university of groningen

faculty of science and engineering

Computing the rational torsion subgroup of Jacobians of hyperelliptic curves.

Master Project Mathematics

November 2020

Student: Berno Reitsma

First supervisor: dr. J.S. (Steffen) Müller

Second supervisor: prof. dr. J. Top

Abstract

This thesis describes and proves the correctness of an algorithm that computes the rational torsion subgroup for the Jacobian of any hyperelliptic curve, and describes the explicit theory that is required by this algorithm. It does not require a procedure that performs the group law on the rational points of the Jacobian. Furthermore, all the required procedures are explicitly described and implemented for Jacobians of hyperelliptic curves of genus 3. Both the design of the algorithm and many required procedures are based on work by Michael Stoll. The rational torsion structures of many Jacobians of hyperelliptic curves of genus 3 with low discriminant have been computed for the LMFDB.

Contents

1 Introduction

In arithmetic geometry, techniques that aim to solve Diophantine equations often involve exploring the group structure of the Jacobian of a given curve defined over a number field k. A classical example is an elliptic curve E, for which the Jacobian is equal to the curve. The set of rational points $E(k)$ is a finitely generated abelian group, so one can find $E(k)$ by finding generators and relations of $E(k)$.

For elliptic curves, all possible rational torsion structures are determined [33]. The rational torsion structures of higher-dimensional abelian varieties (such as Jacobians of hyperelliptic curves) are not known in general, and are tied to the uniform boundedness conjecture, stating that the order of the k-rational torsion subgroup of an abelian variety A defined over a number field k is bounded in terms of the dimension of A and the number field k [48, Chapter 2]. Several authors have tried to construct curves corresponding to Jacobians that have a rational torsion point with large order [29] [43], but, so far, complete algorithms for the computation of $J(\mathbb{Q})_{\text{tors}}$ have only been known for Jacobians of hyperelliptic curves of genus 1 and 2. Having a method to compute $J(\mathbb{Q})_{\text{tors}}$ could give more insight on the possible torsion structures that can be found.

Finding $J(\mathbb{Q})_{\text{tors}}$ is also a first step ro compute $J(\mathbb{Q})_{\text{tors}}$. By the theorem of Mordell-Weil, $J(\mathbb{Q})_{\text{tors}}$ is a finite abelian group. $J(\mathbb{Q})_{\text{tors}}$ can be used to gain experimental insight on the behavior of the rank of J, which is connected to conjectures such as the Birch and Swinnerton-Dyer conjecture for abelian varieties [2]. In refined versions of the Birch and Swinnerton-Dyer conjecture, the cardinality of $J(\mathbb{Q})_{\text{tors}}$ is directly considered [58]. Furthermore, if one has obtained enough information on $J(\mathbb{Q})$, one can attempt to determine $C(\mathbb{Q})$ using the method of Chabauty and Coleman [34], provided that the rank of $J(\mathbb{Q})$ is strictly less than the genus of C.

Given an elliptic curve E defined over $\mathbb{Q}$, one can use reduction modulo p (where p is a suitable prime) [49, §VII.2, VII.3] and Nagell-Lutz Theorem [49, Corollary VIII.7.2] to determine $E(\mathbb{Q})_{\text{tors}}$. Techniques using reduction modulo p generalize for higher-dimensional abelian varieties, but no analogue for the Nagell-Lutz theorem is known. For genus 2 hyperelliptic curves, an algorithm that computes the rational torsion subgroup of Jacobians of hyperelliptic curves of genus 2 is proposed as an application to the height difference bound between the canonical and naive height on the Jacobian by Michael Stoll in [52, §11]. This thesis contains a detailed proof of correctness of the generalization of this algorithm to any genus. Also, the necessary objects that are required to make this generalization practical are described. Furthermore, this thesis contains a generalization of a lifting procedure used in [52, §11]. In practice, this allows us to speed up the lifting procedure.

Given the Jacobian J, most of the computations are performed on the Kummer variety $K := J/\{\pm 1\}$ corresponding to the Jacobian. Using a generalization of the Montgomery ladder for elliptic curves, one can perform multiplication-by-n on the Kummer variety, provided that certain doubling formulae and biquadratic forms are known. These doubling formulae and biquadratic forms are nontrivial to compute. Our generalization of the lifting procedure allows us to compute $J(\mathbb{Q})_{\text{tors}}$ for many curves without using these biquadratic forms. Hence, an explicit computation of the biquadratic forms is less essential compared to the original design.

A recent paper by Stoll [55] shows how to find a height difference bound on Jacobians for hyperelliptic curves of genus 3, together with an algebraic description of its corresponding Kummer variety. Also, doubling formulae and biquadratic forms that give the sum-and-difference-laws on the Kummer variety are introduced and made available on Michael Stoll's web page [51]. Developing an algorithm that computes $J(\mathbb{Q})_{\text{tors}}$ for Jacobians of hyperelliptic curves of genus 3 is a natural next step. In fact, an implementation of such an algorithm is requested by Andrew Sutherland in the workshop "Arithmetic aspects of explicit moduli problems" held in Banff, 2017 [1, final report: 3.10].

This thesis finishes the description of the quotient map $\kappa\colon J \to K$ for the special cases that are not explicitly described in [55]. Using this, we give a method to test whether the pre-image of a given point on K under κ is rational. This explicit description of κ is important because most of the actual computations are done on K. For example, the arithmetic on $J(\mathbb{Q})$ can be replaced entirely by arithmetic on $K(\mathbb{Q})$, hence we

do not do not require arithmetic on $J(\mathbb{Q})$. This is one of the strengths of the algorithm because in general, no algorithm for arithmetic on $J(k)$ is known if no rational point on $C(k)$ is known. However, we do need an implementation of the arithmetic on $\tilde{J}(\mathbb{F}_p)$, where $\tilde{J}$ is a reduced Jacobian over $\mathbb{F}_p$. By choosing particular reduced Jacobians $\tilde{J}$, we can always find a rational point $\tilde{P} \in \tilde{C}(\mathbb{F}_p)$ for the corresponding curve $\tilde{C}$, hence an algorithm for arithmetic on these $\tilde{J}$ is known.

A complete implementation of the algorithm for genus 3 hyperelliptic curves is constructed and made available via `https://github.com/bernoreitsma/g3hyptorsion`. The code is based on the file `G3Hyp.m` in [51] (containing base code for the case where C has the model $y^2 = f(x)$ where f is of odd degree) and the implementation for genus 2 hyperelliptic curves in MAGMA [4] due to Stoll.

We also applied this algorithm to 67879 genus 3 hyperelliptic curves over $\mathbb{Q}$ of low discriminant. This database is maintained by Andrew V. Sutherland and will be added to the L-functions and Modular Forms Database (LMFDB) [3]. Some example computations are showcased in this thesis.

Chapter 2 introduces preliminary theory on hyperelliptic curves, the Jacobian, and the Kummer variety. Chapter 3 discusses the strategy of the algorithm and introduces the specific background theory that is relevant for the algorithm. A complete description and proof of correctness of the algorithm is given in Chapter 4, together with a small discussion on applications of the generalization of the lifting procedure. Chapter 5 discusses the explicit formulae and algorithms that are necessary to make the algorithm work on genus 3 hyperelliptic curves. After that, results and examples of the computations on genus 3 hyperelliptic curves are discussed in Chapter 6.

2 Hyperelliptic curves, Jacobians and the Kummer variety

This chapter introduces preliminary theory on hyperelliptic curves, Jacobians, and the Kummer variety. If the reader is familiar with elliptic curves, but not very familiar with hyperelliptic curves, they are recommended to keep the case of elliptic curves in mind and note that often, the theory here is a generalization of the theory on elliptic curves.

2.1 Hyperelliptic curves

The main goals of this section are to provide a definition of hyperelliptic curves, and introduce some basic theory. We often restrict ourselves to what is relevant to this thesis. For a more elaborate introduction, we refer to [23], which is also one of the main references used in this section.

2.1.1 Hyperelliptic curves and rational points

Before we define hyperelliptic curves, we first define a suitable ambient space. Then, we define hyperelliptic curves.

Definition 2.1. Let k be a field and let $g \in \mathbb{Z}_{\geq 0}$. The *weighted projective plane* $\mathbb{P}^2_g = \mathbb{P}^2_{1,g+1,1}$ is the geometric object whose points over a given field k are elements of

$$(\mathbb{A}^3(k) \setminus \{0\})/\sim \tag{2.2}$$

where $\sim$ is the equivalence relation such that $(\rho, \eta, \zeta) \sim (\rho', \eta', \zeta')$ if and only if there exists a $\lambda \in k^\times$ such that $(\rho, \eta, \zeta) = (\lambda\rho', \lambda^{g+1}\eta', \lambda\zeta')$.

The *coordinate ring* $k[\mathbb{P}^2_g]$ over k of $\mathbb{P}^2_g$ is the ring $k[x, y, z]$ together with the grading such that x and z have degree 1, and y has degree $g + 1$. A polynomial in the coordinate ring of $\mathbb{P}^2_g$ is *homogeneous of degree* d if it consists of a combination of monomials of degree d.

For a point $(\rho, \eta, \zeta) \in \mathbb{A}^3 \setminus \{0\}$, we denote its equivalence class in $\mathbb{P}^2_g$ by $(\rho : \eta : \zeta)$.

Definition 2.3. Let k be a perfect field of characteristic $\neq 2$, and let $g \in \mathbb{Z}_{\geq 1}$. A *hyperelliptic curve of genus* g is a subvariety C of $\mathbb{P}^2_g$ defined by the equation

$$y^2 = F(x, z) := f_{2g+2}x^{2g+2} + \cdots + f_0 z^{2g+2} \tag{2.4}$$

where $F \in k[x, z]$ is squarefree and homogeneous of degree $2g + 2$.

Remark 2.5. An *elliptic curve* defined over k can be defined as a hyperelliptic curve of genus 1 that contains a k-rational point.

Indeed, C is a subvariety of $\mathbb{P}^2_g$ because the polynomial $y^2 - F(x, z)$ is homogeneous of degree $2g + 2$ in the coordinate ring of $\mathbb{P}^2_g$. The coordinate ring $k[C]$ of C is the ring $k[x, y, z]/(y^2 - F(x, z))$ with its induced grading.

Hyperelliptic curves and points on hyperelliptic curves are also often described using an affine equation for practical reasons. It is important to clarify how these two descriptions interact precisely, so we derive the affine description here. The intersection of C with the affine patch of $\mathbb{P}^2_g$ defined by $z = 1$ is the affine variety C^{aff} defined by

$$y^2 = F(x, 1) := f(x) = f_{2g+2}x^{2g+2} + \cdots + f_0. \tag{2.6}$$

Since F is squarefree, we must have that $f \in k[x]$ is squarefree and $\deg f$ is equal to $2g + 1$ or $2g + 2$. The coordinate ring $k[C^{\text{aff}}]$ of C^{aff} is then $k[x, y]/(y^2 - f(x))$ with its induced grading, i.e., $\deg(x) = 1$ and $\deg(y) = g + 1$.

The *points at infinity* $C^{\inf}$ of C consist of the intersection of C with the line $z = 0$ in $\mathbb{P}^2_g$. We observe that $C = C^{\text{aff}} \cup C^{\inf}$. If $(\rho : \zeta : \eta) \in C^{\inf}$, then $\zeta^2 = f_{2g+2}\rho^{2g+2}$, hence $C^{\inf} = \{(1 : \alpha : 0), (1 : -\alpha : 0)\}$, where $\alpha^2 = f_{2g+2}$. It follows that C has one point at infinity if $f_{2g+2} = 0$ and two points at infinity otherwise. Also, C has two k-rational points at infinity if $f_{2g+2} \in k^2 \setminus \{0\}$, where k^2 denotes the set of squares in k. The curve C contains precisely one k-rational point at infinity if $f_{2g+2} = 0$ and no k-rational points at infinity if $f_{2g+2} \notin k^2$.

Theorem 2.7. Let k be a perfect field of characteristic $\neq 2$, and let C be a hyperelliptic curve of genus g. Then, C is a smooth, geometrically irreducible curve.

Proof. Besides proving smoothness and geometric irreducibility, we also prove that C is, in fact, a curve, i.e., C has dimension 1.

First, we observe that, $\frac{\partial(y^2 - f(x))}{\partial x} = -f'(x)$ and $\frac{\partial(y^2 - f(x))}{\partial y} = 2y$, hence (using $\text{char}(k) \neq 2$) a singular point on C^{aff} must be of the form $(\alpha, 0)$, such that $f(\alpha) = f'(\alpha) = 0$. This contradicts f being squarefree. The points at infinity are nonsingular by [23, Lemma 10.1.11]. We conclude that C is smooth.

Following the strategy of [23, Lemma 10.1.2], C^{aff} is not geometrically irreducible if and only if $y^2 = f(x)$ factors as an element of $\bar{k}[x, y]$. Equivalently, $y^2 - f(x) = (y - a(x))(y - b(x))$ for some $a, b \in \bar{k}[x]$, which can only be true if $a(x) = -b(x)$, equivalently $f = -a^2$, contradicting f being squarefree. The lemma [23, Lemma 10.1.2] also proves that C^{aff} has dimension 1. We conclude using [23, Theorem 10.1.14] that C is geometrically irreducible and has dimension 1. □

Throughout this thesis, C denotes a hyperelliptic curve defined over a perfect field k of characteristic $\neq 2$, and g denotes the genus of that hyperelliptic curve. With f, we denote the polynomial defining C^{aff} in Equation (2.6), and F denotes its homogenization as described in Equation (2.4). Also, k denotes a perfect field of characteristic $\neq 2$, and $\bar{k}$ denotes its separable closure, which is also its algebraic closure since k is assumed to be perfect. Furthermore, we denote $\ell \supset k$ to be a separable field extension of k. If we consider k-rational points on a curve defined over k, we often refer to k-rational points by simply calling them *rational points* if k is clear from the context.

Many results that follow hold more generally, but we will state them for C instead. If k has characteristic 2, the defining equation 2.6 always leads to a singular curve (see the singularity conditions on points in the proof of Theorem 2.7). For hyperelliptic curves over fields of general characteristic, we refer to [23, Chapter 10].

Remark 2.8. One might wonder why a *weighted* projective plane is necessary for the homogenization of affine curves with defining equation $y^2 = f(x)$. In $\mathbb{P}^2$, for $g \in \mathbb{Z}_{\geq 1}$, homogenization would lead to the projective algebraic equation $y^2 z^{2g} = F(x, z)$. This gives the point $(0 : 1 : 0)$. By taking an affine patch defined by $y = 1$. We can observe that the partial derivatives in the coordinates x and z are both zero, hence this point is always singular. The weighted projective space is not necessary in the case of an elliptic curve. An elliptic curve can be defined by $y^2 z = F(x, z)$ where F has degree 3. Similarly using an affine patch defined by $y = 1$ and taking partial derivatives, we see check that the point at infinity $(0 : 1 : 0)$ is nonsingular in this case: The partial derivative $\frac{\partial(z - f(x))}{\partial z} = 1 - f'(x)$ evaluates to 1 at the point $(x, z) = (0, 0)$.

Definition 2.9. The *function field* $\ell(C)$ of $C \times_k \ell$ is the subfield of the field of fractions of $\ell[C]$ defined as

$$\ell(C) := \{h_1/h_2 : h_1, h_2 \in \ell[C] \text{ are homogeneous of equal degree}\}$$

An element of the function field is called a *rational function* of C over ℓ. A rational function described as the quotient h_1/h_2 with h_1 and h_2 in $\ell[x, y, z]$ is called *regular* at a point $(\rho : \zeta : \eta)$ if $h_2(\rho, \zeta, \eta) \neq 0$. For a point $P = (\rho : \zeta : \eta)$ such that $\phi = h_1/h_2$ is regular at P, the evaluation of ϕ at P is defined as $\phi(P) := h_1(\rho, \zeta, \eta)/h_2(\rho, \zeta, \eta)$. The value of $\phi(P)$ does not depend on the choice of h_1, h_2.

The following is useful to describe rational functions in an affine context.

Lemma 2.10. The function field $k(C^{\text{aff}})$ of C^{aff}, defined as the field of fractions of $k[C^{\text{aff}}]$, is isomorphic to $k(C)$.

Proof. See [23, Corollary 5.4.9]. □

2.1.2 The Galois action on hyperelliptic curves

The action of the Galois group on points on C gives an alternative definition of rational points on C, and is later also used to define an action of the Galois group on points on the Jacobian, which eventually describes rational points on the Jacobian. Let $G_k := G(\bar{k}/k)$ be the *absolute Galois group* of k. An automorphism $\sigma \in G_k$ acts on a point in $\mathbb{P}_2^g$ via its coordinates, i.e., if $P = (\rho : \zeta : \eta)$, then $\sigma(P) = (\sigma(\rho) : \sigma(\zeta) : \sigma(\eta))$.

Lemma 2.11. The following equation of sets holds.

$$\mathbb{P}_g^2(k) = \{P \in \mathbb{P}_g^2(\bar{k}) : \sigma(P) = P \text{ for all } \sigma \in G_k\}. \tag{2.12}$$

Proof. This is proven using Hilbert's Theorem 90 [47, Chapter X, Proposition 2], a proof for general (non-weighted) projective spaces is described in [23, Lemma 5.2.5]. Using that σ is an automorphism, this proof can be generalized to weighted projective spaces. □

Lemma 2.11 tells us that for fields $k \subseteq \ell \subseteq \bar{k}$, we have that ℓ-rational points are the points in $C(\bar{k})$ fixed by $\text{Gal}(\ell/k)$. In particular, we can find the smallest field ℓ for which a point $P \in \mathbb{P}_g^2(\bar{k})$ is ℓ-rational by finding the smallest field extension such that $\text{Gal}(\ell/k)$ fixes P.

2.1.3 Weierstrass points

Weierstrass points are special points that are used throughout this thesis. In essence, the existence of a rational Weierstrass point gives us a canonical representation of rational points on the Jacobian, which is also important for implementing arithmetic on the Jacobian. We use the hyperelliptic involution to define Weierstrass points because it generalizes better if one wants to work in characteristic 2.

Definition 2.13. The map $\iota\colon C \to C$ defined $(x : y : z) \mapsto (x : -y : z)$ is the *hyperelliptic involution* of C. The map $\pi\colon C \to \mathbb{P}^1$ defined by $(x : y : z) \mapsto (x : z)$ is the *quotient map* of C.

Definition 2.14. A point $P \in C$ is called a *Weierstrass point* if $\iota(P) = P$.

We see immediately that $P := (\rho : \zeta : \eta)$ is a Weierstrass point if and only if $\zeta = 0$. The Weierstrass points are also the ramification points of the quotient map.

If k is algebraically closed, C always has rational Weierstrass points. If a rational Weierstrass point exists, it is usually fixed to be at infinity (see Section 2.6). Most literature that assumes k to be algebraically closed only considers curves of odd degree due to the following observation.

Example 2.15. If $f_{2g+2} = 0$ then the point at infinity is a Weierstrass point. If $f_{2g+2} \neq 0$, then the points at infinity are not Weierstrass points. This follows immediately from the discussion of C^{inf} above.

2.2 Divisors and the Picard Group

Before we define the Jacobian, it is important to introduce the divisor group and ℓ-rational divisors. The Picard group is a group of divisors modulo an equivalence relation. The ℓ-rational equivalence classes in the Picard group correspond to ℓ-rational points on the Jacobian. This allows us to create a divisor representation of ℓ-rational points on the Jacobian. In this section, we introduce divisors and the Picard group. Creating divisor representatives for the equivalence classes in the Picard group is done in Section 2.4, after we introduced the Jacobian variety itself in Section 2.3.

2.2.1 Divisors

Definition 2.16. A *divisor* D on C is a $\mathbb{Z}$-linear combination of the form

$$D = \sum_{P \in C(\bar{k})} \alpha_P P$$

such that $\alpha_P = 0$ for all but finitely many points $P \in C(\bar{k})$. The *support* of the divisor is the set of points $P \in C(\bar{k})$ that have nonzero coefficient. For two divisors $D = \sum_{P \in C(\bar{k})} \alpha_P P$ and $D' = \sum_{P \in C(\bar{k})} \alpha'_P P$, we say that $D \geq D'$ if $\alpha_P \geq \alpha'_P$ for all $P \in C(\bar{k})$. Here, "$\geq$" clearly defines a partial order. A divisor D is called *effective* if all coefficients are nonnegative, i.e., $D \geq 0$. The *degree* of a divisor is the sum of its coefficients, i.e., $\deg(D) := \sum_{P \in C(\bar{k})} \alpha_P$.

The set of divisors is denoted by Div_C. Considering addition as operator, Div_C is a free abelian group. We denote the set of divisors of degree $d \in \mathbb{Z}$ by Div_C^d. Clearly, the degree of divisors is additive, hence Div_C^0 is a subgroup of Div_C.

Let G_k be the absolute Galois group of k. The action of G_k on Div_C is defined by its induced action on its points, i.e., if $\sigma \in G_k$, then

$$\sigma\left(\sum_{P \in C(\bar{k})} \alpha_P P\right) = \sum_{P \in C(\bar{k})} \alpha_P \sigma(P).$$

A divisor D is called k-rational if D is fixed under G_k. Clearly, adding two rational divisors results in a rational divisor. Note that this does not require all the points in the support to be rational. We demonstrate this in the following example.

Example 2.17. We will provide an example of a rational divisor D that has no rational points on C in its support. Let C be defined over $\mathbb{Q}$ such that $f_{2g+2} = -1$. Consider the divisor $D = (1 : i : 0) + (1 : -i : 0) \in \mathrm{Div}_C$ where $i^2 = -1$. We have that $i \notin \mathbb{Q}$ lives in the quadratic number field $\mathbb{Q}(i)$. Any $\sigma \in G_{\mathbb{Q}}$ fixes coordinates in $\mathbb{Q}$, and either fixes i or sends i to $-i$. In both cases, we can check that $\sigma(D) = D$, hence D is rational.

2.2.2 Principal divisors

Principal divisors are a particular kind of divisors that can be obtained by considering the roots and poles of a rational function. We consider them because they define the equivalence relation on the Picard group.

Definition 2.18. Let $P \in C(\bar{k})$, then the map $v_P \colon k[C] \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ is defined such that $v_P(h) = 0$ if P is not a root of h, and $v_P(h) = m \geq 1$ if P is a root of multiplicity m in h. We extend v_P to $k(C)^\times$ defining $v_P(h_1/h_2) = v_P(h_1) - v_P(h_2)$.

Since any element in $k(C)$ has finitely many roots and poles (poles are the zeros of the denominator), v_P is well-defined for all $P \in C(\bar{k})$. We usually denote rational functions in $k(C)$ in an affine way, i.e., since rational functions in $k(C^{\mathrm{aff}})$ using Lemma 2.10.

Definition 2.19. Let $\phi \in \bar{k}(C)^\times$. We define a *divisor of the function* ϕ to be

$$\mathrm{div}(\phi) = \sum_{P \in C(\bar{k})} v_P(\phi) \cdot P.$$

A divisor of a function is said to be a *principal divisor*. The set of principal divisors is denoted by Princ_C. The set of ℓ-rational principal divisors are denoted by $\mathrm{Princ}_C(\ell)$.

It is clear that $\mathrm{div}(\phi_1) + \mathrm{div}(\phi_2) = \mathrm{div}(\phi_1\phi_2)$ for functions $\phi_1, \phi_2 \in \bar{k}(C)^\times$. Therefore, the map $\mathrm{div}\colon \bar{k}(C)^\times \to \mathrm{Div}_C$ is a group homomorphism, hence Princ_C is a subgroup of Div_C. Subsequently, $\mathrm{Princ}_C(k)$ is a subgroup of $\mathrm{Div}_C(k)$. The degree of a principal divisor is always equal to zero [54, Lemma 4.7], so $\mathrm{Princ}_C \subseteq \mathrm{Div}_C^0$. Another important property of the map div is Galois-equivariance:

Lemma 2.20. Let $\sigma \in G_k$, let C be defined over k. For any $\phi \in \bar{k}(C)^\times$,

$$\sigma(\mathrm{div}(\phi)) = \mathrm{div}(\sigma(\phi)).$$

Proof. From [23, Lemma 7.4.14], we know that $v_P(\phi) = v_{\sigma(P)}(\sigma(\phi))$. Hence,

$$\begin{aligned}
\sigma(\mathrm{div}(\phi)) &= \sigma\left(\sum_{P \in C(\bar{k})} v_P(\phi) P\right) \\
&= \sum_{P \in C(\bar{k})} v_P(\phi)\sigma(P) \\
&= \sum_{P \in C(\bar{k})} v_{\sigma(P)}(\sigma(\phi))\sigma(P) \\
&= \sum_{P \in C(\bar{k})} v_P(\sigma(\phi)) P. \\
&= \mathrm{div}(\sigma(\phi)).
\end{aligned}$$

□

2.2.3 The Picard group

Now, we can define the Picard group using the divisor theory that is introduced before. We will introduce it shortly here, and its connection to representing rational points on the Jacobian is stated after introducing the Jacobian in Section 2.3.

Definition 2.21. The *Picard group* of C is the abelian group

$$\mathrm{Pic}_C = \mathrm{Div}_C / \mathrm{Princ}_C.$$

Two divisors are called *linearly equivalent* if they differ only by a divisor of a function, i.e., if they are in the same divisor class in Pic_C.

Recall that principal divisors have degree 0. Hence, the degree of a divisor class in Pic_C is well-defined. For $d \in \mathbb{Z}$, we denote Pic_C^d to be the divisor classes of degree d in Pic_C. We observe that Pic_C^0 is a subgroup of Pic_C.

Consider any automorphism $\sigma \in G_k$ and divisor $D \in \mathrm{Pic}_C$. By construction, we can write any divisor in $[D]$ to be $D' = D + \mathrm{div}(\phi)$ for some function $\phi \in \bar{k}(C)^\times$. It follows from Lemma 2.20 that $\sigma(D') = \sigma(D + \mathrm{div}(\phi)) = \sigma(D) + \mathrm{div}(\sigma(\phi))$. Hence, we can define a group action of G_k by setting

$$\sigma([D]) := [\sigma(D)].$$

We define the group of ℓ-rational points on Pic_C to be

$$\mathrm{Pic}_C(\ell) := \{[D] \in \mathrm{Pic}_C : \sigma([D]) = [D] \text{ for all } \sigma \in G_\ell\}.$$

Remark 2.22. Note that it is possible that a divisor class is rational, but no rational divisor in this class exists. Examples can be found in [13, Appendix: Ch. 4]. If C contains a rational point, then a rational divisor class always contains a rational divisor, also explained in [13, Ch. 4: Appendix]. Further discussion can be found in [15] and [44].

2.3 The Jacobian

The central object of study in our thesis will be the Jacobian variety corresponding to a hyperelliptic curve. Before we introduce the Jacobian, we define abelian varieties and introduce some important properties.

Definition 2.23. An abelian variety A over a field k is a projective algebraic variety over k that is also an algebraic group, i.e., there exists a group law on A that is defined by regular functions.

For a detailed introduction, we refer to [25, §A.7]. We note some relevant properties of abelian varieties here.

Observation 2.24. The following properties are satisfied for an abelian variety A defined over a field k

1. A is a smooth variety.
2. The group structure of A is abelian.
3. The set $A(k)$ of k-rational points on A forms an abelian group.

Proof. 1) See [25, §A.7.1].
2) See [25, Lemma A.7.1.3].
3) This follows from the fact that a regular function is also a rational map, and that the group law consists of regular functions. □

Elliptic curves are abelian varieties, hence there exists an abelian group law on rational points of elliptic curves, which consists of chord-and-tangent addition, see, e.g., [49, III.2]. Hyperelliptic curves C of genus $g \geq 2$ are not abelian varieties in general. Instead, we use an embedding into an abelian variety: the Jacobian of C.

Theorem 2.25. Given C/k of genus g, there exists an abelian variety over k with dimension g such that, for each field extension $\ell \supseteq k$, $J(\ell) = \mathrm{Pic}^0_C(\ell)$.

This theorem is further described in [25, §A.8].

Definition 2.26. The abelian variety J described in Theorem 2.25 is called the *Jacobian* of C.

The (geometric) dimension of the Jacobian J corresponding to a curve of genus g is equal to g [25, A.8.1.ii]. One way of defining the geometric dimension of a variety is that it is the transcendence degree of its coordinate ring. (This is already used in the proof of Theorem 2.7). Since this theory is not explicitly used in this thesis, we will simply refer for more details to [25].

The following theorem, called the *Mordell-Weil Theorem* is a foundational theorem in arithmetic geometry.

Theorem 2.27. (Mordell-Weil) For a number field $k \supseteq \mathbb{Q}$ and an abelian variety A over k, $A(k)$ is a finitely generated group.

This theorem has been proven for elliptic curves over $\mathbb{Q}$ by Louis Mordell [37], and later generalized to Jacobians of curves of higher genus by André Weil [59]. The theorem in the current form, assuming k to be any number field and A to be any abelian variety, is later proven: for a brief survey of the history of Mordell-Weil Theorem, see [12]. For an elaborate discussion, see also [25, Part C].

Remark 2.28. Using [25, A.8.1], there exists a natural embedding $C \hookrightarrow J$ that maps $P \mapsto [P - D]$, where D is a fixed divisor of degree 1. This map restricts to $C(\ell) \hookrightarrow J(\ell)$ if $D \in \mathrm{Div}_C(\ell)$. In particular, if there exists a point $P_0 \in C(\ell)$, one can choose $D = P_0$ as rational divisor.

Since the goal of our thesis is to search the rational torsion points of the Jacobian, we can use the Mordell-Weil Theorem to conclude that

Corollary 2.29. The rational torsion subgroup $J(\mathbb{Q})_{\text{tors}}$ is finite.

Note that this particular result does not need Mordell-Weil theorem to be proven, one can use height theory to show that for a bound B, only finitely many points have a height less than B, and the height of a rational torsion point is always bounded. See Theorem 3.13 and [25, Chapter B.5].

2.4 The Riemann-Roch Theorem, representing divisor classes

In order to perform arithmetic on the Jacobian, one has to find a way to represent points on J. A natural first attempt would be to observe that J is a projective variety, hence one could embed J into some projective space $\mathbb{P}^N$. One such embedding exists for $N = 4^g - 1$ [39, Chapter III]. For genus 2, such a basis is explicitly constructed in [13, §2.1].

Considering J as a projective variety using an embedding in $\mathbb{P}^{4^g-1}$ becomes difficult very quickly when larger g are considered. It is much easier to describe points on $J(k)$ as divisor classes in the Picard group using Theorem 2.25. We will construct a way to use divisors to represent a class on $\text{Pic}^0_C(k)$. For this, we use Riemann-Roch spaces and the Riemann-Roch Theorem.

Definition 2.30. Given C defined over k, we define the *Riemann-Roch Space* as the k-linear space

$$\mathcal{L}(D) = \{\phi \in \bar{k}(C)^\times : \text{div}(\phi) + D \geq 0\} \cup \{0\}.$$

Theorem 2.31. (Riemann-Roch) Let C be of genus g, defined over k. For every divisor $D \in \text{Div}_C(k)$, we have that $\dim_k \mathcal{L}(D)$ is finite. Moreover, there exists a divisor $M \in \text{Div}(k)$ such that

$$\dim_k \mathcal{L}(D) = \deg(D) - g + 1 + \dim_k \mathcal{L}(M - D).$$

The class of M is unique, it is called the *canonical class*. A divisor in the canonical class is called a *canonical divisor*.

