyset$.

Example 2.16. It is well-known (see, for example [4, §1] and [16, Theorem A.4.3.2.]) that the Hasse principle holds for curves of genus 0.

Remark 2.17. The Hasse principle does not hold for curves of higher genus. Moreover, these higher genus curves tend to have points everywhere locally. Indeed, Poonen and Stoll estimate that roughly 87% of genus 2 hyperelliptic curves have points everywhere locally [25, §9].

The following example, due to Selmer, illustrates how the Hasse principle may fail. We paraphrase Cohen's presentation of the example [7, Corollary 6.4.12].

Example 2.18. Let C be the projective plane curve with defining equation

$$C\colon 3x^3 + 4y^3 + 5z^3 = 0. \tag{2.15}$$

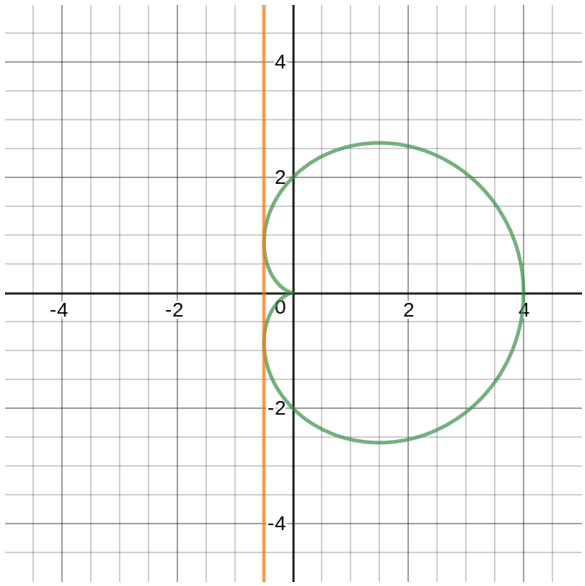

Figure 2.1: The line $x = -0.5$ is bitangent to the cardioid $(x^2 + y^2 - 2x)^2 = 4(x^2 + y^2)$ at $\left(-\frac{1}{2}, \pm\frac{\sqrt{3}}{2}\right)$.

Then $C(\mathbb{Q}_v) \neq \emptyset$ for any place v of $\mathbb{Q}$, but $C(\mathbb{Q}) = \emptyset$.

Proof. See Cohen [7, Corollary 6.4.12]. □

2.7 Bitangents, syzygetic quadruples and Aronhold sets

Let C be a projective plane curve. A *bitangent* to C is a line that is tangent to C at two points. Figure 2.1 provides a concrete example.

The language of divisors (see Hartshorne [13, II, §6]) and intersection cycles (see Fulton [11, ch. 5, §§1,5]) allows us to formalise the definition to match that in [3, §12.2]:

Definition 2.19. A *bitangent* to a quartic plane curve C is a line $l \subset \mathbb{P}^2$ such that the intersection $l \cdot C$ is $2\beta_l$ for some $\beta_l \in \operatorname{Div} C$.

In the case of plane quartic curves, we are indebted to Julius Plücker for the following classical result.

Theorem 2.20 (Plücker)**.** *Smooth plane quartic curves have precisely 28 bitangents.*

Remark 2.21. This theorem is analogous (see Geiser [12]) to that of Plücker's contemporaries Cayley and Salmon, who proved that a smooth cubic surface over an algebraically closed field contains 27 lines.

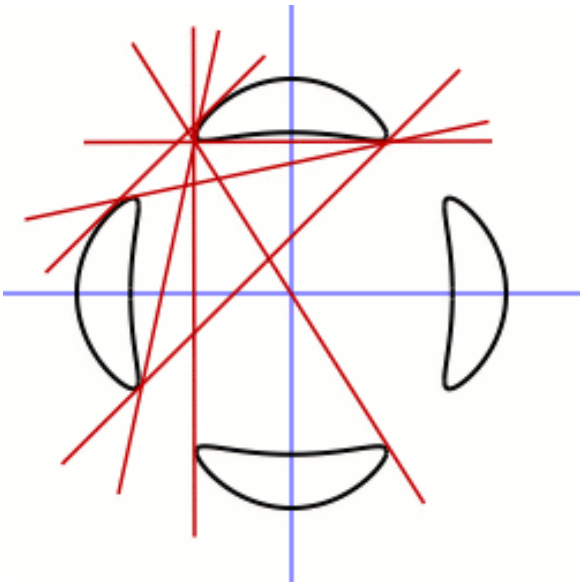

Figure 2.2: The Trott curve (2.16) is shown, together with 7 of its 28 bitangents [26]. The remaining 21 occur in precisely the same manner, with 7 bitangents emanating from each of the other 3 components.

Remark 2.22. Note that it is not necessary for the 28 bitangents to a plane quartic curve to lie in the real plane. We say a bitangent is *real* if it is defined by a linear form with real coefficients. Michael Trott (see Figure 2.2) provided a straightforward example of a plane quartic curve with all 28 bitangents real [34], namely

$$C\colon 144(x^4+y^4)-225(x^2+y^2)+350x^2y^2+81=0. \tag{2.16}$$

Bruin et al. recall the classical definition of a *syzygetic quadruple* as a set of four bitangents $\{l_1,\dots,l_4\}$ that satisfy any of three equivalent conditions [3, §12.2]. For present purposes, we only need one of these:

Definition 2.23. A four-element set $\{l_1,\dots,l_4\}$ of bitangents to C is called a *syzygetic quadruple* if there is a conic $Q\subseteq\mathbb{P}^2$ (possibly reducible) such that

$$\beta_{l_1}+\cdots+\beta_{l_4}=Q\cdot C. \tag{2.17}$$

Remark 2.24. One can show (see for example [3, §12.2] or [9, §6.2.1]) that if C is a plane quartic curve, then there are precisely 315 distinct syzygetic quadruples of bitangents. Moreover, each pair of bitangents is part of 5 syzygetic quadruples.

Definition 2.25. A *syzygetic triple* is a 3-element set formed by removing one element from a syzygetic quadruple.

Proposition 2.26. *Any syzygetic triple can be completed to a syzygetic quadruple in only one way.*

Proof. Suppose otherwise, so we have a syzygetic triple $\{\ell_1, \ell_2, \ell_3\}$ and distinct bitangents ℓ_i, ℓ_j with

$$\ell_1\ell_2\ell_3\ell_i = d_1p_1^2 + c_if,$$
$$\ell_1\ell_2\ell_3\ell_j = d_2p_2^2 + d_if,$$

where $c_i, d_i \in k^*$ and $p_i, f \in k[x, y, z]$. Then, in $k(C)$, we have

$$\frac{\ell_i}{\ell_j} = \frac{d_1p_1^2}{d_2p_2^2} = \left(\sqrt{\frac{d_1}{d_2}}\frac{p_1}{p_2}\right)^2. \tag{2.18}$$

While the left-hand expression $\frac{\ell_i}{\ell_j}$ is a degree 4 function on C, we obtain on the right-hand side the degree 2 function $\frac{p_1}{p_2}$ on C. Thus, we see that the curve C is hyperelliptic, and this is a contradiction since C is a plane quartic curve. □

Definition 2.27. If a finite set $\{l_1, \ldots, l_n\}$ of bitangents to C does not contain a syzygetic triple as a subset, we call the set *azygetic*. We call an azygetic set $\{l_1, \ldots, l_7\}$ of seven bitangents an *Aronhold set*, or *Aronhold system*.

We will refer to an Aronhold set $\{l_1, \ldots, l_7\}$ with each $l_i(x, y, z) \in \mathbb{Q}[x, y, z]$ as a *rational Aronhold system*.

2.8 Morphisms

In this section we discuss non-constant morphisms between smooth projective curves. The key result to recall from Hartshorne [13, I, Theorem 4.4] is that, for C and D smooth projective curves over k, there is a bijection

$$\{\text{non-constant morphisms } \phi\colon D \to C\} \longleftrightarrow \{k\text{-algebra homomorphisms } \phi^*\colon k(C) \to k(D)\}. \tag{2.19}$$

The *degree* of a morphism ϕ is then simply the degree of the field extension induced by the pullback ϕ^*.

If $\deg(\phi) = 1$, then ϕ is invertible and ϕ^{-1} is a non-constant morphism $C \to D$. In this case, C and D are called *birationally equivalent* (often simply *birational*), or *isomorphic* — see [29, ch.2 §3.1] as for why the terminology is interchangeable in this setting.

The following definitions are adapted from [30, §II.2, X.2].

Definition 2.28. The set of isomorphisms from C to itself over k forms a group, the *automorphism group* $\mathrm{Aut}_k(C)$ of C over k. We write $\mathrm{Aut}(C) = \mathrm{Aut}_{\overline{k}}(C)$. Suppose that $\phi\colon D \to C$ is a non-constant morphism. We write $\mathrm{Aut}(D/C)$ for the subgroup of automorphisms $\tau \in D$ such that $\phi \circ \tau = \phi$. If $\#\,\mathrm{Aut}(D/C) = \deg(\phi)$, then ϕ is called a *Galois* cover and we write $\mathrm{Gal}(D/C) = \mathrm{Aut}(D/C)$.

Definition 2.29. A curve D over k that is isomorphic to C over $\overline{k}$ by a morphism $\phi\colon D \to C$ (but not necessarily over k) is called a *twist* of C. We write $\mathrm{Twist}(C/k)$ for the set of twists of C modulo isomorphisms over k.

In order to state the Riemann–Hurwitz formula, we need first recall the definition of the ramification index $e_P(\phi)$ of a morphism $\phi\colon D \to C$ at a point $P \in D(\overline{k})$. Recall first from Fulton [11, ch. 3, §2 Theorem 1] that P is non-singular if and only if the local ring $\mathcal{O}_P(D)$ is a discrete valuation ring. More generally, a scheme (resp. variety) is *normal* if all of its local rings are integrally closed domains [13, II, §3].

Let $\phi\colon D \to C$ be a non-constant morphism of curves over k. Let $P \in D(\overline{k})$ and $Q = \phi(P) \in C(\overline{k})$. Let $t_Q \in k(C)$ be a local parameter at Q; that is, t_Q generates the maximal ideal $\mathfrak{m}_Q$ of the local ring $\mathcal{O}_Q(C) \subset k(C)$.

Definition 2.30. We define the *ramification index* $e_P(\phi)$ of ϕ at P as $e_P(\phi) = \mathrm{ord}_P(\phi^*(t_Q))$. We say ϕ is *ramified* at P if $e_P(\phi) > 1$.

Remark 2.31. If $\mathrm{char}(k) = 0$, then $\sum_{P \in \phi^{-1}(Q)} e_P(\phi) = \deg(\phi)$.

Remark 2.32. Morphisms are ramified at only finitely many points.

Theorem 2.33 (Hurwitz)**.** *Let $\phi\colon D \to C$ be a non-constant morphism of smooth curves over a field k of characteristic 0. Then*

$$2(\mathrm{genus}(D) - 1) = 2\deg(\phi)(\mathrm{genus}(C) - 1) + \sum_{P \in D(\overline{k})} (e_P(\phi) - 1). \tag{2.20}$$

2.9 The Chevalley–Weil theorem

The following theorem, due to Chevalley and Weil, is crucial to our methods. We borrow the statement as presented in [16, §C.5].

Theorem 2.34 (Chevalley–Weil)**.** *Let $\phi\colon X \to Y$ be an unramified covering of normal projective varieties defined over a number field k. Then there exists a finite extension K/k such that $\phi^{-1}(Y(k)) \subset X(K)$.*

2.10 The Hasse–Weil bound

Weil extended Hasse's bound on the number of points on an elliptic curve over a finite field to the case of curves of higher genus. The result, a corollary of his proof of the *Weil conjectures* (see [27, §V.2]) in the case of curves, is as follows:

Theorem 2.35. *Let $C/\mathbb{F}_q$ be a smooth, projective, geometrically irreducible curve of genus $g \geq 1$ defined over a finite field. Then*

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}. \tag{2.21}$$

2.11 A multidimensional Hensel's lemma

Hensel's lemma is a fundamental result in p-adic analysis. For the usual statement and proof, see for instance [17, Theorem 3]). For our purposes in Section 3.6, we shall require the following multidimensional analogue:

Theorem 2.36 (Multidimensional Hensel's lemma)**.** *Let $f(x,y) \in \mathbb{Z}_p[x,y]$, and suppose*

1. *$v_p(f(0,0)) \geq r$, for some integer $r \geq 1$, and*
2. *$v_p\left(\frac{\partial}{\partial x} f(0,0)\right) = 0$.*

Then for any $y_0 \in p^r\,\mathbb{Z}_p \pmod{p^{r+1}}$ there exists a unique $x_0 \in p^r\,\mathbb{Z}_p \pmod{p^{r+1}}$ such that $f(x_0,y_0) = 0$.

