SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Finding rational torsion points on hyperelliptic curves with an application to point counting on a moduli space

av

Daniel Lännström

2016 - No 3

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Finding rational torsion points on hyperelliptic curves with an application to point counting on a moduli space

Daniel Lännström

Självständigt arbete i matematik 30 högskolepoäng, avancerad nivå

Handledare: Jonas Bergström

2016

Abstract

For elliptic curves it is well-known that the zeroes of the division polynomials characterize the torsion points. Here we will instead consider hyperelliptic curves and present two algorithms for finding the rational torsion points. The first algorithm is a naive brute-force search. The second algorithm is based on the Cantor division polynomials – a generalization of the classical division polynomials to hyperelliptic curves. We focus mainly on hyperelliptic curves defined over finite fields of genus 2.

As an application we will compute the number of $\mathbb{F}_q$-rational points on the moduli space of hyperelliptic curves of genus 2 with marked Weierstrass point and level N structure.

Acknowledgments

I wish to thank my advisor Jonas Bergström.

Contents

1 Introduction

1.1 Background: Modular curves

The modular curves are curves that parametrize elliptic curves together with some additional data (see for example [9]). In other words, each point on the modular curve corresponds to an isomorphism class of elliptic curves, together with additional data. In general, spaces that classifies some objects are called **moduli spaces** ('moduli' is an old word for parameter). The interesting property of moduli spaces is that they have both a 'classifying structure' and a topological structure.

The 'additional data' we will consider here is an elliptic curve together with a point of order N.

Definition 1. Let k be a field and consider pairs (E, P) where E is an elliptic curve defined over k and $P \in E(k)$ with $\mathrm{ord}(P) = N$. We define an equivalence relation by $(E, P) \sim (E', P')$ iff there exists an isomorphism $\phi\colon E \to E'$ defined over $\bar{k}$ such that $\phi(P) = P'$. Let

$$S_1[N](k) = \{(E, P)\}/\sim .$$

We will write $[E, P]$ for the equivalence class of (E, P).

Remark. We stress that a priori, $S_1[N](k)$ is just a set of equivalence classes.

Modular curves as Riemann surfaces

Let $N > 0$ be an integer called the level and let

$$\Gamma_1(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{\mathrm{N}} \right\},$$

where $*$ denotes an arbitrary element in $\mathbb{Z}/N\mathbb{Z}$. Then $\Gamma_1(N)$ acts on the complex upper half plane $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\, z \geq 0\}$ as Möbius transformations, i.e.,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az + b}{cz + d}.$$

The orbit space $Y_1(N) = \Gamma_1 \backslash \mathbb{H}$ can be given structure as a non-compact Riemann surface. Compactifying this space by adding the so called cusps gives the modular curve $X_1(N)$. Remarkably, $Y_1(N)$ can be proven to be the moduli space of pairs (E, P) in Definition 1 with $k = \mathbb{C}$. A little more precisely, there is a natural bijection,

$$Y_1(N)(\mathbb{C}) \longleftrightarrow S_1[N](\mathbb{C}).$$

Algebraic modular curves

Modular curves can also be defined algebraically. Let $k = \mathbb{Q}$ or $k = \mathbb{F}_q$ with $q = p^r$ and $p \nmid N$. From this algebraic perspective, $X_1(N)$ is a complete algebraic curve (variety of dimension 1) defined over k. Let,

$$Y_1(N) = X_1(N) - \{\text{cusps}\}.$$

Then $Y_1(N)$ becomes an affine algebraic curve defined over k. Furthermore, there is similarly a natural bijection,

$$Y_1(N)(k) \longleftrightarrow S_1[N](k).$$

So it makes sense to talk about $Y_1(N)$ as a moduli space.

By an important theorem by Igusa [9, Theorem 8.6.1], for each prime $p \nmid N$, we have good reduction of $X_1(N)/\mathbb{Q}$ modulo p. Additionally, reducing modulo p is compatible with the moduli structure defined in Definition 1. This intuitively means, for $p \nmid N$,

$$X_1(N)/\mathbb{Q} \pmod{\text{p}} = X_1(N)/\mathbb{F}_{\mathbb{p}},$$

In other words, starting with $k = \mathbb{Q}$ and reducing modulo p gives the same modular curve as starting with $k = \mathbb{F}_p$.

Now, to the global object $X_1(N)$ defined over $\mathbb{Q}$ we associate a so called incomplete global zeta function $\zeta_{X_1(N),\mathbb{Q}}(s)$. Recall that this function is given in terms of the local zeta functions for the reductions of $X_1(N)$ modulo p (see for example [11]). For $p \nmid N$, let V_p denote the reduction of $X_1(N)$ modulo p and let $\zeta_{V_p,\mathbb{F}_p}$ denote the corresponding local zeta function. Then,

$$\zeta_{X_1(N),\mathbb{Q}}(s) = \prod_{p \nmid N} \zeta_{V_p,\mathbb{F}_p}(s). \tag{1.1}$$

But by the discussion above we have $V_p = X_1(N)/\mathbb{F}_p$. Furthermore recall that for $q = p^r$ the local $\zeta_{X_1(N),\mathbb{F}_q}(s)$ is obtained by a coordinate change from

$$Z_{X_1(N),\mathbb{F}_q}(u) = \exp\left(\sum_{m=1}^{\infty} N_m \frac{u^m}{m}\right), \tag{1.2}$$

where $K_m = \#X_1(N)(\mathbb{F}_{q^m})$, i.e. the number of $\mathbb{F}_{q^m}$-rational points on the curve $X_1(N)$ defined over $\mathbb{F}_q$.

Next, suppose we can find $\#S_1(N)(\mathbb{F}_{p^m})$ for all prime p and $m > 0$. Then adding the number of rational cusps will give us $K_m = \#X_1(N)(\mathbb{F}_{p^m})$. From this we determine (1.2) for each p and hence also the global zeta function (1.1). Intuitively, we study the global object $X_1(N)$ over $\mathbb{Q}$, corresponding to the global moduli problem, by solving the local moduli problems at p^n. This is one motivation for computing $\#S_1(N)(\mathbb{F}_q) = \#Y_1(N)(\mathbb{F}_q)$.

Number of $\mathbb{F}_q$-rational points on $Y_1(N)$

Applying the Lefschetz-Grothendieck trace formula to $X_1(N)$ yields,

$$|X_1(N)(\mathbb{F}_{q^n})| = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n, \tag{1.3}$$

where $\{\alpha_i\} \in \mathbb{C}$ are eigenvalues of the Frobenius map acting on the Euler characteristic in ℓ-adic étale cohomology. In particular, $\{\alpha_i\}$ are independent of n.

For modular curves there is a theory of so called Hecke operators (see for example [17]) that connects the eigenvalues $\{\alpha_i\}$ with certain modular forms (complex analytic functions on $\mathbb{H}$ that respects the group action of Γ_1). Let $S_2(\Gamma_1(N))$ denote the vector space of cusps forms of weight 2 and level N. As a special consequence of the general theory we have,

$$\dim S_2(\Gamma_1(N)) = 0 \implies \alpha_i = 0 \text{ for } 1 \leq i \leq 2g$$

The mathematical software package Sage [8] has functionality for computing the dimension of $S_2(\Gamma_1(N))$ for a given level N.

```
sage: [Gamma1(n).dimension_cusp_forms() for n in [1..18]]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 2, 1, 1, 2, 5, 2]
```

This computation shows, in particular, that $\dim S_2(\Gamma(N)) = 0$ for $1 \leq N \leq 10$, i.e. there are no non-trivial cusp forms of weight 2 for levels below 11.

Hence, for $1 \leq N \leq 10$, (1.3) becomes,

$$|X_1(N)(\mathbb{F}_{q^n})| = q^n + 1. \tag{1.4}$$

Let c_{N,q^n} denote the number of cusps in $X_1(N)(\mathbb{F}_{q^n})$. Then (1.4) implies, for $1 \leq N \leq 10$,

$$|Y_1(N)(\mathbb{F}_{q^n})| = q^n + 1 - c_{N,q^n}. \tag{1.5}$$

Proposition 1. Let N be a odd prime and let ζ_N be a primitive Nth root of unity.

(i) The are a total of $N-1$ cusps in $X_1(N)(\bar{\mathbb{F}}_q)$. Of these $(N-1)/2$ lie $\mathbb{F}_q$ and $(N-1)/2$ lie in $\mathbb{F}_q(\zeta_N + \zeta_N^{-1})$.

(ii) If $q \equiv \pm 1 \pmod{\text{N}}$ then $\zeta_N + \zeta_N^{-1}$ lies in $\mathbb{F}_q$. If $q \not\equiv \pm 1 \pmod{\text{N}}$ then $\zeta_N + \zeta_N^{-1}$ lies in $\mathbb{F}_{q^m}$ where m is the least integer such that $q^m \equiv \pm 1 \pmod{\text{N}}$.

Proof. For (a) see [18, Example 13.3].

To prove (b) it is enough to show $\zeta_N + \zeta_N^{-1}$ lies in $\mathbb{F}_{q^m}$ iff $q^m \equiv \pm 1 \pmod{\text{N}}$. Recall that the Frobenius map fixes exactly $\mathbb{F}_{q^m}$. This means, $\zeta_N + \zeta_N^{-1} \in \mathbb{F}_{q^m}$ iff $(\zeta_N + \zeta_N^{-1})^{q^m} = \zeta_N + \zeta_N^{-1}$. But since we are working in characteristic p, we have $(\zeta_N + \zeta_N^{-1})^{q^m} = \zeta_N^{q^m} + (\zeta_N^{-1})^{q^m}$. Hence the following equation is equivalent to $\zeta_N + \zeta_N^{-1} \in \mathbb{F}_{q^m}$.

$$\zeta_N^{q^m} + \zeta_N^{-q^m} = \zeta_N + \zeta_N^{-1} \tag{1.6}$$

If $q \equiv 1 \pmod{N}$ then by Fermat's little theorem, $\zeta_N^{q^m} = \zeta_N$ and $\zeta_N^{-q^m} = \zeta_N$. Similarly, if $q \equiv -1 \pmod{N}$ then $\zeta_N^{q^m} = \zeta_N^{-1}$ and $\zeta_N^{-q^n} = \zeta_N$. This proves one direction.

Conversely, assume that Equation (1.6) holds. Multiplying (1.6) with $\zeta_N^{q^m}$ yields,

$$\begin{aligned} \zeta_N^{q^m+1} + \zeta_N^{q^m-1} = \zeta_N^{2q^m} + 1 &\iff \zeta_N^{2q^m} - \zeta_N^{q^m+1} - \zeta_N^{q^m-1} + 1 = 0 \\ &\iff (\zeta_N^{q^m} - \zeta_N)(\zeta_N^{q^m} - \zeta_N^{-1}) = 0. \end{aligned} \tag{1.7}$$

Hence either $\zeta_N^{q^m} = \zeta_N$ or $\zeta_N^{q^m} = \zeta_N^{-1}$. This implies that $q^m \equiv 1 \pmod{N}$ or $q^m \equiv -1 \pmod{N}$. □

Assume that N is an odd prime. Then it follows that,

$$c_{N,q^n} = \begin{cases} N-1 & \text{if } q^n \equiv \pm 1 \pmod{N} \\ (N-1)/2 & \text{otherwise} \end{cases}. \tag{1.8}$$

Then for N an odd prime and $q^n \equiv \pm 1 \pmod{N}$,

$$|Y_1(N)(\mathbb{F}_{q^n})| = q^n + 1 - (N-1) = q^n - N + 2. \tag{1.9}$$

On the other hand, if $q^n \not\equiv \pm 1 \pmod{N}$, then

$$|Y_1(N)(\mathbb{F}_{q^n})| = q^n + 1 - (N-1)/2. \tag{1.10}$$

In more general terms, this means there are a pair of polynomials

$$\begin{aligned} f_1(x) =& x + 1 - (N-1) \\ f_2(x) =& x + 1 - (N-1)/2, \end{aligned}$$

such that,

$$|Y_1(N)(\mathbb{F}_{q^n})| = \begin{cases} f_1(q^n) & q^n \equiv \pm 1 \pmod{N} \\ f_2(q^n) & q^n \not\equiv \pm 1 \pmod{N} \end{cases}. \tag{1.11}$$

We say that the pair (f_1, f_2) are **point counting polynomials** for the moduli space $Y_1(N)$.

Let $\mathcal{M}(N)$ be any moduli space and assume there exist point counting polynomials f_1, f_2 for $\mathcal{M}(N)$. Then by calculating a number of data points $(q^n, \#\mathcal{M}(N)(\mathbb{F}_{q^n}))$ with $q^n \equiv \pm 1 \pmod{N}$ we can determine f_1 by polynomial interpolation. Similarly, by calculating a number of data points $(q^n, \#\mathcal{M}(N)(\mathbb{F}_{q^n}))$ with $q^n \not\equiv \pm 1 \pmod{N}$ we can determine f_2.

The number of data points needed will depend on the degree of the polynomials f_i. In the case of $Y_1(N)$ we know that f_i is a linear polynomial, so we only need 2 points to uniquely determine f_1, f_2.

1.2 Moduli space of hyperelliptic curves

Definition 2. Let k be a field and let C be a smooth, projective curve of genus $g \geq 1$ over k. If there exists a finite separable morphism $\phi\colon C \to \mathbb{P}^1_k$ such that $\deg \phi = 2$ we say that C is a **hyperelliptic curve**. As usual we let $C(k)$ denote the k-rational points.

Intuitively, the morphism ϕ give a $2:1$ cover of $\mathbb{P}^1$. The ramification points of this cover are called **Weierstrass points.** In general when $\operatorname{char} k \neq 2$, a hyperelliptic curve will admit a Weierstrass equation of the form $y^2 = f(x)$ where $\deg f = 2g+2$ and the zeroes of $f(x)$ are the Weierstrass points. However, in the special case when there exists a k-rational Weierstrass point $\omega \in C(k)$ it is possible to move ω to ∞ and hence get a Weierstrass equation of the form $y^2 = g(x)$ where $\deg g = 2g+1$.

The next natural question is: What is the generalization of modular curves for hyperelliptic curves? Or, in other words, how can we represent the moduli space of hyperelliptic curves with some additional level data? When $g = 2$ the moduli space is given as a 3-dimensional affine variety defined over $\mathbb{Z}[1/N]$.

We follow the same idea as for modular curves, i.e. determine the number of rational points on the moduli space locally at p^n.

However, recall that elliptic curve has a geometric group structure, which is implicit in Definition 1. To generalize this definition we need to associate a group structure with the the hyperelliptic curve C. The so called Jacobian $J(C)$ (defined later) is a group structure associated with the curve C.

Definition 3. Consider pairs (C, P) where C is a hyperelliptic curve of genus g defined over k and $P \in J(C)(k)$ such that $\operatorname{ord}(P) = N$. Let $(C, P) \sim (C', P')$ iff there exists a $\bar{k}$-isomorphism $\phi\colon C \to C'$ such that $\phi(P) = P'$. Then, define,

$$\mathcal{H}_g[N](k) = \{(C, P)\}/\sim . \tag{1.12}$$

Let $[C, P]$ denote the equivalence class of (C, P).

As mentioned above $\mathcal{H}_g[N]$ can be defined as an algebraic variety over $\mathbb{Z}[1/N]$.

Langlands program is a series of deep conjectures that relates algebraic number theory with representation theory. The modular forms are generalized to so called automorphic forms. The conjectures implies, in particular, a generalization of the Hecke theory.

This implies a similar result for $\mathcal{H}_2[N]$ as for the modular curve $Y_1(N)$. More precisely, let N be an odd prime. Then if the dimension of a certain vector space of automorphic forms of level N is zero, then the moduli space $\mathcal{H}_2[N]$ admits a pair of point counting polynomials f_1, f_2. Similarly, to the modular curve case we expect the first few spaces to have dimension 0.

Furthermore, in the modular curve case (dimension 1) the point counting polynomials f_i are linear. For $\mathcal{H}_2[N]$ (dimension 3) we instead expect $\deg f_i = 3$.

A slightly different moduli space

Unfortunately, the techniques presented later will not allow us to compute $\#\mathcal{H}_2[N](\mathbb{F}_{q^n})$ easily. The main machinery only works with hyperelliptic curves with a marked $\mathbb{F}_{q^n}$-rational Weierstrass point (equivalently has a Weierstrass equation of degree 5). So we will only be able to count pairs (H, P) where H is in this specific subclass of hyperelliptic curves. Because of this limitation, we will consider the moduli space $\mathcal{H}_2^{\omega}[N]$ (defined later) where every hyperelliptic curve comes with marked $\mathbb{F}_{q^n}$-rational Weierstrass point.

Note that $\mathcal{H}_2^\omega[N]$ is not a subset of $\mathcal{H}_2[N]$ since for $\mathcal{H}_2^\omega[N]$ we will define the equivalence relation on pairs (H, P) differently. However, there is a map

$$\begin{aligned} \phi\colon \mathcal{H}_2^\omega[N] &\to \mathcal{H}_2[N] \\ (H,P)/\sim_{\mathcal{H}_2^\omega[N]} &\mapsto (H,P)/\sim_{\mathcal{H}_2[N]} . \end{aligned} \tag{1.13}$$

For $g = 2$ the Weierstrass points of a hyperelliptic curve are the 6 ramification points. In other words, if the hyperelliptic curve is given by $y^2 = f(x)$ where $\deg f = 6$ then the Weierstrass points are the roots of $f(x)$. Similarly, if $y^2 = f(x)$ for $\deg f = 5$ then the Weierstrass points are the 5 roots and ∞. This implies that the map ϕ has degree 6.

However, heuristically, it seems likely there are point counting polynomials for $\mathcal{H}_2^\omega[N]$ iff there are point counting polynomials for $\mathcal{H}_2[N]$.

Experimental results

By explicit computer calculations we have determined $\#\mathcal{H}_2^\omega[N](\mathbb{F}_q)$ for $N = 3, 5, 7$ and some odd prime powers q (see Table 1.1). For $N = 3, 5$ these data points do lie on appropriate point counting polynomials (see Conjectures 1 and 2). However, for $N = 7$ we can't interpolate the data with appropriate polynomials. This suggests (assuming Langlands conjecture) that there exists a non-zero automorphic form for $N = 7$.

q	$q \pmod 3$	$\lvert\mathcal{H}_2^\omega[3](\mathbb{F}_q)\rvert$	$q \pmod 5$	$\lvert\mathcal{H}_2^\omega[5](\mathbb{F}_q)\rvert$	$q \pmod 7$	$\lvert\mathcal{H}_2^\omega[7](\mathbb{F}_q)\rvert$
3	0	-	3	24	3	18
5	2	82	0	-	5	108
7	1	256	2	340	0	-
9	0	-	4	746	2	708
11	2	1108	1	1356	4	1302
13	1	1882	3	2194	6	2142
17	2	4366	2	4910	3	4860
19	1	6172	4	6916	5	6810
23	2	11152	3	12164	2	12114
27	0	-	2	19680	6	9765
29	2	22762	4	24486	1	?
31	1	27928	1	29896	3	?

Table 1.1: Number of $\mathbb{F}_q$-rational points on $\mathcal{H}_2^\omega[N]$ for $N = 3, 5, 7$.

In the table, the '-' symbol means there is no good reduction since $p|N$. The '?' symbol denotes a value that is theoretically possible to compute with the techniques/implementation given later, but it has not been computed because of time constrains.

The conjectured point counting polynomials looks like this:

Conjecture 1. For $q = p^r$ where $p \neq 3$ we have

$$|\mathcal{H}_2^\omega[3](\mathbb{F}_q)| = q^3 - 2q^2 + 2q - 3. \tag{1.14}$$

Conjecture 2. For $q = p^r$ where $p \neq 5$ we have

$$|\mathcal{H}_2^{\omega}[5](\mathbb{F}_q)| = \begin{cases} q^3 + 4q - 19 & q \equiv 1, 4 \pmod 5 \\ q^3 - 3 & q \equiv 2, 3 \pmod 5 \end{cases} \tag{1.15}$$

1.3 Overview

Our main goal will be to find an algorithm to compute $|\mathcal{H}_2^{\omega}[N](\mathbb{F}_q)|$. We will not enumerate pairs $[H, P]$ directly. Instead our first logical step is the following formula (proved later in Chapter 4, Theorem 10),

$$|\mathcal{H}_2^{\omega}[N](\mathbb{F}_q)| = \sum_{[H]_k} \frac{\mathrm{c}(H)}{\mathrm{Aut}_k(H)}, \tag{1.16}$$

where $\mathrm{c}(H)$ denotes the number of points $P \in J(H)(\mathbb{F}_q)$ with $\mathrm{ord}(P) = N$.

To calculate the sum (1.16) we will find,

(i) an algorithm to compute $\mathrm{c}(H)$, and,

(ii) a way to rewrite the sum (1.16) into an expression not involving the automorphism groups.

To find an algorithm for computing $\mathrm{c}(H)$ we will consider N-division points in $J(H)(\mathbb{F}_q)$. These are points P such that $NP = 0$, or equivalently, $\mathrm{ord}(P)|N$. In Chapter 3, we will give two algorithms for finding the N-division points. First a naive algorithm, based on a brute-force approach and, secondly, a more sophisticated algorithm utilizing the Cantor division polynomials. In practice, the first algorithm ended up faster than the second.

In Chapter 4 we will rewrite (1.16) using the Orbit-Stabilizer theorem. From this we will finally obtain an algorithm (Algorithm 13) to compute $|\mathcal{H}_2^{\omega}[N](\mathbb{F}_q)|$.

2 Preliminaries

2.1 Division polynomials for elliptic curves

Later we will see a generalization of the classical division polynomials to hyperelliptic curves. Therefore, we begin by giving an overview of the classical division polynomials for elliptic curves. For details see [19].

Let k be a field with $\operatorname{char}(k) \neq 2, 3$. Then an elliptic curve over k is given by a **Weierstrass equation** of the form

$$y^2 = x^3 + Ax + B, \tag{2.1}$$

where the discriminant $\Delta = -16(4A^3 + 27B^2)$ is non-zero (this is equivalent with the curve being non-singular).

The point $P = (a, b)$ lies on the elliptic curve E if $a, b \in \bar{k}$ and (a, b) satisfies the equation (2.1). We use the notation $E(k)$ to denote points $(a, b) \in E$ with $a, b \in k$.

The most interesting property of an elliptic curve E is that there is a geometric group structure on the points of E (usually called the group law). In fact this group is abelian. So for points $P, Q \in E$ we denote the group operation by $P + Q \in E$. The neutral element in the group is the **point at infinity** which we denote 0.

For a positive integer n there is a endomorphim $[n] \colon E \to E$ given by

$$P \mapsto nP = P + P + \cdots + P.$$

A **n-torsion point** is a point $P = (x, y) \in E$ in the kernel of $[n]$, i.e. $nP = 0$ in the group law. We let $E[n] \subset E$ denote the subset of n-torsion points on E.

We will see that we can characterize $E[n]$ as the roots of the so called division polynomials defined over k.

The **integer division polynomials** $\psi_n \in \mathbb{Z}[A, B, x, y]$ are defined inductively.

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 8B^2 - A^3)
\end{aligned}$$

And,

$$\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \text{ for } m \geq 2 \\
\psi_{2m} &= \frac{\psi_m}{\psi_2}(\psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2), \text{ for } m \geq 3.
\end{aligned} \tag{2.2}$$

Furthermore define two more families of polynomials ϕ_n and ω_n.

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1} \text{ for } m \geq 1, \\
\omega_1 &= y, \\
\omega_m &= \frac{1}{2\psi_2}(\psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2) \text{ for } m \geq 2.
\end{aligned}$$

The key property is that we can obtain the division polynomials for $E\colon y^2 = x^3+Ax+B$ defined over k from the integer division polynomials $\psi_n \in \mathbb{Z}[A, B, x, y]$ defined by the formulas above. Indeed, let $\tau\colon \mathbb{Z}[A, B, x, y] \to k[x, y]$ by the linear extension of the natural map $\mathbb{Z}[A, B] \to k$, given by

$$\begin{aligned}
A &\mapsto A \\
B &\mapsto B \\
n \in \mathbb{Z} &\mapsto n1_k.
\end{aligned} \tag{2.3}$$

Then $\tau(\psi_n) \in k[x, y]$ is the division polynomial for E defined over k.

To save space let ψ_n, ϕ_n, ω_n denote $\tau(\psi_n), \tau(\phi_n), \tau(\omega_n)$ respectively.

Theorem 1. Let $P = (x, y)$ be a point on the elliptic curve E defined over k. Then

$$nP = \Big(\frac{\phi_n(x, y)}{\psi_n^2(x, y)}, \frac{\omega_n(x, y)}{\psi_n^3(x, y)}\Big)$$

Proof. This is usually proved analytically by properties of the Weierstrass P-functions. See [19, Section 9.5]. □

From this, we can characterize the n-torsion points.

Proposition 2. Let $P = (x, y)$ be a point on an elliptic curve E defined over k. Then $nP = 0$ iff $\psi_n(x, y) = 0$.

