Universitat de Lleida

Algorithms for l-sections on genus two curves over finite fields and applications

Edgardo Riquelme Faúndez

http://hdl.handle.net/10803/393881

ALGORITHMS FOR ℓ-SECTIONS ON GENUS TWO CURVES OVER FINITE FIELDS AND APPLICATIONS

EDGARDO RIQUELME

Instituto de Matemática y Física
Universidad de Talca, Chile.
Programa de Doctorat en Enginyeria i Tecnologies de la Informació.
Universitat de Lleida, Espanya.

Thesis adviser:
Steen Ryom-Hansen, University of Talca.
Jordi Pujolàs Boix, University of Lleida.
Nicolas Thériault, University of Santiago of Chile.

ALGORITHMS FOR ℓ-SECTIONS ON GENUS TWO CURVES OVER FINITE FIELDS AND APPLICATIONS

EDGARDO RIQUELME

A thesis submitted in partial fulfillment of
the requirements for the degree of
Doctor of Mathematics

Institute of Mathematics and Physics
University of Talca

Thesis adviser:
Steen Ryom-Hansen, University of Talca.
Jordi Pujolàs Boix, University of Lleida.
Nicolas Thériault, University of Santiago of Chile.

Contents

Agradecimientos

Quiero comenzar agradeciendo al Dr. Nicolas Thériault por su apoyo y guía para realizar esta tesis doctoral. Su ayuda no solamente ha sido importante en la dirección de este trabajo, sino también en mi formación como matemático e investigador. Agradezco su paciencia y buena disposición a responder mis dudas en relación a esta tesis. Su motivación en momentos importantes y su apoyo para realizar estancias internacionales. Además agradezco su ayuda en aspectos computacionales, en la redacción y el orden del contenido de esta tesis y por todas las sugerencias realizadas a este trabajo durante estos años.

Agradezco también al Dr. Jordi Pujolàs por su ayuda y apoyo durante mis estancias en España y en la dirección de este trabajo en general. Estoy agradecido de su buena disposición a la hora investigar y responder dudas sobre esta tesis. Agradezco también por ampliar de diversas maneras mi formación como investigador. Además agradezco toda su ayuda en aspectos computacionales, en redacción y por todas las sugerencias realizadas a este trabajo.

También quiero agradecer al grupo de investigación de Criptografía y Grafos de la Universidad de Lleida. En especial agradecer al Dr. Josep M. Miret por su ayuda y preocupación durante mis estancias en la Universidad de Lleida.

Agradezco a mi familia por su preocupación y apoyo en esta etapa de mi vida. Agradezco también por ser de gran importancia en mi formación como persona.

Gracias a mis compañeros y amigos que preguntaron por este trabajo. En especial mencionar a mis amigos del GBU de España y de la Iglesia Bautista de Lleida por su ayuda durante mis estancias en España y a mis amigos del GBU de Chile no solo por su preocupación en lo relacionado a mi tesis, sino por ser de gran importancia en mi paso por la universidad.

Finalmente como creyente quiero dar gracias a Dios pues a través de la fe he aprendido a valorar desde diferentes perspectivas mi carrera científica y a apreciar cada día de esta importante etapa de mi vida.

Abstract

We study ℓ-section algorithms for Jacobian of genus two over finite fields. We provide trisection (division by $\ell = 3$) algorithms for Jacobians of genus 2 curves over finite fields $\mathbb{F}_q$ of odd and even characteristic. In odd characteristic we obtain a symbolic trisection polynomial whose roots correspond (bijectively) to the set of trisections of the given divisor. We also construct a polynomial whose roots allow us to calculate the 3-torsion divisors. We show the relation between the rank of the 3-torsion subgroup and the factorization of this 3-torsion polynomial, and describe the factorization of the trisection polynomials in terms of the galois structure of the 3-torsion subgroup. We generalize these ideas and we determine the field of definition of an ℓ-section with $\ell \in \{3, 5, 7\}$. In characteristic two for non-supersingular hyperelliptic curves we characterize the 3-torsion divisors and provide a polynomial whose roots correspond to the set of trisections of the given divisor. We also present a generalization of the known algorithms for the computation of the 2-Sylow subgroup to the case of the ℓ-Sylow subgroup in general and we present explicit algorithms for the computation of the 3-Sylow subgroup. Finally we show some examples where we can obtain the central coefficients of the characteristic polynomial of the Frobenius endomorphism reduced modulo 3 using the generators obtained with the 3-Sylow algorithm.

This work was supported by CONICYT, Chile doctoral scholarship.

Resumen

En esta tesis se estudian algoritmos de ℓ-división para Jacobianas de curvas de género 2. Se presentan algoritmos de trisección (división por $\ell = 3$) para Jacobianas de curvas de género 2 definidas sobre cuerpos finitos $\mathbb{F}_q$ de característica par o impar indistintamente. En característica impar se obtiene explícitamente un polinomio de triseccón, cuyas raíces se corresponden biyectivamente con el conjunto de trisecciones de un divisor cualquiera de la Jacobiana. Asimismo se proporciona otro polinomio a partir de cuyas raíces se calcula el conjunto de los divisores de orden 3. Se muestra la relación entre el rango del subgrupo de 3-torsión y la factorización del polinomio de la 3-torsión, y se describe la factorización del polinomio de trisección en términos de las órbitas galoisianas de la 3-torsión. Se generalizan estas ideas para otros valores de ℓ y se determina el cuerpo de definición de una ℓ-sección para $\ell = 3, 5, 7$. Para curvas no-supersingulares en característica par también se da una caracterización de la 3-torsión y se proporciona un polinomio de trisección para un divisor cualquiera. Se da una generalización, para ℓ arbitraria, de los algoritmos conocidos para el cómputo explícito del subgrupo de 2-Sylow, y se detalla explícitamente el algoritmo para el cómputo del subgrupo de 3-Sylow. Finalmente, se dan ejemplos de cómo obtener los valores de la reducción módulo 3 de los coeficientes centrales del polinomio característico del endomorfismo de Frobenius mediante los generadores proporcionados por el algoritmo de cálculo del 3-Sylow.

Este trabajo fue financiado por una beca doctoral de CONICYT, Chile.

Resum

En aquesta tesi s'estudien algoritmes de ℓ-divisió per a grups de punts de Jacobianes de corbes de gènere 2. Es presenten algoritmes de trisecció (divisió per $\ell = 3$) per a Jacobianes de corbes de gènere 2 definides sobre cossos finits $\mathbb{F}_q$ de característica parell o senar indistintament. En característica parell s'obté explícitament un polinomi de trisecció, les arrels del qual estan en bijecció amb el conjunt de triseccions d'un divisor de la Jacobiana qualsevol. De manera semblant, es proporciona un altre polinomi amb les arrels del qual es calcula el conjunt dels divisors d'ordre 3. Es mostra la relació entre el rang del subgrup de 3-torsió i la factorització del polinomi de la 3-torsió, i es descriu la factorització del polinomi de trisecció en termes de les òrbites galoisianes de la 3-torsió. Es generalitzen aquestes idees a altres valors de ℓ i es determina el cos de definició d'una ℓ-secció per a $\ell = 3, 5, 7$. Per a corbes no-supersingulars en característica 2 també es proporciona una caracterització de la 3-torsió i un polinomi de trisecció per a un divisor qualsevol. Es dóna una generalització, per a ℓ arbitrària, dels algoritmes coneguts per al càlcul explícit del subgrup de 2-Sylow, i es detalla explícitament en el cas del 3-Sylow. Finalment es mostren exemples de com obtenir els valors de la reducció mòdul 3 dels coeficients centrals del polinomi característic de l'endomorfisme de Frobenius fent servir els generadors proporcionats per l'algoritme de càlcul del 3-Sylow.

CHAPTER 1

Introduction

The main reason to study ℓ-sections for genus 2 curves over finite fields resides in their application to Schoof-like algorithms in the computation of the group order of hyperelliptic Jacobians and the construction of secure random curves of genus 2 over prime fields. Efficient point counting algorithms in genus 2 were first studied by Kampkötter in 1991. Gaudry and Harley in 2000 presented examples for $p \cong 2^{16}$ where they started to use bisection algorithms ($\ell = 2$). Gaudry and Schost (2004) presented examples for $p \cong 2^{82}$, where they take advantadge of the 2-torsion subgroup to compute bisections and also begin to use trisection algorithms ($\ell = 3$). Gaudry and Schost in 2012 presented several improvents on Schoof-like algorithms with examples of cryptographic size $p \cong 2^{127}$. They used Kummer surfaces in the case of bisections, homotopy techniques for the trisection algorithms, and began to use ℓ-section for $\ell = 5, 7$. They also presented theoretical results for ℓ-sections for any ℓ.
On the other hand, alternative bisection techniques in even and odd characteristic have been obtained in [12, 14, 15] by reversing reduction in divisor class arithmetic. Trisection in characteristic two has also been studied in [17] in the supersingular case.

The general aim of this thesis is to study ℓ-section algorithms for any divisor in the Jacobian of the curve based in reversing the reduction step in divisor class arithmetic. The methods presented in this thesis are a generalization of the methods used in [12, 14, 15]. The particular objectives are the following: The first is to obtain ℓ-section polynomials which are completely consistent for small ℓ, focussing on the case of $\ell = 3$. The second objective is to study the factorization of ℓ-torsion polynomials. For elliptic (genus 1) curves, this was studied by Verdure [20]. For curves of genus 2 an analysis of the upper bound for the irreducible factors can be found in [11], and an application to the factorization types of ℓ-modular polynomials can be found in [9]. The methods we use are based on those in [9] but with significant variations to find the type of factorization of ℓ-torsion polynomial (the precise Galois orbits of the

ℓ-torsion divisors). The third objective is to establish the relationship between the type of factorization of the ℓ-torsion polynomial (the precise Galois orbits of the ℓ-torsion divisors) and the ℓ-section polynomial (the field of definition of the ℓ-sections). The fourth objective is to study the factorization of the ℓ-section polynomial in extensions of degree ℓ. The final objective is to study the impact on Schoof-like algorithms.

The structure of the thesis is as follows: In Chapter 2 we recall the necessary background on mathematics and cryptography. In Chapter 3 we study the first four objectives for fields of odd characteristic. We provide trisection (division by 3) algorithms for Jacobians of genus 2 curves over finite fields $\mathbb{F}_q$ of odd characteristic which rely on the factorization of a polynomial whose roots correspond (bijectively) to the set of trisections of the given divisor. We also construct a polynomial whose roots allow us to calculate the 3-torsion divisors. We show the relation between the rank of the 3-torsion subgroup and the factorization of this 3-torsion polynomial, and describe the factorization of the trisection polynomials in terms of the Galois structure of the 3-torsion subgroup. We also generalize these ideas for $\ell \in \{5, 7\}$. In Chapter 4 we studied part of the fifth objective, providing symbolic trisection polynomial for Jacobians of genus 2 curves over finite field $\mathbb{F}_q$ of odd characteristic. These polynomials can be used to improve the efficiency of trisection algorithms, which may then be used to obtain faster point counting algorithms. In Chapter 5 we study division by 3 in Jacobians of genus 2 curves over binary fields with a 2-torsion subgroup of rank 1 or 2. Finally, in Chapter 6 we study part of the fifth objective, presenting a generalization of the algorithms that explicitly determine the 2-power torsion of genus 2 curves over finite fields [16] to the case of ℓ-power torsion. We study the case of ℓ-power torsion in general and we present explicit algorithms for the computation of the 3-Sylow subgroup. These algorithms can be used to improve the choice of ℓ-torsion divisors of index ℓ^k used in Schoof-like algorithms.

The first four objectives studied in chapter 3 in the case of odd characteristic are part of *Trisection for genus 2 curves in odd characteristic*, published online (30 January 2016) in journal Applicable Algebra in Engineering Communication and Computing (AAECC).

The first four objectives in the case of characteristic two, studied in chapter 5, are part of *Trisection for non-supersingular genus 2 curves in characteristic 2* published online (06 Jul 2015) in International Journal of Computer Mathematics.

The fifth objective is studied in chapters 4 and 6. Chapter 4 is part of the paper *Symbolic trisection polynomials for genus 2 curves in odd characteristic* (preprint).

CHAPTER 2

Mathematical and Cryptographic Background

2.1 Background

Definition 1. *Let C be a genus two curve over finite field $\mathbb{F}_q$ given in the model.*

$$C : y^2 + h(x)y = f(x). \tag{2.1.1}$$

Curve C is called a nonsingular hyperelliptic curve of genus 2 over $\mathbb{F}_q$ if no point on the curve over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ satisfies both partial derivatives $2y + h(x) = 0$ and $f'(x) - h'(x)y = 0$ at the same time.

Definition 2. *A **divisor** on C is a finite formal sum of points on C*

$$D = \sum_{P \in C} m_p P$$

where $m_p \in \mathbb{Z}$ are 0 for all but finitely many P. The degree of D is defined by $\sum_{P \in C} m_p$. We denote Div^0 the set of all degree zero divisors of C.

If

$$\mathbb{F}[C] = \frac{\mathbb{F}[x, y]}{(y^2 + h(x)y - f(x))}$$

denotes the coordinate ring of C over $\mathbb{F}$, then the field of fractions $\mathbb{F}(C)$ is called the function field of C over $\mathbb{F}$.

Definition 3. *A divisor D is called a **principal** divisor if*

$$D = div(R) = \sum_{P \in C} (ord_p(R))P$$

for a non-zero rational function R in $\mathbb{F}(C)$.

Definition 4. *The quotient group $J = Div^0/P$ is called **Jacobian** of C, where P is the set of all pincipal divisor in Div^0.*

A divisor **semi-reducido** D is a divisor of the form $D = \sum m_i P_i - (\sum m_i) \infty$ with $P_i = (x_i, y_i)$ where

- $m_i \geq 0 \ \forall \ i$.

- if $(x_i, y_i) = (x_j, -y_j)$ and $m_i > 0$, then $m_j = 0$

- if $(x_i, y_i) = (x_i, -y_i)$ and $m_i > 0$, then $m_i = 1$

A semi-reduced divisor D is called reduced, if D satisfies $\sum m_i \leq g$ (g is the genus of C) . We will call $\sum m_i$ the weight of D.

Theorem 1. *(Mumford respresentation)*

- *For each point $P \in C(\overline{\mathbb{F}}_q)$ we associate a divisor $D(P) = P - \infty$*

- *All reduced divisors $D = \sum_{i=1}^{k} D(P_i)$ can be represented by an unique pair of polynomials $[u, v]$ such that $u, v \in \overline{\mathbb{F}_q}[x]$ with $u(x) = \prod_{i=1}^{k}(x - x_i)$ y $v(x_i) = y_i \ \forall i$ such that the degree of $v(x) <$ degree of $u(x) \leq g$ and $u(x)$ divide $v(x)^2 + h(x)v(x) - f(x)$, and all such pairs of polynomial represent a reduced divisor D.*

- *A divisor $D = [u(x), v(x)]$ is in $Jac(C)(\mathbb{F}_q)$ if only if $u(x), v(x) \in \mathbb{F}_q[x]$*

We work in the group of $\mathbb{F}_q$-points of the Jacobian Jac(C), in terms of the Mumford coordinates $[u(x), v(x)]$. In genus 2, every element in $Jac(C) - \{0\}$ can be represented by reduced divisors of weight one $[x + u_0, v_0]$ or two $[x^2 + u_1 x + u_0,\ v_1 x + v_0]$ (we refer to the degree of the effective divisor associated to D as its weight). An algorithm due to Cantor [3] allows us to compute in the divisor class group with this representation of elements. It works in two steps: a "composition" and "reduction".

Algorithm 1 Composition

```
Require: Reduced divisors $[u_1(x), v_1(x)]$ and $[u_2(x), v_2(x)]$.
Ensure: Semi-reduced divisor $[u(x), v(x)]$.
$d(x) = gcd(u_1(x), u_2(x), v_1(x) + v_2(x) + h(x))$,
    $d(x) = s_1(x)u_1(x) + s_2(x)u_2(x) + s_3(x)(v_1(x) + v_2(x) + h(x))$
$u(x) = u_1(x)u_2(x)/d(x)^2$
$v(x)$ is the remainder of
    $$\frac{s_1(x)u_1(x)v_2(x) + s_2(x)u_2(x)v_1(x) + s_3(x)(v_1(x)v_2(x) + f(x))}{d(x)}$$
    modulo $u(x)$
```

Cantor's general reduction step uses $\alpha, \beta, \gamma \in \mathbb{F}_q[x]$ such that $\beta = \gamma u + \alpha v$ with $deg(\beta) \leq \frac{m+2}{2}$ and $deg(\alpha) \leq \frac{m-3}{2}$, where m is $deg(u(x))$

Algorithm 2 Reduction

```
Require: Semi-reduced divisor $D = [u(x), v(x)]$.
Ensure: Reduced divisor $D'$ equivalent to $D$.
Use the extended Euclidean algorithm on $u, v$ to find $\alpha, \beta, \gamma \in \mathbb{F}[x]$ with degrees given above and such that $\beta = \gamma u + \alpha v$
Let $u_2 = \gcd(\beta, \alpha) = \gcd(u, \alpha)$ and compute $u_1 = \frac{u}{u_2}$,$\beta_1 = \frac{\beta}{u_2}$, $\alpha_1 = \frac{\alpha}{u_2}$
Let $u_3 = \frac{\beta_1^2+\alpha_1\beta_1 h+\alpha_1^2 f}{u_1}$ and compute $\alpha'$ such that $\alpha_1\alpha' \equiv 1 \bmod u_3$
(From which $v_3 = -\alpha'\beta_1 - h \bmod u_3$)
Finally, use the composition algorithm to compute the divisor sum $D'$ of $[u_3, v_3]$ and $[u_2, v]$
```

Theorem 2. *Let C be a hyperelliptic curve defined over $\mathbb{F}$. If the characteristic of $\mathbb{F}$ is either zero or a prime p with $\gcd(n, p) = 1$ then the set of n-torsion elements satifies*

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

If the characteristic is p and $n = p^e$ then

$$Jac(C)[p^e] \cong (\mathbb{Z}/p^e\mathbb{Z})^r$$

with $0 \leq r \leq g$, fixed for all $e \geq 1$.

Definition 5. *We call ℓ-sections the set of pre-images $D = [u, v] \in Jac(C)(\mathbb{F}_q)$ of any given divisor $D_\ell = [u_\ell, v_\ell]$ under the multiplication by ℓ map*

$$\begin{array}{rcl} [\ell] : Jac(C)(\mathbb{F}_q) & \rightarrow & Jac(C)(\mathbb{F}_q) \\ D & \rightarrow & D_\ell = \ell D. \end{array}$$

2.2 Cryptographic motivation

Suppose that Alice and Bob want to communicate a secret through an insecure channel of communication (like the internet) and they do not want Eve to understand the communication, even trough she may be able to record to copy of the transmission. They must encrypt each message, transmit the result and then decrypt. The method used to encrypt and decrypt is called a cryptosystem. There are many very efficient system if Alice and Bob have an common secret, called "private key system". The mayor problem with the private key system is the distribution of the key, sometimes is not convenient for Alice and Bob to meet in person to exchange a secret before each communication.

In 1976, Whitfield Diffie and Martin Hellman published the paper "New Directions in Cryptography" proposed a new method for the distribution of encryption keys.

Definition 6. ***The computational Diffie-Hellmann problem (CDH).*** *Let G be a group. Given g, g^x and g^y in G , deduce the value of g^{xy}.*

Except in some very special cases, the only known approach to solving the CDH goes through the solution of the Discrete Logarithm Problem (DLP)

Definition 7. *Let G be a group. Given $g \in G$ and $h \in < g >$, find $k \in \mathbb{Z}$ such that $h = g^k$.*

The DLP in $G =< g >$ can be computed easily if the order of g has only small factors. If we assume n composite and let $p|n$. If $[t]g = h$ we have that $[t \bmod p]\frac{n}{p}g = [\frac{n}{p}]h$. Then t modulo each of the primes such that $p|n$ can be found by solving the DLP in a cyclic group of order p. If n is a product of distinct primes, then t can be recovered using the Chinese remainder theorem. If n is not squarefree, the p-adic expansion can be used to compute t modulo the highest power of p dividing n for all primes p. This was first observed by Silver, Pohlig, and Hellman. Thus the complexity of computing discrete logarithms in a group of composite order n is bounded from above by the complexity of solving the DLP in a group whose order is the largest prime factor of n. Then algorithms as either Pollards rho or Baby-step giant-step can be used to solve the DLP in this group.

Therefore in the case of Jacobian of the genus two curves we must examine the possible group orders that can occur in the interval of Hasse-Weil. For these reason, if we want to know if the Jacobian of the genus two curves can be considered computationally secures we have to calculate the order of group.

2.3 Schoof-like algorithms and ℓ-sections

We denote by π to the q-th power Frobenius automorphism $\pi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ extended to the Jacobian.

Theorem 3. *Let C by a hyperelliptic curve of genus g defined over $\mathbb{F}_q$. The Frobenius endomorphism satisfies a characteristic polynomial of degree $2g$ given by*

$$\chi(T) = T^{2g} + s_1 T^{2g-1} + \ldots + s_g T^g + \ldots + s_1 q^{g-1} T + q^g$$

where $s_i \in \mathbb{Z}$, $1 \leq i < g$. The absolute value of the j-th coefficient of $\chi(T)$ is bounded by $\binom{2g}{j} q^{\frac{2g-j}{2}}$

Proposition 1. *For n coprime to q the restriction of ϕ_q to $\mathrm{Jac}(C)[n]$ has characteristic polynomial $\chi(T) \mod n$.*

In genus 2 the characteristic polynomial has the form

$$\chi(T) = T^4 - s_1 T^3 + s_2 T^2 - q s_1 T + q^2$$

and the absolute value of s_1 and s_2 satisfied $|s_1| \leq 4\sqrt{q}$ and $|s_2| \leq 6q$. The bound on s_2 can be refined to $2|s_1|\sqrt{p} - 2p \leq s_2 \leq \frac{s_1^2}{4} + 2p$.
Since $|\mathrm{Jac}(\mathbb{F}_q)| = \chi(1)$ computing s_1 and s_2 allows to obtain $\#\mathrm{Jac}(\mathbb{F}_q)$.
Sketch of a genus 2 Schoof algorithm

1. For sufficiently many small primes:
   - Construct ℓ-torsion divisors D_ℓ.
   - Eliminate those elements $(s_1, s_2) \bmod \ell$ such that

     $$\pi^4(D_\ell) + [p^2 \bmod \ell]D_\ell - [s_1 \bmod \ell](\pi^3(D_\ell) - [p \bmod \ell]\pi(D_\ell)) \\ \neq [s_2 \bmod \ell]\pi^2(D_\ell).$$

   - Deduce $(s_1, s_2) \bmod \ell$ from the remaining pair.
2. Deduce (s_1, s_2) from the pairs $(s_1, s_2) \bmod \ell$ by Chinese remaindering.

The relation between ℓ-sections and Schoof-like algorithms for points counting is studied by Gaudry and Schost in the case of absolutely simple varieties. They show that

Lemma 1. *(Gaudry-Schost 2012) There exists an integer $\kappa \geq 0$ such that for any $k > \kappa$, , the equality*

$$\pi^4(P_k) - [s_1]\pi^3(P_k) + [s_2]\pi^2(P_k) - [ps_1]\pi(P_k) + [p^2](P_k) = 0$$

uniquely determines (s_1, s_2) modulo $\ell^{k-\kappa}$.

where κ is related to the following properties

Lemma 2. *(Gaudry-Schost 2012) There exists an integer $k_0 \geq 1$ and $P \in \mathrm{Jac}(C)[\ell^{k_0}]$ such that $\mathrm{Jac}(C)[\ell]$ is contained in the subgroup generated by P and its conjugates.*

Lemma 3. *(Gaudry-Schost 2012) Let $k_0 \geq 1$ and let $P \in \mathrm{Jac}(C)$ be such that $\mathrm{Jac}(C)[\ell^k]$ is contained in the subgroup generated by P and its conjugates. Then for any $Q \in \mathrm{Jac}$ such that $P = [\ell]Q$, $\mathrm{Jac}(C)[\ell^{k+1}]$ is contained in the subgroup generated by Q and its conjugates.*

They also study of the field of definition of P_k

Lemma 4. *Let d be a positive integer such that the points of $\mathrm{Jac}(C)[\ell]$ are defined over $\mathbb{F}_{p^d}$, and let $P \in \mathrm{Jac}$ be defined over $\mathbb{F}_{p^d}$ as well. Then any $Q \in \mathrm{Jac}(C)$ such that $P = [\ell]Q$ is defined over $\mathbb{F}_{p^{\ell d}}$.*

Lemma 5. *For $k \geq 1$, let d_k be the smallest integer such that the points of $\mathrm{Jac}[\ell^k]$ are defined over $\mathbb{F}_{p^{d_k}}$. Then for k large enough, we have $d_{k+1} = \ell d_k$.*

The importance of these results is that if we want to obtain for example the values of s_1 for a curve over a field $\mathbb{F}_q$ of order around 2^{120}. We need to get s_1 mod $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots 47 \cdot 53 > 4\sqrt{q}$. . On the other hand using ℓ-section for $\ell = 2, 3$ we need to get s_1 mod $2^{17} \cdot 3^7 \cdot 5 \cdot 7 \cdot 11 \cdots 29 \cdot 31 > 4\sqrt{q}$. (The approach of Gaudry-Schost (2012) to obtain $\ell = 31$ requires about 10 CPU days and to obtain 2^{17} requires about 5 CPU days).

CHAPTER 3

Trisection in odd characteristic

Trisection algorithms for genus 2 curves over finite fields in odd characteristic have been used by Gaudry and Schost in [7] and [8]. The main interest of these algorithms resides in their application in Schoof-like algorithms to compute the group order of the Jacobian of genus 2 curves. The aim of this chapter is to present alternative algorithms for trisecting any divisor in the Jacobian of the curve based in reversing reduction in divisor class arithmetic. The methods presented in this chapter are loosely based on those used in [15] to find bisections, but with significant variations that are required to deal with the added complexity coming from the size of the system to solve. Trisections in characteristic 2 have been considered in [17] and [18].

Our methods produce two polynomials associated to divisors of 3-torsion (general for the curve) and trisections of a specific divisor. The first has degree 80 and its roots can be used to produce the 3-torsion divisors, whereas the second has degree 81 in general and its roots can be used to produce the preimages of multiplication-by-3 for the given divisor. Note that in both cases, any unwanted roots ("false positives") are removed explicitly from the polynomial. We also show the relation between the possible factorization types of these two polynomials (3-torsion and trisection), which can be used to specialize the factorization technique used in the trisection algorithm.

The structure of the rest of the chapter is as follows: in Section 3.1, we recall generalities about genus 2 curves in odd characteristic. In Section 3.2 we present the basic algorithms that will be used in the construction of the trisection algorithm. In Section 3.3, we construct a polynomial of degree 80 whose roots allow us to calculate the 3-torsion divisors. In Sections 3.4 and 3.5 we provide a constructive method to find trisections of any divisor from the roots of certain polynomials of degree 81. In Section 3.6 we show how we can remove parasitic factors ("false positives") by explaining how they appeared. In Section 3.7 we give a classification of the rank of the 3-torsion subgroup in terms of the factorization of the 3-torsion polynomial and we describe the factorization of our trisection polynomials in terms of the Galois structure of the 3-torsion subgroup. We also generalize these ideas for $\ell \in \{5, 7\}$.

3.1 Generalities

Let C be a non-singular genus 2 curve over a finite field $\mathbb{F}_q$ of odd characteristic greater than 5 given in the model

$$\mathrm{C} : y^2 = f(x) \tag{3.1.1}$$

where $f(x) = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{F}_q[x]$ has no multiple roots.

We work in the group of $\mathbb{F}_q$-points of the Jacobian Jac(C), in terms of Mumford coordinates $[u(x), v(x)]$ corresponding to the ideal generated by $u(x)$ and $y - v(x)$ in the ideal class group. In genus 2, every element in $\mathrm{Jac(C)} - \{0\}$ can be represented by reduced divisors of weight one $[x + u_0, v_0]$ or two $[x^2 + u_1x + u_0,\ v_1x + v_0]$ (we refer to the degree of the effective divisor associated to D as its weight). An algorithm due to Cantor [3] allows us to compute in the group with this representation of elements of Jac(C). Cantor's group operation algorithm works in two steps: composition and reduction.