Proof. For the proof of C defined over algebraically closed fields, we refer to [30, Theorem 2.7]. Then, a generalization to general k is described just underneath [25, Theorem A.4.2.1], using [25, Proposition A.2.2.10]. □

The Riemann-Roch Theorem was first proven for $k = \mathbb{C}$ by Bernhard Riemann [45] and Gustav Roch [46]. Later, the theorem was generalized to algebraic curves.

Recall that a divisor $D \in \text{Div}_C$ is effective if $D \geq 0$. Given $D \in \text{Div}_C(k)$, the Riemann-Roch Theorem gives us information about the space of rational functions whose corresponding principal divisors can be added to D to result in an effective divisor. This gives us information on linearly equivalent effective divisors on D. In order to create a divisor representation of points in $J(kf)$, we consider effective divisors and subtract a certain fixed divisor an appropriate number of times in order to create a divisor representation in Pic^0_C. We use the Riemann-Roch Theorem to find an effective divisor such that, when subtracting a fixed divisor, we land in Pic^0_C, and no linearly equivalent effective divisors in this form exist.

Another condition we impose on our divisor representation is that the divisor is in general position.

Definition 2.32. A divisor $D \in \text{Div}_C$ is *in general position* if it is effective and there is no point $P \in C$ such that $D \geq P + \iota P$, and, in case the degree of f is odd, the point at infinity P_∞ is not in the support of D.

In this section, we only create a divisor representation for curves C where f has odd degree. The case where f has even degree is more complicated, especially when g is odd. For genus 3, this case is treated in Section 5.2. Before we describe a divisor representation, we will make some useful observations on divisors.

Lemma 2.33. Let D and D' be divisors of C, let M be a canonical divisor.

1. If $D' \geq D$, then $\mathcal{L}(D) \subseteq \mathcal{L}(D')$.

2. If $\deg(D) < 0$, then $\mathcal{L}(D) = 0$.

3. If $D' \geq D$ and $\deg D' = \deg D + 1$, then $\dim_k \mathcal{L}(D') - \dim_k \mathcal{L}(D) \in \{0, 1\}$.

4. We have $\dim_k \mathcal{L}(M) = g$ and $\deg M = 2g - 2$.

5. If $\deg D \geq 2g - 1$, then $\dim_k \mathcal{L}(D) = \deg(D) - g + 1$.

Proof. Within this proof, $\phi \in \bar{k}(C)^\times$.

1. If $D' \geq D$, then $\operatorname{div}(\phi) + D \geq 0$ implies that $\operatorname{div}(\phi) + D' \geq 0$.

2. Recall that the degree of a principal divisor is equal to 0. Hence, $\deg(D) < 0$ implies that $D + \operatorname{div}(\phi) < 0$ for any $\phi \in \bar{k}(C)^\times$.

3. Assume $D' \geq D$ and $\deg D' = \deg D + 1$. Using the Riemann-Roch Theorem, $\dim_k \mathcal{L}(D') - \dim_k \mathcal{L}(D) = 1 - \dim_k \mathcal{L}(M - D') + \dim_k \mathcal{L}(M - D)$. Using (1), we have $-\dim_k \mathcal{L}(M - D') + \dim_k \mathcal{L}(M - D) \geq 0$ and using $D' \geq D$, we have $\dim_k \mathcal{L}(D') - \dim_k \mathcal{L}(D) \geq 0$, hence $\dim_k \mathcal{L}(D') - \dim_k \mathcal{L}(D) \in \{0, 1\}$.

4. Note that $\dim_k \mathcal{L}(0) = \dim_k(k) = 1 = 1 - g + \dim_k \mathcal{L}(M)$, hence $\dim_k \mathcal{L}(M) = g$, and using this fact, it follows that $\deg M = \dim_k \mathcal{L}(M) - 1 + g - \dim_k \mathcal{L}(0) = 2g - 2$.

5. If $\deg(D) \geq 2g - 1$, then $\deg(M - D) < 0$ using (4), hence $\dim_k \mathcal{L}(M - D) = 0$, using (2). The result follows from the Riemann-Roch Theorem.

□

Now, we are ready to introduce a divisor representation for $J(k)$ corresponding to C defined over k where f has odd degree.

Theorem 2.34. Let C be a hyperelliptic curve defined over k such that f has odd degree. Let $P_\infty \in C(k)$ be the unique point at infinity and let $Q \in J(k)$. Then, there exists a unique effective divisor $D_Q \in \operatorname{Div}_C(k)$ in general position and of minimal degree such that $Q = [D_Q - \deg(D_Q)P_\infty]$.

Proof. First, we prove the existence of an effective divisor D_Q of minimal degree, this is also written in [54, Corollary 4.14].

Let D be any divisor such that $Q = [D]$. Define $L_m = \mathcal{L}(D + mP_\infty)$ for $m \in \mathbb{Z}_{\geq 0}$. Since $\deg(D) = 0$, $L_m = \{0\}$ for $m < 0$ using (2) of Lemma 2.33, and from (3) it follows that $0 \leq \dim_k L_{m+1} - \dim_k L_m \leq 1$.

For sufficiently large m, part (5) of Lemma 2.33 implies that $\dim L_m = \deg(D + mP_\infty) - g + 1 > 0$. Hence, there exists an $n \in \mathbb{N}$ such that $\dim_k L_{n+1} - \dim_k L_n = 1$. We can now conclude that there exists a minimal n such that $\dim_k L_n = 1$. From now on within this proof, we fix this n.

Let $\phi \in L_n$. Define $D_Q = \operatorname{div}(\phi) + D + nP_\infty \geq 0$. Then, $Q = [D] = [D + \operatorname{div}(\phi)] = [D_Q - nP_\infty]$, and $\deg(D_Q) = n$. Since ϕ is unique up to scaling, D_Q is unique and of minimal degree.

To show that $D_Q \in \operatorname{Div}_C(k)$, we take an arbitrary $\sigma \in G_k$, and observe that

$$\begin{aligned}
[D_Q - nP_\infty] &= Q \\
&= \sigma(Q) && \text{because } Q \text{ is } k\text{-rational} \\
&= \sigma([D_Q - nP_\infty]) \\
&= [\sigma(D_Q - nP_\infty)] && \text{Galois-action on } \operatorname{Pic}^0_C(\bar{k})
\end{aligned}$$

Since P_∞ is rational, $Q = [\sigma(D_Q) - nP_\infty]$. Note that $\sigma(D_Q)$ is effective and in general position. Since D_Q is the unique effective divisor in general position of minimal degree such that $Q = [D_Q - nP_\infty]$ and $\deg(D_Q) = \deg(\sigma(D_Q))$, we conclude that $\sigma(D_Q) = D_Q$.

The proof that D_Q is in general position and of minimal degree can be found in [54, Lemma 4.17]. □

An important, immediate observation is that $\deg(D_Q)$ can be bounded.

Corollary 2.35. For D_Q as found in Theorem 2.34, $\deg D_Q \leq g$.

Proof. Using the Riemann-Roch Theorem, $\dim_k L_m \geq \deg(D + mP_\infty) - g + 1 = 1$ if $m = g$. Hence $n \leq g$. □

With this divisor representation, one practical observation is that applying the hyperelliptic involution to a point in the support of D_Q corresponds to negation in Pic^0_C.

Lemma 2.36. Let C be defined over k where f has odd degree. As divisors, $P + \iota(P) \sim 2P_\infty$. Hence, applying ι to D_Q corresponds to negation on J in the divisor representation given in Theorem 2.34

Proof. This is a particular case of [54, Example 4.5]. □

As an example, if $D_Q = P_1 + P_2$ in general position, and we add a point on $J(k)$ represented by the divisor $\iota(P_1)$ in general position, then we can reduce $P_1 + P_2 + \iota(P_1)$ to P_2 in the divisor representation.

2.5 Mumford representation

Provided that $\deg(f)$ is odd, we can now represent a point in $J(k)$ using a divisor on its corresponding curve C in general position of minimal degree. The next step is to find a procedure that performs arithmetic on $J(k)$. More precisely, given divisors in general position D, D' on C that represent points Q and Q' in $J(k)$, we can see that $[D + D'] = Q + Q'$, but generally $D + D'$ is not in general position, and is not of minimal degree. Therefore, a method to find a linearly equivalent divisor in general position of minimal degree is necessary. We introduce the Mumford representation, which is a way to represent divisors in general position. The Mumford representation is then used to create a procedure that performs addition as described above. Moreover, the Mumford representation is also a conveniently compact way of representing divisors in general position using polynomials.

Theorem 2.37. Let C be a hyperelliptic curve. Let D be an effective divisor on C in general position such that all points in its support are affine. Write $D = \sum_{P \in C(\bar{k})} \alpha_P P$. Define a tuple $\langle a, b \rangle$ where $a, b \in k[x]$ such that the following conditions hold:

1. The polynomial a is monic of degree $\deg D =: d$.
2. For all $P \in C^{\mathrm{aff}}$, $P \in \mathrm{Supp}(D)$ if and only if $\alpha_P > 0$. Moreover, $v_P(D)$ is the multiplicity of $x(P)$ as a root of a.
3. We have $\deg(b) < \deg(a)$, and for all P in the support of D, we have $b(x(P)) = y(P)$
4. As polynomials, $a | (f - b^2)$.

Then, there exists a bijection between the set of such polynomial tuples $\langle a, b \rangle$ and divisors D in general position.

Proof. See [54, Lemma 4.16] □

Mumford representation was first introduced by by David Mumford in [39, §3, page 3.25]. In order to perform arithmetic on $J(k)$, one first takes two divisors in general position D and D' and adds them together to a divisor in general position (but not of minimal degree). This is called *Cantor's composition algorithm*. Then, one finds the linearly equivalent divisor in general position that is of minimal degree, so that we get the unique divisor in general position as described in Theorem 2.34. This step is called *Cantor's reduction algorithm*. These algorithms work very well in the case where f has odd degree.

Algorithm 2.38. Let C be defined over k of genus g such that f has odd degree. Let D_1, D_2' be k-rational divisors on C in general position of minimal degree, and let $\langle a_1, b_1\rangle, \langle a_2, b_2\rangle$ be the Mumford representations of D_1 and D_2, respectively. Then, we can compute the divisor D in general position of minimal degree such that $D \in [D_1 + D_2]$ as follows.

1. Composition: Find a divisor in $[D_1 + D_2]$ in general position.
   1.1. Set $d := \gcd(a_1, a_2, b_1 + b_2)$
   1.2. Set $a := a_1 a_2 / d^2$
   1.3. Set b to be the unique polynomial of degree $< \deg(a)$, such that $b \equiv b_1 \mod a_1/d$, $b \equiv b_2 \mod a_2/d$, $f \equiv b^2 \mod a$
2. Reduction: Reduce the divisor with Mumford representation $\langle a, b\rangle$ to minimal degree.
   Repeat the following steps while $\deg(a) > g$:
   2.1. Write $f - \lambda ac$ such that $\lambda \in k^\times$, $c \in k[x]$ monic.
   2.2. Replace a by c
   2.3. Replace b by the remainder of $-b \mod a$

We conclude that the divisor D corresponding to the Mumford representation of $\langle a, b\rangle$ is in general position, of minimal degree, and $D - \deg(D)P_\infty \sim D_1 + D_2 \in \mathrm{Pic}^0_C(k)$.

Proof. See [54, Theorem 4.18]. □

One can also implement addition of points on the Jacobian in the more general case, where f has even degree and/or where k may have characteristic 2. A detailed description can be found in [23, §10.3 - §10.4]. In the case where C has odd genus and f has even degree, it is not always possible to find an obvious addition algorithm. Section 5.2 describes the cases where generalizations of Cantor's algorithms can be implemented for the case where $g = 3$.

2.6 Transformations

This section introduces isomorphisms on hyperelliptic curves. Since we do explicit computations with many objects corresponding to a hyperelliptic curve, it is useful to use isomorphisms to fix certain *models*: one can think of a hyperelliptic curve as an isomorphism class, and a model as a curve defined by a specific algebraic equation of the form (2.4). Throughout this thesis, we will refer to hyperelliptic curves assuming a fixed model, but isomorphisms are sometimes applied to obtain a desired model.

2.6.1 Isomorphisms of hyperelliptic curves

Let C_1 and C_2 be hyperelliptic curves defined over k. An *isomorphism over ℓ of hyperelliptic curves* $C_1 \to C_2$ is a map $\phi\colon C_1 \to C_2$ that is an isomorphism of varieties defined over ℓ. Instead of introducing the notion of isomorphisms of varieties, we refer to [49, §I.3]. This chapter gives an elementary introduction to rational maps, using rational functions as defined in Definition 2.9, and the notion of a regular function at a point P as described in the same definition. We will rewrite the alternative definition of a rational map and regularity in [49, Remark I.3.2] to fit the definition of a *weighted* projective variety: This only changes a few homogeneity conditions.

Remark 2.39. The alternative definition of a rational map in [49, Remark I.3.2] can be written for hyperelliptic curves in $\mathbb{P}^2_g$ as follows: Let C_1 and C_2 be hyperelliptic curves, both of genus g, defined over k, defined by the equations $y^2 - F_1(x, z)$ and $y^2 - F_2(x, z)$, respectively. A rational map $\phi\colon C_1 \to C_2$ is a map of the form $\phi(x, y, z) = [\phi_1(x, y, z), \phi_2(x, y, z), \phi_3(x, y, z)]$ where $\phi_i \in \bar{k}[C]$ are homogeneous (in the weighted sense) polynomials in $k[C_1]$, such that the following conditions hold:

(i) $\deg(\phi_2) = (g+1)\deg(\phi_1) = (g+1)\deg(\phi_3)$,

(ii) for every h in the ideal $(y^2 - F_2(x,z))$, $h(\phi_1(x,y,z), \phi_2(x,y,z), \phi_3(x,y,z)) \in (y^2 - F_1(x,y,z))$.

Such a rational map is regular at $P \in C_1$ if there exist homogeneous (in the $\mathbb{P}^2_g$-weighted sense) polynomials $\varphi_1, \varphi_2, \varphi_3 \in \bar{k}(C)$ such that the following conditions hold:

(i) $\deg(\varphi_2) = (g+1)\deg(\varphi_1) = (g+1)\deg(\varphi_3)$,

(ii) $\phi_i\varphi_j \equiv \phi_j\varphi_i \mod y^2 - F_1(x,z)$ for all $1 \leq i,j \leq 3$,

(iii) $\varphi_i(P) \neq 0$ for some $1 \leq i \leq 3$.

2.6.2 An explicit description of isomorphisms of hyperelliptic curves

There is a general description for isomorphisms of hyperelliptic curves defined over k.

Theorem 2.40. Let C_1, C_2 be hyperelliptic curves over k. Any isomorphism of hyperelliptic curves $\phi\colon C_1 \to C_2$ defined over $\ell \supseteq k$ can be described as

$$(x : y : z) \mapsto (ax + bz : ey : cx + dz)$$

where

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\ell)$$

and $0 \neq e \in \ell^\times$.

Proof. Apply [23, Theorem 10.2.1], and note that if we consider curves defined by $y^2 + h(x)y = f(x)$ where $h = 0$, then the polynomial t in the cited theorem is also equal to 0. Furthermore, the maps that do not fix the point at infinity must map a point $(x_0, y_0) \in C_1^{\mathrm{aff}}$ to infinity. It can be checked that these maps are described by $(x : y : z) \mapsto (z : ey : z - x_1)$. □

Corollary 2.41. An isomorphism of hyperelliptic curves sends Weierstrass points to Weierstrass points (and hence, non-Weierstrass points to non-Weierstrass points.)

Proof. This follows immediately from Theorem 2.40 and noting that ι sends y to $-y$, but fixes the coordinates x and z. □

2.6.3 Isomorphisms between Jacobians induced by isomorphisms between hyperelliptic curves.

The search for the torsion structure of $J(k)$ is made easier by observing that the group structure of $J(k)$ is preserved under an isomorphism of hyperelliptic curves. This produces the main motivation to apply isomorphisms in this thesis.

Theorem 2.42. Let C_1 and C_2 be hyperelliptic curves defined over k. Let $\phi\colon C_1 \to C_2$ be an isomorphism of hyperelliptic curves over $\ell \supseteq k$. Then, the induced map $\phi_*\colon \mathrm{Pic}^0_{C_1}(\ell) \to \mathrm{Pic}^0_{C_1}(\ell)$ defined by mapping a divisor P to $\phi(P)$ is a group isomorphism.

Proof. Apply [23, Corollary 8.3.10] and observe that such an induced change of coordinates identifies divisors that are fixed under actions of the absolute Galois group G_k. □

Corollary 2.43. If C_1 and C_2 are two hyperelliptic curves that are isomorphic over k, then for their corresponding Jacobians J_1, J_2, it follows that $J_1(k) \cong J_2(k)$.

Lemma 2.44. Let C_1 be a hyperelliptic curve defined over k. Then, C_1 contains a rational Weierstrass point if and only if C_1 is isomorphic over k to a curve C_2 that is defined by $y^2 = f(x)$, such that f has odd degree.

Proof. If C_1 has odd degree, then the statement is trivial, using that P_∞ is a Weierstrass point. Otherwise, if C_1 has no rational Weierstrass points, then Corollary 2.41 implies no isomorphism to C_2 exists such that C_2 does have a rational Weierstrass point, so in particular f cannot have odd degree. In the case that C_1 has a rational Weierstrass point, then an isomorphism that maps this rational Weierstrass point to infinity has a codomain with a Weierstrass point at infinity using Corollary 2.41. It follows that the polynomial f corresponding to C_2^{aff} has odd degree. This isomorphism exists by the following explicit construction. We can use the change of coordinates corresponding to the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & -x_1 \end{pmatrix}. \tag{2.45}$$

in the notation of Theorem 2.40, where $(x_1, 0)$ is a rational Weierstrass point in $C_1(k)$ □

Within this thesis, it is useful to apply certain isomorphisms to fix a model of a hyperelliptic curve. One example where we can use this is found in Theorem 2.34: Recall from Example 2.15 that P_∞ is a Weierstrass point. In the divisor representation $[D_Q - P_\infty] = Q \in J(k)$, one can replace P_∞ with any Weierstrass point instead. We can fix a rational Weierstrass point at infinity by using a change of coordinates that maps the point to infinity.

Another application is the *quadratic twist* of a curve C. At a certain point in the algorithm, we want to reduce the discriminant of f, here defined over $\mathbb{Z}$, for optimization. (See Remark 3.16.) Hence, if the coefficients of f share a factor c such that c is a square in k, then one can apply the isomorphism $(x : ey : z)$ where $e = 1/\sqrt{c} \in \mathbb{Q}$, that is defined over $\mathbb{Q}$.

2.7 The Kummer variety

Recall from Section 2.4 that the Jacobian variety is a very complicated variety to work with. This is motivation to construct procedures that describe points using divisor representations and perform arithmetic in terms of Mumford representations in Sections 2.4 and 2.5, respectively. For operations such as reduction and Hensel lifting (described later in Sections 3.2 and 3.3), it is better to work on a projective variety. To avoid working on the very complicated variety J, we introduce its corresponding Kummer variety. It turns out that much of the coordinates of J in $\mathbb{P}^{4^g-1}$ are simply necessary to encode the "sign" of a point, i.e., to distinguish between P and $-P$ on J. By identifying group inverses on J, we essentially stop tracking a large amount of data that conveys only a small amount of information.

2.7.1 Definition, general properties

Definition 2.46. The *Kummer variety* is defined as $K := J/\{-1\}$. We denote the corresponding quotient map by $\kappa\colon J \to K$.

A reader that is familiar with elliptic curves may note the analogy of the Kummer variety in the following way: An elliptic curve E is an abelian variety, and the quotient map $\pi\colon E \to \mathbb{P}^1$ that maps P to $x(P)$ loses the distinction between P and $-P$. by only looking at the x-coordinate. For an elliptic curve $\mathbb{P}^1 = K$ is the Kummer variety.

The construction of the Kummer variety is based on theory that we will not introduce here. Instead, we will summarize important properties in one theorem. For this theorem, and also later in the thesis, we use the following notational convention: For a given abelian group G and an integer $n \in \mathbb{Z}_{\geq 1}$, we denote $G[n]$ to be the subgroup of G that consists of points of order n, which is called the n-torsion subgroup.

Theorem 2.47. The Kummer variety K satisfies the following conditions.

1. K is an algebraic variety.

2. A point $R \in K$ is singular if and only if $R \in \kappa(J[2])$.

3. We have that κ is $2:1$ except at points of order 2 in J, where it is injective.

4. K can be embedded in $\mathbb{P}^{2^g-1}$ such that the image of this embedding is defined by quartic relations.

5. If we fix the embedding $K \subseteq \mathbb{P}^{2^g-1}$, then the map $\kappa\colon J \to K \subseteq \mathbb{P}^{2^g-1}$ is a rational map.

Proof. For (1) and (2), we refer to [38]. (See also [8, §4.8] for the complex case). We also use this to conclude that we can embed K into $\mathbb{P}^{2^g-1}$. Property (3) follows by construction: κ is a degree 2 map that ramifies on $J[2]$. Properties (4) and (5) follow from [40, Proposition 3.1]. □

From now on, we denote the Kummer variety of a Jacobian by K, and its corresponding quotient map is denoted by $\kappa\colon J \to K$. Since K can be embedded into $\mathbb{P}^{2^g-1}$, we treat K as a fixed subvariety of $\mathbb{P}^{2^g-1}$. When considering κ, we refer to a fixed map $\kappa\colon J \to K \subseteq \mathbb{P}^{2^g-1}$ such that $\kappa(J)$ corresponds to K as fixed in $\mathbb{P}^{2^g-1}$ as above. Throughout this thesis, we always work with a coordinate system in K that maps $0 \in J$ to $\kappa(0) = (0 : \ldots : 0 : 1)$. This is called the *origin of the Kummer*.

An explicit construction of the defining equations of K for genus $g \geq 2$ is nontrivial. Moreover, for C over k algebraically closed, C always contains k-rational Weierstrass points, so f can be assumed to be of odd degree using Lemma 2.44. In an arithmetic context, we often work with k not algebraically closed, hence for our purpose, we may not assume f has odd degree. For genus 2, a generic construction is given in [13, §3.1]. For the corresponding map κ, see, e.g., [21]. For genus 3, [55, §2] develops the defining equations of K in the general case. For a summary, see also Section 5.3. The corresponding map κ is also given in [55, §2], except in a few special cases. This thesis describes these special cases in Section 5.4.

2.7.2 Pseudo-arithmetic on the Kummer

Cantor's Algorithm as described in Algorithm 2.38 allows us to perform arithmetic on the Jacobian J if f has odd degree. In this thesis, most of the procedures are done on the Kummer variety. Since K identifies inverses on J by definition, the group structure is lost, but enough information remains such that we can replace the necessary arithmetic of J by certain steps on K.

For a given J, $n \in \mathbb{Z}$ the *multiplication-by-n-map* is the map $[n]\colon J \to J$ such that

$$[n]P\colon P \mapsto \underbrace{P + \cdots + P}_{n \text{ times}}.$$

Clearly, $[-1] \circ [n] = [n] \circ [-1]$ because J has an abelian group structure, so we can define multiplication-by-n (denoted here by $[[n]]$) on K such that the following diagram commutes:

$$\begin{array}{ccc} J & \xrightarrow{[n]} & J \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} \\ K & \xrightarrow{[[n]]} & K \end{array} \tag{2.48}$$

Now, the goal is to find a procedure that takes $R \in K$ as input, and gives $[[n]]R$ as output.

The first ingredient is a procedure that doubles a point: given R, the output is $[[2]]R$. For genus 2 [19] and 3 [55, §7], doubling formulae are developed to do this: explicit polynomials δ_i, homogeneous and of degree 4, are developed such that the following holds: given $R \in K$,

$$(\delta_1(R) : \ldots : \delta_k(R)) = [[2]]R.$$

If we assume a scaling $(r_1 : \ldots : r_{2^g}) = R$ such that the first nonzero coordinate is equal to 1, then $\delta_i \in \mathbb{Z}[f_1, \ldots f_d][r_1, \ldots, r_{2^g}]$.

Remark 2.49. Doubling formulae are also used to develop a height difference bound for genus 2 and 3. This is discussed in Section 3.4.

The second ingredient, pseudo-addition, tries to replicate addition of two points on J. Replicating addition on K is not completely possible because we lost information. Suppose that we are only given $\kappa(Q_1)$ and $\kappa(Q_2)$ on K (we do not know $Q_1, Q_2 \in J$). Then, it is impossible to determine $\kappa(Q_1 + Q_2)$. The best we can do, given this information, is to find an unordered pair $\{\kappa(Q_1 + Q_2), \kappa(Q_1 - Q_2)\}$. Hence, addition is not possible on K. However, *pseudo-addition* requires a bit more input: if we get $\kappa(Q_1), \kappa(Q_2), \kappa(Q_1 - Q_2)$ as input, we can determine $\kappa(Q_1 + Q_2)$ as output.

Consider $\kappa(Q_1), \kappa(Q_2) \in K$, denote $\kappa := (\kappa_1 : \ldots : \kappa_{2^g})$. For genus 2 [13, §3.4] and genus 3 [55, §8], biquadratic forms B_{ij} are developed such that, projectively, for all $0 \leq i \leq j \leq 2^g$,

$$B_{ij}(\kappa(Q_1), \kappa(Q_2)) = \kappa_i(Q_1 + Q_2)\kappa_j(Q_1 - Q_2) + \kappa_i(Q_1 - Q_2)\kappa_j(Q_1 + Q_2). \tag{2.50}$$

If we normalize the coordinates $\kappa(Q)$ such that the first nonzero coordinate is equal to 1, then the coefficients of B_{ij} are in $\mathbb{Z}[f_0, \ldots f_{2g+2}]$. For $1 \leq i, j \leq 2^g$,

$$B_{jj}(\kappa(Q_1), \kappa(Q_2)) = 2\kappa_j(Q_1 - Q_2)\kappa_j(Q_1 + Q_2) \tag{2.51}$$

and

$$\kappa_j(Q_1 - Q_2)B_{ij}(\kappa(Q_1), \kappa(Q_2)) = \kappa_i(Q_1 + Q_2)\kappa_j(Q_1 - Q_2)^2 + \kappa_j(Q_1 - Q_2)\kappa_i(Q_1 - Q_2)\kappa_j(Q_1 + Q_2). \tag{2.52}$$

From (2.51) and (2.52), we see that

$$2\kappa_j(Q_1 - Q_2)B_{ij}(\kappa(Q_1), \kappa(Q_2)) - \kappa_i(Q_1 - Q_2)B_{jj}(\kappa(Q_1), \kappa(Q_2)) = 2\kappa_i(Q_1 + Q_2)\kappa_j(Q_1 - Q_2)^2. \tag{2.53}$$

Now, we perform pseudo-addition as follows: fix j such that $\kappa_j(Q_1 - Q_2) \neq 0$. Then, compute $2\kappa_i(Q_1 + Q_2)\kappa_j(Q_1 - Q_2)^2$ by substituting the input $\kappa(Q_1), \kappa(Q_2), \kappa(Q_1 - Q_2)$ in the left-hand side of Equation (2.53) for each $1 \leq i \leq 2^g$. This produces coordinates for $\kappa(Q_1 + Q_2)$.

We conclude that, if doubling formulae and biquadratic forms are explicitly known for C, then one can perform the procedures that are given as the following functions.

- `Double`: Given input $\kappa(Q)$ for $Q \in J(k)$, the output is $[[2]]\kappa(Q) = \kappa([2]Q)$.
- `PseudoAdd`: Given input $\kappa(Q_1), \kappa(Q_2), \kappa(Q_1 - Q_2)$ for $Q_1, Q_2 \in J(k)$, the output is $\kappa(Q_1 + Q_2)$.

This leads to the following procedure for computing $[[n]]R$.

Algorithm 2.54. Multiplication-by-n on the Kummer
Input: R where $R \in K(k)$, $n \in \mathbb{Z}$
Output: $[[n]]R$
Requirements: doubling formulae and biquadratic Forms for K as described above.

1. $\boldsymbol{x} = (0 : \ldots : 0 : 1)$, $\boldsymbol{y} = R, \boldsymbol{z} = R$. Set $m := |n|$.
2. Repeat the following steps while $m \neq 0$
   2.1. If m is odd, then set $\boldsymbol{x} := \texttt{PseudoAdd}(\boldsymbol{x}, \boldsymbol{z}, \boldsymbol{y})$. Else, set $\boldsymbol{y} := \texttt{PseudoAdd}(\boldsymbol{y}, \boldsymbol{z}, \boldsymbol{x})$,
   2.2. Set $\boldsymbol{z} := \texttt{Double}(\boldsymbol{z})$,.
   2.3. Set $m := \left\lfloor \frac{m}{2} \right\rfloor$.
3. Conclude: $\boldsymbol{x} = [[m]]R$.

proof of correctness. In order to prove the correctness of the algorithm, we first note that since n is finite, the iteration terminates.

We can see this iteration as a deconstruction of m into its binary expansion, where each iteration treats and deletes the most right coefficient. Denote

$$m = m_1 + 2m_2 + \cdots 2^r m_r$$

for some $r \in \mathbb{N}$, $m_i \in \{0, 1\}$ for $0 \leq i \leq r$. Let $Q \in \kappa^{-1}(R) \subset J$. Then, after the algorithm, we want to arrive at

$$\boldsymbol{x} = \kappa([m]Q = [m_1]Q + [2m_2]Q + \cdots + [2^r m_r]Q),$$

using that $[-1]$ commutes with $[n]$ on J. Examining step 2.3, in the i-th iteration, m is odd if $m_i = 1$ and m is even if $m_i = 0$.

The variable $\boldsymbol{z}$ governs the order of magnitude we consider, hence the iteration starts with $\boldsymbol{z} = \kappa([1]Q)$, and doubles $\boldsymbol{z}$ after each iteration on K. Before the first iteration, if $i = 0$,

$$\begin{aligned}
\boldsymbol{z} &= \kappa([2^i]Q) = R \\
\boldsymbol{x} &= \kappa([m_1]Q \cdots [m_i]Q) = \kappa(0) \\
\boldsymbol{y} &= \kappa([2^i]Q - [m_1]Q \cdots [m_i]Q) = R.
\end{aligned}$$

Given that the above is true before the i-th iteration, then for the $i+1$-th iteration, clearly $\boldsymbol{z} = \kappa([2^{i+1}]Q) = \texttt{Double}(\kappa([2^i]Q))$. In the case m is odd, $m_{i+1} = 1$, hence

$$\boldsymbol{x} = \kappa([m_1]Q \cdots [m_{i+1}]Q) = \texttt{PseudoAdd}(\boldsymbol{x}, \boldsymbol{z}, \boldsymbol{y}).$$

In the case m is even, $m_{i+1} = 0$, hence

$$\boldsymbol{y} = \kappa([2^{i+1}]Q - [m_1]Q - \cdots [m_i]Q) = \kappa([2^i]Q - [m_1]Q - \cdots - [m_i]Q + [2^{i+1}]Q) = \texttt{PseudoAdd}(\boldsymbol{y}, \boldsymbol{z}, \boldsymbol{x})$$

By induction, we conclude that, after iteration $i = r$,

$$\boldsymbol{x} = \kappa([m_1]Q \cdots [m_r]Q) = \kappa([m]Q) = [[m]]Q \in K.$$

□

Remark 2.55. For elliptic curves, Algorithm 2.54 is equivalent to the *Montgomery Ladder*, introduced by Peter L. Montgomery, finding many applications in cryptography [36]. This procedure turns out to be very useful for cryptographic applications. For genus 2, fast arithmetic on the Kummer surface has also proven useful for cryptographic applications. See for example [9].