Proof. By Theorem 1, $nP = 0$ is equivalent to

$$\Big(\frac{\phi_n(x, y)}{\psi_n^2(x, y)}, \frac{\omega_n(x, y)}{\psi_n^3(x, y)}\Big) = 0.$$

But $\Big(\frac{\phi_n(x,y)}{\psi_n^2(x,y)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\Big)$ represents the point at infinity iff the denominators are zero. That is, $\psi_n(x, y) = 0$. □

Furthermore, it turns out that if n is odd then $\psi_n(x, y)$ can be reduced by the equation $y^2 = f(x)$ to a polynomial in only x. If n is even then $\psi_n = \psi_2 P_n(x)$ where P_n is a polynomial in only x. We define **univariate division polynomials** $P_n \in \mathbb{Z}[A, B, x]$ by

$$P_n(x) = \begin{cases} \psi_n & \text{if n odd} \\ \psi_n/\psi_2 & \text{if n even} \end{cases} \tag{2.4}$$

A similar recursion as for the ψ_n holds for the univariate P_n.

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, i.e , $A, B \in \mathbb{F}_q$. Then as before we consider P_n as a polynomial in $\mathbb{F}_q[x]$. If $(a, b) \in E$ is a n-torsion point with $b \neq 0$ then $P_n(a, b) = 0$ by Proposition 2. Further, if $a, b \in \mathbb{F}_q$ we get the following proposition by the polynomial remainder theorem.

Proposition 3. Let $P = (a, b) \in E(\mathbb{F}_q)$ with $b \neq 0$. Then $nP = 0$ iff $P_n(x) \equiv 0 \pmod{(x-a)}$ in $\mathbb{F}_q[x]$.

Note that $(a, 0) \in E(\mathbb{F}_q)$ has order 2. But these are exactly the $\mathbb{F}_q$-rational zeroes of $x^3 + Ax + B$. It is pretty clear these are the only solutions we discard when going from ψ_n to P_n. From this observation we can devise a simple algorithm to finding all $\mathbb{F}_q$-rational n-torsion points: $E[n](\mathbb{F}_q)$.

Algorithm 1. Given an elliptic curve E defined over $\mathbb{F}_q$ with equation $y^2 = x^3 + Ax + B$ and $n > 0$ the following algorithm will find $E[n](\mathbb{F}_q)$.

1. Record $0 = \infty$ as a n-torsion point.

2. If n is even, record all $\mathbb{F}_q$-rational zeros of $x^3 + Ax + B$.

3. Compute the polynomial $P_n(x)$ by computing the integer polynomial and reducing modulo p.

4. Factor $P_n(x)$ into irreducible factors $f_1, f_2, \dots f_k$ over $\mathbb{F}_q$.

5. For each factor f_i:

   (a) If f_i is linear then the zero α of f_i is the x-coordinate of a n-torsion point.

   (b) Lift α to E by finding the corresponding y-values $\{\beta_j\}$ in the Weierstrass equation such that $\beta_j \in \mathbb{F}_q$

   (c) Record $\{(\alpha, \beta_j)\}_j$.

Proof. Note that for each zero $\alpha \in \mathbb{F}_q$ we have either (i) $\beta = 0$ or (ii) $\beta = \pm\sqrt{\alpha^3 + A\alpha + B}$. However, the square root does not need to lie in $\mathbb{F}_q$ (it can also lie in $\mathbb{F}_{q^2}$).

Further, we prove that if $(\alpha, \beta_1), \beta_1 \neq 0$, is a n-torsion point then $(\alpha, \beta_2) = (\alpha, -\beta_1)$ is also a n-torsion point. Recall that the inverse operation in the group law is given by $P = (x, y) \mapsto -P = (x, -y)$. So, if (α, β) is a n-torsion point, i.e. $n(\alpha, \beta) = 0$, then

$$n(\alpha, -\beta) = n(-(\alpha, \beta)) = -n(\alpha, \beta) = -0 = 0.$$

Thus $(\alpha, -\beta)$ is a n-torsion point. This proves correctness. □

We will generalize the above algorithm to hyperelliptic curves.

2.2 Jacobian of hyperelliptic curves

To every hyperelliptic curve H we will associate a group structure $J(H)$ called the Jacobian of H. If H is an elliptic curve then $J(H)$ is isomorphic to the geometric group law on H. We follow the exposition in [19].

2.2.1 Divisors

Assume k is a field with $\operatorname{char} k \neq 2$. From this point forward, a **hyperelliptic curve** H will be assumed to have a rational Weierstrass point. Or equivalently, we assume a hyperelliptic curve is given as the of the vanishing locus of a Weierstrass equation of the form

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

where $f \in k[x]$ is a polynomial of degree $2g+1$.

Definition 4. For a point $P = (x, y)$ on H, $P' = (x, -y)$ is also on H since $(-y)^2 = y^2 = f(x)$. The map $w\colon H \to H$ given by

$$P = (x, y) \mapsto w(P) = (x, -y).$$

is called the **hyperelliptic involution**.

Definition 5. Let H be a hyperelliptic curve. Then the **divisor** D is a finite formal sum

$$\sum_i n_i[P_i], \tag{2.5}$$

where $n_i \in \mathbb{Z}$ and $P_i \in H$. Let $\operatorname{div}(H)$ denote the group of divisors of H.

For a divisor D, we define the **degree** of D as $\deg D = \sum_i n_i$. The subgroup of divisors of degree 0 is denoted $\operatorname{div}_0(H)$.

Remark. Note that $\operatorname{div}(H)$ is the free group generated by the set of points on H. In particular, $\operatorname{div}(H)$ is abelian.

Since every point P_i in a divisor D either has positive or negative coefficient, we can decompose D as

$$D = \operatorname{div}_0(D) + \operatorname{div}_\infty(D), \tag{2.6}$$

where,

$$\operatorname{div}_0(D) = \sum_{n_i > 0} n_i[P_i], \tag{2.7}$$

$$\operatorname{div}_\infty(D) = \sum_{n_i < 0} n_i[P_i]. \tag{2.8}$$

We also let $\deg_0(D) = \deg \operatorname{div}_0(D)$.

Now recall that the function field of an algebraic variety $k(V)$ is the rational functions on V. To every rational function $f \in \bar{k}(H)$ we associate a divisor $D \in \operatorname{div}(H)$ representing the 'zeroes' and 'poles' of f.

Recall that for any meromorphic function $f\colon \mathbb{C} \to \mathbb{C}$ we talk about poles and zeroes. For example $f(z) = z$ has a pole of order 1 at infinity and a zero of order 1 at $z = 0$. We say that $f(z)$ has order 1 at $z = 0$ and order -1 at $z = \infty$.

Interestingly, it is possible to define an *algebraic* analogue: For $f \in \bar{k}(H)$ and $P \in H$ we denote the **order of vanishing** of f at P by $\operatorname{ord}_P(f)$. We will not prove this here, cf. [18, II.3]).

Example 1. Let $k = \mathbb{Q}$ and consider the elliptic curve $C : y^2 = x^3 + 1$. Consider the rational function x on C. Plugging in $x = 0$ gives $y^2 = 1$ i.e. $y = \pm 1$. So the function x vanishes exactly at the points $(0, 1), (0, -1)$. Since $x/x = 1$ has no zeroes, the zeros at $(0, 1)$ and $(0, -1)$ are simple, i.e. the order is 1.

What happens at infinity? Note that,

$$x = \frac{x^3}{x^2} = \frac{x^3 + 1 - 1}{x^2} = \frac{y^2 - 1}{x^2}.$$

Switching to projective coordinates we get

$$\frac{(Y/Z)^2 - 1}{(X/Z)^2} = \frac{Y^2 - Z^2}{X^2}.$$

Hence x has a pole of order 2 at $(0 : 1 : 0) = 0$.

Definition 6. The **principal divisor** associated with f is

$$\operatorname{div}(f) = \sum \operatorname{ord}_P(f)[P], \tag{2.9}$$

where the sum is taking over all points on P.

Denote the subgroup of principal divisors with $\operatorname{Princ}(H)$. That is,

$$\operatorname{Princ}(H) = \{D \in \operatorname{div}(H) \mid \operatorname{div}(f) = D \text{ for some rational function f }\}.$$

Remark. Note that the definition only makes sense if finitely many $\operatorname{ord}_P(f)$ is non-zero. This is true but we will not prove this here. See [18, Proposition II.1.2].

Example 2. Continuing Example 1 we see that

$$\operatorname{div}(x) = [(0, 1)] + [(0, -1)] - 2[\infty].$$

Recall that meromorphic functions has the same number of poles as zeroes (counting multiplicity). Analogously:

Theorem 2. Principal divisors have degree 0. That is, $\deg \operatorname{div}(f) = 0$ for all $f \in \bar{k}(H)$.

Proof. See [18, Proposition II.3.1(b)]. □

Theorem 2 implies that $\operatorname{Princ}(H) \subset \operatorname{div}_0(H)$. Then define:

Definition 7. Let H be a hyperelliptic curve. Then the **Jacobian** of H, denoted $J(H)$, is the quotient group $\operatorname{div}_0(H)/\operatorname{Princ}(H)$.

Equivalently, the elements of the Jacobian are **divisor classes** under the equivalence relation $D \sim D'$ iff $D - D' \in \operatorname{Princ}(H)$.

2.2.2 Mumford representation

Definition 8. A divisor $D = \sum_i c_i([P_i] - [\infty])$ where $P_i = (a_i, b_i)$ is called **semi-reduced** if, for all i,

1. $c_i \geq 0$,

2. if $b_i = 0$ then $c_i = 1$,
3. only one of P_i, $w(P_i) = [(a_i, -b_i)]$ appears in D.

If further, $\deg_0(D) \leq g$, then D is called **reduced**.

Definition 9. For any two divisors $D = \sum_i d_i[P_i]$ and $E = \sum_j e_j[P_j]$ we define the **greatest common denominator** of D, E as

$$\gcd(D, E) = \sum_i c_i[P_i],$$

where $c_i = \max(d_i, e_i)$.

Theorem 3. There is a bijection between semi-reduced divisors D and polynomial pairs $(U(x), V(x))$ such that,

1. U is monic,
2. $\deg(U) = \sum_i c_i$ and $\deg(V) < \deg(U)$,
3. $U|(V^2 - f)$.

The bijection is given by,

$$(U, V) \mapsto \gcd(\operatorname{div}(U), \operatorname{div}(y - V)).$$

Furthermore, the above bijection maps reduced divisors D to (U, V) such that $\deg V < \deg U \leq g$.

Proof. See [19, Theorem 13.5]. □

Given an arbitrary divisor D with degree 0 there is a semi-reduced divisor D' representing the same divisor class, i.e. $D' \sim D$. The following example illustrates the general technique.

Example 3. Let $P = (a, b)$ be a point on the hyperelliptic curve $C : y^2 = x^5 + 1$ with $b \neq 0$. Then consider the divisor $D = -1[(a, b)] + 2[(a, -b)] - [\infty]$. Note that D is **not** semi-reduced since (i) it contains a negative coefficient and (ii) it contains both $[(a, b)]$ and $[(a, -b)]$. However,

$$\begin{aligned} D &\sim -1[(a, b)] + 2[(a, -b)] - [\infty] + \operatorname{div}(x - a) \\ &\sim -1[(a, b)] + 2[(a, -b)] - [\infty] + [(a, b)] + [(a, -b)] - 2[\infty] \\ &\sim 3[(a, -b)] - 3[\infty] \end{aligned}$$

Hence $[D]$ is represented by the semi-reduced divisor $D' \sim 3[(a, -b)] - 3[\infty]$. Moreover, since C has genus 2 and $\deg_0(D') = 3 > 2$, D' is not reduced.

Using the technique in the example, it is not hard to believe:

Proposition 4. Every divisor class can be represented by a semi-reduced divisor.

The next problem is going from a semi-reduced divisor to a reduced divisor in the same divisor class. In the next section we will give an algorithm that solves this problem.

Proposition 5. Every divisor class is uniquely represented by a reduced divisor.

Proof. Existence follows from the algorithm in the next section. Uniqueness is more complicated, requiring the Riemann-Roch theorem. See [19, Proposition 13.6] for proof. □

Combining Theorem 3 and Proposition 5, it follows that every divisor class corresponds to a polynomial pair $(U(x), V(x))$.

Corollary 1. Every divisor class $[D]$ is uniquely represented by a pair of polynomials (U, V) such that

1. U is monic
2. $\deg(V) < \deg(U) \leq g$
3. $U|(V^2 - f)$

The pair $(U(x), V(x))$ is called the **Mumford representation** of the class $[D]$.

Furthermore, there is a there is a natural way to view points $P \in H$ as divisors in $J(H)$.

Proposition 6. For a point $P = (x, y)$ consider the map $i\colon H \to J(H)$ given by $P \mapsto [P] - [\infty]$. The claim is that i is injective.

To save space we will write $(x, y) \in J(H)$ for the image of $P = (x, y) \in H$ under i.

Proof. For any P, $D = [P] - [\infty]$ is a reduced divisor with degree $1 \leq g$. Hence the class is uniquely represented by D. This proves i is injective. □

2.2.3 Reduction algorithm

In this section we will compute the unique Mumford representation for a given semi-reduced divisor D.

Lemma 1. (a) Let

$$U(x) = \prod_{i=1}^{k}(x - a_i)^{c_i},$$

where $a_i \in \bar{k}$ and $c_i \in \mathbb{Z}$, i.e. $U(x)$ is rational function. Then

$$\operatorname{div}(U(x)) = \sum_{i=1}^{k} c_i([P_i] + [w(P_i)] - 2[\infty]),$$

where $P_i = (a_i, \sqrt{f(a_i)})$ and $w(P_i) = (a_i, -\sqrt{f(a_i)})$.

(b) Let $V(x)$ be a polynomial. Then $\operatorname{div}(y - V(x)) = D$ is a semi-reduced divisor and $\operatorname{div}(y + V(x)) = w(D)$.

(c) Let $A(x), B(x)$ be polynomials. Then $\operatorname{div}(A(x) - B(x)y) = D$ is a semi-reduced divisor and $\operatorname{div}(A(x) + B(x)y) = w(D)$.

Proof. For (a),(b), see [19, Proposition 13.2].

(c) Let $D = \mathrm{div}(A(x) - B(x)y)$. Then since,

$$A(x) - B(x)y = B(x)(A(x)/B(x) - y), \tag{2.10}$$

we have,

$$D = \mathrm{div}(A(x) - B(x)y) = \mathrm{div}(B(x)) + \mathrm{div}(A(x)/B(x) - y) \tag{2.11}$$

Note that $A(x)/B(x) - y$ will have finite poles $(a_i, \pm\sqrt{f(a_i)})$ where a_i are the zeroes of $B(x)$. So every finite pole of $\mathrm{div}(A(x)/B(x) - y)$ will cancel out one of the zeros $(a_i, \pm\sqrt{f(a_i)})$ in $\mathrm{div}(B(x))$. Hence D is semi-reduced.

Furthermore, since $A(x) + B(x)y = B(x)(A(x)/B(x)) + y)$,

$$\mathrm{div}(A(x) + B(x)y) = \mathrm{div}(B(x)) + \mathrm{div}(A(x)/B(x) + y). \tag{2.12}$$

The finite poles $(a_i, \pm\sqrt{f(a_i)})$ in $\mathrm{div}(A(x)/B(x)+y)$ have opposite signs on the y-coordinate. Moreover by (b),

$$\mathrm{div}_0(A(x)/B(x) + y) = w(\mathrm{div}_0(A(x)/B(x) - y)). \tag{2.13}$$

Hence,

$$\mathrm{div}(A(x) + B(x)y) = w(D). \tag{2.14}$$

□

Algorithm 2. Let D be a semi-reduced divisor and let (U, V) be the polynomial pair corresponding to D by Theorem 3. Then the following algorithm computes the Mumford representation of the unique reduced divisor D' such that $D \sim D'$.

1. Let $U' = (f - V^2)/U$ and $V' = -V \pmod{U'}$.
2. Multiply U' with a constant to make U' monic.
3. If $\deg U' \leq g$ then output (U', V') otherwise let $U = U'$ and $V = V'$ and goto step 1.

Proof. Since (U, V) is a semi-reduced divisor, $U \mid (f - V^2)$ so U' is a polynomial. Because V' is the remainder when dividing with U' it follows that $\deg V' < \deg U'$. Further,

$$f - (V')^2 \equiv f - (-V)^2 \equiv f - V^2 \pmod{U'}.$$

But since $U' \mid f - V^2$ we have $f - (V')^2 \equiv 0 \pmod{U'}$. Hence (U', V') is a semi-reduced divisor.

Next, we need to prove (i) that the divisor (U', V') is equivalent to the divisor (U, V) in step 1, and (ii) that the loop terminates.

Let

$$D = (U, V) = \gcd(\mathrm{div}(U(x)), \mathrm{div}(y - V(x))).$$

Then $\mathrm{div}(U(x)) = D + w(D)$. Further, take $E = D - \mathrm{div}(y - V(x))$, then, $\mathrm{div}(y - V(x)) = D + E$.

Suppose to get a contradiction that $[(a, b)]$ is a common divisor of $w(D)$ and E. If (i) $b = 0$ then (a, b) is a zero of both $y - V(x)$ and $y + V(x)$ and therefore also a zero of $U(x)$. Then D contains both $[(a,b)]$ and $[(a,-b)]$ which contradicts that D is a semi-reduced divisor.

If (ii) $b \neq 0$ then $D+E$ contains both $[(a,b)]$ and $[(a,-b)]$. This contradicts that $D+E = \operatorname{div}(y - V(x))$ is a semi-reduced divisor by Lemma 1(b). Thus $\gcd(E, w(D)) = 1$.

Now, by Lemma 1(b),

$$\operatorname{div}(y + V(x)) = w(D+E) = w(D) + w(E). \tag{2.15}$$

A similar argument as above shows that $\gcd(E, w(E)) = 1$.

But since,

$$UU' = f - V^2 = (y - V(x))(y + V(x)), \tag{2.16}$$

we have,

$$\operatorname{div}(U) + \operatorname{div}(U') = D + E + w(D+E). \tag{2.17}$$

By subtracting $\operatorname{div}(U) = D + w(D)$ from both sides we get,

$$\operatorname{div}(U') = E + w(E). \tag{2.18}$$

Further, by definition,

$$\gcd(\operatorname{div}(U'(x)), \operatorname{div}(y - V'(x))) = \gcd(\operatorname{div}(U'(x)), \operatorname{div}(y + V(x))). \tag{2.19}$$

Recall that $\gcd(E, w(E)) = 1$ and $\gcd(E, w(D)) = 1$. Thus combining Equations (2.19), (2.18) and (2.15) yields,

$$(U', V') = \gcd(\operatorname{div}(U'(x)), \operatorname{div}(y + V(x))) = w(E) \tag{2.20}$$

But

$$D - \operatorname{div}(y - V(x)) = -E = w(E) - \operatorname{div}(U'). \tag{2.21}$$

Hence $D \sim w(E)$. This proves (i).

To prove that the algorithm terminates we show that the degree of U decreases in every iteration of the loop. Suppose that $\deg U \geq g+1$. Then because $\deg f = 2g+1$,

$$\deg f < 2 \deg U.$$

Further since $\deg V < \deg U$,

$$\deg(V^2) = 2 \deg V < 2 \deg U.$$

Now (2.16) gives,

$$\deg U + \deg U' = \deg(f - V^2) < 2 \deg U.$$

Hence $\deg U' < \deg U$. This concludes the proof. □

2.2.4 Cantor's algorithm

The Mumford representation gives a very concrete and computational realization of the elements of $J(H)$. We present an algorithm by David Cantor [4] for efficiently computing $D_1 + D_2$ when D_1, D_2 are given in Mumford representation.

Algorithm 3. Let $D_1 = (U_1, V_1), D_2 = (U_2, V_2)$ be given points of $J(H)$. The following algorithm computes the Mumford representation of the sum $D_3 = D_1 + D_2$.

1. Let $d = \gcd(U_1, U_2, V_1 + V_2)$. Use the Extended Euclidean Algorithm to find polynomials h_1, h_2, h_3 such that
$$d = U_1h_1 + U_2h_2 + (V_1 + V_2)h_3. \tag{2.22}$$
Let
$$V_0 = (U_1V_2h_1 + U_2V_1h_2 + (V_1V_2 + f)h_3)/d, \tag{2.23}$$
and
$$U = \frac{U_1U_2}{d^2}, V = V_0(\text{mod U}). \tag{2.24}$$
Then $D' = (U, V)$ is semi-reduced and $D' \sim D_1 + D_2$.
2. Reduce $D' = (U, V)$ to Mumford representation D_3 by the reduction algorithm. Then D_3 is the unique Mumford representation of the divisor class $D_1 + D_2$.

Proof. We only prove correctness here. Refer to [4] for time complexity.

Note that $d|U_1$ and $d|U_2$. Further, since $d|U_1$ and $U_1|(f - V_1^2)$ we have $d|(f - V_1^2)$. Hence,
$$V_1V_2 + f = V_1(V_1 + V_2) + (f - V_1^2),$$
is divisible by d. This shows (2.23) is well-defined.

First we prove that $D' = (U, V)$ is semi-reduced. It is clear U is a monic polynomial and $\deg V < \deg U$. Furthermore, tedious but routine calculations show, $V^2 - f \equiv 0 \pmod U$. Thus $D' = (U, V)$ is a semi-reduced divisor.

Now it remains to show $D' \sim D_1 + D_2$. We do this by showing:

$$\text{There is a } D'' \sim D_1 + D_2 \text{ such that } \operatorname{ord}_P(D'') = \operatorname{ord}_P(D') \text{ for all } P \tag{2.25}$$

Let $P = (a, b)$ be an arbitrary point. Assume r_i is the order of vanishing of P in D_i and s_i the order of vanishing of $w(P)$. That is,
$$D_1 = (U_1, V_1) = r_1([P] - [\infty]) + s_1([w(P)] - [\infty]) + \dots \tag{2.26}$$
$$D_2 = (U_2, V_2) = r_2([P] - [\infty]) + s_2([w(P)] - [\infty]) + \dots \tag{2.27}$$

We begin by showing:

Lemma 2. $\operatorname{ord}_P((y - V_0)d) \geq r_1 + r_2$.

Proof. The following functions
$$U_1U_2, (y - V_1)U_2, (y - V_2)U_1, (y - V_1)(y - V_2) = f + V_1V_2 - (V_1 + V_2)y,$$
have order of vanishing at least $r_1 + r_2$ at P by (2.26) and (2.27).

Then the lemma follows from,
$$(y - V_2)U_1h_1 + (y - V_1)U_2h_2 + ((V_1 + V_2) - f - V_1V_2)h_3 = dy - dV_0 = d(y - V_0).$$
□

Back to the proof of Algorithm 3. There are several cases.

Case A. $s_1 = s_2 = 0$ or $b = 0$.

If $b = 0$ then $P = w(P) = (a, 0)$. But since D_1, D_2 are semi-reduced, we can assume with loss of generality that $s_1 = s_2 = 0$.

We will prove,

1. $\mathrm{ord}_P(U) = r$
2. $\mathrm{ord}_P(y - V_0) \geq r$

where

$$r = \begin{cases} r_1 + r_2 & \text{if } b \neq 0 \\ r_1 + r_2 (\text{mod } 2) & \text{if } b = 0 \end{cases}.$$

When $b \neq 0$ this implies that $\mathrm{ord}_P(D') = \mathrm{ord}_P(U, V) = r_1 + r_2$ since

$$(U, V) = \gcd(\mathrm{div}(U), \mathrm{div}(y - V)) = \gcd(\mathrm{div}(U), \mathrm{div}(y - V_0)), \tag{2.28}$$

where the last equality follows from $V = V_0$ (mod U). Hence (1), (2) implies that $\mathrm{ord}_P(D') = \mathrm{ord}_P(D_1 + D_2)$.

Moreover, when $b = 0$, we have $P = w(P) = (a, 0)$. Then for some k, $r_1 + r_2 = r + 2k$ and

$$D_1 + D_2 = (r + 2k)([P] - [\infty]) + \ldots,$$

where the dots represent remaining terms without P and $w(P)$. But since $2k([P] - [\infty]) = k(2[P] - 2[\infty])$ is principal, we can let $D'' = r([P] - [\infty]) + \ldots$ represent the divisor class $D_1 + D_2$. Then $\mathrm{ord}_P(D'') = r$. Therefore (1) and (2) implies $\mathrm{ord}_P(D') = \mathrm{ord}_P(D'')$.

Subcase 1. $r_1 = r_2 = 0$

In this case $U_i(P) \neq 0$, so $U(P) \neq 0$ and $d(P) \neq 0$. Then neither P nor $w(P)$ appears in (U, V). So $\mathrm{ord}_P(U, V) = 0 = r_1 + r_2$. Since $d(P) \neq 0$, Lemma 2 implies that $\mathrm{ord}_P(y - V_0) \geq r_1 + r_2$.

Subcase 2. At least one $r_i > 0$ and $b \neq 0$. If both $r_i > 0$ then $(V_1 + V_2)(P) = V_1(a) + V_2(a) = 2b \neq 0$. On the other hand, assume exactly one $r_i > 0$, say $r_1 > 0$. Then $V_1(a) = b$. Suppose that $V_2(a) = -b$. Then $y - V_2$ vanishes at P. But by assumption $r_2 = 0$ so U_1 does not vanish at P by (2.27). In either case $d(P) \neq 0$. But since $U = U_1 U_2 / d^2$, this implies that $\mathrm{ord}_P(U) = \mathrm{ord}_P(U_1) + \mathrm{ord}_P(U_2) = r_1 + r_2$. (ii) follows from $d(P) \neq 0$, as in the previous case.