Algorithm 3 Composition

```
Require: $D_1 = [u_1(x), v_1(x)]$ and $D_2 = [u_2(x), v_2(x)]$, semireduced divisors.
Ensure: A semireduced divisor $D = [u(x), v(x)]$ equivalent to $D_1 + D_2$.
1: Use the Euclidean algorithm to compute $d = \gcd(u_1, u_2, v_1 + v_2)$, with
   $d = s_1u_1 + s_2u_2 + s_3(v_1 + v_2)$
2: Set $u = u_1u_2/d^2$
3: Set $v(x)$ as the remainder of $\dfrac{s_1u_1v_2 + s_2u_2v_1 + s_3(v_1v_2 + f)}{d}$ mod $u$
```

The reduction step of Cantor's algorithm [3] consists in the transformation of a semireduced divisor (with unreduced coordinates) into a reduced divisor. Let D be a semireduced divisor represented by $D = [\widetilde{u}(x), \widetilde{v}(x)]$ with $m = \deg(\widetilde{u}(x))$. Cantor gives two versions of the reduction step. The first one uses direct operation which, after a number of repetitions, outputs a reduced divisor. The second version of Cantor's reduction algorithm works via a single reduction step. Both versions are equivalent (as they produce the same reduced divisor). The first is often preferred in practice due to its simplicity (and lower complexity for small genera), but the second reduction approach is more useful in our context. It applies if there exist $\beta, \alpha, \gamma \in \mathbb{F}[x]$ such that $\beta = \gamma\widetilde{u} + \alpha\widetilde{v}$, where $\deg(\beta) \leq (m + g)/2$ and $\deg(\alpha) \leq (m - g - 1)/2$ with $m = deg(\tilde{u}(x))$, and such that $\gcd(\gamma, \alpha) = 1$. For $g = 2$, this gives the following algorithm:

Algorithm 4 Reduction

```
Require: $D = [\widetilde{u}(x),\ \widetilde{v}(x)]$, a semireduced divisor.
Ensure: A reduced divisor $E$ equivalent to $D$.
1: Use a partial Euclidean algorithm to obtain $\beta, \alpha, \gamma \in \mathbb{F}[x]$
   such that $\beta = \gamma\widetilde{u} + \alpha\widetilde{v}$, with $\deg(\beta) \leq (m+2)/2$
   and $\deg(\alpha) \leq (m-3)/2$ with $m = deg(\tilde{u}(x))$
2: Set $\widehat{u} = \gcd(\beta, \alpha) = \gcd(\widetilde{u}, \alpha)$ and define $\overline{u} = \widetilde{u}/\widehat{u}, \overline{\beta} = \beta/\widehat{u}$,
   and $\overline{\alpha} = \alpha/\widehat{u}$
3: Set $u = \dfrac{\overline{\beta}^2 - \overline{\alpha}^2 f}{\overline{u}}$ and compute $\overline{\alpha}^{-1}$ such that $\overline{\alpha}^{-1} \cdot \overline{\alpha} \equiv 1 \bmod u$
4: $E$ is COMPOSITION of $E_1 = \mathrm{div}(u, -\overline{\alpha}^{-1}\overline{\beta})$ and $E_2 = \mathrm{div}(\widehat{u}, v)$
   (note that $E_2$ is the divisor zero when $\widehat{u} = 1$ in Step 2)
```

We define the *trisections* of a given divisor $D_3 = [u_3(x), v_3(x)]$ as the set of pre-images $D = [u(x), v(x)] \in \mathrm{Jac(C)}(\mathbb{F}_q)$ under the multiplication by 3 map

$$\begin{aligned} [3] : \mathrm{Jac(C)}(\mathbb{F}_q) &\to \mathrm{Jac(C)}(\mathbb{F}_q) \\ D &\to D_3 = 3D. \end{aligned}$$

3.2 Basic Algorithms

In this section we present a generalization of the technique of *de-reduction* used in [15] which consists in searching for the linear polynomial involved in the reduction part of the addition law. The basic idea consists in reversing the reduction step of Cantor's algorithm to find (all) the semireduced divisors in the class of D_3 which are the direct composition of a reduced divisor with itself (in the case of bisections). To apply this idea to trisections, the main difference is that we want the de-reduced divisor to be the composition of 3 copies of a reduced divisor. In practice, when computing $3D$ it would be natural to use twice the "simple" recursive reduction step (reduction via principal divisors of the form $y - v(x)$) to fully reduce $3D$. When the weight of the semireduced divisor is somewhat small, this version of the reduction is usually more efficient in direct computations, but when computing trisections, the two layers of de-reduction produce systems that are a little more difficult to solve.

Algorithm REDUCTION transforms unreduced coordinates $[\widetilde{u}(x), \widetilde{v}(x)]$ to obtain a reduced divisor $D = [u(x), v(x)]$. Our method consists in reversing REDUCTION, working mostly on Step (iii), to obtain an unreduced divisor of a specific form. For this, we suppose the general case $\gcd(\widetilde{u}(x), \alpha(x)) = 1$ in Step (ii) (otherwise see Section 3.6). Hence the coordinates $[\widetilde{u}(x), \widetilde{v}(x)]$ in Step (iii) satisfy

$$u(x) = \epsilon \frac{\beta(x)^2 - \alpha(x)^2 f(x)}{\widetilde{u}(x)},$$

(with $\epsilon \in \mathbb{F}_q^\times$ to equate leading coefficients), and Step (iv) returns $E = E_1$.

Starting from the coordinates $[u(x), v(x)]$ of D with $\beta = \gamma u + \alpha v$, we re-write this equation as

$$\begin{aligned} \epsilon \cdot \widetilde{u} &= \frac{\beta^2 - \alpha^2 f}{u} \\ &= \gamma^2 \cdot u + \gamma\alpha \cdot 2v + \alpha^2 \cdot \frac{v^2 - f}{u} \quad , \end{aligned} \tag{3.2.1}$$

which we use to compute the de-reduction. Recall that the division $\frac{v^2-f}{u}$ is exact since $D = [u(x), v(x)]$ is a divisor (the divisibility condition is part of Mumford's representation).

The following part of the method holds for an arbitrary natural n. Starting with the coordinates $[u(x), v(x)] = [u_n(x), v_n(x)]$ of D_n, we want to obtain the coordinates $[\widetilde{u}(x), \widetilde{v}(x)] = [u_1^n(x), ...]$ of the "de-reduced" divisor nD_1 (the unreduced composition of n copies of $D_1 = [u_1(x), v_1(x)]$). To determine the required degrees for α and γ, we consider the parity of the degrees on both sides of the equality, taking into account both u_1 and u_n should be monic of degree at most 2 since they are coordinates of (proper reduced) divisors. Hence $\deg(v_n) < \deg(u_n) \leq 2$ and $\deg((v_n^2 - f)/u_n) = 5 - \deg(u_n) > 3$, so the leading term on the left-hand side comes from the term in γ^2 or α^2 depending on the degree on the left-hand side. Furthermore, either $\alpha(x)$ or $\gamma(x)$ can be made monic if we require that $\epsilon = \pm 1$ (since $u(x)$, $\widetilde{u}(x)$ and $f(x)$ are monic). The correct combinations of $\deg(\alpha)$, $\deg(\gamma)$ and ϵ can be summarized in the following table:

$n\deg(u_1)$	$\deg(u_n)$	$\deg(\alpha)$	$\deg(\gamma)$	monic	ϵ
even	2	$\leq \frac{n\deg u_1 - 2}{2}$	$\frac{n\deg(u_1) - 2}{2}$	γ	1
even	1	$\frac{n\deg u_1 - 4}{2}$	$\leq \frac{n\deg(u_1) - 3}{2}$	α	-1
odd	2	$\frac{n\deg u_1 - 3}{2}$	$\leq \frac{n\deg(u_1) - 3}{2}$	α	-1
odd	1	$\leq \frac{n\deg u_1 - 5}{2}$	$\frac{n\deg(u_1) - 1}{2}$	γ	1

It is possible that $u_n(x) = u_1(x)$ (see Section 3.3), and both must be obtained during the de-reduction, but in general $u_n(x)$ is known and $u_1(x)$ is unknown. Algorithm 5 below summarizes the whole process.

In this way, we turn the reduction step in Cantor's algorithm into a polynomial system. If the solution of this system satisfies $\gcd(u_1, \alpha) \neq 1$, we do not compute α^{-1} and we must find v_1 in other form (see Example 3 in Section 3.6). We call *general de-reduction* method that undoes one-step-reduction in Cantor's algorithm. Note that de-reduction always looks for an unreduced divisor of a very specific form. Otherwise there would be infinitely many solutions.

The tool to solve our polynomial system will be the resultant. Let p_1 and p_2 be two polynomials in several variables. We denote $\mathrm{Res}_x(p_1, p_2)$ the resultant with respect to a variable x.

Algorithm 5 De-reduction

```
Require: Values of $n$, $\deg(u_1)$, $\deg(u_n)$, and $D_n$ (if it is fixed).
Ensure: A reduced divisor $D_1$ such that $nD_1$ is equivalent to $D_n$
        (if $D_n$ is not fixed, consider $D_n = -D_1$).
1: Determine the degrees of $\alpha(x)$ and $\gamma(x)$, which one is monic and $\epsilon$ using the previous table
2: Set the coefficients of $u_1(x)$, $v_1(x)$, $\alpha(x)$ and $\gamma(x)$ as unknowns
3: If $D_n = [u_n(x), v_n(x)]$ is known, use its coefficients as fixed values, otherwise set $u_n(x) = u_1(x)$ and $v_n(x) = -v_1(x)$
4: Compute (symbolically) the left-hand side $\epsilon \cdot u_1(x)^n$
5: Compute (symbolically) the right-hand side
       $$\gamma^2 \cdot u_n + \gamma\alpha \cdot 2v_n + \alpha^2 \cdot \frac{v_n^2 - f}{u_n}$$
6: Equate both sides, matching the different powers of $x$
7: Solve the resulting system
```

3.3 Computing 3-torsion divisors

To compute divisors of order 3, we look for divisors satisfying the equation $2D \equiv -D$. This avoids having to work directly with the class 0. We know that (non-zero) 3-torsion divisors must have weight 2, otherwise there would exist a principal divisor whose affine support consists of exactly 3 points, but if the genus of C is at least 2, such a divisor cannot be principal. Thus a divisor D of order 3 is of the form $[u(x), v(x)] = [x^2+u_1x+u_0, v_1x+v_0]$ with $v^2-f = 0 \bmod u$. Using COMPOSITION we obtain unreduced coordinates of the form $[u^2, \tilde{v}]$ for $2D$. On the other hand, $-D = [u(x), -v(x)]$, which we de-reduce using the intersection between $y^2 - f(x)$ and $\alpha(x)y - \beta(x)$. Then $\beta(x)^2 - \alpha(x)^2 f(x) = 0 \bmod u(x)$ follows, and (3.2.1) becomes the polynomial identity

$$u^2 = \frac{(\gamma u - \alpha v)^2 - \alpha^2 f}{u} = \gamma^2 u - 2\alpha\gamma v + \alpha^2 \left(\frac{v^2 - f}{u}\right). \tag{3.3.1}$$

By matching degrees, the only possibility is $\beta(x) = \gamma(x)u(x) + \alpha(x)(-v(x))$, $\gamma = x + c_0$ and $\alpha = a_0$ (assumed non-zero since in the intersection we cannot contain $\alpha(x)$).

Matching coefficients we obtain 4 equations in 6 unknowns (u_1, u_0, v_1, v_0, c_0 and a_0). The divisibility condition $v^2 - f = 0 \bmod u$ gives us two more equations. All together we find the following set of equations:

$$0 = -u_1 + 2c_0 - a_0^2 \tag{3.3.2}$$

$$0 = 2c_0u_1 - 2a_0v_1 + a_0^2u_1 - u_0 + c_0^2 - u_1^2 \tag{3.3.3}$$

$$\begin{aligned}0 = & -2a_0c_0v_1 - 2u_1u_0 - 2a_0v_0 - a_0^2u_1^2 + 2c_0u_0 + c_0^2u_1 \\ & + a_0^2u_0 - a_0^2f_3 \qquad (3.3.4)\\ 0 = & -u_0^2 + a_0^2u_1f_3 - 2a_0^2u_1u_0 - 2a_0c_0v_0 + c_0^2u_0 + a_0^2v_1^2 \\ & - a_0^2f_2 + a_0^2u_1^3 \qquad (3.3.5)\\ 0 = & -u_1^2f_3 - f_1 + 3u_0u_1^2 + u_0f_3 - u_0^2 - u_1^4 + 2v_1v_0 + u_1f_2 - u_1v_1^2. \qquad (3.3.6)\\ 0 = & \, u_0f_2 - f_0 - u_0u_1f_3 + 2u_0^2u_1 + v_0^2 - u_0u_1^3 - u_0v_1^2. \qquad (3.3.7)\end{aligned}$$

From (3.3.2), we can write u_1 in terms of a_0 and c_0:

$$u_1 = 2c_0 - a_0^2. \qquad (3.3.8)$$

(3.3.3) and (3.3.4) can then be used to write u_0 and v_0 in terms of a_0, c_0 and v_1:

$$\begin{aligned}u_0 =& c_0^2 + 4c_0a_0^2 - 2a_0v_1 - 2a_0^4, \qquad (3.3.9)\\ v_0 =& c_0v_1 - 5c_0^2a_0 + 10c_0a_0^3 - 3a_0^2v_1 - \frac{7}{2}a_0^5 - \frac{1}{2}a_0f_3. \qquad (3.3.10)\end{aligned}$$

Substituting identities (3.3.8),(3.3.9) and (3.3.10) into (3.3.5), (3.3.6), (3.3.7) gives us polynomials E_1, E_2 and E_3 of degree 2, 2 and 3 in v_1 respectively. We then compute $r_1 = \mathrm{Res}_{v_1}(E_1, E_2)$, $r_2 = \mathrm{Res}_{v_1}(E_1, E_3)$, $r_3 = \mathrm{Res}_{v_1}(E_2, E_3)$. From r_1, r_2 and r_3 we can remove trivial factors of a_0. We then compute $R_1 = \mathrm{Res}_{c_0}(r_1, r_2)$ and $R_2 = \mathrm{Res}_{c_0}(r_1, r_3)$. Finally $T(a_0) = \gcd(R_1, R_2)$ has degree 80 in a_0. These computations can be performed symbolically in the ring $\mathbb{Z}[f_3, f_2, f_1, f_0, v_1, v_0, u_1, u_0, a_0]$.

Proposition 2. *For any genus 2 curve* C *as in (3.1.1), the polynomial* $T(a_0)$ *in* $\mathbb{F}_q[a_0]$ *obtained above has* 80 *non-zero roots in* $\overline{\mathbb{F}_q}$ *(counted with multiplicity).*

Proof: $T(a_0)$ is monic of degree 80 and has constant term $2^{16}3^{12}\mathrm{Res}_x^2(f, f')$. Since C is nonsingular, we must have $\mathrm{Res}_x^2(f, f') \neq 0$. Hence none of the roots can be zero. □

See [21] for a MAGMA function to compute the 3-torsion.

3.4 Weight-2 trisections

In this section we explain how to find, for any given weight-2 divisor D_3, those divisors D_1 such that $3D_1 = D_3$. We assume that divisors D_1 and D_3 are of the form $[u_1(x), v_1(x)] = [x^2 + u_{11}x + u_{10}, v_{11}x + v_{10}]$, $[u_3(x), v_3(x)] = [x^2 + u_{31}x + u_{30}, v_{31}x + v_{30}]$ since this is the general case. We consider weight 1 divisors D_3 in Section 3.5, and we forget about trisections D_1 of weight 1 since they are easily found from those of weight 2 and the 3-torsion subgroup.

After the composition step of Cantor's algorithm, we obtain divisors of the form $[u^3, \tilde{v}]$ for $3D_1$. We de-reduce as above and $\beta^2 - \alpha^2 f = 0 \bmod u_3$ follows.

As above, we obtain:

$$u_1^3 = \frac{(\gamma u_3 + \alpha v_3)^2 - \alpha^2 f}{u_3} = \gamma^2 u_3 + 2\alpha\gamma v_3 + \alpha^2 \left(\frac{v_3^2 - f}{u_3} \right) \tag{3.4.1}$$

and then similarly $\beta = \gamma u_3 + \alpha v_3$ with $\gamma = x^2 + c_1 x + c_0$ and $\alpha = a_1 x + a_0$ (here a_1 is assumed non-zero).

Matching coefficients we obtain 6 equations in 6 unknowns (u_{11}, u_{10}, c_1, c_0, a_1 and a_0):

$$0 = -\, a_1^2 + u_{31} + 2c_1 - 3u_{11} \tag{3.4.2}$$

$$\begin{aligned} 0 = &-\, 2a_1 a_0 + 2a_1 v_{31} + 2c_1 u_{31} + a_1^2 u_{31} + u_{30} + c_1^2 + 2c_0 \\ &- 3u_{10} - 3u_{11}^2 \end{aligned} \tag{3.4.3}$$

$$\begin{aligned} 0 = {} & c_1^2 u_{31} + 2a_0 v_{31} - a_1^2 f_3 - a_1^2 u_{31}^2 + 2c_1 c_0 - 6u_{11} u_{10} + 2c_0 u_{31} \\ &+ 2a_1 c_1 v_{31} + 2u_{30} c_1 + u_{30} a_1^2 - a_0^2 + 2v_{30} a_1 - u_{11}^3 + 2a_1 a_0 u_{31} \end{aligned} \tag{3.4.4}$$

$$\begin{aligned} 0 = &-\, a_1^2 f_2 + 2u_{30} a_1 a_0 - 2u_{30} a_1^2 u_{31} + a_0^2 u_{31} - 3u_{11}^2 u_{10} + a_1^2 u_{31}^3 \\ &+ a_1^2 v_{31}^2 + 2v_{30} a_1 c_1 - 2a_1 a_0 u_{31}^2 + a_1^2 u_{31} f_3 + 2a_0 c_1 v_{31} \\ &+ 2c_1 c_0 u_{31} + c_0^2 + 2v_{30} a_0 + 2u_{30} c_0 + u_{30} c_1^2 - 3u_{10}^2 \\ &+ 2a_1 c_0 v_{31} - 2a_1 a_0 f_3 \end{aligned} \tag{3.4.5}$$

$$\begin{aligned} 0 = {} & 2u_{30} c_1 c_0 - a_0^2 u_{31}^2 - a_0^2 f_3 + 2a_0 c_0 v_{31} + 2v_{30} a_1 c_0 - 3u_{11} u_{10}^2 \\ &+ c_0^2 u_{31} + 2v_{30} a_0 c_1 + 2a_1 a_0 u_{31} f_3 + 2a_1 a_0 u_{31}^3 + u_{30} a_0^2 \\ &+ 2a_1 a_0 v_{31}^2 - 4u_{30} a_1 a_0 u_{31} - 2a_1 a_0 f_2 \end{aligned} \tag{3.4.6}$$

$$\begin{aligned} 0 = {} & a_0^2 u_{31} f_3 + a_0^2 v_{31}^2 - a_0^2 f_2 - 2u_{30} a_0^2 u_{31} \\ &- u_{10}^3 + 2v_{30} a_0 c_0 + u_{30} c_0^2 + a_0^2 u_{31}^3. \end{aligned} \tag{3.4.7}$$

From (3.4.2) we can write u_{11} in terms of a_1 and c_1

$$u_{11} = \frac{2c_1 + u_{31} - a_1^2}{3}, \tag{3.4.8}$$

and then (3.4.3) can be used to write u_{10} in terms of a_1, c_1, a_0 and c_0:

$$\begin{aligned} u_{10} = {} & \frac{1}{9}(3u_{30} + 6v_{31} a_1 + 6c_0 - c_1^2 + 2u_{31} c_1 \\ &+ 5a_1^2 u_{31} - 6a_1 a_0 + 4c_1 a_1^2 - u_{31}^2 - a_1^4). \end{aligned} \tag{3.4.9}$$

In the general case we assume $-c_1 + u_{31} + 2a_1^2$ is nonzero. Then (3.4.4) can be used to write c_0 in terms of a_1, a_0 and c_1,

$$\begin{aligned} c_0 = {} & \frac{1}{-18c_1 + 18u_{31} + 36a_1^2}(-90a_1 a_0 u_{31} - 18u_{30} c_1 - 54v_{30} a_1 \\ &+ 18u_{30} u_{31} + 27a_0^2 + 3c_1^2 u_{31} - 33u_{31} a_1^4 + 27a_1^2 f_3 + 60a_1^2 u_{31}^2 \\ &- 5u_{31}^3 - 54v_{31} a_0 - 4c_1^3 - 45u_{30} a_1^2 + 5a_1^6 + 60c_1 a_1^2 u_{31} \\ &+ 42c_1^2 a_1^2 + 6c_1 u_{31}^2 - 30c_1 a_1^4 + 18c_1 v_{31} a_1 - 72c_1 a_1 a_0 \\ &+ 36u_{31} v_{31} a_1 - 36a_1^3 v_{31} + 36a_1^3 a_0). \end{aligned} \tag{3.4.10}$$

Substituting identities (3.4.8), (3.4.9) and (3.4.10) into (3.4.5), (3.4.6), (3.4.7) we obtain polynomials E_1, E_2 and E_3 of degrees 4, 4 and 6 in a_0 respectively. The coefficient of a_0^4 in (3.4.5) is a non-zero constant, so we can replace E_2 and E_3 by $\widetilde{E_2} = E_2 \bmod E_1$ and $\widetilde{E_3} = E_3 \bmod E_1$. We then compute $r_1 = \mathrm{Res}_{a_0}(E_1, \widetilde{E_2})$, $r_2 = \mathrm{Res}_{a_0}(E_1, \widetilde{E_3})$ and $r_3 = \mathrm{Res}_{a_0}(\widetilde{E_2}, \widetilde{E_3})$. From r_1, r_2 and r_3 we can remove unwanted factors of $-c_1 + u_{31} + 2a_1^2$, obtaining $\widetilde{r_1}, \widetilde{r_2}, \widetilde{r_3}$ (which can easily computed symbolically). Next we compute $R_1 = \mathrm{Res}_{c_1}(r_1, r_2)$, $R_2 = \mathrm{Res}_{c_1}(r_1, r_3)$ and then $G = \gcd(R_1, R_2)$. If we remove the trivial factors (in a_1) from G, we obtain a polynomial of degree 135 in a_1. Finally we can easily identify and remove from G three copies of a predictable factor $G_f(a_1)$ of degree 18 (for more details on this, see Section 3.6), obtaining in the end a polynomial $P(a_1)$ of degree 81. Our trisection algorithm for this case is the following:

Algorithm 6 Trisection (general case)

```
Require: $D_3 = [x^2 + u_{31}x + u_{30}, v_{31}x + v_{30}] \in \mathrm{Jac(C)}(\mathbb{F}_q)$.
Ensure: $D = [u_1(x), v_1(x)]$ such that $3D = D_3$.
Evaluate $\widetilde{r_i}$ in the coefficient of $f(x)$, $u_3(x)$, and $v_3(x)$
Compute $R_1$ and $R_2$
Compute $G(a_1) = \gcd(R_1, R_3)$
Compute $P(a_1) = G(a_1)/G_f(a_1)^3$
Find a root $A_1$ of $P(a_1)$
Compute $G_1(c_1) := \gcd(r_1(A_1, c_1), r_2(A_1, c_1))$
Find a root $C_1$ of $G_1(c_1)$
If $-C_1 + u_{31} + 2A_1^2 \neq 0$ compute
    $G_2(a_0) := \gcd(E_1(A_1, C_1, a_0), \widetilde{E_2}(A_1, C_1, a_0)), \widetilde{E_3}(A_1, C_1, a_0))$
Find a root $A_0$ of $G_2(a_0)$
Find $C_0$ replacing in (3.4.10)
Find $u_{11}, u_{10}$ replacing in (3.4.8), (3.4.9)
Find $v_1 = -\alpha^{-1}\beta \bmod u_1$
```

See [22] for a MAGMA function to compute trisections of divisors D_3 of weight 2.

Example 1. *Consider $p = 2^{160} - 47$ and the curve*

$$\mathrm{C} : y^2 = x^5 + 7x^3 + x^2 + x$$

over $\mathbb{F}_p$. For this curve, the factorization of the 3-torsion polynomial is of the form $(1)^2(2)^3(3)^2(6)^{11}$ and we obtain two 3-torsion divisors, $\pm D_3$, with

$$\begin{aligned} D_3 :=(x^2 &+ 931762944096586147279230027121070745020815857375x+ \\ &488873756787536501744810044052577766667795825339, \\ &1305126933853188150337554885652469543169375406912x+ \\ &507085985232638779600803004953929238989759913638). \end{aligned}$$

By successively applying the trisection algorithm from D_3, we obtain a divisor

$$\begin{aligned}D_{81} :=(&x^2 + 2193356622481333966545693197372081654587976654 41x+\\ &762120291454194142545198530846238796230952679247,\\ &245403343317120493492667348268584111024316847588x+\\ &1333409534098972462678370037821289793015805103806)\end{aligned}$$

of order 81*, which cannot be trisected further, so the 3-Sylow group is of the form* $\mathrm{Jac(C)}[3^\infty] = \langle D_{81}\rangle \equiv \mathbb{Z}_{3^4}$.

3.5 Weight-1 trisections

In this section we explain how to find, for any given divisor D_3 of weight-1, those divisors D_1 such that $3D_1 = D_3$. If we assume D_3 is of the form $D_3 = [u_3(x), v_3(x)] = [x + u_{30}, v_{30}]$ with $v_{30} \neq 0$ (i.e. the support of D_3 does not contain a Weierstrass point), then D_1 must have the form $[u_1(x), v_1(x)] = [x^2 + u_{11}x + u_{10}, v_{11}x + v_{10}]$. Similarly to Section 3.4 above, de-reduction yields the polynomial identity

$$u_1^3 = \frac{(\gamma u_3 + \alpha v_3)^2 - \alpha^2 f}{u_3} = \gamma^2 u_3 - 2\alpha\gamma v_3 + \alpha^2\left(\frac{v_3^2 - f}{u_3}\right). \tag{3.5.1}$$

with $\beta(x) = \gamma(x)u_3(x) + \alpha(x)v_3(x)$ and $\gamma(x) = c_2x^2 + c_1x + c_0$ (here c_2 is assumed non-zero) and $\alpha(x) = x + a_0$. Matching coefficients we obtain 6 equations in 6 unknowns (u_{11}, u_{10}, c_2, c_1, c_0 and a_0):

$$0 = c_2^2 + u_{30} - 2a_0 + 3u_{11} \tag{3.5.2}$$

$$0 = c_2^2u_{30} + 2c_2c_1 + 2a_0u_{30} - f_3 - u_{30}^2 - a_0^2 + 3u_{10} + 3u_{11}^2 \tag{3.5.3}$$

$$\begin{aligned}0 = {}&2c_2c_0 + 2v_{30}c_2 + u_{30}f_3 - 2a_0f_3 - 2a_0u_{30}^2 + a_0^2u_{30} + 6u_{11}u_{10}\\ &+ 2c_2c_1u_{30} + c_1^2 - f_2 + u_{30}^3 + u_{11}^3\end{aligned} \tag{3.5.4}$$

$$\begin{aligned}0 = {}&c_1^2u_{30} + 2c_1c_0 + 2v_{30}c_1 + u_{30}f_2 - u_{30}^2f_3 - 2f_2a_0 + 2a_0u_{30}^3\\ &- a_0^2f_3 - a_0^2u_{30}^2 + 3u_{11}^2u_{10} + 2c_2c_0u_{30} + 2v_{30}a_0c_2\\ &+ 2a_0u_{30}f_3 - f_1 - u_{30}^4 + 3u_{10}^2\end{aligned} \tag{3.5.5}$$

$$\begin{aligned}0 = {}&3u_{11}u_{10}^2 + 2v_{30}c_0 - 2a_0f_1 - 2a_0u_{30}^4 - a_0^2f_2 + a_0^2u_{30}^3\\ &+ 2c_1c_0u_{30} + 2v_{30}a_0c_1 + 2a_0u_{30}f_2 - 2a_0u_{30}^2f_3 + a_0^2u_{30}f_3 + c_0^2\end{aligned} \tag{3.5.6}$$

$$0 = 2v_{30}a_0c_0 + a_0^2u_{30}f_2 - a_0^2u_{30}^2f_3 + c_0^2u_{30} - a_0^2f_1 - a_0^2u_{30}^4 + u_{10}^3. \tag{3.5.7}$$

From (3.5.2) we can write u_{11} in terms of a_0 and c_2 and then (3.5.3) and (3.5.4) can be used to write u_{10} and c_0 in terms of c_2, a_0 and c_1. Substituting expressions for u_{11}, u_{10} and c_0 into (3.5.5), (3.5.6), (3.5.7) gives us polynomials E_1, E_2 and E_3 of degrees 3, 4 and 4 in c_1 respectively. The coefficient of c_1^3 in (5.2.7) is a non-zero constant, so we can replace E_2 and E_3 by $\widetilde{E_2} = E_2 \bmod E_1$ and $\widetilde{E_3} = E_3 \bmod E_1$. We then compute $r_1 = \mathrm{Res}_{c_1}(E_1, \widetilde{E_2})$, $r_2 = \mathrm{Res}_{c_1}(E_1, \widetilde{E_3})$, $r_3 = \mathrm{Res}_{c_1}(\widetilde{E_2}, \widetilde{E_3})$. Finally we compute $R_1 = \mathrm{Res}_{a_0}(r_1, r_2)$, $R_2 = \mathrm{Res}_{a_0}(r_1, r_3)$

and then $G = \gcd(R_1, R_2)$. If we remove the trivial factors of c_2 from G, we obtain a polynomial of degree 132 in c_2. Finally we can easily remove from G a predictable factor of degree 17 which appears 3 times, obtaining a polynomial $P(c_2)$ of degree 81 in c_2. The resulting trisection algorithm for weight-1 divisor is analogous to Algorithm 4 TRISECTION (General case). See [23] for a MAGMA function to compute trisections of divisors D_3 of weight 1.