Explicit defining equations for K, the biquadratic forms and the doubling formulae have been computed for genus 2 and 3. For hyperelliptic curves of genus 4, this is work in progress by Ludwig Fürst.

2.8 The action of the 2-torsion subgroup on K

In some parts of the theory used throughout this thesis, it is useful to examine the action of points of order 2 on K. Most of the theory is not directly considered or applied in this thesis, but several results use this theory as referenced, so it is useful to briefly introduce some of the results here. First, the doubling formulae δ that yield the function `Double` on K as described in Section 2.7 must be invariant under $J[2]$, see, e.g., [55, Lemma 7.1]. In Section 4.7, the problem of trying to find a way to compute the pre-image of the doubling function comes up. The difference between two points in this pre-image is a 2-torsion point, and some of the theory introduced here is used for a theoretical strategy for "halving a point", that is, given $R \in K$, we try to find $R' \in K$ such that $2R' = R$.

For elliptic curves, an introduction can be found in [42, §2], for genus 2 hyperelliptic curves, we refer to [52, §3-5] and for genus 3 hyperelliptic curves, we refer to [55, §5-7].

Recall that the 2-torsion subgroup is denoted by $J[2]$. We consider the action of $T \in J[2]$ on $K \subset \mathbb{P}^{2^g-1}$. Let $R \in K$ and fix Q be one point in $\kappa^{-1}(R)$ (The other point in $\kappa^{-1}(R)$ is then $-Q$ if $Q \neq -Q$). Then, for $T \in J[2]$,

$$\kappa(Q+T) = \kappa(-Q-T) = \kappa(-Q+T),$$

hence we can define the action of T on K to be the map $R \mapsto \kappa(Q+T)$, and this action is well-defined. If we denote $R = (r_1 : \ldots : r_{2^g})$, then we can represent this action as a linear projective transformation in $\mathrm{PGL}(2^g, \bar{k})$. We take the coordinates $(r_1 : \ldots : r_{2^g})$ and examine homogeneous forms in $\bar{k}[r_1, \ldots, r_{2^g}]$. Now, we can define an action of $J[2]$ on such homogeneous forms as the induced action of $J[2]$ on the coordinates $r_1, \ldots, r_{2^g}$. For a point $R \in K$ and a form $y \in \bar{k}[r_1, \ldots, r_{2^g}]$, we denote the action of $T \in J[2]$ by $T \cdot R$ and $T \cdot y$, respectively.

Let k^{spl} be the splitting field of f, and let R be the set of roots of f in k^{spl}. Let $\{S, S'\}$ be a partition of R into two subsets, both of cardinality $g+1$. Note that, in the case of $g = 3$, these two subsets correspond to all *even* 2-torsion points, as introduced in [55, §5].

Lemma 2.56. For C, J, K where C has genus $g = 1, 2$ or 3, there exists a quadratic form $y_{\{S,S'\}} \in k^{\mathrm{spl}}[r_1, \ldots r_{2^g}]$ such that for any $T \in J[2]$

$$T \cdot y_{\{S,S'\}} = \epsilon(T, T') y_{\{S,S'\}}$$

where $\epsilon(T, T') = \pm 1$ is the *Weil pairing* of T and T'. (The Weil pairing is described in [42, §2], [52, §3], [55, §5] for genus 1,2,3, respectively)

proof. For genus 1, this is constructed in the proof of [42, Proposition 2.1]. For genus 2, see [52, §4], and for genus 3, see [55, §6]. □

We can now express these quadratic forms in terms of δ_i.

Theorem 2.57. For C of genus $g = 1, 2, 3$, there exist constants $b_{\{S,S'\}}$ such that for $R \in K$, and the δ_i-polynomials as introduced in Section 2.7,

$$y_{\{S,S'\}}(R)^2 = \sum_{i=1}^{2^g} b_{\{S,S'\}} \delta_i(R) \tag{2.58}$$

proof. This follows from the fact that $y^2_{\{S,S'\}}$ is a quartic form in $k^{\mathrm{spl}}[r_1, \ldots, r_{2^g}]$ that is T-invariant due to Lemma 2.56, together with the observation that the δ_i form a basis for the linear space of quartic, T-invariant forms in $k^{\mathrm{spl}}[r_1, \ldots r_{2^g}]$: this result is given in the proof of [42, Proposition 2.1] for genus 1, [52, Lemma 5.1] for genus 2, and [55, Lemma 7.1] for genus 3. □

There is also an explicit way of computing r_i^2 and $r_i r_j$ in terms of $y_{\{S,S'\}}$.

Theorem 2.59. For C of genus $g = 1, 2, 3$, There exists constants $a_{i,j,\{S,S'\}}$ such that for $R := (r_1 : \ldots : r_{2^g}) \in K$,

$$r_i r_j = \sum_{\{S,S'\}} a_{i,j,\{S,S'\}} y_{\{S,S'\}}(R) \tag{2.60}$$

and

$$r_i^2 = \sum_{\{S,S'\}} a_{i,i,\{S,S'\}} y_{\{S,S'\}}(R). \tag{2.61}$$

proof. See [42, Proposition 2.1] for genus 1, and note that, in the notation of the referenced material, a similar argument for x_i^2 also holds for $x_1 x_2$ because $x_1 x_2 \in \mathrm{Sym}^2 V$, where V is the vector space of k-linear forms in x_1, x_2 as used in the proof of the referenced proposition. See [52, Formula 10.3, 10.4] for genus 2, and [55, Lemma 6.8] for genus 3. □

3 The theory of computing $J(\mathbb{Q})_{\text{tors}}$.

3.1 Goal and motivation

In the previous chapter, we have introduced the preliminary theory on hyperelliptic curves, its Jacobian and the Kummer variety. We will now focus more on the strategy involved in finding $J(\mathbb{Q})_{\text{tors}}$ if C is defined over $\mathbb{Q}$. Before we go into the more detailed preliminaries for the algorithm to compute this object, we will motivate this goal by providing some reasons why one may be interested in the $J(\mathbb{Q})_{\text{tors}}$.

Arithmetic geometry uses geometry to find rational solutions of certain polynomial equations over number fields. Solving such polynomial equations is, in general, difficult. For many types of algebraic equations over $\mathbb{Q}$, an algorithm to compute the solution, or supply a description of their structure, is still an open problem.

We apply the Mordell-Weil Theorem (Theorem 2.27), for an abelian variety A defined over $\mathbb{Q}$, and observe that

$$A(\mathbb{Q}) \cong A(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$$

in which $r \in \mathbb{Z}_{\geq 0}$ is called the *rank* of A. Suppose $r = 0$, then $A(\mathbb{Q}) = A(\mathbb{Q})_{\text{tors}}$, hence finding $A(\mathbb{Q})_{\text{tors}}$ gives us a method to find $A(\mathbb{Q})$, i.e., all solutions to a defining set of polynomial equations of A over $\mathbb{Q}$.

For example, an elliptic curve E is an abelian variety, and if we find generators for $E(\mathbb{Q})$, a complete set of solutions of the curve equation over $\mathbb{Q}$ can be described. A general method for finding the rank of an elliptic curve is an open problem [49, VIII.10], but for specific cases, one can compute the rank of an elliptic curve, see for example [49, X.6]. In the case where $r = 0$, we have $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}}$, and we can solve the defining equation of E over $\mathbb{Q}$ by only computing $E(\mathbb{Q})_{\text{tors}}$.

Hyperelliptic curves of genus $g \geq 2$ are not, in general, abelian varieties. However, it is proven (in particular) in [17] that C defined over $\mathbb{Q}$ of genus ≥ 2 contain finitely many rational points. In order to find these points explicitly, we often inject a point $P \in C(\mathbb{Q})$ into its Jacobian $J(\mathbb{Q})$. (See Remark 2.28). Similarly to the elliptic curves case, if the rank of J can be proven to be 0, one can completely determine $C(\mathbb{Q})$ using $J(\mathbb{Q})_{\text{tors}}$. If $r > 0$, then there are infinitely many points on $J(\mathbb{Q})$, hence it is harder to find the points that have a pre-image in $C(\mathbb{Q})$ precisely. One attempt to decide if certain curves have any rational point, the *Mordell-Weil sieve*, requires the computation of generators for $J(\mathbb{Q})$, hence in particular also the generators for $J(\mathbb{Q})_{\text{tors}}$ [11]. Provided that the rank is strictly less than the genus of C, another method method to find rational points uses p-adic integrals, the *Chabauty-Coleman* method. This also uses the fact that these integrals vanish on torsion points, see for example [34].

The rank of an abelian variety is, in general, difficult to compute, even for elliptic curves. The *Birch and Swinnerton-Dyer conjecture* [7] is a conjecture that would imply a method for computing the rank of $E(\mathbb{Q})$ [50, Proposition 2.2]. This conjecture is an open problem, and in fact one of the seven Millennium problems of the Clay Mathematics Institute [2]. In §3 of the problem description written by Andrew Wiles in the given reference, a generalization to higher dimensional abelian varieties can be found. Also, a refinement is discussed that directly considers the order of the rational torsion subgroup of an abelian variety, see also [58]. To gather numerical evidence for the full conjecture, we need to compute $\#A(\mathbb{Q})_{\text{tors}}$.

On elliptic curves, all possible rational torsion structures are determined in [33]. For Jacobians of hyperelliptic curves of genus $g \geq 2$, this is still an open problem. Some research has been done by producing Jacobians with large torsion points (see [29], [43]). Clearly, having a decisive method that computes the rational torsion structure (even if this is done implicitly, i.e., without computing generators) can give insight into what rational torsion structures exist in higher dimensional abelian varieties.

The strategy for computing $J(\mathbb{Q})_{\text{tors}}$ can be summarized as follows. One first uses reduction modulo p for certain primes p to find a small set of reduced points that could potentially lift to a rational torsion point on J. This a generalization of the approach in elliptic curves described in [49, §VII.2, VII.3]. Then, one applies Hensel lifting on the Kummer variety to find a rational lift of the reduced point. We use the theory of heights to determine a precision of this Hensel lifting at which we can conclude whether a reduced point lifts to $J(\mathbb{Q})_{\text{tors}}$ or not.

3.2 Reduction

The first step in finding the Jacobian is to look at the reduction of its Jacobian. Essentially, we reduce points on J modulo a suitable prime number p to a corresponding Jacobian $\tilde{J}$ over $\mathbb{F}_p$. This interacts well with the curve C, and gives us useful information on the rational torsion subgroup of $J(\mathbb{Q})$.

3.2.1 A brief introduction to p-adics

Reduction can be defined over $\mathbb{Q}$, but we introduce this theory in the setting of p-adic numbers. This is necessary because we will use Hensel lifting, a p-adic analytic method, in Section 3.3. Usually, p-adics are defined by introducing the p-adic valuation. A valuation is a function defined on a field k that behaves logarithmitically in the sense that multiplication of elements in k corresponds to addition on the image under the valuation. A valuation can be used to define an absolute value on k. Instead of thoroughly introducing notions such as local fields and valuations, we refer to two sources. For an introduction of the theory involved that is closely related to this thesis, we refer to [54, §3]. For a more general and elaborate introduction, we refer to [35, Chapter 7].

Definition 3.1. Let $a \in \mathbb{Z}$ and p be a prime number. The *p-adic valuation* $v_p(a)$ is the valuation defined by

$$v_p(a) = \begin{cases} \infty & \text{if } a = 0 \\ \max\{n : p^n | a\} & \text{otherwise.} \end{cases}$$

Using that v_p is a valuation, we can extend it to $\mathbb{Q}$. Let us say $q := a/b \in \mathbb{Q}$, then we can define $v_p(q) := v_p(a) - v_p(b)$.

Now, we define the p-adic absolute value.

Definition 3.2. For a prime number p, the p-adic absolute value is the absolute value $\|\cdot\|_p \colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ that is defined by

$$\|q\|_p = \begin{cases} 0 & \text{if } q = 0 \\ p^{-v_p(q)} & \text{if } q \neq 0. \end{cases}$$

An absolute value induces a metric, which induces a topology. Similarly to the real numbers $\mathbb{R} \supset \mathbb{Q}$, the *$p$-adic numbers* are the topological completion $\mathbb{Q}_p \supset \mathbb{Q}$ with respect to the topology induced by $\|\cdot\|_p$. One can then extend v_p, hence $\|\cdot\|_p$ to $\mathbb{Q}_p$. A construction is described in [35, Chapter 7]. A point $\alpha \in \mathbb{Q}_p$ can be approximated by the series $\cdots \alpha_{-1}p^{-1} + \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$ such that $\alpha_i \in \mathbb{Z}$ and $0 \leq \alpha_i < p$. The ring of *p-adic integers* $\mathbb{Z}_p$ is the subring $\{a \in \mathbb{Q}_p : v_p(a) \geq 0\}$. If $\alpha \in \mathbb{Z}_p$, then $\alpha_i = 0$ for all $i < 0$ (i.e., $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$). For $\mathbb{Q}$, all absolute values are equivalent to the real absolute value denoted by $\|\cdot\|_\infty$ or $\|\cdot\|_p$ for a prime p. This is Ostrowski's theorem, see [35, Theorem 7.12].

3.2.2 $\mathbb{Q}_p$-rational curves and reduction modulo p

Definition 3.3. Let C be defined over $\mathbb{Q}_p$ such that F has coefficients in $\mathbb{Z}_p$. Then, its *reduction modulo p* is the curve $\tilde{C}$ defined by $y^2 = \tilde{F}(x, z)$, where $\tilde{F} \in \mathbb{Z}_p[x, z]$ is obtained by reducing the coefficients of F modulo p.

Its corresponding *reduction map*, $\rho_{C,p} \colon C(\mathbb{Q}_p) \to \tilde{C}(\mathbb{F}_p)$ maps a point $P \in C$ to its reduction modulo p in the following way. Let P be represented by coordinates $(\rho : \eta : \zeta)$ in the weighted projective plane $\mathbb{P}^2_g$ such that $\rho, \eta, \zeta \in \mathbb{Z}_p$ and at least one of ρ, η, ζ is a unit. Then, we map P to $\tilde{C}$ by reducing its coordinates to $(\tilde{\rho} : \tilde{\eta} : \tilde{\zeta})$.

If, for a prime p, the corresponding reduced curve $\tilde{C}$ is nonsingular, then $\tilde{C}$ is a hyperelliptic curve. In this case, p is called a *prime of good reduction for p*. If p is not a prime of good reduction for C, then p is called a *prime of bad reduction for C*. Using Section 2.1, clearly $\tilde{C}$ is singular if and only if $\tilde{F}$ has repeated

roots, or $p = 2$. Hence, p is a prime of bad reduction for C if and only if $p|2\text{Disc}(F)$. It follows immediately that there are only finitely many primes of bad reduction for C.

Now, we will introduce reduction on $J(\mathbb{Q}_p)$, and show that reduction on J interacts with reduction on C in a nice way.

Theorem 3.4. Let p be a prime of good reduction of C. Let $\tilde{C}$ be the reduced curve corresponding to C and p. Let $\tilde{J}$ be the Jacobian (defined over $\mathbb{F}_p$) of $\tilde{C}$. Then, there exists a reduction map $\rho_{J,p}\colon J(\mathbb{Q}_p) \to \tilde{J}(\mathbb{F}_p)$ that is a group homomorphism. If $C(\mathbb{Q}_p)$ is nonempty, consider the embedding $j\colon C \hookrightarrow J$ introduced in Remark 2.28 for a fixed base point $P_0 \in C(\mathbb{Q}_p)$, and the embedding $\tilde{j}\colon \tilde{C} \hookrightarrow \tilde{J}$ for the base point $\tilde{P}_0$. Then, the following diagram commutes:

$$\begin{array}{ccc} C(\mathbb{Q}_p) & \xrightarrow{j} & J(\mathbb{Q}_p) \\ \downarrow{\scriptstyle \rho_{C,p}} & & \downarrow{\scriptstyle \rho_{J,p}} \\ \tilde{C}(\mathbb{F}_p) & \xrightarrow{\tilde{j}} & \tilde{J}(\mathbb{F}_p) \end{array}$$

proof. From [54, Lemma 4.20], we show this by noting that we can extend $\rho_{C,p}$ to a group homomorphism on $\text{Div}_C(\mathbb{Q}_p)$ by linearity. Note that the degree is fixed under $\rho_{C,p}$. Given a function $h = h_1/h_2 \in \bar{\mathbb{Q}}_p(C)$, we can see for $i \in \{1, 2\}$ that the roots and poles of h map to roots and poles of $\tilde{h_1}/\tilde{h_2}$ under $\rho_{J,p}$ with corresponding multiplicities. Hence, principal divisors map to principal divisors under reduction, so $\rho_{J,p}$ is a well-defined group homomorphism. The commutativity of the diagram follows by construction. □

Note that if $C(\mathbb{Q}_p) = \emptyset$, then the commutative diagram is vacuously true. Hence, for any C and prime of good reduction p, reducing modulo p and considering the corresponding Jacobian commutes with considering J and then reducing modulo p.

3.2.3 Reduction on the torsion subgroup

Now that we have introduced reduction modulo p, we will introduce theory that gives us further information on $J(\mathbb{Q})_{\text{tors}}$.

Theorem 3.5. Let p be a prime of good reduction for C defined over $\mathbb{Q}_p$. For any integer m coprime to p, the restriction of $\rho_{J,p}$ to $J(\mathbb{Q}_p)[m]$ is injective.

proof. See [25, Theorem C.1.4]. The proof is given in Section C.2 of the given reference. □

Now, the following procedure gives us a lot of insight on $J(\mathbb{Q})_{\text{tors}}$. From now on, for a given prime q and finite abelian group G, we consider the q-part of G to be the subgroup of G consisting of points of order q^n such that $n \in \mathbb{Z}_{\geq 0}$, i.e. the q-part of G is the q-Sylow subgroup of G.

1. Select a few primes of good reduction for C.
2. Determine a finite set S of primes q such that the q-part of $\tilde{J}(\mathbb{F}_p)$ is nontrivial for a certain number of primes $p \neq q$. For each such q, we compute the largest subgroup G_q that is contained in the q-parts of all $\tilde{J}(\mathbb{F}_p)$ considered where $p \neq q$. Using Theorem 3.5, we then conclude that $J(\mathbb{Q})_{\text{tors}} \subseteq \cap_{q \in S} G_q =: G$.

In step 2, we consider $\tilde{J}(\mathbb{F}_p)$. If we have $\tilde{C}(\mathbb{F}_p) \neq \emptyset$, then using the commutative diagram in Theorem 3.4 and the discussion in Section 2.5, one can consider $\tilde{J}(\mathbb{F}_p)$ and perform arithmetic using Mumford representation. Hence, one can determine $\tilde{J}(\mathbb{F}_p)$. A weaker method is to simply look at $\#\tilde{J}(\mathbb{F}_p)$. For hyperelliptic curves of genus 2, a simple combinatorial approach [13, §8.2] gives

$$\#\tilde{J}(\mathbb{F}_p) = \frac{1}{2}\#\tilde{C}(\mathbb{F}_{p^2}) + \frac{1}{2}(\#\tilde{C}(\mathbb{F}_p))^2 - p.$$

For higher genus, counting formulae are constructed using Frobenius endomorphisms [5, Corollary 5.70].

Example 3.6. Let

$$C\colon y^2 = x^7 - 4.$$

The discriminant of $x^7 - 4$ is $2^{12} \cdot 7^7$, hence we avoid the bad primes 2 and 7. (In fact, 2 is *always* a bad prime when using the form $y^2 = f(x)$.) Since f has odd degree, $\tilde{f}$, the polynomial with reduced coefficients modulo a prime p, has odd degree, so arithmetic is implemented for each Jacobian $\tilde{J}$ reduced modulo a prime of good reduction.

We compute that $\tilde{J}(\mathbb{F}_{11}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/688\mathbb{Z}$. Also, $\tilde{J}(\mathbb{F}_{29})) \cong \mathbb{Z}/26957\mathbb{Z}$. Note that $688 = 2^4 \cdot 43$, and $26957 = 7 \cdot 3851$. We can see that no nontrivial group can embed into both $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/688\mathbb{Z}$ and $\mathbb{Z}/26957\mathbb{Z}$, so we conclude using Theorem 3.5 that $J(\mathbb{Q})_{\text{tors}}$ is trivial.

Example 3.7. This example shows why we prefer to use the group structure on reduced Jacobians instead of just counting points. Let

$$C\colon y^2 = x^8 + 2x^7 + 3x^6 + 4x^5 + 9x^4 + 8x^3 + 7x^2 + 2x + 1.$$

Let p be a prime of good reduction for C. Since $f_8 = 1$ is always a square in $\mathbb{F}_p$, arithmetic is implemented on any reduced $\tilde{J}$ by fixing one such point, following from the discussion in Section 2.5. The primes of bad reduction for C are 2, 3 and 13177. We examine the reduced Jacobians modulo the good primes 5 and 7 and observe that

$$\tilde{J}(\mathbb{F}_5) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$$
$$\tilde{J}(\mathbb{F}_7) \cong \mathbb{Z}/666\mathbb{Z}.$$

Using Theorem 3.5, we conclude that $J(\mathbb{Q})_{\text{tors}}$ is a subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. It is easily observed that $J(\mathbb{Q})[2]$ is trivial (this will be discussed in Remark 4.19). Had we not been able to consider the group structure of the two reduced Jacobians, then we would merely know that $\#\tilde{J}(\mathbb{F}_5) = 180$, $\#\tilde{J}(\mathbb{F}_7) = 666$, hence also points of order 9 would still have to be considered.

In fact, a point of order 3 shows up on all reduced Jacobians. This leads us to believe that there might, in fact, be a point of order 3 in $J(\mathbb{Q})_{\text{tors}}$. Therefore, we focus on approximating the pre-image of the $\rho_{J,p}$ in $J(\mathbb{Q}_p)$ in Section 3.3. In this case, if $p \neq 3$, then Theorem 3.5 tells us that a reduced point has as unique pre-image in $J(\mathbb{Q}_p)[3]$. This is called the *lift* of a reduced point.

3.3 Hensel Lifting

Using Section 3.2, we have a (usually small) finite abelian group G such that $J(\mathbb{Q})_{\text{tors}}$ must be isomorphic to a subgroup of G. We know from Theorem 3.5 that, given a reduced point $\tilde{Q}$ of order m on $\tilde{J}(\mathbb{F}_p)$ for a prime of good reduction p that is coprime to m, we have a unique pre-image on $\rho_{J,p}$ in $J(\mathbb{Q}_p)_{\text{tors}}$. Hence, the core question we need to ask is whether $\rho_{J,p}^{-1}(\tilde{J}(\mathbb{F}_p))$ is in $J(\mathbb{Q})_{\text{tors}} \subseteq J(\mathbb{Q}_p)_{\text{tors}}$.

As discussed in Section 3.2, we can write $\alpha \in \mathbb{Z}_p$ as

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$$

where $\alpha_i \in \mathbb{Z}$ such that $0 \leq \alpha_i < p$. Using the p-adic absolute value, a rational approximation of α of p-adic precision $O(p^n)$, where $n \in \mathbb{Z}_{\geq 0}$, consists of the first n terms of this formal power series.

The absolute value $\|\cdot\|_p$ produces a norm on vector spaces $\mathbb{Q}_p^d$ for $d \in \mathbb{Z}_{\geq 0}$, hence we can use some p-adic analytic strategies to do this rational approximation. A point is on an affine variety if it solves a system of polynomial equations. Since a reduced point modulo p in $\mathbb{F}_p^d$ satisfies these equations up to precision $O(p)$, we can use Newton iteration p-adically. This approach is called *Hensel's Lemma*. We refer to [14] for general results. Since we work on projective varieties, we need to find affine patches to work with coordinates in the vector space $\mathbb{Q}_p^d$. Another remark is that in our situation, we do not have to check the *existence* of a unique root that we approximate: we simply know that by Theorem 3.5.

We now consider $J(\mathbb{Q}_p)$ as an object in p-adic analysis.

Lemma 3.8. The group $J(\mathbb{Q}_p)$ is a p-adic abelian Lie group.

proof. By [10, III, §8, Corollary 2]. we check that $J(\mathbb{Q}_p)$ is a topological group that is locally analytic around $0 \in J(\mathbb{Q}_p)$. This follows from the construction of the p-adic topology on J, see [32]. □

Since $J \subseteq \mathbb{P}^{4^g-1}$ is a coordinate system that is too complicated to work with in practice (at least for genus $g \geq 3$), we perform the lifting procedure on $K \subseteq \mathbb{P}^{2^g-1}$. The precise method is proven in Lemma 4.5. For this lemma, we first need to find any lift. In other words, given an affine patch K^{aff} of K, and any point $R \in K^{\text{aff}}(\mathbb{Z}/p^n\mathbb{Z})$ such that there exists a lift of R in $K(\mathbb{Q}_p)$, we need to find a point $R' \in K^{\text{aff}}(\mathbb{Z}/p^{2n}\mathbb{Z})$ such that in $\mathbb{Q}_p^{2^g-1}$, $R \equiv R' \mod p^n$. If $D_K(R)$ is the Jacobian matrix of K^{aff} evaluated at R, and $K_{\text{eq}}(R)$ is the vector of equations of K^{aff} evaluated at R, and v is a solution to the linear system $D_K(R)v = K_{\text{eq}}(R)$ up to $O(p^{2n})$, then we can take $R' = R - v$ using Newton iteration. If R is nonsingular, or equivalently R does not come from a point of order 2 on $J(\mathbb{Q}_p)$ (see Theorem 2.47), and R is a p-adic approximation of its unique lift up to $O(p^n)$, then this system is always solvable, using the assumption that a lift of R always exists.

Given *any* lift, Lemma 4.5 yields a p-adic approximation to precision p^{2n} for $\kappa(Q)$, where $Q \in J(\mathbb{Q}_p)_{\text{tors}}$ is the unique lift, i.e., $\rho_{J,p}^{-1}(\tilde{Q})$.

Example 3.9. In Example 3.7, we considered the curve

$$C\colon y^2 = x^8 + 2x^7 + 3x^6 + 4x^5 + 9x^4 + 8x^3 + 7x^2 + 2x + 1,$$

and collected evidence that there might be a point of order 3 in $J(\mathbb{Q})_{\text{tors}}$ because such a point shows up on all reduced Jacobians we considered. We pick $p = 17$ because the 3-part of $\tilde{J}(\mathbb{F}_{17})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. We map the reduced point $\tilde{Q}$ of order 3 to the reduced Kummer variety. If its lift $Q \in J(\mathbb{Q}_p)$ is indeed in $J(\mathbb{Q})$, then $\kappa(Q) \in K(\mathbb{Q})$. After a few iterations of the Hensel lifting, we can check whether the coordinates define a point on $K(\mathbb{Q})$. Indeed, after computing the power series up to p^4, we arrive at a point in $K(\mathbb{Q})$ such that $[[3]]R = \kappa(0)$, and we check that $\kappa^{-1}(Q) \subseteq J(\mathbb{Q})_{\text{tors}}$. Using theory introduced in Chapter 5, we can find a point Q in $J(\mathbb{Q})$ represented by the divisor class $[2(0,-1) - 2P_{\infty,1}]$ where $(0,-1) \in C^{\text{aff}}$ and $P_{\infty,1} := (1:1:0)$.

Note that this approach does not always work! The approximation we used is not guaranteed to terminate. In fact, a rational lift of a reduced point may not exist at all. Section 3.4 introduces the theory of heights on J: using the height bound for rational torsion points, we can determine a termination point for the Hensel lifting introduced in this section such that we are sure that the rational coordinates of this approximation is a "last candidate" that may lift. Hence, if this point is not a rational lift, we can conclude that no rational lift exists.

3.4 Heights

The theory of heights is used to find a point at which we can terminate our p-adic approximation using Hensel lifting and be certain we have not missed any rational torsion points. The height gives us a measure of the arithmetic complexity of a point on an abelian variety with respect to a rational map to a projective space. Most of the literature defines heights over a number field $k \supset \mathbb{Q}$. Since we are specifically interested in heights of points over $\mathbb{Q}$, we restrict our definitions to $\mathbb{Q}$. The main reference used in this section is [25, Chapter B].

We can define the height function on projective spaces. In the context of abelian varieties that have, by definition, a map to projective space, this is often called the *naive height*. Recall that $\|\cdot\|_\infty$ is the usual (real) absolute value.

Definition 3.10. Let $d \in \mathbb{Z}_{\geq 1}$. Let $P := (x_0 : \ldots : x_d) \in \mathbb{P}^d(\mathbb{Q})$ with $x_0, \ldots, x_d \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_d) = 1$. Then, the *naive height* $H\colon \mathbb{P}^d(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ is defined by mapping P to

$$H(P) := \max(\|x_0\|_\infty, \ldots, \|x_d\|_\infty).$$

Furthermore, the *logarithmic naive height* is defined by

$$h(P) := \log H(P).$$

By simply considering all possible coordinates, we can immediately observe that for a given $B > 0$, the set

$$\{R \in \mathbb{P}^d(\mathbb{Q}) : H(R) < B\}$$

is finite.

Since the lifting procedure discussed in Section 3.3 takes place on K instead of J, we define the height of a point Q in $J(\mathbb{Q})$ using its image on $K(\mathbb{Q})$, which is a generalization of [49, VIII.6], noting that κ is surjective by construction and a rational map to $K \subseteq \mathbb{P}^{2^g-1}$, using Theorem 2.47.

Definition 3.11. For $Q \in J(\mathbb{Q})$, we define the height relative to κ of Q to be the height function $H_\kappa \colon J(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ defined by $H_\kappa(Q) := H(\kappa(Q))$. Again, we say that the logarithmic height relative to κ is $h_\kappa(Q) := \log H_\kappa(Q)$.

Since our work with heights is always considered on K, we simply refer to H_κ and h_κ by $H, h \colon J(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ respectively. It follows from [25, Theorem B.3.2(d)] that heights defined by rational functions only differ up to a constant. We now define the *canonical height*. The canonical height function is well-defined using Theorem [25, Corollary B.3.4] together with the fact that κ is a symmetric function, meaning $\kappa(Q) = \kappa(-Q)$ for all $Q \in J(\mathbb{Q})$.

Definition 3.12. We define the *canonical height* to be the map $J(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ defined by

$$\hat{H}(Q) = \lim_{n \to \infty} \frac{h([n]Q)}{n^2}.$$

Similarly to earlier definitions, we define $\hat{h}(Q) := \log \hat{H}(Q)$.

The canonical height has several interesting and useful properties.

Theorem 3.13. (Néron–Tate) For $Q \in J(\mathbb{Q})$, the following properties are satisfied.

1. $\hat{h}([n]Q) = n^2 \hat{h}(Q)$ for all $n \in \mathbb{Z}$.
2. $\hat{h}(Q) = 0$ if and only if $Q \in J(\mathbb{Q})_{\text{tors}}$.
3. The set $\{Q \in J(\mathbb{Q}) : \hat{h}(Q) \leq B\}$ is finite for any constant $B \geq 0$.
4. The height difference $|\hat{h}(Q) - h(Q)|$ is bounded.

proof. For (1), see [25, Theorem B.5.1]. (2) follows from [25, Proposition B.5.3], (3) follows from [25, Corollary B.5.4.1], and (4) follows from [25, Theorem B.5.5]. □

Suppose that we can explicitly compute the height difference bound in (4), i.e., suppose we find a $\beta \geq 0$ such that

$$|\hat{h}(Q) - h(Q)| < \beta \tag{3.14}$$

for all $Q \in J(\mathbb{Q})$. In particular, by (2), $h(Q) < \beta$ for $Q \in J(\mathbb{Q})_{\text{tors}}$. The strategy to compute $J(\mathbb{Q})_{\text{tors}}$ is then as follows: Hensel lifting as described in Section 3.3 can be performed for arbitrary finite p-adic precision. Given a certain approximation $\tilde{Q}$, we can embed all possible lifts in a 2^g-dimensional integer lattice L. Using LLL-reduction, we can obtain a necessary condition for the shortest vector of L to correspond to a lift that has projective height less than β. This is all described in detail in Section 4.4.