Proof. Write

$$f(x,y) = a_{00} + a_{10}x + a_{01}y + \sum_{i+j\geq 2} a_{ij}x^i y^j. \tag{2.22}$$

Our two assumptions tell us that $a_{10} \not\equiv 0 \pmod{p}$ and $v_p(a_{00}) \geq r$. Since we are specifying $f(x_0,y_0) = 0$, we can rewrite (2.22) in the form

$$x_0 = (-a_{10})^{-1}\left(a_{00} + a_{01}y_0 + \sum_{i+j\geq 2} a_{ij}x_0^i y_0^j\right). \tag{2.23}$$

Since $y_0 \in p^r\,\mathbb{Z}_p \pmod{p^{r+1}}$, we have $v_p(x_0^i y_0^j) \geq r$ when $i+j \geq 2$, and so

$$v_p\left(\sum_{i+j\geq 2} a_{ij}x_0^i y_0^j\right) \geq 2r \geq r+1. \tag{2.24}$$

Thus, we can recover x_0 uniquely, modulo p^{r+1}, as

$$x_0 = (-a_{10})^{-1} (a_{00} + a_{01} y_0) . \tag{2.25}$$

□

Corollary 2.37. *Let $f(x, y) \in \mathbb{Z}_p[x, y]$, and suppose*

1. *$v_p(f(x_0, y_0)) \geq r$, for some integer $r \geq 1$, and*
2. *$v_p\left(\frac{\partial}{\partial x} f(x_0, y_0)\right) = 0$.*

Then for any $y_1 \in y_0 + p^r \mathbb{Z}_p \pmod{p^{r+1}}$ there exists a unique $x_1 \in x_0 + p^r \mathbb{Z}_p \pmod{p^{r+1}}$ such that $f(x_1, y_1) = 0$.

Proof. Apply Theorem 2.36 to $\tilde{f}(x, y) = f(x - x_0, y - y_0)$. □

Remark 2.38. See, for instance, Eisenbud [10, §7.7] for an even more general statement.

2.12 The Jacobian variety

The definition of the Jacobian variety Jac_C of a curve C is rather involved. We only have a passing need for it, and we only require a few of its properties. In this section we give a very brief description, without proofs, of the properties we need. See Milne [20], for instance, for a fuller description.

Fix an algebraic extension field L of k, so $k \subseteq L \subseteq \overline{k}$. We characterise the Jacobian as a dimension $g = \mathrm{genus}(C)$ *abelian variety* over k such that

$$\mathrm{Jac}_C(L) \cong \mathrm{Pic}^0(C/\overline{k})^{\mathrm{Gal}(\overline{k}/L)}. \tag{2.26}$$

We should, therefore, explain briefly what an abelian variety is.

Definition 2.39. [20, §1] A *group variety* over k is a variety V over k together with morphisms

$$\begin{aligned} m &\colon V \times V \to V, \\ \mathrm{inv} &\colon V \to V, \end{aligned}$$

and an element $\epsilon \in V(k)$ such that the structure on $V(\overline{k})$ defined by m and inv is that of a group with identity element ϵ. A complete group variety (see [13, II.4]) is called an *abelian variety*.

Chapter 3

Two-cover descent

In this chapter we introduce *two-cover descent*. This is a procedure that in many cases allows one to prove that a curve has no rational points. The method is described for hyperelliptic curves in [4] and [5], and in [3] for non-hyperelliptic genus 3 curves: the case of interest to us. For technical details, we refer to [3].

3.1 Setup

Let C be a smooth projective plane curve with defining equation

$$C\colon f(x,y,z)=0,$$

for some homogeneous degree 4 polynomial $f \in \mathbb{Z}[x,y,z]$, together with equations $\ell_1,\dots,\ell_7 \in \mathbb{Z}[x,y,z]$ defining an Aronhold set of bitangents (see Definition 2.27). In the following description, we may take $k=\mathbb{Q}$, $\mathbb{Q}_p$ or $\mathbb{R}$ — all fields of characteristic zero.

We define a partial map

$$\begin{aligned}\delta\colon C(k) &\dashrightarrow \left(k^*/k^{*2}\right)^6\\ P &\mapsto \left(\frac{\ell_1(P)}{\ell_7(P)},\dots,\frac{\ell_6(P)}{\ell_7(P)}\right).\end{aligned} \tag{3.1}$$

The description given here is valid only for points $P \in C(k)$ for which $\ell_i(P) \neq 0$ for all $i \in \{1,\dots,7\}$. This is why δ is only, for now, a *partial* map. We will see in the next section how the existence of syzygetic quadruples allows one to extend the domain of definition of δ to all of $C(k)$.

In fact, for each place $v \in k$, we have the following commutative diagram, which is fundamental to the two-cover descent method.

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\delta} & \left(\mathbb{Q}^* \,/\, \mathbb{Q}^{*2}\right)^6 \\ \Big\downarrow & & \Big\downarrow{\scriptstyle \rho_v} \\ C(\mathbb{Q}_v) & \xrightarrow{\delta_v} & \left(\mathbb{Q}_v^* \,/\, \mathbb{Q}_v^{*2}\right)^6. \end{array} \tag{3.2}$$

The vertical maps arise from the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$.

3.2 Using the syzygetic relations

In order to extend the partial map given in (3.1) to a well-defined map on all of $C(k)$, we need a way of evaluating the map at points $P \in C(k)$ for which some bitangent from the Aronhold set vanishes: $\ell_\alpha(P) = 0$, with $\alpha \in \{1, \ldots, 7\}$. Fortunately, the syzygetic quadruples we introduced in Section 2.7 provide precisely such a tool.

Suppose $\ell_\alpha(P) = 0$. As we saw in Section 2.7, there are 315 syzygetic quadruples, and necessarily the bitangent ℓ_α features in 45 of these.

In what follows, we refer to such a quadruple as $\{\ell_\alpha, \ell_i, \ell_j, \ell_k\}$, and assume further that $\ell_i(P) \neq 0$, $\ell_j(P) \neq 0$ and $\ell_k(P) \neq 0$. We can always find such a quadruple, for $\ell_\alpha(P) = 0 \implies \ell_i(P) \neq 0$ for all $i \neq \alpha$ (else the point P would be a contact point of two distinct bitangents, forcing P to be singular).

Since this quadruple is syzygetic, on $k[x, y, z]/(f)$ we have the congruence

$$\ell_\alpha \ell_i \ell_j \ell_k \equiv dc^2 \pmod{f}, \tag{3.3}$$

for some $d \in k^*$ and $c \in k[x, y, z]$. Thus, working modulo squares, we can recover

$$\ell_\alpha \equiv d\ell_i \ell_j \ell_k \pmod{\square}. \tag{3.4}$$

Therefore, we replace $\ell_\alpha(P) = 0$ with

$$\tilde{\ell}_\alpha(P) \equiv \begin{cases} \ell_\alpha(P) \pmod{\square}, & \text{if } \ell_\alpha(P) \neq 0, \\ d\ell_i(P)\ell_j(P)\ell_k(P) \pmod{\square}, & \text{if } \ell_\alpha(P) = 0. \end{cases} \tag{3.5}$$

3.3 Explicit description

Next we explicitly describe a family of two-covers $D_{\underline{\delta}}$ to our curve C. While we shall not use this model explicitly in our computations, it helps for the theoretical understanding of the procedure and for the correctness proof of our method. We follow closely the approach in [5, §3], defining our two-covers in the same way, but providing commentary.

We consider smooth plane quartics, and we write the projective model as

$$C\colon f(x,y,z) = \sum_{i+j+k=4} a_{ijk} x^i y^j z^k = 0, \tag{3.6}$$

with coefficients $a_{ijk} \in k$.

Definition 3.1. A *two-cover* is a non-singular absolutely irreducible cover D of C such that

- D/C is unramified and Galois over $\overline{k}$,
- $\mathrm{Aut}_{\overline{k}}(D/C) \cong (\mathbb{Z}/2\mathbb{Z})^6$ (where here the exponent of six arises as $2g = 2 \times 3 = 6$).

Remark 3.2. By a cover D of C, we mean there is a non-constant morphism $\phi\colon D \to C$, but our notation suppresses the covering map ϕ. Moreover, the condition that the cover be *absolutely irreducible* means that D is irreducible over $\overline{k}$.

We construct a two-cover of C as follows, working in the affine patch $\mathbb{A}^2_2$ given by specialising $z = 1$. First, precisely as in (3.3), for each $i \in \{1,\dots,6\}$ we augment the pair ℓ_i, ℓ_7 with two more bitangents ℓ_j, ℓ_k, say, to form a syzygetic quadruple, so on $k[x,y,z]/(f)$ we have

$$\ell_i \ell_j \ell_k \ell_7 \equiv d_i c_i^2 \pmod{f}, \tag{3.7}$$

with $d_i \in k^*$ and $c_i \in k[x,y,z]$. This enables us to define, for each $i \in \{1,\dots,6\}$, a smooth projective curve D_{δ_i}, where $\delta_i \in k^*$ is a representative of a class modulo squares, with affine model

$$D_{\delta_i}\colon \begin{cases} \delta_i \ell_i(x,y,1) \cdot \ell_7(x,y,1) = u_i^2 \\ \ell_j(x,y,1) \cdot \ell_k(x,y,1) = d_i \delta_i v_i^2, \\ u_i v_i = c_i(x,y,1), \\ f(x,y,1) = 0, \end{cases} \tag{3.8}$$

together with maps

$$\begin{aligned} \pi_i\colon D_{\delta_i} &\to C \\ (x,y,u_i,v_i) &\mapsto (x:y:1). \end{aligned} \tag{3.9}$$

Theorem 3.3. *Each covering curve D_{δ_i} is an unramified, degree 2 cover of C.*

In order to prove Theorem 3.3, we will require the following lemma:

Lemma 3.4. *Suppose $D \to C$ is a degree 2 morphism of smooth curves and that $k(D) = k(C)(\sqrt{g})$ for some nonzero $g \in k(C)$. If $Q \in C(k)$ and $\mathrm{ord}_Q(g)$ is even, then D/C is unramified over Q.*

Also, note that the property of a morphism being unramified is stable under base extension [31, Lemma 02GA], so we may pass to the algebraic closure: $D \to C$ is unramified if and only if $D(\overline{k}) \to C(\overline{k})$ is unramified. Let $P \in D$ and $Q \in C$ with $\pi(P) = Q$. Then the pullback $\pi^* \colon k(C) \to k(D)$ induces an injection of local rings

$$\mathcal{O}_{C,Q} \subset \mathcal{O}_{D,P}, \tag{3.10}$$

and, taking completions,

$$\hat{\mathcal{O}}_{C,Q} \subset \hat{\mathcal{O}}_{D,P}. \tag{3.11}$$

Since C is smooth, we may realise $\hat{\mathcal{O}}_{C,Q} \cong \overline{k}((T))$ as the formal Laurent series in a uniformiser T at Q (see [29, ch. 2, §2.2]).

Proof of Lemma 3.4. Write $\mathrm{ord}_Q\, g = 2m$, for $m \in \mathbb{Z}$. Then

$$\sqrt{g} = T^m \sqrt{c_{2m} + c_{2m+1}T + c_{2m+2}T^2 + \dots} \tag{3.12}$$

$$= T^m \sqrt{c_{2m}} \sqrt{1 + \frac{c_{2m+1}}{c_{2m}}T + \frac{c_{2m+2}}{c_{2m}}T^2 + \dots}, \tag{3.13}$$

with $c_{2m} \neq 0$.

In each case, we take a square root of a Laurent series with constant term 1, and such a series is a perfect square in $\overline{k}((T))$. Thus, we see that $g \in \overline{k}((T)) \cong \hat{\mathcal{O}}_{C,Q}$ and so $\hat{\mathcal{O}}_{C,Q} \cong \hat{\mathcal{O}}_{D,P}$. Thus for any uniformiser T at Q, the ramification index

$$e_P(\pi) = \mathrm{ord}_P(\pi^* T) = 1, \tag{3.14}$$

and so the cover is unramified. □

Proof of Theorem 3.3. To reduce the number of subscripts, we write $D = D_{\delta_i}$ and $\pi = \pi_{\delta_i}$.

The cover $\pi\colon D \to C$ induces a morphism of function fields

$$\begin{aligned} \pi^*\colon \overline{k}(C) \to \overline{k}(D) \cong \overline{k}(C)\left(\sqrt{\frac{\delta_i \ell_i}{\ell_7}}\right) \\ g \mapsto g \circ \pi. \end{aligned} \tag{3.15}$$

Consider an arbitrary point $Q = [X : Y : 1] \in C(\overline{k})$. Then, looking at (3.8), only the first equation provides any new information: combined with the third equation, we recover the second equation. The coordinate u_i is a root of a univariate quadratic polynomial over $\overline{k}$, for a maximum of 2 possibilities. The third equation then specifies v_i uniquely. Thus the degree of the cover is 2.