Example 2. *Consider $p = 10007$ and the curve defined by*

$$\mathrm{C}y^2 = x^5 + 1321x^3 + 3239x^2 + 8829x + 525$$

over $\mathbb{F}_p$. The factorization of the 3-torsion polynomial is of the form $(20)^4$, so the order of the group is relatively prime to 3. Therefore, all divisors D_3 in $\mathrm{Jac(C)}(\mathbb{F}_q)$ will have a unique trisection defined over $\mathbb{F}_q$. For example, given

$$D_3 := (x + 1179, 507),$$

its trisection polynomial $P(x = a_1)$ is

$$(x + 2698)(x^{80} + 9672x^{79} + \ldots + 2054x + 8698)$$

and we find that the only trisection of D_3 is

$$\frac{1}{3}D_3 = \{(x^2 + 9485x + 2588, 2977x + 7494)\}$$

with $c_2 = 7309, a_0 = 1864, c_1 = 2365, c_0 = 4063$.

3.6 Predictable false positives (parasitic factors)

We now explain why we can remove the factor G_f of degree 18 in a_1 which appears three times in G in Section 3.4 above. One assumption to obtain (3.4.1) is that $u_1(x)$ and $\alpha(x)$ do not have factors in common. Let us now consider the general case $\gcd(u_1, \alpha) \neq 1$. From the definition of α, β and γ, we must have $\gcd(u_1(x), \alpha(x)) = \alpha(x)$ with $\alpha(x)$ of degree 1. We can therefore write $u_1(x) = \alpha(x)(x - t)$ and $\gamma(x) = \alpha(x)(a_1^{-1}x + k_0)$. Note that the value a_1 in $\gamma(x)$ is the same a_1 as in $\alpha(x) = a_1x + a_0$ (Section 3.4). Any root a_1 obtained in case $\gcd(u_1(x), \alpha(x)) = \alpha(x)$ which is also a root of G in Section 3.4 can be removed safely. Equation (3.4.1) becomes

$$\alpha(x)(x - t)^3 = \frac{((a_1^{-1}x + k_0)u_3(x) + v_3(x))^2 - f(x)}{u_3(x)}.$$

The coefficients of x^3, x^2, x^1 and x^0 provide 4 equations in 4 unknowns t, k_0, a_1 and a_0. From the coefficient of x^3 we can write a_0 in terms of t, k_0 and a_1. Substituting for a_0 in the coefficients of x^2, x^1 and x^0 we obtain polynomials E_1, E_2 and E_3. We then compute $r_1 = \mathrm{Res}_{k_0}(E_1, E_2)$, $r_2 = \mathrm{Res}_{k_0}(E_1, E_3)$, $r_3 = \mathrm{Res}_{k_0}(E_2, E_3)$, $s_1 = \mathrm{Res}_t(r_1, r_2)$, $s_2 = \mathrm{Res}_t(r_1, r_3)$ and finally $s = \gcd(s_1, s_2)$. If we remove the trivial factors (in a_1) from s, we obtain a polynomial of degree 18 in a_1 which is exactly the factor G_f that we wanted to exclude in Section 3.4. In general we just obtain false roots, but if this case is successful we can obtain solutions (see example 3).

By a similar argument, we can exclude the predictable factor of degree 17 in c_2 which appears three times in G in Section 3.5 .

Example 3. *Consider $p = 127$ and the curve*

$$\mathrm{C} : y^2 = x^5 + x^3 + x^2 + 3x + 1$$

over $\mathbb{F}_p$. The factorization of the 3-torsion polynomial is of the form $(10)^8$. Again the order of the group is relatively prime to 3, hence all $D_3 \in \mathrm{Jac(C)}(\mathbb{F}_q)$ have a unique trisection defined over $\mathbb{F}_q$. For example, given

$$D_3 := (x^2 + 104x + 108, 77x + 40),$$

its trisection polynomial $P(a_1 = x)$ is

$$(x + 123)(33x^{80} + 32x^{79} + \ldots + 30x + 92),$$

the G_f factor of degree 18 is

$$(x + 123)(12x^{17} + 110x^{16} + \ldots + 62x + 80),$$

and the only trisection is

$$\frac{1}{3}D_3 = \{(x^2 + 82x + 58, 125x + 98)\}$$

with $\alpha(x) = 123x + 69$ and $\gamma(x) = x^2 + 79x + 78$. Observe that $\gcd(x^2 + 82x + 58, 123x + 69) = x + 78$. *We obtained v_1 as* $-(\gamma(x)/\alpha(x) \cdot u_3(x) + v_3(x)) \bmod u_1(x)$.

3.7 Factorization of polynomials of ℓ-torsion and ℓ-sections

The possible factorization type of the ℓ-torsion polynomial is determined by the characteristic polynomial $\chi(x)$ of the Frobenius endomorphism π reduced modulo ℓ. For elliptic (genus 1) curves, this was studied by Verdure [20]. For hyperelliptic curve of genus 2, the number of distinct cases to deal with increases significantly. An analysis of the upper bound for the irreducible factors can be found in [11], and an application to the factorization types of ℓ-modular polynomials can be found in [9]. The methods we use are based on those in [9] for ℓ-modular polynomials but with significant variations since we want to establish the relationship between the type of factorization of ℓ-torsion polynomial (the precise Galois orbits of the ℓ-torsion divisors) and the field of definition of the ℓ-sections. Let π be the Frobenius endomorphism of $\mathbb{F}_q$ and

$$\tilde{\chi}(x) = x^4 - \tilde{s_1}x^3 + \tilde{s_2}x^2 - \tilde{s_1}\tilde{q}x + \tilde{q}^2 \tag{3.7.1}$$

be the characteristic polynomial of π, where $\tilde{q}, \tilde{s_1}, \tilde{s_2} \in \mathbb{F}_\ell$. A classification of the factorization types of $\tilde{\chi}$ over $\mathbb{F}_\ell$ is given by Gaudry and Schost in [9]. We first establish the following lemma which will be used throughout the section.

Lemma 6. *Let D be a divisor in* Jac$[\ell]$ *and let*

$$V_D := Span_{\mathbb{F}_\ell}\{\pi^n(D), n \in \mathbb{N}\}.$$

Let P be the minimal polynomial of π restricted a V_D. Then the degree of extension of $\mathbb{F}_q$ where D is defined is

$$ord'(P) := min\{k \in \mathbb{N}^* : x^k - 1 = 0 \ mod \ P\}.$$

Proof: If the field of definition of a divisor D is $\mathbb{F}_{q^k}$ then $(\pi^k - Id)(D)$ is trivial on V_D, thus $x^k - \ 1 \equiv 0 \bmod P$ where P is the minimal polynomial in V_D.

Suppose that for some $k' < k$ we have $x^{k'} - \ 1 \equiv 0 \bmod P$ on V_D. Then D is defined over $\mathbb{F}_{q^{k'}}$. As the field of definition is the smallest k' that satisfies this condition then k' must be $ord'(P)$. □

For $\ell = 3$ we now establish the relation between factorization types of the 3-torsion polynomial $T(a_0)$ with the factorization types of the characteristic polynomial of Frobenius $\tilde{\chi}(x)$.

Proposition 3. *The possible degrees of the irreducible factor of $T(a_0)$ from Proposition 2 are as follows:*

$\tilde{\chi}(x)$	$T(a_0)$			
(4)	$(5)^{16}$,	$(10)^8$,	$(20)^4$	
$(2)^2$	$(4)^2(12)^6$,	$(4)^{20}$,	$(8)(24)^3$,	$(8)^{10}$
$(2)(2)$	$(8)(24)^3$,	$(8)^{10}$		
$(2)(1)^2$	$(2)(4)^6(6)(12)^4$,	$(1)^2(3)^2(4)^6(12)^4$,	$(2)^4(4)^{18}$,	$(1)^8(4)^{18}$
$(2)(1)(1)$	$(1)^2(2)^3(8)^9$			
$(1)^4$	$(1)^2(3)^8(9)^6$,	$(1)^8(3)^{24}$,	$(1)^{26}(3)^{18}$,	$(1)^{80}$,
	$(2)(6)^4(18)^3$,	$(2)^4(6)^{12}$,	$(2)^{13}(6)^9$,	$(2)^{40}$
$(1)^2(1)^2$	$(1)^2(2)^3(3)^2(6)^{11}$,	$(1)^2(2)^{12}(3)^2(6)^8$,	$(1)^8(2)^9(6)^9$,	$(1)^8(2)^{32}$

Proof: From the factorizations of $\tilde{\chi}(x)$ given in [9], we discard the cases $(1)^2(1)(1)$, $(1)(1)(1)(1)$ since they require 3 or 4 distinct rational roots in $\mathbb{F}_\ell$ as there are only 2 non zero elements in $\mathbb{F}_3$.

We show the details for the case with $\chi(x) = x^4 + 2x^3 + 2x^2 + 2x + 1 = (x^2 + 1)(x + 1)^2$, all other cases are analogous. For this polynomial $\chi(x)$ there are 2 possible Jordan forms for the matrix associated to the Frobenius:

$$A_1 := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \quad A_2 := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

We now show how to obtain the factorization of $T(a_0)$ for A_1. The work for the other case is similar. Note that $B_1 := \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$ is the companion matrix of $p(x) = (x^2 + 1)$, the minimal polynomial. Also note that $B_2 := \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ has minimal polynomial $(x + 1)^2$. Given D_1, D_2, D_3, and D_4 the generators of Jac(C)[3] associated to the matrix A_1, and let V_{B_1} be the vector space generated by the conjugates of $0 \neq D \in \langle D_1, D_2 \rangle$. Then the characteristic polynomial of π restricted to V_D is the characteristic (minimal) polynomial of matrix B_1. Then every D in V_{B_1} is defined over an extension of degree $ord'(x^2+1) = 4$. For all $0 \neq D \in \langle D_3 \rangle$ where $\pi(D_3) = 2D_3$, D is defined over an extension of degree $ord'(x+1) = 2$. Let V_{B_2} be the vector space generated by the characteristic (minimal) polynomial of matrix B_2. Then all D in $V_{B_2} - \langle D_3 \rangle$ are defined over an extension of degree $ord'((x+1)^2) = 6$. Let $D = E + F$ with $E \in \langle D_3 \rangle$ and $F \in V_{B_1}$. Then D is defined over an extension of order $ord'((x^2+1)(x+1)) = 4$. Finally, $D = E + F$ with $E \in V_{B_1}$ and $F \in V_{B_2} - \langle D_3 \rangle$ is defined over an extension of degree $ord'((x^2+1)(x+1)^2) = 12$. The 3-torsion polynomial therefore factors in the form $(2)(4)^6(6)(12)^4$. □

We now study the possible factorizations of $P(a_1)$ and $P(c_2)$, taking advantage of the factorization of the 3-torsion polynomial.

Proposition 4. *The degrees of the irreducible factors of $P(a_1)$ (and $P(c_2)$) are shown in tables 3.1 and 3.2.*

Table 3.1: Factorization for curves of 3-rank 0 over $\mathbb{F}_q$.

$T(a_0)$	Trisection
$(5)^{16}$	$(1)(5)^{16}$
$(10)^8$	$(1)(10)^8$
$(20)^4$	$(1)(20)^4$
$(4)^2(12)^6$	$(1)(4)^2(12)^6$
$(4)^{20}$	$(1)(4)^{20}$
$(8)(24)^3$	$(1)(8)(24)^3$

$T(a_0)$	Trisection
$(8)^{10}$	$(1)(8)^{10}$
$(2)(4)^6(6)(12)^4$	$(1)(2)(4)^6(6)(12)^4$
$(2)^4(4)^{18}$	$(1)(2)^4(4)^{18}$
$(2)(6)^4(18)^3$	$(1)(2)(6)^4(18)^3$
$(2)^{13}(6)^9$	$(1)(2)^{13}(6)^9$
$(2)^{40}$	$(1)(2)^{40}$

Proof: First note that when there is no 3-torsion over $\mathbb{F}_q$ then the cardinality of $\mathrm{Jac(C)}(\mathbb{F}_q)$ is relatively prime to 3. In this case, for any $D \in \mathrm{Jac(C)}(\mathbb{F}_q)$ we see $(3^{-1} \bmod \#\mathrm{Jac(C)}(\mathbb{F}_q)) \cdot D$ is a trisection of D over $\mathbb{F}_q$ and then the factorization of the trisection polynomial is given from the factorization of 3-torsion polynomial by adding a linear factor. Thus we only need to study the cases where the rank of $\mathrm{Jac(C)}(\mathbb{F}_q)[3]$ is ≥ 1. There are 12 cases:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

$(1)^2(3)^2(4)^6(12)^4$ $\qquad$ $(1)^8(4)^{18}$ $\qquad$ $(1)^2(2)^3(8)^9$

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$(1)^2(2)^3(8)^9$ $\qquad$ $(1)^2(3)^8(9)^6$ $\qquad$ $(1)^{26}(3)^{18}$

Table 3.2: Factorization for curves of 3-rank ≥ 1 over $\mathbb{F}_q$.

	$T(a_0)$	Successful trisection	Unsuccessful trisection
Rank 1	$(1)^2(3)^2(4)^6(12)^4$	$(1)^3(3)^2(4)^6(12)^4$	$(3)^3(12)^6$
	$(1)^2(2)^3(8)^9$	$(1)^3(2)^3(8)^9$	$(3)(6)(24)^3$
	$(1)^2(3)^8(9)^6$	$(1)^3(3)^8(9)^6$	$(9)^9$
	$(1)^2(2)^{12}(3)^2(6)^8$	$(1)^3(2)^{12}(3)^2(6)^8$	$(3)^3(6)^{12}$
	$(1)^2(2)^3(3)^2(6)^{11}$	$(1)^3(2)^3(3)^2(6)^{11}$	$(3)^3(6)^{12}$
	$(1)^2(2)^{12}(3)^2(6)^8$	$(1)^3(2)^{12}(3)^2(6)^8$	$(3)^3(6)^{12}$
Rank 2	$(1)^8(2)^9(6)^9$	$(1)^9(2)^9(6)^9$	$(3)^3(6)^{12}$
	$(1)^8(4)^{18}$	$(1)^9(4)^{18}$	$(3)^3(12)^6$
	$(1)^8(2)^{32}$	$(1)^9(2)^{32}$	$(3)^3(6)^{12}$
	$(1)^8(3)^{24}$	$(1)^9(3)^{24}$	$(3)^{27}$
Rank 3	$(1)^{26}(3)^{18}$	$(1)^{27}(3)^{18}$	$(3)^{27}$
Rank 4	$(1)^{80}$	$(1)^{81}$	$(3)^{27}$

$$\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&1\end{pmatrix}$$

$(1)^8(3)^{24}$

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$$

$(1)^{80}$

$$\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&2&1\\0&0&0&2\end{pmatrix}$$

$(1)^2(2)^3(3)^2(6)^{11}$

$$\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&2&0\\0&0&0&2\end{pmatrix}$$

$(1)^2(2)^{12}(3)^2(6)^8$

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&2&1\\0&0&0&2\end{pmatrix}$$

$(1)^8(2)^9(6)^9$

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&2&0\\0&0&0&2\end{pmatrix}$$

$(1)^8(2)^{36}$

We show the details for the case $(1)^2(2)^3(3)^2(6)^{11}$, the other cases are analogous. From the matrix, the basis satisfies $w_1^\pi = w_1$, $w_2^\pi = w_1 + w_2$, $w_3^\pi = 2w_3$, and $w_4^\pi = w_3 + 2w_4$. Let D_1 be a trisection of D_3. Then the length of its orbit under π determines the extension degree of $\mathbb{F}_q$ where it is defined and the degrees of the factor of $P(a_1)$ to which it is associated. The length of the orbit depends on the image D_1^π of D_1 under the Frobenius. Write

$$D_1^\pi = D_1 + m_1w_1 + m_2w_2 + m_3w_3 + m_4w_4$$

with $m_i \in \{0,1,2\}$ for $i = 1,2,3,4$. We first look for trisections of D_3 fixed under the Frobenius endomorphism. If $D_1 + l_1w_1 + l_2w_2 + l_3w_3 + l_4w_4$ is a trisection defined over $\mathbb{F}_q$ we need $l_i \in \{0,1,2\}$ such that

$$\begin{aligned} &D_1 + l_1w_1 + l_2w_2 + l_3w_3 + l_4w_4 = (D_1 + l_1w_1 + l_2w_2 + l_3w_3 + l_4w_4)^\pi \\ =&D_1 + (m_1 + l_1 + l_2)w_1 + (m_2 + l_2)w_2 + (m_3 + 2l_3 + l_4)w_3 + (m_4 + 2l_4)w_4, \end{aligned}$$

from which we obtain the following linear system:

$$\begin{aligned} m_1 + l_2 &= 0 \\ m_2 &= 0 \\ m_3 + l_3 + l_4 &= 0 \\ m_4 + l_4 &= 0. \end{aligned}$$

Solving this system, we obtain that

$$\begin{aligned} &(D_1 + 2m_1w_2 + (2m_3 + m_4)w_3 + 2m_4w_4)^\pi \\ &= D_1 + 2m_1w_2 + (2m_3 + m_4)w_3 + 2m_4w_4 \end{aligned}$$

is fixed under the Frobenius. Since we have a trisection over $\mathbb{F}_q$ and the remaining ones are obtained by adding a 3-torsion divisor, the factorization type of the trisection polynomial corresponds to the factorization type of the 3-torsion polynomial $T(a_0)$ with an additional linear factor. Thus we only need to study the cases where $m_2 \neq 0$. We now show the orbits when $m_1 = m_3 = m_4 = 0$ and $m_2 = 1$, the other cases are analogous.

$$\{D_1, D_1 + w_2, D_1 + w_1 + 2w_2\}$$

$$\{D_1 + w_1, D_1 + w_1 + w_2, D_1 + 2w_1 + 2w_2\}$$

$$\{D_1 + 2w_1, D_1 + w_2 + 2w_1, D_1 + 2w_2\}$$

$$\begin{aligned} \{&D_1 + 2w_1 + 2w_3 + w_4, D_1 + 2w_2 + 2w_4, D_1 + 2w_1 + w_2 + w_3 + w_4, \\ &D_1 + 2w_2 + w_4, D_1 + 2w_1 + w_3 + 2w_4, D_1 + 2w_1 + w_2 + 2w_3 + 2w_4\} \end{aligned}$$

$$\begin{aligned} \{&D_1 + w_2 + 2w_3 + 2w_4, D_1 + w_2 + 2w_3 + w_4, D_1 + w_1 + 2w_2 + 2w_4, \\ &D_1 + w_1 + 2w_2 + w_4, D_1 + 2w_3 + w_4, D_1 + w_2 + w_2 + w_3 + w_4\} \end{aligned}$$

$$\begin{aligned} \{&D_1 + w_1 + 2w_2 + w_3 + w_4, D_1 + w_2 + 2w_3 + w_4, D_1 + w_1 + 2w_2 + 2w_3 + 2w_4, \\ &D_1 + 2w_4, D_1 + w_2 + w_3 + 2w_4, D_1 + w_4\} \end{aligned}$$

$$\begin{aligned} \{&D_1 + w_1 + 2w_2 + w_3 + 2w_4, D_1 + w_2 + w_4, D_1 + w_3 + w_4, \\ &D_1 + w_1 + 2w_2 + 2w_3 + w_4, D_1 + 2w_3 + 2w_4, D_1 + w_2 + 2w_4\} \end{aligned}$$

$$\begin{aligned} \{&D_1 + 2w_1 + 2w_4, D_1 + 2w_1 + w_2 + w_3 + 2w_4, D_1 + 2w_1 + 2w_2 + 2w_4, \\ &D_1 + 2w_2 + 2w_3 + w_4, D_1 + 2w_1 + w_3 + w_4, D_1 + 2w_1 + 2w_3 + 2w_4\} \end{aligned}$$

$$\begin{aligned} \{&D_1 + 2w_1 + 2w_4, D_1 + 2w_1 + w_2 + w_3 + 2w_4, D_1 + 2w_2 + w_3 + w_4, \\ &D_1 + w_1 + w_3 + w_4, D_1 + w_1 + 2w_3 + w_4, D_1 + w_1 + w_2 + w_3 + w_4\} \end{aligned}$$

$$\begin{aligned} \{&D_1 + w_1 + w_2 + 2w_3 + 2w_4, D_1 + w_1 + w_3 + 2w_4, D_1 + 2w_1 + 2w_2 + 2w_4, \\ &D_1 + 2w_1 + 2w_2 + w_4, D_1 + w_1 + 2w_3 + w_4, D_1 + w_1 + w_2 + w_3 + w_4\} \end{aligned}$$

$$\begin{aligned} \{&D_1 + 2w_1 + 2w_3, D_1 + 2w_1 + w_2 + 2w_3, D_1 + 2w_1 + w_3, \\ &D_1 + 2w_2 + 2w_3, D_1 + 2w_1 + w_2 + w_3, D_1 + 2w_2 + w_3\} \end{aligned}$$

$$\begin{aligned} \{&D_1 + 2w_1 + 2w_2 + 2w_3 + w_4, D_1 + w_1 + w_2 + w_4, D_1 + 2w_1 + 2w_2 + w_3 + 2w_4, \\ &D_1 + w_1 + w_3 + w_4, D_1 + w_1 + 2w_3 + 2w_4, D_1 + w_1 + w_2 + 2w_4\} \end{aligned}$$

$$\begin{aligned} \{&D_1 + w_1 + 2w_2 + w_3 + 2w_4, D_1 + w_2 + w_4, D_1 + w_3 + w_4, \\ &D_1 + w_1 + 2w_2 + 2w_3 + w_4, D_1 + 2w_3 + 2w_4, D_1 + w_2 + 2w_4\} \end{aligned}$$

$$\begin{aligned} \{&D_1 + 2w_1 + 2w_4, D_1 + 2w_1 + w_2 + w_3 + 2w_4, D_1 + 2w_2 + w_3 + w_4, \\ &D_1 + 2w_1 + w_4, D_1 + 2w_2 + 2w_3 + 2w_4, D_1 + 2w_1 + w_2 + 2w_3 + w_4\} \end{aligned}$$

$$\begin{aligned} \{&D_1 + 2w_1 + 2w_3 + w_4, D_1 + 2w_2 + 2w_4, D_1 + 2w_1 + w_2 + w_3 + w_4, \\ &D_1 + 2w_2 + w_4, D_1 + 2w_1 + w_2 + 2w_3 + 2w_4, D_1 + 2w_1 + w_3 + 2w_4\} \end{aligned}$$

In view of these orbits, working out the details for all posible images of D_1, we conclude the only factorization type is $(3)^3(6)^{12}$ if there are no trisections over $\mathbb{F}_q$. □

From table 4.2, we obtain the following result regarding the minimal extension degree of $\mathbb{F}_q$ where trisections lie.

Corollary 1. *If the curve has 3-rank $r \geq 1$ in $\mathbb{F}_q$ and $D_3 \in \mathrm{Jac(C)}(\mathbb{F}_q)$ then*

- *If the 3-torsion polynomial factors in the form* $(1)^2(3)^8(9)^6$*, then* D_3 *admits trisections in either* $\mathbb{F}_q$ *or* $\mathbb{F}_{q^9}$*.*

- *In all other cases,* D_3 *admits at least* 3^r *trisections in* $\mathbb{F}_q$ *or* $\mathbb{F}_{q^3}$

Table 3.3: Factorization for curves of 5-rank ≥ 1 over $\mathbb{F}_q$.

	5-torsion Galois orbits	successful 5-section	unsuccessful 5-section
Rank 1	$(1)^4(2)^{10}(4)^{150}$	$(1)^5(2)^{10}(4)^{150}$	$(5)(10)^2(20)^{30}$
	$(1)^4(5)^{124}$	$(1)^5(5)^{124}$	$(5)^{125}$
	$(1)^4(2)^{10}(5)^4(10)^{58}$	$(1)^5(2)^{10}(5)^4(10)^{58}$	$(5)^5(10)^{60}$
	$(1)^4(2)^{60}(5)^4(10)^{48}$	$(1)^5(2)^{60}(5)^4(10)^{48}$	$(5)^5(10)^{60}$
	$(1)^4(4)^5(5)^4(20)^{29}$	$(1)^5(4)^5(5)^4(20)^{29}$	$(5)^5(20)^{30}$
	$(1)^4(4)^{30}(5)^4(20)^{24}$	$(1)^5(4)^{30}(5)^4(20)^{24}$	$(5)^5(20)^{30}$
	$(1)^4(4)^5(5)^4(20)^{29}$	$(1)^5(4)^5(5)^4(20)^{29}$	$(5)^5(20)^{30}$
	$(1)^4(4)^{30}(5)^4(20)^{24}$	$(1)^5(4)^{30}(5)^4(20)^{24}$	$(5)^5(20)^{30}$
	$(1)^4(2)^{10}(4)^{150}$	$(1)^5(2)^{10}(4)^{150}$	$(5)(10)^2(20)^{30}$
	$(1)^4(2)^{10}(4)^{25}(20)^{25}$	$(1)^5(2)^{10}(4)^{25}(20)^{25}$	$(5)(10)^2(20)^{30}$
	$(1)^4(2)^{10}(4)^{150}$	$(1)^5(2)^{10}(4)^{150}$	$(5)(10)^2(20)^{30}$
	$(1)^4(2)^{10}(4)^{25}(20)^{25}$	$(1)^5(2)^{10}(4)^{25}(20)^{25}$	$(5)(10)^2(20)^{30}$
	$(1)^4(2)^{10}(4)^{25}(20)^{25}$	$(1)^5(2)^{10}(4)^{25}(20)^{25}$	$(5)(10)^2(20)^{30}$
	$(1)^4(5)^4(6)^{20}(30)^{16}$	$(1)^5(5)^4(6)^{20}(30)^{16}$	$(5)^5(30)^{20}$
	$(1)^4(4)^5(24)^{25}$	$(1)^5(4)^5(24)^{25}$	$(5)(20)(120)^5$
	$(1)^4(4)^5(8)^{75}$	$(1)^5(4)^5(8)^{75}$	$(5)(20)(40)^{15}$
	$(1)^4(4)^5(24)^{25}$	$(1)^5(4)^5(24)^{25}$	$(5)(20)(120)^5$
	$(1)^4(2)^{10}(12)^{50}$	$(1)^5(2)^{10}(12)^{50}$	$(5)(10)^2(60)^{10}$
	$(1)^4(4)^5(24)^{25}$	$(1)^5(4)^5(24)^{25}$	$(5)(20)(120)^5$
	$(1)^4(4)^5(24)^{25}$	$(1)^5(4)^5(24)^{25}$	$(5)(20)(120)^5$
	$(1)^4(2)^{10}(12)^{50}$	$(1)^5(2)^{10}(12)^{50}$	$(5)(10)^2(60)^{10}$
	$(1)^4(4)^5(8)^{75}$	$(1)^5(4)^5(8)^{75}$	$(5)(20)(40)^{15}$
	$(1)^4(3)^{40}(15)^{32}(5)^4$	$(1)^5(3)^{40}(15)^{32}(5)^4$	$(5)^5(15)^{40}$
Rank 2	$(1)^{24}(5)^{120}$	$(1)^{25}(5)^{120}$	$(5)^{125}$
	$(1)^{24}(6)^{100}$	$(1)^{25}(6)^{100}$	$(5)^5(30)^{20}$
	$(1)^{24}(4)^{150}$	$(1)^{25}(4)^{150}$	$(5)^5(20)^{30}$
	$(1)^{24}(4)^{25}(20)^{25}$,	$(1)^{25}(4)^{25}(20)^{25}$	$(5)^5(20)^{30}$
	$(1)^{24}(4)^{150}$	$(1)^{25}(4)^{150}$	$(5)^5(20)^{30}$
	$(1)^{24}(2)^{50}(10)^{50}$,	$(1)^{25}(2)^{50}(10)^{50}$	$(5)^5(10)^{60}$
	$(1)^{24}(4)^{150}$	$(1)^{25}(4)^{150}$	$(5)^5(20)^{30}$
	$(1)^{24}(4)^{25}(20)^{25}$,	$(1)^{25}(4)^{25}(20)^{25}$	$(5)^5(20)^{30}$
	$(1)^{24}(2)^{300}$	$(1)^{25}(2)^{300}$	$(5)^5(10)^{60}$
	$(1)^{24}(3)^{200}$	$(1)^{25}(3)^{200}$	$(5)^5(15)^{40}$
Rank 3	$(1)^{124}(5)^{100}$	$(1)^{125}(5)^{100}$	$(5)^{125}$
Rank 4	$(1)^{624}$	$(1)^{625}$	$(5)^{125}$

The technique used to study the factorization of the 3-torsion and trisection polynomial can be generalized for any ℓ. If we know the orbits of ℓ-torsion divisors, we can determine the factorization of ℓ-section polynomials. When there is no ℓ-torsion over $\mathbb{F}_q$ we obtain that $(\ell^{-1} \bmod \#\text{Jac(C)}) \cdot D$ is a ℓ-section of D over $\text{Jac(C)}(\mathbb{F}_q)$ and then the field of definition of a ℓ-section is given from the field of definition of ℓ-torsion elements. We can therefore restrict ourselves to study the cases where the rank of $\text{Jac(C)}(\mathbb{F}_q)[\ell]$ is ≥ 1, which is equivalent to study the polynomials of the form $p = x^4 - \tilde{s_1}x^3 + \tilde{s_2}x^2 - \tilde{s_1}\tilde{q}x + \tilde{q}^2$ such that $(x-1)|p$. From each polynomial we obtain the possible Jordan forms for the matrix associated to the Frobenius. For each matrix we can compute all possible orbits for D_1^{π} (for an algorithm to compute all possible orbits, see [24]).