For genus 1, 2 and 3, a method for computing the height bound is found by decomposing the difference between the naive height and the canonical height into local components (see [21, Theorem 4]), and using the relations in Theorem 2.57 and Theorem 2.59 to obtain estimates for these bounds. For genus 2, this is described in [52], and for genus 3, this is described in [55].

Theorem 3.15. Let $g \in \{2, 3\}$. Define

$$\beta = \begin{cases} 2^{4/3}|\lambda|^{-2}|\mathrm{disc}(f)|^{1/3}c_\infty^{-1/3} & \text{if } g = 2 \\ 2^2|\mathrm{disc}(f)|c_\infty^{-1/3} & \text{if } g = 3 \end{cases}$$

where c_∞ is the *height constant at infinity*. Then, for all $Q \in J(\mathbb{Q})_{\mathrm{tors}}$, we have $H(Q) < \beta$.

proof. For genus 2, see [52, Corollary 8.2]. For genus 3, see [55, Corollary 10.3]. □

We call β as in Theorem 3.15 the *torsion height bound*. For genus $g = 1, 2, 3$, there is an iterative method to estimate the height constant at infinity c_∞. This is described in [42, §4], [41, §16] and [55, Lemma 10.5] for genus 1, 2 and 3 respectively. This iterative method makes use of the quadratic form $y_{S,S'}$ and the relations as given in (2.58) and (2.61). Recall that for a partition $\{S, S'\}$ of the roots of f there exist coordinates $a_{i,j,\{S,S'\}}, b_{\{S,S'\}}$ such that

$$r_i^2 = \sum_{\{S,S'\}} a_{i,i\{S,S'\}} y_{\{S,S'\}}(R).$$

and

$$y_{\{S,S'\}}(R)^2 = \sum_{i=1}^{2^g} b_{\{S,S'\}}\delta_i(R)$$

where $R := (r_1 : \ldots : r_{2^g}) \in K$ is scaled such that first nonzero coordinate of R is equal to 1. We introduce the function

$$\begin{aligned} \varphi\colon \mathbb{C}^{2^g} &\to \mathbb{C}^{2^g} \\ R &\mapsto \left(\sqrt{\sum_{\{S,S'\}} |a_{i,i,\{S,S'\}}| \sqrt{\sum_{j=1}^{k+1} |b_{\{S,S'\},j}| r_j}} \right)_{1 \le i \le 2^g}. \end{aligned}$$

It is proven by the aforementioned sources that the sequence

$$c_n := \frac{4^n}{4^n - 1} \log(\|\phi^{\circ n}(1, 1)\|)$$

converges to a limit $\tilde{c}$ such that $c_\infty \le \tilde{c}$, where c_∞ is the height constant of c at infinity. This allows us to estimate c_∞, and hence gives a complete torsion height bound β via Theorem 3.15.

Remark 3.16. One could use quadratic twists defined over k as described in Section 2.6 to reduce the discriminant of F such that $F \in \mathbb{Z}[x, z]$. This gives a refinement of the height bound β.

4 A generalized algorithm for finding $J(\mathbb{Q})_{\mathbf{tors}}$.

4.1 Description and required procedures

In this chapter, we give a complete description and proof of the algorithm that computes the rational torsion subgroup of a Jacobian of a hyperelliptic curves. We identify all objects and procedures that are required to carry out this algorithm. The original design of the algorithm can be found in [52, §11]. This chapter generalizes the algorithm to general genus, gives a proof of correctness and also generalizes the lifting procedure slightly. The input of the algorithm is the definition of the curve C, and its output is the torsion structure of $J(\mathbb{Q})$ and explicit generators. Without a unique, explicit representation of points on $J(\mathbb{Q})$, one can still describe the torsion structure implicitly. This is discussed at the appropriate parts within the chapter.

We fix a hyperelliptic curve C of genus $g \in \mathbb{Z}_{\geq 1}$ defined over $\mathbb{Q}$, and we assume a model of the form $y^2 = f(x)$ where f has coefficients in $\mathbb{Z}$. Using changes of coordinates described in Section 2.6, we can always find such a model. We denote the Jacobian of C by J, and we fix an embedding of its Kummer variety K in $\mathbb{P}^{2^g-1}$, together with a corresponding quotient map $\kappa\colon J \to K \subseteq \mathbb{P}^{2^g-1}$.

The strategy of the algorithm can be described as follows: using reduction modulo good primes p, one can identify a finite amount of potential reduced points of finite order. Then, using Hensel lifting on K, one can lift these points in $J(\mathbb{Q}_p)$. Finally, we use the torsion height bound to decide whether such a reduced point lifts to $J(\mathbb{Q}) \subset J(\mathbb{Q}_p)$ or not.

The nontrivial procedures that are required are:

- An implementation of the group law on $\tilde{J}(\mathbb{F}_p)$ for primes of good reduction p.
- Equations for $K \subseteq \mathbb{P}^{2^g-1}$; an explicit description of $\kappa\colon J \to K$
- A way to compute $\kappa^{-1}(R) \subseteq J(\mathbb{Q})$ for $R \in K(\mathbb{Q})$.
- Doubling formulae; biquadratic forms that allow us to use sum-and-difference laws on K as described in Section 2.7.
- A way to compute a height bound β for $J(\mathbb{Q})_{\mathrm{tors}}$.

Remark 4.1. If one is only interested in the torsion *structure* of $J(\mathbb{Q})$, one can simply check *whether* $\kappa^{-1}(R) \subset J(\mathbb{Q})$. No explicit computations on $J(\mathbb{Q})$ are needed to compute its torsion structure.

4.2 Checking whether reduced points lift

The central, most challenging part of the algorithm is to check whether a reduced point lifts or not. More specifically, given a prime of good reduction p and a point $\tilde{Q} \in \tilde{J}(\mathbb{F}_p)$ of order m coprime to p, we know, using Theorem 3.5, that there exists a unique lift $Q \in J(\mathbb{Q}_p)[m]$ such that $\rho_{J,p}(Q) = \tilde{Q}$. This algorithm decides whether $Q \in J(\mathbb{Q}) \subseteq J(\mathbb{Q}_p)$. Also, if $Q \in J(\mathbb{Q})$, we will try to compute Q, but do not distinguish between Q and $-Q$ for the following reason:

Since we ultimately search for generators of $J(\mathbb{Q})[m]$, arbitrarily selecting one point from Q and $-Q$ suffices, there is no need to precisely distinguish which point is the actual lift of $\tilde{Q}$. This allows us to perform the actual computations on the Kummer variety. Instead of lifting $\tilde{Q}$ to Q on $J(\mathbb{Q}_p)$, we consider $\tilde{\kappa}(\tilde{Q}) := \tilde{R}$, where $\tilde{\kappa}\colon \tilde{J}(\mathbb{F}_p) \to K(\mathbb{Z}/p\mathbb{Z})$. We search for a lift R of $\tilde{R}$ such that $[[m]]R = \kappa(0)$. If such a lift exists, we have $\kappa^{-1}(R) = \{Q, -Q\}$. The following algorithm uses this strategy to determine whether Q is a point in $J(\mathbb{Q}) \subseteq J(\mathbb{Q}_p)$ or not, and if $Q \in J(\mathbb{Q})$, we return Q or $-Q$.

Algorithm 4.2. Lifting Torsion Points
Given a point $\tilde{Q} \in J(\mathbb{F}_p)$ of order $m > 2$, a height bound β such that $H(Q) < \beta$ for any $Q \in J(\mathbb{Q})_{tors}$, and an integer N such that $p^N \geq 2^{(2^g+g)}\beta^2$, this algorithm determines whether the point $\tilde{Q}$ lifts to a point $Q \in J(\mathbb{Q})_{tors} \subseteq J(\mathbb{Q}_p)_{tors}$, and computes Q or $-Q$ in the case where $Q \in J(\mathbb{Q})_{tors}$.

1. Choose $M = 1 + am$ such that $M \not\equiv 1 \mod p$
2. Let $\tilde{R}_0$ be $\tilde{\kappa}(\tilde{Q})$ considered on an affine patch in $\mathbb{A}^{2^g}(\mathbb{Z}/p\mathbb{Z})$ normalized such that the first nonzero coordinate is equal to 1. Set $r = 1$, $n = 0$.
3. While $r < N$, repeat the following steps:
   3.1. Replace r by $\min\{2r, N\}$.
   3.2. Let $\tilde{R}'_n$ be any lifting of $\tilde{R}_n$ in $\mathbb{A}^{2^g}(\mathbb{Z}/p^r\mathbb{Z})$.
   3.3. Set $\tilde{R}_{n+1} = \frac{1}{M-1}(M\tilde{R}'_n - [[M]]\tilde{R}'_n)$, where $M\tilde{R}'_n$ is obtained by multiplying the coordinates of $\tilde{R}'_n$ by M.
   3.4. Replace n by $n + 1$.
4. Now, consider $\tilde{R}_n =: (\tilde{r}_1 : \ldots : \tilde{r}_{2^g})$ in $K(\mathbb{Z}/p^N\mathbb{Z})$ again. Let $(r_1, \ldots, r_{2^g}) \in \mathbb{Z}^{2^g}$ be such that its coordinates reduce to $(\tilde{r}_1, \ldots, \tilde{r}_{2^g})$ modulo p^N and $0 \leq r_i < p^N$. Let L be the lattice generated by $(r_1, \ldots, r_{2^g})$ and $p^N e_1, \ldots, p^N e_{2^g}$, where e_i are the standard basis vectors in $\mathbb{Z}^{2^g}$. Let R' be the first basis vector of an LLL-reduced basis of L. Now, set R to be the point in $\mathbb{P}^{2^g-1}(\mathbb{Q})$ whose coordinates are the coordinates of R'.
5. If $R \notin K(\mathbb{Q})$ or $H(R) > B$, conclude "$\tilde{Q}$ does not lift to $J(\mathbb{Q})_{\text{tors}}$".
6. If $[[m]]R$ is not the origin of $K(\mathbb{Q})$, conclude "$\tilde{Q}$ does not lift to $J(\mathbb{Q})_{\text{tors}}$".
7. If $\kappa^{-1}(R) \subseteq J(\mathbb{Q})$, conclude "$\tilde{Q}$ lifts to $J(\mathbb{Q})_{\text{tors}}$" and return $\kappa^{-1}(R)$. Otherwise conclude "$\tilde{Q}$ does not lift to $J(\mathbb{Q})_{\text{tors}}$".

The first goal of this chapter is to prove the correctness of the algorithm. This is done using results that are proven in the upcoming sections.

Theorem 4.3. Algorithm 4.2 terminates and returns the expected output as described in the algorithm.

proof. It is clear to see that the algorithm terminates. The proof of correctness of the output follows from a combination of Theorem 4.4, Theorem 4.12 and Proposition 4.16 as proven in the next sections. □

4.3 The lifting procedure

This section will prove that the lifting procedure as described in step 3 of Algorithm 4.2 lifts to the m-torsion point we want to approximate.

Theorem 4.4. After step 3 of Algorithm 4.2, $\tilde{R}_n$ is the unique m-torsion point in $K(\mathbb{Z}/p^N\mathbb{Z})$ that reduces to $\kappa(\tilde{Q})$.

In order to prove Theorem 4.4, we first prove that the approximation we use in step 3.3 approximates Q with m-torsion lifts to the required p-adic precision p^N. Recall from Lemma 3.8 that $J(\mathbb{Q}_p)$ is a p-adic abelian Lie group, whose topology is the local product topology: a neighborhood of a point $Q \in J(\mathbb{Q}_p)$ is a neighborhood U of Q contained in an affine space. see [32, §6], and the p-adic topology on $\mathbb{A}^d(\mathbb{Q}_p) = \mathbb{Q}_p^d$ for a given $d \in \mathbb{Z}_{\geq 1}$ is induced by the norm

$$\|Q\|_p = \max(\|q_1\|_p, \ldots, \|q_d\|_p),$$

where $Q = (q_1, \ldots, q_d) \in \mathbb{Q}_p^d$ [28, §2].

Lemma 4.5. Let $Q \in J(\mathbb{Q}_p)$ be a torsion point of order m, not divisible by p. Given $n \in \mathbb{N}$, let $\phi\colon J \to \mathbb{A}^n$ be a rational, differentiable map defined over $\mathbb{Q}_p$ that is a p-adic immersion near Q, and let $a \in \mathbb{Z}$. If $U \subseteq J(\mathbb{Q}_p)$ is a neighborhood of Q, then for any $Q' \in U$, the following identity holds:

$$\phi([1+am]Q') - \phi(Q) = (1+am)(\phi(Q') - \phi(Q)) + O(\|\phi(Q') - \phi(Q)\|_p^2). \tag{4.6}$$

Intuitively, one can interpret ϕ as a map providing local affine coordinates of Q, in such a way that we can find a best linear approximation of the multiplication-by-$(1+am)$-map in a p-adic sense.

proof. For the proof, we use $M := 1 + am$, hence $[M]Q = Q$. By [10, Chapter III, §2.2] the differential of the multiplication-by-M-map $[M]$ is scalar multiplication on the tangent space.

Let us define $[[M]]$ to be the map that makes the following diagram commute.

$$\begin{array}{ccc} J(\mathbb{Q}_p) & \xrightarrow{[M]} & J(\mathbb{Q}_p) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ \phi(J(\mathbb{Q}_p)) & \xrightarrow{[[M]]} & \phi(J(\mathbb{Q}_p)) \end{array} \tag{4.7}$$

Near Q, the map $[[M]] = \phi \circ [M] \circ \phi^{-1}$ is well-defined because ϕ is an immersion, hence locally injective. Note that since ϕ is a rational mapping, we have that $\phi(J(\mathbb{Q}_p))$ consists of the $\mathbb{Q}_p$-rational points on a variety over $\mathbb{Q}_p$. Since ϕ maps to $\mathbb{A}^n$, it is an affine variety.

To arrive at the approximation described in the lemma, we want to prove that the differential of $[[M]]$ at $\phi(Q)$ is scalar multiplication by M. For p-adic manifolds A and B and a differentiable map $h\colon A \to B$ and $Q \in J$, we now denote $T_h(Q)$ to be the differential of h around Q. In this notation,

$$\begin{aligned} T_{[[M]]}(\phi(Q)) &= T_{\phi\circ[M]\circ\phi^{-1}}(\phi(Q)) \\ &= T_\phi([M]Q) \circ T_{[M]}(Q) \circ T_{\phi^{-1}}(\phi(Q)) \\ &= T_\phi(Q) \circ T_{[M]}(Q) \circ T_{\phi^{-1}}(\phi(Q)). \end{aligned}$$

Let $v \in T_{\phi(J(\mathbb{Q}_p))}$, Then, using linearity and composition laws,

$$\begin{aligned} T_{[[M]]}(\phi(Q))(v) &= T_\phi(Q) \circ T_{[M]}(Q) \circ T_{\phi^{-1}}(\phi(Q))(v) \\ &= (T_\phi(Q) \circ (M \cdot T_{\phi^{-1}}(\phi(Q)))(v)) \\ &= M \cdot (T_\phi(Q) \circ T_{\phi^{-1}}(\phi(Q)))(v)) \\ &= M \cdot v \end{aligned}$$

Note that $[[M]]$ is a map from the $\mathbb{Q}_p$-rational points of an affine variety $\phi(J)$ to itself. Hence, its differential $T_{[[M]]}(\phi(P))$ is the best linear approximation of $[[M]]$ around $\phi(P)$ with respect to the p-adic metric, i.e., it consists of the linear terms of the Taylor expansion of $[[M]]$ around $\phi(Q)$.

Let Q' be p-adically near Q. Then. using that ϕ is an immersion, $\phi(Q')$ is p-adically near $\phi(Q)$, hence

$$[[1+am]]\phi(Q') - [[1+am]]\phi(Q) = (1+am) \cdot (\phi(Q') - \phi(Q)) + O(\|\phi(Q') - \phi(Q)\|_p^2).$$

Using (4.7), we have $[[1+am]]\phi(Q) = \phi([1+am]Q) = \phi(Q)$. The approximation (4.6) follows. □

We now apply Lemma 4.5 to $\kappa\colon J \to K$.

proof of Theorem 4.4. Note that $\kappa\colon J \mapsto K$ is rational, smooth and 2:1 on points outside $J[2]$, hence κ is differentiable outside $J[2]$. Since $\rho_{J,p}$ is a group homomorphism by Theorem 3.4, it follows that for any $Q \in J(\mathbb{Q}_p) \setminus J(\mathbb{Q}_p)[2]$, we have that $\rho_{J,p}(Q) \neq \rho_{J,p}(-Q)$, hence we can find a neighborhood $U \subseteq J(\mathbb{Q}_p)$ such that κ is injective at U, and we obtain the commutative diagram

$$\begin{array}{ccc} J(\mathbb{Q}_p) & \xrightarrow{\rho_{J,p}} & \tilde{J}(\mathbb{F}_p) \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \tilde{\kappa}} \\ K(\mathbb{Q}_p) & \xrightarrow{\rho_{K,p}} & \tilde{K}(\mathbb{F}_p), \end{array} \tag{4.8}$$

where $\rho_{K,p}\colon K(\mathbb{Q}_p) \to \tilde{K}(\mathbb{F}_p)$ is the map that reduces the coefficients of K modulo p, and $\tilde{\kappa}$ is the quotient map $\tilde{J} \to \tilde{K}$.

Since all these properties are local, composing κ with a map that projects onto an affine patch still results in a differentiable map that is a local immersion. Hence, if $\kappa^{(i)}$ is the map κ composed with the projection onto an affine patch in the i-th coordinate, then $\kappa^{(i)}$ satisfies all the conditions of Lemma 4.5. Substituting an appropriate $\kappa^{(i)}$ in Equation (4.6) results in

$$[[M]]\tilde{R}'_n - \tilde{R}_{n+1} = M(\tilde{R}'_n - \tilde{R}_{n+1}) + O(\|\tilde{R}_{n+1} - \tilde{R}'_n\|_p^2).$$

Therefore, using that $\|\tilde{R}_{n+1} - \tilde{R}'_n\|_p^2 = r$ in the context of step 3 of Algorithm 4.2,

$$\tilde{R}_{n+1} = \frac{1}{M-1}(M\tilde{R}'_n - [[M]]\tilde{R}'_n) + O(p^r)$$

is the m-torsion point on $K(\mathbb{Z}/p^r\mathbb{Z})$ that reduces to $\kappa(\tilde{Q})$. Theorem 4.4 follows from the iteration in step 3 until $r = N$. □

Remark 4.9. For elliptic curves and hyperelliptic curves of genus 2, applying Hensel lifting as in step 3.2 (explained in Section 3.3) is less complicated because the Kummer variety is defined by at most one equation. For genus 3, a system of equations defines the Kummer variety, hence we need to use multivariate Hensel lifting in the lifting procedure.

Remark 4.10. In [52, §11], it is assumed that p divides M. Here, this assumption is being replaced by the assumption $M \not\equiv 1 \mod p$. This is a generalization that allows for more flexibility in choosing M. One way to utilize this in practice is to choose M to be a power of 2 because doubling is slightly faster than pseudo-addition. In case we need M to be quite large to be a power of 2, it is usually more efficient to pick M as small as possible.

In Section 4.7, we see that if m is odd, we can always find an M that is a power of 2. In Section 4.8, we explore alternative methods for finding $J(\mathbb{Q})[2^n]$ for $n \in \mathbb{Z}_{\geq 1}$, and conclude that for most curves, $J(\mathbb{Q})$ can be found entirely without the need for the biquadratic forms on K as described in Section 2.7.

Remark 4.11. The approximation in step 3.3 can use a different projection onto $\mathbb{A}^{2^g}$ in every iteration of step 3. This ensures that we do not encounter problems when we change i in our map $\kappa^{(i)}$ in every iteration, which could be necessary if, for example, the first coordinate of R is $\equiv 0 \mod p^r$, but $\not\equiv 0 \mod p^{2r}$ for a certain $r \in \mathbb{Z}_{\geq 1}$.

4.4 Computing a p-adic precision that allows us to terminate the lifting procedure conclusively

Theorem 4.4 allows us to create a p-adic approximation of $\kappa(\tilde{Q})$ to precision $O(p^N)$ of arbitrary $N \in \mathbb{Z}_{\geq 1}$. This section proves that we can find a p-adic precision such that the corresponding rational approximation $\tilde{R}_n$ is either the rational lift $R = \kappa(Q)$ such that $Q \in J(\mathbb{Q})$, or no such rational lift exists.

Theorem 4.12. Let $N \in \mathbb{Z}$ be such that $p^N > 2^{(g+2^g)}\beta^2$. Let $\tilde{R}_n$, $(r_1, \ldots, r_{2^g})$, L, R' and R be as computed in step 4 of Algorithm 4.2. Then, the following statements hold.

1. If $H(R) \leq \beta$, then R is the unique point in $\mathbb{P}^{2^g-1}(\mathbb{Q})$ of height $\leq \beta$ reducing to $\tilde{R}_n$.
2. If $H(R) > \beta$, then no point on $\mathbb{P}^{2^g-1}(\mathbb{Q})$ with height $\leq \beta$ exists that reduces to $\tilde{R}_n$.

Before we prove this theorem, we observe a simple injection.

Lemma 4.13. Let $B \in \mathbb{Z}_{\geq 1}$. For $d \in \mathbb{Z}_{\geq 1}$, let

$$S = \{R \in \mathbb{P}^d(\mathbb{Q}) : H(R) \leq B\}.$$

Let $n \in \mathbb{Z}_{\geq 1}$ such that $p^n \geq 2B^2$. For $r \in \mathbb{Z}$, write $\tilde{r} := r \mod p^n$. We define the map

$$\varphi \colon S \to \mathbb{P}^d(\mathbb{Z}/p^n\mathbb{Z})$$

as follows: Write $R := (r_1 : \ldots : r_d)$ such that all $r_i \in \mathbb{Z}$ and $\gcd(r_1, \ldots, r_d) = 1$. Then, we set

$$\varphi(R) = (\tilde{r}_1 : \ldots : \tilde{r}_d).$$

Then, the map φ is injective.

proof. Let $R := (r_1 : \ldots : r_{d+1}) \in S$ and $T := (t_1 : \ldots : t_{d+1}) \in S$ scaled such that all $r_i, t_i \in \mathbb{Z}$, and $\gcd(r_1, \ldots r_{d+1}) = \gcd(t_1, \ldots, t_{d+1}) = 1$. Suppose $\varphi(R) = \varphi(T)$. Then, there exists a $\tilde{\lambda} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ such that $\tilde{\lambda}\tilde{r_i} = \tilde{t_i}$ for all $i \in \{1, \ldots, d+1\}$. In particular, for a fixed $1 \leq i \leq d+1$ such that $\tilde{r_i} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, $\tilde{\lambda} = \tilde{t_i}\tilde{r_i}^{-1}$. Hence, for any $j \in \{1, \ldots d+1\}$

$$\tilde{t_i}\tilde{r_j} = \tilde{t_j}\tilde{r_i}.$$

Note that $R, T \in S$, and the coordinates are normalized in such a way that

$$\tilde{r_i}, \tilde{t_i}, \tilde{r_j}, \tilde{t_j} \in \{-\tilde{B}, \ldots, 0, \ldots, \tilde{B}\}.$$

It follows that

$$\tilde{t_i}\tilde{r_j}, \tilde{t_j}\tilde{r_i} \in \{-\tilde{B}^2, \ldots, 0, \ldots, \tilde{B}^2\}.$$

Since $p^n \geq 2B^2$, we have $t_i r_j = t_j r_i$ for all j, hence we can take

$$\lambda = \frac{t_i}{r_i},$$

well-defined because $r_i \neq 0$, and we see that $\lambda r_j = t_j$ for all $j \in \{1, \ldots, d+1\}$, hence $R = T \in S$. □

This lemma tells us that, given $B \in \mathbb{Z}_{\geq 1}$, we can determine a p-adic precision $O(p^n)$ for which there is at most one rational $R \in \mathbb{P}^{2^g-1}(\mathbb{Q})$ of height $H(R) < B$ that reduces to a point $\tilde{R} \in \mathbb{P}^{2^g-1}(\mathbb{Z}/p^n\mathbb{Z})$. Hence, for sufficiently large p-adic precision, we know that a lift within a given height bound is unique. The next challenge is to actually find this lift.

Lemma 4.14. Let $n, d \in \mathbb{Z}_{\geq 1}$ and $\tilde{R} \in \mathbb{P}^d(\mathbb{Z}/p^n\mathbb{Z})$. Let $R := (r_1 : \ldots : r_{d+1}) \in \mathbb{P}^d(\mathbb{Q})$ be scaled such that $r_i \in \mathbb{Z}$ and $\gcd(r_1, \ldots, r_{d+1}) = 1$. Let

$$v := (r_1, \ldots r_{d+1}) \in \mathbb{Z}^{d+1}.$$

Then, the lattice L generated by $\{v\} \cup \{e_i p^n : 0 \leq i \leq d\}$ contains all vectors whose coordinates taken as a point in $\mathbb{P}^d(\mathbb{Q})$ reduce modulo p^n to $\tilde{R}_n$. Moreover, write

$$w = a_0 v + p^n a_1 e_1 + \cdots p^n a_{d+1} e_{d+1} \in L$$

where $a_i \in \mathbb{Z}$. If w has the property that $a_0 \neq 0$, the point in $\mathbb{P}^d(\mathbb{Q})$ corresponding to w reduces modulo p^n to $\tilde{R} \in \mathbb{P}^d(\mathbb{Z}/p^n\mathbb{Z})$.

proof. We can obtain all vectors corresponding to points reducing modulo p^n to $\tilde{R}$ by considering $v_0 := v$, and following a combination of either of the following steps iteratively:

- obtaining $v_{j+1} := av_j$ for an integer $a \neq 0$
- obtaining $v_{j+1} := v_j + p^n e_i$ for $1 \leq i \leq d+1$.

The resulting vectors are clearly in L, and of the form $w = a_0 v + p^n a_1 e_1 + \cdots p^n a_{d+1} e_{d+1}$ with $a_i \in \mathbb{Z}$ and $a_0 \neq 0$. □

Consider $\tilde{R}_n \in \mathbb{P}^{2^g-1}(\mathbb{Z}/p^N\mathbb{Z})$ as obtained after step 3 of Algorithm 4.2. Using Lemma 4.14, the lattice L in step 4 is the integer lattice that contains all vectors that are integer representatives of points in $\mathbb{P}^{2^g-1}(\mathbb{Q})$ reducing to $\tilde{R}_n$. Moreover, any vector that corresponds to a lift of $\tilde{R}_n$ is of the form $a_0 v + p^n a_1 e_1 + \cdots p^n a_{2^g} e_{2^g}$ with $a_0 \neq 0$.

Finding the unique lift within a given height bound is then achieved by finding a short vector in the lattice L. It is known that finding the shortest vector (in the euclidean sense) in a lattice is a difficult problem. The Lenstra-Lenstra-Lovász-reduction algorithm (LLL-reduction) finds relatively short vectors efficiently. Assuming a parameter $\delta = 3/4$, the first basis vector of an LLL-reduced basis has euclidean length less than or equal to

$$2^{(2^g-1)/2}\|\lambda\| \tag{4.15}$$

in which λ is the shortest nonzero vector. LLL-reduction was invented in [31]. See also [23, §17.2].

Using LLL-reduction, we can determine the p-adic precision that makes the short vector obtained by LLL-reduction represent a possible "last candidate" for a rational lift in $\mathbb{P}^{2^g-1}(\mathbb{Q})$. The precise determination uses that vectors with a certain euclidean length give estimates on the heights of the points in $\mathbb{P}^{2^g-1}(\mathbb{Q})$ they represent. These computations prove Theorem 4.12.

proof of Theorem 4.12.

In this proof, we use the correspondence between a point $R' \in \mathbb{P}^{2^g}(\mathbb{Q})$ and a vector $v \in \mathbb{Z}^{2^g}$ as in Lemma 4.14: a point $R' \in \mathbb{P}^{2^g}(\mathbb{Q})$ with coordinates $(r'_1 : \ldots : r'_{2^g})$ scaled such that $r'_i \in \mathbb{Z}$ and $\gcd(r'_1, \ldots, r'_{2^g}) = 1$ corresponds uniquely to a vector $v' = (r'_1, \ldots, r'_{2^g}) \in \mathbb{Z}^{2^g}$.

Proof of 1): If $H(R) \leq \beta$, then R is the unique point in $\mathbb{P}^{2^g-1}(\mathbb{Q})$ of height $\leq \beta$ reducing to $\tilde{R}_n$.

Suppose $H(R) \leq \beta$. Then, $H(R) \leq 2^{(2+2^g)}\beta^2 < p^N$. Let R correspond to the vector

$$w = a_0 v + p^N a_1 e_1 + \cdots + p^N a_{d+1} e_{d+1} \in L.$$

By design of the algorithm, $R \neq 0$, hence if $a_0 = 0$, then $H(R) \geq p^N$, which is a contradiction. Hence, $a_0 \neq 0$, so R reduces to $\tilde{Q}$ using Lemma 4.14. The uniqueness follows from the injectivity of the map in Lemma 4.13, using that $p^N \geq 2^{(2+2^g)}\beta^2 > 2\beta^2$.

Proof of 2): If $H(R) > \beta$, then no point on $\mathbb{P}^{2^g-1}(\mathbb{Q})$ with height $\leq \beta$ exists that reduces to $\tilde{R}_n$.

Suppose $H(R) > \beta$. Let

$$S_0 = \{T \in \mathbb{P}^{2^g-1}(\mathbb{Q}) : H(T) \leq \beta\} \subseteq \mathbb{P}^{2^g-1}(\mathbb{Q}).$$

Hence, $R \notin S_0$. For any $T \in S_0$, we can create the corresponding integer vector $v_0 \in \mathbb{Z}^{2^g}$. Since the maximal absolute value of each coordinate of v_0 is $\leq \beta$, v_0 has euclidean length at most $\sqrt{(2^g)\beta^2} = \sqrt{2^g}\beta$. Hence, the vector v_0 lies in the 2^g-dimensional sphere of radius $\sqrt{2^g}\beta$

$$D_0 := \{w \in \mathbb{R}^{2^g} : \|w\| \leq \sqrt{2^g}\beta\} \subseteq \mathbb{R}^{2^g}$$

centered at the origin of $\mathbb{R}^{2^g}$.