Now, since ℓ_i and ℓ_7 are bitangents, we have

$$\operatorname{ord}_Q \sqrt{\frac{\ell_i}{\ell_7}} \in \{-4, -2, 0, 2, 4\}. \tag{3.16}$$

Thus, we may apply Lemma 3.4 to complete the proof. □

Now, as we did in (3.8), we define, for each $\underline{\delta} = (\delta_1, \ldots, \delta_6) \in (k^*)^6$, a smooth projective curve $D_{\underline{\delta}}$ with affine model

$$D_{\underline{\delta}}\colon \begin{cases} \delta_i \ell_i(x, y, 1) \cdot \ell_7(x, y, 1) = u_i^2, & i \in \{1, \ldots, 6\}, \\ \ell_j(x, y, 1) \cdot \ell_k(x, y, 1) = d_i \delta_i v_i^2, & i \in \{1, \ldots, 6\}, \\ u_i v_i = c_i(x, y, 1), & i \in \{1, \ldots, 6\}, \\ f(x, y, 1) = 0. \end{cases} \tag{3.17}$$

Proposition 3.5. *$D_{\underline{\delta}}/C$ is a two-cover.*

Proof. The extension

$$k(D_{\underline{\delta}}) = k(C)\left(\sqrt{\frac{\delta_1 \ell_1}{\ell_7}}, \ldots, \sqrt{\frac{\delta_6 \ell_6}{\ell_7}}\right) \tag{3.18}$$

is a compositum of unramified quadratic extensions (by Lemma 3.4), and therefore is also unramified. Furthermore, the six automorphisms $\sigma_j\colon D_{\underline{\delta}} \to D_{\underline{\delta}}$ given by $\sigma_j^*(u_j) = -u_j$ and $\sigma_j^*(u_i) = u_i$ for $i \neq j$ generate a group in $\operatorname{Aut}_{\overline{k}}(D_{\underline{\delta}}/C)$ that is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^6$. Last, we require that $D_{\underline{\delta}}$ is absolutely irreducible. That is, we are to show that (3.18) is a field extension of degree 64 over $\overline{k}$. So we need to show that the square roots in (3.18) are independent. Since the bitangents $\ell_1, \ldots, \ell_7$ form an Aronhold set, there are no syzygetic

triples among them. We use the result in [3, Corollary 5.3(a)] that every class in $\mathrm{Jac}_C[2]$ can be written as a difference of contact points of bitangents. We see that the syzygetic quadruples generate the relations modulo squares, and so the absence of syzygetic triples forces the square roots to be independent. □

Proposition 3.6. *The $D_{\underline{\delta}}/C$ are twists of one another.*

Proof. It is straightforward to check that the isomorphism class of $D_{\underline{\delta}}$ as a cover of C only depends on the square classes of the δ_i. Therefore, if we write $\underline{1} = (1,1,1,1,1,1)$, then we see that over $k(\sqrt{\delta_1}, \ldots, \sqrt{\delta_6})$ we have that $D_{\underline{\delta}}$ is isomorphic to $D_{\underline{1}}$. It follows that over $\overline{k}$, all $D_{\underline{\delta}}$ are isomorphic. □

So now we have a collection of twists $D_{\underline{\delta}}/C$. If it is true that any rational point on C has a rational preimage on one of the covers $D_{\underline{\delta}}$, then we call such a set of covers a *covering collection*. This motivates us to prove the following result:

Proposition 3.7. *The $D_{\underline{\delta}}$ form a covering collection.*

Proof. Suppose the curve C has a k-rational point $P \in C(k)$. If we let $P = (x, y, 1)$ and $\underline{\delta}(P) = (\delta_1(P), \ldots, \delta_6(P)) = \left(\frac{\tilde{\ell}_1(P)}{\tilde{\ell}_7(P)}, \ldots, \frac{\tilde{\ell}_6(P)}{\tilde{\ell}_7(P)}\right)$, then we can rearrange the equations (3.17) defining $D_{\underline{\delta}}$ to solve for u_i and v_i for each $i \in \{1, \ldots, 6\}$. Note that $u_i = 0$ will occur if $\ell_i = 0$ or $\ell_7 = 0$, and $v_i = 0$ is possible otherwise. We conclude that $P \in C(k)$ has a k-rational preimage on $D_{\underline{\delta}(P)}$. □

Remark 3.8. Now we have a covering collection $D_{\underline{\delta}}$ over k. Applying the Chevalley–Weil theorem, we see that the $D_{\underline{\delta}}$ are all isomorphic over a finite extension field K/k. We may therefore conclude that there are only finitely many $D_{\underline{\delta}}$ in our covering collection. We spell out this argument explicitly below.

We define $\mathrm{Cov}^{(2)}(C/k)$ as the covering collection $D_{\underline{\delta}}$.

Remark 3.9. Geometric class field theory (see Serre [28, §2]) gives that over $\overline{k}$, there is only one isomorphism class of two-covers for a given curve C. It follows that we can view $\mathrm{Cov}^{(2)}(C/k)$ as the set of isomorphism classes of two-covers of C over k.

Lemma 3.10. *Suppose that $D_{\underline{\delta}^{(1)}}$ and $D_{\underline{\delta}^{(2)}}$ both have a rational point above the same point $P \in C(k)$. Then $D_{\underline{\delta}^{(1)}}$ and $D_{\underline{\delta}^{(2)}}$ are isomorphic.*

Proof. Say $Q_1 \in D_{\underline{\delta}^{(1)}}(k)$ and $Q_2 \in D_{\underline{\delta}^{(2)}}(k)$ with $\pi_{\underline{\delta}^{(1)}}(Q_1) = \pi_{\underline{\delta}^{(2)}}(Q_2) = P = (x, y, 1) \in C(k)$. From the defining equations (3.17) of the $D_{\underline{\delta}^{(\alpha)}}$, we see that for $i \in \{1, \ldots, 6\}$ we have

$$\begin{aligned} \delta_i^{(1)} \ell_i(x, y, 1) \cdot \ell_7(x, y, 1) &= (u_i^{(1)})^2, \\ \delta_i^{(2)} \ell_i(x, y, 1) \cdot \ell_7(x, y, 1) &= (u_i^{(2)})^2. \end{aligned} \tag{3.19}$$

So, working modulo squares, we see that

$$\delta_i^{(1)} \equiv \ell_i(x, y, 1) \cdot \ell_7(x, y, 1) \equiv \delta_i^{(2)} \pmod{\square}, \tag{3.20}$$

and so the result follows. □

Remark 3.11. Lemma 3.10 implies that the map $\delta\colon C(k) \to (k^*/k^{*2})^6$ can be interpreted as a map $C(k) \to \mathrm{Cov}^{(2)}(C/k)$, sending $P \in C(k)$ to the unique two-cover of the form $D_{\underline{\delta}}$ that has a rational preimage above P.

The next definition and proposition will play an important part in our method.

Definition 3.12. The *(two-)Selmer set* $\mathrm{Sel}^{(2)}(C/k) \subset \mathrm{Cov}^{(2)}(C/k)$ is the set of isomorphism classes of everywhere locally solvable two-covers of C:

$$\mathrm{Sel}^{(2)}(C/k) = \left\{ (\phi\colon D \to C) \in \mathrm{Cov}^{(2)}(C/k)\colon D(k_v) \neq \emptyset \text{ for all places } v \text{ of } k \right\}. \tag{3.21}$$

Proposition 3.13. *If* $\mathrm{Sel}^{(2)}(C/k) = \emptyset$*, then* $C(k) = \emptyset$*.*

Proof. Suppose $\mathrm{Sel}^{(2)}(C/k) = \emptyset$ but $P \in C(k)$. By Remark 3.11, we have a map $C(k) \to \mathrm{Cov}^{(2)}(C/k)$, sending $P \in C(k)$ to the two-cover, ϕ say, that has a rational preimage above P. Then $\phi \in \mathrm{Sel}^{(2)}(C/k)$, so the Selmer set is non-empty. This contradiction completes the proof. □

The following results allow us to pinpoint precisely which $\underline{\delta}$ we are to include to make up a finite covering collection. Let S be the set of primes containing 2 and the primes of bad reduction for the curve C. Then

$$\mathbb{Z}_S = \mathbb{Z}\left[\frac{1}{\prod_{p \in S} p}\right], \tag{3.22}$$

and, writing $s = \#S$,

$$\mathbb{Z}_S^* \,/\, \mathbb{Z}_S^{*2} = \langle -1, p_1, \ldots, p_s \rangle \cong \mu_2^{s+1}, \tag{3.23}$$

where $\mu_2 = \{\pm 1\}$ denotes the second roots of unity. Note that, as abelian groups, we have $\mu_2 \cong \mathbb{F}_2$.

Lemma 3.14. *We have*

$$\mathbb{Z}_S^* / \mathbb{Z}_S^{*2} = \{\overline{\alpha} \in \mathbb{Q}^* / \mathbb{Q}^{*2} : v_p(\overline{\alpha}) \equiv 0 \pmod 2 \text{ for all } p \notin S\}. \tag{3.24}$$

Proof. Let $\overline{\alpha} \in \{\overline{\alpha} \in \mathbb{Q}^* / \mathbb{Q}^{*2} : v_p(\overline{\alpha}) \equiv 0 \pmod 2 \text{ for all } p \notin S\}$. By the unique factorisation of integers, write $\alpha = \pm q_1^{e_1} \dots q_r^{e_r}$ with $q_i \in \mathbb{Z}$ prime and $e_i \in \mathbb{Z}$. Then

$$\begin{aligned} q_i \notin S &\iff e_i \equiv 0 \pmod 2 \\ &\iff \alpha \equiv \pm p_1^{f_1} \dots p_s^{f_s} \pmod \square, \text{ with } f_i \in \{0,1\} \\ &\iff \overline{\alpha} \in \mathbb{Z}_S^* / \mathbb{Z}_S^{*2}. \end{aligned}$$

□

Theorem 3.15. *Suppose that $f \in \mathbb{Z}_p[x,y,z]$, where p is an odd prime that does not divide $I_{27}(f)$. Let $C\colon f(x,y,z) = 0$ be the smooth plane quartic curve defined by f, and suppose that $\ell_1, \dots, \ell_7$ is an Aronhold system of bitangents defined over $\mathbb{Q}$. If $P \in C(\mathbb{Q}_p)$, then all components of $\delta(P)$ have even valuation at p.*

Proof. Let ℓ_j, ℓ_k be a pair of bitangents such that $\ell_i, \ell_j, \ell_k, \ell_7$ form a syzygetic quadruple, for some $1 \leq i \leq 6$. This means that restricted to C, we have $\ell_i \ell_j \ell_k \ell_7 = d_i c_i(x,y,z)^2$, for some $d_i \in \mathbb{Q}_p^*$ and $c_i \in \mathbb{Q}_p[x,y,z]$. Our assumptions imply that C has good reduction at p, so the 28 bitangents of C must reduce to distinct bitangents over $\mathbb{F}_p$ as well, and their contact points are distinct. In particular, we have that $v_p(d_i) = 0$. It follows that the parities of $v_p(\ell_i(P)/\ell_7(P))$ and $v_p(\ell_j(P)/\ell_k(P))$ agree. Furthermore, we have that the reduction of P can be a contact point of at most one bitangent modulo p, so at most one of these valuations is nonzero. It follows that $\delta(P)$ has only even valuation components. □

Remark 3.16. We will need the special case of the theorem with $f \in \mathbb{Z}[x,y,z]$ and $P \in C(\mathbb{Q})$.

Corollary 3.17. *If S is the set of primes containing 2 and the primes of bad reduction, then $\{D_{\underline{\delta}} : \underline{\delta} \in (\mathbb{Z}_S^* / \mathbb{Z}_S^{*2})^6\}$ is a finite covering collection for C over $\mathbb{Q}$.*

Proof. Suppose a prime $p \notin S$. Then p is an odd prime that does not divide $I_{27}(f)$. So, by Remark 3.16, if $P \in C(\mathbb{Q})$, then all components of $\delta(P)$ have even valuation at p. Thus we can conclude by Lemma 3.14 that each of these components is an element of $\mathbb{Z}_S^* / \mathbb{Z}_S^{*2}$. □

To prove that the Selmer set (defined in (3.21)) is finite, we require the following lemma:

Lemma 3.18. *Suppose $\underline{\delta} = (\delta_1, \dots, \delta_6) \in (k^*)^6$ has a component of odd valuation at a prime p of good reduction. Then $D_{\underline{\delta}}(\mathbb{Q}_p) = \emptyset$.*

Proof. Suppose there exists a $\mathbb{Q}_p$-rational point $Q \in D_{\underline{\delta}}(\mathbb{Q}_p)$. Then Q lies above a $\mathbb{Q}_p$-rational point $P \in C(\mathbb{Q}_p)$. But then Theorem 3.15 implies that all components of $\delta(P)$ have even valuation at p, contradicting our hypothesis. □

Theorem 3.19. *The two-Selmer set* $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$ *is finite.*

Proof. We saw in Remark 3.11 that we can identify two-covers $\phi \in \mathrm{Cov}^{(2)}(C/\mathbb{Q})$ with vectors $\underline{\delta} = (\delta_1, \dots \delta_6) \in (\mathbb{Q}^* / \mathbb{Q}^{*2})^6$. We need to show that only finitely many of these two-covers are everywhere locally solvable. To do so, we show that the 2-Selmer set $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$, which we now view as a subset of $(\mathbb{Q}^* / \mathbb{Q}^{*2})^6$, lies in the finite set $(\mathbb{Z}_S^* / \mathbb{Z}_S^{*2})^6$.