When going through the possible images $D_1^{\pi} = D_1 + m_1w_1 + m_2w_2 + m_3w_3 + m_4w_4$, it is convenient to first identify if there are divisors fixed under the Frobenius, since the orbits are then obtained trivially (from the ℓ-torsion divisors) instead of computed one by one, reducing the work significantly. We briefly review the steps of this process.

Algorithm 7 Fields of definition (of ℓ-sections)

```
Require: Polynomial $\tilde{\chi}(x) = x^4 - \tilde{s_1}x^3 + \tilde{s_2}x^2 - \tilde{s_1}\tilde{q}x + \tilde{q}^2 \in \mathbb{F}_\ell[x]$ divisible by
    $x - 1$.
Ensure: The set of possible factorization types for the $\ell$-section polynomial.
Factorize $\tilde{\chi}(x)$ in $\mathbb{F}_\ell[x]$
Compute all the possible Jordan forms of the matrix associated to the
    Frobenius endomorphism
for each Jordan form, set $\{w_1, w_2, w_3, w_4\}$ the associated basis do
    Compute the orbits of the space $\langle w_1, w_2, w_3, w_4 \rangle$ under the Frobenius
    Discard the orbit $\{0\}$
    Lengths of the orbits $\rightarrow$ factorization type of the $\ell$-torsion polynomial
    for each quadruple $\{m_1, m_2, m_3, m_4\} \in (\mathbb{F}_\ell)^4$ do
        Set the image of $D_1$ under the Frobenius as
            $$D_1^\pi = D_1 + m_1 w_1 + m_2 w_2 + m_3 w_3 + m_4 w_4$$
        if some divisor in $D_1 + \langle w_1, w_2, w_3, w_4 \rangle$ is fixed under the Frobenius
        then
            $\ell$-torsions $\rightarrow$ factorization type of the $\ell$-section polynomial
        else
            Set $S = D_1 + \langle w_1, w_2, w_3, w_4 \rangle$
            repeat
                Choose $D \in S$ and compute its orbit
                Remove all the elements of this orbit from $S$
            until $S = \emptyset$
            Lengths of orbits $\rightarrow$ factorization type of the $\ell$-section polynomial
        end if
    end for
end for
```

Using these ideas, we can determine all the possible fields of definition for ℓ-sections (with ℓ small). In Table 3.3, we give the field of definition of 5-sections according to 5-torsion Galois orbit when the rank of $\mathrm{Jac(C)}(\mathbb{F}_q)[5]$ is ≥ 1.

For $\ell = 7$, the number of distinct cases to deal increases significantly (see Table 3.4). We summarize the result for $\ell \in \{5, 7\}$ in the next corollary.

Corollary 2. *If the curve has ℓ-rank $r \geq 1$ with $\ell \in \{5, 7\}$ in $\mathbb{F}_q$ and $D_\ell \in \mathrm{Jac(C)}(\mathbb{F}_q)$ then D_ℓ admits at least ℓ^r ℓ-sections in $\mathbb{F}_q$ or $\mathbb{F}_{q^\ell}$.*

Table 3.4: Curves of 7-rank ≥ 1 over $\mathbb{F}_q$.

	7-torsión Galois orbits	successful 7-section	unsuccessful 7-section
Rank 1	$(1)^6(3)^{112}(7)^6(21)^{96}$	$(1)^7(3)^{112}(7)^6(21)^{96}$	$(7)^7(21)^{112}$
	$(1)^6(3)^{14}(6)^{392}$	$(1)^7(3)^{14}(6)^{392}$	$(7)(21)^2(42)^{56}$
	$(1)^6(3)^{14}(6)^{49}(42)^{49}$	$(1)^7(3)^{14}(6)^{49}(42)^{49}$	$(7)(21)^2(42)^{56}$
	$(1)^6(2)^{21}(16)^{147}$	$(1)^7(2)^{21}(16)^{147}$	$(7)(14)^3(112)^{21}$
	$(1)^6(4)^{84}(7)^6(28)^{72}$	$(1)^7(4)^{84}(7)^6(28)^{72}$	$(7)^7(28)^{84}$
	$(1)^6(2)^{21}(16)^{147}$	$(1)^7(2)^{21}(16)^{147}$	$(7)(14)^3(112)^{21}$
	$(1)^6(2)^{21}(7)^6(14)^{165}$	$(1)^7(2)^{21}(7)^6(14)^{165}$	$(7)^7(14)^{168}$
	$(1)^6(2)^{168}(7)^6(14)^{144}$	$(1)^7(2)^{168}(7)^6(14)^{144}$	$(7)^7(14)^{168}$
	$(1)^6(6)^{56}(7)^6(42)^{48}$	$(1)^7(6)^{56}(7)^6(42)^{48}$	$(7)^7(42)^{56}$
	$(1)^6(3)^{14}(6)^{49}(42)^{49}$	$(1)^7(3)^{14}(6)^{49}(42)^{49}$	$(7)(21)^2(42)^{56}$
	$(1)^6(3)^{14}(6)^{392}$	$(1)^7(3)^{14}(6)^{392}$	$(7)(21)^2(42)^{56}$
	$(1)^6(2)^{21}(3)^{14}(6)^{385}$	$(1)^7(2)^{21}(3)^{14}(6)^{385}$	$(7)(14)^3(21)^2(42)^{55}$
	$(1)^6(3)^{14}(12)^{196}$	$(1)^7(3)^{14}(12)^{196}$	$(7)(21)^2(84)^{28}$
	$(1)^6(7)^{342}$	$(1)^7(7)^{342}$	$(7)^{343}$
	$(1)^6(3)^{14}(24)^{98}$	$(1)^7(3)^{14}(24)^{98}$	$(7)(21)^2(168)^{14}$
	$(1)^6(6)^7(48)^{49}$	$(1)^7(6)^7(48)^{49}$	$(7)(42)(336)^7$
	$(1)^6(3)^{14}(24)^{98}$	$(1)^7(3)^{14}(24)^{98}$	$(7)(21)^2(168)^{14}$
	$(1)^6(2)^{21}(16)^{147}$	$(1)^7(2)^{21}(16)^{147}$	$(7)(14)^3(112)^{21}$
	$(1)^6(6)^7(48)^{49}$	$(1)^7(6)^7(48)^{49}$	$(7)(42)(336)^7$
	$(1)^6(6)^7(48)^{49}$	$(1)^7(6)^7(48)^{49}$	$(7)(42)(336)^7$
	$(1)^6(2)^{21}(16)^{147}$	$(1)^7(2)^{21}(16)^{147}$	$(7)(14)^3(112)^{21}$
	$(1)^6(6)^7(48)^{49}$	$(1)^7(6)^7(48)^{49}$	$(7)(42)(336)^7$
	$(1)^6(2)^{21}(3)^{14}(6)^{385}$	$(1)^7(2)^{21}(3)^{14}(6)^{385}$	$(7)(14)^3(21)^2(42)^{55}$
	$(1)^6(2)^{21}(3)^{14}(6)^{385}$	$(1)^7(2)^{21}(3)^{14}(6)^{385}$	$(7)(14)^3(21)^2(42)^{55}$
	$(1)^6(3)^{14}(12)^{196}$	$(1)^7(3)^{14}(12)^{196}$	$(7)(21)^2(84)^{28}$
	$(1)^6(6)^7(48)^{49}$	$(1)^7(6)^7(48)^{49}$	$(7)(42)(336)^7$
	$(1)^6(6)^7(7)^6(42)^{55}$	$(1)^7(6)^7(7)^6(42)^{55}$	$(7)^7(42)^{56}$
	$(1)^6(6)^{56}(7)^6(42)^{48}$	$(1)^7(6)^{56}(7)^6(42)^{48}$	$(7)^7(42)^{56}$
	$(1)^6(6)^7(7)^6(42)^{55}$	$(1)^7(6)^7(7)^6(42)^{55}$	$(7)^7(42)^{56}$
	$(1)^6(6)^{56}(7)^6(42)^{48}$	$(1)^7(6)^{56}(7)^6(42)^{48}$	$(7)^7(42)^{56}$
	$(1)^6(6)^7(48)^{49}$	$(1)^7(6)^7(48)^{49}$	$(7)(42)(336)^7$
	$(1)^6(7)^6(8)^{42}(56)^{36}$	$(1)^7(7)^6(8)^{42}(56)^{36}$	$(7)^7(56)^{42}$
	$(1)^6(3)^{14}(6)^{392}$	$(1)^7(3)^{14}(6)^{392}$	$(7)(21)^2(42)^{56}$
	$(1)^6(3)^{14}(7)^6(21)^{110}$	$(1)^7(3)^{14}(7)^6(21)^{110}$	$(7)^7(21)^{112}$
	$(1)^6(3)^{112}(7)^6(21)^{96}$	$(1)^7(3)^{112}(7)^6(21)^{96}$	$(7)^7(21)^{112}$
	$(1)^6(3)^{14}(24)^{98}$	$(1)^7(3)^{14}(24)^{98}$	$(7)(21)^2(168)^{14}$
	$(1)^6(6)^7(48)^{49}$	$(1)^7(6)^7(48)^{49}$	$(7)(42)(336)^7$
	$(1)^6(3)^{112}(7)^6(21)^{96}$	$(1)^7(3)^{112}(7)^6(21)^{96}$	$(7)^7(21)^{112}$
	$(1)^6(3)^{14}(24)^{98}$	$(1)^7(3)^{14}(24)^{98}$	$(7)^7(21)^2(168)^{14}$
	$(1)^6(3)^{112}(21)^{98}$	$(1)^7(3)^{112}(21)^{98}$	$(7)(21)^{114}$
	$(1)^6(3)^{798}$	$(1)^7(3)^{798}$	$(7)(21)^{114}$
	$(1)^6(3)^{14}(6)^{392}$	$(1)^7(3)^{14}(6)^{392}$	$(7)(21)^2(42)^{56}$
	$(1)^6(3)^{112}(21)^{98}$	$(1)^7(3)^{112}(21)^{98}$	$(7)(21)^{114}$
	$(1)^6(3)^{798}$	$(1)^7(3)^{798}$	$(7)(21)^{114}$
	$(1)^6(7)^6(8)^{42}(56)^{36}$	$(1)^7(7)^6(8)^{42}(56)^{36}$	$(7)^7(56)^{42}$
	$(1)^6(2)^{21}(3)^{14}(6)^{385}$	$(1)^7(2)^{21}(3)^{14}(6)^{385}$	$(7)(14)^3(21)^2(42)^{55}$
Rank 2	$(1)^{48}(6)^{49}(42)^{49}$	$(1)^{49}(6)^{49}(42)^{49}$	$(7)^7(42)^{56}$
	$(1)^{48}(6)^{392}$	$(1)^{49}(6)^{392}$	$(7)^7(42)^{56}$
	$(1)^{48}(6)^{392}$	$(1)^{49}(6)^{392}$	$(7)^7(42)^{56}$
	$(1)^{48}(8)^{294}$	$(1)^{49}(8)^{294}$	$(7)^7(56)^{42}$
	$(1)^{48}(3)^{784}$	$(1)^{49}(3)^{784}$	$(7)^7(21)^{112}$
	$(1)^{48}(3)^{98}(21)^{98}$	$(1)^{49}(3)^{98}(21)^{98}$	$(7)^7(21)^{112}$
	$(1)^{48}(3)^{784}$	$(1)^{49}(3)^{784}$	$(7)^7(21)^{112}$
	$(1)^{48}(3)^{98}(21)^{98}$	$(1)^{49}(3)^{98}(21)^{98}$	$(7)^7(21)^{112}$
	$(1)^{48}(3)^{784}$	$(1)^{49}(3)^{784}$	$(7)^7(21)^{112}$
	$(1)^{48}(8)^{294}$	$(1)^{49}(8)^{294}$	$(7)^7(56)^{42}$
	$(1)^{48}(6)^{49}(42)^{49}$	$(1)^{49}(6)^{49}(42)^{49}$	$(7)^7(42)^{56}$
	$(1)^{48}(4)^{588}$	$(1)^{49}(4)^{588}$	$(7)^7(28)^{84}$
	$(1)^{48}(2)^{1176}$	$(1)^{49}(2)^{1176}$	$(7)^7(14)^{168}$
	$(1)^{48}(2)^{147}(14)^{147}$	$(1)^{49}(2)^{147}(14)^{147}$	$(7)^7(14)^{168}$
	$(1)^{48}(6)^{392}$	$(1)^{49}(6)^{392}$	$(7)^7(42)^{56}$
	$(1)^{48}(7)^{336}$	$(1)^{49}(7)^{336}$	$(7)^{343}$
Rank 3	$(1)^{342}(7)^{294}$	$(1)^{343}(7)^{294}$	$(7)^{343}$
Rank 4	$(1)^{2400}$	$(1)^{2401}$	$(7)^{343}$

CHAPTER 4

Symbolic trisection polynomials

Efficient trisection (division by three) algorithms for divisors in hyperelliptic curves in odd characteristic have been studied by Gaudry and Schost [7] as well as the authors [19]. The main interest of these algorithms resides in their application in Schoof-like algorithms to compute the group order for the Jacobian of curves of genus 2. A drawback of these methods is that they rely on solving a system of equations in several variables, and at least the final steps of the solution must be done in a case-by-case basis as the final polynomials whose roots produce the solutions of the system are not available symbolically (i.e. described in terms of the curve parameters and representation of the divisor). Symbolic equations are available up to some point in the solution process, after which techniques that reduce a system in several variables to obtaining the roots of an equation in one variable must be applied every time a trisection is performed, and only then can polynomial factorization methods be applied.

It is reasonable to expect the efficiency of these algorithms to improve once a symbolic description of the final polynomial is available, which would then reduce the trisection problem to evaluating and factoring polynomials in one variable. However, direct symbolic computation is not feasible due to the sizes of the intermediate polynomials produced during the process. Nevertheless, our main objective in this chapter is to compute the trisections polynomials of [19] symbolically, and to show it can be used to improve the speed of trisection in practice.

The chapter is organized as follows: In Section 4.1, we recall generalities about genus two curves in odd characteristic. In Section 4.2, we present some basic properties of weighted homogeneous polynomials and their consequences for polynomial interpolation. In Section 4.3, we obtain theoretical results on the trisection polynomial that are required to make the symbolic computation practical. We give further details on the symbolic computation in Section 4.4. We complete in Section 4.5 with an example of a trisection polynomial obtained from the symbolic polynomial and a discussion on how to use the symbolic polynomial in practice.

4.1 Background

Let C be a genus two curve over a finite field $\mathbb{F}_q$ of odd characteristic (greater than 5) given in the model

$$C : y^2 = f(x) \tag{4.1.1}$$

where the polynomial $f(x) = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{F}_q[x]$ has no double roots. We work here in the group of $\mathbb{F}_q$-points of the Jacobian $\mathrm{Jac}(C)$, in terms of Mumford coordinates $[u(x), v(x)]$. In genus 2, every element of $Jac(C) - \{0\}$ can be represented uniquely by a reduced divisor of weight one $(u(x) = x + u_0,\ v(x) = v_0)$ or two $(u(x) = x^2 + u_1x + u_0,\ v(x) = v_1x + v_0)$. An algorithm due to Cantor [3] allows us to compute in the group with this representation of elements of $\mathrm{Jac}(C)$.

To determine the set of pre-images $\frac{1}{3}D_3$ with $D_3 \in Jac(C)(\mathbb{F}_q)$, we will use methods studied in [19]. The idea consists in reversing Cantor's algorithms to the triplication of a divisor. For example, if we assume that D_3 is of the form $D_3 = [u_3(x), v_3(x)] = [x + u_{30}, v_{30}]$ with $v_{30} \neq 0$ (i.e. the support of D_3 does not contain a Weierstrass point), then D_1 must have the form $[u_1(x), v_1(x)] = [x^2 + u_{11}x + u_{10}, v_{11}x + v_{10}]$.

Using the composition step of Cantor's algorithm, we obtain a pair of coordinates of the form $[u^3, \tilde{v}]$ for $3D_1$. We *de-reduce* $D_3 = [u_3, v_3]$ via the polynomial $\beta^2 - \alpha^2 f \equiv 0 \bmod u_3$ with $\beta = \gamma u_3 + \alpha v_3$, where polynomials γ and α are of the form $\gamma = x^2 + c_1x + c_0$ and $\alpha = a_1x + a_0$ (with a_1 assumed non-zero). Matching the first coordinates, we obtain the identity

$$u_1^3 = \frac{(\gamma u_3 + \alpha v_3)^2 - \alpha^2 f}{u_3} \quad . \tag{4.1.2}$$

The coefficients of x^5, x^4, x^3, x^2, x^1 and x^0 in this identity provide 6 equations in 6 unknowns (u_{11}, u_{10}, c_1, c_0, a_1 and a_0), giving us a system whose solutions correspond to the the different trisections of D_3.

4.2 Weighted homogeneous polynomials

In this section, we show some properties of weighted homogeneous polynomials and their impact on multivariate interpolation. These results will be essential tools for the symbolic computation of a trisection polynomial.

Definition 8. *Let $p \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial in n variables and take integers $d_1, d_2, ..., d_n$. The polynomial p is said to be a weighted homogeneous polynomial (WHP) of weight k if for all $t \in \mathbb{F} \setminus \{0\}$ we have:*

$$p(t^{d_1}x_1, t^{d_2}x_2, ..., t^{d_n}x_n) = t^k p(x_1, x_2, ..., x_n) \quad . \tag{4.2.1}$$

The integers $d_1, d_2, ..., d_n$ are called the weights of variables $x_1, ..., x_n$

4.2.1 Properties of WHPs

From the definition of weighted homogeneous polynomials, it is easy to see that the product of two WHPs will be a WHP. Similarly, the sum or difference of two WHPs of the same weight will be either zero or a WHP of that same weight.

We also observe that in any product of two weighted non-homogeneous polynomials, the terms of highest weight are the product of the terms of highest weight in both polynomials, without any impact from the terms of lower weight. Similarly, the terms of lowest weight of the product depend only on the terms of lowest weight in both polynomials. If the product is homogeneous, then the two original polynomials must have been homogeneous too. We can therefore conclude that WHPs factorize into products of WHPs, and the gcd of two (or more) WHPs is also a WHP. We now show the same applies for resultant and subresultants of WHPs.

Definition 9. *Let $f(x)$ and $g(x)$ be two polynomials of degree m and n respectively, and let S be the $m+n$ by $m+n$ Sylvester matrix associated to these polynomials. Then the resultant of $f(x)$ and $g(x)$ is $Res_x(f,g) = \det(S)$, and the j-subresultant is the polynomial of degree j defined by*

$$S_j(f,g) = \det(S_{0j}) + \det(S_{1j})x + \ldots + \det(S_{jj})x^j \ ,$$

where S_{ij} is the matrix determined from S by deleting $2j$ rows and columns as follows:

1. *rows $n-j+1$ to n (each having coefficients of $f(x)$)*
2. *rows $m+n-j+1$ to $m+n$ (each having coefficients of $g(x)$)*
3. *columns $m+n-2j$ to $m+n$, except for column $m+n-i-j$.*

Note that we could extend this definition so $Res_x(f,g) = S_0(f,g)$.

Lemma 7. *Let f and g be two weighted homogeneous polynomials with weight p_1 and p_2 respectively. Let x be an arbitrary variable of weight p, and m and n the degrees in x of f and g respectively. Then $S_j(f,g)$ is weighted homogeneous with weight*

$$p_1(n-j) + p_2(m-j) - (nm - j - j^2)p \ .$$

Proof From the definition of the (sub)resultants (as determinants coming from the Sylvester matrix), they are clearly polynomials in the coefficients of f and g. Let a_i be the coefficient of x^i in f and b_i be the coefficient of x^i in g. Since both f and g are WHPs, then a_i is a WHP of weight $p_1 - ip$ (with $i \in \{1,..,(m-1)\}$) and b_i is a WHP of weight $p_2 - ip$ (with $i \in \{1,..,(n-1)\}$). For each entry of the Sylvester matrix, if we replace each variable x_k by $t^{w_k}x_k$

(where w_k is its weight), then the Sylvester matrix becomes:

$$\tilde{S} = \begin{bmatrix} t^{p_1-mp}a_m & t^{p_1-(m-1)p}a_{m-1} & \dots & 0 & 0 & 0 \\ 0 & t^{p_1-mp}a_m & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \dots & \vdots & & \vdots \\ 0 & 0 & \dots & t^{p_1-p}a_1 & t^{p_1}a_0 & 0 \\ 0 & 0 & \dots & t^{p_1-2p}a_2 & t^{p_1-p}a_1 & t^{p^1}a_0 \\ t^{p_2-np}b_n & t^{p_2-(n-1)p}b_{n-1} & \dots & 0 & 0 & 0 \\ 0 & t^{p_2-np}b_n & \dots & 0 & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & t^{p_2-p}b_1 & t^{p_2}b_0 & 0 \\ 0 & 0 & \dots & t^{p_2-2p}b_2 & t^{p_2-p}b_1 & t^{p_2}b_0 \end{bmatrix}$$

and similarly, the matrices S_{ij} become matrices $\tilde{S}_{ij}$ by removing the corresponding rows and columns from $\tilde{S}$.

If we multiply the k-th row by $t^{p_2+(m-n+k-1)p}$ for $k = 1,..,n$ and by $t^{p_1+(k-n-1)p}$ for $k = n+1,..,n+m$ we obtain

$$\hat{S} = \begin{bmatrix} t^{p_1+p_2-np}a_m & t^{p_1+p_2-(n-1)p}a_{m-1} & \dots & 0 \\ 0 & t^{p_1+p_2-(n-1)p}a_m & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & t^{p_1+p_2+(m-1)p}a_0 \\ t^{p_1+p_2-np}b_n & t^{p_1+p_2-(n-1)p}b_{n-1} & \dots & 0 \\ 0 & t^{p_1+p_2-(n-1)p}b_n & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & t^{p_1+p_2+(m-1)p}b_0 \end{bmatrix}$$

where all the terms in the k-th column are multiplied by $t^{p_1+p_2-(n+1-k)p}$ with respect to the terms in the k-th column of S. Similarly, matrices $\tilde{S}_{ij}$ become $\hat{S}_{ij}$.

Since $\tilde{S}_{ij}$ and $\hat{S}_{ij}$ contain only rows 1 to $n-j$ and $n+1$ to $n+m-j$ of $\tilde{S}$ and $\hat{S}$ respectively (and removing the same columns in both cases), then (since $\hat{S}$ is obtained multiplying rows of $\tilde{S}$ by powers of t) we have:

$$\begin{aligned} \det(\hat{S}_{ij}) &= \det(\tilde{S}_{ij}) \cdot \left(\prod_{k=1}^{n-j} t^{p_2+(m-n+k-1)p} \right) \cdot \left(\prod_{n+1}^{m+n-j} t^{p_1+(k-n-1)p} \right) \\ &= t^{\ell_2} \det(\tilde{S}_{ij}) \ . \end{aligned}$$

Similarly, S_{ij} and $\hat{S}_{ij}$ contain only columns 1 to $m+n-2j-1$ as well as column $m+n-i-j$ of S and $\hat{S}$ respectively (removing the same rows in both cases), so the relation between the columns of $\hat{S}$ and S gives us:

$$\begin{aligned} \det(\hat{S}_{ij}) &= \det(S_{ij}) \cdot \left(\prod_{k=1}^{m+n-2j-1} t^{p_1+p_2-(n+1-k)p} \right) \cdot t^{p_1+p_2+(m-j-i-1)p} \\ &= t^{\ell_1-ip} \det(S_{ij}) \ . \end{aligned}$$

We can therefore conclude that

$$\det(\tilde{S}_{ij}) = \frac{t^{\ell_1 - ip}}{t^{\ell_2}} \det(S_{ij})$$

with

$$\ell_1 = \left(\sum_{k=1}^{m+n-2j-1} p_1 + p_2 - (n+1-k)p \right) + p_1 + p_2 + (m-j-1)p,$$
$$\ell_2 = \left(\sum_{k=1}^{n-j} p_2 + (m-n-1+k)p \right) + \left(\sum_{k=n+1}^{n+m-j} p_1 + (-n-1+k)p \right).$$

Replacing x by $t^p x$ in the definition of $S_j(f,g)$, we find that the whole polynomial has been multiplied by t^{ℓ_1}/t^{ℓ_2}, so the j-subresultant is a WHP of weight $\ell = \ell_1 - \ell_2 = p_1(n-j) + p_2(m-j) - (nm - j - j^2)p$. □

Corollary 3. *Let f and g two weighted homogeneous polynomials of weight p_1 and p_2 respectively. Let x be an arbitrary variable of weight p and m and n be the degrees in x of f and g respectively, then $Res_x(f,g)$ is weighted homogeneous with weight $p_1 n + p_2 m - nmp$.*

4.2.2 Number of monomials in a WHP

As we will see in the following sections, although computing the trisection polynomial directly is not practical due to extremely high degrees encountered in intermediate steps (namely, the degrees of the final resultants, before the gcd is computed), it can be computed via interpolation techniques.

Knowing that the trisection polynomial is weighted homogeneous is critical to its explicit computation, since it allows us to reduce the computational cost of the interpolation techniques by several orders of magnitudes.

The main advantage of knowing that the polynomial is homogeneous comes from reducing the number of (possible) monomials in the polynomial when comparing with a polynomial of equivalent degrees. Suppose that $p(v_1, \ldots, v_k)$ is a WHP of weight w, with weight w_i for variable v_i (note that this kind of information will typically come from using Corollary 3 and similar results), and assume that $w_1 \leq w_2 \leq \ldots \leq w_k$. if we let d_i be the maximal degree of variable v_i, with $d_i \leq \lfloor w/w_j \rfloor$ (we allow an inequality since in some cases we may have a stronger bound on the degree than what is given by the weight of the polynomial), then the polynomial can be written as

$$p(v_1, \ldots, v_k) = \sum_{\substack{\beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_k w_k = w \\ \beta_i \leq d_i}} \alpha_{\beta_1, \ldots, \beta_k} v_1^{\beta_1} \cdots v_k^{\beta_k} .$$

To illustrate the impact of restricting to WHP, let us consider two multivariate polynomials, the first one non-homogeneous and the second one a WHP of weight w, and assume that in both polynomials all variables reach the maximal degree $d_i = \lfloor w/w_j \rfloor$. The first polynomial will be a sum of up to

$$\prod_{j=1}^{k} \left(\left\lfloor \frac{w}{w_j} \right\rfloor + 1 \right)$$

monomials, which correspond to all the integer points of a k-dimensional lattice in a hyperbox with sides of length d_i.