Now, let D_1 be the sphere of radius $2^{(2^g-1)/2}\sqrt{2^g}\beta$, i.e.,

$$D_1 := \{w \in \mathbb{R}^{2^g} : \|w\| \leq 2^{(2^g-1)/2}\sqrt{2^g}\beta\}.$$

Using the bound (4.15), if an LLL-reduced short nonzero vector v of L is not in D_1, then the shortest nonzero vector of L cannot be in D_0. Finally, define

$$S_1 := \{T \in \mathbb{P}^{2^g-1}(\mathbb{Q}) : H(T) \leq 2^{(2^g-1)/2}\sqrt{2^g}\beta\}.$$

The points in $\mathbb{P}^{2^g-1}(\mathbb{Q})$ corresponding to all vectors in D_1 are contained in S_1. Note that $2 \cdot (2^{(2^g-1)/2}\sqrt{2^g}\beta)^2 = 2^{2^g}(2^g)\beta^2 = N$, hence S_1 injects into $\mathbb{P}^k(\mathbb{Z}/p^N\mathbb{Z})$ using Lemma 4.13. We now consider two cases.

Case 1: If $R \in S_1$ (but recall $R \notin S_0$), then R is the unique lift in S_1, using that S_1 maps injectively into $\mathbb{P}^k(\mathbb{Z}/p^N\mathbb{Z})$. Since $H(R) > \beta$, no point R' exists such that $H(R') \leq \beta$ and R' reduces to $\tilde{R}$.

Case 2: If $R \notin S_1$, it follows that its corresponding vector $v \in L$ obtained by LLL-reduction is not in D_1. Hence, the shortest vector of L cannot be in D_0. Therefore, no vector in L corresponds to a point in S_0. Since all possible lifts of $\tilde{R}$ are contained in L, there does not exist a point in S_0 (i.e., of height $\leq \beta$) that reduces to $\tilde{R}$. □

4.5 The conclusions of the lift-checking algorithm

Since we obtain a "last candidate" R using Theorem 4.12, steps 5-7 of Algorithm 4.2 determine whether $R \in \mathbb{P}^{2^g-1}(\mathbb{Q})$ is actually a point on $K(\mathbb{Q})$ such that $\kappa^{-1}(R) \subseteq J(\mathbb{Q})[m]$. Recall that we use Theorem 3.5 to obtain $\tilde{Q} \in \tilde{J}(\mathbb{F}_p)$ such that there exists a unique lift $Q \in J(\mathbb{Q}_p)$ of order m. To conclude Algorithm 4.2, we determine whether $Q \in J(\mathbb{Q})[m]$ or not.

Proposition 4.16. Let $R \in \mathbb{P}^{2^g-1}(\mathbb{Q})$ be as obtained after step 4 in Algorithm 4.2. Then, the unique lift $Q \in J(\mathbb{Q}_p)[m]$ of $\tilde{Q} \in \tilde{J}(\mathbb{F}_p)$ is a point in $J(\mathbb{Q})[m]$ if and only if

- $R \in K(\mathbb{Q})$,
- $[[m]]R = \kappa(0)$,
- $\kappa^{-1}(R) \subseteq J(\mathbb{Q})$.

proof. Using Theorem 4.5 and Theorem 4.12, $Q \in J(\mathbb{Q})[m]$ if and only if $R = \kappa(Q)$ and $Q \in J(\mathbb{Q})$. Clearly, $R = \kappa(Q)$ and $Q \in J(\mathbb{Q})$ implies that $R \in K(\mathbb{Q})$, $[[m]]R = \kappa(0)$, and $\kappa^{-1}(R) = \{Q, -Q\} \subseteq J(\mathbb{Q})$.

To prove the converse, we assume that all three conditions described in steps 5-7 are satisfied. It follows that $\kappa^{-1}(R) \subseteq J(\mathbb{Q})[m]$. The commutative diagram (4.8) implies that $\kappa^{-1}(R)$ contains the unique point $Q \in J(\mathbb{Q})[m]$ that reduces to $\tilde{Q}$.

□

Remark 4.17. In practice, when the necessary precision is not yet reached in step 3, one can already determine R, and try if the conditions of steps 5-7 are satisfied. If they are, we have already found a point $Q \in J(\mathbb{Q})[m]$ that reduces to $\tilde{Q}$. However, if no such point is found, it is not guaranteed that no other candidate exists.

Remark 4.18. The algorithm does not require a procedure that performs the group law on $J(\mathbb{Q})$. This is completely replaced by the arithmetic on K, which is performed in step 3.3 and step 6 of Algorithm 4.2. It turns out that in most cases, we can restrict ourselves to doubling on K, so we do not require the biquadratic forms as described in Section 2.7. This is described in detail in Section 4.7.

4.6 Computing the rational torsion subgroup

Now that we can conclusively say whether a reduced point on a nonsingular reduced Jacobian $\tilde{J}(\mathbb{F}_p)$ lifts to $J(\mathbb{Q})$ or not, we can construct a procedure that computes the rational torsion subgroup of Jacobians of hyperelliptic curves.

Remark 4.19. Since $\kappa(J[2])$ consists of singular points, we cannot use the lifting procedure as described in Algorithm 4.2 when we lift points of order 2. Therefore, we need a different approach for computing $J(\mathbb{Q})[2]$. This is not difficult: it is well known that the nontrivial elements of $J(\mathbb{Q})[2]$ can be found using the prime factorization of f in $\mathbb{Q}[x]$, see [53, Lemma 4.3, Lemma 5.6]. The case where $g = 3$ is discussed in Section 5.6.

Using Theorem 3.5, the reduction map $\rho_{J,p}$ is injective on q-parts of $J(\mathbb{Q})_{\text{tors}}$ where $q \neq p$ is a prime number. We take several primes of good reduction p, compute $\tilde{J}(\mathbb{F}_p)$, and determine a finite (and usually small) amount of reduced points that may potentially lift to $J(\mathbb{Q})$, together with their order. This has been implemented using the function `TorsionBound` in MAGMA [4]. We will introduce the algorithm that describes how to compute $J(\mathbb{Q})_{\text{tors}}$. This is again a generalized version of the idea proposed in [52, §11].

Algorithm 4.20. Computing the q-part of a Torsion Subgroup
Given a hyperelliptic curve C and a prime $q > 3$, compute the q-part of $J(\mathbb{Q})_{tors}$.

1. Set G_0 to be the q-part of $\tilde{J}(\mathbb{F}_p)$, where p is a good prime not equal to q (for a strategy on choosing p, see Remark 4.23). Set $T_0 = \{0\} \subset G_0$, $S_0 = G_0 \setminus \{0\}$, $S_0' = \{0\}$. (G_i and T_i are groups, S_i and S_i' are sets throughout the procedure)

2. Set $n = 0$, repeat the following steps until $S_n = \emptyset$.

   2.1. Let $g \in S_n$, then g is an element of G (preferably a primitive element).

   2.2. Compute the smallest m such that $q^m g$ lifts to $J(\mathbb{Q})$.

   2.3. Set

$$\begin{aligned} T_{n+1} &= \langle T_n, q^m \cdot g \rangle \\ G_{n+1} &= G_n / \langle q^m \cdot g \rangle \\ S'_{n+1} &= S'_n \cup \langle g \rangle \\ S_{n+1} &= G_{n+1} \setminus S'_{n+1} \end{aligned}$$

   2.4. Replace n with $n + 1$

3. Return T_n.

In the algorithm, each G_n represents the group of points that do not lift or are yet to be checked. T_n is the group of points that we have found to lift so far, S_n is the set of points that are yet to be checked, and S'_n are points that have been checked.

Remark 4.21. Algorithm 4.2 excludes the case $q = 2$. This is necessary because the image $\kappa(J[2])$ consists of singular points (see Theorem 2.47), hence the lifting procedure proven in Theorem 4.4 does not work on points of order 2. However, we can adjust Algorithm 4.20 to compute all points of $J(\mathbb{Q})[2^s]$ for an integer $s \geq 2$. In step 2.2, if $q^m g \in \tilde{J}(\mathbb{F}_p)$, then one sets $m := m + 1$ and proceeds to step 2.3. By computing $J(\mathbb{Q})[2]$ as in Remark 4.19, one can compute the 2-part of $J(\mathbb{Q})$ entirely by finding relations. Arithmetic on $J(\mathbb{Q})$ is not necessary: for a 4-torsion point $Q \in J(\mathbb{Q})$ and a 2-torsion point $Q' \in J(\mathbb{Q})$, we have $2Q = Q'$ if and only if $\delta(\kappa(Q)) = \kappa(Q')$, where δ is the system of doubling formulae that maps $R \in K$ to $[[2]]R \in K$ as described in Section 2.7.

Algorithm 4.22. Computing the Torsion Subgroup
Given a hyperelliptic curve C of genus g, this algorithm computes the rational torsion subgroup of the Jacobian $J(\mathbb{Q})_{tors}$.

1. Compute an upper bound for the height constant at infinity c_∞ as described in Section 3.4.
2. Compute a torsion height bound β.
3. Compute a multiplicative upper bound t for the size of the torsion subgroup by using a reasonable number of good primes and computing the structure of $J(\mathbb{F}_p)$.
4. For each prime factor $q > 3$ of t, compute the q-part of $J(\mathbb{Q})_{\text{tors}}$ using algorithm 4.20.
5. Compute $J(\mathbb{Q})[2]$ as discussed above, and use Remark 4.21 to compute the 2-part of $J(\mathbb{Q})$.
6. For $q \neq 2$, use the generators of q-parts of $J(\mathbb{Q})$ to compute generators for $J(\mathbb{Q})_{\text{tors}}$.

Remark 4.23. In step 3, we typically choose the 10 smallest primes of good reduction p and compute $\tilde{J}(\mathbb{F}_p)$. In step 4, we choose a particular prime $p \neq q$ to compute the q-part of $\tilde{J}(\mathbb{F}_p)$. Hence, we prefer to pick a prime p such that the q-part of $\tilde{J}(\mathbb{F}_p)$ is the smallest, so Algorithm 4.20 needs to test fewer reduced points.

Remark 4.24. If one is simply interested in the torsion structure or a unique representation of points on $J(\mathbb{Q})$ is unknown, one can simply check *whether* a reduced point in $\tilde{J}(\mathbb{F}_p)$ lifts to $J(\mathbb{Q})$ or not, without explicitly computing $\kappa^{-1}(R)$ in step 7 of Algorithm 4.2. By counting the rational points of order 2 and finding the structure of the q-parts of $J(\mathbb{Q})_{\text{tors}}$, one can use the Chinese Remainder Theorem to construct elementary divisors of $J(\mathbb{Q})$ in step 6 of Algorithm 4.22.

4.7 Avoiding the use of sum-and-difference-laws

Recall from Section 2.54 that an implementation of the multiplication-by-n-map $[[n]]$ is based on doubling formulae and biquadratic forms that allow us to perform Algorithm 2.54. In this section, we refer to "the biquadratic forms" as the biquadratic forms specifically designed to perform the `PseudoAdd`-function as described in Section 2.7.

The biquadratic forms are nontrivial to compute for Jacobians of hyperelliptic curves. They are also more memory-intensive compared to the doubling formulae. Computing $[[n]]\kappa(Q)$ for $Q \in J(\mathbb{Q})$ and $n \in \mathbb{Z}$ using the multiplication algorithm as described in Algorithm 2.54 is typically more efficient when n is small and of the form $n = \pm 2^s$ for an integer s. In this case, we can simply repeatedly apply the doubling formulae. In the algorithm that computes $J(\mathbb{Q})_{\text{tors}}$, one applies $[[M]]$ in step 3.3 in Algorithm 4.2, and one applies $[[m]]$ in step 6 of the same algorithm.

The discovery that prompted this research is described in Remark 4.10: the original design for genus 2 hyperelliptic curves in [52, §11] requires in step 3.3 that p divides M. This algorithm is a generalization in the sense that we only require that $M \not\equiv 1 \mod p$. This gives more freedom in choosing M. In practice, it turns out that it is more efficient to choose M to be an integer such that $|M|$ is small, that is preferably of the form $\pm 2^s$.

We first focus on step 3.3. Let us be given a reduced point $\tilde{Q} \in \tilde{J}(\mathbb{F}_p)$ of order m. By design of Algorithm 4.20, this m is always a prime power q^t for a prime $q \geq 2$ (we consider $q = 2$ using Remark 4.21). We require M to satisfy $M \equiv 1 \mod m$ and $M \not\equiv 1 \mod p$. The smallest such M is obtained by setting $M = 1 - m$. In this case, $M \not\equiv 1 \mod p$ because $\gcd(m, p) \neq 1$ in the algorithm. Now, we consider the cases where M can be chosen to be of the form 2^s for an integer s.

Assume that m is odd. We must now find M of the form $M = 2^s$ and $M = 1 + am$, i.e., $M \equiv 1 \mod m$. Since m is odd, we can set s to be the order of $2 \in (\mathbb{Z}/m\mathbb{Z})^\times$, and we find $M = 2^s \equiv 1 \mod m$. (In fact, one can also take s such that $2^s = -1 \in (\mathbb{Z}/m\mathbb{Z})^\times$) and take $M = -2^s$ to increase efficiency in some cases.)

Assume that m is even. Then, clearly no $M = \pm 2^s$ exists such that $M \equiv 1 \mod m$. Recall that we can already compute $J(\mathbb{Q})[2]$ as discussed in Remark 4.19. Since the doubling formulae consist of a system of polynomials in δ for the coordinates in K (see Section 2.54), one can try to solve such a system directly. Given a point $R \in K(\mathbb{Q})$, it turns out that we can compute all $R' \in K(\mathbb{Q})$ such that

$$[[2]]R' = R, \tag{4.25}$$

this is discussed in Section 4.8. This idea results in the following algorithm.

Algorithm 4.26. Computing the 2-part of $J(\mathbb{Q})_{\mathbf{tors}}$ without employing biquadratic forms.
Given a hyperelliptic curve C, computes the 2-part of $J(\mathbb{Q})_{tors}$.
Requirements: A procedure that, given R, computes all R' as in Equation (4.25). An algorithm to compute $\kappa(J(\mathbb{Q})[2])$.

1. Set T, S_2 to $\kappa(J(\mathbb{Q})[2])$ as a set, set $n = 2$.
2. Repeat until S_n is empty:
   2.1. Set $S_{2n} = \emptyset$
   2.2. For each $R \in S_n$, compute all $R' \in K(\mathbb{Q})$ such that $[[2]]R' = R$, and append them to S_{2n}.
   2.3. Delete every item R in S_{2n} where $\kappa^{-1}(R) \not\subseteq J(\mathbb{Q})$.
   2.4. Set T to $T \cup S_{2n}$.
   2.5. Replace n by $2n$.
3. Conclude that T is the 2-part of $J(\mathbb{Q})_{\text{tors}}$, and $S_n = J(\mathbb{Q})[n]$.

Based on some tests in genus 3 in practice, computing R' such that $[[2]]R' = R$ in $K(\mathbb{Q})$ makes the computations slow enough that using the original method to compute the 2-part of $J(\mathbb{Q})$ is more efficient. Hence, it seems better in practice to use biquadratic forms if they are available. However, if no biquadratic forms are available, we can still find points the 2-part of $J(\mathbb{Q})$.

The other step where arithmetic on K is used to compute $J(\mathbb{Q})_{\text{tors}}$ is at step 6 in Algorithm 4.2. Here, we check whether a point $R \in K(\mathbb{Q})$ satisfies $[[m]]R = 0$. If arithmetic on $J(\mathbb{Q})$ is implemented, we can replace step 6 by computing $\kappa^{-1}(R)$ first (i.e., step 7), and in the case $\kappa^{-1}(R) \subseteq J(\mathbb{Q})$, we can pick one of its two points Q in the pre-image, and directly check whether $[m]Q = 0 \in J(\mathbb{Q})$. Here, we simply replace arithmetic on $K(\mathbb{Q})$ by arithmetic on $J(\mathbb{Q})$.

Suppose that no arithmetic is implemented on $J(\mathbb{Q})$. We try to check that $[[m]]R = 0$ using only doubling formulae on K. Here, the order of the prime factors q in step 4 of Algorithm 4.22 must be taken carefully in such a way that we already have some information on other parts of $J(\mathbb{Q})_{\text{tors}}$. The following observations help us check whether a point $R = \kappa(Q) \in K$ maps to the origin of K under $[[m]]$.

- $[4]Q = 0 \iff [[4]]R = 0$.
- $[8]Q = 0 \iff [[8]]R = 0$.
- $[3]Q = 0 \iff [[2]]R = R$ and $R \neq \kappa(0)$.
- $[9]Q = 0 \iff [[8]]R = R$ and $Q \notin J(\mathbb{Q})[7]$.
- $[5]Q = 0 \iff [[4]]R = R$ and $Q \notin J(\mathbb{Q})[3]$.
- $[7]Q = 0 \iff [[8]]R = R$ and $Q \notin J(\mathbb{Q})[9]$.

Note that computing $J(\mathbb{Q})[7]$ depends on knowing $J(\mathbb{Q})[9]$ and computing $J(\mathbb{Q})[9]$ depends on knowing $J(\mathbb{Q})[7]$. Therefore, we cannot avoid using the biquadratic forms this way if the torsion bound used in step 3 of Algorithm 4.22 divides both 7 and 9. For prime powers $11 \leq m \leq 60$, the only cases where m can be written as a sum or difference of 2-powers are 17 and 31 (and obviously 32 gives no problems).

We summarize this section by describing the precise conditions for which we can compute $J(\mathbb{Q})_{\text{tors}}$ without the use of the biquadratic forms. Given a hyperelliptic curve C of genus g such that the required explicit theory as discussed in Section 4.1 *except the biquadratic forms* is known, we can compute generators for $J(\mathbb{Q})_{\text{tors}}$ if one of the following conditions is satisfied:

- we have an implementation of the group law on $J(\mathbb{Q})$,
- all points that we find in step 3 of Algorithm 4.22 have orders that divide prime powers in $\{2^u : u \in \mathbb{Z}_{\geq 1}\} \cup \{3, 9, 5, 7, 17, 31\}$, and a point of order 7 and a point of order 9 are not both found.

Considering that most of the torsion points on $J(\mathbb{Q})$ have a small order, we expect that for a large amount of curves C of genus g, we can compute $J(\mathbb{Q})_{\text{tors}}$ without requiring the biquadratic forms. For genus 4 hyperelliptic curves, the doubling formulae are computed by Ludwig Fürst. Since an algorithm for arithmetic on hyperelliptic curves of genus 4 is known (in fact, it is easier than the genus 3 cases due to [57, Remark 2.5]), one does not need the biquadratic forms to compute $J(\mathbb{Q})_{\text{tors}}$.

4.8 Halving a rational point on K.

In the previous section, we have explored options to compute $J(\mathbb{Q})_{\text{tors}}$ without requiring biquadratic forms as described in Section 2.54. We described how a procedure that computes the pre-image of the doubling formulae δ for a certain point $R \in K(\mathbb{Q})$ gives a way to compute $J(\mathbb{Q})_{\text{tors}}$ without such biquadratic forms.

Here, we propose two methods to compute the pre-image of δ on K. Given a point $R \in K(\mathbb{Q})$, we try to find R' such that

$$\delta(R') = R.$$

Lemma 4.27. Let C be defined over a perfect field k of characteristic $\neq 2$, and $R \in K$, then $\#\delta^{-1}(R) = \#J[2] = 2^{2g}$.

proof. Since $\delta(R + R') = \delta(R)$ if and only if $\delta(R') = \kappa(0)$ for a point $R \in K$, the δ-polynomials are precisely invariant under the action of $J[2]$, as defined in Section 2.8. Therefore, $\#\delta^{-1}(R) = \#J[2]$. The fact that $\#J[2] = 2^{2g}$ is well-known, see [25, Theorem A.7.2.7(ii)]. □

The first approach for computing $\delta^{-1}(R)$ is a direct approach. We observe that given R, we can simply try to solve the system of homogeneous polynomial equations $\delta(R') = R$ projectively. Since this system has finitely many solutions, its corresponding variety has dimension 0. MAGMA [4] provides an algorithm that finds all solutions using `Points(X) : Sch -> SetIndx`, which gives all points on a zero-dimensional scheme using Gröbner Basis computations, see [16, Chapter 2] This approach works, but computing such pre-images is, in practice, significantly slower than simply using the lifting methods.

For genus 3 hyperelliptic curves, the CPU time of computing the pre-image of δ on K on an Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz is tested for 254 randomly selected rational 2-torsion points. The average CPU time required was ≈ 74 seconds. The fastest computation took 13.38 seconds, and the slowest computation took 279.38 seconds. The points $R \in K(\mathbb{Q})$ that have a larger height $H(R)$ seem to require a larger computational effort, see Figure 1.

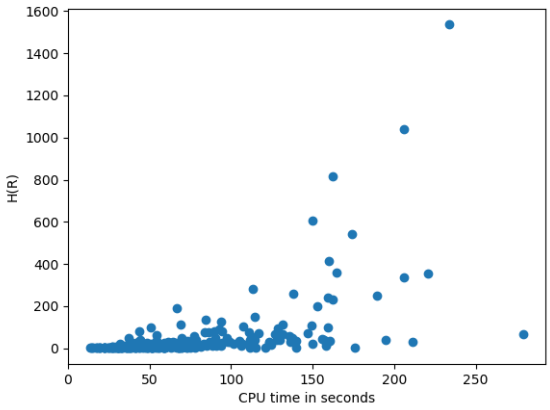

Figure 1: Computational effort of computing $\delta^{-1}(R)$ compared to $H(R)$ on 254 points.

An alternative approach is proposed in [52, §5] for genus 2 hyperelliptic curves. Let $\mathbb{Q}_f^{\mathrm{spl}}$ be the splitting field of f over $\mathbb{Q}$. Using Theorem 2.57, for a partition $\{S, S'\}$ of roots of f in $\mathbb{Q}_f^{\mathrm{spl}}$, we can find the squares of quadratic forms $(y_{\{S,S'\}}(R))^2$ in terms of $r_i = \delta_i(R')$. Then, we take square roots of $(y_{\{S,S'\}}(R))^2$ to find $\pm y_{\{S,S'\}}(R)$. Suppose that we can determine the sign of $y_{\{S,S'\}}(R)$. Then, Theorem 2.59 yields $r'_i r'_j$ for $1 \leq i \leq j \leq 2^g$, so by finding a nonzero $r_i'^2$, one can compute $R' = (r'_1 r_i : \ldots : r'_{2^g} r'_i)$.

For genus 2 hyperelliptic curves, relations that determine the signs of $y_{\{S,S'\}}$ are given in [52, Formula 10.5]. This method can be generalized to genus 3 hyperelliptic curves if similar relations are explicitly computed for genus 3 hyperelliptic curves. Note that one works over a quadratic extension of $\mathbb{Q}_f^{\mathrm{spl}}$, hence if f does not split completely over $\mathbb{Q}$, then computations could slow down significantly. This method may not be very efficient in practice.

5 Computing $J(\mathbb{Q})_{\mathbf{tors}}$ for Jacobians of genus 3 hyperelliptic curves

5.1 Overview

Chapter 4 gives a complete procedure that computes the torsion subgroup for hyperelliptic curves of genus g, assuming certain objects and procedures exist. This chapter discusses the work that must be done in order to compute $J(\mathbb{Q})_{\text{tors}}$ for Jacobians of hyperelliptic curves of genus 3. Throughout this chapter, we fix a hyperelliptic curve C of genus 3 defined over a perfect field k of characteristic $\neq 2$, and denote J to be its Jacobian.

Recall from Section 4.1 that the required procedures for applying the algorithm to compute $J(\mathbb{Q})_{\text{tors}}$ are the following:

- An implementation of the group law on $\tilde{J}(\mathbb{F}_p)$ for primes of good reduction p.
- Equations for $K \subseteq \mathbb{P}^{2^g-1}$; an explicit description of $\kappa\colon J \to K$
- A way to compute $\kappa^{-1}(R) \subseteq J(\mathbb{Q})$ for $R \in K(\mathbb{Q})$.
- Doubling formulae; biquadratic forms that allow us to use sum-and-difference laws on K as described in Section 2.7.
- A way to compute a height bound β for $J(\mathbb{Q})_{\text{tors}}$.

5.1.1 Explicit theory known in the literature

In the literature, explicit theory on hyperelliptic curves C of genus 3 is usually first developed for the case where the polynomial f in the defining equation $y^2 = f(x)$ has odd degree: if C contains a rational Weierstrass point, then we can map this point to infinity under an isomorphism, see Section 2.6. This results in a model $y^2 = f(x)$ such that $\deg(f) = 7$. In this case, points in $J(k)$ can be represented by a divisor representation as discussed in Section 2.4, and arithmetic is implemented using Mumford representation and Cantor's addition algorithm as introduced in Section 2.5. An embedding $\kappa\colon J \to K \subseteq \mathbb{P}^7$ and an explicit description of $K = \kappa(J) \subseteq \mathbb{P}^7$ is found in [40].

If k is algebraically closed, it follows by construction (see Section 2.1.3) that there exist precisely $2g+2$ rational Weierstrass points. Since we consider the base field $\mathbb{Q}$, we need to consider curves that do not contain a rational Weierstrass point. Hence, we need a more general description of $\kappa\colon J \to \mathbb{P}^7$ such that $\kappa(J) \cong K$, where we do not assume $\deg(f) = 7$. Such a description is given in [55] and summarized in Section 5.3. Defining equations of $\kappa(J) \cong K$ in $\mathbb{P}^7$ are computed. We now fix this $K := \kappa(J) \subseteq \mathbb{P}^7$, and we fix $\kappa\colon J \to K \subseteq \mathbb{P}^7$. Although κ is computed for generic points, some special cases are not explicitly considered. Since we need a complete explicit description of κ, we will finish this description in Section 5.4. It is useful to note that the Kummer variety constructed in [55] directly generalizes the construction of the Kummer variety in [40]: if we assume $f_8 = 0$, then $K \subseteq \mathbb{P}^7$ corresponds precisely to the explicit embedding of the Kummer variety in $\mathbb{P}^7$ as given in [40], see [55, §3].

Moreover, the doubling formulae and biquadratic forms that allow us to perform arithmetic on K are developed in [55] and made available on Michael Stoll's web page [51] in the file `G3HypHelp.m`. More precisely, the duplication map δ is given in [55, Theorem 7.3] and introduced in the same section. The biquadratic forms B_{ij} as introduced in (2.50) are constructed in [55, Section 8]. The same reference also provides a method to compute the torsion height bound β in [55, Corollary 10.3], recall from Theorem 3.15 that

$$\beta = 2^2 |\text{disc}(f)| c_\infty^{-1/3}.$$

Remark 5.1. As a result of the explicit description of K, we can consider a naive method to compute $J(\mathbb{Q})_{\text{tors}}$: a procedure that considers a reduced point $\tilde{R} \in \tilde{K}(\mathbb{F}_p)$ for a prime of good reduction p, and finds all

possible lifts within the height bound β in $\mathbb{P}^7(\mathbb{Q})$ by considering a lattice L of vectors in $\mathbb{Z}^8$ that correspond to all possible lifts of $\tilde{R}$.

This approach can be performed using the function `FindRationalPoints()` in the file [51, G3Hyp.m]. To be precise, the input of the function is a hyperelliptic curve C, a reduced point $\tilde{R} \in \tilde{K}$ for a prime of good reduction p, and a real number B that gives the maximal height considered. The approach is as follows: for any $R \in \mathbb{P}^7(\mathbb{Q})$, write coordinates $R := (r_1 : \ldots : r_8)$ such that all $r_i \in \mathbb{Z}$ and $\gcd(r_1, \ldots, r_8) = 1$. Consider a lattice L of vectors $(r_1, \ldots, r_8)$ in $\mathbb{Z}^8$, corresponding to the coordinates of possible rational lifts $R \in K(\mathbb{Q})$. Then, one searches for a shortest vector $s_v \in L$, projects onto a quotient lattice $L' = L/\langle s_v \rangle$ and searches for short vectors v' that lift to a vector $v := s_v n + v' \in L$ with $H(v) < B$. This search is performed recursively, through these sublattices. The number of layers of recursion is then determined by the optional paramter `count` (default: 3).

Hence, one could execute `FindRationalPoints()` and check whether the rational lifts of reduced points are torsion points. However, there are some issues with this approach. Computing the vector s_v is a difficult problem that is very time-consuming. Moreover, this process is executed recursively. For an 8-dimensional lattice, this procedure is conclusive if we apply 7 layers of recursion, reducing to a 1-dimensional lattice. However, this is not feasible in practice. The parameter `count` is put at 3 by default. Increasing the parameter `count` increases the computational effort. If one wants to make an educated guess, the function is a simple tool to find some points. However, if one wants to compute $J(\mathbb{Q})_{\text{tors}}$ completely, this method uses a computational effort that is not feasible in practice.

5.1.2 Explicit theory previously unknown

In order to make the algorithm work, some explicit theory still needs to be computed. We need to finish a description of $\kappa\colon J \to K$ for all cases. Then, we need to find a way to check whether $\kappa^{-1}(R) \subseteq J(k)$ for $R \in K(k)$. Moreover, we need to consider an implementation of arithmetic on reduced Jacobians $\tilde{J}(\mathbb{F}_p)$ for primes of good reduction p.

In order to describe $\kappa\colon J \to K$ completely, we first discuss how we can represent points in $J(k)$ using divisors in Section 5.2. Then, we summarize the theory on the computing κ explicitly in Section 5.3. Section 5.4 then finishes the description of κ.

Recall that the algorithm in Chapter 4 does not require an implementation of arithmetic in $J(\mathbb{Q})$. We do apply arithmetic on reduced Jacobians $\tilde{J}(\mathbb{F}_p)$ for primes of good reduction p in step 3 of Algorithm 4.22 and step 2.2 of Algorithm 4.20, called in step 4 of Algorithm 4.22. In MAGMA, arithmetic on $J(k)$ is implemented if C^{inf} consists of rational points. Using a change of coordinates, we can map any rational point to infinity. Therefore, we can use arithmetic on $J(k)$ if any rational point on $C(k)$ is known. In Section 5.5, we describe how we can always find primes p such that $\tilde{C}(\mathbb{F}_p)$ contains a rational point, and how the algorithm can be adjusted precisely.

The final thing we need is a way to determine whether $\kappa^{-1}(R) \subseteq J(k)$ for $R \in K(k)$. For generic points, this test is described in [55, §4], but for some special cases, we describe a test using the explicit description of κ in Section 5.4.

5.2 Describing points on the Jacobian

5.2.1 Finding a divisor representation

In order to give an explicit map $\kappa\colon J \to \mathbb{P}^7$ such that $\kappa(J)$ is a model of K, we need an explicit description of points on J. If $\deg(f) = 7$, then we simply refer to Section 2.4 for a representation of rational points in terms of a rational divisor. If we can find any rational Weierstrass point, then we use Lemma 2.44 to find a model such that $\deg(f) = 7$. However, if no rational Weierstrass point exists, then we need to consider a model with $\deg(f) = 8$. We will now show that we can represent points Q on J using divisors of degree 4, but we cannot generally expect uniqueness anymore.

Suppose $\deg(f) = 8$. Write $P_{\infty,1}, P_{\infty,2}$ for the two points at infinity. We follow arguments that are found in [55, §2] to find a divisor that represents a point $Q \in J(k)$. Recall from Definition 2.32 that a divisor D on C is *in general position* if D is effective and there is no point $P \in C$ such that $D \geq P + \iota P$. An approach similar to Theorem 2.34 is now harder because, in the notation of the proof of Theorem 2.34, we now consider the vector space $L_k = \mathcal{L}(D + k(P_{\infty,1} + P_{\infty,2}))$. It follows that D_Q must have even degree, hence we need to consider divisors of degree $4 = g + 1$. From now on, we denote D_∞ to be the divisor $D_\infty = P_{\infty,1} + P_{\infty,2}$.