Identify $\phi \in \mathrm{Sel}^{(2)}(C/\mathbb{Q})$ with $\underline{\delta} \in (\mathbb{Q}^* / \mathbb{Q}^{*2})^6$. Since $\phi \in \mathrm{Sel}^{(2)}(C/\mathbb{Q})$, we have $D_{\underline{\delta}}(\mathbb{Q}_v) \neq \emptyset$ for all places v of $\mathbb{Q}$. Then Lemma 3.18 implies that all components of $\underline{\delta}$ must have even valuation at primes of good reduction for C. So, for all $i \in \{1, \dots, 6\}$, we have $v_p(\delta_i) \equiv 0 \pmod 2$ for each $p \notin S$. Thus, by Lemma 3.14, each $\delta_i \in \mathbb{Z}_S^* / \mathbb{Z}_S^{*2}$, and the result follows. □

We saw in Proposition 3.5 that the compositum $\overline{k}(C)\left(\sqrt{\frac{\delta_1 \ell_1}{\ell_7}}, \dots, \sqrt{\frac{\delta_6 \ell_6}{\ell_7}}\right)$ is unramified and of degree $2^6 = 64$. So the Riemann–Hurwitz formula (2.20) gives

$$\mathrm{genus}(D_{\underline{\delta}}) = 64(3-1) + 1 = 129. \tag{3.25}$$

Let p be a prime of good reduction for C, so $p \nmid I_{27}(f)$. We have a reduction map

$$D_{\underline{\delta}}(\mathbb{Q}_p) \to \tilde{D}_{\underline{\delta}}^{(p)}(\mathbb{F}_p), \tag{3.26}$$

where $\tilde{D}_{\underline{\delta}}^{(p)}(\mathbb{F}_p)$ is the reduction (introduced in Section 2.5). Now we reduce each of the equations (3.17) defining $D_{\underline{\delta}}$ modulo p, and argue precisely as in the proof of Theorem 3.15. So, if all components of $\underline{\delta}$ have even valuation at p, then we can conclude that all points in $D_{\underline{\delta}}(\mathbb{Q}_p)$ reduce to non-singular points. It follows that $\tilde{D}_{\underline{\delta}}^{(p)}(\mathbb{F}_p)$ has only non-singular points. So by Hensel lifting, any point in $\tilde{D}_{\underline{\delta}}^{(p)}(\mathbb{F}_p)$ lifts to a point in $D_{\underline{\delta}}(\mathbb{Q}_p)$.

The above observation allows us to prove the following proposition.

Proposition 3.20. *If p is a good prime satisfying*

$$\sqrt{p} + \frac{1}{\sqrt{p}} > 258 = 2 \times \mathrm{genus}(D_{\underline{\delta}}), \tag{3.27}$$

and $\underline{\delta}$ has components of even valuation at p, then $D_{\underline{\delta}}(\mathbb{Q}_p) \neq \emptyset$.

Proof. The Hasse–Weil bound (2.21) for the number of points on a non-singular curve over a finite field of cardinality q implies that if q satisfies the inequality (3.27) with q in place of p, then the reduction $\tilde{D}_{\underline{\delta}}^{(q)}(\mathbb{F}_q)$ has a non-singular point. So if p is a good prime satisfying (3.27), then $\tilde{D}_{\underline{\delta}}^{(p)}(\mathbb{F}_p)$ has a non-singular point. Since this point lifts to a point in $D_{\underline{\delta}}(\mathbb{Q}_p)$, we see then that $D_{\underline{\delta}}(\mathbb{Q}_p) \neq \emptyset$. □

It follows that we can only have $D_{\underline{\delta}}(\mathbb{Q}_p) = \emptyset$ for primes p of bad reduction — of which there are only finitely many — or for primes satisfying $p < 258^2 = 66564$. For any particular p, testing whether $D_{\underline{\delta}}(\mathbb{Q}_p)$ is empty can be decided in finite time (see Bruin [2, §5] for the relevant algorithms). Therefore, for each $D_{\underline{\delta}}$ it is a finite computation to check whether $D_{\underline{\delta}}$ has points everywhere locally, and hence whether $\underline{\delta} \in \mathrm{Sel}^{(2)}(C/\mathbb{Q})$. By Corollary 3.17, we know that we only have to consider the finitely many candidates $\underline{\delta} \in (\mathbb{Z}_S^* / \mathbb{Z}_S^{*2})^6$.

We saw that if $p > 66564 = 258^2$, then $\#D_{\underline{\delta}}^{(p)}(\mathbb{F}_p) > 0$, and so we conclude that $\underline{\delta}$ lies in the local image $\delta_p(C(\mathbb{Q}_p))$. Thus, for good primes larger than 66553, we see — with no computation necessary — that the local image consists of all the unramified $\underline{\delta}$. Moreover, for any prime $p \leq 66553$, including the good primes, it is in principle possible that the local image provides non-trivial information; that is, consists of fewer than all of the unramified elements.

3.4 Practical considerations for avoiding combinatorial explosion

With Proposition 3.7, we have an explicit covering collection for smooth plane quartics over $\mathbb{Q}$ with a rational Aronhold system. With the procedures in Sections 5.4 and 5.5, we show that the local image $\delta_v(C(\mathbb{Q}_v))$ can be computed in finite time for any place v. Furthermore, from Theorem 2.35, we see that for finite places v of residue characteristic larger than 66564 where C has good reduction, the local image consists of the full unramified part. That gives us, at least in theory, a procedure to compute $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$:

Let S be the set of primes containing 2 and the primes of bad reduction. Let T be the set of S together with all the primes below 66564. To determine $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$, we can enumerate all $\delta \in (\mathbb{Z}_S^* / \mathbb{Z}_S^{*2})^6$ and check if $\rho_v(\delta) \in \delta_v(C(\mathbb{Q}_v))$ for all $v \in T$, where ρ_v is as defined in (3.2).

This procedure has the severe practical problem that the set $(\mathbb{Z}_S^* / \mathbb{Z}_S^{*2})^6$ is usually too large to enumerate completely. We need a way to identify a subset that is small enough to enumerate. In this section we discuss how to do this. We use that $(\mathbb{Z}_S^* / \mathbb{Z}_S^{*2})^6$ can be considered as an $\mathbb{F}_2$-vector space. Instead of working with the images $\delta_v(C(\mathbb{Q}_v))$ as sets, we

consider the $\mathbb{F}_2$-vector spaces they generate, and determine the $\mathbb{F}_2$-vector space of $(\mathbb{Z}_S^* / \mathbb{Z}_S^{*2})^6$ that is the intersection of the inverse images under ρ_v. As an added benefit, we find that the $\mathbb{F}_2$-vector space spanned by $\delta_v(C(\mathbb{Q}_v))$ is often easier to determine than the set itself.

In (3.1) we defined a map $\delta_v \colon C(\mathbb{Q}_v) \dashrightarrow (\mathbb{Q}_v / \mathbb{Q}_v^{*2})^6$, and we saw in Section 3.2 how to extend this to a map on all of $C(\mathbb{Q}_v)$. We can, in fact, extend the map δ_v to $\mathrm{Div}(C/\mathbb{Q}_v)$ by linearity. The idea is as follows. For a divisor $D = \sum n_P P$, we define $\delta_v(D) = \prod_P \delta_v(P)^{n_P}$. Not all divisors defined over $\mathbb{Q}_v$ can be represented as a sum of points on C defined over $\mathbb{Q}_v$, but [3, §6.2.2] explains how, by taking norms in appropriate ways, we can deal with this appropriately. This yields a group homomorphism

$$\delta_v \colon \mathrm{Div}(C/\mathbb{Q}_v) \to (\mathbb{Q}_v^* / \mathbb{Q}_v^{*2})^6. \tag{3.28}$$

Furthermore, [3, Prop. 6.4] shows that this map (denoted there by $\tilde{C}$) is trivial on principal divisors, so we obtain a homomorphism

$$\delta_v \colon \mathrm{Pic}(C/\mathbb{Q}_v) \to (\mathbb{Q}_v^* / \mathbb{Q}_v^{*2})^6. \tag{3.29}$$

Because we assume that $C(\mathbb{Q}_v)$ is non-empty, we can identify $\mathrm{Jac}_C(\mathbb{Q}_v)$ with $\mathrm{Pic}^0(C/\mathbb{Q}_v) \subset \mathrm{Pic}(C/\mathbb{Q}_v)$ and restrict δ_v.

Fact 3.21. The resulting map

$$\delta_v \colon \mathrm{Jac}_C(\mathbb{Q}_v) \to (\mathbb{Q}_v / \mathbb{Q}_v^{*2})^6, \tag{3.30}$$

is a group homomorphism, with kernel $2\,\mathrm{Jac}_C(\mathbb{Q}_v)$.

Remark 3.22. Technically, we should still be referring to $\delta_v \colon \mathrm{Jac}_C(\mathbb{Q}_v) \to (\mathbb{Q}_v / \mathbb{Q}_v^{*2})^6$ as a partial map, as it is only defined for those divisor classes that can be represented by divisors over $\mathbb{Q}_v$. However, if $C(\mathbb{Q}_v) \neq \emptyset$ then this is true for all divisor classes, while if $C(\mathbb{Q}_v) = \emptyset$ then we need not consider the map δ_v at all.

Observe now that we know precisely the size of the local image $\delta_v(\mathrm{Jac}_C(\mathbb{Q}_v))$:

Proposition 3.23. *The local image $\delta_v(\mathrm{Jac}_C(\mathbb{Q}_v))$ forms a subspace of $(\mathbb{Q}_v^* / \mathbb{Q}_v^{*2})^6$ with*

$$\dim_{\mathbb{F}_2} \delta_v(\mathrm{Jac}_C(\mathbb{Q}_v)) = \dim_{\mathbb{F}_2} \mathrm{Jac}_C[2](\mathbb{Q}_v) + 3 \log_2 |2|_v. \tag{3.31}$$

Proof. This is a restatement of [24, Lemma 12.10] with $k = \mathbb{Q}$ and $p = 2$ (in their paper they consider curves with defining equations of the form $y^p = f(x)$). □

For a point $P_0 \in C(\mathbb{Q}_v)$ we fix an Abel-Jacobi map $u\colon C(\mathbb{Q}_v) \to \mathrm{Jac}_C(\mathbb{Q}_v)$ given by $Q \mapsto [Q - P_0]$. It now follows we get a commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}_v) & \xrightarrow{\delta_v} & (\mathbb{Q}_v \,/\, \mathbb{Q}_v^{*2})^6 \\ \big\downarrow{\scriptstyle u} & & \big\downarrow{\scriptstyle u'} \\ \mathrm{Jac}_C(\mathbb{Q}_v) & \xrightarrow{\delta_v} & (\mathbb{Q}_v \,/\, \mathbb{Q}_v^{*2})^6, \end{array} \tag{3.32}$$

where u' is translation over $\delta_v(P_0)$.

It follows that $\delta_v(C(\mathbb{Q}_v)) \subset \delta_v(P_0) + \delta_v(\mathrm{Jac}_C(\mathbb{Q}_v))$. Therefore, we see that the $\mathbb{F}_2$-vector space spanned by $\delta_v(C(\mathbb{Q}_v))$ lies in the vector space spanned by $\delta_v(P_0)$ and $\delta_v(\mathrm{Jac}_C(\mathbb{Q}_v))$.

Since we know the size of $\delta_v(\mathrm{Jac}_C(\mathbb{Q}_v))$, it can often be determined without an exhaustive search. For instance, if we can find a finite set of points $\{P_0, P_1, \ldots, P_m\} \subset \mathrm{Jac}_C(\mathbb{Q}_v)$ such that

$$\langle \delta_v(P_i)\delta_v(P_0) : i = 1, \ldots, m \rangle$$

has the expected dimension, then this span equals $\mathrm{Jac}_C(\mathbb{Q}_v)$. In practice, one finds that often the set of contact points of the bitangents that happen to be $\mathbb{Q}_v$-valued points has this property.