For the WHP, the monomials correspond to integer points of the intersection between the hyper box and a hyperplane (of dimension $k-1$) passing through the k elementary vertices of the box. The number of monomials is then

$$\sum_{\beta_1=0}^{\left\lfloor \frac{w}{w_1} \right\rfloor} \sum_{\beta_2=0}^{\left\lfloor \frac{w-w_1\beta_1}{w_2} \right\rfloor} \cdots \sum_{\beta_{k-1}=0}^{\left\lfloor \frac{w-w_1\beta_1-\ldots-w_{k-2}\beta_{k-2}}{w_{k-1}} \right\rfloor} \chi_k(\beta_1,\ldots,\beta_{k-1})$$

where $\chi_k(\beta_1,\ldots,\beta_{k-1})$ is 1 if $\frac{w-w_1\beta_1-\ldots-w_{k-1}\beta_{k-1}}{w_k}$ is an integer, and 0 otherwise. Note that we obtain similar sums (with the same total) for any re-ordering of the variables, in particular if we start from v_k down to v_1:

$$\sum_{\beta_k=0}^{\left\lfloor \frac{w}{w_k} \right\rfloor} \sum_{\beta_{k-1}=0}^{\left\lfloor \frac{w-w_k\beta_k}{w_{k-1}} \right\rfloor} \cdots \sum_{\beta_2=0}^{\left\lfloor \frac{w-w_3\beta_3-\ldots-w_k\beta_k}{w_2} \right\rfloor} \chi_1(\beta_2,\ldots,\beta_k) \; .$$

The number of monomials will therefore be a proportion close to

$$1 \; : \; \frac{(k-1)!w}{\min\{w_i\}}$$

of the number obtained using only the maximal degrees.

When it comes to computing the polynomial, this reduction is critical: in order to interpolate the polynomial, we need at least one evaluation point per monomial, so reducing the number of (possible) monomials reduces the number of evaluations required. The remainder of this section will be dedicated to showing how to perform the interpolation with this minimal number of evaluations.

Interpolation of WHPs

Before going through the fine details of the interpolation process for trisection polynomials, we will describe the general idea of interpolation for homogeneous weighted polynomials and illustrate this idea with a small example.

If we interpolate considering only the maximal degree in each variable, we need evaluations for $d_j + 1$ distinct values of variable v_j, independently of the other variables, for a total of $\prod_{j=1}^{k}(d_j+1)$ evaluations. In this situation, for each tuple in $(v_2,\ldots,v_k)$ we have $d_1 + 1$ values to interpolate a polynomial of degree d_1 in v_1 (one such polynomial for each tuple). Then, for each tuple in

$(v_3, \ldots, v_k)$, we have $d_2 + 1$ polynomials in v_1 which we combine coefficient-by-coefficient (i.e. for each powers of v_1), considering that each coefficient is a polynomial of degree d_2 in v_2. This process is then iterated for the remaining variables, producing the complete polynomial.

When working with WHPs, the idea is similar. For a fixed tuple $(v_2, \ldots, v_k)$, we use the evaluations of the polynomials for the different values of v_1 to obtain an interpolation polynomial in v_1, and this process is then iterated in the other variables (working from the coefficients of the distinct powers of v_1) to obtain the complete polynomial.

However, having fixed weight for the monomials means that even with a single tuple $(v_2, \ldots, v_k)$ used, some of the monomials (those of highest degree in v_1) will be completely determined from the polynomial in v_1 that we obtained (since they cannot depend on the remaining variables, otherwise the total weight would be greater than the weight of the WHP). Each time a monomial is completely determined, it is removed from the evaluated values before doing further interpolations (that is to say, we subtract the evaluation of this monomial from the value of the complete polynomial at the point $(v_1, \ldots, v_k)$), which has the effect of decreasing the degree of the polynomial to interpolate, and so decreases the number of evaluation points required. As a result, the number of distinct values of v_1 required for each tuple in $(v_2, \ldots, v_k)$ will decrease over time, going down by one each time all the monomials containing v_1 to a given power have been completely determined. Once again, this process is iterated in the remaining variables.

In this approach, if we first interpolate in terms of variable v_1, then each tuple $(v_2, \ldots, v_k)$ can be viewed as a stack of values in v_1, and we interpolate using the highest stacks first (i.e. those with the most values) so we can compute the terms of highest degrees in v_1 and make our way down (after removing these terms from the values of the shorter stacks). The process then runs iteratively for the next variable, using the coefficients of the resulting polynomials in v_1 as the values for the next iteration.

Following this idea, we can reduce the number of evaluations of the polynomial to one tuple (in $(v_1, \ldots, v_k)$) for each of the possible monomials in the polynomial expansion. Note that in this description, the final variable will never need interpolation since if we have fixed the degrees in $v_1, \ldots, v_{k-1}$, then there is only one possible power of v_k to obtain total weight w, and the “interpolation” is done with a single point.

A natural adjustment of the interpolation to take into account this observation is to choose one variable which will be evaluated to the fixed value 1 right from the start (effectively making it the last variable in the description above) and compute a non-homogeneous polynomial of weight bounded by w in the remaining $k - 1$ variables. The polynomial obtained is then “filled-up” to a WHP of weight w. We prefer to do this with v_1 (the variable of lowest weight) since it simplifies the arithmetic required to ensure the filling up is possible. If $w_1 = 1$, we only need to "fill-up" the monomials up to weight w by multiplying to the appropriate degree of v_1. If $w_1 > 1$ (this will be the case in our interpolations), we first have to restrict the possible monomials so their total weight is of the form $w - \beta w_1$ (with β an integer), so the filling-up consists in multiplying the monomial by v_1^β.

4.2.3 Example

Suppose that we have a WHP of weight 15 in $\mathbb{Z}[x, y, z]$, with variables x, y and z having respective weights 1, 3 and 5. It is easy to see that $f(x, y, z)$ must be of the form

$$\begin{aligned} f(x,y,z) = {} & \alpha_1 x^{15} + \alpha_2 x^{12} y + \alpha_3 x^9 y^2 + \alpha_4 x^6 y^3 + \alpha_5 x^3 y^4 \\ & + \alpha_6 y^5 + \alpha_7 x^{10} z + \alpha_8 x^7 yz + \alpha_9 x^4 y^2 z \\ & + \alpha_{10} x y^3 z + \alpha_{11} x^5 z^2 + \alpha_{12} x^2 y z^2 + \alpha_{13} z^3 \end{aligned}$$

so it has 13 monomials instead of the $16 \cdot 6 \cdot 4 = 384$ that would be expected if we only bounded by the maximal degrees in each variable (the proportion 13 to 384 is close to the expected 1 in $2! \cdot 15 = 30$ from the discussion above).

Evaluating x in 1, we are left with

$$\begin{aligned} f(1,y,z) = {} & \alpha_1 + \alpha_2 y + \alpha_3 y^2 + \alpha_4 y^3 + \alpha_5 y^4 + \alpha_6 y^5 + \alpha_7 z \\ & + \alpha_8 yz + \alpha_9 y^2 z + \alpha_{10} y^3 z + \alpha_{11} z^2 + \alpha_{12} y z^2 + \alpha_{13} z^3, \end{aligned}$$

which has degree 5 in y and degree 3 in z, so to interpolate, we need the value of the polynomial in 6 values of y: y_1, y_2, y_3, y_4, y_5, and y_6; and in 4 values of z: z_1, z_2, z_3, and z_4. However, we can complete the interpolation with only 13 pairs of these points (out of a possible 24 pairs):

$$\begin{array}{llllll} (y_1, z_1), & (y_2, z_1), & (y_3, z_1), & (y_4, z_1), & (y_5, z_1), & (y_6, z_1), \\ (y_1, z_2), & (y_2, z_2), & (y_3, z_2), & (y_4, z_2), & & \\ (y_1, z_3), & (y_2, z_3), & & & & \\ (y_1, z_4). & & & & & \end{array}$$

For the sake of this example, let $y_i = i$ and $z_i = i$, and suppose that we have the evaluations:

$$\begin{array}{rrr} f(1,1,1) = 99, & f(1,2,1) = 701, & f(1,3,1) = 4011, \\ f(1,4,1) = 15129, & f(1,5,1) = 43427, & f(1,6,1) = 103869, \\ f(1,1,2) = 211, & f(1,2,2) = 843, & f(1,3,2) = 4215, \\ f(1,4,2) = 15439, & f(1,1,3) = 421, & f(1,2,3) = 1085, \\ f(1,1,4) = 765. & & \end{array}$$

The interpolation proceeds as follows:

1. Interpolate for the points in $z_1 = 1$, obtaining

$$\begin{aligned} g_1(y) &= f(1,y,1) \\ &= 11y^5 + 13y^4 + 5y^3 + 9y^2 + 4y + 57 \end{aligned}$$

   - Extract the coefficients of y^5 and y^4.

2. Using the points in $z_2 = 2$ and subtracting $11y_i^5 + 13y_i^4$, interpolate to obtain the degree 3 polynomial

$$\begin{aligned} g_2(y) &= f(1,y,2) - (11y^5 + 13y^4) \\ &= 7y^3 + 13y^2 + 8y + 159 \end{aligned}$$

   - Using the coefficients of y^3 in $g_1(y)$ and $g_2(y)$, interpolate to obtain the coefficient (in $\mathbb{Z}[z]$) of y^3 in $f(1,y,z)$:

$$(2z+3)\,y^3$$

   - Using the coefficients of y^2 in $g_1(y)$ and $g_2(y)$, interpolate to obtain the coefficient (in $\mathbb{Z}[z]$) of y^2 in $f(1,y,z)$:

$$(4z+5)\,y^2$$

3. Using the points in $z_3 = 3$ and subtracting $11y_i^5 + 13y_i^4 + (2z_i+3)y_i^3 + (4z_i+5)y_i^2$, interpolate to obtain the degree 1 polynomial

$$\begin{aligned} g_3(y) &= f(1,y,3) - (11y^5 + 13y^4 + 2y^3z + 3y^3 + 4y^2z + 5y^2) \\ &= 14y + 357 \end{aligned}$$

   - Using the coefficients of y in $g_1(y)$, $g_2(y)$, and $g_3(y)$, interpolate to obtain the coefficient (in $\mathbb{Z}[z]$) of y in $f(1,y,z)$:

$$\left(z^2 + z + 2\right) y^1$$

4. Using the point in $z_4 = 4$ and subtracting $11y_i^5 + 13y_i^4 + (2z_i+3)y_i^3 + (4z_i+5)y_i^2 + (z_i^2 + z_i + 2)y_i$, obtain the value

$$\begin{aligned} g_4(y) = f(1,y,3) - (11y^5 &+ 13y^4 + 2y^3z + 3y^3 \\ &+ 4y^2z + 5y^2 + yz^2 + yz + 2y) \\ = 687 \end{aligned}$$

   - Using the constant coefficients in $g_1(y)$, $g_2(y)$, $g_3(y)$, and $g_4(y)$, interpolate to obtain the coefficient (in $\mathbb{Z}[z]$) of y^0 in $f(1,y,z)$:

$$\left(6z^3 + 12z^2 + 24z + 15\right) y^0$$

It only remains to multiply the terms of $f(1,y,z)$ by the correct powers of x to obtain a homogeneous weighted polynomial and we find:

$$\begin{aligned} f(x,y,z) = 15x^{15} &+ 2x^{12}y + 5x^9y^2 + 3x^6y^3 + 13x^3y^4 + 11y^5 + 24x^{10}z \\ &+ x^7yz + 4x^4y^2z + 2xy^3z + 12x^5z^2 + x^2yz^2 + 6z^3. \end{aligned}$$

4.3 Trisections

4.3.1 Special cases

In order to study the trisection polynomials for general divisors, we must first look at the special cases that could occur since they will help us during the computation of the trisection polynomial (they allow us to determine the weight exact weight of the polynomial and the coefficients of lowest and highest degrees).

Special cases involving Weierstrass points in the affine support of D_1 can be handled easily within the general cases (see Section 4.3.1). For all special cases discussed in details, D_3 has weight 2, i.e. $[u_3(x), v_3(x)] = [x^2 + u_{31}x + u_{30}, v_{31}x + v_{30}]$, since there are no special cases when D_3 has weight one (unless the affine support is a Weierstrass point).

Weight-1 trisections

The most obvious special case of trisection is when D_1 has weight 1 instead of (the much more common) weight 2.

If we assume that the divisors D_1 is of the form $[u_1(x), v_1(x)] = [x+u_{10}, v_{10}]$, then using the composition step of cantor algorithm we obtain two polynomials of the form $[u^3, \tilde{v}]$ for $3D_1$ and if we de-reduce D_3 via the polynomial $\beta^2 - \alpha^2 f \equiv 0 \bmod u_3$ where $\beta = \gamma u_3 + \alpha v_3$, $\gamma = c_0$ and $\alpha = 1$ and equate the two un-reduced divisors, we obtain:

$$u_1^3 = \frac{(\gamma u_3 + \alpha v_3)^2 - \alpha^2 f}{u_3}. \tag{4.3.1}$$

The coefficients of x^2, x^1 and x^0 give us three equations in u_{10} and c_0:

$$0 = c_0^2 + u_{31} + 3u_{10} \tag{4.3.2}$$

$$0 = c_0^2 u_{31} + 2c_0 v_{31} - f_3 + u_{30} - u_{31}^2 + 3u_{10}^2 \tag{4.3.3}$$

$$0 = c_0^2 u_{30} + 2c_0 v_{30} + v_{31}^2 - f_2 - 2u_{31}u_{30} + u_{31}f_3 + u_{31}^3 + u_{10}^3 \tag{4.3.4}$$

From (4.3.2) we put u_{10} in terms of c_0

$$u_{10} = -\frac{c_0^2 + u_{31}}{3}.$$

Substituting the expression of u_{10} into (4.3.3) and (4.3.4) gives us polynomials of degree 4 and 6 in c_0 respectively:

$$0 = 5c_0^2 u_{31} + 6c_0 v_{31} - 3f_3 + 3u_{30} - 2u_{31}^2 + c_0^4 \tag{4.3.5}$$

$$\begin{aligned} 0 =& 27c_0^2 u_{30} + 54c_0 v_{30} + 27v_{31}^2 - 27f_2 - 54u_{31}u_{30} \\ &+ 27u_{31}f_3 + 26u_{31}^3 - c_0^6 - 3c_0^4 u_{31} - 3c_0^2 u_{31}^2 \end{aligned} \tag{4.3.6}$$

and c_0 must satisfy both equations at the same time. Given such a c_0, backtracking through the equations easily gives us the trisection.

Proposition 5. *D_3 admits a weight 1 trisection if only if the polynomial $L = Res_{c_0}(L_1, L_2)$ (with L_1 and L_2 the polynomials in c_0 appearing in (4.3.5) and (4.3.6)) evaluated in the values of f_2, f_3, u_{30}, u_{31} and v_{31} returns* 0.

Remark 1. If the curve parameters f_i are given weight $10-2i$, and the divisor coordinates u_{3i} and v_{3i} are given weight $4-2i$ and $5-2i$ respectively, then L is a WHP of weight 24.

Simple quadratic de-reduction for weight-2 divisors

When both D_1 and D_3 have weight 2, there is still a situation where the de-reduction approach must be dealt with independently. In the general de-reduction (Section 4.3.2, via the polynomial $\beta^2 - \alpha^2 f \equiv 0 \bmod u_3$ with $\beta = \gamma u_3 + \alpha v_3$, $\gamma = c_2x^2 + c_1x + c_0$ and $\alpha = a_1x + a_0$) we usually asume that $a_1 \neq 0$ in order to solve the system.

However, for some divisors D_1, $a_1 = 0$, and the shape of the system changes drastically. In [16], this situation was called *simple quadratic de-reduction* since it corresponds to using the principal divisor of the quadratic equation $a_0y - c_2x^2 + c_1x + c_0$. In theory, this might be considered part of the general case, but the solution technique uses division by a_1 to solve the system, in effect taking out the simple quadratic de-reduction cases.

We now assume that divisors D_1 are of the form $[u_1(x), v_1(x)] = [x^2 + u_{11}x + u_{10}, v_{11}x + v_{10}]$, and attempt the de-reduction technique via $\beta^2 - \alpha^2 f \equiv 0 \bmod u_3$ with $\beta = \gamma u_3 + \alpha v_3$, $\gamma = x^2 + c_1x + c_0$ and $\alpha = a_0$. D_3 will admit a simple quadratic de-reduction if and only if the resulting system admits a solution.

As in other cases, we have:

$$u_1^3 = \frac{(\gamma u_3 + \alpha v_3)^2 - \alpha^2 f}{u_3} = \gamma^2 u_3 + 2\alpha\gamma v_3 + \alpha^2\left(\frac{v_3^2 - f}{u_3}\right) \ , \tag{4.3.7}$$

and the coefficients of x^5, x^4, x^3, x^2, x^1 and x^0 provide 6 Equations in 5 unknowns (u_1, u_0, c_1, c_0 and a_0):

$$0 = u_{31} + 2c_1 - 3u_{11} \tag{4.3.8}$$

$$0 = 2c_1u_{31} + u_{30} + c_1^2 + 2c_0 - 3u_{10} - 3u_{11}^2 \tag{4.3.9}$$

$$0 = c_1^2u_{31} + 2a_0v_{31} + 2c_1c_0 - 6u_{11}u_{10} + 2c_0u_{31} + 2u_{30}c_1 - u_{11}^3 \tag{4.3.10}$$

$$\begin{aligned} 0 &= a_0^2u_{31} - 3u_{11}^2u_{10} + 2a_0c_1v_{31} + 2c_1c_0u_{31} + c_0^2 + 2v_{30}a_0 \\ &\quad + 2u_{30}c_0 + u_{30}c_1^2 \end{aligned} \tag{4.3.11}$$

$$\begin{aligned} 0 &= 2u_{30}c_1c_0 - a_0^2u_{31}^2 - a_0^2f_3 + 2a_0c_0v_{31} - 3u_{11}u_{10}^2 + c_0^2u_{31} \\ &\quad + 2v_{30}a_0c_1 + u_{30}a_0^2 \end{aligned} \tag{4.3.12}$$

$$\begin{aligned} 0 &= a_0^2u_{31}f_3 + a_0^2v_{31}^2 - a_0^2f_2 - 2u_{30}a_0^2u_{31} + a_0^2u_{31}^3 - u_{10}^3 \\ &\quad + 2v_{30}a_0c_0 + u_{30}c_0^2 \end{aligned} \tag{4.3.13}$$

From (4.3.8) we can write u_{11} in terms of c_1,

$$u_{11} = \frac{2c_1 + u_{31}}{3} \ , \tag{4.3.14}$$

and then (4.3.9) can be used to write u_{10} in terms of c_2 and c_1,

$$u_{10} = \frac{1}{9}(u_{31}^2 + 3u_{30} + 6c_0 - c_1^2 + 2u_{31}c_1) \ . \tag{4.3.15}$$

If we assume that $c_1 \neq u_{31}$, then Equation 4.3.10 can be used to write c_0 in terms of a_0 and c_1,

$$\begin{aligned} c_0 = \frac{1}{18(u_{31} - c_1)}\big(& - 18u_{30}c_1 + 18u_{30}u_{31} + 27a_0^2 + 3c_1^2u_{31} \\ & - 5u_{31}^3 - 54v_{31}a_0 - 4c_1^3 + 6c_1u_{31}^2\big) \ . \end{aligned} \tag{4.3.16}$$

Note that the case $c_1 = u_{31}$ gives a simpler system that can be handled separately to obtain similar (but more restrictive) conditions.

Substituting identities (4.3.14), (4.3.15) and (4.3.16) into (4.3.11), (4.3.12), (4.3.13) we obtain polynomials E_1, E_2 and E_3 of degrees 4, 4 and 6 in a_0 respectively. The coefficient of a_0^4 in (4.3.11) is a non-zero constant, so we can replace E_2 and E_3 by $E_{2a} = E_2 \bmod E_1$ and $E_{3a} = E_3 \bmod E_1$, from which we can remove multiples of $(u_{31} - c_1)$. Let $E_{2b} = (u_{31} - c_1)^{-1}E_{2a}$ and $E_{3b} = (u_{31} - c_1)^{-2}E_{3a}$. We then progressively reduce the degrees in a_0 and c_1 of the three equations: first set $E_{3c} = v_{31}E_{3b} \bmod E_{2b}$ and remove a factor of $(u_{31} - c_1)$ to get $E_{3d} = (u_{31} - c_1)^{-1}E_{3c}$, then let $E_{1a} = E_1 \bmod E_{2b}$, and finally $E_{2c} = v_{31}E_{2b} \bmod E_{3c}$.

We remove the remaining variables using resultants, but to avoid parasitic factors we do it twice (alternating the order of removal) and compute the gcd of the two resulting polynomials to weed out all parasites (since a solution to the system should come out no matter in which order we remove the variables). We compute $r_1 = Res_{a_0}(E_{1a}, E_{2c})$ and $r_2 = Res_{a_0}(E_{1a}, E_{3d})$ and remove a factor of $(u_{31} - c_1)$ from both of them (to obtain $\tilde{r}_1$ and $\tilde{r}_1$), and then compute $R = Res_{c_1}(\tilde{r}_1, \tilde{r}_2)$. Similarly, we compute $s_1 = Res_{c_1}(E_{1a}, E_{2c})$ and $s_2 = Res_{c_1}(E_{1a}, E_{3d})$ and remove a factor of a_0 from both, then compute $S = Res_{a_0}(s_1, s_2)$. We finally obtain $M = gcd(R, S)$.

Proposition 6. *A weight-2 divisor D_3 admits a trisection by simple quadratic de-reduction if only if the polynomial M evaluated in the values of f_2, f_3, u_{30}, u_{31} and v_{31} returns* 0.

Remark 2. If the curve parameters f_i are given weight $10 - 2i$, and the divisor coordinates u_{3i} and v_{3i} are given weight $4 - 2i$ and $5 - 2i$ respectively, then M is a WHP of weight 105.

Trisections with Weierstrass points

When the affine support of trisection D_1 contains one (or more) Weierstrass point, then the assumptions used in the general case to compute $3D_1$ (using

Cantor's algorithm) do not hold, giving rise to a number of special cases. However, these cases do not require a detailed description, as we now show.

If the affine support of D_1 consists of two Weierstrass points, then $D_3 = 3D_1 = D_1$ (i.e. D_3 is its own triple/trisection). In terms of the non-Weierstrass cases, it corresponds to a simple quadratic de-reduction with $\alpha = 0$ and $\gamma = u_3$. This case can be handled directly as part of the special case in Section 4.3.1.

If the affine support of D_1 (of weight 1) consists of one Weierstrass point, then once again $D_3 = 3D_1 = D_1$ (i.e. D_3 is its own trisection). In terms of the non-Weierstrass cases, it corresponds to the equivalent of a simple quadratic de-reduction for weight 1 trisectees, although a correct description would be *simple linear de-reduction*, with $\alpha = 0$ and $\gamma = u_3$. Note that for $D_3 = [x + u_{30}, v_{30}]$, the affine support is a Weierstrass point if and only if $v_{30} = 0$.

Proposition 7. *For D_3 of weight 1, the simple linear de-reduction occurs if and only if $v_{30} = 0$.*

If D_1 has weight 2 and its affine support contains one Weierstrass point $P_0 = (x_0, y_0)$ (and a non-Weierstrass point), the de-reduction can be handled by the general case in Section 4.3.2 if we relax the condition $\gcd(\alpha, \gamma) = 1$. Taking $\gcd(\alpha, \gamma) = (x - x_0)$, so $\alpha = a_1(x - x_0)$ and $\gamma = (x - x_0)(x - s)$ allows us to deal with the factor $(x - x_0)^2$ that is removed in Cantor's algorithm (corresponding to removing the principal divisor $div(x - x_0)$).

4.3.2 General case for weight-2 divisors

To compute the trisection polynomial we solved a trivariate polynomials system where E_1, E_2' and E_3' arepolynomials in $\mathbb{F}_q[a_1, c_0, a_0]$ of degree 4, 4 and 6 in a_0 (reduced modulo E_1 in the case of E_2' and E_3', see [19] for more details). First we compute $r_1 = Res_{a_0}(E_1, E_2')$, $r_2 = Res_{a_0}(E_1, E_3')$ and $r_3 = Res_{a_0}(E_2', E_3')$ (from r_1, r_2 and r_3 can be remove predictable factors). If $R_1 = Res_{c_1}(r_1, r_2)$, $R_2 = Res_{c_1}(r_1, r_3)$ and $G = \gcd(R_1, R_2)$. From G we can remove predictable factors. We obtain a trisections polynomials of degree 81.

Corollary 4. *The trisection polynomial for weight-2 divisors on the curve C is weighted homogeneous, where the curve parameters f_i have weight $10 - 2i$, the divisor coordinates u_{3i} and v_{3i} have weight $4 - 2i$ and $5 - 2i$ respectively and the trisection variable a_1 has weight 1.*

Proof All the equations in the system defining the trisection are WHPs, and the techniques used to obtain the solutions are compatible with the properties described in Section 4.2.1, so all polynomials worked with are WHPs, including the resultants and the final gcd (see Table 4.1). Since the trisection polynomial is a factor of this gcd, it must also be a WHP. □

Proposition 8. *The trisection polynomials for D_3 of weight 2 has the following properties:*

Polynomial	*weight*
E_1	12
E'_2	14
E'_3	18

Polynomial	*weight*
r_1	40
r_2	48
r_3	47

Polynomial	*weight*
R_1	960
R_2	940
G	≤ 940

Table 4.1: Weight of the polynomials used in the trisection

(i) The coefficient of a_1^{81} *is* 0 *if only if one of the trisections* D_1 *has weight 1.*

(ii) The constant coefficient is 0 *if and only if there exists a trisection* D_1 *that can be obtained by simple quadratic de-reduction.*

Proof In general, the polynomial has degree 81 in a_1 corresponding to 81 weight-2 trisections, the only exception being if there are weight-1 trisection, in which case the polynomial degree must be at most 80 (which corresponds to the coefficient of a_1^{81} equal to 0). Therefore the coefficient of a_1^{81} is a constant multiple of a power of L where $L = Res_{c_0}(L_1, L_2)$ from Proposition 5. On the other hand, if the trisection has weight two, then the only situation which is not handled correctly by the general case is the simple quadratic de-reduction, which corresponds to $a_1 = 0$, i.e. the trisection polynomial $p(x)$ is divisible by x. From Proposition 6, the constant term of the trisection polynomial must be a constant multiple of a power of M. □

Corollary 5. *The weight of the trisection polynomial is 105.*

Proof From Remarks 1 and 2, the weights of the constant coefficient and the leading coefficient are multiples of 105 and 24 respectively. The weight of trisection polynomial must satisfy $105a = 81 + 24b$ where a and b are non-negative integers. As $a_0 = b_0 = 1$ is a possible solution, all other solutions are of the form $a = 1 + 8t$ and $b = 1 + 35t$, with $t \in \mathbb{Z}$. The next smallest positive solution will then be $a_1 = 9$ and $b_1 = 36$, which would give weight $9 \cdot 105 = 945$, but the weight of $G = \gcd(R_1, R_2)$ is at most 940. Therefore $a_0 = b_0 = 1$ is the only possible solution. □

4.3.3 General case for weight-1 divisors

The construction of the trisection polynomial for weight-1 divisors follows similar lines to that of weight-2 divisors. To compute the trisection polynomial we solved a trivariate polynomials system obtaining (after simplifications) three equations E'_1, E'_2 and E''_3 in $\mathbb{F}_q[c_2, c_1, a_0]$ of degree 1, 2 and 1 in c_1 respectively (see [19]). From E'_1 we can write c_1 in terms of a_0 and c_2. We then compute $r_1 = Res_{c_1}(E'_1, E'_2)$, $r_2 = Res_{c_1}(E'_1, E''_3)$ and $R = Res_{a_0}(r_1, r_2)$, where R has degree 350 in c_2.