Theorem 5.2. Consider a nontrivial point $Q \in J$ together with its corresponding divisor class in Pic^0_C. There exists an effective divisor D_Q that has degree 4 such that $Q = [D_Q - 2D_\infty]$, and D_Q has exactly one of the following properties:

1. D_Q is in general position,
2. $D_Q \geq D_\infty$ such that $D_Q - D_\infty$ is in general position.

Moreover, any divisor D of degree 4 in general position cannot be linearly equivalent to a divisor $D' \geq D_\infty$ of degree 4 such that $D' - D_\infty$ is in general position.

Sketch of proof. From [55, §2], we know that the map $\mathrm{Pic}^0_C \to \mathrm{Pic}^4_C$ that maps $[D] \mapsto [D] + [2D_\infty]$ is a canonical isomorphism. Then, it is argued that, for a given point $Q \in J$, we can find divisors $D_Q \in \mathrm{Pic}^4_C$ that are either in general position or uniquely of the form $P_1 + P_2 + P + \iota(P)$ such that $P_1 \neq \iota(P_2)$. Since the map induced by ι on Pic^4_C corresponds to multiplication by -1 on J, we can fix $P = P_{1,\infty}$ without loss of generality, hence $P + \iota(P) = D_\infty$. Using Riemann-Roch Theorem, one can observe that a divisor of the form (2) cannot be linearly equivalent to a divisor in the form (1). □

From now on, we say that Q is of *degree* 4 if Q is represented by a divisor D_Q of degree 4 in general position, and we say that Q is of *degree* 2 if Q is represented by a divisor D_Q such that $D_Q - D_\infty$ is in general position. The neutral point $0 \in J$ is defined to have degree 0, one defines the divisor representation on Pic^4_C to be $2D_\infty$.

5.2.2 Determining uniqueness of a divisor representation

The next step is to fix a unique divisor of the form D_Q in the cases where we are able to. We can immediately make the following observation.

Lemma 5.3. For any $Q \in J$ of degree 2, the corresponding divisor D_Q of the form $D_Q = P_1 + P_2 + D_\infty$ as in Theorem 5.2 is uniquely determined.

Sketch of proof. This is also mentioned in [55, §2]. Using Riemann-Roch Theorem, we can conclude that all divisors D in the class $[P_1 + P_2 + D_\infty] \in \mathrm{Pic}^4_C$ with $\iota(P_1) \neq P_2$ are of the form $P_1 + P_2 + P + \iota(P)$ for an arbitrary point $P \in C$. Hence, fixing $P = P_{1,\infty}$ gives the unique effective divisor $D_Q = P_1 + P_2 + D_\infty$ of degree 4 such that $D_Q \geq D_\infty$ and $D_Q - D_\infty$ is in general position. □

Now, we consider the case where $Q \in J$ has degree 4. Using Mumford representation as introduced in Theorem 2.37, we can uniquely represent *affine* divisors $D = \sum_{P \in C(\bar{k})} \alpha_P P$ of degree 4 in general position using the polynomial tuple $\langle a, b \rangle$, with $a, b \in k[x]$ such that

1. a is monic and has degree 4.
2. for all $P \in C^{\mathrm{aff}}$, $P \in \mathrm{Supp}(D)$ if and only if $\alpha_P > 0$. Moreover, $v_P(D)$ is the multiplicity of $x(P)$ as a root of a.
3. $\deg(b) < \deg(a)$, and for all P in the support of D, $b(x(P)) = y(P)$
4. $a | (f - b^2)$.

Now, we can generalize this Mumford representation to include points in $C^{\inf}$ by taking the homogenization of degree 4 of a and b. This is also done in [55].

To be precise, we create a triple of homogeneous polynomials (A, B, C), each of degree 4 such that $A, B, C \in k[x, z]$ where A is the degree 4 homogenization of a, B is the degree 4 homogenization of b, and C satisfies

$$B(x, z)^2 - F(x, z) = A(x, z)C(x, z). \tag{5.4}$$

This "projective Mumford representation" has some properties that we expect: The image of points P in the support of D_Q under the quotient map $\pi\colon C \to \mathbb{P}^1$ corresponds to the roots of A with the correct multiplicity, and we obtain $y(P)$ by evaluating $B(\pi(P))$. However, we may have $A(x, 1)$ be a non-monic polynomial in $k[x]$. This Mumford representation uniquely represents a divisor in general position, but note that if Q has degree 4, then a corresponding divisor D_Q as in Theorem 5.2 is generally not unique. We identify precisely which divisors represent one point of degree 4 in the following Lemma.

Lemma 5.5. Let the group $\Gamma \subset \mathrm{SO}(3)$ be generated by

$$t_\lambda = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda^{-1} \end{pmatrix}, \quad n_\mu = \begin{pmatrix} 1 & \mu & \mu^2 \\ 0 & 1 & 2\mu \\ 0 & 0 & 1 \end{pmatrix}, \quad w = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

for any $0 \neq \lambda, \mu \in k$. Two triples (A, B, C) and (A', B', C') represent the same point on J if and only if there exists a $\gamma \in \Gamma$ such that $(A, B, C) = (A', B', C')\gamma$, and they represent opposite points if and only if there exists a $\gamma \in -\Gamma$ such that $(A, B, C) = (A', B', C')\gamma$.

proof. See [55, Lemma 2.1]. □

Now, we will try to find a unique divisor representation of a given point $Q \in J$ of degree 4. The strategy is to apply the group action of Γ to obtain a triple (A, B, C) such that $A(0, 1) = 0$. We know from Theorem 2.37 that having a Weierstrass point at infinity (equivalently, $f_8 = 0$) results in a unique divisor in general position that represents a k-rational point on J. This argument can be generalized if we have that $P_{\infty,1}, P_{\infty,2}$ are k-rational (equivalently, f_8 is a nonzero square in k) and arbitrarily fix one of these two points at infinity, see for example [57]. Here, we will provide the analogous argument in terms of the parametrization of degree 4 divisors in general position using the homogeneous polynomial triple (A, B, C).

Suppose that $Q \in J(k)$ is of degree 4 and consider a corresponding divisor D_Q of degree 4 in general position that corresponds to a homogeneous polynomial triple (A, B, C). For a binary form $S(x, z)$, we define the notion *leading coefficient* to be the leading coefficient of the polynomial $s(x) := S(x, 1)$. Now, we apply actions of Γ to find a triple (A', B', C') such that $A'(0, 1) = 0$ and A has leading coefficient 1.

Note that the matrix $t_\lambda \in \Gamma$ scales A, hence we can assume without loss of generality that A is monic. Let a_4, b_4, c_4 be the leading coefficients of A, B, C, respectively, and similarly let a_4', b_4', c_4' be the leading coefficients of A', B', C', respectively. We multiply (A, B, C) with

$$wn_\mu w = \begin{pmatrix} 1 & 0 & 0 \\ -2\mu & 1 & 0 \\ \mu^2 & -\mu & 1 \end{pmatrix}$$

and obtain $(A, B, C)t_\lambda = (A', B', C')$ such that

$$a_4' = c_4\mu^2 - 2\mu b_4 + a_4.$$

The right-hand side of this equation is a polynomial in $k[\mu]$ with discriminant $4(b_4^2 - a_4c_4) = 4f_8$, using equation (5.4). It follows that we can fix A such that $A(0, 1) = 0$ uniquely if $f_8 = 0$. Also, if $4f_8$ is a nonzero square in k, then one can fix $\mu \in k$ arbitrarily such that $c_4\mu^2 - 2\mu b_4 + a_4 = 0$, and we fix A such that $A(0, 1) = 0$.

In this approach, the roots of A correspond to the points in the support of its corresponding divisor. Hence, requiring $A(0,1) = 0$ fixes one such point to infinity. Analogously to [57], if we have one rational point at infinity, we can fix it to obtain a unique, canonical divisor representation, and if we have two rational points at infinity, we can arbitrarily fix one of these two points to obtain a unique divisor representation.

Remark 5.6. Note that if f_8 is not a square in k, then for points $Q \in J(k)$ of degree 4, no obvious divisor representation exists. However, for points $Q \in J(k)$ of degree 2, the divisor D_Q as constructed above is unique.

5.2.3 Representing divisors in a Mumford representation

We now find a Mumford representation of points $Q \in J(k)$, provided that C has rational points at infinity. If Q has degree 4, then D_Q is a divisor of degree 4 in general position, hence a Mumford representation is established above. If Q has degree 2, then we can use Mumford representation to represent $D_Q - D_\infty$. This is precisely how MAGMA [4] represents points $Q \in J(k)$ if C^{inf} consists of k-rational points, and to make the Mumford Representation unique, certain coefficients in B are required to be zero [4, Points on the Jacobian]. To distinguish between a point of degree 2 and a point of degree 4, an additional parameter that tracks the degree of the divisor is stored alongside the polynomial tuple of the Mumford representation $\langle a, b\rangle$.

If C^{inf} consists of rational points, then Cantor's Algorithm as described in Theorem 2.38 can be generalized in order to perform arithmetic on $J(k)$ in the case where $\deg(f) = 8$. An implementation in MAGMA keeps track of the points at infinity that contribute to the representation on Pic^4_C directly [4, Points on the Jacobian], and [57] describes Jacobian arithmetic in a specific normalization in detail. If we need to perform the group law on $J(k)$, we only need C to have some k-rational point, and we can fix this point by mapping it to infinity under a change of coordinates. However, note that if $k = \mathbb{Q}$, many curves have no rational points [6]. A strength of our algorithm is that we do not actually need to perform arithmetic on $J(\mathbb{Q})$ because we can replace it by arithmetic on the Kummer completely. Hence, only arithmetic on reduced Jacobians $\tilde{J}(\mathbb{F}_p)$ for a suitable prime p is required. This is discussed more elaborately in Section 5.5.

5.3 The Kummer variety

The Kummer variety of the Jacobian of a hyperelliptic curve of genus 3 is explicitly constructed in [55, §2]. The defining equations of K are constructed by explicitly describing κ for any point $Q \in J$ of degree 4. This section summarizes the construction in [55, §2].

Consider a point $Q \in J$ of degree 4. Let the corresponding triple of homogeneous degree 4 polynomials be (A, B, C), and write

$$\begin{aligned} A(x,z) &= a_4x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4 \\ B(x,z) &= b_4x^4 + b_3x^3z + b_2x^2z^2 + b_1xz^3 + b_0z^4 \\ C(x,z) &= c_4x^4 + c_3x^3z + c_2x^2z^2 + c_1xz^3 + c_0z^4. \end{aligned}$$

Consider the affine variety $\mathcal{V} \subset (\mathbb{A}^5)^3 = \mathbb{A}^{15}$ defined by equation (5.4). In other words, we consider the coefficients of these polynomials as the coordinates of $\mathcal{V}$. Let Γ be the group as defined in Lemma 5.5. Then, we can consider the action of Γ on $\mathcal{V}$ to be the induced action on the coefficients of (A, B, C) on $\mathcal{V}$.

Now, we want to find a map $\mathcal{V} \to \mathbb{P}^7$ that is precisely invariant under $\pm\Gamma$. Using Lemma 5.5, it follows that this map is well-defined on the subset of points of J of degree 4, and it is precisely invariant under negation, i.e., multiplication by -1 on J.

First, we make some observations on Γ-invariant polynomials in the coefficients of the polynomials (A, B, C). Then, we will restrict to $\mathcal{V} \subset \mathbb{A}^{15}$. Consider all Γ-invariant (homogeneous) polynomials of degree 2.

In order to make such polynomials invariant under t_λ and w, we need that any monomial of such a Γ-invariant polynomial is, up to scaling, of the form b_ib_j or a_ic_j for some i or j.

In order to be invariant under n_μ, we specifically require our polynomial to consist of linear combinations of η_{ij}, where

$$\eta_{ij} = \begin{cases} b_{ii}^2 - a_ic_i & \text{if } i = j \\ 2b_{ij}^2 - a_ic_j - a_jc_i & \text{if } i < j. \end{cases}$$

If $i < j$, then

$$\begin{aligned} \eta_{ij} \xmapsto{n_\mu} &2(\mu a_i + b_i)(\mu a_j + b_j) - a_i(\mu^2 a_j + 2\mu b_j + c_j) - a_j(\mu^2 + 2\mu b_i + c_i) \\ =&2b_ib_j + 2\mu(a_ib_j + a_jb_i) + 2\mu^2 a_ia_j - 2\mu^2 a_ia_j - 2\mu(a_ib_j + a_jb_i) - a_ic_j - a_jc_i \\ =&\eta_{ij}, \end{aligned}$$

and η_{ii} is n_μ-invariant under a similar argument.

The η_{ij} can be written as the coefficients of the quadratic form $B_l^2 - A_lC_l \in \mathrm{Sym}^2\langle x_0, x_1, x_2, x_3, x_4\rangle$, where

$$\begin{aligned} A_l &= a_0x_0 + a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 \\ B_l &= b_0x_0 + b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 \\ C_l &= c_0x_0 + c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4, \end{aligned}$$

so

$$B_l^2 - A_lC_l = \sum_{i \le j} \eta_{ij}x_ix_j.$$

Hence, we can define a map $q\colon \mathbb{A}^{15} \to \mathrm{Sym}^2(\mathbb{A}^5)$ that maps the coefficients of (A, B, C) to the quadratic form $B_l^2 - A_lC_l$.

It is important to note that, although this quadratic form looks similar to equation (2.37), we have not restricted to $\mathcal{V} \in \mathbb{A}^{15}$ yet: this is a characterization of homogeneous Γ-invariant polynomials of degree 2 over points in $\mathbb{A}^{15}$.

Now, we consider the image of $\mathcal{V} \subset \mathbb{A}^{15}$ under q by requiring the relation described in (5.4). It follows from this relation that we can express the coefficients of f in terms of η_{ij}.

$$\begin{aligned} f_0 &= \eta_{00} \\ f_1 &= \eta_{01} \\ f_2 &= \eta_{02} + \eta_{11} \\ f_3 &= \eta_{03} + \eta_{12} \\ f_4 &= \eta_{04} + \eta_{13} + \eta_{22} \\ f_5 &= \eta_{14} + \eta_{23} \\ f_6 &= \eta_{24} + \eta_{33} \\ f_7 &= \eta_{34} \\ f_8 &= \eta_{44} \end{aligned}$$

Each η_{ij} consists of linear combinations of monomials of degree 2 of the form a_ic_j or b_ib_j (up to scaling). Therefore, negating all coefficients of B will not change this polynomial. It follows that these polynomials are $(\pm\Gamma)$-invariant.

Now, we consider such $(\pm\Gamma)$-invariant polynomials as projective coordinates in $\mathbb{P}^7$. We construct such coordinates in terms of functions because, canonically, a basis for the Riemann-Roch space $\mathcal{L}(2\Theta)$, where Θ

is the *Theta Divisor*, gives a projective embedding in $\mathbb{P}^7$. Further details are beyond the scope of this thesis, references can be found in the proof of Theorem 2.47 and Theorem 5.10.

We take six functions

$$\eta_{02}, \eta_{03}, \eta_{04}, \eta_{13}, \eta_{14}, \eta_{23},$$

together with the constant function 1. The last function is found using an approximation

$$Q_\lambda \xrightarrow{\lambda \to \infty} Q,$$

where $Q_\lambda \in J$ are points of degree 4 and

$$Q = [(x_1 : y_1 : 1) + (x_2 : y_2 : 1) - D_\infty]$$

is of degree 2 such that $(x_1 : y_1 : 1) \neq (x_2 : y_2 : 1)$ and $(x_1 : y_1 : 1) \neq \iota((x_2 : y_2 : 1))$. For details on this approximation, see [55, pg. 8]. The functions $\eta_{ij}^{(\lambda)}$ corresponding to Q_λ via the coefficients of the triple $(A, B.C)$ grow like

$$\begin{aligned}
\eta_{02}^{(\lambda)} &= -(x_1 x_2)\lambda^2 + O(\lambda) \\
\eta_{03}^{(\lambda)} &= (x_1 + x_2)x_1 x_2 \lambda^2 + O(\lambda) \\
\eta_{04}^{(\lambda)} &= -(x_1 x_2)\lambda^2 + O(\lambda) \\
\eta_{13}^{(\lambda)} &= (x_1^2 + x_2^2)\lambda^2 + O(\lambda) \\
\eta_{14}^{(\lambda)} &= (x_1 + x_2)\lambda^2 + O(\lambda) \\
\eta_{24}^{(\lambda)} &= -\lambda^2 + O(1).
\end{aligned} \tag{5.7}$$

Since the function

$$\eta = \eta_{02}\eta_{24} - \eta_{03}\eta_{14} + \eta_{04}^2 + \eta_{04}\eta_{13} \tag{5.8}$$

also grows like λ^2 and is linearly independent of the other 7 functions considered, we use η to be the last function to define the embedding $\kappa \colon J \to \mathbb{P}^7$.

In order to keep the relations simple, we replace the function η_{13} with $\eta_{04} + \eta_{13}$:

$$\begin{aligned}
\bar{\xi} &= (1 : \eta_{24} : \eta_{14} : \eta_{04} + \eta_{13} : \eta_{03} : \eta_{02} : \eta) \\
&:= (\xi_1 : \xi_2 : \xi_3 : \xi_4 : \xi_5 : \xi_6 : \xi_7 : \xi_8).
\end{aligned}$$

Now, (5.8) translates to the quadratic equation

$$\xi_1\xi_8 - \xi_2\xi_7 + \xi_3\xi_6 - \xi_4\xi_5 = 0. \tag{5.9}$$

Recall from Theorem 2.47 that K is always defined by quartic relations. In fact, the quadratic (5.9) divides 36 defining quartic relations on K [55, Theorem 2.5]. In genus 2, no quadratic relation is found: in this case, the Kummer variety is a hypersurface defined by one quartic relation[21, Eq. (1)]. Due to work by Ludwig Fürst, we now know that many quadratic relations show up for the Kummer variety of Jacobians of hyperelliptic curves of genus 4.

We now have found a map $\kappa \colon J \to \mathbb{P}^7$ defined by

$$\kappa \colon Q \mapsto (\xi_1 : \xi_2 : \xi_3 : \xi_4 : \xi_5 : \xi_6 : \xi_7 : \xi_8).$$

that is precisely invariant under multiplication by -1 on J.

Theorem 5.10. The image of the map κ describes an embedding of the Kummer variety $K \subseteq \mathbb{P}^7$ that is well-defined. Furthermore, K is defined by 70 quartics, of which 36 are multiples of the quadratic (5.9).

proof. Since all coordinates ξ_i are Γ-invariant, κ is well-defined, and since all coordinates ξ_i are $(-\Gamma)$-invariant, κ maps to $K \subseteq \mathbb{P}^7$. Now, we want to prove that the image of κ is equal to K.

There exists a canonical *Theta Divisor* Θ (see [8, Theorem 4.8.1] for the complex case, and [38] for an algebraic construction) such that an 8-dimensional basis of the (generalized) Riemann-Roch Space $\mathcal{L}(2\Theta)$ gives an embedding $K \to \mathbb{P}^7$. Since $\xi_1, \dots \xi_8$ are $\bar{k}$-linearly independent by construction, the image of κ indeed forms a basis of $\mathcal{L}(2\Theta)$.

The fact that K is defined by 70 quartics for which 36 are multiples of the quadratic (5.9) follows from the proof of [55, Theorem 2.5]. □

Remark 5.11. The 70 quartics are found in [55, pg. 9-10]. 15 of those quartics are found by observing that the rank of the symmetric matrix corresponding to the quadratic form $B_l^2 - A_l C_l$ is at most 3, hence 15 quartics can be found by determining the 4×4-minors and requiring them to vanish. The symmetric matrix corresponding to this quadratic form is

$$M = \begin{pmatrix} 2\eta_{00} & \eta_{01} & \eta_{02} & \eta_{03} & \eta_{04} \\ \eta_{01} & 2\eta_{11} & \eta_{12} & \eta_{13} & \eta_{14} \\ \eta_{02} & \eta_{12} & 2\eta_{22} & \eta_{23} & \eta_{24} \\ \eta_{03} & \eta_{13} & \eta_{23} & 2\eta_{33} & \eta_{34} \\ \eta_{04} & \eta_{14} & \eta_{24} & \eta_{34} & 2\eta_{33} \end{pmatrix} \tag{5.12}$$

and can be described in terms of $\xi_1, \dots \xi_7$ [55, eq. (2.7)]:

$$M = \begin{pmatrix} 2f_0\xi_1 & f_1\xi_1 & \xi_7 & \xi_6 & \xi_4 \\ f_1\xi_1 & 2(f_2\xi_1 - \xi_7) & f_3\xi_1 - \xi_6 & \xi_5 - \xi_4 & \xi_3 \\ \xi_7 & f_3\xi_1 - \xi_6 & 2(f_4\xi_1 - \xi_5) & f_5\xi_1 - \xi_3 & f_7\xi_1 \\ \xi_6 & \xi_5 - \xi_4 & f_5\xi_1 - \xi_3 & 2(f_6\xi_1 - \xi_2) & f_7\xi_1 \\ \xi_4 & \xi_3 & \xi_2 & f_7\xi_1 & 2f_8\xi_1 \end{pmatrix} \tag{5.13}$$

5.4 An explicit description of κ for points of degree 2.

In the end of [55, §2], an explicit mapping for κ is introduced for all points $Q \in J$ of degree 4. Also, using the approximation (5.7), for $Q = [P_1 + P_2 - D_\infty]$, the image of κ is described for the case where P_1 and P_2 are in C^{aff} and $P_1 \neq P_2$. This section provides a description of κ for all other possible cases.

Let $Q \in J$ be of degree 2; hence we can write

$$Q = [(x_1 : y_1 : z_1) + (x_2 : y_2 : z_2) - D_\infty],$$

and we denote $P_i = (x_i : y_i : z_i)$ for $1 \leq i \leq 2$.

Case 1: $z_1 = z_2 = 1, x_1 \neq x_2$

This is the case we have treated already in (5.7), see also [55, pg. 8]. Using the approximation (5.7), it is clear that ξ_1 vanishes as we approach such a point. We approach the point

$$\kappa(Q) = \left(0 : 1 : -(x_1 + x_2) : x_1x_2 : x_1^2 + x_1x_2 + x_2^2 : -(x_1 + x_2)x_1x_2 : (x_1x_2)^2 : \frac{2y_1y_2 - G(x_1, x_2)}{(x_1 - x_2)^2}\right) \tag{5.14}$$

where

$$G(x_1, x_2) = 2\sum_{j=0}^{4} f_{2j}(x_1x_2)^j + (x_1 + x_2)\sum_{j=0}^{3} f_{2j+1}(x_1x_2)^j. \tag{5.15}$$

Case 2: $P_1 = P_2, z_1 = z_2 = 1$

The approximation used to achieve (5.14) does not work in an affine way since $\ell(x)$ in the approximation [55, pg. 8] is undefined. We use the following expansion: let $A(x,z) = x^2 + \sigma_1 xz + \sigma_0 z^2 = (x - x_1 z)(x - x_2 z)$ as introduced in [55, pg. 11-12]. We can describe $\kappa(Q)$ by

$$\kappa(Q) = (0 : \sigma_0^2 : \sigma_0\sigma_1 : \sigma_0\sigma_2 : \sigma_1^2 - \sigma_0\sigma_2 : \sigma_1\sigma_2 : \sigma_2^2 : \xi_8), \tag{5.16}$$

where ξ_8 is expressed by expanding

$$((x_1 - x_2)^2\xi_8 - G(x_1, x_2))^2 - 4f(x_1)f(x_2) = 0 \tag{5.17}$$

in terms of ξ_8, dividing every coefficient by $(x_1 - x_2)^2 = \sigma_1^2 - \sigma_0\sigma_2$. The full expansion can be found in [55, §2] and is included in the appendices, in Equation (A.1). We denote s_i to be the coefficients of the expansion (A.1) so the expansion is written

$$s_2\xi_8^2 + s_1\xi_8 + s_0 = 0. \tag{5.18}$$

We have $(x_1 - x_2)^2 = s_2 = 0$. Also,

$$s_1 = -2G(x_1, x_1) = -4f(x_1),$$

hence if $s_1 = 0$, then $f(x_1) = 0$, hence P_1 is a Weierstrass point, so the divisor $P_1 + P_2 = 2P_1$ is not in general position. (In fact, we obtain $Q = 0 \in J$). It follows that we may assume that $s_1 \neq 0$, hence we have that ξ_8 is uniquely determined as $-s_0/s_1$.

We conclude that in this case,

$$\kappa(Q) = (0 : 1 : -2x_1 : x_1^2 : 3x_1^2 : -2x_1^3 : x_1^4 : -s_0/s_1). \tag{5.19}$$

Case 3: $P_1 \in C_{\text{aff}}$, $P_2 = (1 : w : 0)$ for some $w \in \bar{k}$.

We observe that $w^2 = f_8$. We use the following approximation. Let $Q_\lambda = (x_1, y_1) + (\lambda, w_\lambda) - D_\infty$ such that $w_\lambda^2 = f(\lambda)$. Then, note that

$$w_\lambda = (\pm w)\lambda^4 + O(\lambda^{7/2}).$$

We choose w_λ such that $w_\lambda \to w$ (and not $w_\lambda \to -w$) as $\lambda \to \infty$.

Using (5.14), we get that the coordinates of $\kappa(Q_\lambda)$ grow like

$$\begin{aligned}
\xi_1 &= O(1)\\
\xi_2 &= O(1)\\
\xi_3 &= -\lambda + O(1)\\
\xi_4 &= x_1\lambda + O(1)\\
\xi_5 &= \lambda^2 + O(\lambda)\\
\xi_6 &= -x_1\lambda^2 + O(\lambda)\\
\xi_7 &= x_1^2 + O(\lambda)\\
\xi_8 &= (y_1 w - 2f_8 x_1^2 - f_7 x_1^3)\lambda^2 + O(\lambda)
\end{aligned}$$

(To justify ξ_8, note that $G(x_1, \lambda) = (2f_8 x_1^4 + f_7 x_1^3)\lambda^4 + O(\lambda^3)$, and its denominator is $\lambda^2 + O(1)$. It is important to remember that the projective model is given in the weighted projective plane $\mathbb{P}_3^2 = \mathbb{P}_{1,4,1}^2$.)

We conclude, using this approximation, that

$$\kappa(Q) = (0 : 0 : 0 : 0 : 1 : -x_1 : x_1^2 : 2y_1 w - 2f_8 x_1^4 - f_7 x_1^3). \tag{5.20}$$

Case 4: $P_1 = P_2 = (1 : w : 0)$ for a $w \in \bar{k}$.

Note that $[2P_{\infty,1} - D_\infty] = -[2P_{\infty,2} - D_\infty]$, hence $\kappa([2P_{\infty,1} - D_\infty) = \kappa([2P_{\infty,2} - D_\infty])$, therefore we have a unique point on K whose pre-image under κ consists of these two points.

Similarly to case 2, we take the expansion (5.18) and remark that in our case, $\sigma_1 = \sigma_2 = 0$, which reduces equation (A.1) to

$$4f_8\xi_8 - 4f_6f_8 + f_7^2 = 0,$$

hence

$$\kappa(Q) = (0:0:0:0:0:0:4f_8:4f_6f_8 - f_7^2). \tag{5.21}$$

Lastly, [55] describes that the origin of J can be found by approximating $0 = [(x_1, y_1) + (x_1, -y_1) - D_\infty]$. This will give the point

$$\kappa(0) = (0:0:0:0:0:0:0:1). \tag{5.22}$$

Remark 5.23. One might wonder why the expansion (5.18) is not immediately used for points represented by one affine point. The issue here is that $s_2 = (x_1 - x_2)^2 \neq 0$, which gives us two options for ξ_8. Hence, this expansion does not take into account which point at infinity is in the support of D_Q.

Remark 5.24. In [40, §2], the explicit map κ is given for the case where f has degree 7, using the corresponding divisor representation on Pic^3_C.

5.5 Using arithmetic on reduced Jacobians to compute rational torsion points

Recall from Section 5.2 that we can represent every point $Q \in J(k)$ uniquely in terms of a divisor in general position if $C^{\inf}$ consists of rational points, and that the Mumford representation of Q induces a generalization of Cantor's Algorithm; an implementation is found in [4]. A description and corresponding implementation is found in [57]. If we find any rational point $P \in C(k)$, then we can use a change of coordinates that maps P to infinity, using the transformation defined by the matrix in (2.45). Hence, there is a known algorithm to perform arithmetic on $J(k)$ if we know a rational point in $C(k)$, but no algorithm is known for the case where we do not know a rational point in $C(k)$.

As discussed in Section 4.1 and in Section 5.1, we do not need to perform arithmetic on $J(\mathbb{Q})$ in order to find $J(\mathbb{Q})_{\mathrm{tors}}$. We only need to perform arithmetic on the reduced Jacobians $\tilde{J}(\mathbb{F}_p)$ for certain primes of good reduction p. Specifically, in step 3 of Algorithm 4.22 we compute the structure of reduced Jacobians $\tilde{J}(\mathbb{F}_p)$ for some primes of good reduction p, and in step 2.2 of Algorithm 4.20, which is called in step 4 of Algorithm 4.22, we search for elements g of the q-parts of $\tilde{J}(\mathbb{F}_p)$ and find the smallest $m \geq 1$ such that $q^m \cdot g$ lifts to $J(\mathbb{Q})$.

In both steps, we select the primes p to be primes of good reduction p, and when considering q-parts of $\tilde{J}(\mathbb{F}_p)$, we require $p \neq q$. This still allows us to choose from an infinite amount of primes p. Therefore, we can adjust the procedure in a way that we pick primes that have particularly nice properties in the context of reduction modulo p.

Recall from Section 4.1 that we use a model such that $f \in \mathbb{Z}[x]$.

Case 1: If f_8 is a square in $\mathbb{Z}$, then $\tilde{f}_8 \equiv f_8 \mod p$ is a square in $\mathbb{F}_p$ for any prime p. Hence, the points in $\tilde{C}^{\inf}$ are rational and arithmetic on $\tilde{J}(\mathbb{F}_p)$ is already implemented.

Case 2: If f_8 is not a square in $\mathbb{Z}$, but a naive search for points on $C(\mathbb{Q})$ gives us some rational point $P = (x_1, y_1) \in C(\mathbb{Q})$, we can simply use the transformation defined by the matrix (2.45) to map P to $C^{\inf}$, and we proceed as in case 1.

Case 3.1: If f_8 is not a square in $\mathbb{Z}$, and no rational point $P \in C(\mathbb{Q})$ is found, then in step 2 of Algorithm 4.22, we try to consider primes of good reduction p such that $\tilde{f}_8 \equiv f_8 \mod p$ is a square in $\mathbb{F}_p$.

Case 3.2: If primes of good reduction p such that $\tilde{f}_8$ is a square in $\mathbb{F}_p$ are not easily found, we search for primes p such that $\tilde{C}(\mathbb{F}_p)$ contains any rational points. The Hasse-Weil bound gives us a guarantee that we can always find such primes:

Theorem 5.25. Hasse-Weil Let C be a smooth, projective, absolutely irreducible curve of genus g over a finite field $\mathbb{F}_p$. Then,

$$|\#C(\mathbb{F}_p) - p + 1| \leq 2g\sqrt{p}.$$

proof. This is a particular case of the first part of [23, Exercise 10.7.9]. We show that it follows by using the notation of the referenced book. This identity follows directly from the Weil bound [23, Theorem 10.7.5], the fact that $|\alpha_i| \leq \sqrt{q}$, and the triangle inequality on $\mathbb{C}$. □

Applying this to our case gives

$$\#\tilde{C}(\mathbb{F}_p) \geq p - 1 - 6\sqrt{p},$$

hence $\#\tilde{C}(\mathbb{F}_p) \geq 1$ if $p \geq 41$. Therefore, we can always find primes of good reduction p such that a rational point on $\tilde{C}(\mathbb{F}_p)$ exists, and it is easy to find such a rational point.