Write $W_v = \delta_v(C(\mathbb{Q}_v))$. A key observation is that

$$\mathrm{Sel}^{(2)}(C/\,\mathbb{Q}) = \bigcap_{v \in S} \rho_v^{-1}(W_v) \subset \bigcap_{v \in S} \langle \rho_v^{-1}(W_v) \rangle = \bigcap_{v \in S} \rho_v^{-1} \langle W_v \rangle. \tag{3.33}$$

where the intersections are taken over all places $v \in S$, including the infinite place. In particular,

$$\mathrm{Sel}^{(2)}(C/\,\mathbb{Q}) \subset \bigcap_{v \in S} \rho_v^{-1} \langle W_v \rangle. \tag{3.34}$$

While $\rho_v^{-1}\langle W_v \rangle$ is not finite-dimensional, we can reduce the problem to a finite one with the observation that the Selmer set is supported on S-units, as we saw in the proof of Theorem 3.19, so we can refine (3.2) to

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\delta} & \left(\mathbb{Z}_S^* \,/\, \mathbb{Z}_S^{*2}\right)^6 \\ \big\downarrow & & \big\downarrow{\scriptstyle \rho_v} \\ C(\mathbb{Q}_v) & \xrightarrow{\delta_v} & \left(\mathbb{Q}_v^* \,/\, \mathbb{Q}_v^{*2}\right)^6. \end{array} \tag{3.35}$$

Now

$$\mathrm{Sel}^{(2)}(C/\mathbb{Q}) \subset \bigcap_{v\in S} \rho_v^{-1}\langle W_v\rangle. \tag{3.36}$$

and this time the right-hand-side is finite-dimensional, and so can be computed using $\mathbb{F}_2$-linear algebra. We detail the process in the next section.

3.5 Span computations

As we saw in Section 3.4, we should next compute

$$V = \bigcap_{v\in S} \rho_v^{-1}(\mathrm{span}(W_v)), \tag{3.37}$$

working with spans to prevent combinatorial explosion.

Note that we can now view the 2-Selmer set as the subset

$$\mathrm{Sel}^{(2)}(C/\mathbb{Q}) = \{w \in V : \rho_v(w) \in W_v \quad \forall v \in S\} \subseteq V. \tag{3.38}$$

It follows, therefore, that

$$V = \emptyset \implies \mathrm{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset \implies C(\mathbb{Q}) = \emptyset. \tag{3.39}$$

In practice, we may quite easily compute $\mathrm{span}(W_p)$ for some $p \in S' = \{q_1, \ldots, q_{s'}\} \subseteq S \setminus \{\infty\}$: if the span of the p-adic contact points of the bitangents has dimension six (nine for $p = 2$), then this makes up the whole span. So, we compute

$$\#(\mathbb{Z}_S^* \,/\, \mathbb{Z}_S^{*2})^6 = 2^{6(s+1)} \tag{3.40}$$

as a trivial upper bound on the size of the 2-Selmer set. We tighten the bound by computing

$$V_v = (\mathbb{Z}_S^* \,/\, \mathbb{Z}_S^{*2})^6 \cap \rho_v^{-1}(\mathrm{span}(W_v)). \tag{3.41}$$

In particular, we compute the sizes of

$$V_\infty = (\mathbb{Z}_S^* \,/\, \mathbb{Z}_S^{*2})^6 \cap \rho_\infty^{-1}(\mathrm{span}(W_\infty)), \tag{3.42}$$

(for details, see Section 5.5), and

$$V_{\infty,q_1} = V_\infty \cap \rho_{q_1}^{-1}(\mathrm{span}(W_{q_1})) = V_\infty \cap V_{q_1}, \tag{3.43}$$

and, for $i = 2, \ldots, s'$,

$$V_{\infty,q_1\ldots,q_i} = V_{\infty,q_1\ldots,q_{i-1}} \cap \rho_{q_i}^{-1}(\mathrm{span}(W_{q_i})) = V_\infty \cap V_{q_1} \cap \cdots \cap V_{q_i}. \tag{3.44}$$

Thus we construct a descending chain

$$\mathrm{Sel}^{(2)}(C/\mathbb{Q}) \subseteq V \subseteq V_{\infty,q_1,\ldots,q_{s'}} \subseteq \cdots \subseteq V_{\infty,q_1} \subseteq V_\infty \subseteq (\mathbb{Z}_S^* / \mathbb{Z}_S^{*2})^6. \tag{3.45}$$

If there exists an i such that $V_{\infty,q_1,\ldots,q_i} = 0$, then we conclude via (3.39) that $C(\mathbb{Q}) = \emptyset$. In practice, though, this has never occured. We can, however, reduce the bound further by computing local images at small primes, as we explain in the following sections. If we include all primes $p < 66564$, we will obtain the best possible bound. In practice, however, computing only at primes $p < 50$ will usually suffice.

3.6 Computing the local image

In this section we set out the definitions and structure theorems that allow us to compute the local image $\delta_v(C(\mathbb{Q}_v))$. Details of the implementation are postponed to Chapter 5.

It is straightforward to provide an explicit description of $C(\mathbb{Q}_p)$ consisting of three affine patches in $\mathbb{P}^2_{\mathbb{Q}_p}$:

$$C(\mathbb{Q}_p) = \{(x : y : 1) \colon x, y \in \mathbb{Z}_p, f(x, y, 1) = 0\} \tag{3.46}$$

$$\cup \{(x : 1 : pz) \colon x, z \in \mathbb{Z}_p, f(x, 1, pz) = 0\} \tag{3.47}$$

$$\cup \{(1 : py : pz) \colon y, z \in \mathbb{Z}_p, f(1, py, pz) = 0\}. \tag{3.48}$$

We require a finite, computable presentation of $C(\mathbb{Q}_p)$ carrying sufficient information to compute the local image $\delta_p(C(\mathbb{Q}_p)$. To this end, we make the following definitions.

Definition 3.24. An *(affine) p-adic disc* of radius p^{-e} and centre $(x_1, y_1) \in \mathbb{Z}_p^2$ is

$$(x_1 + O(p^e), y_1 + O(p^e)) = \{(x, y) \in \mathbb{Z}_p^2 : |x - x_1|_p \leq p^{-e} \text{ and } |y - y_1|_p \leq p^{-e}\}. \tag{3.49}$$

Definition 3.25. We say that the affine p-adic disc $(x_1+O(p^e), y_1+O(p^e))$ is *Hensel-liftable* if, writing $\tilde{f} = f(x_1 + p^{e-1}X, y_1 + p^{e-1}Y)$ and normalising $\bar{f} = \frac{1}{p^v} \cdot \tilde{f}$, where

$$v = \min\{v_p(a), \text{ where } a \text{ runs through the coefficients of } \tilde{f}\}; \tag{3.50}$$

$(0,0)$ is a non-singular point on the reduction $\bar{f} \equiv 0 \pmod{p}$.

So now we have a description of $C(\mathbb{Q}_p)$: we take a collection of Hensel-liftable affine p-adic discs that covers $C(\mathbb{Q}_p)$. We take the discs to be sufficiently small that δ_p is constant on each disc.

Lemma 3.26. *Let p be an odd prime, and suppose $(x_1 + O(p^e), y_1 + O(p^e))$ is a Hensel-liftable affine p-adic disc that contains at most one bitangent contact point. Then δ_p is constant on the disc $(x_1 + O(p^e), y_1 + O(p^e))$.*

Proof. If a bitangent ℓ_i does not have zeroes in the disc, then $\ell_i(x_1 + O(p^e), y_1 + O(p^e)) \in p^v c + O(p^{v+1})$, for some $v \geq 1$. So, ℓ_i is constant modulo squares on the disc: $\ell_i \equiv p^v c \pmod{\square}$.

If we can compute δ_p on the disc using only bitangents that don't have a zero in the disc, we get a constant value on the disc. Otherwise, there is at most one bitangent that has a zero in the disc. In this case, we can use syzygetic relations (precisely as in (3.5)) to avoid using that bitangent. □

Remark 3.27. For $p = 2$ we require smaller discs: argue as above, but this time the values of the bitangents on the disc lie in discs of the form $2^v c + O(2^{v+3})$. Again, we can take our discs sufficiently small to ensure this is the case for all but at most one bitangent.

Remark 3.28. After obtaining a collection of Hensel-liftable p-adic discs, we can get a collection of discs small enough that δ_p is constant in only finitely many refinement steps. In fact, often no refinement is necessary!

Before we present the lifting algorithm in a future section, a few remarks are due regarding the behaviour of any such method at the prime $p = 2$. We can write

$$\mathbb{Q}_p^* = \{p^e u \colon u \in \mathbb{Z}_p^*, e \in \mathbb{Z}\}. \tag{3.51}$$

In particular, $p \nmid u$, so for $p \neq 2$ the *Legendre symbol*

$$\left(\frac{u}{p}\right) := \begin{cases} 1, & \exists a \text{ such that } a^2 \equiv u \pmod{p}, \text{ and } u \not\equiv 0 \pmod{p}, \\ -1, & \nexists a \text{ such that } a^2 \equiv u \pmod{p}, \\ 0, & u \equiv 0 \pmod{p}, \end{cases} \tag{3.52}$$

is nonzero. This leads us to define a map as follows.

Lemma 3.29. *When p is odd, we have an isomorphism*

$$\begin{aligned} \varphi\colon \mathbb{Q}_p^* / \mathbb{Q}_p^{*2} &\xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ p^e u &\mapsto \left(e, \left(\frac{u}{p}\right)\right), \end{aligned} \tag{3.53}$$

where for $\alpha \in \mathbb{Q}_p^*$ we set $e = v_p(\alpha)$ and $u = \alpha p^{-e} \in \mathbb{Z}_p^*$.

Proof. We specify the map φ entirely:

$$\begin{aligned} \varphi\colon \mathbb{Q}_p^* / \mathbb{Q}_p^{*2} &\xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ 1 &\mapsto (0,0) \\ p &\mapsto (1,0) \\ u &\mapsto (0,1) \\ pu &\mapsto (1,1). \end{aligned} \tag{3.54}$$

□

For the case $p = 2$, we observe that

$$(\mathbb{Z}/8\mathbb{Z})^* = \{\pm\bar{1}, \pm\bar{3}\} \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}). \tag{3.55}$$

Thus, we define the morphism in the following way.

Lemma 3.30. *When $p = 2$, we have an isomorphism*

$$\begin{aligned} \psi\colon \mathbb{Q}_2^* / \mathbb{Q}_2^{*2} &\xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \\ 2^e u &\mapsto (e, u \pmod 8), \end{aligned} \tag{3.56}$$

where for $\alpha \in \mathbb{Q}_2^*$ we set $e = v_2(\alpha)$ and $u = \alpha 2^{-e} \in \mathbb{Z}_2^*$.

Proof. Write out the eight cases to argue precisely as in the proof of Lemma 3.29. □

Last, we consider the Archimedean case $v = \infty$.

Lemma 3.31. *We have an isomorphism*

$$\rho\colon \mathbb{R}^* / \mathbb{R}^{*2} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \tag{3.57}$$
$$x \mapsto \frac{1}{2}(1 - \operatorname{sgn}(x)) = \begin{cases} 0, & \text{if } x > 0, \\ 1, & \text{if } x < 0. \end{cases}$$

Proof. All positive reals are squares, so vanish in the quotient. The other class consists of the negative reals. □

Chapter 4

Constructing plane quartics with all bitangents rational

In this chapter we describe how to construct smooth plane quartics with a rational Aronhold system. The construction is based on the classic relation between del Pezzo surfaces of degree 2 and smooth plane quartic curves. We only describe the construction here to the extent needed to carry it out. For further details we refer the reader to Dolgachev [9, chs. 6,8].

Consider a set $\mathcal{P} = \{p_1, \ldots, p_7\} \subseteq \mathbb{P}^2$ of seven distinct points in the projective plane. We assume further that the points *lie in general position*; that is, no three of the points are colinear and no six lie on a conic.

Consider next the linear system L of cubic curves through these points. Since the points lie in general position, it follows that L is of dimension two and consists solely of irreducible cubics. Any subpencil in L will have two base points outside the base locus of L. The line spanned by these points (or the common tangents should these points coincide) is a point in the dual plane. Thus we may identify the net L with the plane $\mathbb{P}^2$ in which the seven points lie. We write $L^\vee$ for the dual variety of the linear system as a linear projective variety, and ϕ for the duality map (see Dolgachev [9, §1.2.2]).