Several parasitic factors can be removed from R: Since the polynomial E'_1 is used to remove c_1 from E'_2 and E''_3, we get parasitic factors if the whole polynomial is 0 independent of c_1, that is to say if both m_1 and m_2 are 0 at the same time, where m_1 and m_0 are the coefficients of degrees c_1^1 and c_1^0 in E_1'. Let $s_r = Res_{a_0}(m_1, m_0)$, then $\gcd(R, s_r)$ is a polynomial of degree 109 in c_2 which be removed twice from R. Let $s_r = Res_{a_0}(m_1, m_0)$, then $gcd(R, s_r)$ (and its factorization) produces two factors that can be removed from R: one of degree 109 which appears twice, and one of degree 17 which appears three times, leaving us with a polynomial $p(c_2)$ of degree 81 in c_2.

Corollary 6. *The trisection polynomial for weight-1 divisors on the curve C is weighted homogeneous, where the curve parameters f_i have weight $10 - 2i$, the divisor coordinates u_{30} and v_{30} have weight 2 and 5 respectively and the trisection variable c_2 has weight 1.*

Proof The argument are identical to those in Corollary 4, with the weights in Table 4.2. □

Polynomial	*weight*
E_1	9
E_2	12
E_3	14

Polynomial	*weight*
r_1	32
r_2	28
R	448

Table 4.2: Weight of the polynomials used in the trisection

Corollary 7. *The weight of the trisection polynomial is 96.*

Proof We follow a similar approach to that of Corollary 5. From Proposition 7, the weight of the coefficient of c_2^{81} is a multiple of 5. For the constant coefficient, we do not have a special case of de-reduction, but we can "construct" one: we set $c_2 = 0$ and solve the resulting system to equations $E_1 = 0$, $E_2 = 0$ and $E_3 = 0$ (as above) but in only two variables (c_1 and a_0), and use a similar approach to that used in the simple quadratic de-reduction to remove parasitic factors, obtaining a polynomial of weight 96. The weight of trisection polynomial must then satisfy $96a = 81 + 5b$ where a and b are non-negative integers. As $a_0 = 1$, $b_0 = 3$ is a possible solution, all other solutions are of the form $a = 1+5t$ and $b = 3+96t$, with $t \in \mathbb{Z}$. The next smallest positive solution will then be $a_1 = 6$ and $b_1 = 99$, which would give weight $6 \cdot 96 = 576$, but the weight of $R = \gcd(r_1, r_2)$ is 448. Therefore $a_0 = 1$, $b_0 = 3$ is the only possible solution. □

4.4 Symbolic computation

We now give some further details on the techniques required to make the homogeneous interpolation fully practical to compute trisection polynomials. For simplicity, we will write the description in terms of the general weight-2 case, the weight-1 case is similar.

Since the theory of trisection polynomials is based on obtaining a degree 81 polynomial in a_1 (that is to say, the form of the polynomial in a_1 is known), whereas the theory does not directly tell us the form of the "trisection polynomial" in terms of the other variable/parameters, our interpolation techniques are based on interpolation "points" which are polynomials in a_1 rather than constants. Also recall that the coefficient of a_1^{81} is known up to a constant factor (we will return to this in Section 4.4.3), and can be computed directly. Although we could also compute the coefficient of a_1^0, its weight makes it rather costly to use and we in fact "forget" it in the following computations (and compute it as any other coefficient rather than computing it directly).

Rather than interpolate the trisection polynomial as a whole of weight w, we interpolate the coefficients of each of the 81 remaining powers of a_1 (from a_1^0 to a_1^{80}), where the coefficient of a_1^j is homogeneous of weight $w - j$.

4.4.1 Parity and interpolation points

When interpolating for trisection polynomials, one of the variables has weight 1 (variable a_1), one has weight 2 (variable u_{30}) and the remaining variables have weight greater than 2. Since we obtain polynomials in a_1, the variable of lowest weight that we can work with is u_{30} with weight 2. This variable is set to value 1 and the total weight of the remaining variables (including a_1) must be of the same parity as w.

To ensure this, we first interpolate in the variables of odd weight, and observe that the degrees of the last of these (say v_j) must be either all odd or all even (depending on the degrees of the other variables of odd weight), which leads to an odd or even function in v_j. Taking advantage of the identity $f(-v_j) = f(v_j)$ for even functions and $f(-v_j) = -f(v_j)$ (with $f(0) = 0$) for odd functions, we can reduce the number of evaluations in v_j by a factor close to 2 (and hence the number of polynomials in a_1 by a similar factor). In effect, if v_j has weight k, then for the interpolation process it will behave as a variable of weight $2k$.

In order to interpolate the general trisection polynomials, we used the following approach:

- The set of values for a given variables does not (in general) have to depend on the values taken by the others variables. We preferred to "re-use" the same sets of values so the interpolation process could be accelerated with precomputations.

- The tuples are chosen in terms of interpolation, but each tuple corresponds to a curve and a divisor in the Jacobian of that curve. Note that some of the curve coefficients do not appear directly in the tuple, for example f_0, but are fully determined by the coordinates of the divisor (due to the divisibility condition: $u(x)|f(x)-v(x)^2$). In general, distinct tuples will be correspond to distinct curves, although in some rare occasions two tuple could correspond to the same curve (this does not cause any problem for the interpolation).

- Some tuples must be avoided at all cost, namely those that correspond to singular curves (for which the trisection polynomial will not have the same form).
- We also avoid all tuples for which the coefficient of a_1^{81} would be 0. Since the symbolic form of this coefficient is known, this can be checked quickly for all tuples before actually computing the trisection polynomials.

We used value sets of the form $\{b+1, b+2, b+3, \ldots, b+k\}$ where b is an offset to avoid all singular curves and coefficients of a_1^{81} that go to 0. For our computation, $b=7$ was sufficient (for the weight-1 case, we can take $b=0$).

4.4.2 Finite fields vs the integers

Although the trisection polynomials we are looking for should be defined over the integers, it is impractical to compute them via interpolation over the integers themselves. Mainly, this is due to the computation of the trisection polynomial itself: the partial computations (in particular the last round of resultants, before the final gcd computation) produces polynomials whose degrees are close to one thousand.

Since we need to evaluate at a large number of points, the values of the of each variable cannot be restricted to $0, \pm 1$, and the evaluation of each monomial in the trisection polynomial can then be expected to have more than a thousand bits in size. Taking into account the cumulative effect of the large number of terms (a little over one million in the final result, and much higher in the intermediate polynomials), one could reasonably expect some of the evaluations to give values of more than one billion bits. Simply storing these evaluations would become prohibitive, not to mention the cost of the integer arithmetic.

It then becomes much more practical to perform the work over prime fields $\mathbb{F}_{p_i}$, to obtain the symbolic trisection polynomial mod p_i for various p_i and then combine them via the Chinese Remainder Theorem. Each coefficient will then be approximated modulo $p = \prod p_i$, and if p is large enough, the smallest (signed) value modulo p of each coefficient gives us its value over the integers.

To give an upper bound on the (absolute) value of the coefficients, we looked at the smallest of the final resultants ($R_2 = res_{c_1}(r_1, r_3)$ in Section 4.3.2) and bounded its largest coefficient. We first observe that the sum of the absolute value of the coefficients in r_1 is 15389396856842800, and the similar sum for r_3 is 111609314342607003444436134. These two values are used to obtain bounds on the coefficients when we take products of parts of r_1 with parts of r_3.

We first operated on the terms in the Sylvester matrix as follows: each non-zero entry in the matrix is replaced by the bound on the coefficients of the polynomial it comes from. This substitution will give a matrix with 3 possible values for the entries: 0, 15389396856842800 (for the first 19 rows) and 11160931434260700344436134 (for the last 20 rows). Given the form of the matrix, a recursive determinant algorithm would compute $10! \cdot 11! \cdot 20!$ different products of 39 terms, 19 of which are 15389396856842800 and the other 20 are 11160931434260700344436134. We then ignore all signs in the determinant computation and obtain an upper bound of

$$10! \cdot 11! \cdot 20! \cdot 15389396856842800^{19} \cdot 11160931434260700344436134^{20} \ .$$

The resulting 2794-bit value is then an upper bound for the sum of (the absolute value of) all the coefficients in the resultant, which we then take as an upper bound on the coefficient themselves, and on the coefficient of the trisection polynomial (which is a factor of the resultant).

Even though we obtained a bound of 2794 bits, it is much larger than the maximal size of the coefficients observed in the final trisection polynomials, which stands at 134 bits. This difference is not surprising: first of all, the bound ignored all possible cancellation during the computation of the resultants, and accumulates all the coefficients together (and will therefore overestimate the largest value). Secondly, the bound did not take into account the factors that can be explained theoretically [19] nor those that are removed when we take the gcd of the final set of resultants (Section 4.3.2). Since the weight of the (smallest) resultant is almost 9 times larger than that of the of trisection polynomial, it is not surprising that the bound on the coefficients is at least 9 times larger than desired.

For the computation, we first worked modulo a single prime p of 320 bits, and used the signed residue mod p to obtain the coefficient over the integers. We found that all coefficients were less than 2^{135}, which indicated that we had 185 bits of redundancy. The result could then be verified modulo 6 primes of 416 bits each, to give us the a total bound of 2816 bits (and confirming the redundancy in the computations). Dividing the verification into 6 primes was done to simplify running the computation as three parallel processes and minimizing the total time.

4.4.3 Re-scaling the interpolation points

The main problem to interpolate trisection polynomials is that they are obtained via resultants and gcds. When working over a field, these operations preserve the factorization properties of the polynomials (their roots), but will not be concerned with multiplying (or dividing) the polynomial by a constant factor. In fact, most implementations of the gcd computation will return a monic polynomial, whereas the symbolic polynomial may not be monic at all. This problem becomes even more acute if we consider that most of the work is performed over finite fields, whereas the polynomial that we are looking for is defined over the ring of the integers (and in general cannot be made monic).

Here the theoretical results on the coefficients of a_1^{81} and a_1^0 used in Section 4.3 to obtain the weight of the trisection polynomial come to our help once again. Knowing the form of the highest and lowest degree coefficients of the trisection polynomial can clearly be used to "re-scale" it (i.e. return it to the form it should have been before being made monic). However, both of these terms are known in terms of their roots, so both may be missing a constant factor, which required some extra care, especially if the gcd of the missing factors is greater than 1.

To get a good idea of the actual coefficient, we first did some computations over the integers with a limited number of symbolic variables (a_1 and 2 or 3 others), giving the remaining variables value 1. In this way, we could be fairly confident of the "extreme terms" in the trisection polynomial (monomials in which at most 3 of the variables appear, for example $f_3^6 \cdot a_1^{81}$ or v_{30}^{21}) and comparing with the theoretical form, get a fairly good idea of the missing constant factor (if any).

At this point, we could not completely exclude that some small constant factors were incorrectly removed due to the evaluation of the remaining variables as 1. Typically, "incorrect" factors of 2 or 3 may be expected to show up in the polynomial when doing such evaluation, due to the accumulations of various terms together. We could have introduced a few extra factors (e.g. powers of 2 and 3) as a precaution, but we first tried the computations as if there was no missing factor, and then checked if the results were consistent throughout the trisection polynomial. This assumption proved correct, since the coefficients obtained were so much smaller than the 320-bit prime and, any missing factor would have been easily identified.

For simplicity, we only used the coefficient of a_1^{81} for re-scaling, and kept the coefficient of a_1^0 as a safety check for the computation (that is to say, we re-interpolated it as if we did not know it, and checked that the result matched the theory). This was done mostly to save the work of repeatedly evaluating a weight 105 polynomial, and because the difference in interpolating down to a_1^1 or a_1^0 is minimal (especially when taking advantage of the parity).

One problem remains with re-scaling: interpolation points where the coefficient of a_1^{81} goes to zero (so there would be no value to "re-scale" with). As we stated at the end of Section 4.4.1, it is easy to check beforehand if any tuples will give a trisection polynomial of degree less than 81 and avoid it. In fact, avoiding singular curves appeared to be more difficult than when using "small" values for the variables to interpolate, but in any case both sets of "bad" curves appear to be sparse on a larger scale.

4.4.4 Symbolic trisection polynomial

Remark 3. The full computation (with verification) took 682.7 hours using Magma on a 2.9 GHz Intel core i5 running Mac OS X. For the weight-1 trisection polynomial, the total computation time was 11 hours and 26 minutes. To obtain these timings, it was necessary to take maximum advantage of all the optimizations described in this chapter (using WHP, determining the exact weight of the polynomial, reducing the number of variables, using parity).

For weight 2 divisors, the trisection polynomial has weight 105 and depends on a_1, u_{31}, u_{30}, v_{31}, v_{30}, f_3 and f_2. The degree in a_1 is 81, and the degrees of the other variables can be obtained from their weight, hence we have degrees 52, 26, 28, 21, 24 and 17 respectively in u_{31}, u_{30}, v_{31}, v_{30}, f_3 and f_2. Based only on the degrees, we would need

$$53 \cdot 27 \cdot 29 \cdot 22 \cdot 25 \cdot 18 = 410,840,100$$

trisection polynomials in a_1 to interpolate the complete polynomial, however this goes down to $123,399$ if we use the approach of Section 4.2.2. Since the variable of lowest weight to interpolate WHP is u_{31} (of weight 2), we can use the parity of the weights (with v_{31} and v_{30} being the only ones of odd weight), to reduce this to $65,565$ polynomials in a_1.

Remark 4. The weight-2 trisection polynomial has 1,220,793 non-zero coefficients.

For weight 1 divisors, the trisection polynomial has weight 96 and depends on c_2, u_{30}, v_{30}, f_3, f_2 and f_1. The degree in c_2 is 81, and the degrees of the other variables can be obtained from their weight, hence we have degrees 48, 19, 24, 15 and 12 respectively in u_{30}, v_{30}, f_3, f_2 and f_1. Based only on the degrees, we would need

$$48 \cdot 19 \cdot 24 \cdot 15 \cdot 12 = 3,939,840$$

trisection polynomials in c_2 to interpolate the complete polynomial, however, using the WHP approach of Section 4.2.2 and the parity (with v_{30} the only variable of odd weight), the number of polynomials required decreases to $4,535$.

Remark 5. The weight-1 trisection polynomial has 66,124 non-zero coefficients.

Note that the number of zero coefficients in the trisection polynomial (with respect to a general homogeneous polynomial of similar characteristic) represent $\approx 0.17\%$ and $\approx 2.86\%$ of the total number of terms for the weight-1 and weight-2 trisection polymials.

Remark 6. Assuming the average size of coefficients in the trisection polynomials to be between 1 and 2794 bits (based on Section 4.4.2) and that most of the coefficients are non-zero (based on the previous observation), then the memory requirements for the intermediate polynomials in the computation of the weight-1 trisection polynomials would be at least 3 terabytes (and possibly in the ten thousand terabytes range), whereas those for the weight-2 trisection polynomials would run in the 25,000 terabytes (and possibly in the hundred million terabyte range). Even ignoring time constraints, direct symbolic computation of the trisection polynomials is therefore outside of practical reach.

4.5 Using the trisection polynomial

4.5.1 Example of trisection polynomial

Consider $p = 127$ and the curve defined over $\mathbb{F}_p$ by $y^2 = x^5 + x^3 + 3x^2 + 2x + 1$. if we want to trisect

$$D_3 = (x^2 + 22x + 23, 119x + 48) \ ,$$

the trisection polynomials is

$$\begin{aligned} p(x) = {} & 110x^{81} + 106x^{80} + 58x^{79} + 50x^{78} + 33x^{77} + 76x^{76} + 120x^{75} + 7x^{74} \\ & + 103x^{73} + 70x^{72} + 67x^{71} + 76x^{70} + 4x^{69} + 114x^{68} + 93x^{67} + 22x^{66} \\ & + 36x^{65} + 39x^{64} + 118x^{63} + 29x^{62} + 33x^{61} + 47x^{60} + 88x^{59} + 22x^{58} \\ & + 16x^{57} + 23x^{56} + 7x^{55} + 37x^{54} + 11x^{53} + 62x^{52} + 32x^{50} + 106x^{49} \\ & + 116x^{48} + 95x^{47} + 13x^{46} + 124x^{45} + 26x^{44} + 85x^{43} + 122x^{42} \\ & + 113x^{41} + 116x^{40} + 85x^{39} + 105x^{38} + 103x^{37} + 101x^{36} + x^{35} \\ & + 40x^{34} + 59x^{33} + 72x^{32} + 101x^{31} + 69x^{30} + 28x^{29} + 43x^{28} + 11x^{27} \\ & + 97x^{26} + 27x^{25} + 20x^{24} + 92x^{23} + 113x^{22} + 15x^{21} + 69x^{20} + 90x^{19} \\ & + 16x^{18} + 64x^{17} + 68x^{16} + 111x^{15} + 71x^{14} + 34x^{13} + 18x^{12} + 69x^{11} \\ & + 21x^{10} + 31x^{9} + 104x^{8} + 2x^{7} + 49x^{6} + 62x^{5} + 77x^{4} + 56x^{3} \\ & + 27x^{2} + 107x \ , \end{aligned}$$

and since $p(x)$ is divisible by x (but not by x^2), there is a (single) trisectee D_1 that can be obtained by simple quadratic de-reduction:

$$D_1 = (x^2 + 62x + 51, 46x + 47) \ .$$

4.5.2 Evaluation of trisection polynomials

Evaluating a polynomial consisting of 1,220,793 terms (for divisors of weight 2) or even of 66,124 terms (for divisors of weight 1) must be done with some care to avoid unnecessary costs.

An efficient approach consists in fixing an order for the evaluation of the variables, iteratively using Horner's rule to perform the evaluations, and recording the terms of the polynomial according to this evaluation (so no search is required to locate the next coefficient). It is of course useful to keep in mind that the trisection polynomials are weighted homogeneous, which allows to restrict the degrees in the remaining variables following similar ideas to those of Section 4.2.2. The parity tricks of Section 4.4.1 can also be applied without difficulty.

In some situations, especially in point counting algorithms, we may need to compute a large number of trisection polynomials for divisors defined over the same curve. In the case of point counting algorithms, the divisors may be defined over extension fields (with increasing extension degrees), whereas the curve is defined over a fixed base field. In these cases, it becomes very advantageous to first evaluate the parts of the trisection polynomial that relate to the curve parameters, and then "re-evaluate" the resulting polynomial for each divisor to trisect (evaluating in the coordinates of the divisor). This is particularly true when the divisors are defined over field extensions (relative to the curve) since this approach keeps the evaluations in the base field (where the arithmetic is less expensive) for as long as possible.

In this context, we can optimize the evaluation a little further. For divisors of weight 2, the coordinates $[u_{31}, u_{30}, v_{31}, v_{30}]$ contain some redundancy and can therefore be simplified, due to the divisibility condition $u_3 | v_3^2 - f$ on Mumford's representation $D = [u_3(x), v_3(x)]$. This divisibility condition gives two polynomial $C_1, C_0 \in \mathbb{F}_q[u_{31}, u_{30}, v_{31}, v_{30}]$, both of which must be 0 for all divisor D of weight 2. From C_0 we obtain

$$v_{30}^2 = -2u_{31}u_{30}^2 + u_{30}u_{31}^3 + f_0 - u_{30}f_2 + u_{30}u_{31}f_3 + u_{30}v_{31}^2 \ ,$$

so any polynomial in $\mathbb{F}_q[u_{31}, u_{30}, v_{31}, v_{30}]$ can be limited to degree 1 in v_{30}. Taking $C_2 = Res_{v_0}(C_1, C_0)$, we obtain a new condition which is monic of degree 4 in u_{30}. We can then also limit the polynomial in $\mathbb{F}_q[u_{31}, u_{30}, v_{31}, v_{30}]$ to degree 3 in u_{30} (after the reduction in u_{30}). Finally, the parity technique can be applied to reduce the possible degrees in v_{31}. Note that these substitutions involve the curve parameters f_1 and f_0, which were not used in the computation of the trisection.

In general, this approach may not be very interesting since it only reduces the degrees in v_{30} and u_{30} (without eliminating them completely) at the cost of introducing f_1 and f_0, in effect increasing the number of "variables" (and most likely the number of terms in the polynomial). However, since we are evaluating at the curve parameters first, evaluating at f_1 and f_0 is included in the "pre-evaluation" for the curve (at a minimal increase in cost). With this approach, the number of terms in the evaluation goes down from $1,220,793$ to $112,759$.

For divisors of weight 1, the situation is similar although simplified by the reduced number of variable. Using the divisibility condition, the polynomial in

$\mathbb{F}_q[u_{30}, v_{30}]$ can be limited to degree 1 in v_{30}, with the power in v_{30} corresponding to the parity of the power in c_2. The number of terms in the evaluation goes down from $66,124$ to $2,255$. However, since weight-1 divisors are rather scarce, it is less likely the pre-evaluation technique would pay out for these, and direct evaluation is likely to be preferred.

Remark 7. To compare the efficiency of using the symbolic trisection polynomial, we ran a few experiments the largest extension fields for which [8] reported timings for trisection. We chose a curve over the field $\mathbb{F}_p$ with $p = 2^{127} - 1$, and divisors defined over a degree $2430 = 10 \cdot 3^5$ extension. Preparing the trisection polynomial in terms of the curve parameters (i.e. such that it only remains to evaluate in $[u_{31}, u_{30}, v_{31}, v_{30}]$) took $34.21s$, after which obtaining the trisection polynomial took $1,743.67s$.

This compares extremely well with the timings of $31,035s$ (pre-factoring) reported by Gaudry and Schost, that it to say we obtain a speed-up factor of close to 18. It should be noted that even though the difference in CPU speed should account for a speed-up of roughly 33%, our implementation uses the default field arithmetic of Magma whereas [8] uses NTL and optimizes the field arithmetic. the field arithmetic.

If we consider that at these field sizes, [8] reports similar timings for the pre-factorization part of trisection as for the factorization itself, we obtain an overall speed-up factor close to 1.87 in the complete trisection computation.

CHAPTER 5

Trisection in characteristic 2

The full solution to divisor trisection in Jacobians Jac(C) of genus 2 curves requires arduous computations, much heavier than divisor bisection. This is because the 2-torsion subgroup reflects the natural $2:1$ morphism to $\mathbb{P}^1$, while the 3-torsion does not. Moreover, understanding trisection as a variant of the discrete logarithm problem (given the exponent 3 and any value Q, find the base P such that $3P = Q$), an attempt to analyze the underlying complexity seems justified.

The case of trisection for elliptic curves in odd characteristic was set in [13]. In this paper we show how to trisect divisors in Jac(C)($\mathbb{F}_{2^m}$) when C is a non-supersingular genus 2 curve over a binary field $\mathbb{F}_{2^m}$. The supersingular cases were addressed in [17]. We use coordinates $D = [x^2 + u_1x + u_0, v_1x + v_0]$, and we reverse Cantor's reduction algorithm for divisor class arithmetic as in [12, 15, 17]. Cantor's reduction takes semireduced coordinates $[\tilde{u}(x), \tilde{v}(x)]$, and computes

$$u(x) = \frac{\beta(x)^2 + \alpha(x)\beta(x)h(x) + \alpha(x)^2 f(x)}{\tilde{u}(x)}$$

with $\alpha(x), \beta(x) \in \mathbb{F}_{2^m}[x]$ such that $gcd(\alpha(x), \tilde{u}(x)) = 1$ of the appropiate degrees, until $u(x)$ has degree 2 (see [3]). Our method takes the coordinates $[u(x), v(x)]$ of D and equates *unreduced* coordinates $[\tilde{u}(x), \tilde{v}(x)]$. Namely, we put

$$\tilde{u}(x) = \frac{\beta'(x)^2 + \alpha'(x)\beta'(x)h(x) + \alpha'(x)^2 f(x)}{u(x)} \tag{5.0.1}$$

with $\beta'(x) = \gamma'(x)u(x) + \alpha'(x)v(x)$ and we aim to find $\alpha'(x), \gamma'(x), \tilde{u}(x)$. In trisecting D, we know $\tilde{u}(x)$ has to be of the form $(u'(x))^3$ from Cantor's algorithm. Similarly, for the 3-torsion, we equate

$$\tilde{u}(x) = u(x)^2 = \frac{\beta'(x)^2 + \alpha'(x)\beta'(x)h(x) + \alpha'(x)^2 f(x)}{u(x)}. \tag{5.0.2}$$

In both cases we obtain a solvable polynomial equation.

We choose models

$$\mathrm{C} : y^2 + (h_2x^2 + h_1x + h_0)y = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0$$

with non-constant $h(x) = h_2x^2+h_1x+h_0$, and distinguish the cases $\deg(h(x)) = 1, 2$ because the computational effort is different. The 2-rank in the first case is 1, but it is 1 or 2 in the second. Further, we assume $h_0 = f_1 = 0$ in $\deg(h(x)) = 1$ and $f_3 = f_2 = 0$ in $\deg(h(x)) = 2$ ([1, 10]). See [5] for details on models corresponding to each 2-rank.

In [17] the authors provided a basis of the 3-Sylow subgroup with the same u_1-coordinate at every level. Because of the higher 2-rank, our formulas have more terms and they don't allow such a full regularity. However, in both degrees $\deg(h(x)) = 1, 2$ we show conditions to obtain trisections D' such that $3D'$ and D' share the same u_1. In contrast with [17], 3-torsion divisors very occasionally satisfy this condition, and therefore such trisections rarely are enough to generate Jac(C)$[3^\infty]$.

Our results are shown explicitly for curves with $\deg(h(x)) = 1$. In the case $\deg(h(x)) = 2$, there are many more terms. We propose a multivariable interpolation procedure to simplify the computation, but in $\deg(h(x)) = 2$ the results are too long to write down in full generality. We show several examples, where we take the generator ω of the finite field as the default generator used in Magma [2] for that given field size.

5.1 The 3-torsion subgroup

Since all divisors of order 3 must have weight 2, we solve the equation $2D = -D$ with $\gamma'(x) = x + c_0$ and $\alpha'(x) = a_0$, with $c_0, a_0 \neq 0$. Then (5.0.2) for generic hyperelliptic polynomials $f(x), h(x)$ together with he divisibility condition $v(x)^2 + h(x)v(x) + f(x) \equiv 0 \bmod u(x)$ gives

$$a_0h_2 + a_0^2 + u_1 = 0, \quad (5.1.1)$$

$$a_0^2u_1 + a_0h_1 + a_0c_0h_2 + u_1^2 + u_0 + c_0^2 = 0, \quad (5.1.2)$$

$$a_0h_0 + a_0^2u_0 + a_0^2u_1^2 + c_0^2u_1 + a_0^2f_3 + a_0c_0h_1 + a_0^2h_2v_1 = 0, \quad (5.1.3)$$

$$\begin{aligned} a_0^2u_1f_3 + a_0^2h_1v_1 + a_0^2h_2v_0 + a_0c_0h_0 + a_0^2u_1h_2v_1 + a_0^2v_1^2 \\ + a_0^2f_2 + a_0^2u_1^3 + c_0^2u_0 + u_0^2 = 0, \quad (5.1.4) \end{aligned}$$

$$\begin{aligned} u_0f_3 + u_0u_1^2 + h_1v_0 + u_1f_2 + u_1h_2v_0 + u_1h_1v_1 + u_1^2h_2v_1 + h_0v_1 \\ + u_0^2 + u_1^4 + u_1v_1^2 + f_1 + u_1^2f_3 + u_0h_2v_1 = 0, \quad (5.1.5) \end{aligned}$$

$$\begin{aligned} f_0 + u_0f_2 + u_0u_1f_3 + u_0u_1^3 + h_0v_0 + h_1u_0v_1 + h_2u_0v_0 \\ + h_2u_0u_1v_1 + v_0^2 + u_0v_1^2 = 0. \quad (5.1.6) \end{aligned}$$

Proposition 9. *If* $\deg(h(x)) = 1$ *then* $D = [x^2 + u_1x + u_0, v_1x + v_0] \in$ Jac(C)$(\mathbb{F}_{2^m})[3]$ *if and only if* $p_{u_1}(x)$ *and* $p_{v_1}(x, y)$ *are both zero when evalu-*

ated in $x = u_1$ *and* $y = v_1$*, where*

$$\begin{aligned}
p_{u_1}(x) &= x^{40} + h_1^8 x^{28} + h_1^{12} x^{22} + h_1 f_3^4 x^{20} + h_1^{14} x^{19} + f_3^8 h_1^8 x^{12} \\
&\quad + (h_1^{16} + f_3^{12}) f_3^4 x^8 + h_1^{22} x^7 + f_3^8 h_1^{12} x^6 + h_1^8 f_3^{12} x^4 + f_3^8 h_1^{14} x^3 \\
&\quad + h_1^{20} f_3^4 x^2 + h_1^{26} x + h_1^{20} f_0^2, \qquad (5.1.7) \\
p_{v_1}(x,y) &= h_1 y^2 + h_1^2 y + x^9 + h_1 x^6 + h_1^2 x^3 + h_1 f_3 x^2 + f_3^2 x + h_1 f_2 + h_1^3, \\
v_0 &= \frac{1}{h_1^5}\Big(u_1^{10} + h_1^2 u_1^7 + h_1^2 f_3 u_1^5 + h_1^4 u_1^4 + h_1^2 f_3^2 u_1^3 + f_3^4 u_1^2 \\
&\quad + (h_1^4 + h_1^3 v_1 + h_1^2 (v_1^2 + f_2) + f_3^3) h_1^2 u_1 + (u_1^2 + f_3) h_1^5 \sqrt{u_1} \Big), \\
u_0 &= (u_1^3 + f_3 u_1 + f_2 + v_1^2 + v_1)\sqrt{u_1}.
\end{aligned}$$

Proof. If $\deg(h(x)) = 1$, from Equations (5.1.1), (5.1.2) and (5.1.3) we obtain $u_1 = a_0^2, u_0 = a_0 h_1 + c_0^2$ and $c_0 = \dfrac{a_0(a_0^4 + f_3 + a_0 h_1)}{h_1}$. All these in (5.1.4) imply

$$\begin{aligned}
v_0 = \frac{a_0}{h_1^5}\Big(& a_0^{19} + h_1^2 a_0^{13} + h_1^2 f_3 a_0^9 + h_1^4 a_0^7 + h_1^2 f_3^2 a_0^5 + f_3^4 a_0^3 \\
& + (h_1^4 + h_1^3 v_1 + h_1^2 (v_1^2 + f_2) + f_3^3) h_1^2 a_0 + (a_0^4 + f_3) h_1^5 \Big).
\end{aligned}$$

Then into (5.1.5) and (5.1.6) we obtain 2 equations $p_1(u_1, v_1) = 0$, $p_2(u_1, v_1) = 0$, one with left hand side as $p_{v_1}(x,y)$ above. Finally, $Res_{v_1}(p_1, p_2) = 0$ is exactly $p_{u_1}(u_1) = 0$. □

Our $p_{u_1}(x)$ is the even characteristic version of the 3-modular polynomial of [9]. The u_1-coordinates of 3-torsion divisors are roots of $p_{u_1}(x)$, but the converse does not hold because at the same time $p_{v_1}(x,y)$ has to have a root over $\mathbb{F}_{2^m}$ too. The set of solutions of $p_{u_1}(x), p_{v_1}(x,y)$ in Proposition 9 is faithful to Jac(C)[3]($\mathbb{F}_{2^m}$).