Subcase 3. Both $r_1, r_2 > 0$ and $b = 0$ Since D_1, D_2 are reduced by assumption, $r_1 = r_2 = 1$. On the other hand, U_1, U_2 has simple zeros at $x = a$. Further since $V_1(a) = 0$ and $V_2(a) = 0$ it follows that $V_1 + V_2$ has at least a simple zero at P. Hence d has a simple zero at P. This implies that $U = U_1 U_2 / d^2$ does not vanish at $x = a$. Moreover, since $d(y - V_0)$ vanishes of order at least $r_1 + r_2 = 2$, but d only has a simple zero, we have $\mathrm{ord}_P(y - V_0) \geq 1$. Hence (1), (2) holds with $r = 0$.

Subcase 4. Exactly one $r_i > 0$ and $b = 0$ Assume $r_1 = 1$ and $r_2 = 0$. Suppose that $(V_1 + V_2)(P) = 0$. Then $V_2(a) = 0$ so $y - V_2$ has a zero at P. But since $r_2 = 0$ this implies that U_2 does not vanish at P. In either case, $d(P) \neq 0$. Hence as in subcase (2), $\mathrm{ord}_P(U) = r$ and $\mathrm{ord}_P(y - V_0) \geq 1$ with $r = 1$.

Case B. $r_1 > 0$, $s_2 > 0$ and $b \neq 0$.

Because D_1, D_2 are semi-reduced this implies that $r_2 = 0$ and $s_1 = 0$.

Since $s_2 > 0$ it follows $V_2(a) = -b$. Then $(y - V_2)(P) = 2b \neq 0$. But since $(y + V_2)(y - V_2) = f - V_2^2$, $U_2|(f - V_2^2)$ and $\mathrm{ord}_P(U_2) \geq s_2$,

$$\mathrm{ord}_P(y + V_2) \geq s_2.$$

Then because $V_1 + V_2 = (y + V_2) - (y - V_1)$,

$$\mathrm{ord}_P(V_1 + V_2) \geq \min(r_1, s_2)$$

But since d is the gcd,

$$\mathrm{ord}_P(d) = \min(r_1, s_2).$$

Now, assume without loss of generality that $r_1 \geq s_2$. Then

$$\mathrm{ord}_P(U) = r_1 + s_2 - 2\min(r_1, s_2) = r_1 - s_2. \tag{2.29}$$

Furthermore because $\mathrm{ord}_P((y - V_0)d) \geq r_1 + r_2 = r_1$,

$$\mathrm{ord}_P(y - V_0) = \mathrm{ord}_P((y - V_0)d) - \mathrm{ord}_P(d) \geq r_1 - s_2.$$

Hence $\mathrm{ord}_P(D') = \mathrm{ord}_P(U, V) = r_1 - s_2$.

If $r_1 = s_2$ then

$$\begin{aligned} D_1 + D_2 &= r_1([P] - [\infty]) + s_2([w(P)] - [\infty]) + D'' \\ &= r_1([P] + [w(P)] - 2[\infty]) + D'', \end{aligned}$$

where D'' denotes the rest of the terms. Then since $([P] + [w(P)] - 2[\infty])$ is principal, $D'' \sim D_1 + D_2$. Further, (2.29) implies that $U(P) \neq 0$ so D' does not contain P or $w(P)$. Hence D' and D'' agree on the points P, $w(P)$.

Assume that $r_1 - s_2 > 0$. Then since D' is semi-reduced, D' does not contain $[w(P)] - [\infty]$. Consider $D'' = D_1 + D_2 - s_2([P] + [w(P)] - 2[\infty])$. Because $([P] + [w(P)] - 2[\infty])$ is principal, $D'' \sim D_1 + D_2$. On the other hand D'' agrees with D' on P and $w(P)$. That is, $\mathrm{ord}_P(D'') = r_1 - s_2$ and $\mathrm{ord}_{w(P)}(D'') = 0$.

The cases (C) $r_1 = r_2 = 0$, and (D) $s_1 > 0$ and $r_2 > 0$ follows by letting P and $w(P)$ switch places.

□

Remark. Cantor's algorithm requires concrete elements in k for the coefficients of (U, V). This means we can't let the coefficients of $U(X)$ be polynomials themselves in some indeterminate. More precisely, the algorithm needs to determine the degree of the polynomial which is impossible if the coefficients are indeterminate. This is a crucial difference from the special case of elliptic curves where we have an addition map.

Remark. We further note here that for different applications it might be useful to consider some of the explicit special cases of Cantor's algorithm in [6]. However these also only operates on concrete coefficients.

To motivate the next section, we note that the above discussion does suggest a naive algorithm for calculating torsion points over finite fields. Since we are working with finite fields, we can just check for every $x, y \in \mathbb{F}_q$ if $n(x, y) = 0$ in the Jacobian using Cantor's algorithm.

Algorithm 4. Let H be a hyperelliptic curve over the finite field $\mathbb{F}_q$. Then the following algorithm algorithm will find all $\mathbb{F}_q$-rational n-torsion points.

1. For each x in $\mathbb{F}_q$:
   (a) Find the $y \in \mathbb{F}_q$ such that $(x, y) \in H$. I.e. plug in the x-value and solve the curve's equation for y over $\mathbb{F}_q$.
   (b) Calculate $n(x, y)$ using Cantor's algorithm (Algorithm 3).
   (c) If $n(x, y) = 0$ record (x, y) as a torsion point. Otherwise continue.

One obvious drawback with Algorithm 4 is that the run-time will increase (at least) linearly with q since we are looping over all the elements of $\mathbb{F}_q$. In the next chapter we will present a more sophisticated approach that will not have this heavy dependence on q.

2.2.5 Jacobians defined over a finite field

We shall now consider certain subgroups of the Jacobian $J(H)$, similar to the subgroup $E(\mathbb{F}_q)$ of points on the elliptic curve E defined over $\mathbb{F}_q$.

Let $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. For any zero-degree divisor $D = \sum_i n_i([(x_i, y_i)] - [\infty])$ we extend the action of σ to $J(H)$ by letting $\sigma(D) = \sum_i n_i([\sigma x_i, \sigma y_i] - [\infty])$.

Definition 10. Let $\mathbb{F}_q$ be a finite field. Then the divisor $D \in \mathrm{Div}_0(H)$ is **defined over** $\mathbb{F}_q$ if D is fixed by the Galois group, i.e.

$$\sigma(D) = D$$

for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$.

Similarly, for a divisor class $[D] \in J(H)$ with unique reduced representative D, we say $[D]$ is **defined over** $\mathbb{F}_q$ if $D = \sigma(D)$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Let $J(H)(\mathbb{F}_q)$ denote the divisor classes defined over $\mathbb{F}_q$.

Remark. Let $D = [(x_0, y_0)] + [(x_1, y_1)] - 2[\infty]$ defined over $\mathbb{F}_q$. Note that it is **not** necessarily true that $x_0, x_1, y_0, y_1 \in \mathbb{F}_q$. Instead the coordinates might lie in some field extension of $\mathbb{F}_q$.

A priori $J(H)(\mathbb{F}_q)$ is not a group. We need to check that if D_1, D_2 are two divisors defined over $\mathbb{F}_q$ then $D_1 + D_2$ is also defined over $\mathbb{F}_q$. Since $J(H)(\mathbb{F}_q)$ is by definition a subset of $J(H)$ it then follows that $J(H)(\mathbb{F}_q)$ inherits an addition from $J(H)$.

Theorem 4. A divisor class in $J(H)$ with Mumford representation $(U(X), V(X))$ is defined over $\mathbb{F}_q$ iff $U(X), V(X) \in \mathbb{F}_q[X]$.

Proof. First assume that $U(X), V(X)$ in $\mathbb{F}_q$. Then the automorphisms $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ permute the zeroes of $U(X)$ and $V(X)$. This implies σ fixes the divisor $(U(X), V(X)) = \gcd(\mathrm{div}(U), \mathrm{div}(y - V))$. Hence (U, V) is defined over $\mathbb{F}_q$.

Conversely, let $D = (U(X), V(X))$ and assume $[D] = [\sigma(D)]$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Let R be the unique reduced divisor representing D. Then consider $\sigma(R)$. Since $[R] = [D]$ there exists some f such that $D - R = \mathrm{div}(f)$. But then $\sigma(D) - \sigma(R) = \mathrm{div}(\sigma(f))$. Hence $[\sigma(R)] = [\sigma(D)]$. Further by considering the definition of reduced divisor, $\sigma(R)$ is reduced.

Next, let $\sigma(R)$ be represented by (U', V'). The claim is that $U' = \sigma(U)$, $V' = \sigma(V)$ where σ acts on the coefficients of U respective V. By definition,

$$\sigma(R) = \sum_i n_i([\sigma x_i, \sigma y_i] - [\infty]).$$

Then since σ is an automorphism,

$$U'(X) = (X - \sigma x_0)(X - \sigma x_1) \dots (X - \sigma x_t) = X^t - \sigma e_1 X^{t-1} + \dots + (-1)^t \sigma e_t,$$

where e_i are the elementary symmetric polynomials in $x_0, x_1, \dots, x_t$, i.e. the coefficients of U. Thus $U' = \sigma(U)$.

Recall that V' is uniquely determined by the condition $V'(\sigma x_i) = \sigma y_i$. But,

$$\begin{aligned} \sigma(V)(\sigma x_i) &= \sigma a_s (\sigma x_i)^s + \sigma a_{s-1} (\sigma x_i)^{s-1} + \dots + \sigma a_0 \\ &= \sigma a_s \sigma x_i^s + \sigma a_{s-1} \sigma x_i^{s-1} + \dots + \sigma a_0 \\ &= \sigma(a_s x_i^s + \dots + a_0) = \sigma y_i. \end{aligned}$$

Hence $V' = \sigma(V)$.

Now, since both R and $\sigma(R)$ are reduced, $R = \sigma(R)$. So $(U', V') = (U, V)$. That is, the coefficients of U, V are fixed by all σ. Then since the fixed field of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is $\mathbb{F}_q$ it follows that the coefficients of U, V lies in $\mathbb{F}_q$. □

Proposition 7. The set $J(H)(\mathbb{F}_q)$ is a well-defined group and a subgroup of $J(H)$.

Proof. By the discussion above it is enough to show $J(H)(\mathbb{F}_q)$ is closed under divisor addition. Take $D_1 = (U_1, V_1), D_2 = (U_2, V_2) \in J(H)(\mathbb{F}_q)$. Then Cantor's algorithm let us compute $D_1 + D_2 = (U, V)$. Since every step in the algorithm is polynomial arithmetic it follows $U, V \in \mathbb{F}_q$ and hence $D_1 + D_2 \in J(H)(\mathbb{F}_q)$. □

3 Division points

3.1 Torsion points and division points

We will in this chapter find two algorithms for computing so called division points.

Let H be a hyperelliptic curve of genus g defined over a finite field $\mathbb{F}_q$. For any integer $n \geq 0$ there is an endomorphism $[n]\colon J(H) \to J(H)$ given by $D \mapsto nD = D + D + \cdots + D$. If $n < 0$ we take $[n](D) = -[-n](D)$.

It turns out the kernel of $[n]$ has an easy description [16, pp. 4].

Theorem 5. Assume that $\gcd(n, p) = 1$. Then, over the algebraic closure $\bar{\mathbb{F}}_q$,

$$\ker[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g},$$

where the right-hand expression is a direct sum of $2g$ copies of $\mathbb{Z}/n\mathbb{Z}$.

Definition 11. A point $P = (x, y) \in H(\mathbb{F}_{\mathrm{q}})$ such that $i(x, y) \in \ker[n]$ is called a **n-torsion point**. Alternatively, we write this as $n(x, y) = 0$ in $J(H)$. We let $H[n](\mathbb{F}_q)$ denote the set of n-torsion points.

Remark. We require as part of the definition that a torsion point is $\mathbb{F}_q$-rational.

Problem 1. Assume we are given a hyperelliptic curve H defined over $\mathbb{F}_q$ and integer $n > 1$. How do we find all n-torsion points?

Using the terminology in [5], we define:

Definition 12. Let H be a hyperelliptic curve defined over $\mathbb{F}_q$. A divisor D in $J(H)(\mathbb{F}_q)$ is called a ***n*-divisor point** for H if $D \in \ker[n]$. We let $J(H)[n](\mathbb{F}_q)$ denote the set of n-division points.

Remark. Note that n-torsion points are (rational) points on the curve. In contrast, division points are divisors in the Jacobian.

Clearly if $P = (x, y) \in H$ is a n-torsion point then $i(x, y) \in J(H)$ is a n-division point. In other words, finding n-torsion points is a subproblem of the more general problem:

Problem 2. Assume we are given a hyperelliptic curve H defined over $\mathbb{F}_q$ and integer $n > 1$. How do we find all n-division points?

Next, we will see that we can solve Problem 1 by a direct analogue of Algorithm 1 using a generalization of division polynomials to hyperelliptic curves.

3.2 Cantor's division polynomials

In [5] Cantor generalizes the classical division polynomials for elliptic curves to hyperelliptic curves. We will give an outline of the construction here but leave

n	ψ_n
1	0
2	1
3	$4a_5x^5 + 4a_4x^4 + 4a_3x^3 + 4a_2x^2 + 4a_1x + 4a_0$
4	$10a_5^3x^12 + 24a_4a_5^2x^11 + 16a_4^2a_5x^10 + 26a_3a_5^2x^10 + 40a_3a_4a_5x^9 + 20a_2a_5^2x^9$ $+30a_3^2a_5x^8 + 40a_2a_4a_5x^8 - 10a_1a_5^2x^8 + 80a_2a_3a_5x^7 - 80a_0a_5^2x^7 - 2a_3^3x^6$ $+8a_2a_3a_4x^6 - 16a_1a_4^2x^6 + 64a_2^2a_5x^6 + 68a_1a_3a_5x^6 - 112a_0a_4a_5x^6 - 4a_2a_3^2x^5$ $+16a_2^2a_4x^5 - 8a_1a_3a_4x^5 - 64a_0a_4^2x^5 + 152a_1a_2a_5x^5 - 8a_0a_3a_5x^5 - 10a_1a_3^2x^4$ $+40a_1a_2a_4x^4 - 80a_0a_3a_4x^4 + 110a_1^2a_5x^4 + 120a_0a_2a_5x^4 - 40a_0a_3^2x^3$ $+40a_1^2a_4x^3 + 240a_0a_1a_5x^3 + 10a_1^2a_3x^2 - 40a_0a_2a_3x^2 + 80a_0a_1a_4x^2$ $+160a_0^2a_5x^2 + 4a_1^2a_2x - 16a_0a_2^2x + 8a_0a_1a_3x + 64a_0^2a_4x + 2a_1^3$ $-8a_0a_1a_2 + 16a_0^2a_3$
5	$4(5a_5^4x^{16} + 16a_4a_5^3x^{15} + 16a_4^2a_5^2x^{14} + 20a_3a_5^3x^{14} + 56a_3a_4a_5^2x^{13} + 70a_3^2a_5^2x^{12}$ $+56a_2a_4a_5^2x^{12} - 140a_1a_5^3x^{12} + 280a_2a_3a_5^2x^{11} - 224a_1a_4a_5^2x^{11} - 560a_0a_5^3x^{11}$ $-28a_3^3a_5x^{10} + 112a_2a_3a_4a_5x^{10} - 224a_1a_4^2a_5x^{10} + 336a_2^2a_5^2x^{10} + 252a_1a_3a_5^2x^{10}$ $-1232a_0a_4a_5^2x^{10} - 8a_3^3a_4x^9 + 32a_2a_3a_4^2x^9 - 64a_1a_4^3x^9 - 80a_2a_3^2a_5x^9$ $+256a_2^2a_4a_5x^9 - 48a_1a_3a_4a_5x^9 - 1088a_0a_4^2a_5x^9 + 1040a_1a_2a_5^2x^9$ $-360a_0a_3a_5^2x^9 - 3a_3^4x^8 - 8a_2a_3^2a_4x^8 + 80a_2^2a_4^2x^8 - 64a_1a_3a_4^2x^8 - 320a_0a_4^3x^8$ $-64a_2^2a_3a_5x^8 - 148a_1a_3^2a_5x^8 + 880a_1a_2a_4a_5x^8 - 1248a_0a_3a_4a_5x^8$ $+990a_1^2a_5^2x^8 + 1000a_0a_2a_5^2x^8 - 8a_2a_3^3x^7 + 32a_2^2a_3a_4x^7 - 80a_1a_3^2a_4x^7$ $+256a_1a_2a_4^2x^7 - 640a_0a_3a_4^2x^7 - 64a_2^3a_5x^7 - 48a_1a_2a_3a_5x^7 - 640a_0a_3^2a_5x^7$ $+1040a_1^2a_4a_5x^7 + 512a_0a_2a_4a_5x^7 + 2720a_0a_1a_5^2x^7 - 28a_1a_3^3x^6$ $+112a_1a_2a_3a_4x^6 - 560a_0a_3^2a_4x^6 + 336a_1^2a_4^2x^6 - 224a_1a_2^2a_5x^6$ $+252a_1^2a_3a_5x^6 - 560a_0a_2a_3a_5x^6 + 2912a_0a_1a_4a_5x^6 + 2240a_0^2a_5^2x^6$ $-168a_0a_3^3x^5 + 280a_1^2a_3a_4x^5 - 448a_0a_2a_3a_4x^5 + 896a_0a_1a_4^2x^5 - 224a_1^2a_2a_5x^5$ $-448a_0a_2^2a_5x^5 + 784a_0a_1a_3a_5x^5 + 2688a_0^2a_4a_5x^5 + 70a_1^2a_3^2x^4 - 280a_0a_2a_3^2x^4$ $+56a_1^2a_2a_4x^4 - 224a_0a_2^2a_4x^4 + 672a_0a_1a_3a_4x^4 + 896a_0^2a_4^2x^4 - 140a_1^3a_5x^4$ $-560a_0a_1a_2a_5x^4 + 1120a_0^2a_3a_5x^4 + 56a_1^2a_2a_3x^3 - 224a_0a_2^2a_3x^3$ $+112a_0a_1a_3^2x^3 + 896a_0^2a_3a_4x^3 - 560a_0a_1^2a_5x^3 + 16a_1^2a_2^2x^2 - 64a_0a_2^3x^2$ $+20a_1^3a_3x^2 - 48a_0a_1a_2a_3x^2 + 240a_0^2a_3^2x^2 - 80a_0a_1^2a_4x^2 + 256a_0^2a_2a_4x^2$ $-640a_0^2a_1a_5x^2 + 16a_1^3a_2x - 64a_0a_1a_2^2x - 8a_0a_1^2a_3x + 160a_0^2a_2a_3x$ $-64a_0^2a_1a_4x - 320a_0^3a_5x + 5a_1^4 - 24a_0a_1^2a_2 + 16a_0^2a_2^2 + 32a_0^2a_1a_3 - 64a_0^3a_4)$ $(a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0)$

Table 3.1: First generic division polynomials for the genus 2 hyperelliptic curve $y^2 = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$.

out the technical proofs. See Table 3.1 and Appendix A for examples of division polynomials.

Let H be a hyperelliptic curve with Weierstrass equation $y^2 = \sum_{i=1}^{2g+1} a_i x^i$ with $a_{2g+1} \neq 0$. Let $\mathcal{R}$ be the ring $\mathbb{Z}[a_0, \ldots, a_n]$. Cantor finds polynomials $\psi_n(x, y) \in \mathcal{R}[x, y]$ such that the following characterization of torsion points holds. This is a generalization of the characterization in Proposition 2 for elliptic curves.

Proposition 8. Let $P \in H$ be a point on the curve and $n \geq g+1$ be an integer. Then $nP = 0$ in $J(H)$, if and only if,

1. $\psi_{n-g}(P) \neq 0$, and
2. $\psi_{n+i}(P) = 0$ for $-g+1 \leq i \leq g-1$.

Let $\mathcal{K} = \mathcal{R}[x, y]$. We will find polynomials $\delta_n(X), \epsilon_n(X) \in \mathcal{K}[X]$ (i.e. the coefficients are polynomials in $\mathcal{R}[x, y]$) such that the following theorem holds.

Theorem 6 (8.35 in [5])**.** Let $r \geq g+1$ and let (x, y) be a generic point on H. Then

$$n(x, y) = (\delta_n\Big(\frac{x - X}{4y^2}\Big), \epsilon_n\Big(\frac{x - X}{4y^2}\Big)), \tag{3.1}$$

where the RHS is a pair corresponding to the Mumford representation of the divisor $n(x, y) \in J(H)$.

Remark. We remark that $\delta_n\left(\frac{x-X}{4y^2}\right)$ is not necessarily a monic polynomial so we need to divide by the leading coefficient to obtain the Mumford representation.

Remark. The caveat 'generic point' avoids some degenerate cases where the formula does not hold. For our purposes, this limitation will not be important.

Remark. For $g = 1$ (elliptic curves) this reduces to the formula in Theorem 1.

We will prove Theorem 6 later in this section and Proposition 8 at the end of Section 3.3.

The torsion points will be shown to be characterized by the vanishing of certain coefficients of $\delta_r(X)$. These coefficients will be proved to be the division polynomials ψ_{n+i} in Proposition 8.

However, to be able to use the Cantor's division polynomials we need an efficient way to compute them. Fortunately, Cantor derived a recursion generalizing the simple recursion (2.2) for classical division polynomials. The derivation is laborious and technical but the recursion formula itself is relatively simple and easy to implement.

3.2.1 The Padé problem

The first step is to reduce the problem of finding n-torsion points to the well-known problem of finding Padé approximants.

Recall that the Taylor series is the best approximation of a function by a polynomial $P(x)$. Analogously, the Padé approximant $R(x)$ is the best approximation by rational function $R(x) = A(x)/B(x)$.

Definition 13. Let f be a function with power series expansion

$$S(x) = \sum_{i=0}^{\infty} s_i x^i,$$

and $m \leq 0, n \leq 1$ integers. The **Padé approximation** of order (m, n) is $R(x) = A(x)/B(x)$ where $A(x), B(x)$ are polynomials with $\deg A \leq m$ and $\deg B \leq n$. Further we require that the power series expansion of $R(x)$ agree with S up to order $m + n$. More explicitly,

$$\begin{array}{rcl} R(0) &=& f(0) = s_0 \\ R'(0) &=& f'(0) = s_1 \\ &\vdots& \\ R^{(m+n)}(0) &=& f^{(m+n)}(0) = s_{m+n} \end{array} \tag{3.2}$$

Let $H(x)$ be the power series expansion of $R(x)$. Then the condition (3.2) is the same as

$$S(x) - H(x) = O(x^{(m+n+1)}).$$

Then since $A(x)/B(x) = H(x)$,

$$\begin{aligned} A(x) - B(x)S(x) &= A(x) - B(x)(H(x) + O(x^{(m+n+1)})) \\ &= A(x) - B(x)H(x) + B(x)O(x^{(m+n+1)})) \\ &= B(x)O(x^{(m+n+1)})) = O(x^{(m+n+1)})). \end{aligned}$$

So condition (3.2) is equivalent to $A(x) - B(x)S(x)$ being divisible by $x^{(m+n+1)}$.

3.2.2 Reduction to the Padé problem

Let H be a hyperelliptic curve of genus g given by $Y = F(X)$. We want to compute the reduced representative of $r(x, y)$ for some integer $r \geq g + 1$ and point $(x, y) \in H$.

First we make a variable change such that the point (x, y) becomes

$$P_0 = (0, (-1)^{g+1} y).$$

The sign on y is chosen such that the division polynomials ψ_r gets positive leading coefficients.

Let z, Y' be the new variables. Set $X = x - z$, and $E(z) = F(x - z)$. Then $H' : Y'^2 = E(z)$ is a hyperelliptic curve of genus g such that $P_0 \in H'$.

Let

$$\sqrt{E(z)} = \sum_{i=0}^{\infty} s_i z^i, \tag{3.3}$$

be the formal Taylor series expansion of $\sqrt{E(z)}$ with constant term $s_0 = (-1)^{g+1} y$.

Assume for the moment that we have polynomials $A_r(z), B_r(z)$ such that,

(a) z^r divides $A_r(z) - B_r(z)\sqrt{E(z)}$

(b) $2 \deg A_r \leq r + g$ and $2 \deg B_r + 2g + 1 \leq r + g$.

We will prove that finding such A_r, B_r is an instance of the Padé problem in Proposition 10. A general solution to the Padé approximation problem is given in the next section.

The next theorem is a stepping stone towards the central formula (3.1).

Theorem 7. Let $r \geq g + 1$. Then the reduced divisor representing $r(0, s_0)$ has z-coordinates given by the zeroes of the polynomial

$$D_r(z) = -(A_r(z)^2 - B_r(z)^2 E(z))/z^r. \tag{3.4}$$

Before the proof, we need two lemmas.

Lemma 3. If $r \geq g + 1$ then $D_r(z)$ is a polynomial and $\deg D_r(z) = g$.

Proof. See [5, Lemma 7.1 pp. 129]. □

Lemma 4. The function $A_r(z) - B_r(z)Y'$ has exactly $r + g$ zeros. Further,

$$\operatorname{div}(A_r(z) - B_r(z)Y') = r[P_0] + D' - (r + g)[\infty], \tag{3.5}$$

where D' is a positive divisor of degree g such that $D' - g[\infty]$ is a reduced divisor of degree 0.