Theorem 4.1. *The rational map $\phi\colon L \dashrightarrow L^\vee$ given by the linear system L is of degree 2. It extends to a regular degree two finite map $\pi\colon X \to L^\vee \cong \mathbb{P}^2$, where X is the blow-up of the set $\mathcal{P}$. The branch curve of ϕ is a smooth plane quartic C in $L^\vee$, and the ramification curve R is the proper transform of a curve $B \subseteq L$ of degree 6 with double points at each p_i. Conversely, given a smooth plane quartic curve C, the double cover of $\mathbb{P}^2$ ramified over C is a non-singular surface isomorphic to the blow-up of 7 points $p_1, \ldots, p_7$ in general position in the plane.*

Proof. See Dolgachev [9, ch. 8]. □

The surface X is a *del Pezzo surface of degree 2*. We shall not delve very far into the theory of del Pezzo surfaces — for that see Dolgachev [9, ch. 8] — but for present purposes we shall make the following definitions.

We consider *weighted projective space* $V = \mathbb{P}(2:1:1:1)$, where $V(\overline{k})$ is the set of nonzero vectors in $\overline{k}^4$ modulo the equivalence relation $\sim$ such that $(r_1 : u_1 : v_1 : w_1) \sim (r_2 : u_2 : v_2 : w_2)$ if and only if there is a nonzero scalar $\lambda \in \overline{k}$ such that $(r_1, u_1, v_1, w_1) = (\lambda^2 r_2, \lambda u_2, \lambda v_2, \lambda w_2)$. Algebraic subvarieties of V are defined analogously to those in ordinary projective space, but now one considers *weighted* homogeneous ideals of the polynomial ring $k[r, u, v, w]$.

Definition 4.2. A *del Pezzo surface of degree 2* is the variety

$$X \colon r^2 = f(u, v, w), \tag{4.1}$$

for some non-constant polynomial $f \in \overline{k}[u, v, w]$, where $X \in \mathbb{P}(2:1:1:1)$.

Remark 4.3. Clearly, the del Pezzo surface X defined by (4.1) is branched along $f(u, v, w) = 0$ as a cover of $\mathbb{P}^2_{uvw}$.

We interpret the theorem via the following commutative diagram:

$$\begin{array}{ccc} & X & \\ & \swarrow^{\sigma} \quad \searrow^{\pi} & \\ \mathcal{P} \subseteq \mathbb{P}^2_{xyz} & \xrightarrow{\phi=(f_1:f_2:f_3)} & C \subseteq \mathbb{P}^2_{uvw}. \end{array} \tag{4.2}$$

Blowing up $\mathcal{P} \subseteq \mathbb{P}^2_{xyz}$ gives a morphism $\sigma \colon X \to \mathbb{P}^2_{xyz}$, and $\pi \colon X \to \mathbb{P}^2_{uvw}$ is the regular degree two finite map extending ϕ, whose existence is guaranteed by Theorem 4.1. It suffices, therefore, for us to provide a full description of the map $\phi \colon \mathbb{P}^2_{xyz} \to \mathbb{P}^2_{uvw}$, explaining how the bitangents to C arise in the construction.

Let $f \in k[x, y, z]_3$ be a cubic form, so $f = \sum a_{ijk} x^i y^j z^k$ for some positive integers i, j, k satisfying $i + j + k = 3$. There are ten monomials of degree 3, so if we stipulate that f vanishes at each of the seven points of $\mathcal{P}$, this leaves a $10 - 7 = 3$-dimensional solution space $\langle f_1, f_2, f_3 \rangle$. Thus we may take our rational map ϕ to be that given by $\phi = (f_1 : f_2 : f_3)$.

Now we follow Dolgachev's exposition [9, §6.3.3], emphasising the key points. Lines $\ell \in \mathbb{P}^2_{uvw}$ are the image of non-singular elements of $\mathbb{P}^2_{xyz}$ if and only if ℓ intersects C transversally; that is, without tangency. Tangent lines $\ell \in \mathbb{P}^2_{uvw}$ therefore arise as the images of irreducible cubic curves with a singularity at an element of $\mathcal{P}$. Bitangents are the images of varieties

with two singularities, which may in fact coincide, should it be an *inflection* bitangent. As Dolgachev argues, the preimage in $\mathbb{P}^2_{uvw}$ of a bitangent in $\mathbb{P}^2_{xyz}$ is either an irreducible cubic F_i with a double point at p_i, or the union of a line $\overline{p_ip_j}$ and the conic K_{ij} passing through the point p_k, $k \neq i, j$. There are clearly 7 bitangents of the former kind, one for each of the points p_i of $\mathcal{P}$, and it makes sense to denote the bitangent corresponding to F_i by ℓ_i. We denote those bitangents corresponding to $\overline{p_ip_j} + K_{ij}$ by ℓ_{ij}. There are $\binom{7}{2} = 21$ of these, and so we have indeed taken account of all 28 bitangents of C.

Dolgachev argues further that the 7 bitangents we have denoted ℓ_i form an Aronhold set. The key point, from our perspective, is that if we take points $p_1, \ldots, p_7 \in \mathbb{P}^2(\mathbb{Q})$, then the bitangents we obtain are defined by $\mathbb{Q}$-rational data. Thus, the bitangents themselves are defined over $\mathbb{Q}$.

4.1 Syzygetic relations

Having now labelled our bitangents systematically, we may next determine the syzygetic relations between the bitangents.

To aid us in the combinatorics, dealing only with 2-digit positive integers, it makes sense to rewrite the ℓ_i as ℓ_{i8}. Now all the bitangents are denoted by a pair of digits from the set $\{1, \ldots, 8\}$. Following Dolgachev [9, §6.1.2], who himself follows Cayley, we denote such a pair by a line |. If two pairs share a common digit, we make them intersect. Thus we have:

- Pairs of bitangents: 210 of type || and 168 of type $\vee$.
  - There are $\binom{8}{2} = 28$ bitangents (as we know from Theorem 2.20), and therefore $28 \times 27 \times \frac{1}{2} = 378$ pairs of bitangents.
  - Of these, $28 \times 12 \times \frac{1}{2} = 168$ share a common digit, and the remaining $378 - 168 = 210$ do not.
- Triples of bitangents: 420 of type $\sqcup$ and 840 of type ||| (these are syzygetic);
  56 of type $\triangle$, 1680 of type $\vee|$ and 280 of type $\perp$ (azygetic).
  - There are $28 \times 27 \times 26 \times \frac{1}{3!} = 3276$ triples of bitangents.
  - Of these, $28 \times 6 \times 5 \times \frac{1}{2} = 420$ take the form $\sqcup$, while $28 \times 15 \times 6 \times \frac{1}{3} = 840$ take the form |||.
  - Of the remaining 2016, $28 \times 6 \times 1 \times \frac{1}{3} = 56$ take the form $\triangle$, $28 \times 12 \times 10 \times \frac{1}{2} = 1680$ take the form $\vee|$, and the remaining $28 \times 12 \times 5 \times \frac{1}{6} = 280$ take the form $\perp$.

- Quadruples of bitangents: 105 of type |||| and 210 of type □ (syzygetic).
  We are not concerned with the others (see [9, §6.1.2] for details).
  - $28 \times 15 \times 6 \times 1 \times \frac{1}{4!} = 105$ of the form ||||.
  - $28 \times 6 \times 5 \times \frac{1}{4} = 210$ of type □.
- Aronhold sets: we have fixed an Aronhold set of type ✳. There are 8 possibilities for this — one for each of the 8 digits in $\{1, \ldots, 8\}$ that may have been omitted. Note that our earlier choice to omit 8 was arbitrary.

Chapter 5

Implementation details

In this chapter we describe the specific design choices we have made in implementing the procedures described in Chapters 3 and 4.

5.1 Reordering the bitangents

From the description in Section 4.1 it follows that, given a labelled Aronhold set, the other bitangents can be labelled uniquely based on the syzygetic relations. In this section we describe how to recover such a labelling.

We ensure that $\ell_1, \ldots, \ell_7$ form an Aronhold set by making sure that no triple is part of a syzygetic quadruple. For each of the remaining bitangents $\ell_7, \ldots, \ell_{28}$, we define a bitangent labelling as follows.

Definition 5.1. A *bitangent labelling* assigns to each bitangent ℓ_j, where $j \in \{7, \ldots, 28\}$, a 5-tuple $\underline{v}^{(j)} = (a_1^{(j)}, \ldots, a_5^{(j)}) \in \mathbb{F}_2^5$, such that

$$a_i^{(j)} = \begin{cases} 0, & \{\ell_1, \ell_{i+1}, \ell_j\} \text{ forms a syzygetic triple,} \\ 1, & \text{otherwise.} \end{cases} \tag{5.1}$$

Remark 5.2. Suppose $\{\ell_1, \ldots, \ell_7\}$ forms an Aronhold system for C. Then $\underline{v}^{(7)} = (1, 1, 1, 1, 1)$.

The configuration of syzygetic quadruples is essentially the same for each smooth plane quartic, so in each case we see the same labels. Each label occurs once. Therefore, we may

simply order the bitangents according to fixed labels. For instance, we can take

$$\begin{aligned}
\underline{v}^{(8)} &= (0,0,1,1,1), & \underline{v}^{(15)} &= (1,1,0,0,1), & \underline{v}^{(22)} &= (0,1,1,1,1),\\
\underline{v}^{(9)} &= (1,0,1,1,0), & \underline{v}^{(16)} &= (1,0,0,1,1), & \underline{v}^{(23)} &= (1,1,1,1,0),\\
\underline{v}^{(10)} &= (1,1,0,1,0), & \underline{v}^{(17)} &= (1,1,0,1,1), & \underline{v}^{(24)} &= (0,0,1,0,0),\\
\underline{v}^{(11)} &= (0,0,0,1,0), & \underline{v}^{(18)} &= (1,0,0,0,0), & \underline{v}^{(25)} &= (0,1,0,1,1),\\
\underline{v}^{(12)} &= (1,0,1,1,1), & \underline{v}^{(19)} &= (0,0,0,0,0), & \underline{v}^{(26)} &= (0,1,1,0,1),\\
\underline{v}^{(13)} &= (1,1,1,0,0), & \underline{v}^{(20)} &= (1,0,1,0,1), & \underline{v}^{(27)} &= (0,1,1,1,0),\\
\underline{v}^{(14)} &= (1,1,1,0,1), & \underline{v}^{(21)} &= (0,1,0,0,0), & \underline{v}^{(28)} &= (0,0,0,0,1).
\end{aligned} \tag{5.2}$$

We can check that with this presentation, the action of the *symplectic group* $\mathrm{Sp}_6(\mathbb{F}_2)$ — defined as the group of transformations of $V = \mathbb{F}_2^6$ of determinant 1 preserving some skew-symmetric, non-degenerate bilinear form $Q : V \times V \to \mathbb{F}_2$ — is through the permutation group

$$\Gamma = \langle \sigma, \tau \rangle \leq \mathrm{S}_{28}, \tag{5.3}$$

where

$$\begin{aligned}
\sigma &= (1,2)(4,5)(8,21)(10,13)(11,25)(14,17)(16,20)(19,22)(24,26)(27,28), \\
\tau &= (1,3,11)(2,9,21,4,12,25)(5,15,19,23,26,28)(6,24,27,13,16,17)(7,8,10,14,18,22).
\end{aligned} \tag{5.4}$$

Furthermore, with our bitangents thus labelled, we know precisely which quadruples are syzygetic. Thus, after this relabelling, we can select syzygetic quadruples without further computation.

5.2 Approximating $C(\mathbb{Q}_p)$

In Section 3.6 we introduced affine p-adic discs, and what it means for them to be Hensel-liftable. Our lifting algorithm can then be characterised as one that tries to compute a finite list of Hensel-liftable affine p-adic discs that cover all of $C(\mathbb{Q}_p)$. The main (recursive) algorithm — which we now present — then takes as input an affine $f \in \mathbb{Z}[x,y]$ and produces as output a finite list of Hensel-liftable affine p-adic discs that cover all the $\mathbb{Z}_p$-valued solutions of $f(x,y) = 0$. We will need this algorithm to compute local images at finite places.