We perform arithmetic on $\tilde{J}(\mathbb{F}_p)$ as follows. We fix p, and take $\tilde{P} \in \tilde{C}(\mathbb{F}_p)$. Let $\phi\colon \tilde{C} \to \tilde{C}'$ be a change of coordinates such that $\phi(\tilde{P})$ is a point at infinity. If $\tilde{J}'$ is the Jacobian of $\tilde{C}'$, then we have an algorithm for arithmetic on $\tilde{J}'(\mathbb{F}_p)$. Since $\tilde{J}'(\mathbb{F}_p) \cong \tilde{J}(\mathbb{F}_p)$, we use this to do arithmetic on $\tilde{J}(\mathbb{F}_p)$.

Now, one has to be careful. Although an isomorphism $\phi_* : \tilde{J} \to \tilde{J}'$ exists, we still need to lift original points $\tilde{Q} \in \tilde{J}(\mathbb{F}_p)$. To make the strategy precise, we adjust step 3 and 4 of Algorithm 4.22 in the following way. Here, by $\tilde{K}$ and $\tilde{K}'$, we denote the Kummer varieties of $\tilde{J}$ and $\tilde{J}'$, respectively.

- In step 3 and 4 of Algorithm 4.22, we find suitable primes p with the extra condition that $\tilde{C}(\mathbb{F}_p)$ is not empty. Hence, we have a rational point $\tilde{P} \in \tilde{C}(\mathbb{F}_p)$
- In Algorithm 4.20 called in step 4 of Algorithm 4.22, set G_0 to be the q-part $\tilde{J}'(\mathbb{F}_p)$. In step 2.2, find the smallest m such that $\kappa(\phi^{-1}(q^m \cdot g))$ lifts to $J(\mathbb{Q})$.

Remark 5.26. Although not necessary, it is convenient to have an induced change of coordinates $\phi_K : K \to K'$ for a change of coordinates $\phi\colon C \to C'$. A description is given in Appendix B. In the notation above, we can replace $\kappa \circ \phi_*^{-1}$ by $\phi_K^{-1} \circ \kappa'$ using the commutative diagram (B.1). This is convenient in the implementation of the algorithm.

5.6 Computing the rational two-torsion points.

As mentioned in Section 4.6, we use a global computation of the structure of $J(\mathbb{Q})[2]$. This follows from [53, Lemma 4.3, Lemma 5.6] for any field extension of $k \supseteq \mathbb{Q}$. The structure of $J(k)[2]$ can be found by factorizing f. Here, we will describe how we find $J(k)[2]$ for genus 3 hyperelliptic curves.

We first treat the case where $\deg(f) = 7$. Using [53, Lemma 4.3], we obtain the prime factorization of $f = g_1 \cdots g_r$ over k (since f is separable, the g_i are pairwise coprime). Then the generators of $J(\mathbb{Q})[2]$ are represented by divisors corresponding to the Mumford representation (as discussed in Theorem 2.37) of the form

$$\langle g_1, 0\rangle, \ldots, \langle g_{r-1}, 0\rangle.$$

Now, suppose $\deg(f) = 8$. Using [53, Lemma 5.6], we find generators of $J(\mathbb{Q})[2]$ by considering all monic, irreducible polynomials $g_1, \ldots, g_r$ of even degree that divide f. The polynomials g_i correspond to points on $J(\mathbb{Q})[2]$ in the following sense: we use [55, §5] to observe that each point in $J[2]$ (not necessarily k-rational) is represented by divisors

$$\left[\sum_{\omega\in\Omega_1} (\omega, 0)\right] - \frac{\#\Omega_1}{2}[D_\infty] = \left[\sum_{\omega\in\Omega_2} (\omega, 0)\right] - \frac{\#\Omega_1}{2}[D_\infty] \tag{5.27}$$

where $\{\Omega_1, \Omega_2\}$ is a partition of $\Omega = \{\text{roots of } f \text{ over } \bar{\mathbb{Q}}\}$, where both Ω_1 and Ω_2 have even cardinality.

Now, each g_i of degree 2 induces the Mumford representation $\langle g_i, 0\rangle$, corresponding to a point of degree 2 on $J[2]$ that is k-rational. These points are the *odd* rational 2-torsion points in [55, §5].

For a factor g_i dividing f that has degree 4, the Mumford representation $\langle g_i, 0\rangle$ corresponds to point of degree 4 on $J[2]$ that is k-rational. Such points are the *even* rational 2-torsion points in [55, §5].

Now, we refer back to [53, Lemma 5.6]. We find generators as follows: if $f = g_1 \cdots g_r$, then $J(\mathbb{Q})[2]$ is generated by points corresponding to the polynomials $g_1, \ldots g_{r-1}$. If $g_1 \ldots g_r \neq f$, then $J(\mathbb{Q})[2]$ is generated by points corresponding to the polynomials $g_1, \ldots, g_r$.

5.7 Checking whether a rational point on the Kummer has a rational pre-image on the Jacobian.

This section gives a procedure that decides whether the pre-image in κ of a point

$$R = (\xi_1 : \ldots : \xi_8) \in K(k)$$

is in $J(k)$ or not. This is performed in step 7 of Algorithm 4.2. Throughout this section, we assume a scaling such that the first nonzero coordinate of R is equal to 1.

By construction, if $Q \in J$ such that $\kappa(Q) = R$, then Q is of degree 4 if and only if $\xi_8 \neq 0$. Also, $Q = 0$ if and only if $R = (0:0:0:0:0:0:0:1)$, see (5.22).

5.7.1 Finding a pre-image for degree 4 points

The case where $Q \in J$ has degree 4 is treated in [55, §4]. The method can be summarized as follows. For any nonzero function h on J that is odd (i.e., $h(Q') = -h(-Q')$ for all $Q' \in J$), we have that h^2 is an even function on J (i.e., $h^2(Q') = h^2(-Q')$ for all $Q' \in J$). Since h^2 is even, one can find an induced function h_k^2 on K such that $h^2(Q') = h_K^2(\kappa(Q'))$ for all $Q' \in J$. Suppose that $Q \in J$ is rational, then $h^2(Q) = h_K^2(R)$ is a square in k. Conversely, suppose $h_K^2(R)$ is a *nonzero* square in k. Since $R = \kappa(Q) \in K(k)$, we have that $\sigma(Q) = \pm Q$ for all $\sigma \in G_k$. If Q is not rational, then $\sigma(Q) = -Q$. Hence,

$$\sigma(h(Q)) = h(\sigma(Q)) = h(-Q) \neq h(Q),$$

but this contradicts with $h(Q) \in k$. It follows that Q must be a rational point in J.

By choosing some particular functions h, an image $h_K^2(R)$ is derived to be an expression in 3×3-minors of M, where M is the matrix given in (5.13), and one can check whether a point $R \in K(k)$ has a pre-image in $J(k)$. If one of these expressions is not a square in k, then $\kappa^{-1}(R)$ does not consist of rational points. If all expressions are squares in k and one of them is nonzero, then $\kappa^{-1}(R)$ consists of rational points. If all expressions are equal to $0 \in k$, then a change of basis implies that $Q \in J[2]$. Hence, the pre-image $\kappa^{-1}(R)$ consists of a unique, rational point on $J(k)$.

5.7.2 Finding a pre-image for degree 2 points

If Q has degree 2, or equivalently $\xi_1 = 0$, then [55, §4] suggests to simply consider the map κ explicitly. We follow this suggestion by using our explicit description of κ for points of degree 2 on J. From now on, we assume $\xi_1 = 0$.

Recall that we can fix D_Q such that $Q = [D_Q]$ of the form

$$D_Q = P_1 + P_2 - D_\infty$$

for points P_1, P_2 in C. We check whether $Q \in J(k)$ using the uniqueness of the divisor D_Q.

Lemma 5.28. Let Q be of the form described in Equation (5.29). Then, $Q \in J(k)$ if and only if the divisor D_Q corresponding to Q is fixed under G_k.

proof. Q is rational if and only if G_k fixes the divisor class $[D_Q - D_\infty] \in \mathrm{Pic}_C^0$ (see Section 2.2). Using Lemma 5.3, D_Q is the unique divisor of degree 4 such that $D_Q - D_\infty$ is in general position. For any element $\sigma \in G_k$, we have that $\sigma(D_Q - D_\infty) = \sigma(D_Q) - D_\infty$ is in general position and of degree 2. If $Q \in J(k)$, then it follows by uniqueness that $D_Q = \sigma(D_Q)$. If $D_Q = \sigma(D_Q)$, then $\sigma(D_Q - D_\infty) = D_Q - D_\infty$, hence $D_Q - D_\infty$ is a rational divisor, hence Q is rational. □

Using the explicit maps of κ as described in Section 5.4, we can always observe how many of the points P_1, P_2 are at infinity. It turns out that the cases where at least one of the points P_1, P_2 is at infinity are the easiest to determine.

First, if $\xi_3 = \xi_4 = 0$, but $\xi_5 \neq 0$, then we have the form described in Equation (5.20). The pre-image is in $J(k)$ if and only if the divisor $(x_1 : y_1 : z_1) + P_{\infty,1}$ is rational, which we check by testing whether $f(-\xi_6) = y_1^2$ is a square in k and C has rational points at infinity.

Now, if $\xi_3 = \xi_4 = \xi_5 = \xi_6 = 0$, but $\xi_7 \neq 0$, then the pre-image of R has the form $[2P_{\infty,1} - D_\infty]$, and is rational if and only if C has rational points at infinity.

The case where $\xi_3 \neq 0$ is left. Using Equation (5.14), $Q \in \kappa^{-1}(R)$ has the form

$$Q = [(x_1 : y_1 : 1) + (x_2 : y_2 : 1) - D_\infty] \tag{5.29}$$

and R has the form

$$\left(0 : 1 : -(x_1 + x_2) : x_1x_2 : x_1^2 + x_1x_2 + x_2^2 : -(x_1 + x_2)x_1x_2 : (x_1x_2)^2 : \frac{2y_1y_2 - G(x_1, x_2)}{(x_1 - x_2)^2}\right) \in K(k),$$

where

$$G(x_1, x_2) = 2\sum_{j=0}^{4} f_{2j}(x_1x_2)^j + (x_1 + x_2)\sum_{j=0}^{3} f_{2j+1}(x_1x_2)^j.$$

We will now give an approach to decide whether $\kappa^{-1}(R)$ is in $J(k)$ or not. Note that $R \in K(k)$, so we can find $x_1 + x_2, x_1x_2$ and y_1y_2, and these three expressions are in k.

Using this information, we can find

$$\begin{aligned} y_1^2 + y_2^2 &= f(x_1) + f(x_2) \\ &= \sum_{j=0}^{8} f_j(x_1^j + x_2^j). \end{aligned} \tag{5.30}$$

given that, using binomial expansion,

$$x_1^j + x_2^j = \sum_{\substack{r+2s=j,\\ r,s\in\mathbb{Z},\\ r\geq 0, s>0}} \binom{s}{n}(x_1^r + x_2^r)(x_1x_2)^s.$$

Since we know $x_1^j + x_2^j$ for $0 \leq j \leq 2$ using the coordinates of R, we can compute subsequent terms inductively. Using this, we can compute $y_1^2 + y_2^2$. Knowing y_1y_2, we now can compute $(y_1 + y_2)^2$ and $(y_1 - y_1)^2$.

Using Lemma 5.28, Q is a rational point if and only if the divisor D_Q is rational. Since D_∞ is always rational, we need to check whether the divisor $D := (x_1, y_1) + (x_2, y_2)$ is rational. The divisor D is a rational divisor if and only if $\sigma(D) = D$ for all $\sigma \in G_k$. The first step is to determine whether $y_1 + y_2$ is rational.

Lemma 5.31. If $(y_1 + y_2)^2$ is not a square in k, then Q is not a rational point on $J(k)$.

proof. Assume that $(y_1 + y_2)^2$ is not a square in k, then $y_1 + y_2$ is not in k. Hence, the polynomial $b := (y - y_1)(y - y_2) = y^2 - (y_1 + y_2)y + y_1y_2$ is not defined over k. Since $y_1y_2 \in k$, the field extension $k(y_1, y_2) \neq k$ is not quadratic. It follows that the minimal polynomial of y_1 has roots distinct from y_1, y_2, hence there exists a $\sigma \in G_k$ such that $\sigma(y_1) \neq y_1$ and $\sigma(y_1) \neq y_2$. Clearly, $\sigma(D) \neq D$, hence Q is not a rational point. □

Now, we can determine whether $\kappa^{-1}(R)$ is rational or not. For this, we define the polynomials $a := (x - x_1)(x - x_2)$ and $b := (y - y_1)(y - y_2)$. Since $x_1 + x_2, x_1x_2 \in k$, we have that a is defined over k. If $(y_1 + y_2)^2$ is a square in k, then we similarly have that b is defined over k.

Lemma 5.32. Let R be such that $y_1 + y_2 \in k$. Define the polynomials $a := (x - x_1)(x - x_2)$ and $b := (y - y_1)(y - y_2)$. Then, $\kappa^{-1}(R)$ consists of rational points if and only if one of the following conditions is satisfied:

1. $\mathrm{Disc}(a), \mathrm{Disc}(b)$ are squares in k
2. $\mathrm{Disc}(a)$ is not a square in k, $\mathrm{Disc}(b) = 0$
3. $\mathrm{Disc}(b)$ is not a square in k, $\mathrm{Disc}(a) = 0$
4. $\mathrm{Disc}(a)$ and $\mathrm{Disc}(b)$ are both not squares in k, and have the same squarefree part in k.

proof. We prove this lemma using a case distinction.

Clearly, if $\mathrm{Disc}(a), \mathrm{Disc}(b)$ are squares in k, then $x_1, x_2, y_1, y_2 \in k$, hence $\sigma(D) = D$ for all $\sigma \in G_k$. Hence, (1) implies that Q is rational.

If $\mathrm{Disc}(a)$ is not a square in k, then the field $k(x_1, x_2)$ is a quadratic field extension of k, hence Galois (recall that $\mathrm{char}(k) \neq 2$). The nontrivial automorphism $\sigma \in \mathrm{Gal}(k(x_1, x_2)/k)$ satisfies $\sigma(x_1) = x_2$. In this case, $\sigma(D) = D$ if and only if $\sigma(y_1) = y_2$. If we then have that $\mathrm{Disc}(b)$ is a square in k, we have $y_1, y_2 \in k$, hence $\sigma(y_1) = y_2$ if and only if $y_1 = y_2$, equivalently, $\mathrm{Disc}(b) = 0$. Hence, (2) implies that Q is rational. Analogously, (3) implies that Q is rational.

Conversely, if $\mathrm{Disc}(a)$ is a square in k and Q is rational, then (1) or (3) must hold. Similarly, if $\mathrm{Disc}(b)$ is a square in k and Q is rational, then (1) or (2) must hold.

Now, suppose $\mathrm{Disc}(a)$ and $\mathrm{Disc}(b)$ are both not squares in k, and have the same squarefree part. Then, $\ell := k(x_1, x_2) = k(y_1, y_2)$ is a quadratic extension of k, hence a Galois extension. The minimal polynomial of x_1 is a, and the minimal polynomial of y_1 is b. It follows that the nontrivial automorphism $\sigma \in \mathrm{Gal}(\ell/k)$ satisfies $\sigma(x_1) = x_2$ and $\sigma(y_1) = y_2$. Hence, (4) implies that Q is rational.

Conversely, suppose $\mathrm{Disc}(a)$ and $\mathrm{Disc}(b)$ are both not squares in k and have a distinct squarefree part d. Then, $k(x_1, x_2) \neq k(y_1, y_2)$. Since $k(x_1, x_2)$ and $k(y_1, y_2)$ are quadratic extensions of k, they are Galois extensions of k, hence the compositum ℓ of $k(x_1, x_2)$ and $k(y_1, y_2)$ is a Galois extension of k. It follows that $\mathrm{Gal}(\ell/k)$ is of size 4 with two generators. One of these generators σ then satisfies $\sigma(x_1) = x_2$ and $\sigma(y_1) = y_1$. For $\sigma(D) = D$ to hold, we must have $\sigma(y_1) = y_2$. Since $\mathrm{Disc}(b)$ is not a square in k, in particular $\mathrm{Disc}(b) \neq 0$, hence $y_1 \neq y_2$. It follows that Q cannot be rational in this case. □

6 Examples and results

6.1 Overview

We have implemented the algorithm of Chapter 4 for hyperelliptic curves of genus 3 using the explicit theory discussed in Chapter 5. The implementation used the MAGMA computational algebra system [4]. The source code can be found on `https://github.com/bernoreitsma/g3hyptorsion`. This chapter provides some examples of curves where $J(\mathbb{Q})_{\text{tors}}$ was previously unknown. Furthermore, we have computed rational torsion subgroup of Jacobians of 67879 hyperelliptic curves of genus 3 with low discriminant, provided in a database that is maintained by Andrew V. Sutherland [56], which is planned to be put into the LMFDB [3]. Sometimes, some MAGMA-procedures are mentioned, for this we refer to [4].

6.2 Example computations

The following example has been suggested by Andrew V. Sutherland. Since no rational point in $C(\mathbb{Q})$ is known, this example illustrates how we can compute $J(\mathbb{Q})_{\text{tors}}$ without an implementation of the group law on $J(\mathbb{Q})$.

Example 6.1. Let C be a hyperelliptic curve defined over $\mathbb{Q}$ with the model

$$y^2 + (x^4 + x^3 + 1)y = x^8 - 4x^7 + 8x^6 - 9x^5 + 7x^4 - 4x^2 + 5x - 2.$$

Using MAGMA, we find a simplified, reduced Weierstrass model

$$y^2 = 5x^8 - 14x^7 + 33x^6 - 36x^5 + 30x^4 + 2x^3 - 16x^2 + 20x - 7.$$

The Jacobian J of C seems to have a point of order 13 locally everywhere, but no rational point on J has previously been found. Since $f_8 = 5$ is not a square in $\mathbb{Q}$, and C does not appear to have any rational points, there is no obvious transformation to a curve that has a rational point at infinity: we land in case 3 in Section 5.5, so we have to find suitable primes such that we can find rational points on reduced curves that we can fix at infinity using transformations.

Indeed, when requesting `TorsionBound()` in MAGMA, the result is a multiplicative upper bound of 13. For our reduction, we pick the prime of good reduction $p = 3$, resulting in the reduced model

$$\tilde{y}^2 = 2\tilde{x}^8 + \tilde{x}^7 + 2\tilde{x}^3 + 2\tilde{x}^2 + 2\tilde{x} + 2.$$

Since $2 \notin \mathbb{F}_3^2$, we map the point $(2 : 1 : 1)$ to infinity using the transformation defined by the matrix

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

the isomorphic image curve $\tilde{D}$ of this transformation is then defined by

$$\tilde{y}^2 = \tilde{x}^8 + \tilde{x}^7 + \tilde{x}^6 + 2\tilde{x}^3 + \tilde{x}^2 + 2$$

which has a a unique Mumford representation since $\tilde{f}_8 = 1$ is a square in $\mathbb{F}_3$. Using Appendix B with A^{-1}, we compute the Kummer variety $K_{\tilde{C}}$ of $\tilde{C}$ using $K_{\tilde{D}}$ and create the induced change of coordinates $K_{\tilde{D}} \to K_{\tilde{C}}$.

During the lifting procedure, we indeed find a point of order 13 on $K(\mathbb{Q})$. Explicitly,

$$R = (0 : 1 : -1 : 1 : 0 : -1 : 1 : 20).$$

which, using our implementation of Section 5.7, has a pre-image $\kappa^{-1}(R)$ in $J(\mathbb{Q})$. We will explicitly compute a divisor representing this rational point.

We fix Q to be one of the two points in $\kappa^{-1}(R)$. Using Section 5.4, the unique divisor D_Q representing the point Q has affine support of degree 2, and we can write it in the form $Q = [(x_1 : y_1 : 1) + (x_2 : y_2 : 1) - D_\infty]$. Equation (5.14) tells us that $x_1 + x_2 = x_1 x_2 = 1$, hence $a(x) = (x - x_1)(x - x_2) = x^2 - x + 1$. After some more calculations on ξ_8, and computing $y_1^2 + y_2^2$ using Equation (5.30), we see that $2y_1y_2 = 2$, $y_1^2 + y_2^2 = -1$. It follows that $y_1 + y_2 = \pm 1$, and, defining $b(y) = (y - y_1)(y - y_2)$, we compute $\mathrm{Disc}(b) = -3$. Hence, $x_1, x_2, y_1, y_2 \in \mathbb{Q}(\sqrt{-3})$.

Since $a(x) = x^2 - x + 1$, we fix (without loss of generality) $x_1 = 1 + \zeta_3$ and $x_2 = \frac{1}{x_1} = 1 + \zeta_3^2 = 1 + \bar{\zeta_3}$, where $\zeta_3 = \frac{\sqrt{-3}-1}{2}$ is the primitive 3rd root of unity, and $\bar{\zeta} = \frac{-\sqrt{-3}-1}{2}$ is the conjugate of ζ_3 with respect to the number field $\mathbb{Q}(\sqrt{-3})$. Equivalently, x_1 and x_2 are primitive 6-th roots of unity. Since $y_1^2 = f(x_1) = \zeta_3$, y_1 is also a 6-th root of unity, and we can conclude the following:

$J(\mathbb{Q})_{\mathrm{tors}}$ is a cyclic group of order 13 generated by the point

$$Q = [(1 + \zeta_3 : 1 + \zeta_3 : 1) + (1 + \bar{\zeta_3} : 1 + \bar{\zeta_3} : 1) - D_\infty].$$

We conclude that $Q \in J(\mathbb{Q})$ using Lemma 5.28: the nontrivial action $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$ fixes Q.

The following example is found in [29, Example 3.9].

Example 6.2. The curve C defined by

$$y^2 = \frac{46656}{3125}x^7 + \frac{407097961}{39062500}x^6 + \frac{281238453}{3906250}x^5 - \frac{22959453}{312500}x^4 - \frac{2767361}{15625}x^3 + \frac{381951}{2500}x^2 + \frac{3093}{6250}x + \frac{1}{2500}$$

has a torsion point of order 41. We use `IntegralModel()` and `ReducedModel()` to find a reduced Weierstrass model with integral coefficients with f equal to

$$583200000x^7 + 40709761x^6 + 2812384530x^5 - 2869931625x^4 - 6918402500x^3 + 5967984375x^2 + 19331250x + 15625.$$

Indeed, we find a point of order 41. Since the `TorsionBound()` of the curve is also 41, we have immediately found $J(\mathbb{Q})_{\mathrm{tors}}$ entirely. Since the defining polynomial of C is of degree 7, we have a unique point at infinity, and hence a canonical divisor representation. The divisor

$$(0 : 125 : 1) - P_\infty$$

represents an explicit point of order 41 with the divisor representation as introduced in Theorem 2.34.

It is also noteworthy that this Jacobian is absolutely irreducible (simple), this is checked by finding a sufficient condition for absolute irreducibility using [27, §3], as implemented the Steffen Müller. An abelian variety A defined over k is said to be absolutely irreducible if it has no sub-abelian varieties other than A itself and the trivial variety over $\bar{k}$. Hence, it is not possible to decompose J into abelian varieties of lower dimension. Therefore, this torsion structure cannot be constructed using lower-dimensional varieties such as the Jacobians of genus 2 hyperelliptic curves or elliptic curves, e.g., along the lines of [26]

One may wonder whether the high complexity of the curves' coefficients poses a challenge on the computational aspect of the algorithm. The height bound β for torsion points as computed in Theorem 3.15 is such that $\log(\beta) \approx 97$, hence we need $N \log(p) \geq 11 \log(2) + 194$ in step 3 of Algorithm 4.2. We pick $p = 7$; this leads us to the required p-adic precision $O(p^N)$ where $N = 128$, which is reached in just 7 steps in step 3, due to our approximation being quadratic.

Moreover, in practice, we check whether a p-adic approximation already lifts to a 41-torsion point after every iteration using Remark 4.17: if we find a lift R in $K(\mathbb{Q})$ of order 41 and $\kappa^{-1}(R) \subseteq J(\mathbb{Q})$, then we have found the unique lift $R \in K(\mathbb{Q})$ already. In practice, we reach p-adic precision $O(p^N)$ where $N = 32$ in the lifting procedure, and we already find the point generating $J(\mathbb{Q})_{\mathrm{tors}}$.

6.3 Results from the database computations

Andrew V. Sutherland has a file with 67879 genus 3 hyperelliptic curves of small discriminant [56], which is aimed to be provided to the L-functions and Modular Forms Database (LMFDB) [3]. The rational torsion subgroups of the corresponding Jacobians have been computed using this implementation. For the complete database corresponding to the 67879 curves, we refer to the file `database.txt` in `https://github.com/bernoreitsma/g3hyptorsion`. This section provides some statistics on this database, and also presents some curves that have specific properties.

6.3.1 Statistics

We gathered some statistics from this database. All torsion structures and the frequency of their appearance can be found in Appendix C. Here, we mention a few statistics.

- 39707 of the 67879 ($\approx 58.5\%$) of the curves yield a trivial rational torsion subgroup.
- 5597 Jacobians ($\approx 8.2\%$) give an odd torsion point.
- 24489 Jacobians ($\approx 36.1\%$) have a nontrivial cyclic rational torsion subgroup, hence 3683 ($\approx 5.4\%$) have 2 or more generators.
- Of the non-cyclic torsion subgroups found, 3413 have 2 generators, 265 have 3 generators, and 5 torsion subgroups have 4 generators. The 5 curves that have four generators all have at least 3 of these generators of order 2.
- From the database, 13 Jacobians have a torsion subgroup such that there are two elementary divisors that are not equal to 2.

Among the Jacobians found with two elementary divisors not equal to 2 is the Jacobian with the largest rational torsion found, where $J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This case is featured in Example 6.5.

In [43, Section 3.1], a survey of all torsion points of a certain order that have been found for Jacobians of hyperelliptic curves of genus 2, 3, and 4 is given. Compared to all known orders of torsion points of Jacobians corresponding to hyperelliptic curves of genus 3, as presented in [43, Table 3.2], we have found the following points with new orders during our computations:

$$12, 13, 14, 16, 17, 18, 20, 21, 23, 46, 60.$$

(Note that a point of order 46 implies that we also found a point of order 23). With the exception of order 60, we were also able to determine an example of a curve that has an absolutely irreducible Jacobian with a rational torsion point of these orders. Examples of each of these are given in Appendix C. Also, for the torsion points of order $11, 19, 24$, no verified absolutely irreducible Jacobians have been found to date. We were able to verify irreducible Jacobians with rational points of these orders. Example curves are also included in Appendix C.

6.3.2 Examples

Example 6.3. (torsion point with large prime order)
The rational point with the largest prime order that we found is of order 37 on the Jacobian J of the curve C defined by

$$y^2 = -4x^7 + 12x^6 - 4x^5 - 8x^4 + 4x^2 + 4x + 1.$$

The point of order 37 represented by

$$(0, 1) - P_\infty$$

generates $J(\mathbb{Q})_{\text{tors}}$. Using the same check as in Example 6.2, J turns out to be absolutely irreducible.

Example 6.4. (torsion point with large order)
The rational point with the largest order that we found is of order 60 on the Jacobian J of the curve C defined by

$$y^2 = x^8 - 4x^7 + 8x^6 - 12x^5 + 18x^4 - 12x^3 + 8x^2 - 4x + 1.$$

On K, we find the points R_1, R_2, R_3 that have generators of $J(\mathbb{Q})_{\text{tors}}$ in the pre-image under κ:

$$\begin{aligned} R_1 &= (0:0:0:0:1:0:0:2) \\ R_2 &= (1:0:-4:2:18:-4:0:20) \\ R_3 &= (1:4:4:-2:-10:4:4:20). \end{aligned}$$

It is easily checked that a point Q_1 in $\kappa^{-1}(R_1)$ has order 4 in $J(\mathbb{Q})$. Similarly, $Q_2 \in \kappa^{-1}(R_2)$ has order 3 in $J(\mathbb{Q})$ and $Q_3 \in \kappa^{-1}(R_3)$ has order 5 in $J(\mathbb{Q})$. Therefore, $Q = Q_1 + Q_2 + Q_3$ is a point of order 60 in $J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/60\mathbb{Z}$. Since $f_8 = 1$ is a square in $\mathbb{Q}$, arithmetic on the Jacobian is implemented.

Using (5.20), we see that Q_1 is of degree 2. Hence, it is represented by the unique divisor D_Q. From the coordinates of R_1, we conclude that D_Q has precisely one affine point $P_1 := (x_1, y_1)$ in its support. Using (5.20), $x_1 = -\xi_6 = 0$. In the notation of (5.20), $\xi_8 = 2y_1 w = 2$, hence $\kappa^{-1}(R_1) = \{[(0:1:1) + (1:1:0) - D_\infty], [(0:-1:1) + (1:-1:0) - D_\infty]\}$. We pick

$$Q_1 = [(0:1:1) + (1:1:0) - D_\infty] \in J(\mathbb{Q}).$$

The pre-image of R_2 and R_3 are computed using the implementation of [55, §4] in `G3Hyp.m`. We find a point Q_2 such that $\kappa(Q_2) = R_2$ in the class

$$Q_2 = [(0:1:1) + (i:2:0) + (-i:2:0) + (1:1:0) - 2D_\infty] \in J(\mathbb{Q})$$

where $i^2 = 1$. We see that D_Q is invariant under the non-trivial isomorphism in $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$, hence $Q_2 \in J(\mathbb{Q})$.

Similarly, a point of order 5 in $\kappa^{-1}(R_3)$ is represented by

$$Q_3 = [2 \cdot (0:-1:1) + 2 \cdot (1:1:0) - 2D_\infty]. \in J(\mathbb{Q})$$

Now, we can compute $Q = Q_1 + Q_2 + Q_3$ using MAGMA, we employ Cantor's Algorithm to find a point Q of order 60, represented by the divisor

$$Q = [(1:-2:1) + (1:-1:0) - D_\infty] \in J(\mathbb{Q}).$$

Example 6.5. (largest torsion subgroup) Let C be defined by

$$y^2 = x^8 - 4x^7 + 2x^6 + 8x^5 - 13x^4 + 8x^3 + 2x^2 - 4x + 1.$$

Similarly as before, using the coordinates on K, we find two points of order 3,

$$\begin{aligned} Q_1 &= [2 \cdot (0:-1:1) + 2 \cdot (1:1:0) - 2D_\infty] \\ Q_2 &= [2 \cdot (0:-1:1) + 2 \cdot (1:-1:0) - 2D_\infty]. \end{aligned}$$

The two-torsion points are found using Section 5.6. We find the factorization

$$f(x) = (x^2 - 3x + 1)(x^2 - x - 1)(x^2 - x + 1)(x^2 + x - 1) := g_1 g_2 g_3 g_4$$

and pick the three first factors to create the points with Mumford representation $Q_3 := \langle g_1, 0\rangle, Q_4 := \langle g_2, 0\rangle$ and $Q_5 := \langle g_3, 0\rangle$, and $Q_3 + Q_4 + Q_5 = \langle g_4, 0\rangle$. Then, the generators of $J(\mathbb{Q})_{\text{tors}}$ can be picked as $Q_1 + Q_3$, $Q_2 + Q_4$ and Q_5. Hence,

$$J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

7 Summary and outlook

7.1 Summary

In this thesis, we explicitly generalized the lifting algorithm that is proposed in [52] to general hyperelliptic curves, explained how the lifting procedure can be generalized, and gave a detailed proof of correctness of the algorithm. We explained how the generalization of this lifting procedure makes the algorithm more efficient, and how one can apply the generalization to compute the rational torsion subgroup of many Jacobians if biquadratic forms that allow us to apply the sum-and-difference-laws are not computed.