Proof. By Lemma 1(c), $\operatorname{div}(A_r(z) - B_r(z)Y')$ is semi-reduced. It only remains to show (i) $A_r(z) - B_r(z)Y'$ has exactly $r + g$ zeroes and (ii) $A_r(z) - B_r(z)Y'$ has a zero of order r at P_0.

Assume $A_r(z) - B_r(z)Y'$ has α zeroes. By Equation (2.14), $A_r(z) - B_r(z)Y'$ and $A_r(z) + B_r(z)Y'$ has the same number of zeroes. Then

$$A_r(z)^2 - B_r(z)^2 Y'^2 = (A_r(z) - B_r(z)Y')(A_r(z) + B_r(z)Y')$$

has exactly 2α zeroes. But

$$A_r(z)^2 - B_r(z)^2 Y'^2 = A_r(z)^2 - B_r(z)^2 E(z) = -z^r D_r(z)$$

is a polynomial in z of degree $r + g$ by Lemma 3. For every zero z_0 of the polynomial either (i) $E(z_0) \neq 0$ and we have two zeroes $(z_0, \pm\sqrt{E(z_0)})$ on H', or (ii) $E(z_0) = 0$ in which case $(z_0, 0)$ is a double root on H'. Therefore the number of zeroes of $A_r(z)^2 - B_r(z)^2 Y'^2$ is $2(r + g)$. Hence $\alpha = r + g$.

Moreover, condition (a) implies that $A_r(z) - B_r(z)Y'$ has a zero of at least order r at P_0. This proves (3.5). □

Proof of Theorem 7. Consider $A_r(z) - B_r(z)Y'$ as an element in the function field of H'.

Note that $\operatorname{div}(A_r(z) - B_r(z)Y') \sim 0$. Then rewriting (3.5) using the notation $(0, s_0) = i(0, s_0) = [(0, s_0)] - [\infty]$ gives

$$D' + r[P_0] - (r + g)[\infty] = D' - g[\infty] + r(0, s_0) \sim 0$$

Therefore,

$$D' - g[\infty] \sim -r(0, s_0).$$

So $D' - g[\infty]$ is the reduced divisor representing $-r(0, s_0)$.

Furthermore, since $-D \sim w(D)$ for any divisor D,

$$r(0, s_0) = -(-r(0, s_0)) \sim w(-r(0, s_0)) \sim w(D' - g[\infty]) = w(D') - g[\infty]. \quad (3.6)$$

Hence the reduced divisor representing $r(0, s_0)$ is $w(D') - h[\infty]$.

By definition of the w-map, D' and $w(D')$ have the same z-coordinates. Therefore, to prove the theorem it is enough to show the z-coordinates of D' are the zeroes of $D_r(z)$.

Now by definition, D' is given by the zeroes of $A_r(z) - B_r(z)Y'$ except the order r zero at P_0.

On the other hand, by Lemma 1(c),

$$\operatorname{div}(A_r(z) + B_r(z)Y') = w(D) - (r + h)[\infty] = -r(0, s_0) + w(D') - h[\infty]. \quad (3.7)$$

Hence $w(D')$ is given by the zeroes of $A_r(z) + B_r(z)Y'$ except the order r zero at P_0. Thus the g (with multiplicity) z-coordinates of D' are among the zeroes of

$$\begin{aligned} D_r(z) &= -(A_r(z) - B_r(z)\sqrt{E(z)})(A_r(z) + B_r(z)\sqrt{E(z)})/z^r \\ &= -(A_r(z)^2 - B_r(z)^2 E(z))/z^r. \end{aligned}$$

But by Lemma 3, $\deg D_r(z) = g$ so the zeroes are exactly the z-coordinates in D'.

□

After a 'normalization', $D_r(z)$ will become the δ_r in (3.1). Finding r-torsion points will then amount to finding which $P = (x, y)$ makes certain coefficients in $\delta_r(X)$ vanish.

3.2.3 General solution to the Padé problem

Fist we give the classical solution to the Padé approximant problem in terms of determinants and then we prove that the conditions $(a), (b)$ on A_r, B_r is an instance of the Padé problem.

Let $S(z) = \sum_{j=0}^{\infty} s_j z^j$ be a formal power series and consider the $n \times n$-matrix,

$$H_{m,n} = \begin{pmatrix} s_{m-n+1} & s_{m-n+2} & \cdots & s_m \\ s_{m-n+2} & s_{m-n+3} & \cdots & s_{m+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m-1} & s_m & \cdots & s_{m+n-2} \\ s_m & s_{m+1} & \cdots & s_{m+n-1} \end{pmatrix}. \quad (3.8)$$

Let $h_{m,n} = \det H_{m,n}$ for $m \geq 0, n \geq 1$. For $n = 0$ let $h_{m,n} = 1$ and for $n \leq -1$ let $h_{m,n} = 0$.

Further let $S_j = \sum_i^j s_i z^i$, and consider the $(n + 1) \times (n + 1)$-matrix

$$U_{m,n}(z) = \begin{pmatrix} s_{m-n+1} & s_{m-n+2} & \cdots & s_{m+1} \\ s_{m-n+2} & s_{m-n+3} & \cdots & s_{m+2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m-1} & s_m & \cdots & s_{m+n-1} \\ s_m & s_{m+1} & \cdots & s_{m+n} \\ z^n S_{m-n} & z^{n-1} S_{m-n+1} & \cdots & S_m \end{pmatrix}. \tag{3.9}$$

Define $u_{m,n}(z) = \det U_{m,n}(z)$. Note that $u_{m,n}$ is a polynomial in z with degree less than m. Next let

$$V_{m,n} = \begin{pmatrix} s_{m-n+1} & s_{m-n+2} & \cdots & s_{m+1} \\ s_{m-n+2} & s_{m-n+3} & \cdots & s_{m+2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m-1} & s_m & \cdots & s_{m+n-1} \\ s_m & s_{m+1} & \cdots & s_{m+n} \\ z^n & z^{n-1} & \cdots & 1 \end{pmatrix}. \tag{3.10}$$

And let $v_{m,n}(z) = \det V_{m,n}(z)$. Then $v_{m,n}$ is a polynomial in z with degree less than n.

For $w_{m,n} = u_{m,n} - v_{m,n}S(z)$ we have,

$$w_{m,n} = -\sum_{j=0}^{\infty} z^{m+n+j+1} \det \begin{pmatrix} s_{m-n+1} & s_{m-n+2} & \cdots & s_{m+1} \\ s_{m-n+2} & s_{m-n+3} & \cdots & s_{m+2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m-1} & s_m & \cdots & s_{m+n-1} \\ s_m & s_{m+1} & \cdots & s_{m+n} \\ s_{m+1+j} & s_{m+2+j} & \cdots & s_{m+n+1+j} \end{pmatrix}. \tag{3.11}$$

Proposition 9. The coefficient of z^m in $u_{m,n}(z)$ is $(-1)^n h_{m,n+1}$. The coefficient of z^n in $v_{m,n}(z)$ is $(-1)^n h_{m+1,n}$.

Proof. The coefficient in z^m in $z^{n-j}S_{m-n}$ is s_{m-n+j}. So the coefficient of z^m in $u_{m,n}(z)$ is

$$\begin{aligned} \begin{vmatrix} s_{m-n+1} & s_{m-n+2} & \cdots & s_{m+1} \\ s_{m-n+2} & s_{m-n+3} & \cdots & s_{m+2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m-1} & s_m & \cdots & s_{m+n-1} \\ s_m & s_{m+1} & \cdots & s_{m+n} \\ s_{m-n} & s_{m-n+1} & \cdots & s_m \end{vmatrix} &= (-1)^n \begin{vmatrix} s_{m-n} & s_{m-n+1} & \cdots & s_m \\ s_{m-n+1} & s_{m-n+2} & \cdots & s_{m+1} \\ s_{m-n+2} & s_{m-n+3} & \cdots & s_{m+2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m-1} & s_m & \cdots & s_{m+n-1} \\ s_m & s_{m+1} & \cdots & s_{m+n} \end{vmatrix} \\ &= (-1)^n h_{m,n+1}. \end{aligned}$$

Now consider (3.10). By the cofactor expansion of the last row, the terms containing z^n are

$$C_{1,n+1} = (-1)^{n+2} M_{1,n+1} = (-1)^n \begin{vmatrix} s_{m-n+2} & \cdots & s_{m+1} \\ s_{m-n+3} & \cdots & s_{m+2} \\ \vdots & \ddots & \vdots \\ s_m & \cdots & s_{m+n-1} \\ s_{m+1} & \cdots & s_{m+n} \end{vmatrix} = (-1)^n h_{m+1,n}$$

□

The following classical theorem by Jacobi solves the Padé problem [1].

Theorem 8. The Padé approximant of order (m,n) is equal to $(u_{m,n}(z), v_{m,n}(z))$ up to a constant.

The A_r, B_r are given as certain Padé approximations of $\sqrt{E(z)}$. Let

$$m_r = \left\lfloor \frac{r+g}{2} \right\rfloor, n_r = \left\lfloor \frac{r-g-1}{2} \right\rfloor, \tag{3.12}$$

Proposition 10. Finding polynomials A_r, B_r such that $(a), (b)$ are satisfied are an instance of the Padé approximation problem.

Proof. The claim is that A_r, B_r is the Padé approximant of order (m_r, n_r) to $\sqrt{E(z)}$.

First note that $2 \deg A_r \leq r+g$ is equivalent to $\deg A_r \leq \lfloor \frac{r+g}{2} \rfloor = m_r$ and similarly $2 \deg B + 2g + 1 \leq r + g$ is equivalent to $\deg B \leq n_r$.

If $r+g$ is even then $r - 2g = r + g - 2g$ is also even. Then

$$m_r + n_r = \frac{r+g}{2} + \frac{r-g-2}{2} = r - 1.$$

On the other hand if $r+g$ is odd then

$$m_r = \frac{r+g-1}{2}, n_r = \frac{r-g-1}{2},$$

so $m_r + n_r = r - 1$.

Then (a) states, $z^r = z^{m_r+n_r+1}$ divides $A_r(x) - B_r(x)\sqrt{E(z)}$. But this is equivalent to condition (3.2) in the definition of Padé approximant. □

3.2.4 Formulas for A_r, B_r

Now we get formulas for A_r, B_r in terms of the determinants defined above.

Let

$$A_r(z) = \begin{cases} -z^r & \text{if } 0 \leq r \leq g \\ u_{m_r,n_r} & \text{if } g+1 \leq r \end{cases} \tag{3.13}$$

$$B_r(z) = \begin{cases} 0 & \text{if } 0 \leq r \leq g \\ v_{m_r,n_r} & \text{if } g+1 \leq r \end{cases} \tag{3.14}$$

$$C_r(z) = \begin{cases} 1 & \text{if } 0 \leq r \leq g \\ -w_{m_r,n_r}/z^r & \text{if } g+1 \leq r \end{cases} \tag{3.15}$$

$$f_r = \begin{cases} 0 & \text{if } -1 \leq r \leq g-1 \\ h_{m_{r+1},n_{r+1}} & \text{if } g \leq r \end{cases} \tag{3.16}$$

From Theorem 8 and Proposition 10 the above formulas for $A_r(z), B_r(z)$ satisfies the conditions (a), (b).

The $C_r(z)$ is an error term representing how far $R(z) = A_r(z)/B_r(z)$ is from approximating $\sqrt{E(z)}$. Moreover, f_r is an expression (not necessarily a polynomial) which becomes the division polynomial $\psi_r(x, y)$ after a normalization and switching back to x, y-coordinates.

From Proposition 9 this essential proposition follows.

Proposition 11. The leading coefficient of $D_r(z)$ is $-f_r^2$ if $r + g$ is even and $-a_{2g+1}f_r^2$ if $r + g$ is odd.

Proof. For $r \leq g$ it follows trivially from the definition, so assume $r \geq g + 1$.

Recall that

$$D_r(z) = -(A_r(z)^2 - B_r(z)^2 E(z))/z^r \tag{3.17}$$

is a polynomial of degree g. Let d_g be the coefficient of z^g.

Also, $A_r(z), B_r(z)$ are polynomials of degree m_r and n_r. Let a_{m_r} and b_{n_r} denote the leading coefficients of A_r, B_r.

If $r+g$ is even then $\deg A_r = m_r = (r+g)/2$ and $\deg B_r = n_r = (r-g-2)/2$. Since $\deg E_r = 2g + 1$, the term $B_r(z)^2 E(z)$ has degree

$$(r - g - 2) + 2g + 1 = r + g - 1 < r + g$$

so $B_r(z)^2 E(z)$ can not contribute to the leading coefficient of D_r. But $\deg A_r(z)^2 = r + g$, so $d_g = -a_{m_r}^2$. By Proposition 9, $a_{m_r} = h_{m_r,n_r+1}$.

But since $r + g$ is even, $m_{r+1} = m_r$ and $n_{r+1} = n_r + 1$. Then

$$h_{m_r,n_r+1}^2 = h_{m_{r+1},n_{r+1}}^2 = f_r^2.$$

Thus $d_g = -f_r^2$.

On the other hand if $r+g$ is odd then $m_r = (r+g-1)/2, n_r = (r-g-1)/2$. Then

$$\deg A_r(z)^2 = r + g - 1 < r + g$$

but

$$\deg B_r(z)^2 E(z) = r - g - 1 + 2g + 1 = r + g.$$

Since $E(z)$ has leading coefficient $-a_{2g+1}$, Equation (3.17) yields $d_g = -a_{2g+1}b_{n_r}^2$. By Proposition 9 again, $b_{n_r}^2 = h_{m_r+1,n_r}^2$. Because $r + g$ is odd $m_{r+1} = m_r + 1$ and $n_{r+1} = n_r$. Then

$$h_{m_r+1,n_r}^2 = h_{m_{r+1},n_{r+1}}^2 = f_r^2.$$

Thus $d_g = -a_{2g+1}f_r^2$. □

3.2.5 Normalization

A priori f_j is not a polynomial since we need square roots in the Taylor series (3.3). We need to multiply by a normalizing factor to finally get the division polynomials.

Example 4. Consider the curve $C\colon y^2 = x^5+1$. Then f_5 contains roots $\sqrt{x^5+1}$. Factorizing f_5 yields,

$$f_5 = \frac{5\left(x^{10} - 108\,x^5 + 16\right)\left(x^5 - 4\right)x}{128\,(x^5+1)^{\frac{7}{2}}}$$

which still isn't a polynomial, but the square roots disappeared since $g = 2$ is even.

We need to multiply f_r by a factor $(2y)^{v_r}$ (v_r defined below) to get a polynomial.

Example 5. Let's try (rabbit out of hat) to multiply last example with $(2y)^9$. Then using the curve's equation,

$$\begin{aligned}\psi_5 &= (2y)^9 f_5 = 2^9(x^5+1)^{9/2} f_5\\ &= 20\left(x^{10} - 108\,x^5 + 16\right)\left(x^5 - 4\right)\left(x^4 - x^3 + x^2 - x + 1\right)(x+1)x.\end{aligned}$$

Furthermore,

$$\psi_5/(2y)^2 = 5\left(x^{10} - 108\,x^5 + 16\right)\left(x^5 - 4\right)x.$$

This is analogous with elliptic curve division polynomials being divisible by $2y$ if r is odd and this will allow us to generalize the univariate division polynomials in (2.4).

Before continuing we need notation for truncating polynomials and formal power series.

Definition 14. Let

$$f(z) = \sum_{i=0}^{n} a_i x^i$$

be a formal power series with $n \leq \infty$ and $r \geq 0$ be an integer. Then denote the truncated formal power series of degree r with

$$f(z)\{1_r\} = \sum_{i=0}^{r} a_i x^i. \tag{3.18}$$

Similarly let $f(z)[1_r]$ denote the sequence

$$a_0, a_1, \ldots, a_r.$$

Remark. Note that Cantor's definition allows us to 'splice' the polynomial. That is, select coefficients from a given index set. The notation here is chosen to be consistent with [5].

Now we can define the **normalized division polynomials**.

Let

$$v_r = \binom{r}{2} - \binom{g}{2} = (r^2 - r - g^2 + g)/2,$$

and define,

$$
\begin{aligned}
\psi_r &= (2y)^{v_r} f_r, && (3.19)\\
\alpha_r(z) &= 2(2y)^{v_{r-1}-1} A_r(4y^2 z)\{1_g\}, && (3.20)\\
\beta_r(z) &= (2y)^{v_{r-1}} B_r(4y^2 z)\{1_g\}, && (3.21)\\
\gamma_r(z) &= (2y)^{v_{r+1}} C_r(4y^2 z)\{1_g\}, && (3.22)\\
\delta_r(z) &= (2y)^{2v_r} D_r(4y^2 z). && (3.23)
\end{aligned}
$$

Let $\mathcal{R}$ be the ring $\mathbb{Z}[a_0, \ldots a_n]$ where a_i are the coefficients in the curve's equation. Then, the following analogue of the elliptic curve case holds.

Theorem 9 (Theorem 8.15 in [5])**.** *If $n - g$ is even then $\psi_n \in \mathcal{R}[x]$. Further, if $n - g$ is odd then $\psi_n \in (2y)^g \mathcal{R}[x]$.*

Moreover, Proposition 11 carries over to the normalized division polynomials.

Proposition 12. *Let $r \geq g + 1$. Then the leading coefficient of $\delta_r(z)$ is $-(4y^2)^g \psi_r^2$ if $r + g$ is even and $-a_{2g+1}(4y^2)^g \psi_r^2$ if $r + g$ is odd.*

Proof. If $r + g$ is even then the leading coefficient of $\delta_r(z) = (2y)^{2v_r} D_r(4y^2 z)$ is, by Proposition 11,

$$-f_r^2 (4y^2)^g (2y)^{2v_r} = -(f_r (2y)^{v_r})^2 (4y^2)^g = -\psi_r^2 (4y^2)^g.$$

The case when $r + g$ is odd follows similarly. □

Next we state a formula (without proof) that allows us to compute ϵ_r from the previously defined normalized division polynomials.

Proposition 13 (Equation (8.15) in [5])**.** *When $r \geq g + 1$,*

$$\epsilon_r(z) = \frac{yz(\psi_{r-1}^2 \delta_{r+1}(z) - \psi_{r+1}^2 \delta_{r-1}(z))}{\psi_{r-1}\psi_r^2\psi_{r+1}} (\text{mod } \delta_r(z)). \qquad (3.24)$$

3.2.6 Recursion

Similar to the elliptic curve case $g = 1$, the ψ_r can be recursively computed.

For $g = 2$ and $s \geq r$, it holds [5, Equation (1.8)],

$$\psi_s\psi_r\psi_{s+r}\psi_{s-r} = \begin{vmatrix} \psi_{s-2} & \psi_{s-1}\psi_{r+} & \psi_s\psi_{r+2} \\ \psi_{s-1}\psi_{r-1} & \psi_r\psi_s & \psi_{s+1}\psi_{r+1} \\ \psi_s\psi_{r-2} & \psi_{s+1}\psi_{r-1} & \psi_{s+2}\psi_r \end{vmatrix} \qquad (3.25)$$

If $g > 2$ the recursion formula becomes more complicated.

We define a $(g+1) \times (g+1)$ matrix below. The last column is written on block matrix notation so the sequence $\gamma_{r-g+1}\gamma_{s+1}[1_{g-2}]$ should be expanded to $g - 2$ entries.

$$\mathscr{B}_{r,s} = \begin{pmatrix} \psi_{r-g}\psi_s & \psi_{r-g+1}\psi_{s+1} & \gamma_{r-g+1}\gamma_{s+1}[1_{g-2}] \\ \psi_{r-g+1}\psi_{s-1} & \psi_{r-g+2}\psi_s & \gamma_{r-g+2}\gamma_s[1_{g-2}] \\ \vdots & \vdots & \vdots \\ \psi_r\psi_{s-g} & \psi_{r+1}\psi_{s-g+1} & \gamma_{r+1}\gamma_{s-g+1}[1_{g-2}] \end{pmatrix} \qquad (3.26)$$

Then the following formula [5, Equation (8.26)] holds for $2g-1 \leq r \leq s$,

$$\det \mathscr{B}_{s,r} = \psi_{s-r}\psi_{s+r} \prod_{k=2}^{g} (\psi_{r-g+k}\psi_{s-g+k}). \tag{3.27}$$

Note that this formula expresses ψ_{r+s} in previous ψ_i, so we can use it to recursively compute ψ_n.

Since $\psi_r = 0$ for $r < g$ the left hand side is 0 if $s - r < g$. So we assume $s - r \geq g$. Then $s \geq 3g - 1$ and hence $r + s \geq 5g - 2$. So for $n \geq 5g - 2$ we can write $n = s + r$ and use (3.27) to compute ψ_n recursively.

Algorithm 5. The following algorithm computes the division polynomial ψ_n for $n \geq 0$.

1. If $n < 5g - 2$ then compute ψ_n from the determinant definition (3.16).
2. Otherwise, if $n - g$ is even let
$$r = \left\lfloor \frac{n-g}{2} \right\rfloor, s = \left\lfloor \frac{n+g}{2} \right\rfloor,$$
and if $r - g$ is odd, let
$$r = \left\lfloor \frac{n-g}{2} \right\rfloor, s = \left\lfloor \frac{n+g}{2} \right\rfloor + 1.$$
3. Then compute ψ_n recursively for $n = r + s$ using (3.27).

Proof. Let $n \geq 5g - 2$. Then

$$r \geq \left\lfloor \frac{5g-2-g}{2} \right\rfloor = 2g - 1,$$

so the condition $2g - 1 \leq r \leq s$ holds.

It remains to show $r+s = n$ in both cases. If $n-g$ is even, so is $n-g+2g = n+g$. Then

$$r + s = (n-g)/2 + (n+g)/2 = n.$$

On the other hand if both are odd then

$$r + s = (n-g-1)/2 + (n+g-1)/2 + 1 = n.$$

□

3.3 Torsion algorithm

We define the **univariate division polynomials** analogously to the elliptic curve case:

$$P_n = \begin{cases} \psi_n & n-g \text{ even} \\ \psi_n/(2y)^g & n-g \text{ odd.} \end{cases} \tag{3.28}$$

Then similar to Proposition 8.

Proposition 14. Let H be a hyperelliptic curve and let $P = (x, y) \in H$. Assuming that $\text{ord}(P) \neq 2$, then $n(x, y) = 0$ in $J(H)$ iff for all

$$n - g + 1 \leq i \leq n + g - 1$$

we have $P_i(x) = 0$.

Proof. We show that this follows from Proposition 8. Note that the only zeroes of ψ_n we lose going to P_n are the zeroes of $(2y)^g$, i.e. points with y-coordinate 0. Moreover a point $P = (x, y)$ has y-coordinate 0 iff $\text{ord}(P) = 2$. □

Fix a finite field $\mathbb{F}_q$ with characteristic $p \neq 2$ and let H be a curve defined over $\mathbb{F}_q$. The latter assumption means $a_i \in \mathbb{F}_q$. Then let $\overline{P_n}$ be the result of reducing the coefficients of P_n modulo p. More precisely, if

$$P_n = p_0 + p_1 x + \cdots + p_k x^k,$$

with $p_i \in \mathbb{Z}$, then

$$\overline{P_n} = \overline{p_0} + \overline{p_1} x + \cdots + \overline{p_k} x^k,$$

where $\overline{p_i} \equiv p_i (\text{mod p})$. Thus while $P_n \in \mathcal{R}[x]$ we have in contrast $\overline{P_n} \in \mathbb{F}_q[x]$.

The key proposition is the following.

Proposition 15. Let H be an hyperelliptic curve and let $P = (x, y) \in H$ with $x, y \in \mathbb{F}_q$. Assuming that $\text{ord}(P) \neq 2$, then $n(x, y) = 0$ in $J(H)(\mathbb{F}_q)$ iff $\overline{P_i}(x) = 0$ for $n - g + 1 \leq i \leq n + g - 1$.

Proof. The construction of the Cantor division polynomials P_n goes through working in $\mathbb{F}_q$ instead of $\mathcal{R}$. □

Now we can state the aforementioned algorithm.

Algorithm 6. Let H be an hyperelliptic curve given by a Weierstrass equation $y^2 = \sum_{i=1}^{2g+1} a_i x^i$ where $a_i \in \mathbb{F}_q$ and let $n \geq g + 1$ be an integer. Then the following algorithm computes $H[n](\mathbb{F}_q)$, i.e. the n-torsion points.

1. If n is even, record the points with order 2.
2. Compute the $2g - 1$ polynomials $P_{n-g+1}, P_{n-g+2}, \ldots P_{n+g-1}$ using the recursion.
3. Reduce the coefficients of P_i modulo p to get $\overline{P_i}$ for $n-g+1 \leq i \leq n+g-1$.
4. Let $g(x) = \gcd(\overline{P_{n-g+1}}, \overline{P_{n-g+2}}, \ldots, \overline{P_{n+g-1}})$.
5. Factor $g(x)$ into irreducible factors over $\mathbb{F}_q$.
6. For each linear irreducible factor $x - \alpha$ in $g(x)$:
   (a) Find the y-values β such that $(\alpha, \beta) \in H(\mathbb{F}_q)$.
   (b) Record (α, β) as a n-torsion point.

The correctness of the algorithm follows from Proposition 14. We will now prove Proposition 8.

Lemma 5. Let $r > g$ and assume we have $f_r \neq 0$, $f_{r+i} = 0$ for $i = 1, 2, \ldots 2h-1$. Then (i) $h \leq g$ and (ii) $z^h | C_r$.