Algorithm 1 LIFT – Lifting affine p-adic discs to the level of Hensel-liftability

Input: f, p, x_0, y_0, e

f – a bivariate polynomial in $\mathbb{Z}[x, y]$ describing a smooth affine curve

p – a prime

x_0, y_0 – integers

e – a non-negative integer

Output: Points

A list of Hensel-liftable affine p-adic discs that cover all $\mathbb{Z}_p$-valued solutions to $f(x, y) = 0$ satisfying $x \equiv x_0 \pmod{p^e}$, $y \equiv y_0 \pmod{p^e}$ ▷ c.f. Definition 3.25

$\nabla f \leftarrow \left(\frac{df}{dx}, \frac{df}{dy}\right)$
Points $\leftarrow \{\}$
$W_{xy} \leftarrow \{(x, y) : x, y \in \{0, \ldots, p-1\}$ and $f(x, y) \equiv 0 \pmod{p}\}$
for P in W_{xy} **do**
    $x_1 \leftarrow x(P)$
    $y_1 \leftarrow y(P)$
    if $\exists g \in \nabla f$ such that $g(P) \neq 0$ **then**
        Add $(x_0 + p^e x_1, y_0 + p^e y_1) \in \mathbb{Z}_p^2$ to Points.
    else
        $g \leftarrow f(x_1 + px, y_1 + py)$
        Add the result of LIFT$(g/\operatorname{cont}(g), p, x_0 + p^e x_1, y_0 + p^e y_1, e + 1)$ to Points
    end if
end for
return Points

Further Explanation:
We loop through representatives (x_1, y_1) of the solutions $x, y \in \mathbb{F}_p$ to $\bar{f}(x, y) \equiv 0 \pmod{p}$. If $\partial\bar{f}/\partial x(x, y) \not\equiv 0$ or $\partial\bar{f}/\partial y(x, y) \not\equiv 0$, then (x_1, y_1) lies p-adically close to the rational points on L. Otherwise, we lift higher.

The idea then is to work through each of the affine patches (3.46), (3.47), (3.48). Normalise f by writing $\tilde{f} = f/\operatorname{cont}(f)$, and compute $\textsc{lift}(\tilde{f}, p, 0, 0, 0)$ in each case. Then, we obtain 3 point-sets, one for each affine patch:

$$\begin{aligned} P_1 &= \{(x_i + O(p^{e_i}), y_i + O(p^{e_i}), 1)\}, \\ P_2 &= \{(x_j + O(p^{e_j}), 1, y_j + O(p^{e_j})\}, \\ P_3 &= \{(1, x_k + O(p^{e_k}), y_k + O(p^{e_k})\}. \end{aligned}$$

Taking the union of these point-sets, we obtain our output list of Hensel-liftable affine p-adic discs.

We postpone consideration of the real case $C(\mathbb{R})$ until Section 5.5. For now, simply note that there shall not be any need to go through any such expensive p-adic lifting process.

5.3 Computing d-values

We described in Section 3.2 how the existence of syzygetic quadruples $\{\ell_\alpha, \ell_i, \ell_j, \ell_k\}$ implies that in the function field $k(C)$ we have equalities of the form (3.3). To recover the d-values, it is then simply a case of expanding the left-hand-side of the equality

$$\ell_\alpha \ell_i \ell_j \ell_k + cf - d\left(\sum_{i+j\leq 2} a_{ij} x^i y^j z^{2-i-j}\right)^2 = 0, \tag{5.5}$$

to form a system of equations in c, d, a_{ij}. As $\{\ell_\alpha, \ell_i, \ell_j, \ell_k\}$ are syzygetic, this system has a solution. We solve for $d \in \mathbb{Q}$, and since we only care for the value of d modulo squares (c.f. (3.4)), we take the square-free part of the product of the numerator and denominator of d to obtain $\tilde{d} \in \mathbb{Z}$.

We see that 210 of our 315 syzygetic quadruples contain a bitangent from the Aronhold set $\{\ell_1, \ldots, \ell_7\}$ (c.f. Section 4.1). For $j = 1, \ldots, 7$, we pick out the syzygetic quadruples including ℓ_j, compute and store the d-values (we called $\tilde{d}$ above) together with the indices of the syzygetic triple formed by omitting ℓ_j. This list comes in useful in our local image computations, which we next detail.

5.4 Computing the local image at a finite place

With an approximation to $C(\mathbb{Q}_p)$ now in hand (see Section 5.2), we continue to describe our implementation of the two-cover descent method we set out in Section 3.1. In particular, we now wish to compute the local image $\delta_p(C(\mathbb{Q}_p))$.

Remark 5.3. Recall from Section 3.6 that the codomain of the map δ_v is $(\mathbb{Q}_v^* / \mathbb{Q}_v^{*2})^6$, which can be considered as an $\mathbb{F}_2$-vector space. By Lemmas 3.29 and 3.30, it is isomorphic to $\mathbb{F}_2^{18}$ for $v = 2$, and isomorphic to $\mathbb{F}_2^{12}$ for odd finite v.

The following routine takes as input a Hensel-liftable affine p-adic disc and evaluates what values δ_p takes on the points of $C(\mathbb{Q}_p)$ that lie in the disc:

1. See if $\ell_1, \ldots, \ell_7$ take well-defined values (modulo squares) on the p-adic disc. If so, we simply determine the image via (3.1). For odd p, this means that the disc contains no points of these bitangents.

2. Determine the values of the other 21 bitangents as well. For each $i = 1, \ldots, 7$ for which ℓ_i is not ostensibly constant (modulo squares) on the disc, see if there is a syzygetic quadruple where the other three bitangents take well-defined values. Use the relations (3.5) to replace the ℓ_i where necessary, and then compute once again via (3.1).

3. If we failed for one of $i = 1, \ldots, 7$ in the two above steps, split the Hensel-liftable p-adic disc of radius p^{-e} into p Hensel-liftable discs of radius p^{-e-1} and repeat with those discs.

Remark 5.4. Since the curve C under consideration is smooth, the contact points of bitangents are necessarily distinct. So, if we reduce our radii sufficiently, we can ensure that no more than one contact point lies in a p-adic disc. Thus we can deduce the value of all but at most one of the bitangents. We conclude that step 2 listed above will always eventually succeed.

We will shortly provide an example to clarify how the above routine works. Before that, though, we should consider how to go about computing the local image at the infinite place $v = \infty$.

5.5 Real bitangents

We deal now with the Archimedean case, where we consider the completion of $\mathbb{Q}$ at the infinite place $v = \infty$, so $k = \mathbb{Q}_\infty = \mathbb{R}$. In this case we have the commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\delta} & \left(\mathbb{Q}^* / \mathbb{Q}^{*2}\right)^6 \\ \downarrow & & \downarrow \rho_\infty \\ C(\mathbb{R}) & \xrightarrow{\delta_\infty} & \left(\mathbb{R}^* / \mathbb{R}^{*2}\right)^6. \end{array} \tag{5.6}$$

The idea is as before. If $\delta_\infty(C(\mathbb{R}))$ is empty, then we have a local obstruction, and so conclude that $C(\mathbb{Q})$ is empty. Otherwise, we know that the Selmer set $\mathrm{Sel}^{(2)}(C/k) = \prod_{v \in S} \rho_v^{-1}(\delta_v(C(\mathbb{Q}_v))$ lies inside $\rho_\infty^{-1}(\delta_\infty(C(\mathbb{R})))$, so it is important we include this data in the computations we set out in Section 3.5.

We saw in Lemma 3.31 that

$$\mathbb{R}^* / \mathbb{R}^{*2} \cong \{\pm 1\}, \tag{5.7}$$

with all positive reals in one class and all negatives in the other. Thus our task is considerably simpler in this case: there is no need to go through the expensive p-adic lifting process of Section 3.6. Instead, we compute $\delta_\infty(C(\mathbb{R}))$ according to the following lemma, and the resulting procedure.

Lemma 5.5. *The map δ_∞ is constant on the connected components of $C(\mathbb{R})$.*

Proof. Since bitangents to $C\colon f(x, y, 1) = 0$ are given by linear equations $\ell_i(x, y, 1) = 0$, each bitangent ℓ_i to C divides the plane $\mathbb{A}^2(\mathbb{R})$ in two according to the sign of ℓ_i. Because the bitangents have even order contact with the curve C, it follows that each component of $C(\mathbb{R})$ lies in one of these half-planes. From this we see that the sign of ℓ_i is constant on each component of C, and so (3.1) implies the result. □

Computation of $\delta_\infty(C(\mathbb{R}))$ is then simply a matter of picking a point on each connected component. The full procedure is as follows. For simplicity we restrict our attention to the affine patch found by setting $z = 1$.

1. Compute the resultant $R = \mathrm{res}_x(f_x, f_y) \in \mathbb{R}[x, y]$.
2. Let y_i be the roots of the equations $R(0, y_i) = 0$, and x_i such that $f_x(x_i, y_i) = f_y(x_i, y_i) = 0$. Write $P_i = (x_i, y_i)$. So these are the critical points of $f(x, y)$ as a real function in two variables.

3. Parametrise the lines P_iP_j for which $f(P_i)$ and $f(P_j)$ have opposite signs.

4. Compute the points Q_r where f intersects the line P_iP_j. We obtain 2 or 4 points in each case. In total we are guaranteed to find points on each of the real components.

5. Evaluate the Aronhold system of bitangents to f at each intersection point. Use the isomorphism as abelian groups $\{\pm 1\} \xrightarrow{\sim} \mathbb{F}_2$ to assign 0 to those bitangents evaluating to positive numbers, and assign 1 to their negative counterparts. Call the resulting vector $m_r \in \mathbb{F}_2^7$. Ignoring duplicates, this forms a set of vectors $W = \{m_{11}, \ldots, m_{71}, m_{12}, \ldots, m_{7t}\}$ with each $m_{rs} \in \mathbb{F}_2^7$, and $1 \leq r \leq 7$, $1 \leq s \leq t$, for some positive integer t.

6. We track the values (modulo squares) of ℓ_i/ℓ_7 at each of the intersection points: set

$$\tilde{W} = \{m_{11} + m_{71}, \ldots, m_{61} + m_{71}, m_{12} + m_{72}, \ldots m_{6t} + m_{7t}\}. \tag{5.8}$$

Remark 5.6. Although it is not necessary in computing the local image, it may be useful to further compute the span of the translate of the entire set over a member, $m_{11} + m_{71}$, say. So

$$\langle \tilde{\tilde{W}} \rangle = \langle m_{21} - m_{11}, \ldots, m_{61} - m_{11}, m_{12} + m_{72} - (m_{11} + m_{71}), \ldots, m_{6t} + m_{7t} - (m_{11} + m_{71}) \rangle. \tag{5.9}$$

Remark 5.7. Proposition 3.23 allows us to check whether the local image obtained is of the correct $\mathbb{F}_2$-dimension. If not, we exclude the local information at this place from our computations, as described in Section 3.5.

Further Explanation:
ad 1–4. As Plaumann et al. [23, §1] show, plane quartic curves have at most 4 connected components in the Euclidean topology. If we take lines joining the critical points of $f(x, y)$ — considered as a function in two variables — and assume that all 9 contact points lie in the chosen affine patch $\mathbb{A}_2^2$, then we intersect each component at least once.

ad 5. We evaluate the bitangents at the intersection points identified in step 4. By construction, the values obtained will be nonzero. Due to (5.7), we care only for the sign. The isomorphism is given

$$\begin{aligned} \{\pm 1\} &\xrightarrow{\sim} \mathbb{F}_2 \\ m_i &= \frac{1}{2}(1 - \operatorname{sgn}(\ell_i(x, y, 1)), \end{aligned} \tag{5.10}$$

for each $i \in \{1, \ldots, 7\}$.

ad 6. Note that in forming $\tilde{W}$ we have followed an additive analogy of the construction of (3.1), and so $\tilde{W} = \delta_\infty(C(\mathbb{R}))$ as claimed.

Remark 5.8. In principle, it could happen that one of the intersection points Q_r is a contact point of one of the bitangents $\ell_1, \ldots, \ell_7$. In this case, one could use the syzygetic relations to compute the value of δ_∞ anyway (see Section 3.2). In practice, however, we have never run into this problem.

5.6 A worked example

The routine suggested in the previous two sections is perhaps best illustrated by means of an example:

Example 5.9. The plane quartic curve with minimal model

$$C\colon X^4 - 2X^3Y + 23X^2Y^2 - 76X^2Z^2 - 22XY^3 + 76XYZ^2 + 16Y^4 - 311Y^2Z^2 + 1024Z^4 = 0 \tag{5.11}$$

has as bitangents:

$$\begin{aligned}
Z &= 0, & 2X + 10Y - 5Z &= 0,\\
2X - 11Y &= 0, & 2X + 31Y - 2Z &= 0,\\
58X - 25Y + 38Z &= 0, & 6X - 75Y - 2Z &= 0,\\
22X - 23Y + 10Z &= 0, & Y &= 0,\\
62X - 47Y + 40Z &= 0, & 14X + 7Y + 10Z &= 0,\\
78X - 135Y + 50Z &= 0, & 2X - 4Y + Z &= 0,\\
54X - 3Y + 34Z &= 0, & 42X + 25Z &= 0,\\
102X - 99Y + 70Z &= 0, & 122X - 125Y + 70Z &= 0,\\
130X - 85Y + 78Z &= 0, & 6X - 5Y + 4Z &= 0,\\
6X + 9Y + 10Z &= 0, & 14X - 14Y + 9Z &= 0,\\
42X - 21Y + 22Z &= 0, & 22X + 5Y + 14Z &= 0,\\
10X - 13Y + 10Z &= 0, & 18X - 15Y + 14Z &= 0,\\
8X - 2Y + 5Z &= 0, & 10X - 13Y + 14Z &= 0,\\
16X - 25Y + 12Z &= 0, & 14X - 35Y + 4Z &= 0.
\end{aligned}$$

The bad primes are $\{2, 3, 5, 7, 13\}$. So this makes up our set S for computation (see Corollary 3.17). Thus $\#S = s = 5$.