For genus 3, we completed the explicit description of the map $\kappa\colon J \to K$ for any point in $J(k)$. Furthermore, for the case $k = \mathbb{Q}$, we created a method to check whether $R \in K(k)$ has a pre-image $\kappa^{-1}(R)$ that consists of rational points in $J(k)$. For the case where C has no rational points, a method to compute $J(\mathbb{Q})_{\text{tors}}$ with the use of transformations on reduced Jacobians is given. Together with theory in [55], an implementation of the algorithm for genus 2 hyperelliptic curves in MAGMA and base code for genus 3 hyperelliptic curves [51], we used the new explicit theory to implement a general method that computes the rational torsion structure of the Jacobian of any hyperelliptic curve of genus 3. In practice, this method is made more efficient as a result of the generalization of the lifting procedure.

We used this implementation to compute the rational torsion structure of Jacobians of hyperelliptic curves of genus 3 of low discriminant from a database of 67879 curves that is planned to be put into the LMFDB. Since the algorithm does not require an implementation of arithmetic on J, some of these curves have Jacobians J where no implementation on $J(\mathbb{Q})$ is known, but we can still compute $J(\mathbb{Q})_{\text{tors}}$.

In the database for the LMFDB, we already found an absolutely irreducible Jacobian with a rational torsion point of order 37, and two Jacobians with torsion order 60 (that may be reducible). Furthermore, we found absolutely irreducible Jacobians of hyperelliptic curves of genus 3 with rational torsion points of the following orders: $11, 12, 13, 14, 16, 17, 18, 19, 20, 21, 24, 46$; such Jacobians seem to be unknown in the literature.

7.2 Outlook

Computing $J(\mathbb{Q})_{\text{tors}}$ for Jacobians of genus 3 hyperelliptic curves and describing and proving a method that generalizes to genus g hyperelliptic curves makes it easier to search for rational torsion structures on any Jacobian of any hyperelliptic curve. The possible rational torsion structures of elliptic curves are completely determined by Mazur [33]. For higher-dimensional abelian varieties for fixed dimension over $\mathbb{Q}$, the uniform boundedness conjecture predicts that there is a finite list of possible torsion stuctures. This conjecture is unproven to date, even for dimension 2 [48]. Several authors have constructed certain curves in order to find rational torsion points of large prime order [29], [43]. By simply computing the torsion structure of large sets of Jacobians, one can gain more insight on how frequently certain torsion structures appear. Furthermore, instead of finding a torsion point of large order by design, one can now always compute the complete rational torsion structure for these Jacobians.

The generalization of the lifting procedure allows us to describe a method that only uses multiplication-by-2 on the Kummer variety, and for many curves we can completely avoid the use of sum-and-difference-laws. Ludwig Fürst has already computed the doubling formulae for hyperelliptic curves of genus 4. Since a divisor representation of $J(\mathbb{Q})$ of hyperelliptic curves of genus 4 is less problematic [57, Remark 2.5], one can apply Cantor's Algorithm to do arithmetic on $J(\mathbb{Q})$. Hence, our generalization of the lifting procedure implies a method for finding $J(\mathbb{Q})_{\text{tors}}$ of genus 4 hyperelliptic curves that requires doubling on K, but does not need the full sum-and-difference-laws.

For genus 3, as mentioned in Section 5.2, no unique divisor representation is known for points on $J(\mathbb{Q})$ if no rational point in $C(\mathbb{Q})$ is known. If a unique representation for points on $J(\mathbb{Q})$ can be found such that arithmetic on $J(\mathbb{Q})$ can be implemented, for example by considering a number field k such that $C(k) \neq \emptyset$, then one can implement arithmetic on $J(k)$, and one can do explicit computations on $J(\mathbb{Q})$ for all Jacobians

corresponding to hyperelliptic curves of genus 3. Note that considering a curve C the quadratic number field $k := \mathbb{Q}(\alpha)$ where $\alpha^2 = f_8$ always yields two k-rational points at infinity.

Another potential generalization of this algorithm is to consider number fields k and try to find $J(k)_{\text{tors}}$. For this, one would need to use generalized theory on reduction and Hensel lifting on nonarchimedean $\mathfrak{p}$-adic fields for a prime ideal $\mathfrak{p}$ of K, see, e.g., [35, Chapter 7]. Note that if $\mathfrak{p}$ splits in k, then we can still work over $\mathbb{Q}_p$. Then, one needs to apply generalized theory on LLL-reduction (e.g. [18]) for $\mathcal{O}_k$-modules, where $\mathcal{O}_k$ is the order of k, and find a criterion that terminates Algorithm 4.2. The required explicit theory of K does not depend on k, a way to compute the torsion height bound β is already given for number fields for genus 2, 3 in [52] and [55] respectively.

One application of a generalized algorithm on number fields is to consider geometrically hyperelliptic curves over $\mathbb{Q}$ without a rational point. Let C be a geometrically hyperelliptic curve defined over $\mathbb{Q}$. This means that C is a double cover of a conic over $\mathbb{Q}$. Hence, the geometrically hyperelliptic curve is a generalization of the hyperelliptic curve, which is a double cover of $\mathbb{P}^1$. Using [24, Section 2], we can find a quadratic number field k and a hyperelliptic curve C' defined over k such that C and C' are isomorphic over k. Then, we can compute $J'(k)_{\text{tors}} \cong J(k)_{\text{tors}}$ where $J := \text{Jac}(C)$, $J' := \text{Jac}(C')$. We find $J(\mathbb{Q})_{\text{tors}}$ by finding all points on $J(k)_{\text{tors}}$ that are in $J(\mathbb{Q})$. For this approach, we only need the algorithm to work over quadratic number fields.

A further generalization is to consider general curves C of genus 3 defined over $\mathbb{Q}$. Nonsingular curves of genus 3 that are not (geometrically) hyperelliptic curves can be described as *smooth plane quartics*. For instance, one could first consider Picard curves. If k is a field of characteristic $\neq 2, 3$, then *Picard curves* defined over k have a model

$$y^3 z = F(x, z)$$

in $\mathbb{P}^3$ such that $F \in k[x, z]$ is homogeneous of degree 4. An embedding into $\mathbb{P}^7$ of the Kummer variety of the Jacobian of C is computed in [43, §4.4]. One would still need a way to compute a torsion height bound β and explicit arithmetic on the Kummer variety for this embedding. Since $P_\infty := (0 : 1 : 0)$ is always a rational point, we can fix P_∞ as a base point and find a unique divisor representation. Then, arithmetic on $J(k)$ is implemented using an isomorphism between the class group of the integral closure of the ring $k[x]$ in $k(C)$ and Pic^0_C [22, Proposition 3]. Hence, we do not need the full sum-and-difference-laws on K; doubling formulae δ that double a point on the Kummer variety suffices.

References

[1] Arithmetic aspects of explicit moduli problems. See `https://www.birs.ca/events/2017/5-day-workshops/17w5065`.

[2] The Birch and Swinnerton-Dyer Conjecture. See `http://www.claymath.org/millennium-problems/birch-and-swinnerton-dyer-conjecture`.

[3] L-functions and Modular Forms Database. See `https://www.lmfdb.org/`.

[4] MAGMA computational algebra system. See `http://magma.maths.usyd.edu.au/magma/`.

[5] R. M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography*, volume 34 of *Discrete Mathematics and its Applications*. Chapman & Hall/CRC (Taylor & Francis Group), 2005.

[6] M. Bhargava. Most hyperelliptic curves over Q have no rational points. Pre-print available at arXiv:1308.0395; v1: 2 Aug 2013.

[7] B. Birch and H. Swinnerton-Dyer. Notes on elliptic curves. II. *Journal für die reine und angewandte Mathematik*, 218:79–108, 1965.

[8] C. Birkenhake and H. Lange. *Complex Abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften*. Springer, second edition, 2004.

[9] J. W. Bos, C. Costello, H. Hisil, and K. Lauter. Fast cryptography in genus 2. *Journal of Cryptology*, 29:28–60, 2016.

[10] N. Bourbaki. *Elements of Mathematics: Lie Groups and Lie Algebras, Part I, Chapters 1-3*. Hermann, Publishers in Arts and Science, 1971.

[11] N. Bruin and M. Stoll. Deciding existence of rational points on curves: an experiment. *Experimental Mathematics*, 17:181–189, 2008.

[12] J. Cassels. Mordell's finite basis theorem revisited. *Mathematical Proceedings of the Cambridge Philosophical Society*, 100:31–41, 1986.

[13] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a Middlebrow arithmetic of curves of genus 2*. Cambridge University Press, 1996.

[14] K. Conrad. A multivariable Hensel's lemma. see `https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf`.

[15] D. Coray and C. Manoil. On large Picard groups and the Hasse principle for curves and K3 surfaces. *Acta Arithmetica*, 76:165–189, 1996.

[16] D. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, 2005.

[17] G. Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpern. (German). *Inventiones Mathematicae*, 73:349–366, 1984.

[18] C. Fieker and D. Stehlé. Short bases of lattices over number fields. In *Algorithmic number theory*, pages 157–173. Springer, 2010.

[19] E. Flynn. The group law on the Jacobian of a curve of genus 2. *Journal für die Reine und Angewandte Mathematik.*, 439:45–69, 1993.

[20] E. Flynn and C. Grattoni. Descent via isogeny on elliptic curves with large rational torsion subgroups. *Journal of Symbolic Computation*, 43:293–303, 2008.

[21] E. Flynn and N. Smart. Canonical heights on the Jacobians of curves of genus 2 and infinite descent. *Acta Arithmetica*, 79:333–352, 1997.

[22] S. Galbraith, S. Paulus, and N. Smart. Arithmetic on superelliptic curves. *Mathematics of Computation*, 71(237):393–405, 2002.

[23] S. D. Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, 2012. Version 2 (2018) is used: see `https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf`.

[24] D. Harvey, M. Massierer, and A. V. Sutherland. Computing L-series of geometrically hyperelliptic curves of genus three. *LMS Journal of Computation and Mathematics*, 19:220–234, 2016.

[25] M. Hindry and J. H. Silverman. *Diophantine geometry: An introduction*. Springer, 2000.

[26] E. W. Howe, F. Leprévost, and B. Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Mathematicum*, 12:315–364, 2000.

[27] E. W. Howe and H. J. Zhu. On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. *Journal of Number Theory*, 92:139–163, 2002.

[28] N. Koblitz. *p-adic numbers, p-adic analysis and Zeta-functions.*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, 1984.

[29] M. Kronberg. *Explicit construction of rational torsion divisors on Jacobians of curves*. PhD thesis, Carl von Ossietzky Universität Oldenburg, 2015.

[30] S. Lang. *Introduction to algebraic and abelian functions*. Springer Verlag, New York-Berlin, second edition edition, 1982.

[31] A. Lenstra, H. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[32] A. Mattuck. Abelian varieties over p-adic ground fields. *Annuals of Mathematics (2)*, 62:92–119, 1955.

[33] B. Mazur. Rational isogenies of prime degree. *Inventiones Mathematicae*, 44:129–162, 1978.

[34] W. McCallum and B. Poonen. *The method of Chabauty and Coleman*, pages 91–117. 2012.

[35] J. S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.

[36] P. L. Montgomery. Speeding the Pollard and elliptic curve methods for factorization. *Math. Comp*, 48:243–264, 1987.

[37] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proceedings of the Cambridge Philosophical Society*, XXI:179–192, 1922.

[38] D. Mumford. On the equations defining abelian varieties. I. *Inventiones Mathematicae*, 1:287–354, 1966.

[39] D. Mumford. *Tata Lectures on Theta II: Jacobian theta functions and differential equations*. Birkhäuser Boston, 1984.

[40] J. S. Müller. Explicit Kummer varieties of hyperelliptic Jacobian threefolds. *LMS Journal of Computation and Mathematics*, 17:496–508, 2014.

[41] J. S. Müller and M. Stoll. Canonical heights of genus-2 Jacobians. *Algebra Number Theory*, 10:2153–2234 (issue 10), 2016.

[42] J. S. Müller and C. Stumpe. Archimedean local height differences on elliptic curves. *Acta Arithmetica*, 190(3):293–303, 2019.

[43] C. Nicholls. *Descent methods and torsion on Jacobians of higher genus curves.* PhD thesis, University of Oxford, 2018.

[44] B. Poonen and E. F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *Journal für die reine und angewandte Mathematik*, 488:141–188, 1997.

[45] B. Riemann. Theorie der Abel'schen functionen. *Journal für die reine und angewandte Mathematik.*, 54:115–155, 1857.

[46] G. Roch. Ueber die anzahl der willkürlichen constanten in algebraischen functionen. *Journal für die reine und angewandte Mathematik.*, 64:372–376, 1865.

[47] J.-P. Serre. *Local fields.*, volume 67 of *Graduate texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[48] A. Silverberg. *Open questions in arithmetic algebraic geometry.*, volume 9 of *IAS/Park City Math. Ser.* 2001.

[49] J. H. Silverman. *The arithmetic of elliptic curves.*, volume 106 of *Graduate texts in Mathematics*. Springer, 2nd edition edition, 2009.

[50] W. Stein and C. Wuthrich. Algorithms for the arithmetic of elliptic curves using Iwasawa theory. *Mathematics of Computation*, 283:1757–1792, 2013.

[51] M. Stoll. MAGMA-related directory. See `http://www.mathe2.uni-bayreuth.de/stoll/magma/index.html`.

[52] M. Stoll. On the height constant for curves of genus two. *Acta Arithmetica*, 90:183–201, 1999.

[53] M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arithmetica*, 98:245–277, 2001.

[54] M. Stoll. Arithmetic of hyperelliptic curves, 2014. `http://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2014/Skript-ArithHypCurves-pub-screen.pdf`, Course Notes for Summer Semester 2014.

[55] M. Stoll. An explicit theory of heights for hyperelliptic Jacobians of genus three. *Algorithmic and experimental methods in algebra, geometry, and number theory*, pages 665–715, 2017.

[56] A. V. Sutherland. Genus 3 hyperelliptic curves of small discriminant over Q. see `https://math.mit.edu/~drew/gce_genus3_hyperelliptic.txt`.

[57] A. V. Sutherland. Fast Jacobian arithmetic for hyperelliptic curves of genus 3. *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, pages 425–442, 2018.

[58] J. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki*, volume 9, pages 415–440. Société Mathématique de France, 1995. originally published in 1968.

[59] A. Weil. L'arithmétique sur les courbes algébriques. *Acta Mathematica*, 52:218–315, 1929.

A Formulas

This is the expansion of Equation (5.18) divided by $\sigma_1^2 - 4\sigma_0\sigma_2$. This expansion can also be found on [55, §2].

$$
\begin{aligned}
&(\sigma_1^2 - 4\sigma_0\sigma_2)\xi_8^2 \\
&(4f_0\sigma_0^4 - 2f_1\sigma_0^3\sigma_1 + 4f_2\sigma_0^3\sigma_2 - 2f_3\sigma_0^2\sigma_1\sigma_2 + 4f_4\sigma_0^2\sigma_2^2 \\
&- 2f_5\sigma_0\sigma_1\sigma_2^2 + 4f_6\sigma_0\sigma_2^3 - 2f_7\sigma_1\sigma_2^3 + 4f_8\sigma_2^4)\xi_8 \\
&+ (-4f_0f_2 + f_1^2)\sigma_0^6 + 4f_0f_3\sigma_0^5\sigma_1 - 2f_1f_3\sigma_0^5\sigma_2 - 4f_0f_4\sigma_0^4\sigma_1^2 \\
&+ (-4f_0f_5 + 4f_1f_4)\sigma_0^4\sigma_1\sigma_2 + (-4f_0f_6 + 2f_1f_5 - 4f_2f_4 + f_3^2)\sigma_0^4\sigma_2^2 \\
&+ 4f_0f_5\sigma_0^3\sigma_1^3 + (8f_0f_6 - 4f_1f_5)\sigma_0^3\sigma_1^2\sigma_2 + (8f_0f_7 - 4f_1f_6 + 4f_2f_5)\sigma_0^3\sigma_1\sigma_2^2 \\
&+ (-2f_1f_7 - 2f_3f_5)\sigma_0^3\sigma_2^3 - 4f_0f_6\sigma_0^2\sigma_1^4 + (-12f_0f_7 + 4f_1f_6)\sigma_0^2\sigma_1^3\sigma_2 \\
&+ (-16f_0f_8 + 8f_1f_7 - 4f_2f_6)\sigma_0^2\sigma_1^2\sigma_2^2 + (8f_1f_8 - 4f_2f_7 + 4f_3f_6)\sigma_0^2\sigma_1\sigma_2^3 \\
&+ (-4f_2f_8 + 2f_3f_7 - 4f_4f_6 + f_5^2)\sigma_0^2\sigma_2^4 + 4f_0f_7\sigma_0\sigma_1^5 \\
&+ (16f_0f_8 - 4f_1f_7)\sigma_0\sigma_1^4\sigma_2 + (-12f_1f_8 + 4f_2f_7)\sigma_0\sigma_1^3\sigma_2^2 \\
&+ (8f_2f_8 - 4f_3f_7)\sigma_0\sigma_1^2\sigma_2^3 + (-4f_3f_8 + 4f_4f_7)\sigma_0\sigma_1\sigma_2^4 - 2f_5f_7\sigma_0\sigma_2^5 \\
&- 4f_0f_8\sigma_1^6 + 4f_1f_8\sigma_1^5\sigma_2 - 4f_2f_8\sigma_1^4\sigma_2^2 + 4f_3f_8\sigma_1^3\sigma_2^3 - 4f_4f_8\sigma_1^2\sigma_2^4 \\
&+ 4f_5f_8\sigma_1\sigma_2^5 + (-4f_6f_8 + f_7^2)\sigma_2^6 \\
&= 0.
\end{aligned}
\tag{A.1}
$$

B Explicit change of coordinates on the Kummer variety of Jacobians of genus 3 hyperelliptic curves

In Section 2.6, we introduced a change of coordinates on C. Such a change of coordinates gives an induced map on the Jacobian. Now that we have described κ completely, we can also give an explicit induced change of coordinates on the Kummer variety. This is not necessary for the algorithm, but nevertheless very convenient in practice.

Let $\phi\colon C \to C'$ be a change of coordinates represented by

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and $e = 1$ in the notation of Theorem 2.40. Let $\phi_*\colon J \to J'$ be the induced map on the Jacobian, denoting J and J' to be the Jacobians of C and C' respectively. Also, let C be defined by

$$C\colon y^2 = f(x) := f_8x^8 + \cdots + f_0,$$

and let C' be defined by

$$C'\colon y^2 = g(x) := g_8x^8 + \cdots + g_0.$$

Consider ϕ_K to be the map that makes the following diagram commute.

$$\begin{array}{ccc} J & \xrightarrow{\phi} & J' \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa'} \\ K & \xrightarrow{\phi_K} & K' \end{array} \tag{B.1}$$

Here, K and K' are the Kummer varieties corresponding to J and J' respectively, and $\kappa\colon J \to K$, $\kappa'\colon J' \to K'$ are the explicit quotient maps as described above.

This section describes how ϕ_K maps a point $\kappa(Q) := (\xi_1 : \ldots : \xi_8)$ to $\kappa'(Q') := (\xi'_1 : \ldots : \xi'_8)$. The main step in this induced change of coordinates is done by using the coordinate transformation on the matrix M given in 5.13 representing the η_{ij}-coordinates, this is described in [55, §3]. This method computes $\xi'_1, \ldots, \xi'_7$. Since ξ'_8 is not involved in M, we need to find ξ'_8 separately. We do this explicitly using the information on κ we have obtained.

Case 0: $\xi'_1 = \cdots = \xi'_7 = 0$.

Obviously, we can choose $\xi'_8 = 1$, and we conclude that we map to the origin of K'.

Case 1: $\xi'_1 \neq 0$.

We use the quadratic equation (5.9) and solve for ξ'_8.

Case 2 $\xi'_1 = 0$, $\xi'_5 = 3\xi'_4$.

Now, Q' has the form $Q' = [2P - D_\infty]$ because $\xi'_5 - 3\xi'^2_4 = (x_1 - x_2)^2 = 0$ in the notation of Equation (5.14). We consider two cases:

Case 2.1: $\xi'_5 = \xi'_4 = 0$ implies $\kappa'(Q')$ has the form of Equation (5.21), hence $\xi'_8 = \frac{4g_6g_8 - g_7^2}{4g_8}$, scaling such that $\xi_7 = 1$.

Case 2.2: $\xi'_5, \xi'_4 \neq 0$ gives us the explicit case of Equation (5.19), so the affine support of the divisor representation is of degree 2. We scale $\sigma_2 = 1$, and use the form (5.16) to set $\sigma_1 = \xi'_3$ and $\sigma_0 = \xi'_4$, and compute $\xi_8 = -s_0/s_1$ in the notation of (5.18), using (A.1).

Case 3: $\xi'_1 = 0$, $\xi'_5 \neq 3\xi'_4$.

Now, we have $Q' = [P'_1 + P'_2 - D_\infty]$, such that $P'_1 := (x'_1 : y'_1 : z'_1)$ and $P'_2 := (x'_2 : y'_2 : z'_2)$ are distinct. We first determine $2y'_1y'_2$. This seems to be obviously equal to $2y_1y_2$ since $e = 1$. However, the issue is that

the map as described in Section 5.4 assumes points on C to have their coordinates scaled in a certain way: for points $P := (\rho : \eta : \zeta)$, we have that if $\zeta \neq 0$, then we scale such that $\zeta = 1$. If $\zeta = 0$, then we scale such that $\rho = 1$. This means that we have to take several case distinctions in order to find $2y_1'y_2'$ in the way that P_1' and P_2' has coordinates as assumed by describing κ in Section 5.4.

If $\xi_2 = \xi_3 = \xi_4 = 0$, then $\kappa(Q)$ is of the form (5.20). The map is based on the coordinates $Q = [(x_1 : y_1 : 1) + (1 : y_2 : 0) - D_\infty]$, Note that $\phi_*(Q) = [(ax_1 + b : y_1 : cx_1 + d) + (a : y_2 : c) - D_\infty]$. Since $\xi_5' \neq 3\xi_4'$, not both $z_1' = cx_1 + d = 0$ and $z_2' = c = 0$. Hence, after normalizing,

$$\begin{aligned} 2y_1'y_2' &= \frac{\xi_8 + 2f_8x_1^4 + f_7x_1^3}{\nu_1^4} \\ &= \frac{\xi_8 + 2f_8\xi_6^4 - f_7\xi_6^3}{\nu_1^4} \end{aligned}$$

where

$$\nu_1 = \begin{cases} c(-c\xi_6 + d) & \text{if } c(-c\xi_6 + d) \neq 0 \\ c(-a\xi_6 + d) & \text{if } -c\xi_6 + d = 0 \\ a(-c\xi_6 + d) & \text{if } c = 0. \end{cases} \tag{B.2}$$

If at least one of ξ_2, ξ_3, ξ_4 is nonzero, then $\kappa(Q)$ is of the form (5.14). We assumed $\xi_5' \neq 3\xi_4'$, hence $\xi_5 \neq 3\xi_4$, otherwise two distinct points are mapped to the same point under an isomorphism. Here, Q is of the form $Q = [(x_1 : y_1 : 1) + (x_2 : y_2 : 1) - D_\infty]$, so $Q' = [(ax_1 + b : y_1 : cx_1 + d) + (ax_2 + b : y_2 : cx_2 + d) - D_\infty]$. Denote $G_C(x_1, x_2)$ as in (5.15) corresponding to C, then $G_C(x_1, x_2)$ can be rewritten to the form

$$\begin{aligned} G_C(x_1, x_2) &= 2\sum_{j=0}^{4}(x_1x_2)^j + (x_1 + x_2)\sum_{j=0}^{3}(x_1x_2)^j \\ &= 2\sum_{j=0}^{4}\xi_4^j - \xi_3\sum_{j=0}^{3}\xi_4^j. \end{aligned} \tag{B.3}$$

Now, we can write, using (5.14),

$$\begin{aligned} 2y_1'y_2' &= \frac{(\xi_8 + G_C(x_1, x_2))(x_1 - x_2)^2}{\nu_2^4} \\ &= \frac{(\xi_8 + G_C(x_1, x_2))(\xi_5 - 3\xi_4)}{\nu_2^4} \end{aligned}$$

where ν_2 is again our scaling factor such that $2y_1'y_2$ respects the scaling of points assumed in Section 5.4.

Computing ν_2 depends on whether P_1 or P_2 map to infinity or not. We first note that not both P_1 and P_2 map to infinity: if that were the case, either $Q' = \kappa(0)$ or $P_1' = P_2'$: both contradict $\xi_5' \neq 3\xi_4'$.

Note that the image of z_1z_2 under ϕ is

$$z_1'z_2' = (cx_1 + d)(cx_2 + d) = c^2\xi_4 - cd\xi_3 + d^2$$

hence if $c^2\xi_4 - cd\xi_3 + d^2 \neq 0$, then P_1', P_2' are affine and we set $D_2 = c^2\xi_4 - cd\xi_3 + d^2 \neq 0$.

We are left with the case that precisely one of P_1', P_2' is affine. We fix P_1' to be affine without loss of generality, so $-\xi_6' = x_1'$ in Equation (5.20). Denote

$$A^{-1} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

and we fix P_1 to be the pre-image of P_1' under ϕ. Then,

$$x_1 = \frac{a'x_1' + b'}{c'x_1' + d'}$$

and $z_1' = cx_1 + d$, hence we scale the affine point by $z_1' = cx_1 + d$. Now, we also scale y_2' by considering $P_2' \in C^{\inf}$. We have that $(x_2 : y_2 : 1)$ maps to a point at infinity, hence we need to scale by $x_2' = ax_2 + b$ where

$$-(x_1 - (x_1 + x_2)) = -(x_1 - \xi_3).$$

In summary,

$$\nu_2 = \begin{cases} c^2\xi_4 - cd\xi_3 + d^2 & \text{if } c^2\xi_4 - cd\xi_3 + d^2 \neq 0 \\ \left(c\frac{-a'\xi_6' + b'}{-c'\xi_6' + d'} + d\right)\left(a\left(\frac{-a'\xi_6' + b'}{-c'\xi_6' + d'} - \xi_3\right) + b\right) & \text{otherwise.} \end{cases} \tag{B.4}$$

From all of the above in case 3, we conclude that

$$2y_1'y_2' = \begin{cases} \frac{\xi_8 + 2f_8\xi_6^4 - f_7\xi_6^3}{\nu_1^4} & \text{if } \xi_2 = \xi_3 = \xi_4 = 0 \\ \frac{(\xi_8 + G_C(x_1, x_2))(\xi_5 - 3\xi_4)}{\nu_2^4} & \text{otherwise} \end{cases} \tag{B.5}$$

where ν_1 is as described in (B.2) and ν_2 is as described in (B.4).

Knowing $2y_1'y_2'$, we are ready to compute ξ_8' for the following cases.

Case 3.1: In addition to the assumptions of case 3, $\xi_2' = \xi_3' = \xi_4' = 0$ implies that precisely one of P_1', P_2' is affine, hence $\kappa'(Q')$ has the form (5.20). Here,

$$\xi_8' = 2y_1'y_2' - 2\xi_6'^4 g_8 + \xi_6'^3 g_7.$$

Case 3.2: In addition to the assumptions of case 3, one of ξ_2', ξ_3', ξ_4' is nonzero. This implies that both P_1', P_2' are affine, hence $\kappa'(Q')$ has the form (5.14). Here,

$$\xi_8' = \frac{2y_1'y_2' - G_{C'}}{\xi_5' - 3\xi_4'}$$

where $G_{C'}$ is the G-function as described in (5.15) corresponding to the curve C', which can be computed in terms of ξ_3' and ξ_4', analogously to $B.3$.

We now have a complete, explicit description of $\phi_K \colon K \to K'$ that is induced from a change of coordinates $(x : y : z) \mapsto (ax + bz : y : cx + dz)$ from C to C'.

C Torsion structures found

These are all torsion structures found in the database [56].

Elementary divisors	Frequency
0	39707
2	15956
2, 2	2399
2, 2, 2	163
2, 2, 2, 2	3
3	1044
3, 3	1
4	2697
4, 2	471
4, 2, 2	43
4, 2, 2, 2	1
4, 4	3
4, 6	2
5	600
6	1259
6, 2	155
6, 2, 2	18
6, 3	1
6, 6	2
6, 6, 2	1
7	701
8	601
8, 2	146
8, 2, 2	21
8, 2, 2, 2	1
9	175
10	453
10, 2	87
10, 2, 2	16
10, 5	1
11	31
12	410
12, 2	84
12, 2, 2	2
12, 4	2
13	24
14	303

Elementary divisors	Frequency
14, 2	32
14, 2, 2	1
15	6
16	59
16, 2	7
17	5
18	29
18, 2	2
19	3
20	34
20, 2	6
21	2
22	14
22, 2	1
24	21
24, 2	5
25	4
26	7
27	3
28	16
28, 2	4
30	6
30, 2	1
32	3
33	1
34	1
36	3
37	1
38	2
40	1
42	6
44	1
46	1
49	2
52	2
60	2

order	$f(x)$
11	$-4x^8 - 4x^7 - 3x^6 + 6x^5 + 13x^4 + 14x^3 + 10x^2 + 4x + 1$
12	$4x^7 - 16x^6 + 4x^5 + 9x^4 + 16x^3 + 10x^2 + 4x + 1$
13	$x^8 - 2x^5 + 2x^4 + 4x^3 + 5x^2 + 2x + 1$ (Also: Example 6.1)
14	$12x^7 + 64x^6 + 120x^5 + 104x^4 + 36x^3 - 3x^2 - 4x$
16	$4x^7 + x^6 + 32x^5 + 80x^4 + 98x^3 + 52x^2 + 12x + 1$
17	$4x^7 + 16x^6 + 24x^5 + 28x^4 + 20x^3 + 12x^2 + 4x + 1$
18	$4x^7 + 8x^6 + 16x^5 + 17x^4 + 16x^3 + 10x^2 + 4x + 1$
19	$x^8 - 2x^6 - 2x^5 - x^4 + 2x^3 + 7x^2 + 2x - 7$
20	$x^8 - 12x^6 - 2x^5 + 52x^4 + 16x^3 - 95x^2 - 32x + 60$
21	$-4x^7 + x^6 - 4x^5 + 6x^4 - 2x^3 - 3x^2 + 2x + 1$
23	$4x^8 - 4x^6 - 3x^4 - 4x^3 + 2x^2 + 4x + 1$ (using the point of order 46 found below.)
24	$4x^7 - 8x^6 + 20x^5 - 7x^4 + 4x^3 + 18x^2 + 8x + 1$
46	$4x^8 - 4x^6 - 3x^4 - 4x^3 + 2x^2 + 4x + 1$

Figure 2: Examples of curves whose Jacobian is absolutely irreducible and contains a rational torsion point of given order.