Proof. See [5] Lemma 3.29. □

Let Θ denote the set of divisors with reduced representative D with $\deg_0(D) < g$, i.e. the finite part of D contain less that g points with multiplicity.

Lemma 6. Let $P = (x, y)$ with $y \neq 0$. Then $\psi_n(x, y) = 0 \iff n(x, y) \in \Theta$.

Proof. Let $(U(X), V(X))$ be the Mumford representation of D. Then since $U(x) = 0$ iff the point (x, y) or $(x, -y)$ appear in D, $\deg_0(D) < g$ is equivalent to $\deg U(X) < g$. By Theorem 6, $U(X) = \delta_r$. But the leading coefficient of δ_r is either $-\psi_n^2(4y^2)^g$ or $-a_{2g+1}\psi_n^2(4y^2)^g$ by Proposition 12. This completes the proof. □

Lemma 7. Let h be an integer and let $P = (x, y) \in H$ with $y \neq 0$. Assume $\psi_r(x, y) \neq 0$, $\psi_{r+i}(x, y) = 0$ for $1 \leq i \leq 2h - 1$ and $\psi_{r+2h}(x, y) \neq 0$. Then

$$rP \sim h(x, -y) + D - (g - h)[\infty],$$

where D is a divisor with positive coefficients and exactly $g - h$ finite points (with multiplicity) and no infinite points.

Proof. Let E be the reduced representative of nP (i.e. the unique reduced divisor E such that $nP \sim E$). By Lemma 5, $h \leq g$ and $z^h | C_r(z)$. Since $\psi_n(x, y) \neq 0$ by assumption, $nP \notin \Theta$ by Lemma 6. Therefore, by definition, E contains exactly g finite points.

Since

$$C_r(z) = (A_r - B_r\sqrt{E(z)})/z^r$$

and $z^h | C_r$ we have that $A_r(z) - B_r(z)\sqrt{E(z)}$ is divisible by z^{r+h}. Since the formal series $\sqrt{E(z)}$ is taken so that the constant coefficient is $(-1)^{g+1}y$, we have

$$P_0 = (0, (-1)^{g+1}y)$$

as a zero of $A_r(z) - B_r(z)Y'$ with order $r + h$. Furthermore recall that the number of zeroes of $A_r(z) - B_r(z)Y'$ is r+g. Hence

$$0 \sim \operatorname{div}(A_r(z) - B_r(z)Y') \sim (r + h)[P_0] + D - (r + g)[\infty], \tag{3.29}$$

where D is a positive divisor with $g - h$ finite points. Then

$$r(x, y) \sim -h(x, y) + D - (g - h)[\infty] \sim h(x, -y) + D - (g - h)[\infty], \tag{3.30}$$

since $-h(x, y) \sim h(x, -y)$. □

Finally, we are ready to prove Proposition 8.

Proof of Proposition 8. Let $\psi_{n-g} \neq 0$ and $\psi_{n+i} = 0$ for $-g+1 \leq i \leq g-1$ then $\psi_{n+g} \neq 0$ by Lemma 5. Next by Lemma 7 with $g = h$ we have

$$(n - g)P \sim g[w(P)] - g[\infty]. \tag{3.31}$$

Adding $gP = n[P] - g[\infty]$ to both sides gives,

$$nP \sim g[w(P)] + g[P] - 2g[\infty] \sim 0, \tag{3.32}$$

since $g[P] + g[w(P)] - 2g[\infty] = \operatorname{div}(X - x)$ is principal.

Conversely, assume $nP = 0$ in $J(H)$. Then

$$(n-g)P \sim -gP = -g[P] + g[\infty] \sim g[w(P)] - g[\infty], \tag{3.33}$$

where the last relation comes from adding $g[P] + g[w(P)] - 2g[\infty] \sim 0$.

Note that the right hand side of (3.33) is a reduced divisor with $\deg_0 = g$. So since the reduced representative is unique, $(n-g)P \notin \Theta$. Hence $\psi_{n-g} \neq 0$. Furthermore, adding jP, where $1 \leq j \leq 2g-1$, to both sides in (3.33) gives

$$(n-g+j)P \sim g[w(P)] - g[\infty] + j[P] - j[\infty]. \tag{3.34}$$

If $j \geq g$ then

$$(n-g+j)P \sim (j-g)[P] - (j-g)[\infty]. \tag{3.35}$$

Since $j - g < 2g - g < g$, $(n-g+j)P \in \Theta$.

When $j < g$,

$$(n-g+j)P \sim (g-j)[P] - (g-j)[\infty], \tag{3.36}$$

and so $(n-g+j) \in \Theta$. This proves $\psi_{n+i} = 0$ for all $-g+1 \leq i \leq g-1$. □

3.4 Naive division point algorithm

Algorithm 6 gives an efficient way to solve the torsion problem (Problem 1). We next attempt the division point problem (Problem 2). First we give a naive algorithm based on an exhaustive enumeration.

Recall that by Theorem 4 the Mumford pair (U, V) is defined over $\mathbb{F}_q$ iff $U(X), V(X) \in \mathbb{F}_q[X]$. Since there are only a finite number of polynomials in $\mathbb{F}_q[X]$, the theorem gives us a way to enumerate all divisor classes in $J(H)(\mathbb{F}_q)$.

Algorithm 7. Let H be a hyperelliptic curve defined over $\mathbb{F}_q$ with genus g. The following algorithm finds all n-division points $J(H)[n](\mathbb{F}_q)$.

1. Enumerate all Mumford pairs (U, V) with $U, V \in \mathbb{F}_q$.
2. For each Mumford pair (U,V):
   (a) Compute $n(U, V)$ using Cantor's algorithm (Algorithm 3).
   (b) If $n(U, V) = 0$ in $J(H)$ then record (U, V).

Proof. By Theorem 4 looping over the polynomials (U, V) such that $U, V \in \mathbb{F}_q[X]$ gives all divisors $[D] \in J(H)(\mathbb{F}_q)$. Since we simply check if $nD = 0$ this gives the kernel.

For time complexity the essential part is how we implement Step 1. □

The naive way to implement Step 1 is to loop over all pairs X, Y (not necessarily Mumford) and check if (X, Y) is a valid Mumford pair. Choosing this implementation, the conditions in Corollary 1 implies that Step 1 is given by:

1. For all polynomial $U, V \in \mathbb{F}_q[X]$ with $\deg U \leq g$ and $\deg V < \deg U$,
    (a) If $U \mid f - V^2$ then record (U, V) as a Mumford pair.
    (b) Otherwise, continue.

Since we have q choices for each coefficient, the number of possible U is $\mathcal{O}(q^{g+1})$. Since $\deg V < \deg U$, for a given U, the number of possible V is $\mathcal{O}(q^g)$. So the above implementation has a time complexity of $\mathcal{O}(q^{2g+1})$.

In the next section we will derive a faster algorithm for finding valid Mumford pairs (U, V) given a fixed U. However, even with this implementation we still need to enumerate all U in Step 1. This means that Algorithm 7 is $\mathcal{O}(q^{g+1})$.

3.4.1 Finding V from U

Given a polynomial $U(X) \in \mathbb{F}_q[X]$ we seek the polynomials $V(X) \in \mathbb{F}_q[X]$ such that $(U(X), V(X))$ is a Mumford pair. This is an essential step in the naive algorithm. Furthermore, in the next section we will present a more sophisticated algorithm, based on Cantor's division polynomials, that gives a candidate list of U-values (without corresponding V values).

Consider the general case $g \geq 1$ for the moment. Let

$$U(X) = \prod_{i=1}^{k} (X - \alpha_i)^{c_i}, \tag{3.37}$$

where $k \leq g$ and $c_i \geq 1$. Suppose that (U, V) is a Mumford pair. Then the pair (U, V) represents the divisor $\sum_{i=1}^{k} c_i([(\alpha_i, \beta_i)] - [\infty])$, where $\beta_i = V(\alpha_i)$. In other words, U determines the x-coordinates and V determines the y-coordinates.

Now consider a fixed U. Then by Theorem 3 there is a 1-1 correspondence between polynomials V corresponding to U and reduced divisors of the form

$$D = \sum_{i=1} c_i([(\alpha_i, y_i)] - [\infty]) \tag{3.38}$$

where y_i are such that $(\alpha_i, y_i) \in H$. It is easy to enumerate the divisors D with x-coordinates α_i. Indeed since we must have $y_i = \pm\sqrt{f(\alpha_i)}$, we only need to chose a sign for each y_i.

It remains to give an algorithm to compute the inverse to the bijection in Theorem 3. That is, for a given reduced D find the corresponding pair (U, V). The algorithm is based on the proof of Theorem 13.5 in [19].

Equation (3.37) uniquely determines U from the x-values α_i. Next we need to construct a corresponding V such that (i) $\deg V < \deg U$ and (ii) $f - V^2 \equiv 0 \pmod{U}$.

Assume that we have a sequence of polynomials $V_i(X)$ such that

(i) $V_i(\alpha_i) = \beta_i$, and

(ii) $V_i^2 \equiv f \pmod{(x - \alpha_i)^{c_i}}$.

Consider the system of congruences

$$V \equiv V_i \pmod{(X-\alpha_i)^{c_i}} \tag{3.39}$$

for $1 \leq i \leq k$. Then since the polynomials $(X-\alpha_i)^{c_i}$ are mutually relatively prime for $1 \leq i \leq k$, the Chinese Remainder Theorem tells us that there exists and unique solution V modulo $(X-\alpha_1)^{c_1}\dots(X-\alpha_k)^{c_k} = U$. Then since the solution is defined modulo U, we have $\deg V < \deg U$. Furthermore

$$V \equiv V_i \pmod{(X-\alpha_i)^{c_i}}, \tag{3.40}$$

implies that,

1. $V(\alpha_i) = \beta_i$, and,
2. $f - V^2 \equiv f - V_i^2 \equiv 0 \pmod{(X-\alpha_i)}$.

Then (2) with (ii) implies that for $1 \leq i \leq k$,

$$f - V^2 \equiv 0 \pmod{(x-\alpha_i)^{c_i}}. \tag{3.41}$$

Thus $f - V^2 \equiv 0 \pmod{U}$. Hence (U,V) is the Mumford pair representing D.

It remains to show how to construct the sequence $\{V_i\}$ such that (i), (ii) holds.

To simplify notation, let $W = V_i$, $\alpha = \alpha_i$, $\beta = \beta_i$ and $c = c_i$. If $\beta = 0$ then by the assumption that D is reduced, we must have $c = 1$. Let $W(X) = 0$, then since $W^2(\alpha) = f(\alpha) = 0$, we have $f - W^2 \equiv f - 0 \equiv f \equiv 0 \pmod{(X-\alpha)}$.

Assume that $\beta \neq 0$. We will inductively construct $W(X)$. For $1 \leq j \leq c$, we will construct $W_j(X)$ such that $f - W_j^2 \equiv 0 \pmod{(x-\alpha)^j}$. Then clearly $W = W_c$.

Definition 15. Define sequences $\{W_j\}_{j=1}^c, \{k_j\}_{j=2}^c$, and $\{P_j\}_{j=2}^c$ inductively by

$$W_1(X) = \beta, \tag{3.42}$$

$$W_{j+1}(X) = W_j(X) + k_{j+1}(X-\alpha)^j, \text{ for } 1 \leq j < c, \tag{3.43}$$

where

$$P_{j+1}(X) = \frac{(f - W_j^2)}{(X-\alpha)^j}, \tag{3.44}$$

$$k_{j+1} = P_{j+1}(\alpha)/(2\beta). \tag{3.45}$$

Proposition 16. Then for $1 \leq j \leq c$,

$$f - W_j^2 \equiv 0 \pmod{(x-\alpha)^j}. \tag{3.46}$$

And $P_j(X)$ is a polynomial for $2 \leq j \leq c$.

Proof. Induction on j. Note that $W_1(X) = \beta$ implies $W_1^2(\alpha) = \beta^2 = f(\alpha)$ which yields $f - W_j^2 \equiv 0 \pmod{(x-\alpha)^j}$. By definition it follows that P_2 is a polynomial.

Assume the statement holds for $W_j(X)$. Then it follows from (3.46) that P_{j+1} is a polynomial. Further, $P_{j+1}(\alpha) = 2k_{j+1}\beta = 2k_{j+1}W_j(\alpha)$ implies that

$$P_{j+1}(X) - 2k_{j+1}W_j \equiv 0 \pmod{(X-\alpha)} \tag{3.47}$$

Multiplying (3.47) with $(X-\alpha)^j$ yields

$$f - W_j^2 - 2k_{j+1}W_j(X-\alpha)^j \equiv 0 \pmod{(X-\alpha)^{j+1}}. \tag{3.48}$$

But this means,

$$\begin{aligned} f - W_{j+1}^2 &\equiv f - W_j^2 - 2kW_j(X-\alpha)^j - k^2(X-\alpha)^{2j} && (3.49)\\ &\equiv f - W_j^2 - 2kW_j(X-\alpha)^j \equiv 0 \pmod{(x-\alpha)^{j+1}}. && (3.50)\end{aligned}$$

□

Algorithm 8. Let $D = \sum_{i=1}^k c_i([(\alpha_i, \beta_i)] - [\infty])$ be a reduced divisor. Then the following algorithm finds the corresponding Mumford pair (U, V).

1. Let $U(X) = \prod_{i=1}^k (X - \alpha_i)$.
2. For each $1 \leq i \leq k$, compute V_i recursively using Definition 15.
3. Solve the system of congruences (3.39) using the Chinese Remainder Theorem. Let V be the solution.

By permuting the signs of β_i, this give us a way to generate the set of valid V given a fixed U. For simplicity we will now only consider $g = 2$ and make the idea more explicitly.

Recall that $(U, V) \in J(H)(\mathbb{F}_q)$ is equivalent to $U, V \in \mathbb{F}_q[X]$. Further since $g = 2$ we have $\deg U \leq 2$. Based on the possible degrees of U we can classify U in the following categories.

A. $U(X) = 1$

B. $U(X) = X - \alpha_1$,

C. $U(X) = (X - \alpha_1)(X - \alpha_2)$ for $\alpha_1 \neq \alpha_2$,

D. $U(X) = (X - \alpha_1)^2$.

We describe an algorithm based on the above cases that takes as input a $U(X) \in \mathbb{F}_q[X]$ and output the set of V such that $(U(X), V(X))$ is a Mumford pair.

A

Since $\deg V < \deg U$, the only possibility is $V(X) = 0$. Note that $(1, 0)$ represents the neutral element.

B

Note that V must be a constant since $\deg V < \deg U = 1$. If $f(\alpha_1)$ is a square in $\mathbb{F}_q$ then let $\beta_1 = \pm\sqrt{f(\alpha_1)} \in \mathbb{F}_q$. Then we have two (or one if $\beta_1 = 0$) possibilities, either $V(X) = \beta_1$ or $V(X) = -\beta_1$. If $f(\alpha_1)$ is a non-square in $\mathbb{F}_q$ we can still get a square root $\beta_1 \in \mathbb{F}_{q^2}$, but then $D = [(\alpha_1, \beta_1)] - [\infty]$ is not defined over $\mathbb{F}_q$. Hence in this case there are no V.

C

The divisor $D = [(\alpha_1, \beta_1)] + [(\alpha_2, \beta_2)] - 2[\infty]$, for $\alpha_1 \neq \alpha_2$, is defined over $\mathbb{F}_q$ iff the $\mathrm{Frob}_q(D) = D$, where Frob is the Frobenius map. There are two cases: (i) either $\mathrm{Frob}_q([\alpha_1, \beta_1]) = (\alpha_1, \beta_1)$ and $\mathrm{Frob}_q([\alpha_2, \beta_2]) = (\alpha_2, \beta_2)$, or, (ii) $\mathrm{Frob}_q([\alpha_1, \beta_1]) = (\alpha_2, \beta_2)$ and $\mathrm{Frob}_q([\alpha_2, \beta_2]) = (\alpha_1, \beta_1)$.

Assume $U(X)$ splits over $\mathbb{F}_q$ i.e. $\alpha_1, \alpha_2 \in \mathbb{F}_q$. Recall that $x \in \mathbb{F}_q$ iff $\mathrm{Frob}_q(x) = x$. From this we see that case (i) is equivalent to $\alpha_1, \alpha_2 \in \mathbb{F}_q$. But case (i) also implies that $\mathrm{Frob}_q(\beta_1) = \beta_1$ and $\mathrm{Frob}_q(\beta_2) = \beta_2$. Hence $\beta_1, \beta_2 \in \mathbb{F}_q$. In other words, when $U(X)$ splits over $\mathbb{F}_q$ we only need to look for $\beta_j = \pm\sqrt{f(\alpha_j)} \in \mathbb{F}_q$. In this case we take $\mathbb{K} = \mathbb{F}_q$.

On the other hand if $\mathbb{F}_q$ is irreducible over $\mathbb{F}_q$ then $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}$. Then we are in case (ii) and $\beta_1, \beta_2 \in \mathbb{F}_{q^2}$ since $\mathrm{Frob}_{q^2}(\beta_j) = \mathrm{Frob}_q(\mathrm{Frob}_q(\beta_j)) = \beta_j$. Hence we only need to look for $\beta_j = \pm\sqrt{f(\alpha_j)} \in \mathbb{F}_{q^2}$. We take $\mathbb{K} = \mathbb{F}_{q^2}$.

Let $\beta_1 = \pm\sqrt{f(\alpha_1)} \in \mathbb{K}$ and $\beta_2 = \pm\sqrt{f(\alpha_2)} \in \mathbb{K}$. Here we have 2 choices of sign. For a given choice let $V_1(X) = \beta_1$ and $V_2(X) = \beta_2$. Then we need to solve the system

$$V \equiv V_1 \equiv \beta_1 \pmod{(X - \alpha_1)} \tag{3.51}$$

$$V \equiv V_2 \equiv \beta_2 \pmod{(X - \alpha_2)}. \tag{3.52}$$

Note that this is system over $\mathbb{K}[X]$ so a solution V might not lie in $\mathbb{F}_q[X]$. However, if the solution V does lie in $\mathbb{F}_q[X]$, then $(U(X), V(X))$ is Mumford pair representing a divisor defined over $\mathbb{F}_q$.

D

Let $D = [(\alpha_1, y_1)] + [(\alpha_1, y_2)] - 2[\infty]$. Then $y_2 = \pm y_1$ but since the divisor is reduced we must have $y_1 = y_2$, i.e. we can assume without loss of generality that $D = 2([(\alpha_1, \beta_1)] - 2[\infty])$. Further note we can assume that (i) $\alpha_1 \in \mathbb{F}_q$ and (ii) $\beta_1 \neq 0$ since $y_1 = 0$ implies that $D \sim 0$.

If $f(\alpha_1)$ is not a square in $\mathbb{F}_q$ there is no V. If $f(\alpha_1)$ is a square, we have one choice of sign: $\beta_1 = \pm\sqrt{f(\alpha_1)}$. Then by making Algorithm 8 explicit using Definition 15,

$$V(X) = W_2(X) = W_1(X) + k_2(X - \alpha_1) = \beta_1 + k_2(X - \alpha_1), \tag{3.53}$$

where $P_2(X) = (f - \beta_1^2)/(X - \alpha_1)$ and $k_2 = P_2(\alpha_1)/(2\beta_1)$.

Hence we get two V corresponding the choice of sign.

Algorithm 9. Let H a hyperelliptic curve of genus 2 over $\mathbb{F}_q$. Given a polynomial $U(X) \in \mathbb{F}_q[X]$ the above algorithm finds all $V(X) \in \mathbb{F}_q[X]$ such that $(U(X), V(X))$ is a Mumford pair representing a divisor $D \in J(H)(\mathbb{F}_q)$.

3.5 Cantor's division point algorithm

Since division points and torsion points coincide when $g = 1$ we assume that $g \geq 2$.

3.5.1 Necessary condition

Let $k \leq g$. We will derive a necessary condition for

$$D = (x_1, y_1) + (x_2, y_2) + \cdots + (x_k, y_k),$$

being a division point. In general this will be k equations in two unknown polynomials $a(X), b(X)$ that must be satisfiable. When $g = 2$ this will turn out to imply that two 2×2 determinants vanish. From this we can compute a candidate list of possible U. For each U we then compute all corresponding V and then use Cantor's algorithm to check if $n(U(X), V(X)) = 0$.

Note that since $[n]$ is an homomorphism,

$$nD = n\Big((x_1, y_1) + \cdots + (x_k, y_k)\Big) = \Big(n(x_1, y_1) + \cdots + n(x_k, y_k)\Big). \tag{3.54}$$

Substituting $x = x_i$ in Theorem 6, we get that $n(x_i, y_i)$ is represented by the pair

$$\Big(\delta_n^i\Big(\frac{x_i - X}{4y_i^2}\Big), \epsilon_n^i\Big(\frac{x_i - X}{4y_i^2}\Big)\Big).$$

So $nD = 0$ in $J(H)$ implies that the sum

$$\sum_{i=1}^{k}\Big(\delta_n^i\Big(\frac{x_i - X}{4y_i^2}\Big), \epsilon_n^i\Big(\frac{x_i - X}{4y_i^2}\Big)\Big) \sim 0.$$

This holds iff there is a function $f \in \bar{\mathbb{F}}_q(H)$ such that

$$\operatorname{div}(f) = \sum_{i=1}^{k}\Big(\delta_n^i\Big(\frac{x_i - X}{4y_i^2}\Big), \epsilon_n^i\Big(\frac{x_i - X}{4y_i^2}\Big)\Big). \tag{3.55}$$

By clearing denominators and using the relation $Y^2 = F(X)$ we can assume that f is on the form $f = a(X) + b(X)Y$, where $a(X), b(X)$ are polynomials.

Assume we have such $a(X), b(X)$. Then by Lemma 1(c),

$$(a(X) + b(X)Y)(a(X) - b(X)Y) = a(X)^2 - b(X)^2Y^2 = a(X)^2 - b(X)^2F(X)$$

has roots exactly the x-coordinates of (3.55). If a_i is a zero of δ_n^i then by assumption a_i is a x-coordinate in (3.55) and therefore a zero of $a(X) + b(X)Y$. Thus,

$$a(X)^2 - b(X)^2F(x) \equiv 0 \pmod{(X - a_i)}.$$

for all zeroes a_i of δ_n^i. Hence, for $1 \leq i \leq k$,

$$a(X)^2 - b(X)^2F(x) \equiv 0 \Big(\text{mod } \delta_n^i\Big(\frac{x_i - X}{4y_i^2}\Big)\Big). \tag{3.56}$$

If this system is solvable then, by the Chinese Reminder Theorem, it has an unique solution modulo

$$\delta = \operatorname*{lcm}_{1\leq i\leq k}\Big(\delta_n^i\Big(\frac{x_i - X}{4y_i^2}\Big)\Big).$$

Since $\deg \delta_n^i \leq g$, we have $\deg \delta \leq kg \leq g^2$. So we can assume without loss of generality that the solution to the system satisfies $\deg(a(X)^2 - b(X)^2F(x)) \leq g^2$. This implies that $2\deg a(X) \leq g^2$ and $2\deg b(X) \leq g^2 - 2g - 1$.

But since $(\delta_n^i, \epsilon_n^i)$ is a Mumford pair, $Y = \epsilon_n^i$ for all zeroes of δ_n^i. This proves the following proposition.

Proposition 17. For $k \leq g$ let $D = \sum_{i=1}^k (x_i, y_i)$. If $nD = 0$ in $J(H)$ then there are polynomials $a(X), b(X)$, not both identically zero, with $2\deg a(X) \leq g^2$ and $2\deg b(X) \leq g^2 - 2g - 1$ that satisfies

$$a(X) + b(X)\epsilon_n^i\Big(\frac{x_i - X}{4y_i^2}\Big) \equiv 0 \;\Big(\bmod\; \delta_n^i\Big(\frac{x_i - X}{4y_i^2}\Big)\Big) \tag{3.57}$$

for $1 \leq i \leq k$.

Now consider the special case $g = 2$. Let D be a n-divison point. Then either (i) $k = 1$, i.e. $D = (x_1, y_1)$ is a n-torsion point or (ii) $k = g = 2$. Case (i) is dealt with in Algorithm 6. We will now deal with case (ii).

The degree condition on b implies that $b(X) = 0$. Hence (3.57) implies that

$$\delta_n^i\Big(\frac{x_i - X}{4y_i^2}\Big)\Big) \mid a(X),$$

for $i = 1, 2$. Thus there are polynomials k_1, k_2 such that

$$a(X) = \delta_n^1\Big(\frac{x_1 - X}{4y_1^2}\Big)k_1,$$
$$a(X) = \delta_n^2\Big(\frac{x_2 - X}{4y_2^2}\Big)k_2.$$

That is,

$$\delta_n^1\Big(\frac{x_1 - X}{4y_1^2}\Big)k_1 = \delta_n^2\Big(\frac{x_2 - X}{4y_2^2}\Big)k_2. \tag{3.58}$$

In other words, δ_n^1 and δ_n^2 are proportional.

By assumption,

$$(\delta_n^1, \epsilon_n^1) + (\delta_n^2, \epsilon_n^2) \sim 0. \tag{3.59}$$

Then since for any Mumford pair (U, V),

$$-(U, V) \sim w((U, V)) = (U, -V),$$

it follows, since the Mumford representation is unique,

$$(\delta_n^1, \epsilon_n^1) \sim -(\delta_n^2, \epsilon_n^2) \sim (\delta_n^2, -\epsilon_n^2). \tag{3.60}$$

This implies that ϵ_n^1 and ϵ_n^2 are proportional.