Corollary 8. *If* $\deg(h(x)) = 1$ *then the cardinality of* Jac(C)[3]($\mathbb{F}_{2^m}$) *is twice the cardinality of*

$$\Big\{ \xi \in \mathbb{F}_{2^m} \,\Big|\, p_{u_1}(\xi) = 0,\ Tr_2\Big(\frac{(\xi^9 + h_1^2 \xi^3 + f_3^2 \xi) + (\xi^6 + f_3 \xi^2 + f_2) h_1}{h_1^3} + 1 \Big) = 0 \Big\}$$

plus one.

Proof. The trace condition is equivalent to $p_{v_1}(\xi, x) \in \mathbb{F}_{2^m}[x]$ having a root over $\mathbb{F}_{2^m}$. □

For curves with $\deg(h(x)) = 2$ (momentaneously $h_2 = 1$ to simplify the outcome) we similarly deduce

$$\begin{aligned}
u_0 &= a_0 h_1 + a_0^2 u_1 + u_1^2 + c_0^2 + a_0 c_0, \\
v_0 &= \frac{1}{a_0^2}(a_0^4 u_1^2 + a_0^2(h_1^2 + u_1^3 + (u_1 + h_1) v_1 + v_1^2 + (1 + u_1) c_0^2) \\
&\qquad + a_0 c_0 (h_0 + h_1 c_0 + a_0 c_0^2) + \ u_1^4 + u_1^2 c_0^2).
\end{aligned}$$

Replacing in (5.1.1), (5.1.3), (5.1.5) and (5.1.6) we obtain four polynomials $p_0, p_1, p_2, p_3 \in \mathbb{F}_{2^m}[u_1, v_1, c_0, a_0]$ of degrees 0, 2, 4 and 6 in c_0. Since the leading coefficient of p_1 is $a_0^2 + u_1 \neq 0$, we reduce p_2, p_3 modulo p_1. From p_2 we equate c_0 and we then replace in p_1 and p_3. Since the coefficient of a_0^2 in p_0 is nonzero, we reduce p_1, p_3 modulo p_0. From p_1 we equate a_0 and then replace in p_0 and p_3. Finally we compute $Res_{v_1}(p_0, p_3)$. In contrast with $\deg(h(x)) = 1$, now $\deg_{v_1}(gcd(p_0, p_3))$ can be larger than 2. Still, $Res_{v_1}(p_0, p_3)$ is a multiple of $p_{u_1}(x)^2$ where

$$\begin{aligned} p_{u_1}(x) = x^{40} &+ h_1^2 x^{34} + h_1^6 x^{30} + (h_1^7 + h_1^6 + h_1^4 h_0 + h_1^2 h_0^2 + h_1^2 f_1) x^{29} + \dots \\ &+ \Big(f_1^4 + f_1^3(h_1^3 + h_1) + f_0^2 h_1^4 + f_0 h_1^{10} + f_0 h_1^9 + f_0 h_1^7 h_0 + h_0^8 \\ &\quad + f_1^2(h_1^8 + h_1^7 + h_1^5 h_0 + h_1^5 + h_1^4 h_0 + h_1^3 h_0^2 + h_1^3 h_0 + h_1 h_0^2) \\ &\quad + f_1(f_0 h_1^5 + h_1^9 h_0 + h_1^9 + h_1^8 h_0 + h_1^7 h_0^2 + h_1^5 h_0^2 + h_1^3 h_0^4 + h_1 h_0^4) \\ &\quad + f_0 h_1^5 h_0^2 + h_1^{11} h_0 + h_1^7 h_0^3 + h_1^5 h_0^5 + h_1^4 h_0^5 + h_1^3 h_0^6 + h_1^3 h_0^5 \\ &\quad + h_1 h_0^6 + h_1^{13} \Big) \cdot Res_x(h(x), h_1^2 f(x) + x^8 + f_1^2) \end{aligned} \tag{5.1.8}$$

and the last factor (of the constant term) is the discriminant of the curve.

Example 4. *Let* $\mathrm{C}_1 : y^2 + \omega^{54093} xy = x^5 + \omega^{8322} x^3 + \omega^{4161} x^2 + \omega^{16644}$ *over* $\mathbb{F}_{2^{18}}$*. Then*

$$\begin{aligned} p_{u_1}(x) = x^{40} &+ \omega^{170601} x^{28} + \omega^{124830} x^{22} + \omega^{203889} x^{20} + \omega^{233016} x^{19} \\ &+ \omega^{237177} x^{12} + \omega^{237177} x^8 + \omega^{141474} x^7 + \omega^{191406} x^6 \\ &+ \omega^{8322} x^4 + \omega^{37449} x^3 + \omega^{66576} x^2 + \omega^{95703} x + \omega^{66576} \end{aligned}$$

and $\mathrm{Jac}(\mathrm{C}_1)(\mathbb{F}_{2^{18}})[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/243\mathbb{Z} \times \mathbb{Z}/243\mathbb{Z}$ *with a basis*

$$\begin{aligned} \{&[x^2 + \omega^{67438} x + \omega^{238206}, \omega^{121226} x + \omega^{30028}], \\ &[x^2 + \omega^{127370} x + \omega^{91062}, \omega^{90346} x + \omega^{180924}], \\ &[(x^2 + \omega^{226002} x + \omega^{11845}, \omega^{239840} x + \omega^{29962}]\}. \end{aligned}$$

Example 5. *Let* $\mathrm{C}_2 : y^2 + (x^2 + \omega^{42} x + \omega^{42}) y = x^5 + x + 1$ *over* $\mathbb{F}_{2^6}$*. Then*

$$\begin{aligned} p_{u_1}(x) = x^{40} &+ \omega^{21} x^{34} + x^{30} + x^{29} + \omega^{21} x^{28} + x^{27} + x^{26} + x^{25} \\ &+ \omega^{42} x^{24} + \omega^{21} x^{23} + \omega^{21} x^{22} + \omega^{21} x^{20} + \omega^{21} x^{19} + \omega^{21} x^{18} \\ &+ x^{16} + \omega^{21}(x^{15} + x^{13} + \omega^{21} x^{12} + x^{10} + x^8 + x^4 + x^3 + x), \end{aligned}$$

and $\mathrm{Jac}(\mathrm{C}_2)(\mathbb{F}_{2^6})[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *with a basis*

$$\{[x^2 + \omega^{21}, \omega^{42} x + \omega^{21}], [x^2 + \omega^{57} x + \omega^6, \omega^{56} x + \omega^{28}], [x^2 + \omega^{40} x + \omega^{14}, \omega^{36} x + \omega^{38}]\}.$$

The roots 0, ω^{57}, ω^{40} *have multiplicity* $1, 1, 2$ *in* $p_{u_1}(x)$ *and the factorization types of* $gcd(p_0, p_3)$ *are* $(1)^2(4), (1)^2$ *and* $(1)^4$ *respectively.*

5.2 Trisection

In this section we show how to obtain the trisection polynomial $p_D(x)$ of any weight 2 divisor D. The roots of $p_D(x)$ give the set $\frac{1}{3}D$ of trisections of the trisectee D. We explain first how to find weight 1 trisections of D.

5.2.1 Weight 1 trisections

Here D_1 and $D_3 = 3D_1$ are of the form $[u_1(x), v_1(x)] = [x + u_{10}, v_{10}]$ and $[u_3(x), v_3(x)] = [x^2 + u_{31}x + u_{30}, v_{31}x + v_{30}]$ respectively.

Proposition 10. *Let* C *be a non-supersingular genus* 2 *curve over* $\mathbb{F}_{2^m}$*, then a divisor* $D_3 \in \mathrm{Jac(C)}(\mathbb{F}_{2^m})$ *has a trisection of weight* 1 *if only if* $Res_{c_0}(p_1, p_2) = 0$ *with*

$$\begin{aligned} p_1(c_0) &= v_{31}h_2 + f_3 + u_{30} + c_0^2u_{31} + c_0h_1 + c_0^4 + c_0^2h_2^2, \\ p_2(c_0) &= v_{31}h_1 + v_{30}h_2 + u_{31}f_3 + f_2 + v_{31}^2 + c_0^2u_{30} + c_0h_0 + u_{31}v_{31}h_2 \\ &+ \ c_0^6 + u_{31}c_0^2h_2^2 + u_{31}^2c_0h_2 + c_0^2u_{31}^2 + u_{31}c_0^4 + c_0^5h_2 + c_0^4h_2^2 + c_0^3h_2^3. \end{aligned}$$

Proof. In (5.0.1) with $\gamma = c_0$ and $\alpha = 1$ we obtain

$$u_{31} + c_0^2 + c_0h_2 + u_{10} = 0 \qquad (5.2.1)$$

$$v_{31}h_2 + u_{31}^2 + f_3 + u_{30} + c_0^2u_{31} + c_0h_1 + u_{10}^2 = 0 \qquad (5.2.2)$$

$$\begin{aligned} &v_{31}h_1 + v_{30}h_2 + u_{31}f_3 + f_2 + v_{31}^2 + u_{31}^3 \\ &+c_0^2u_{30} + c_0h_0 + u_{31}v_{31}h_2 + u_{10}^3 = 0. \end{aligned} \qquad (5.2.3)$$

From (5.2.1), $u_{10} = u_{31} + c_0^2 + c_0h_2$, and replacing in (5.2.2) and (5.2.3) we obtain $p_1 = p_2 = 0$. □

Corollary 9. *A divisor* D_3 *admits at most* 4 *trisections of weight* 1*.*

Proof. The degrees of $p_1(c_0)$ and $p_2(c_0)$ above are 4 and 6 respectively. Hence the degree of $gcd(p_1(c_0), p_2(c_0))$ is at most 4, and by (5.2.1) there are at most 4 possible u_{10}'s. □

Example 6. *Let* $\mathrm{C}_3 : y^2 + \omega^{54093}xy = x^5 + \omega^{8322}x^3 + \omega^{4161}x^2 + \omega^{16644}$ *over* $\mathbb{F}_{2^{18}}$*. For*

$$D = [x^2 + \omega^{211084}x + \omega^{50578}, \omega^{169657}x + \omega^{196594}] \in \mathrm{Jac}(\mathrm{C}_3)(\mathbb{F}_{2^{18}}),$$

the polynomials $p_1(c_0), p_2(c_0)$ *above satisfy* $gcd(p_1(c_0), p_2(c_0)) = x^2 + \omega^{33719}x + \omega^{69077}$*, and the corresponding trisections of weight* 1 *of* D *are*

$$[x + \omega^{252372}, \omega^{42058}] \ \textit{and} \ [x + \omega^{247977}, \omega^{197890}].$$

5.2.2 Weight 2 trisections

From (5.0.1) with $\gamma'(x) = x^2 + c_1x + c_0$ and $\alpha'(x) = a_1x + a_0$ we have

$$a_1^2 + a_1h_2 + u_{31} + u_{11} = 0 \tag{5.2.4}$$

$$a_1^2u_{31} + a_1(c_1h_2 + h_1) + a_0h_2 + u_{30} + c_1^2 + u_{10} + u_{11}^2 = 0 \tag{5.2.5}$$

$$\begin{aligned} a_1^2(f_3 + u_{30} + u_{31}^2 + v_{31}h_2) + a_1(h_0 + c_1h_1 + c_0h_2) \\ + a_0^2 + a_0(h_1 + c_1h_2) + u_{11}^3 + c_1^2u_{31} = 0 \end{aligned} \tag{5.2.6}$$

$$\begin{aligned} a_1^2(u_{31}v_{31}h_2 + f_2 + u_{31}^3 + v_{31}^2 + v_{31}h_1 + v_{30}h_2 + u_{31}f_3) \\ + a_1(c_1h_0 + c_0h_1) + c_1^2u_{30} + a_0h_0 + c_0^2 + u_{11}^2u_{10} \\ + a_0c_1h_1 + a_0c_0h_2 + a_0^2u_{31} + u_{10}^2 = 0 \end{aligned} \tag{5.2.7}$$

$$\begin{aligned} a_1c_0h_0 + a_0^2(f_3 + u_{30} + u_{31}^2 + v_{31}h_2) \\ + a_0(c_1h_0 + c_0h_1) + u_{11}u_{10}^2 + c_0^2u_{31} = 0 \end{aligned} \tag{5.2.8}$$

$$\begin{aligned} a_0^2(v_{31}^2 + f_2 + u_{31}^3 + v_{31}h_1 + v_{30}h_2 + u_{31}f_3 + u_{31}v_{31}h_2) \\ + a_0c_0h_0 + c_0^2u_{30} + u_{10}^3 = 0 \end{aligned} \tag{5.2.9}$$

From (5.2.4) and (5.2.5) we have

$$u_{11} = a_1^2 + a_1h_2 + u_{31}, \tag{5.2.10}$$

$$u_{10} = a_1^4 + a_1^2(h_2^2 + u_{31}) + a_1(h_1 + c_1h_2) + a_0h_2 + u_{30} + c_1^2 + u_{31}^2. \tag{5.2.11}$$

In the general case for curves with $\deg(h(x)) = 1$ (so $a_1 \neq 0$), the resolution of (5.2.4) — (5.2.9) is as follows. Replacing (5.2.10) and (5.2.11) in (5.2.6) — (5.2.9) we obtain 4 polynomials in $\mathbb{F}_{2^m}[a_1, a_0, c_1, c_0]$. With one we isolate

$$c_0 = \frac{1}{h_1a_1u_{30}}(a_0^2v_{31}h_1 + h_1a_1c_1^4 + h_1a_1u_{30}^2 + \ldots + u_{30}a_1^2v_{31}^2 + u_{30}a_1^2f_2). \tag{5.2.12}$$

Replacing c_0 in the second equation and then progressively reducing modulo the two other equations gives us an equation of the form $s_1(a_1, a_0)c_1 + s_0(a_1, a_0) = 0$, from which we deduce

$$c_1 = -\frac{s_0(a_0, a_1)}{s_1(a_0, a_1)}. \tag{5.2.13}$$

We then replace c_1 in two of the initial four polynomials and compute their resultant $R(a_1)$, eliminating a_0. From $R(a_1)$ we have to remove a factor of degree 18 raised to power 3 and a predictable quadratic factor before obtaining a degree 81 relation

$$p_D(a_1) = a_1^{81}(u_{31}^8u_{30}^2 + u_{31}^6v_{31}^4 + \ldots + f_3^6) + \ldots + (u_{31}^6h_1^{19}v_{31}^{12} + \ldots + u_{31}^{48}h_1^3) = 0. \tag{5.2.14}$$

We call $p_D(x)$ the trisection polynomial of D. The following algorithm puts together all the steps above.

The bottleneck in our computation above is to find the resultant $R(x)$, which is essentially our trisection polynomial $p_D(x)$ together with some parasite factors. We can avoid to compute $R(x)$ symbolically using multivariate

```
Algorithm 8 Trisection (over $\mathbb{F}_{2^m}$ with $\deg(h(x)) = 1$)
Require: A curve C with $\deg(h(x)) = 1$, $D_3 = [x^2 + u_{31}x + u_{30}, v_{31}x + v_{30}] \in \mathrm{Jac(C)}(\mathbb{F}_{2^m})$.
Ensure: $D = [u_1(x), v_1(x)]$ such that $3D = D_3$.
Find a root $a_1$ of $p_D(x)$ in (5.2.14)
Compute $G(x) := gcd(p_1(a_1, x), p_2(a_1, x))$
Find a root $a_0$ of $G$
Find $c_1$ with (5.2.13)
Find $c_0$ with (5.2.12)
Find $u_{11}, u_{10}$ with $u_{11} = u_{31} + a_1^2$, $u_{10} = u_{30} + a_1^2 u_{31} + u_{31}^2 + a_1^4 + a_1 + c_1^2$
Compute $v_1 = (\alpha')^{-1}(\beta') + h(x) \bmod u_1$ from the polynomials $\alpha'(x) = a_1x + a_0$, $\gamma'(x) = x^2 + c_1x + c_0$, and $\beta'(x) = \gamma'(x)u_3(x) + \alpha'(x)v_3(x)$
```

interpolation as a shortcut to $p_D(x)$. The idea is to assign appropriate weights to the variables in our equations (5.2.4) — (5.2.9) with the purpose that each equation is weighted homogeneous. We accomplish this with the following choices:

h_1	u_{31}	u_{30}	v_{30}	v_{31}	f_3	f_2	f_0
3	2	4	5	3	4	6	10

Since $p_D(x)$ is the final result of a procedure involving addition, products, resultants and gcds of weighted homogeneous polynomials, it must be weighted homogeneous too. A useful trick to simplify the computation is to put $u_{31} = 1$ because homogeneity allows reconstruction. Evaluating the remaining variables at enough points, we recover $p_D(x)$.

In the general case for $\deg(h(x)) = 2$ (so $a_1 \neq 0$), replacing u_{11} and u_{10} in (5.2.6) — (5.2.9) we similarly obtain four polynomials in c_0, c_1, a_0, a_1 and from them we obtain a polynomial of degree 81 in a_1

$$p_D(a_1) = a_1^{81}(u_{30}^2u_{31}^8 + \ldots + v_{31}^8) + \ldots + (h_0^{21} + \ldots + u_{30}^3v_{31}h_1^{30}) = 0 \quad (5.2.15)$$

with about 3 million terms. A similar interpolation trick eases the computation as above.

Interestingly, if the leading coefficient of $p_D(x)$ is zero then there is one trisection of weight 1. This ties together $p_D(x)$ and Proposition 10.

Example 7. *Let* $\mathrm{C}_8 : y^2 + (x^2 + \omega^5x + \omega^5)y = x^5 + \omega x + \omega$ *over* $\mathbb{F}_{2^3}$ *and*

$$D = [x^2 + x + \omega, x + \omega] \in \mathrm{Jac(C_8)}(\mathbb{F}_{2^3}).$$

Then $\frac{1}{3}D = [x + \omega^5, \omega^6]$ *and the trisection polynomial is*

$$p_D(x) = \omega^2x^{80} + \omega^5x^{79} + \omega^5x^{78} + \cdots + \omega^3x^3 + \omega^6x + \omega^4.$$

5.2.3 Easy trisections

From Equations (5.2.10) and (5.2.11), it follows that trisections with the same u_1-coordinate as their trisectees are given by $a_1 = 0$ in curves with $\deg(h(x)) = 1$, while these are given by $a_1 = 0$ or $a_1 = h_2$ in curves with $\deg(h(x)) = 2$. For supersingular curves such easy trisections were enough to generate a basis for the 3-Sylow subgroup (see [17]). Below we show that for us this is not necessarily the case.

Proposition 11. *If* $\deg(h(x)) = 1$ *then* $D_3 = [x^2 + u_{31}x + u_{30}, v_{31}x + v_{30}] \in \mathrm{Jac(C)}(\mathbb{F}_{2^m})$ *has a trisection with the same* u_1*-coordinate if and only if*

$$\begin{aligned} p_{simple}(x) = {} & x^9 + h_1^2x^7 + h_1^2(h_1^2 + u_{31}u_{30})x^5 + u_{31}u_{30}h_1^3x^4 \\ & + h_1^2(h_1^4 + u_{31}u_{30}h_1^2 + u_{31}^2u_{30}^2)x^3 + u_{31}u_{30}h_1^5x^2 + u_{31}^3u_{30}^3h_1^3 \\ & + u_{31}^2\Big(u_{31}^{10} + (u_{30}^2 + f_3^2)u_{31}^6 + h_1^2u_{30}u_{31}^5 + h_1^2u_{30}f_3u_{31}^3 \\ & \qquad + (f_2^2 + v_{31}^4 + h_1^2v_{31}^2)u_{31}^4 + h_1^2u_{30}^3u_{31} + h_1^4u_{30}^2 \\ & \qquad + u_{30}(h_1^3v_{31} + h_1^2f_2 + h_1^2v_{31}^2 + u_{30}f_3^2)u_{31}^2\Big)x \end{aligned}$$

has a root over $\mathbb{F}_{2^m}$*.*

Proof. Necessarily $a_1 = 0$. If $u_{31} \neq 0$, from (5.2.6) we obtain $c_1^2 = u_{31}^2 + a_0(h_1 + a_0)/u_{31}$. Replacing in (5.2.8) and (5.2.9) we obtain $p_1(c_0, a_0) = p_2(c_0, a_0) = 0$. The resultant $Res_{c_0}(p_1, p_2)(a_0) = 0$ is exactly the condition $p_{simple}(x)$ to have a root $a_0 \in \mathbb{F}_{2^m}$. □

Example 8. *Let* $\mathrm{C}_4 : y^2 + \omega^{12}xy = x^5 + \omega x^3 + \omega x^2 + \omega$ *over* $\mathbb{F}_{2^6}$*. For*

$$D = [x^2 + \omega^{32}x + \omega^{55}, \omega^{13}x + \omega^{30}] \in \mathrm{Jac(C_4)}(\mathbb{F}_{2^6}),$$

the trisection polynomial $p_D(x)$ *has no constant term,* $p_{simple}(x)$ *has a root over* $\mathbb{F}_{2^6}$*,*

$$\begin{aligned} p_D(x) &= \omega^{39}x^{81} + \omega^{17}x^{80} + x^{79} + \omega^{12}x^{78} + \ldots + \omega^{35}x^3 + \omega^{19}x^2 + \omega^{41}x, \\ p_{simple}(x) &= (x + \omega^5) \cdot (x^4 + \omega x^3 + \omega^7x^2 + \omega^{46}x + \omega^{14}) \\ & \quad \cdot (x^4 + \omega^{36}x^3 + \omega^{28}x^2 + \omega^{39}x + \omega^{26}), \end{aligned}$$

and $[x^2 + \omega^{32}x + \omega^{12}, \omega^{33}x + \omega^6] \in \frac{1}{3}D$ *shares the* u_1*-coordinate with* D*.*

Even if 3-torsion divisors in carefully chosen instances may satisfy the condition in Proposition 11, such examples are rare in $\deg(h(x)) \geq 1$ (compare with [17]).

Example 9. *Let* $\mathrm{C}_5 : y^2 + \omega^{12}xy = x^5 + \omega x^3 + \omega^5x^2 + \omega^4$ *over* $\mathbb{F}_{2^{12}}$*. Then* $\mathrm{Jac(C_5)}(\mathbb{F}_{2^{12}})[3^\infty] \cong \mathbb{Z}/9\mathbb{Z}$ *with*

$$D = [x^2 + \omega^{1163}x + \omega^{2851}, \omega^{4056}x + \omega^{2808}] \in \mathrm{Jac(C_5)}[3](\mathbb{F}_{2^{12}}).$$

For D – hence for all divisors in $\mathrm{Jac}(\mathrm{C}_5)[3](\mathbb{F}_{2^{12}})$*,* $p_{simple}(x)$ *factors over* $\mathbb{F}_{2^{12}}$ *as*

$$\begin{aligned}p_{simple}(x) = (x^3 + \omega^{1342}x^2 + \omega^{692}x + \omega^{4026}) \cdot (x^3 + \omega^{2707}x^2 + \omega^{2889}x + \omega^{4026})\\ \cdot (x^3 + \omega^{4072}x^2 + \omega^{1390}x + \omega^{4026}).\end{aligned}$$

Consequently, no trisection shares the u_1*-coordinate with* D*:*

$$\begin{aligned}\frac{1}{3}D = \Big\{&[x^2 + \omega^{417}x + \omega^{3774}, \omega^{2732}x + \omega^{1182}],\\ &[x^2 + \omega^{3249}x + \omega^{3189}, \omega^{1374}x + \omega^{2750}],\\ &[x^2 + \omega^{3301}x + \omega^{3574}, \omega^{3077}x + \omega^{3178}]\Big\}.\end{aligned}$$

Trisections with $u_{11} = u_{31}$ for $\deg(h(x)) = 2$ and $a_1 = 0$ are found similarly. We deduce

$$\begin{aligned}c_0 = &\frac{u_{31}^5 + (u_{30} + a_0h_2 + c_1^2)u_{31}^3 + (a_0(c_1h_1 + h_0) + c_1^2u_{30})u_{31}}{a_0(h_1 + u_{31}h_2)}\\ &+ \frac{(v_{31}h_2 + u_{30})a_0^2 + c_1h_0a_0}{a_0(h_1 + u_{31}h_2)}\end{aligned}$$

and similarly we obtain $p_1(a_0)$ and $p_2(a_0)$ (of degrees 6 and 7) as in the proof of Proposition 11. An easy trisection is given by a root of the common factors of p_1 and p_2.

Example 10. *Let* $\mathrm{C}_6 : y^2 + (x^2 + \omega^{12}x + \omega^{12})y = x^5 + \omega x + \omega$ *over* $\mathbb{F}_{2^6}$*. For*

$$D = [x^2 + \omega^9x + \omega^{56}, \omega^{50}x + \omega^{12}] \in \mathrm{Jac}(\mathrm{C}_6)(\mathbb{F}_{2^6}),$$

$p_D(x)$ *has no constant term,* $p_1(x)$ *and* $p_2(x)$ *share a root over* $\mathbb{F}_{2^6}$*,*

$$\begin{aligned}p_D(x) &= \omega^{23}x^{81} + \omega^5x^{80} + \omega^{55}x^{79} + \omega^{14}x^{78} + \ldots + \omega^{20}x^3 + x^2 + \omega^{18}x\\ p_1(x) &= (x + \omega^3)(x + \omega^{16})(x^2 + \omega^{41}x + \omega^{60})(x^3 + \omega^{10}x^2 + \omega^{42}x + \omega^{53})\\ p_2(x) &= (x + \omega^3)(x^5 + \omega^3x^4 + \omega^{21}x^3 + \omega^{21}x^2 + \omega^{44}x + \omega^{58}),\end{aligned}$$

and then $\frac{1}{3}D = [x^2 + \omega^9x, \omega^{11}x + \omega^{62}]$ *shares the* u_1*-coordinate with* D*.*

Easy trisections given by $a_1 = h_2$ are found with a similar pair of polynomials.