The routine takes the affine p-adic disc $P = (25 + O(2^9), 80 + O(2^9), 1)$, and computes $\ell_\alpha(P) \neq 0$ for $\alpha \in \{1, 2, 5, 6, 7\}$, but $\ell_3(P) = \ell_4(P) = 0$. In step 2 we find for ℓ_3 the syzygetic triple $\{\ell_7, \ell_{16}, \ell_{17}\}$ and corresponding d-value $d = -3$, and for ℓ_4 the syzygetic

triple $\{\ell_7, \ell_{10}, \ell_{23}\}$ with d-value $d = 5$. So we compute $\delta_2(P)$, with $\ell_3(P) = 0$ replaced by

$$\tilde{\ell}_3(P) = -3 \cdot \ell_7(P)\ell_{16}(P)\ell_{17}(P) = 5120 + O(2^{14}), \tag{5.12}$$

and $\ell_4(P) = 0$ replaced by

$$\tilde{\ell}_4(P) = 5 \cdot \ell_7(P)\ell_{10}(P)\ell_{23}(P) = -3840 + O(2^{13}). \tag{5.13}$$

We find

$$\delta_2(P) = (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \in \mathbb{F}_2^{18}\,. \tag{5.14}$$

In full, we find 16 distinct local image vectors in $\mathbb{F}_2^{18}$ for the prime $p_1 = 2$. In keeping with our notation in Section 3.5, we denote by W_2 the 16-element set of vectors in $\mathbb{F}_2^{18}$ obtained in this way. We also find an explicit description of the map $\rho_2\colon \mathbb{F}_2^{36} \to \mathbb{F}_2^{18}$, where the 36 arises as the $\mathbb{F}_2$-dimension of $(\mathbb{Z}_S^* \,/\, \mathbb{Z}_S^{*2})^6$, which is $6(s+1) = 6 \times 6 = 36$.

In general, we obtain for each prime $p_i \in S \setminus \{2, \infty\}$ a set of vectors in $\mathbb{F}_2^{12}$, which we call W_{p_i}, accompanied by the map $\rho_{p_i}\colon \mathbb{F}_2^{36} \to \mathbb{F}_2^{12}$. Here the index i starts at 2, so $p_2 = 3$, $p_3 = 5$, etc. allowing for $p_1 = 2$.

For $v = \infty$, we obtain a set of four vectors in $\mathbb{F}_2^6$:

$$\tilde{W} = \{(1, 0, 1, 0, 1, 1), (0, 1, 0, 1, 1, 1), (1, 1, 0, 0, 0, 1), (0, 0, 0, 0, 0, 0)\}, \tag{5.15}$$

together with the corresponding map $\rho_\infty : \mathbb{F}_2^{36} \to \mathbb{F}_2^6$.

Recall from Section 3.5 that

$$V = \bigcap_{v \in S} \rho_v^{-1}(\mathrm{span}(W_v)),$$

and we are to compute

$$V_v = (\mathbb{Z}_S^* \,/\, \mathbb{Z}_S^{*2})^6 \cap \rho_v^{-1}(W_v),$$

so

$$V_\infty = (\mathbb{Z}_S^* \,/\, \mathbb{Z}_S^{*2})^6 \cap \rho_\infty^{-1}(W_\infty),$$

and

$$\begin{aligned}
V_{\infty,3} &= V_\infty \cap \rho_3^{-1}\operatorname{span}(W_3) \\
&= V_\infty \cap V_3, \\
V_{\infty,3,5} &= V_{\infty,3} \cap \rho_5^{-1}\operatorname{span}(W_5) \\
&= V_\infty \cap V_3 \cap V_5, \\
V_{\infty,3,5,7} &= V_{\infty,3,5} \cap \rho_7^{-1}\operatorname{span}(W_7) \\
&= V_\infty \cap V_3 \cap V_5 \cap V_7, \\
V_{\infty,3,5,7,13} &= V_{\infty,3,5,7} \cap \rho_{13}^{-1}\operatorname{span}(W_{13}) \\
&= V_\infty \cap V_3 \cap V_5 \cap V_7 \cap V_{13}.
\end{aligned}$$

We have in this case

Set	$(\mathbb{Z}_S^* / \mathbb{Z}_S^{*2})^6$	V_∞	$V_{\infty,3}$	$V_{\infty,3,5}$	$V_{\infty,3,5,7}$	$V_{\infty,3,5,7,13}$
F_2-dimension	36	33	28	23	18	11

The set we are left with is amenable to enumeration: $\#V_{\infty,3,5,7,13} = 2^{11} = 2048$.

We loop over

$$\{\delta \in V_{\infty,3,5,7,13} : \rho_v(\delta) \in W_v \text{ for } v < 50\}.$$

We find that this set is empty, so its subset $\mathrm{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset$ as well. Hence we conclude via Proposition 3.13 that here $C(\mathbb{Q}) = \emptyset$.

Chapter 6

Experimental results

We remarked in Chapter 3 upon how two-cover descent in many cases allows one to prove that a curve has no rational points, and laid out in Chapter 5 precisely how we went about such an implementation. We now present the results of these investigations.

6.1 Curve generation

We tested our implementation on 1000 randomly generated examples. We produced these examples in the following manner.

1. We pick $p_1 = (1 : 0 : 0)$, $p_2 = (0 : 1 : 0)$, $p_3 = (0 : 0 : 1)$, $p_4 = (1 : 1 : 1)$, and randomly select three more points $p_5 = (x_5 : y_5 : z_5)$, $p_6 = (x_6 : y_6 : z_6)$ and $p_7 = (x_7 : y_7 : z_7)$ by choosing $x_5, \ldots, z_7$ uniformly randomly from $\{-B, \ldots, B\}$ (we used $B = 20$).

2. We test that $p_1, \ldots, p_7$ lie in general position. If they do not, we discard the point and generate new ones.

3. We construct a smooth plane quartic with all its bitangents defined over $\mathbb{Q}$ using the procedure described in Theorem 4.1.

4. We compute the normalised Dixmier–Ohno invariants, utilising the implementation of [18]. Should the invariants of two curves match, the two curves are isomorphic over $\overline{\mathbb{Q}}$, and so we delete the latter. In fact, such a match happens very rarely: it does not occur over our sample of 1000 curves, but larger samples do yield matches.

5. We test how many of our curves are everywhere locally solvable, using the algorithms introduced in [2, §5].

6. We test if there are any obvious rational points on the curve, i.e., we see if any of the contact points of the bitangents are rational. If so, we have determined that the curve does have rational points.

7. We compute $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$ of this curve. If this set is empty then we have determined that the curve has no rational points.

In order to test that the 7 points lie in general position, we need to check that no 3 points lie on a line and no 6 lie on a conic. We do this by using the following lemmas.

Lemma 6.1. *Three points* $(x_1 : y_1 : z_1), (x_2 : y_2 : z_2), (x_3 : y_3 : z_3)$ *lie on a line if and only if*

$$\det \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{pmatrix} = 0. \tag{6.1}$$

Proof. This is a standard result in linear algebra. See for instance Strang [33, §4.2]. □

Lemma 6.2. *Six points* $\{(x_i : y_i : z_i) : i = 1, \ldots, 6\}$ *lie on a conic if and only if the matrix with rows* x_i^2, y_i^2, z_i^2, x_iy_i, x_iz_i, y_iz_i *has determinant zero.*

Proof. The proof is analagous to that of Lemma 6.1. Conics are defined by homogeneous degree 2 equations

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0. \tag{6.2}$$

So if six points $\{(x_i : y_i : z_i) : i = 1, \ldots, 6\}$ are coconic, applying Gaussian elimination to the matrix with rows x_i^2, y_i^2, z_i^2, x_iy_i, x_iz_i, y_iz_i we can force a zero column, and so the matrix has determinant zero. Conversely, if the determinant is zero, then the rank of the matrix is less than 6, and so we can express one column as a linear combination of the other 5. This gives an expression of the form (6.2), and so the points are coconic. □

We check whether $p_1, \ldots, p_7$ lie in general position by applying Lemma 6.1 to each triple of points, and Lemma 6.2 to each of the seven subsets of six points.

6.2 Results

We checked our 1000 test curves for local solvability. There is one curve that does not have $\mathbb{Q}_2$-points and there are six curves that do not have $\mathbb{Q}_{11}$-points. Interestingly, these curves are all of good reduction at the prime p where they fail to have p-adic points.

Over our data set of 1000 isomorphism classes of plane quartic curves (their minimal models are listed in the file `Curves.m`), we exhibit the existence of rational points on 177 of the curves. Two-cover descent allows us to conclude that all of the remaining 823 curves do not have rational points.

Remark 6.3. Testing if any of the contact points of the bitangents are rational allows us to relatively quickly show that $C(\mathbb{Q}) \neq \emptyset$ in many cases. Working on a computer based on four INTEL Core i5-4570 3.20GHz processors, we were able to generate and test the 1000 curve sample in 57 minutes.

6.3 Next steps

Our results for this 1000-curve data set were complete: we showed that either the curve has rational points (177 cases), or does not (823 cases). No curves were left undecided. A priori, it is however possible that a curve could have no rational points but survive a two-cover descent: Bruin and Stoll saw this in the hyperelliptic case.

In [4], Bruin and Stoll applied a "Mordell–Weil sieve" computation to the hyperelliptic curves surviving two-cover descent. Further details of the method, originally due to Scharaschkin, are available in their 2010 paper [6].

To implement a Mordell–Weil sieve routine in the non-hyperelliptic case we are concerned with, we would require generators for $\mathrm{Jac}_C(\mathbb{Q})$, and a degree 1 divisor on $C/\mathbb{Q}$. This information is available in [3], so a Mordell-Weil sieve approach should be practical for plane quartic curves. It is, however, beyond the scope of this thesis, but would be an interesting direction for future research.

Bibliography

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

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

[3] Nils Bruin, Bjorn Poonen, and Michael Stoll. Generalized explicit descent and its application to curves of genus 3. *Forum Math. Sigma*, 4:e6, 80, 2016.

[4] Nils Bruin and Michael Stoll. Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17(2):181–189, 2008.

[5] Nils Bruin and Michael Stoll. Two-cover descent on hyperelliptic curves. *Math. Comp.*, 78(268):2347–2370, 2009.

[6] Nils Bruin and Michael Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010.

[7] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[8] J. Dixmier. On the projective invariants of quartic plane curves. *Adv. in Math.*, 64(3):279–304, 1987.

[9] Igor V. Dolgachev. *Classical algebraic geometry*. Cambridge University Press, Cambridge, 2012. A modern view.

[10] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[11] William Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[12] K. Geiser. Ueber die doppeltangenten einer ebenen curve vierten grades. *Math. Ann.*, 1(1):129–138, 1869.

[13] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[14] Helmut Hasse. Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper. *J. Reine Angew. Math.*, 153:158–162, 1924.

[15] Helmut Hasse. Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper. *J. Reine Angew. Math.*, 153:113–130, 1924.

[16] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[17] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

[18] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling. Reconstructing plane quartics from their invariants, 2016.

[19] Eli Luberoff. Desmos graphing calculator. Last visited on 09/04/2019.

[20] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[21] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[22] T. Ohno. The graded ring of invariants of ternary quartics i. Unpublished, 2005.

[23] Daniel Plaumann, Bernd Sturmfels, and Cynthia Vinzant. Quartic curves and their bitangents. *J. Symbolic Comput.*, 46(6):712–733, 2011.

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

[25] Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999.

[26] Claudio Rocchini. Bitangents of trott curve. From Wikimedia. CC BY 2.5. Last visited on 10/04/2019.

[27] George Salmon. *A treatise on the higher plane curves: intended as a sequel to "A treatise on conic sections"*. 3rd ed. Chelsea Publishing Co., New York, 1960.

[28] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French.

[29] Igor R. Shafarevich. *Basic algebraic geometry. 1.* Springer-Verlag, Berlin, second edition, 1994. Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.

[30] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[31] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2019.

[32] Michael Stoll. Reduction theory of point clusters in projective space. *arXiv e-prints*, page arXiv:0909.2808, Sep 2009.

[33] Gilbert Strang. *Linear algebra and its applications*. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976.

[34] Eric W. Weisstein. Trott curve. From MathWorld—A Wolfram Web Resource. Last visited on 09/04/2019.