Let (Δ_n^1, E_n^1) and (Δ_n^2, E_n^2) be pairs corresponding to $(\delta_n^1, \epsilon_n^1), (\delta_n^2, \epsilon_n^2)$ such that Δ_n^1, Δ_n^2 are monic (see remark in Theorem 6). Then

$$\Delta_n^1 = X^2 + a_1 X + b_1$$

and

$$\Delta_n^2 = X^2 + a_2 X + b_2,$$

where a_i, b_i are polynomials in x_i, y_i. Let

$$f_1(x_1, x_2, y_1, y_2) = \begin{vmatrix} b_1 & b_2 \\ a_1 & a_2 \end{vmatrix} \tag{3.61}$$

The requirement that δ_n^1, δ_n^2 are proportional is then equivalent to $f_1 = 0$. Similarly let

$$E_n^1 = c_1 X + d_1,$$
$$E_n^2 = c_2 X + d_2,$$

and,

$$f_2(x_1, x_2, y_1, y_2) = \begin{vmatrix} c_1 & c_2 \\ d_1 & d_2 \end{vmatrix}. \tag{3.62}$$

Similarly the requirement that $\epsilon_n^1, \epsilon_n^2$ are proportional is equivalent to $f_2 = 0$.

Proposition 18. In summary,

$$f_1(x_1, x_2, y_1, y_2) = f_2(x_1, x_2, y_1, y_2) = 0, \tag{3.63}$$

is a necessary condition for $n((x_1, y_1) + (x_2, y_2)) \sim 0$.

We will show that the condition (3.63) can reformulated as a polynomial condition in the coefficients of U.

Proposition 19. Using the relations $y_1^2 = F(x_1)$ and $y_2^2 = F(x_2)$ we can rewrite $f_1(x_1, x_2, y_1, y_2), f_2(x_1, x_2, y_1, y_2)$ as polynomials $h_1(x_1, x_2), h_2(x_1, x_2)$ in x_1, x_2 only.

Proof. It is enough to show $f_i(x_1, x_2, -y_1, y_2) = f_i(x_1, x_2, y_1, y_2)$ and $f_i(x_1, x_2, y_1, -y_2) = f_i(x_1, x_2, y_1, y_2)$ for $i = 1, 2$

Let $D' = (x_1, -y_1) + (x_2, y_2)$. Then

$$nD' \sim \Big(\delta_n\Big(\frac{x_1 - X}{4(-y_1)^2}\Big), \epsilon_n\Big(\frac{x_1 - X}{4y_1^2}\Big)\Big) + \Big(\delta_n\Big(\frac{x_2 - X}{4y_2^2}\Big), \epsilon_n\Big(\frac{x_2 - X}{4y_2^2}\Big)\Big) \tag{3.64}$$

Let $f_1'(x_1, x_2, y_1, y_2), f_2'(x_1, x_2, y_1, y_2)$ denote the polynomials corresponding to D'. Then $f_i'(x_1, x_2, y_1, y_2) = f_i(x_1, x_2, -y_1, y_2)$.

Because $(-y_1)^2 = y_1^2$, Equation (3.64) implies that D and D' have the same corresponding Δ, E. This means $f_i = f_i'$. Hence

$$f_i(x_1, x_2, -y_1, y_2) = f_i(x_1, x_2, y_1, y_2) \tag{3.65}$$

for $i = 1, 2$.

The proof of $f_i(x_1, x_2, y_1, -y_2) = f_i(x_1, x_2, y_1, y_2)$ is exactly the same.

□

Proposition 20. The polynomials $h_1(x_1, x_2), h_2(x_1, x_2)$ are anti-symmetric.

Proof. We need to show $h_i(x_2, x_1) = -h_i(x_1, x_2)$ for $i = 1, 2$.

Let $D' = (x_2, y_2) + (x_1, y_1)$ (opposite order) and let $h'_1(x_1, x_2), h'_2(x_1, x_2)$ be the h-polynomials corresponding to D'. Then $h'_i(x_1, x_2) = h_i(x_2, x_1)$ by definition (3.62). Further since switching two rows in matrix changes the sign,

$$h_1(x_2, x_1) = h'_1(x_1, x_2) = \begin{vmatrix} c_2 & c_1 \\ d_2 & d_1 \end{vmatrix} = - \begin{vmatrix} c_1 & c_2 \\ d_1 & d_2 \end{vmatrix} = -h_1(x_1, x_2) \tag{3.66}$$

A similar argument shows, $h_2(x_2, x_1) = -h_2(x_1, x_2)$. □

Since h_1, h_2 are anti-symmetric we can divide them by the Vandemonde determinant $(x_1 - x_2)$. Let

$$g_1(x_1, x_2) = h_1(x_1, x_2)/(x_1 - x_2),$$
$$g_2(x_1, x_2) = h_2(x_1, x_2)/(x_1 - x_2).$$

Then g_1, g_2 are symmetric polynomials in x_1, x_2.

We need to deal with any solutions we lose when dividing by $x_1 - x_2$.

Proposition 21. If $D = (x_1, y_1) + (x_2, y_2)$ is an n-division point with $x_1 = x_2$ then D is a $2n$-torsion point.

Proof. The only possibilities when $x_1 = x_2$ is (i) $D = (x_1, y_1) + (x_1, y_1) = 2(x_1, y_1)$ or (ii) $D = (x_1, y_1) + (x_1, -y_1) = 0$. Clearly, we don't lose any solution in (ii). In (i) we have $D = 2(x_1, y_1)$. Hence $nD = 2n(x_1, y_1) = 0$. □

So our dichotomy splits into a trichotomy.

Proposition 22. Let D be a non-trivial n-division point. Then either

1. $D = (x_1, y_1)$ is an n-torsion point,
2. $D = 2(x_1, y_1)$ is a $2n$-torsion point, or,
3. $D = (x_1, y_1) + (x_2, y_2)$ with $x_1 \neq x_2$.

We have already found an efficient algorithm for the torsion problem so it only remains to find an algorithm for Case 3.

Recall that a symmetric polynomial can be rewritten in terms of elementary symmetric polynomials. Let $s_0(x_1, x_2), s_1(x_1, x_2)$ be the elementary symmetric polynomials in x_1, x_2. Then write $\tilde{g}_1(t_0, t_1), \tilde{g}_2(t_0, t_1)$ for polynomials such that $\tilde{g}_1(s_0(x_1, x_2), s_1(x_1, x_2)) = g_1(x_1, x_2)$ and $\tilde{g}_2(s_0(x_1, x_2), s_1(x_1, x_2)) = g_2(x_1, x_2)$.

Let $(U(X), V(X))$ be the Mumford representation of $D = (x_1, y_1) + (x_2, y_2)$. Then by definition

$$U(X) = (X - x_1)(X - x_2) = X^2 - s_0 X + s_1.$$

So $\tilde{g}_1(s_0, s_1) = \tilde{g}_2(s_0, s_1) = 0$ are necessary conditions *on the coefficients* of $U(X)$. This means we can generate a candidate list of possible $U(X)$ by finding all elements $a_0, a_1 \in \mathbb{F}_q$ such that $\tilde{g}_1(a_0, a_1) = \tilde{g}_2(a_0, a_1) = 0$.

Algorithm 10. Let H be a hyperelliptic curve of genus 2 defined over $\mathbb{F}_q$. The following algorithm finds a complete candidate list of n-divisors.

1. Calculate
$$\delta_n^i\Big(\frac{x_i - X}{4y_i^2}\Big), \epsilon_n^i\Big(\frac{x_i - X}{4y_i^2}\Big),$$
for $i = 1, 2$ using the formulas (3.23) and (3.24).
2. Calculate Δ_n^i, E_n^i for $i = 1, 2$.
3. Compute $f_1(x_1, x_2, y_1, y_2), f_2(x_1, x_2, y_1, y_2)$ by evaluating the determinants in (3.61), (3.62).
4. Substitute the relation $y_1^2 = F(x_1)$ and $y_2^2 = F(x_2)$ to obtain $h_1(x_1, x_2)$ and $h_2(x_1, x_2)$.
5. Compute $g_1(x_1, x_2), g_2(x_1, x_2)$ by dividing with $x_1 - x_2$.
6. Determine $\tilde{g}_1(t_0, t_1), \tilde{g}_2(t_0, t_1)$ using Gauss' Algorithm [7].
7. For each $i, j \in \mathbb{F}_q$
   (a) If $g_1(i, j) = g_2(i, j) = 0$ record $X^2 - jX + i$ as a candidate.

For every $U(X), V(X)$ in the candidate list, it is then a simple (and fast) matter of testing if $n(U(X), V(X)) = 0$ using Cantor's Algorithm (Algorithm 3). Since the candidate list is complete this gives us an algorithm for finding the n-division points $J(H)[n](\mathbb{F}_q)$.

Computations suggest the following:

Conjecture 3. Let L be the candidate list generated in Algorithm 10. Then $|L|$ grows, on average, linearly with q. Also, for all curves,

$$|L| \leq q + 1.$$

We summarize Cantor's algorithm for finding n-divison points.

Algorithm 11. Let H be a hyperelliptic curve of genus 2 defined over $\mathbb{F}_q$. Then the following algorithm computes the n-division points $J(H)[n](\mathbb{F}_q)$.

1. Compute and record all n-torsion points using Algorithm 6.
2. Compute all $2n$-torsion points (x_1, y_1). Record $D = 2(x_1, y_1)$ as an n-division point.
3. Compute a candidate list L of possible $U(X)$ using Algorithm 10.
4. For each $U(X) \in L$:
   (a) Compute all $V(X)$ such that $(U(X), V(X))$ is a Mumford pair using Algorithm 9.
   (b) For each pair $(U(X), V(X))$:
      i. Compute $n(U(X), V(X))$ using Cantor's Algorithm (Algorithm 3). If
$$n(U(X), V(X)) = 0,$$
record the divisor $(U(X), V(X))$ as an n-division point.

4 Calculating $\#\mathcal{H}_2^\omega[N](\mathbb{F}_q)$

4.1 The moduli space $\mathcal{H}_2^\omega[N]$

We will now consider the moduli space $\mathcal{H}_2^\omega[N]$ where every hyperelliptic curve comes with a marked k-rational Weierstrass point.

Definition 16. Let C be a hyperelliptic curve (Definition 2) of genus g defined over k and let $\omega \in C(k)$ be a Weierstrass point. We call the pair (C, ω) a **hyperelliptic curve defined over k with Weierstrass point.**

Remark. Recall that an elliptic curve is defined as a pair (E, O) where E is a projective, smooth genus 1 curve defined over k and $O \in C(k)$ is a point fixed to be the origin. So even though hyperelliptic curves with Weierstrass point is a special class of general hyperelliptic curves, the definition is somewhat natural.

We want morphism between hyperelliptic curves with Weierstrass point to preserve the Weierstrass point.

Definition 17. Let $\mathcal{R}_g$ denote the category of $H = (C, \omega)$ hyperelliptic curves of genus g defined over $\bar{k}$ with Weierstrass point. The morphisms $\phi\colon (C, \omega) \to (C', \omega')$ are morphisms $\phi\colon C \to C'$ with the additional requirement that $\phi(\omega) = \omega'$.

Definition 18. For $N \geq 1$ let $\mathcal{H}_g^\omega[N]$ be the moduli space of pairs (H, D) where $H = (C, \omega) \in \mathcal{R}_g$ and $D \in J(H)$ is a divisor with $\mathrm{ord}(D) = N$. And the isomorphisms between (H, D) and (H', D') are given by isomorphisms $\phi\colon H \to H'$ such that the induced isomorphism

$$\begin{aligned} \hat{\phi}\colon J(H) &\to J(H') \\ D &\mapsto D'. \end{aligned} \tag{4.1}$$

The k-rational points $\mathcal{H}_g^\omega[N](k)$ are pairs (H, D) such that H is defined over k and $D \in J(H)(k)$.

Remark. Note that $\mathcal{H}_g^\omega[N]$ consists of equivalence classes $[H, D]_{\bar{k}}$ where the $\bar{k}$ subscript denotes that the isomorphisms ϕ are defined over $\bar{k}$.

For further use we introduce the notation $[H, D]_k$ for the equivalence classes of pairs (H, D) where the isomorphisms ϕ are defined over k.

Definition 19. With N fixed, define for a $H \in \mathcal{R}_g$ defined over k,

$$E(H) = \{D \in J(H)/k \mid \mathrm{ord}(D) = N\} \tag{4.2}$$

$$\mathrm{c}(H) = |E(H)|\,. \tag{4.3}$$

Now, for $k = \mathbb{F}_q$ and $g = 2$, we will use the aforementioned algorithm to count the number of points in $\mathcal{H}_2[N](\mathbb{F}_q)$.

First, note that if N is odd then the division point algorithms allows us to compute $E(H), \mathrm{c}(H)$ in the following way:

Algorithm 12. For odd $N = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, the following algorithm computes $E(H)$ and $\mathrm{c}(H)$.

```
1. Compute the set of N-division points $J(H)[N](\mathbb{F}_q)$ using Algorithm 11.
2. For each $D \in J(H)[N](\mathbb{F}_q)$,
    (a) Loop over $1 \leq i \leq k$.
        For each $i$, compute $(N/p_i)D$ using Cantor's Algorithm (Algorithm 3).
        If $(N/p_i)D = 0$ we discard $D$ and continue the outer loop, otherwise
        continue the inner loop.
    (b) At this point we know $D \in E(H)$.
```

Proof. Since $\mathrm{ord}(D) = N$ implies that $nD = 0$ the set of N-division points are a complete candidate set. Further, if $nD = 0$ but $\mathrm{ord}(D) \neq N$ then $\mathrm{ord}(D) = N'$ for some divisor $N' \neq N$ of N. Since $N' \neq N$ there exists a p_i in the prime decomposition of N such that $p_i \nmid N$. Hence $N' \mid (N/p_i)$ and therefore $(N/p_i)D = 0$. □

Remark. If N is odd prime then $\mathrm{c}(H) = |J(H)[N](\mathbb{F}_q)|$.

Definition 20. Let

$$\mathfrak{H}_2 = \mathcal{R}_2 / \cong_{\mathbb{F}_q} .$$

In other words, $\mathfrak{H}_2$ denotes the $\mathbb{F}_q$-isomorphism classes of $\mathcal{R}_2$.

Our starting point for computing the number of $\mathbb{F}_q$-rational points on $\mathcal{H}_2^\omega[N]$ is the following theorem, based on a technique in [2].

Theorem 10.

$$|\mathcal{H}_2^\omega[N](\mathbb{F}_q)| = \sum_{[H]\in\mathfrak{H}_2} \frac{\mathrm{c}(H)}{|\mathrm{Aut}_{\mathbb{F}_q}(H)|}. \tag{4.4}$$

Proof. To save space let $k = \mathbb{F}_q$ and $\bar{k} = \bar{\mathbb{F}}_q$. Further let R denote the set of $H \in \mathcal{R}_2$ defined over k.

Take a fixed pair $Y = (H, P) \in R$. Then the following identity holds. See [10] or [12] for proof.

$$\sum_{\substack{[X]\in R/\cong_k \\ X \cong_{\bar{k}} Y}} \frac{1}{|\mathrm{Aut}_{\mathrm{k}}(X)|} = 1. \tag{4.5}$$

Then, (4.5) implies that,

$$|\mathcal{H}_2^\omega[N](\mathbb{F}_q)| = \sum_{[H,P]_{\bar{k}}} 1 = \sum_{[H,P]_{\bar{k}}} \sum_{\substack{[C,Q]_k \\ (H,P)\cong_{\bar{k}}(C,Q)}} \frac{1}{|\mathrm{Aut}_k(C,Q)|} \tag{4.6}$$

$$= \sum_{[C,Q]_k} \frac{1}{|\mathrm{Aut}_k(C,Q)|}. \tag{4.7}$$

It remains to prove

$$\sum_{[H,P]_k} \frac{1}{|\operatorname{Aut}_k(H,P)|} = \sum_{[H]_k} \frac{\mathrm{c}(H)}{|\operatorname{Aut}_k(H)|}. \tag{4.8}$$

Note that $G = \operatorname{Aut}_k(H)$ acts on pairs $(H,Q) \in R$. It is clear $(H,Q),(H,P)$ lies in the same G-orbit iff $[H,Q]_k = [H,P]_k$. Further the stabilizer G_P is all the k-automorphisms fixing P, i.e. $G_P = \operatorname{Aut}_k(H,P)$. Then by the Orbit-Stabilizer theorem, $|\operatorname{Aut}_k(H)| = |G.P|\,|G_P|$. Hence,

$$\sum_{[H]_k} \frac{\mathrm{c}(H)}{|\operatorname{Aut}_k(H)|} = \sum_{[H]_k} \sum_{P \in E(H)]} \frac{1}{|\operatorname{Aut}_k(H)|} = \sum_{[H]_k} \sum_{P \in E(H)} \frac{1}{|G.P|\,|G_P|} \tag{4.9}$$

$$= \sum_{[E,P]_k} \frac{1}{|G_P|} = \sum_{[E,P]_k} \frac{1}{|\operatorname{Aut}_k(H,P)|}. \tag{4.10}$$

□

Our next step is to rewrite (4.4) so we don't need to explicitly compute the automorphism groups.

Remark. We mention as a side note that it might be possible to calculate (4.4) directly. For small genus there are (slow) algorithms based on certain invariants that calculate the automorphism group. Moreover, for determining isomorphism classes when $g = 2$ there is a fast algorithm [13]. This functionality is implemented in the software package Magma [3].

4.2 Representative polynomials

Definition 21. Let $S = \{f(x) \in \mathbb{F}_q[x] \mid \deg f = 2g+1, f(x) \text{ square-free}\}$.

Intuitively, we will find a complete set of representatives for S while controlling how much of the automorphism group 'remains'.

Proposition 23. Let k be a field with $\operatorname{char}(k) \neq 2$. For every $f(x) \in S$ there is a corresponding hyperelliptic curve $H_f = (C_f, \infty)$ of genus g defined over k with Weierstrass point. The curve is defined by the equation, $C_f \colon y^2 = f(x)$.

On the other hand, we have already stated that a hyperelliptic curve $H = (C,\omega)$ with Weierstrass point admits a Weierstrass equation $y^2 = f(x)$ with $\deg f = 2g+1$. We also need to determine much choice there are when choosing the Weierstrass equation. Compare with [14, Corollary 4.33] and [15, Proposition 1.2].

Proposition 24 (Proposition 1.2 in [15])**.** Let k be a field with $\operatorname{char}(k) \neq 2$. Let (C,ω) be a hyperelliptic curve with Weierstrass point defined over a field k. Then there exists non-constant functions $x, y \in k(C)$ sending ω to ∞ and satisfying a Weierstrass equation

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

where the polynomial $f \in k[x]$ and $\deg f(x) = 2g+1$. Further, such an equation is unique up to variable change of the form,

$$\begin{aligned} y &\mapsto \gamma y \\ x &\mapsto \alpha x + \beta. \end{aligned} \tag{4.11}$$

where $\gamma, \alpha \in k^*$ and $\beta \in k$.

Thus every hyperelliptic curve $H = (C, \omega)$ defined over k with Weierstrass point is equal to H_f for some non-square polynomial $f \in k[x]$ with $\deg f = 2g+1$.

For $\gamma, \alpha, \beta \in \mathbb{F}_q$ with $\alpha, \gamma \neq 0$, let G denote the group of transformations

$$\begin{aligned} y &\mapsto \gamma y \\ x &\mapsto \alpha x + \beta. \end{aligned} \tag{4.12}$$

Proposition 25. For the group G we have, $|G| = q(q-1)^2$.

Proof. There are q choices for $\beta \in \mathbb{F}_q$ and $(q-1)^2$ choices for $\gamma, \alpha \in \mathbb{F}_q^*$. □

For $f \in S$ consider the equation $y^2 = f(x)$ and let the above G act on the equation resulting in $\gamma^2 y^2 = f(\alpha x + \beta)$. That is, $y^2 = \frac{f(\alpha x+\beta)}{\gamma^2}$. This motivates the following definition.

Proposition 26. For S and G as above the following holds.

(a) The group G acts on the set S. The action of $g \in G$ on S is given by

$$g.f = (\alpha, \beta, \gamma).f = \frac{f(\alpha x + \beta)}{\gamma^2}.$$

(b) For constant $k \in \mathbb{F}_q$ and $f \in S$ we have $k(g.f) = g.(kf)$.

Proof. Clearly, $(1,0,1).f = \frac{f(x+0)}{1} = f$. Further, let $g_1 = (\alpha_1, \beta_1, \gamma_1), g_2 = (\alpha_2, \beta_2, \gamma_2)$. Then the transformation $g_1 g_2$ is given by

$$x \xmapsto{g_2} \alpha_2 x + \beta_2 \xmapsto{g_1} \alpha_2(\alpha_1 x + \beta_1) + \beta_2 = \alpha_1\alpha_2 x + (\beta_2 + \alpha_2\beta_1) \tag{4.13}$$

$$y \xmapsto{g_2} \gamma_1 y \xmapsto{g_1} \gamma_1\gamma_2 y \tag{4.14}$$

Then,

$$(g_1 g_2).f = \frac{f(\alpha_1\alpha_2 x + \beta_1 + \alpha_1\beta_2)}{(\gamma_1\gamma_2)^2}. \tag{4.15}$$

But on the other hand,

$$g_1.(g_2.f) = g_1.\frac{f(\alpha_2 x + \beta_2)}{\gamma_2^2} = \frac{f(\alpha_2(\alpha_1 x + \beta_1) + \beta_2}{\gamma_1^2\gamma_2^2} \tag{4.16}$$

Hence $(g_1 g_2).f = g_1.(g_2.f)$. This proves G is an action on S.

For (b) we have by definition,

$$\begin{aligned} k(g.f) &= k\frac{a_{2g+1}(\alpha x)^5 + \cdots + a_1(\alpha x) + a_0}{\gamma^2} \\ &= \frac{ka_{2g+1}(\alpha x)^5 + \cdots + ka_1(\alpha x) + ka_0}{\gamma^2} \\ &= g.(kf). \end{aligned}$$

□

Proposition 27. Fix a H_f with $f \in S$. Then $g = (\alpha, \beta, \gamma) \in G$ induces an isomorphism $g_* \colon H_f \xrightarrow{\sim} H_{g.f}$. defined over $\mathbb{F}_q$.

Proof. There exists a field isomorphism between the function fields $\bar{\mathbb{F}}_q(H_f), \bar{\mathbb{F}}_q(H_{g.f})$ given by

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto \alpha x + \beta, \\ y &\mapsto \gamma y. \end{aligned}$$

But recall that there is an equivalence of categories between smooth, projective curves and functions fields. Hence there is a corresponding isomorphism $g_* \colon H_f \xrightarrow{\sim} H_{g.f}$. □

Proposition 28. $H_{f_1} \cong_{\mathbb{F}_q} H_{f_2}$ iff $G.f_1 = G.f_2$.

Proof. Proposition 24 proves the 'if' part.

Conversely, assume that $G.f_1 = G.f_2$. Then there is a $g \in G$ such that $g.f_1 = f_2$. Thus by Proposition 27 there is an isomorphism $H_{f_1} \cong_{\mathbb{F}_q} H_{f_2}$.

□

Definition 22. Fix $H_1 \in \mathcal{R}_g^\omega$ and let

$$T(H_1) = \{\psi : H_1 \xrightarrow{\sim} H_2 \mid H_2 \in \mathcal{R}_g^\omega\}.$$

Then there is a bijection $\Psi \colon G \to T(H_1)$ given by $g \mapsto g_*$.

Proposition 29. Let $\Phi \colon \mathfrak{H}_g \to S/G$ be the function given by

$$[H_f] \mapsto G.f$$

Then Φ is well-defined and a bijection.

Proof. Proposition 28 implies that Φ is well-defined and injective and Proposition 23 implies that Φ is surjective. □

Proposition 30. Let G_f denote the stabilizer of the action of G on S. Then $|G_f| = |\mathrm{Aut}(H_f)|$.

Proof. By definition, $G_f = \{g \in G \mid g.f = f\}. \subset G$. For any $g \in G_f$, the induced isomorphism $g_* \in \mathrm{Aut}\, H_f$. Hence $\Psi(G_f) \subset \mathrm{Aut}\, H_f$. Conversely, take $\phi \in \mathrm{Aut}\, H_f$. Then by Definition 22 $\phi = g_*$ for an element $g \in G$ such that $g.f = f$. Thus $g \in G_f$. This proves that $\Psi(G_f) = \mathrm{Aut}(H_f)$. □

In conclusion, orbits of G corresponds to isomorphism classes and stabilizers correspond to automorphism groups. This allows us to rewrite the sum (4.4) using the Orbit-Stabilizer theorem.

$$\sum_{[H]\in\mathfrak{H}_2} \frac{\mathrm{c}(H)}{|\mathrm{Aut}(H)|} = \sum_{f\in S/G} \frac{\mathrm{c}(H_f)}{|G_f|} = \sum_{f\in S/G} \frac{\mathrm{c}(H_f)\,|G.f|}{|G|} \tag{4.17}$$

But since $\mathrm{c}(H)$ only depends on the isomorphism class, this is equal to,

$$\sum_{f\in S} \frac{\mathrm{c}(H_f)}{|G|} \tag{4.18}$$

Equation (4.18) gives us a way to compute the original sum (4.4) without knowing the automorphism groups. However, ideally, we don't want to use (4.18) directly since we need to invoke the division point algorithm for each $f \in S$. We will study the effect of the action and subdivide S into different classes to minimize the number of terms in the sum (i.e. calls to the division point algorithm).

Proposition 31. Assume that $\mathbb{F}_q$ has characteristic different from 5. Let

$$f = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in S.$$

Then there is a representative

$$f' = b_5x^5 + b_3x^3 + b_2x^2 + b_1x + b_0 \in S,$$

i.e. without x^4 term, such that $f' \in G.f$.

Furthermore, for a given $f' \in S$ with $b_4 = 0$ there are exactly q number of $f \in S$ such that f is represented by f'.

Proof. If $\mathrm{char}\,\mathbb{F}_q \neq 5$, the Tschirnhaus transformation $T\colon x \mapsto x - a_4/(5a_5)$ makes the coefficient of x^4 vanish. But this transformation is on the form given in Proposition 24. Let $t = (1, a_4/4, 1) \in G$ be the group element corresponding to T. Then $f' = t.f$ has no x^4 term, so $f' = t.f$ is the representative we seek.

For the second part of the proposition let $f' \in S$ be such that $b_4 = 0$. Then let $g \in G$ be the transformation $x' = x + \beta, y' = y$ for $\beta \in \mathbb{F}_q$. Then, for each $\beta \in \mathbb{F}_q$, $g.f' \in S$ is represented by f'. Conversely, if $f \in S$ is represented by f' then $t.f = f'$. Taking $g_0 = (1, -a_4/4, 1) \in G$ we see that

$$g_0.f' = g_0.(t.f) = (g_0t).f = f.$$

Hence

$$\{g.f' \mid g = (1, \beta, 1), \beta \in \mathbb{F}_q\}$$

are exactly the polynomials in S that is represented by f'. Since there are q choices for β, there are a total of q polynomials $f \in S$ such that f is represented by f'. □

Using Proposition 31 we can simplify the sum (4.18).

$$\sum_{f\in S} \frac{\mathrm{c}(H_f)}{|G|} = \sum_{\substack{f'\in S\\ b_4=0}} \frac{q\,\mathrm{c}(H_{f'})}{|G|} = \sum_{\substack{f'\in S\\ b_4=0}} \frac{q\,\mathrm{c}(H_{f'})}{q(q-1)^2} = \sum_{\substack{f'\in S\\ b_4=0}} \frac{\mathrm{c}(H_{f'})}{(q-1)^2}. \tag{4.19}$$

Intuitively, we rigidify part of the group action G by requiring $a_4 = 0$ for the representatives. We make this statement more precise.

Definition 23. Let

$$S' = \{f = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in S \mid a_4 = 0\},$$

and

$$G' = \{(\alpha, \gamma) \mid (\alpha, 0, \gamma) \in G\} \subset G.$$

Proposition 32. Then,

(a) G' acts on the set S'.

(b) If $g \in G$ such that $g.S' = S'$ then $g \in G'$.

Proof. Let $f_1' = a_5x^5 + a_3x^3 + a_2x^2 + a_1x + a_0 \in S'$ and let $g \in G$ be a transformation with $\beta = 0$. Then

$$g.f_1' = \frac{1}{\gamma^2}(a_5(\alpha x)^5 + a_3(\alpha x)^3 + a_2(\alpha x)^2 a_1(\alpha x) + a_0).$$

That is $g.f_1' \in S'$. This proves (a).

Next let $f_2' \in S'$. Then any $g \in G$ with $\beta \neq 0$ gives a non-zero coefficient of x^4 in $g.f_1'$. Hence for any $g \in G$ such that $g.f_1' = f_2'$ we have $\beta = 0$. This proves G' is exactly the set fixing S'. □

Now by Proposition 32(b), using Proposition 28 for the right equivalence,

$$G'.f_1' = G'.f_2' \iff G.f_1' = G.f_2' \iff H_{f_1'} \cong H_{f_2'}.$$

And further, by Proposition 32(b) and Proposition 30,

$$\left|\operatorname{Aut} H_{f_1'}\right| = \left|G'_{f_1'}\right|.$$

Moreover, the requirement that $\beta = 0$ implies that

$$|G'| = (q-1)^2.$$

Roadmap. The idea is to divide S' into different classes for which better representatives can be found and hence minimize the number of terms in the sum (4.19).

Proposition 33. Let

$$f = a_5x^5 + a_3x^3 + a_2x^2 + a_1x + a_0 \in S' \tag{4.20}$$

such that two consecutive coefficients a_d, a_{d-1} in f are non-zero.

Let $A_f = a_{d-1}^d / a_d^{d-1}$. Then if A_f is a quadratic residue in $\mathbb{F}_q$, the following holds.

(a) There is an *unique* representative $f' \in S'$ with $a_d = a_{d-1} = 1$ such that $f \in G'.f'$, and,

(b) for such $f' \in S'$, we have $|G.f'| = (q-1)^2/2$.

Proof. We make the Ansatz $g = (\alpha, \gamma) \in G'$ and solve for $\alpha, \gamma \in \mathbb{F}_q^*$.

Letting g act on an arbitrary $f \in S'$ gives

$$g.f = \frac{1}{\gamma^2}(a_5\alpha^5x^5 + a_3\alpha^3x^3 + a_2\alpha^2x^2 + a_1\alpha x + a_0) \tag{4.21}$$

We want

$$\frac{a_d\alpha^d}{\gamma^2} = 1 \tag{4.22}$$

$$\frac{a_{d-1}\alpha^{d-1}}{\gamma^2} = 1. \tag{4.23}$$

Dividing (4.22) with (4.23) yields

$$\frac{a_d}{a_{d-1}}\alpha = 1 \iff \alpha = \frac{a_{d-1}}{a_d} \tag{4.24}$$

Hence we have solved for α.

Plugging this in (4.22), (4.23) we get

$$\frac{a_{d-1}^d}{a_d^{d-1}} = \gamma^2 \tag{4.25}$$

By assumption $A_f = a_{d-1}^d / a_d^{d-1}$ is a quadratic residue in $\mathbb{F}_q$. Hence we get two solutions for γ (characteristic is not 2)

$$\gamma = \pm\sqrt{\frac{a_{d-1}^d}{a_d^{d-1}}} \tag{4.26}$$

But since for $g_1 = (\alpha, \gamma), g_2 = (\alpha, -\gamma)$ we have $g_1.f = g_2.f$ for all $f \in S'$, it follows that there is an unique $f' \in S'$ with $b_{d-1} = b_d = 1$ such that $f \in G'.f'$. Since we have no choice anywhere, f' is unique. This proves (a).

For (b) assume $g = (\alpha, \gamma) \in G'$ such that $g.f' = f'$. This holds iff

$$\alpha^{d-1}/\gamma^2 = 1$$
$$\alpha^d/\gamma^2 = 1.$$

This system holds iff $\alpha = 1$ and $\gamma = \pm 1$. Thus $g = (1, \pm 1)$. Hence the stabilizer $\left|G'_{f'}\right| = 2$. Hence by the Orbit-Stabilizer Theorem, $|G'.f'| = \frac{(q-1)^2}{2}$.

□

Proposition 34. Let d be an integer, $1 \leq d \leq 3$. Take

$$f = a_5x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$$

in S' such that $a_d, a_{d-1} \neq 0$. Let r denote a fixed quadratic non-residue in $\mathbb{F}_q$. Then there exists an unique

$$f' = b_5x^5 + \cdots + x^d + x^{d-1} + \cdots \in S'$$

such that either

(i) $f \in G'.f'$, or,

(ii) $f \in G'.(rf')$.

Furthermore, as we go through all polynomials $f \in S'$ with $a_d, a_{d-1} \neq 0$, half will fall in case (i) and half in case (ii).

Proof. Either $A_f = a_{d-1}^d/a_d^{d-1}$ is a quadratic residue or a non-residue in $\mathbb{F}_q$. The first implies (i) by Proposition 33. We show that A_f being non-residue implies (ii).

Let $r \in \mathbb{F}_q^*$ be a quadratic non-residue and consider $rf \in S'$. Then

$$A_{rf} = \frac{a_{d-1}^d}{a_d^{d-1}}.$$

Note that r and a_{d-1}^d/a_d^{d-1} are non-residues by assumption. Then by quadratic reciprocity, ra_{d-1}^d/a_d^{d-1} is a quadratic residue. Hence by Proposition 33, there exists $f' \in S'$ with $b_{d-1} = b_d = 1$ such that $rf \in G'.f'$. We need to show $f \in G'.(rf')$.

Let $g = (\alpha_0, \gamma_0) \in G'$ be such that $g.f' = rf$. Then using Proposition 26(b),

$$r^2 f = rrf = r(g.f') = g.(rf').$$

But by letting $g' = (1, r)$ we see $g'.(r^2 f) = f$. Hence $f \in G'.(rf')$.

Now it remains to prove that exactly half of

$$\{a_{d-1}^d/a_d^{d-1} \mid a_{d-1}, a_d \in \mathbb{F}_q^*\} \tag{4.27}$$

are residues.

Note that a_{d-1}^d/a_d^{d-1} is a residue iff both a_{d-1}^d, a_d^{d-1} are residues. Assume first that d even. Then a_{d-1}^d is always a residue, so a_{d-1}^d/a_d^{d-1} is a residue iff a_d^{d-1} is a residue. But since $d-1$ is odd, a_d^{d-1} is a residue iff a_d is a residue. Hence half of (4.27) are residues.

The case when d is odd follows similarly.

□

Proposition 35. Let $r \in \mathbb{F}_q^*$ be a fixed quadratic non-residue. Let

$$f = a_5x^5 + a_3x^3 + a_2x^2 + a_1x + a_0 \in S'$$

with $a_0 \neq 0$.

Then, (a) there exists a *non-unique*

$$f' = b_5x^5 + b_3x^3 + b_2x^2 + b_1x + 1 \in S'$$

such that either

(i) $f \in G'.f'$, or,

(ii) $f \in G'.(rf')$.

Furthermore:

(a) For each f there are $q-1$ choices for f'.

(b) As we go through $f \in S'$ with $a_0 \neq 0$ half will fall in case (i) and the other half in case (ii).

(c) For each $f' \in S'$ with $b_1 = 1$ we have $|G'.f'| = (q-1)^2/2$.

Proof. (a) Either a_0 is a quadratic residue or not. First assume that a_0 is a residue and take $c \in \mathbb{F}_q^*$ such that $c^2 = a_0$. Then for $g = (1, c) \in G'$,

$$g.f = \frac{1}{c^2}(a_5x^5 + \cdots + a_0) = a_5/a_0x^5 + \cdots + 1.$$

Hence we take $f' = g.f$.

On the other hand if a_0 is a non-residue then ra_0 is a residue by Quadratic Reciprocity. So then $rf = ra_5x^5 + \cdots + ra_0$ satisfies part (a) of the proposition. Let f' be such that $rf \in G'.f'$. Then by Proposition 26(b), $r^2 f \in G'.(rf')$. Since r^2 is a residue, this implies that $f \in G'.(rf')$.

(b) Let $f' \in S'$ with $b_0 = 1$ be in the orbit of either f or rf. Then for each $\alpha \in \mathbb{F}_q^*$ consider $g = (\alpha, 1) \in G'$. Then ,

$$g.f' = b_5(\alpha x)^5 + \cdots + (\alpha x) + 1$$

is another representative for f. Conversely, let f_1', f_2' be representatives with constant term 1. Then the transformation between them must preserve the constant term. Then, $f_2' = g.f_1'$ where $g = (\alpha, 1)$ for some $\alpha \in \mathbb{F}_q$. Hence there are exactly $q-1$ representatives f' for each f.

(c) By Quadratic Reciprocity exactly half of $a_0 \in \mathbb{F}_q^*$ are residues.

(d) Let $f' \in S'$ with $b_1 = 1$. We show that $|G_{f'}| = 1$. For $g = (\alpha, \gamma) \in G'$ assume $g.f' = f'$. This holds iff $\alpha = 1$ and $\gamma = \pm 1$, i.e. $g = e$. □

Proposition 36. Let

$$f = a_5x^5 + a_3x^3 + a_1x \in S'$$

with $a_1 \neq 0$. Then there exists a

$$f' = b_5x^5 + b_3x^3 + x \in S'$$

such that $f \in G'.f'$.

Let D_f denote the number of representatives f' for f. Then for all f,

$$D_f = \begin{cases} (q-1)/4 & \text{if } q \equiv 1(4) \\ (q-1)/2 & \text{if } q \equiv 3(4) \end{cases} \tag{4.28}$$

Furthermore, for each $f' \in S'$ with $b_1 = 1$ and $b_2 = b_0 = 0$ we have

$$|G'.f'| = \begin{cases} (q-1)^2/4 & \text{if } q \equiv 1(4) \\ (q-1)^2/2 & \text{if } q \equiv 3(4) \end{cases} \tag{4.29}$$

Proof. Since $a_1 \neq 0$ we can take $\alpha = 1/a_1$. Then for $g = (\alpha, 1)$ we have,

$$g.f = a_5\alpha^5x^5 + \cdots + a_1\alpha x = a_5\alpha^5x^5 + \cdots + x.$$

Hence we take $f' = f.g$.

Recall that if $q \equiv 1(4)$ then (i) -1 is a residue, and (ii) $-\alpha$ is a residue for every residue $\alpha \in \mathbb{F}_q^*$. On the other hand if $q \equiv 3(4)$ then (i) -1 is a non-residue, and (ii) $-\alpha$ is a non-residue for every residue $\alpha \in \mathbb{F}_q^*$.

We prove (4.28). Consider $f' \in S'$ with $b_1 = 1, b_0 = 0$. For quadratic residues $\alpha \in \mathbb{F}_q^*$ there is a $\gamma \in \mathbb{F}_q^*$ such that $\gamma^2 = \alpha$. For the transformation $g = (\alpha, \gamma)$,

$$g.f' = \frac{\alpha^5}{\gamma^2}a_5x^5 + \frac{\alpha^3}{\gamma^2}a_3x^3 + \frac{\alpha}{\gamma^2}x = \frac{\alpha^5}{\gamma^2}a_5x^5 + \frac{\alpha^3}{\gamma^2}a_3x^3 + x.$$

So $g.f'$ is another representative for f. Conversely, any map between representatives must preserve the linear coefficient, i.e. we require that $\alpha/\gamma^2 = 1 \iff \gamma^2 = \alpha$. Thus $\{g.f'\}$ are exactly the representatives of f. Hence

$$D_f = \left|\{g.f' \mid \alpha \in \mathbb{F}_q^*, \alpha \text{ residue}\}\right|.$$

First assume that $q \equiv 1(4)$. Then $-\alpha \in \mathbb{F}_q^*$ is a residue. Let $\delta \in \mathbb{F}_q^*$ such that $\delta^2 = -\alpha$ and let $g' = (-\alpha, \delta)$. Then

$$g'.f' = \frac{-\alpha^5}{\delta^2}a_5x^5 + \frac{-\alpha^3}{\delta^2} + x.$$

But

$$\frac{-\alpha^5}{\delta^2} = \frac{-\alpha^5}{-\alpha} = \alpha^4 = \frac{\alpha^5}{\gamma^2},$$

and

$$\frac{-\alpha^3}{\delta^2} = \frac{-\alpha^3}{-\alpha} = \alpha^2 = \frac{\alpha^3}{\gamma^2}.$$

Hence $g'.f' = g.f'$. So we are counting the representatives twice by counting residues $\alpha \in \mathbb{F}_q^*$. Hence $D_f = (q-1)/4$.

On the other hand for $q \equiv 3(4)$, let $\alpha, \alpha' \in \mathbb{F}_q^*$ be residues such that $\alpha^4 = (\alpha')^4$ and $\alpha^2 = (\alpha')^2$. Then since $-\alpha$ is not a residue, the only solution is $\alpha = \alpha'$. This proves that $g.f'$ are distinct for each residue $\alpha \in \mathbb{F}_q^*$. Thus $D_f = (q-1)/2$.

Let $f' \in S'$ with $b_1 = 1$ ad $b_2 = b_0 = 0$ and consider the stabilizer $G'_{f'}$. Clearly, $g = (1, 1) = e \in G'$ fixes f'. Assume that $g.f' = f'$. Then equating coefficients yields

$$\frac{\alpha^5}{\gamma^2} = 1 \tag{4.30}$$

$$\frac{\alpha^3}{\gamma^2} = 1 \tag{4.31}$$

$$\frac{\alpha}{\gamma^2} = 1 \tag{4.32}$$

Dividing (4.31) with (4.32) gives $\alpha^2 = 1$. So $\alpha = \pm 1$. For $\alpha = 1$ Equation (4.32) implies that $\gamma = 1$. Hence this solution corresponds to $g = (1, \pm 1)$.

Setting $\alpha = -1$ in (4.32) gives $\gamma^2 = -1$. This equation is solvable iff -1 is a quadratic residue. Hence for $q \equiv 1(4)$ the transformations $g = (-1, \pm\gamma)$ fixes f'. Thus in this case $\left|G'_{f'}\right| = 4$. On the other hand if $q \equiv 3(4)$ then $g = (1, \pm 1)$ are the only transformations fixing f' so $|G'.f'| = 2$. This proves Equation (4.29). □

Definition 24. Let W be the union of the sets of in Table 4.1. We call W the **set of representatives**.

Set	Polynomials
W_A	$f = a_5x^5 + x^3 + x^2 + a_1x + a_0; a_5 \in \mathbb{F}_q^*, a_1, a_0 \in \mathbb{F}_q$
$W_{B.1}$	$f = a_5x^5 + x^2 + x + a_0; a_5 \in \mathbb{F}_q^*, a_1 \in \mathbb{F}_q$
$W_{B.2}$	$f = a_5x^5 + a_2x^2 + 1; a_5, a_2 \in \mathbb{F}_q^*$
$W_{C.1}$	$f = a_5x^5 + a_3x^3 + x + 1; a_5, a_3 \in \mathbb{F}_q^*$
$W_{C.2}$	$f = a_5x^5 + a_3x^3 + 1; a_5, a_3 \in \mathbb{F}_q^*$
$W_{C.3}$	$f = a_5x^5 + a_3x^3 + x; a_5, a_3 \in \mathbb{F}_q^*$
$W_{D.1}$	$f = a_5x^5 + x + 1; a_5 \in \mathbb{F}_q^*$
$W_{D.2}$	$f = a_5x^5 + 1; a_5 \in \mathbb{F}_q^*$
$W_{D.3}$	$f = a_5x^5 + x; a_5 \in \mathbb{F}_q^*$

Table 4.1: Representative sets

We will prove the following theorem later.

Theorem 11. Let $r \in \mathbb{F}_q$ be a fixed quadratic non-residue. Then for each $f \in S'$ there is a $f' \in W$ such that either (i) $f \in G'.f'$ or (ii) $f \in G'.rf'$. However in the case $f' \in W_{C.3}$ or $f' \in W_{D.3}$ we always have (i). More precisely, for $f' \in S'$ define

$$\mathrm{d}(f') = \begin{cases} f' & \text{if } f' \in W_{C.3} \cup W_{D.3} \\ f', rf' & \text{otherwise.} \end{cases}$$

The claim is that $\{\mathrm{d}(f') \mid f' \in W\}$ is a complete set of representatives for S' w.r.t the action of G'.

$a_3, a_2 \neq 0$	$a_3 = 0, a_2 \neq 0$	$a_3 \neq 0, a_2 = 0$	$a_3 = a_2 = 0$
Class A	Class B	Class C	Class D

Table 4.2: A first classification into cases

We classify S' into cases fixing as much of G' as possible using Proposition 34, Proposition 35, and Proposition 36. Our first division into classes is as in Table 4.2. Further we split the sum

$$\sum_{f \in S'} \frac{\mathrm{c}(H_f)}{(q-1)^2}$$

in subsums corresponding to the classes. For $I \in \{A, B, C, D\}$, let

$$U_I = \sum_{f \in I} \frac{\mathrm{c}(H_f)}{(q-1)^2}.$$

We will split the cases and subsums further.

First, we need to make sure that G' respects a division into classes based on non-zero conditions on the coefficients.

Proposition 37. Take an arbitrary $f = a_5x^5 + a_3x^3 + a_2x^2 + a_1x + a_0 \in S'$. Further, let $N(f) = \{i \in \mathbb{N} \mid a_i \neq 0\}$ be the index of the non-zero coefficients of f and let $Z(f) = \{0, 1, 3, 5\} - N(f)$ be the index of the zero coefficients. Then for $g \in G'$, $N(g.f) = N(f)$ and $Z(g.f) = Z(f)$.

Proof. It is enough to prove $N(g.f) = N(f)$.

Let $g = (\alpha, \gamma) \in G'$ then

$$g.f = \frac{\alpha^5}{\gamma^2}a_5x^5 + \frac{\alpha^3}{\gamma^2}a_3x^3 + \frac{\alpha^2}{\gamma^2}a_2x^2 + \frac{\alpha}{\gamma^2}a_1x + \frac{1}{\gamma^2}a_0.$$

Since $\alpha^i/\gamma^2 a_i \neq 0 \iff a_i \neq 0$ the proposition follows. □

Class A

Let $f \in A$ then Proposition 34 implies that there exists an unique $f' \in W_A$ such that either (i) $f \in G'.f'$ or (ii) $f \in G'.rf'$. From this Theorem 11 is proved for $f \in A$. Further, for a representative $f' \in W_A$ the $f \in G'.f' \subset A$ are exactly the $f \in A$ having normal form f'. So by uniqueness of the representative,

$$U_A = \sum_{f \in A} \frac{\mathrm{c}(H_f)}{(q-1)^2} = \sum_{f' \in W_A} \frac{|G'.f'|\,\mathrm{c}(H_{f'})}{(q-1)^2} + \sum_{f' \in W_A} \frac{|G'.f'|\,\mathrm{c}(H_{rf'})}{(q-1)^2}.$$

But by Proposition 33, 34 we have $|G'.f'| = |G'.rf'| = (q-1)^2/2$. Hence,

$$U_A = \sum_{f \in W_A} \frac{\mathrm{c}(H_f)}{2} + \sum_{f \in W_A} \frac{\mathrm{c}(H_{rf})}{2}. \qquad (4.33)$$

Class B

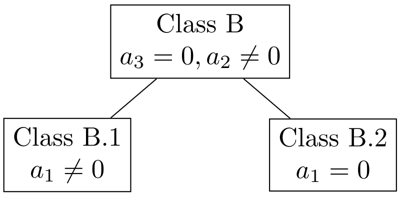

Figure 4.1: Further classification of Class B

If $f \in B.1$ then using a similar argument as for the Class A case proves Theorem 11 for $f \in B.1$ and yields,

$$U_{B.1} = \sum_{f \in W_{B.1}} \frac{\mathrm{c}(H_f)}{2} + \sum_{f \in W_{B.1}} \frac{\mathrm{c}(H_{rf})}{2}. \qquad (4.34)$$

On the other hand assume $f \in B.2$, i.e. $f = a_5x^5 + a_2x^2 + a_0$. Then since f is by assumption separable we can assume without loss of generality that $a_0 \neq 0$. Then by Proposition 35 there exists a normal form $f' \in W_{B.2}$ such that either (i) $f \in G'.f'$ or (ii) $f \in G'.f'$. This proves Theorem 11 for $f \in B.2$. For $f' \in W_{B.2}$ the $f \in G'.f' \subset B.2$ are exactly the $f \in B.2$ with normal form f'. But since every $f \in B.2$ has $q-1$ representatives on normal form, we need to divide the sum with $q-1$. Hence,

$$U_{B.2} = \sum_{f \in B.2} \frac{\mathrm{c}(H_f)}{(q-1)^2} = \sum_{f' \in W_{B.2}} \frac{|G'.f'|\,\mathrm{c}(H_{f'})}{(q-1)(q-1)^2} + \sum_{f' \in W_{B.2}} \frac{|G'.f'|\,\mathrm{c}(H_{rf'})}{(q-1)(q-1)^2}.$$

Then since $|G'.f'| = (q-1)^2/2$,

$$U_{B.2} = \sum_{f \in W_{B.2}} \frac{\mathrm{c}(H_f)}{2(q-1)} + \sum_{f \in W_{B.2}} \frac{\mathrm{c}(H_{rf})}{2(q-1)}. \tag{4.35}$$

Class C

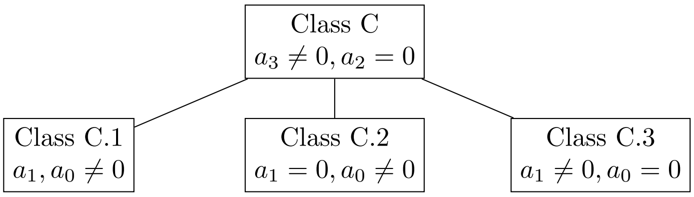

Figure 4.2: Further classification of Class C

If $f \in C.1$ then two consecutive coefficients are non-zero. So we can use the same argument as in Class A to prove Theorem 11 and,

$$U_{C.1} = \sum_{f \in W_{C.1}} \frac{\mathrm{c}(H_f)}{2} + \sum_{f \in W_{C.1}} \frac{\mathrm{c}(H_{rf})}{2}. \tag{4.36}$$

If $f \in C.2$ then we can use Proposition 35 similar to Class $B.2$ to prove,

$$U_{C.2} = \sum_{f \in W_{C.2}} \frac{\mathrm{c}(H_f)}{2(q-1)} + \sum_{f \in W_{C.2}} \frac{\mathrm{c}(H_{rf})}{2(q-1)}. \tag{4.37}$$

Let $f \in C.3$, i.e. $f = a_5x^5 + a_3x^3 + a_1x$. Note that since f is assumed separable, we can assume without loss of generality that $a_1 \neq 0$. Hence f is of the form required by Proposition 36. So there exists a $f' \in W_{C.3}$ such that $f \in G'.f'$. Further each $f' \in W_{C.3}$ corresponds exactly to the $f \in G'.f' \subset C.3$.

First assume that $q \equiv 1(4)$. Then $|G'.f'| = (q-1)^2/4$ and there are $(q-1)/4$ choices for normal form of $f \in W_{C.3}$. Hence,

$$\begin{aligned} U_{C.3} = \sum_{f \in C.3} \frac{\mathrm{c}(H_f)}{(q-1)^2} &= \sum_{f' \in W_{C.3}} \frac{|G'.f'|\,\mathrm{c}(H_{f'})}{(q-1)^2} \frac{4}{q-1} \\ &= \sum_{f' \in W_{C.3}} \frac{\mathrm{c}(H_{f'})}{(q-1)^2} \frac{(q-1)^2}{4} \frac{4}{q-1} = \sum_{f' \in W_{C.3}} \frac{\mathrm{c}(H_{f'})}{q-1}. \end{aligned}$$

On the other hand if $q \equiv 3(4)$ then $|G'.f'| = (q-1)^2/2$ and there are $(q-1)/2$ choices for normal form of $f \in W_{C.3}$. Hence,

$$U_{C.3} = \sum_{f \in C.3} \frac{\mathrm{c}(H_f)}{(q-1)^2} = \sum_{f' \in W_{C.3}} \frac{2\,|G'.f'|\,\mathrm{c}(H_{f'})}{(q-1)^2(q-1)} = \sum_{f' \in W_{C.3}} \frac{\mathrm{c}(H_{f'})}{q-1}.$$

Thus, in both cases,

$$U_{C.3} = \sum_{f \in W_{C.3}} \frac{\mathrm{c}(H_f)}{q-1}. \tag{4.38}$$

Class D

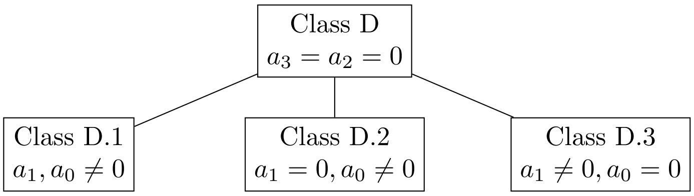

Figure 4.3: Further classification of Class D

For $D.1$ we have two consecutive coefficients non-zero. Then a similar argument as in the Class A case proves,

$$U_{D.1} = \sum_{f \in W_{D.1}} \frac{\mathrm{c}(H_f)}{2} + \sum_{f \in W_{D.1}} \frac{\mathrm{c}(H_{rf})}{2}. \tag{4.39}$$

For $D.2$ an argument similar to the $B.2$ case proves,

$$U_{D.2} = \sum_{f \in W_{D.2}} \frac{\mathrm{c}(H_f)}{2(q-1)} + \sum_{f \in W_{D.2}} \frac{\mathrm{c}(H_{rf})}{2(q-1)}. \tag{4.40}$$

Finally, the $D.3$ case is proved in the same way as the $C.3$ case. Thus,

$$U_{D.3} = \sum_{f \in W_{D.3}} \frac{\mathrm{c}(H_f)}{q-1}. \tag{4.41}$$

4.3 The algorithm

Let

$$U = U_A + U_{B.1} + U_{B.2} + U_{C.1} + U_{C.2} + U_{C.3} + U_{D.1} + U_{D.2} + U_{D.3},$$

where the subsums U_i are given by the equations (4.33) - (4.41).

Proposition 38. For the set W of representatives we have

$$|W| \leq q^3 + 4q^2 - 6q + 1.$$

q	#terms	$Q(q)$
3	67	86
7	831	954
11	3193	3390
13	5043	5436
17	10979	11664
19	15231	16038
23	26579	27786
29	52475	54348

Table 4.3: Number of terms in U depending on q

Furthermore, let u denote the number of terms in the sum U and let

$$Q(q) = 2q^3 + 7q^2 - 11q + 2.$$

Then,

$$u \leq Q(q).$$

Proof. Consider Table 4.1. We give an upper bound by considering all polynomials (including non-separable) of the form in column two. However note that the set W does not contain non-singular polynomials.

For Class A we have $q^2(q-1)$ choices for the coefficients. For $B.1$ we have $q(q-1)$ choices and for $B.2$ we have $(q-1)^2$ choices. For any subclass of C, D we have $(q-1)^2$ and $(q-1)$ respectively. Hence,

$$\begin{aligned}|W| &\leq q^2(q-1) + q(q-1) + (q-1)^2 + 3(q-1)^2 + 3(q-1)\\ &= q^3 + 4q^2 - 6q + 1.\end{aligned}$$

Consider the subsums U_i. Note that for Classes $A, B.1, B.2, C.1, C.2, D.1, D.2$ we have two terms for each representative f' and for Classes $C.3, D.3$ only a single term for each representative. Hence,

$$\begin{aligned}u &\leq 2q^2(q-1) + 2q(q-1) + 2(q-1)^2 + 5(q-1)^2 + 5(q-1)\\ &= 2q^3 + 7q^2 - 11q + 2\end{aligned}$$

□

Remark. Table 4.3 shows the true number of terms in U versus the polynomial $Q(q)$. The difference comes from non-separable polynomials counted by Q but not included in W. But since the majority of polynomials will be separable, the polynomial Q gives a pretty tight bound.

Finally, we state the algorithm for counting rational points on the moduli space $\mathcal{H}_2^\omega[N]$.

Algorithm 13. Let r be a fixed quadratic non-residue in $\mathbb{F}_q$. The following algorithm will generate a set L of tuples (f, b, w) such that

$$|\mathcal{H}_2^\omega[N](\mathbb{F}_q)| = \sum_{(f,b,w)\in L} \mathrm{t}(f, b, w), \tag{4.42}$$

where t is the function

$$\mathrm{t}(f,b,w)=\begin{cases}\frac{1}{w}\,\mathrm{c}(H_f) & \text{if } b \text{ False}\\ \frac{1}{w}(\mathrm{c}(H_f)+\mathrm{c}(H_{rf})) & \text{if } b \text{ True}\end{cases} \tag{4.43}$$

Note that f denotes a representative polynomial, b is a flag signifying if we have the non-residue case in the sum and w is a weight.

The following steps will generate L where each step corresponds to a class in Table 4.1.

A. For all $(a_5,a_1,a_0)\in\mathbb{F}_q^*\times\mathbb{F}_q\times\mathbb{F}_q$, let

$$f=a_5x^5+x^3+x^2+a_1x+a_0,$$

and return $(f,\mathrm{True},1/2)$ if $\mathrm{disc}(f)\neq 0$.

B. (1) For all $(a_5,a_0)\in\mathbb{F}_q^*\times\mathbb{F}_q$, let

$$f=a_5x^5+x^2+x+a_0,$$

and return $(f,\mathrm{True},1/2)$ if $\mathrm{disc}(f)\neq 0$.

(2) For all $(a_5,a_2)\in\mathbb{F}_q^*\times\mathbb{F}_q^*$, let

$$f=a_5x^5+a_2x^2+1,$$

and return $(f,\mathrm{True},1/2(q-1))$ if $\mathrm{disc}(f)\neq 0$.

C. (1) For all $(a_5,a_3)\in\mathbb{F}_q^*\times\mathbb{F}_q^*$, let

$$f=a_5x^5+a_3x^2+x+1,$$

and return $(f,\mathrm{True},1)$ if $\mathrm{disc}(f)\neq 0$.

(2) For all $(a_5,a_3)\in\mathbb{F}_q^*\times\mathbb{F}_q^*$, let

$$f=a_5x^5+a_3x^3+1,$$

and return $(f,\mathrm{True},1/2(q-1))$ if $\mathrm{disc}(f)\neq 0$.

(3) For all $(a_5,a_3)\in\mathbb{F}_q^*\times\mathbb{F}_q^*$, let

$$f=a_5x^5+a_3x^3+x,$$

and return $(f,\mathrm{False},1/(q-1))$ if $\mathrm{disc}(f)\neq 0$.

D. (1) For all $a_5\in\mathbb{F}_q^*$, let

$$f=a_5x^5+x+1,$$

and return $(f,\mathrm{True},1/2)$ if $\mathrm{disc}(f)\neq 0$.

(2) For all $a_5\in\mathbb{F}_q^*$, let

$$f=a_5x^5+1,$$

and return $(f,\mathrm{True},1/2(q-1))$ if $\mathrm{disc}(f)\neq 0$.

(3) For all $a_5\in\mathbb{F}_q^*$, let

$$f=a_5x^5+x,$$

and return $(f,\mathrm{False},1/(q-1))$ if $\mathrm{disc}(f)\neq 0$.

See Appendix B for an example of the output of this algorithm.

4.4 Notes about the implementation

As part of this project, Algorithm 13 for calculating $\#\mathcal{H}_w^{\omega}[N](\mathbb{F}_q)$ was implemented in Sage/Python. The author's implementation of the algorithms in this paper is available as a GitHub repository.[1]

The results of the computations are presented in Tables 1.1. The computations took weeks on a computer with Intel(R) Core(TM) i7 950 CPU and 19,6 GB of RAM.

Naive division point algorithm vs Cantor's division point algorithm

When calculating $|\mathcal{H}_2^{\omega}[N](\mathbb{F}_q)|$ using Algorithm 13 we have two options for determining c(H): either, Cantor's division point algorithm or the naive algorithm. In practice, it turns out that the naive algorithm is actually faster than Cantor's division point algorithm. However, the torsion algorithm (Algorithm 6) can be useful in application where we are interested in torsion points rather than division points.

Another property detrimental to Cantor's division algorithm is that it's time complexity with respect to N grows fast. The naive algorithm seem to have nicer asymptotic behavior with respect to N. This is not surprising since the number of Mumford pairs (U, V) only depends on q (and the genus).

Overall, when computing $|\mathcal{H}_2^{\omega}[N](\mathbb{F}_q)|$, the biggest hurdle is the sheer number of curves (i.e. number of terms in the sum U, c.f. Proposition 38 and Table 4.3). So we require significant speed-ups to be able to continue calculations for bigger q in a reasonable amount of time.

Possible improvements of Cantor's division point algorithm

The performance of Cantor's division algorithm can probably be improved with a better implementation. Our implementation follows the presentation in Chapter 3 closely. It uses symbolic manipulations and then reduces modulo p to get a polynomial in $\mathbb{F}_q[x]$. Instead of working with symbolic expressions in characteristic 0, it would be preferable to work with multivariate polynomials in characteristic p.

The most time intensive part of Cantor's division algorithm is Case 3 (Proposition 22). Instead of deriving necessary conditions on the coefficients on $U(X)$ it might be faster to solve the polynomial equation system in Proposition 17 directly using Gröbner basis algorithms.

[1] https://github.com/neural99/cantor-division-polynomials/

Bibliography

[1] G.A. Baker and P.R. Graves-Morris. *Padé Approximants*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1996.

[2] Jonas Bergström. Equivariant counts of points of the moduli spaces of pointed hyperelliptic curves. *Documenta Mathematica*, 14:259–296, 2009.

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

[4] David G Cantor. Computing in the jacobian of a hyperelliptic curve. *Mathematics of computation*, 48(177):95–101, 1987.

[5] David G Cantor. On the analogue of the division polynomials for hyperelliptic curves. *Journal fur die reine und angewandte Mathematik*, 447:91–146, 1994.

[6] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete Mathematics and Its Applications. CRC Press, 2005.

[7] David Cox, John Little, and Donal O'shea. *Ideals, varieties, and algorithms*, volume 3. Springer, 1992.

[8] The Sage Developers. *Sage Mathematics Software (Version x.y.z)*, YYYY. `http://www.sagemath.org`.

[9] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics. Springer, 2005.

[10] Gerard Van Der Geer and Marcel Van Der Vlugt. Supersingular curves of genus 2 over finite fields of characteristic 2. *Mathematische Nachrichten*, 159(1):73–81, 1992.

[11] K. Ireland and M.I. Rosen. *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics. Springer, 1990.

[12] Nicholas M Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45. American Mathematical Soc., 1999.

[13] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling. Fast computation of isomorphisms of hyperelliptic curves and explicit galois descent. *The Open Book Series*, 1(1):463–486, 2013.

[14] Q. Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford graduate texts in mathematics. Oxford University Press, 2002.

[15] P. Lockhart. On the discriminant of a hyperelliptic curve. *Trans. Amer. Math. Soc.*, 342(2):729–752, feb 1994.

[16] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[17] James S. Milne. Modular functions and modular forms (v1.30), 2012. Available at www.jmilne.org/math/.

[18] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2009.

[19] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. Discrete Mathematics and Its Applications. CRC Press, 2008.

Appendices

A Examples of division polynomials ψ_n

n	ψ_n
0	0
1	0
2	0
3	1
4	$8\left(x^7+x^2+1\right)^{\frac{3}{2}}$
5	$35\,x^{24}+280\,x^{19}+1624\,x^{17}-1920\,x^{14}-6888\,x^{12}-8176\,x^{10}+960\,x^{9}+3552\,x^{7}+3808\,x^{5}+2240\,x^{3}+64\,x^{2}-16$
6	$16\,(7\,x^{29}+378\,x^{24}+4536\,x^{22}-9408\,x^{19}-43064\,x^{17}-58464\,x^{15}+11328\,x^{14}+49392\,x^{12}+72576\,x^{10}-768\,x^{9}+51968\,x^{8}-2880\,x^{7}-7056\,x^{5}-4032\,x^{3}+128\,x^{2}-2688\,x-96)\left(x^7+x^2+1\right)^{\frac{3}{2}}x$
7	$294\,x^{60}+90552\,x^{55}+1558200\,x^{53}-4540368\,x^{50}-22618792\,x^{48}-43267392\,x^{46}-7182336\,x^{45}-72610944\,x^{43}-311235456\,x^{41}+11630080\,x^{40}-389252864\,x^{39}+147399168\,x^{38}+382940096\,x^{36}-66241536\,x^{35}+212583168\,x^{34}-546846720\,x^{33}+104579328\,x^{32}-2056006400\,x^{31}+17170432\,x^{30}-4765603584\,x^{29}+209044480\,x^{28}-5715598336\,x^{27}+1084823040\,x^{26}-2783271936\,x^{25}+2202520320\,x^{24}-386629632\,x^{23}+1851745280\,x^{22}-1428774912\,x^{21}+612577280\,x^{20}-2979809280\,x^{19}+176885760\,x^{18}-4193064960\,x^{17}-115286016\,x^{16}-4034752512\,x^{15}-226443264\,x^{14}-2274148352\,x^{13}-229859840\,x^{12}-569589760\,x^{11}-174354432\,x^{10}+3309568\,x^{9}-127045632\,x^{8}-2476032\,x^{7}-67436544\,x^{6}-3999744\,x^{5}-12861440\,x^{4}-1261568\,x^{3}-4096\,x^{2}-114688\,x-2048$
8	$32\,(21\,x^{72}+27720\,x^{67}+657888\,x^{65}-2873640\,x^{62}-18505760\,x^{60}-63264768\,x^{58}-23339520\,x^{57}-275413600\,x^{55}-2044149184\,x^{53}-72934400\,x^{52}-4222556800\,x^{51}+915071520\,x^{50}+4867721936\,x^{48}-1750325248\,x^{47}+3055555328\,x^{46}-17304698880\,x^{45}+1501491712\,x^{44}-73235185408\,x^{43}+980305920\,x^{42}-181840834560\,x^{41}+12279156736\,x^{40}-236482598912\,x^{39}+65364463360\,x^{38}-125828702208\,x^{37}+158301513216\,x^{36}-25741660160\,x^{35}+192538157056\,x^{34}-112900702208\,x^{33}+135594432512\,x^{32}-286863768576\,x^{31}+58792357888\,x^{30}-486940805120\,x^{29}-5483782144\,x^{28}-541795065856\,x^{27}-9612180480\,x^{26}-348065693696\,x^{25}-12762579200\,x^{24}-106924556288\,x^{23}-27868442624\,x^{22}-13720092672\,x^{21}-38019153920\,x^{20}-24301426688\,x^{19}-22792749056\,x^{18}-30488944640\,x^{17}-2526363648\,x^{16}-30466670592\,x^{15}-243156992\,x^{14}-23103406080\,x^{13}-778846208\,x^{12}-10448994304\,x^{11}-529858560\,x^{10}-2161246208\,x^{9}-167247872\,x^{8}+19013632\,x^{7}-54198272\,x^{6}+8142848\,x^{5}-42205184\,x^{4}-229376\,x^{3}-7364608\,x^{2}-262144\,x-4096)\left(x^7+x^2+1\right)^{\frac{3}{2}}$

Table A.1: Division polynomials ψ_n for the curve $y^2 = x^7 + x^2 + 1$

n	ψ_n
0	0
1	0
2	1
3	$4\,(x^4-x^3+x^2-x+1)(x+1)$
4	$10\,(x^5-4)^2x^2$
5	$20\,(x^{10}-108\,x^5+16)(x^5-4)(x^4-x^3+x^2-x+1)(x+1)x$
6	$5\,(7\,x^{20}-4872\,x^{15}-7408\,x^{10}-12672\,x^5-768)(x^5-4)^2x^2$
7	$8\,(7\,x^{40}-22344\,x^{35}+224896\,x^{30}-9451008\,x^{25}+170240\,x^{20}-57028608\,x^{15} -3272704\,x^{10}-4767744\,x^5-32768)(x^4-x^3+x^2-x+1)(x+1)$
8	$84\,x^{60}-981792\,x^{55}-8072256\,x^{50}-5136395520\,x^{45}-9367057920\,x^{40} -90223337472\,x^{35}-114657705984\,x^{30}-117268611072\,x^{25}-155547729920\,x^{20} -229528043520\,x^{15}-38803603456\,x^{10}+1686110208\,x^5-16777216$
9	$120\,(x^{60}-36688\,x^{55}-4458384\,x^{50}-1658593280\,x^{45}-18198906880\,x^{40} -157336670208\,x^{35}-345653886976\,x^{30}-471787716608\,x^{25}-137167994880\,x^{20} -3177185280\,x^{15}+20634402816\,x^{10}+956301312\,x^5-25165824)(x^5-4)^2 (x^4-x^3+x^2-x+1)(x+1)x^2$
10	$5\,(33\,x^{90}-3375036\,x^{85}-1711423536\,x^{80}-1004715154752\,x^{75} -16454837809920\,x^{70}+107245196473344\,x^{65}+8625335817756672\,x^{60} +45127976765325312\,x^{55}+129275034097025024\,x^{50}+177878883340124160\,x^{45} +112684530311102464\,x^{40}-21097774263042048\,x^{35}-120707800543264768\,x^{30} -113963990249373696\,x^{25}-31192453658705920\,x^{20}-1612226569961472\,x^{15} -294252504416256\,x^{10}+13761075216384\,x^5-137438953472)(x^5-4)x$
11	$20\,(11\,x^{100}-2849880\,x^{95}-4687088560\,x^{90}-4736403754560\,x^{85} -228260548980480\,x^{80}+8318978192722944\,x^{75}+539433596351938560\,x^{70} +4633662928140779520\,x^{65}+19543192767179653120\,x^{60} +44163514993394319360\,x^{55}+105048907680124502016\,x^{50} +192921432429963509760\,x^{45}+215770750752883998720\,x^{40} +104480531283884113920\,x^{35}+24139882138079068160\,x^{30} +6825760756013727744\,x^{25}+4975917911056056320\,x^{20} +581389708311920640\,x^{15}-9399793625333760\,x^{10}+2585226714808320\,x^5 +12094627905536)(x^5-4)^2(x^4-x^3+x^2-x+1)(x+1)x^2$
12	$286\,x^{140}-173476592\,x^{135}-783432002592\,x^{130}-1386703609201664\,x^{125} -1784736108322304000\,x^{120}+194201414409112780800\,x^{115} +1337537876751441264640\,x^{110}+5775492980719979069440\,x^{105} -7021147505634053455872\,x^{100}+57054160389043482787840\,x^{95} +122144118606006006159769 60\,x^{90}+317003067049714264100044 80\,x^{85} +713362107399211871685836 80\,x^{80}+342110600164855061948661760\,x^{75} +118205708908664916289781760 0\,x^{70}+2075789928293154565138677760\,x^{65} +2009314878073796352991559680\,x^{60}+1241067977133844114943508480\,x^{55} +883346574302886168058920960\,x^{50}+1010816491486338401855078400\,x^{45} +835729572546537590127329280\,x^{40}+318007660009052542798397440\,x^{35} +46576321773027950476656640\,x^{30}+24818068249105075588300 80\,x^{25} -3860861088200921186304 00\,x^{20}+1088419419519773426319 36\,x^{15} +228894550341179985100 8\,x^{10}+13982776123059915980 8\,x^5+72057594037927936$

Table A.2: Division polynomials ψ_n for the curve $y^2=x^5+1$

B Example output of Algorithm 13

Polynomial	c	Class	w
$x^5+x^3+x^2+2$	2	A	1/2
$2x^5+2x^3+2x^2+1$	0	A	1/2
$x^5+x^3+x^2+x$	0	A	1/2
$2x^5+2x^3+2x^2+2x$	0	A	1/2
$x^5+x^3+x^2+x+1$	0	A	1/2
$2x^5+2x^3+2x^2+2x+2$	0	A	1/2
$x^5+x^3+x^2+x+2$	0	A	1/2
$2x^5+2x^3+2x^2+2x+1$	0	A	1/2
$x^5+x^3+x^2+2x$	0	A	1/2
$2x^5+2x^3+2x^2+x$	2	A	1/2
$x^5+x^3+x^2+2x+2$	0	A	1/2
$2x^5+2x^3+2x^2+x+1$	2	A	1/2
$2x^5+x^3+x^2+1$	2	A	1/2
$x^5+2x^3+2x^2+2$	0	A	1/2
$2x^5+x^3+x^2+x+1$	0	A	1/2
$x^5+2x^3+2x^2+2x+2$	2	A	1/2
$2x^5+x^3+x^2+x+2$	0	A	1/2
$x^5+2x^3+2x^2+2x+1$	2	A	1/2
$2x^5+x^3+x^2+2x$	0	A	1/2
$x^5+2x^3+2x^2+x$	0	A	1/2
$2x^5+x^3+x^2+2x+1$	0	A	1/2
$x^5+2x^3+2x^2+x+2$	0	A	1/2
$2x^5+x^3+x^2+2x+2$	0	A	1/2
$x^5+2x^3+2x^2+x+1$	0	A	1/2
x^5+x^2+x	0	B.1	1/2
$2x^5+2x^2+2x$	0	B.1	1/2
x^5+x^2+x+1	0	B.1	1/2
$2x^5+2x^2+2x+2$	0	B.1	1/2
x^5+x^2+x+2	0	B.1	1/2
$2x^5+2x^2+2x+1$	0	B.1	1/2
$2x^5+x^2+x$	0	B.1	1/2
x^5+2x^2+2x	2	B.1	1/2
$2x^5+x^2+x+1$	0	B.1	1/2
x^5+2x^2+2x+2	2	B.1	1/2
x^5+1	0	B.2	1/4
$2x^5+2$	0	B.2	1/4
x^5+x^2+1	2	B.2	1/4
$2x^5+2x^2+2$	0	B.2	1/4
x^5+2x^2+1	0	B.2	1/4
$2x^5+x^2+2$	2	B.2	1/4
$2x^5+1$	0	B.2	1/4
x^5+2	0	B.2	1/4
$2x^5+x^2+1$	2	B.2	1/4
x^5+2x^2+2	0	B.2	1/4
$2x^5+2x^2+1$	0	B.2	1/4
x^5+x^2+2	2	B.2	1/4
x^5+x^3+x+1	2	C.1	1/2
$2x^5+2x^3+2x+2$	2	C.1	1/2
$2x^5+x^3+x+1$	0	C.1	1/2
x^5+2x^3+2x+2	0	C.1	1/2
x^5+x^3+1	0	C.2	1/4
$2x^5+2x^3+2$	0	C.2	1/4
x^5+2x^3+1	0	C.2	1/4
$2x^5+x^3+2$	0	C.2	1/4
$2x^5+x^3+1$	0	C.2	1/4
x^5+2x^3+2	0	C.2	1/4
$2x^5+2x^3+1$	0	C.2	1/4
x^5+x^3+2	0	C.2	1/4
$2x^5+x^3+x$	0	C.3	1/2
$2x^5+2x^3+x$	0	C.3	1/2
$2x^5+x+1$	0	D.1	1/2
x^5+2x+2	0	D.1	1/2
x^5+1	0	D.2	1/4
$2x^5+2$	0	D.2	1/4
$2x^5+1$	0	D.2	1/4
x^5+2	0	D.2	1/4
x^5+x	2	D.3	1/2
$2x^5+x$	0	D.3	1/2

Table B.1: Output of algorithm 13 for $N=3, q=3$