Example 11. *Let* $\mathrm{C}_7 : y^2 + (x^2 + \omega^{12}x + \omega^{12})y = x^5 + \omega x + \omega$ *over* $\mathbb{F}_{2^6}$ *and*

$$D = [x^2 + \omega^{46}x + 1, \omega^{11}x + \omega^{19}] \in \mathrm{Jac}(\mathrm{C}_7)(\mathbb{F}_{2^6}),$$

then $\frac{1}{3}D = [x^2 + \omega^{46}x + \omega^3, x + \omega^{14}]$ *and the trisection polynomial has a root at* $x = h_2$*:*

$$p_D(x) = (\omega^{32}x^{80} + \omega^{31}x^{79} + \omega x^{78} + \ldots + x^3 + \omega^{23}x^2 + \omega^{33}x + \omega^{29})(x + 1).$$

Hence, in general one has to expect that none of the 3-torsion divisors will allow for a trisection with the same u_1-coordinate. Therefore distinguished bases are extremely rare in non-supersingular curves.

5.3 Factorization of trisection polynomials

In the same way as in odd characteristic (see [9]), the factorization type of our u_1-coordinate polynomial $p_{u_1}(x)$ for 3-torsion divisors is determined by the characteristic polynomial $\chi_3(x) \in \mathbb{Z}[x]$ of the Frobenius endomorphism π acting in the 3-torsion subgroup. Below we provide the precise Galois orbits of the 3-torsion subgroup.

Proposition 12. *Let* C *be a non-supersingular genus* 2 *curve over* $\mathbb{F}_{2^m}$. *Let* $p_{u_1}(x)$ *be the* u_1*-coordinate polynomial* (5.1.7), (5.1.8) *of the* 3*-torsion divisors and let* $p_D(x)$ *be the trisection polynomial* (5.2.14), (5.2.15). *Then the factorization types of* $p_{u_1}(x)$, $p_D(x)$ *and the Galois orbits of the* 3*-torsion subgroup of* $\mathrm{Jac}(\mathrm{C})(\mathbb{F}_{2^m})$ *are shown in Table 5.1.*

factorization of $p_{u_1}(x)$	3-torsion Galois orbits	factorization of $p_D(x)$ assuming no trisection of weight 1
$(5)^8$	$(5)^{16}$	$(1)(5)^{16}$
	$(10)^8$	$(1)(10)^8$
$(1)(2)^2(3)(4)^2(12)^2$	$(2)^2(4)^6(6)(12)^4$	$(1)(2)^2(4)^6(6)(12)^4$
	$(1)^2(3)^2(4)^6(12)^4$	$(1)^3(3)^2(4)^6(12)^4, (3)^3(12)^6$
$(1)^4(2)^2(4)^8$	$(2)^4(4)^{18}$	$(1)(2)^4(4)^{18}$
	$(1)^8(4)^{18}$	$(1)^9(4)^{18}, (3)^3(12)^6$
$(1)(3)^4(9)^3$	$(1)^2(3)^8(9)^6$	$(1)^3(3)^8(9)^6, (9)^9$
	$(2)(6)^4(18)^3$	$(1)(2)(6)^4(18)^3$
$(1)^{40}$	$(2)^{40}$	$(1)(2)^{40}$
	$(1)^{80}$	$(1)^{81}, (3)^{27}$
$(1)^4(3)^{12}$	$(1)^8(3)^{24}$	$(1)^8(3)^{24}, (3)^{27}$
	$(2)^4(6)^{12}$	$(1)(2)^8(6)^{12}$
$(1)^{13}(3)^9$	$(1)^{26}(3)^{18}$	$(1)^{27}(3)^{18}, (3)^{27}$
	$(2)^{13}(6)^9$	$(1)(2)^{13}(6)^9$
$(4)^{10}$	$(8)^{10}$	$(1)(8)^{10}$
$(2)^2(6)^6$	$(4)^2(12)^6$	$(1)(4)^2(12)^6$
$(2)^{20}$	$(4)^{20}$	$(1)(4)^{20}$
$(1)^2(2)(3)^2(6)^5$	$(1)^2(2)^3(3)^2(6)^{11}$	$(1)^3(2)^3(3)^2(6)^{11}, (3)^3(6)^{12}$
$(1)^5(2)^4(3)(6)^4$	$(1)^2(2)^{12}(3)^2(6)^8$	$(1)^3(2)^{12}(3)^2(6)^8, (3)^3(6)^{12}$
	$(1)^8(2)^3(6)^9$	$(1)^9(2)^9(6)^9$
$(1)^8(2)^{16}$	$(1)^8(2)^{36}$	$(1)^9(2)^{36}, (3)^3(6)^{12}$
$(1)^2(2)(4)(8)^4$	$(1)^2(2)^3(8)^9$	$(1)^3(2)^3(8)^9, (3)(6)(24)^3$
$(4)(12)^3$	$(8)(24)^3$	$(1)(8)(24)^3,$
$(10)^4$	$(20)^4$	$(1)(20)^4$

Table 5.1: Factorization patterns for trisection

Proof. The factorization types of $p_{u_1}(x)$ are as in [9]. We detail how to deduce the 2nd column from the 1st when $\deg(h(x)) = 1$ and the matrix of π in

$\mathrm{Jac(C)}(\mathbb{F}_{2^m})[3]$ is one of

$$A_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

One can check that A_1 and A_2 have the same factorization $(1)(3)(2)^2(4)^2(12)^2$ for $p_{u_1}(x)$, but their Galois orbits in the 3-torsion are different. Indeed, the first non-zero value in the 3rd row discriminates: since it is 1 in A_1, then π leaves one divisor fixed, hence $p_{u_1}(x)$ has a root $\xi \in \mathbb{F}_{2^m}$ for which $p_{v_1}(\xi, y)$ has a root, while this is not the case for A_2. Hence the Galois orbit structures are $(1)^2(3)^2(4)^6(12)^4$ and $(2)(4)^6(6)(12)^4$ respectively. From the kernel of multiplication by 3 the factorization types for $p(a_1)$ follow (see similar arguments in [15] for bisection or chapter 3 for trisection in odd characteristic). □

If a curve has a 3-torsion subgroup of rank 3 or 4 over $\mathbb{F}_{2^m}$ then the type of factorization of $p_{u_1}(x)$ is $(1)^{13}(3)^9$ or $(1)^{40}$ respectively. These cases are only possible when $\chi_3(x) = (x-1)^4 = x^4 + 2x^3 + 2x + 1 \pmod 3$. Since the coefficients of x^3 and x are the same, then $2^m \equiv 1 \bmod 3$, hence $m \equiv 0 \bmod 2$. This is a particular case of [6, Corollary 5.77].

Example 12. *Let $C_9 : y^2 + \omega^{12}xy = x^5 + \omega x^3 + \omega^2 x^2 + \omega$ and $C_{10} : y^2 + \omega^{12}xy = x^5 + \omega x^3 + \omega x^2 + \omega^{11}$ over $\mathbb{F}_{2^6}$. The factorization of $p_{u_1}(x)$ in both Jacobians is $(1)(2)^2(3)(4)^2(12)^2$ but the rank of the 3-torsion is 1 for C_9 and 0 for C_{10} (this ilustrates rows 3 and 4 in the middle column of Table 5.1 with $\deg(h(x)) = 1$ curves).*

Example 13. *Let $\mathrm{C}_{11} : y^2 + (x^2 + \omega^{12}x + \omega^{12})y = x^5 + \omega x + \omega$ over $\mathbb{F}_{2^6}$. The factorization of $p_{u_1}(x)$ is $(1)(2)^2(3)(4)^2(12)^2$, and the polynomials p_0, p_3 (see the discussion after Corollary 8) satisfy $gcd(p_0, p_3) = (x + \omega^{30})(x + \omega^{41})$. Then $\mathrm{Jac}(\mathrm{C}_{11})(\mathbb{F}_{2^6})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z}$ with generator $[x^2 + \omega^{36}x + \omega^4, \omega^{41}x + \omega^{43}]$ (and this ilustrates row 4 of Table 5.1 with a curve with $\deg(h(x)) = 2$).*

CHAPTER 6

Explicit ℓ-Sylow subgroup

We present a generalization of the algorithms in [16] for the case of ℓ-sections. There exists implementations of ℓ-section for $\ell \in \{2, 3, 5, 7\}$ in odd characteristic and ℓ-section for $\ell \in \{2, 3\}$ in characteristic two. We studied the case of ℓ-section in general and we present explicit algorithms for the computation of the 3-Sylow subgroup. The generalization to compute generators of 3-Sylow allow us obtain s_1 and s_2 modulo power of 3 using the generators.

6.1 Determining the ℓ-Sylow in the Jacobian

Let be r the ℓ-rank of $\mathrm{Jac}(C)(\mathbb{F}_q)$. we write

$$\mathrm{Jac}(C)(\mathbb{F}_q)[\ell^\infty] \cong \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell^{n_r}\mathbb{Z}$$

If $\{w_1, \ldots, w_r\}$ is a basis of the ℓ-Sylow subgroup $\mathrm{Jac}(C)(\mathbb{F}_q)[\ell^\infty]$ with, w_i of order ℓ^{n_i}, then any $D \in \mathrm{Jac}(C)(\mathbb{F}_q)[\ell^\infty]$ can be written uniquely in the form

$$D = \sum_{j=1}^{r} \sum_{i=0}^{n_j - 1} \epsilon_{i,j} \ell^i w_j, \epsilon_{i,j} \in \{0, \ldots, \ell - 1\} \qquad (6.1.1)$$

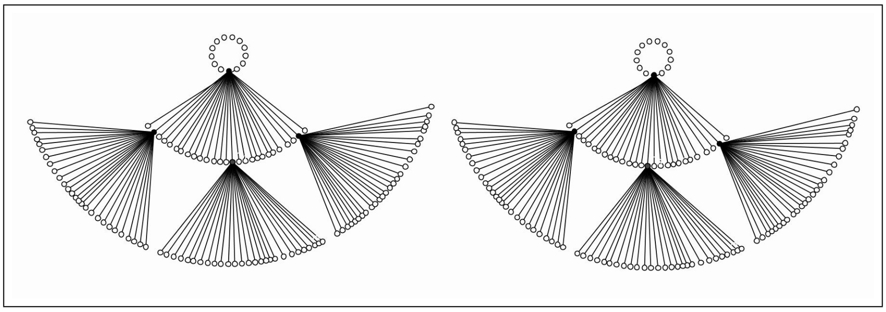

Figure 6.1: The 3-forest of a Jacobian with 3-rank 3 and exponents $n_1 = n_2 = 1$, $n_3 = 3$.

We now present the natural generalizations for definitions of inner, leaf, level and t-relative in [16]

Definition 10. *We say a divisor D is inner if $\frac{1}{\ell}D \neq \emptyset$, and a leaf otherwise.*

Definition 11. *We say that a divisor $D \in \mathrm{Jac}(C)(\mathbb{F}_q)$ is at level k if $ord(D) = \ell^k$. The maximum level in a tree is called the height of the tree.*

Definition 12. *We say that two divisors $D, D' \in \mathrm{Jac}(C)(\mathbb{F}_q)$ in the same level are t-relatives if $\ell^t D = \ell^t D'$. Equivalently, D and D' are t-relatives if and only if $D - D' \in \mathrm{Jac}(C)(\mathbb{F}_q)[\ell^t]$.*

Definition 13. *We say that a divisor $D \in \mathrm{Jac}(C)(\mathbb{F}_q)$ is t-inner if there exists a t-relative divisor which is inner.*

We now present natural generalizations of jumps and gap from [16]

Proposition 13. *(The proportions) Let T be a ℓ-tree of height n_s, and let k an integer such that $1 \leq k < n_s$.*

- *If $1 \leq k \leq n_1$ then all divisors at level k in T are inner.*
- *If $n_j < k \leq n_{j+1}$, $1 \leq j < s$, then $\frac{1}{\ell^j}$ of the divisors at level k in T are inner.*

Proposition 14. *(The gaps) Let T be a ℓ-tree of height n_s , and let t be an integer such that $1 \leq t < n_s$.*

- *If $t \neq n_1, \ldots, t \neq n_{s-1}$, then in each class of t-relatives, all divisors are leaves or otherwise all are $(t-1)$-inner.*
- *If $t = n_i$ and j is the number of times that n_i appears in the sequence $n_1, \ldots, n_s$, then in each class of t-relatives, all divisors are leaves or otherwise for every set of representatives modulo $(t-1)$-relativeness a proportion of $\frac{1}{\ell^j}$ of them are $(t-1)$-inner.*

We need a generalization of theorem 3.1 in [16] for any ℓ in particular for $\ell = 3$ to obtain generators of the 3-Sylow subgroup.

Proposition 15. *(Jumps) Let $D_k \in Jac(C)(\mathbb{F}_q)$ be a divisor of order ℓ^k such that $n_1 \leq n_2 \leq \ldots \leq n_i < k < n_{i+1}$. If $W_1, W_2, \ldots, W_i$ are leaves of orders $\ell^{n_1}, \ell^{n_2}, \ldots, \ell^{n_i}$ generating a subgroup of rank i and a $\mathbb{F}_\ell$-vector space containing leaves only, then one of the sets*

$$\frac{1}{\ell}(D_k + \sum_{j \in J} \epsilon_j W_j)$$

varying $J \subseteq \{1, 2, \ldots, i\}$ and $\epsilon_j \in \{1, 2, \ldots, \ell - 1\}$, is nonempty.

Proof As in [16] we find W_j , $j = i+1, \ldots, r$ divisors of order $\ell^{n_i+2}, \ldots, \ell^{n_r}$ such that

$$< W_1, \ldots, W_i, \ldots, W_r >= Jac(C)(\mathbb{F}_q)[\ell^\infty].$$

we can write

$$D_k = \sum_{j=1}^{r} \sum_{m=1}^{n_j-1} \epsilon_{m,j} \ell^m W_j,\ \epsilon_{m,j} \in \{0, 1, 2, \ldots, \ell - 1\}.$$

Since D_k has order ℓ^k and $n_i < k < n_{i+1}$, then necessarily $\epsilon_{0,j} = 0$ for $j > i$ and $\epsilon_{m,j} \neq 0$ for same $m > 0$ and $j > i$. Then the set

$$\frac{1}{\ell}\left(D_k + \sum_{j=1}^{i}(\ell - \epsilon_{0,j})W_j\right).$$

is nonempty. □

As in [16], the trees in a given ℓ-forest have at most r different heights $h_1 < h_2 < \ldots < h_s$, $s \leq r$. Such different heights $h_1, \ldots, h_s$ take values in the sequence $n_1, ..., n_r$. For every ℓ-forest, if we put $c_i := \#\{\ell\text{-trees of height } h_i\}$, then $c_i = c_j$ for $i = j$.

Proposition 16. *Each c_i is a sum of consecutive powers of ℓ multiply by $(\ell - 1)$, and each tree structure of a ℓ-forest corresponds to one of the ℓ^{r-1} descompositions of $\frac{\ell^r-1}{\ell-1}$ into an ordered sum of the $c_i's$.*

Proof. We observe that if $\frac{1}{\ell}D_\ell$ is a trisection of D_ℓ then $\frac{k}{\ell}D_\ell$ is a trisection of kD_ℓ with $k \in \{1, \ldots, \ell - 1\}$ therefore it is enough study the tree of D_ℓ. As in [16] the decomposition

$$\frac{\ell^r - 1}{\ell - 1} = \ell^{r-1} + \ell^{r-2} + \cdots + \ell + 1 \tag{6.1.2}$$

implies $c_i = \ell^{ri}$. In the less diverse ℓ-forests, some consecutive $n_i's$ coincide, and the $c_i's$ are the corresponding sums of ℓ-powers. □

6.2 The 3-Sylow Algorithm

If D is a 3-torsion divisor, then so is $-D$ and both have the same u-coordinates, and in general terms, they both bring the same information, so we only need to compute one of two. To obtain $\frac{3^r-1}{2}$ (pairs of) 3-torsion divisor, we solve the polynomial system in u_1 instead of a_0. We obtain

Proposition 17. $D_3 = [x^2 + u_1x + u_0, v_1x + v_0] \in \mathrm{Jac}[3]$ *if only if* $M(u_1) = 0$

where M is a polynomial of degree 40 in u_1.

$$\begin{aligned}
u_0 &= 2a_0v_1 + \frac{1}{4}u_1^2 + \frac{5}{2}a_0^2u_1 + \frac{1}{4}a_0^4\\
v_0 &= \frac{5}{4}a_0u_1^2 + \frac{1}{2}u_1v_1 - \frac{5}{2}u_1a_0^3 + \frac{1}{2}a_0f_3 - \frac{5}{2}a_0^2v_1 - \frac{1}{4}a_0^5\\
v_1 &= \frac{160a_0^6u_1 - 32a_0^2u_1f_3 + 48a_0^2f_2 + 450a_0^4u_1^2 - 5u_1^4 - 16f_1}{24a_0(5u_1^2 + 5a_0^4 + 2f_3 + 20a_0^2u_1)}\\
&\quad + \frac{16u_1f_2 - 12u_1^2f_3 + 40a_0^2u_1^3 + 11a_0^8 - 20a_0^4f_3}{24a_0(5u_1^2 + 5a_0^4 + 2f_3 + 20a_0^2u_1)}
\end{aligned}$$

and a_0 is a root of $gcd(p_1(a_0,u_1), p_2(a_0,u_1))$ where p_1, p_2 have degree 7 and 8 in a_0^2.

Remark 8. The polynomial $M(u_1)$ is the 3-modular polynomial in [9].

In Figure 6.1 we represent the 3-forest of 3-rank 3 and exponents $n_1 = n_2 = 1, n_3 = 3$. In two center we painted 26 3-torsion divisors (two center of 13 3-torsion divisors give us two identical figures) , and successively the circles of larger radius show divisors of a higher power order.
The results above are enough to obtain an algorithm to compute generators of $\mathrm{Jac}(C)(\mathbb{F}_q)[3^\infty]$. However, its is also useful to consider the possible tree structures that can appear in the Jacobian of a genus two curve.

Corollary 10. *In ranks $r = 2, 3, 4$ the posible combinations c_i (without multiplying by 2) in the tree structures of the 3-forests are*

Rank 2

$c_1 = 3$ $c_2 = 1$
$c_1 = 4$

Rank 3

$c_1 = 9$ $c_2 = 3$ $c_3 = 1$
$c_1 = 9$ $c_2 = 4$
$c_1 = 12$ $c_2 = 1$
$c_1 = 13$

Rank 4

$c_1 = 27$ $c_2 = 9$ $c_3 = 3$ $c_4 = 1$
$c_1 = 27$ $c_2 = 9$ $c_3 = 4$
$c_1 = 27$ $c_2 = 12$ $c_3 = 1$
$c_1 = 27$ $c_2 = 13$
$c_1 = 36$ $c_2 = 3$ $c_3 = 1$
$c_1 = 36$ $c_2 = 4$
$c_1 = 39$ $c_2 = 1$
$c_1 = 40$

We need the generalization of JumpOnce, JumpTwice and JumpThrice in [16], for example, JumpOnce for $\ell = 3$ is the following:

Algorithm 9 JumpOnce

Require: A polynomial $f \in \mathbb{F}_q[x]$ defining $C : y^2 = f(x)$, a leaf $W_1 \in \mathrm{Jac}(C)(\mathbb{F}_q)$ of order 3^{n_1} , a divisor $S \in \mathrm{Jac}(C)(\mathbb{F}_q)$ and an integer m such that $ord(S) = 3^m$ with $m \geq n_1$.

Ensure: A divisor W_2 such that $S \in W_1, W_2$ and W_1, W_2 generate a vector space of leaves over $\mathbb{F}_3$, and the integer $n_2 = m + n$ where n is the number of halvings performed.

```
$aux \leftarrow 0, \quad n_2 \leftarrow m, \quad T \leftarrow S$
while $aux = 0$ do
  $T \leftarrow T + W_1, \quad W_2 \leftarrow Trisection(T, f(x))$
  if $W_2 \neq T$ then
    $aux \leftarrow 1$
  else
    $T \leftarrow T + 2W_1$ , $\quad W_2 \leftarrow Trisection(T, f(x))$
    if $W_2 \neq T$ then
      $aux \leftarrow 1$
    else
      $aux \leftarrow 2$
    end if
  end if
  while $aux = 1$ do
    $T \leftarrow W_2, \quad W_2 \leftarrow Trisection(T, f(x)), \quad n_2 \leftarrow n_2 + 1$
    if $W_2 = T$ then
      $aux \leftarrow 0$
    end if
  end while
end while
```

For our algorithm, we use function $ThreeModular$ for obtain $\frac{3^r-1}{2}$ 3-torsion divisors such that D_1 and $-D_1$ not appear simultaneously.

In the case of 3-Rank 2 the algorithm for 3-Sylow is given in details in Algorithm 10.

6.3 EXAMPLES

We coded our algorithm in MAGMA. We list below some examples for 3-rank 2, 3, and 4.

Example 14. *Consider* $p = 2^{160} - 47$ *and the curve define by the ecuation*

$$y^2 = x^5 + x$$

over the large prime field $\mathbb{F}_p$. *We obtain that the 3-Sylow is isomorphic to*

Algorithm 10 Generators (3-Rank 2)

```
Require: A polynomial $f(x) \in \mathbb{F}_q[x]$ with 3-Rank 2 defining $C : y^2 = f(x)$.
Ensure: The exponents $n_1, n_2$ and generators $B_1, B_2$ of $\mathrm{Jac}(C)(\mathbb{F}_q)[2^\infty]$.
$(W_1, W_2, W_3, W_4) \leftarrow ThreeModular(f(x))$
for $i = 1, 2, 3, 4$ do
    $n_i \leftarrow 1, \quad W_i' \leftarrow Trisection(W_i, f(x))$
    while $W_i' = W_i$ do
        $W_i \leftarrow W_i', \quad W_i' \leftarrow Trisection(W_i, f(x)), \quad n_i \leftarrow n_i + 1$
    end while
end for
$H \leftarrow \{(n_1, W_1), (n_2, W_2), (n_3, W_3), (n_4, W_4)\}, \quad H[1] \leftarrow \{n_1, n_2, n_3, n_4\}$
$h_1 \leftarrow min(H[1]), \quad m_1 \leftarrow max(H[1]), \quad H_{h_1} \leftarrow \{h \in H | h[1] = h_1\}$
$H_{m_1} \leftarrow \{h \in H | h[1] = m_1\}$
if $\#H_{h_1} = 4$ then
    $(n_1, n_2) \leftarrow (h_1, h_1), \quad (B_1, B_2) \leftarrow (H_{h_1}[1][2], H_{h_1}[2][2])$
end if
if $\#H_{h_1} = 3$ then
    $S \leftarrow H_{m_1}[1][2], \quad W_1 \leftarrow H_{h_1}[1][2]$
    $(W_2, h_2) \leftarrow JumpOnce(f(x), W_1, S, m_1)$
    $(n_1, n_2) \leftarrow (h_1, h_2), \quad (B_1, B_2) \leftarrow (W_1, W_2)$
end if
```

$\mathbb{Z}_{243} \times \mathbb{Z}_{243}$ *with generators*

$$\begin{aligned} w_1 \quad &= (x^2 + 39514305763749093783430851916230692478889505484x \\ &\quad + 448724732024697498281588115834178522172716535578, \\ &46368346753161393223810404775025952070804516 8754x \\ &\quad + 904715675456728052378213536102905799332285438414) \end{aligned}$$

$$\begin{aligned} w_2 \quad &= (x^2 + 1858285664092593466417255706217912343635482062 18x \\ &\quad + 1146156771035184256732545623392790713370851515180, \\ &127956122205862459756386870454301879641663466001x \\ &\quad + 1167566458678377606301428327920815110005508504643) \end{aligned}$$

Example 15. *Consider $p = 127$ and the curve defined by Equation*

$$y^2 = x^5 + x^3 + 3x^2 + 2x + 1$$

over $\mathbb{F}_p$. We obtain that the 3-Sylow is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{27}$ with generators

$$\begin{aligned} w_1 =& (x^2 + 7x + 75, 43x + 90); \\ w_2 =& (x^2 + 16x + 84, 115x + 123); \\ w_3 =& (x^2 + 5x + 107, 104x + 36). \end{aligned}$$

Example 16. *Consider $p = 127$ and the curve define by the equation*

$$y^2 = x^5 + 10x^2 + x$$

over $\mathbb{F}_{p^3}$. We obtain that the 3-Sylow is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_{27} \times \mathbb{Z}_{81}$ with generators

$$\begin{aligned}
w_1 &= (x^2 + (61\omega^2 + 14\omega + 105)x + 75\omega^2 + 25\omega + 35, (76\omega^2 + 126\omega + 102)x + 88\omega^2 + 90\omega + 116);\\
w_2 &= (x^2 + (100\omega^2 + 65\omega + 95)x + 13\omega^2 + 108\omega + 17, (115\omega^2 + 77\omega + 90)x + 20\omega^2 + 93\omega + 124),\\
w_3 &= (x^2 + (112\omega^2 + 122\omega + 84)x + 126\omega^2 + 27\omega + 54, (6\omega^2 + 27\omega + 23)x + 109\omega^2 + 99\omega + 118).
\end{aligned}$$

Finally we shown some interesting cases and we compute s_1 and s_2 using like Schoof algorithms in these cases.

Example 17. *Consider $p = 127$ and the curve define by the equation*

$$y^2 = x^5 + x^3 + x^2 + 2x$$

over $\mathbb{F}_{p^6}$. We obtain that the 3-Sylow is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_{27} \times \mathbb{Z}_{27} \times \mathbb{Z}_{27}$ with generators

$$\begin{aligned}
w_1 = (&x^2 + (42\omega^5 + 24\omega^4 + \omega^3 + 108\omega^2 + 48\omega + 56)x + 69\omega^5 + 106\omega^4 + 104\omega^3 + 59\omega^2 + 60\omega + 108,\\
&(88\omega^5 + 76\omega^4 + 36\omega^3 + 84\omega^2 + 16\omega + 98)x + 42\omega^5 + 19\omega^4 + 74\omega^3 + 105\omega^2 + 35\omega + 53);\\
w_2 = (&x^2 + (51\omega^5 + 16\omega^4 + 10\omega^3 + 25\omega^2 + 85\omega + 28)x + 54\omega^5 + 65\omega^4 + 101\omega^3 + 111\omega^2 + 48\omega + 33,\\
&(47\omega^5 + 3\omega^4 + 37\omega^3 + 90\omega^2 + 63\omega + 29)x + 51\omega^5 + 113\omega^4 + 50\omega^3 + 115\omega^2 + 32\omega + 17)\\
w_3 = (&x^2 + (121\omega^5 + 26\omega^4 + 77\omega^3 + 27\omega^2 + 84\omega + 8)x + 2\omega^5 + 73\omega^4 + 101\omega^3 + 25\omega^2 + 55\omega + 1,\\
&(98\omega^5 + 47\omega^4 + 49\omega^3 + 79\omega^2 + 61\omega + 28)x + 53\omega^5 + 77\omega^4 + 8\omega^3 + 124\omega^2 + 74\omega + 48)\\
w_4 = (&x^2 + (57\omega^5 + 99\omega^4 + 16\omega^3 + 104\omega^2 + 98\omega + 125)x + 123\omega^5 + 62\omega^4 + 46\omega^3 + 80\omega^2 + 58\omega + 114,\\
&(83\omega^5 + 115\omega^4 + 2\omega^3 + \omega^2 + 122\omega + 96)x + 12\omega^5 + 27\omega^4 + 73\omega^3 + 80\omega^2 + 16\omega + 57).
\end{aligned}$$

We can use either w_2 or w_3 to obtain

s_1 mod 27	s_2 mod 27
9	1

Example 18. *Consider $p = 127$ and the curve define by the equation*

$$y^2 = x^5 + 10x^2 + x$$

over $\mathbb{F}_{p^6}$. We obtain that the 3-Sylow is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_{27} \times \mathbb{Z}_{27} \times \mathbb{Z}_{81}$ with generators

$$\begin{aligned}
w_1 = (&x^2 + (40\omega^5 + 112\omega^4 + 34\omega^3 + 70\omega^2 + 53\omega + 6)x + 10\omega^5 + 123\omega^4 + 108\omega^3 + 5\omega^2 + 99\omega + 12,\\
&(34\omega^5 + 54\omega^4 + 7\omega^3 + 45\omega^2 + 75\omega + 80)x + 100\omega^5 + 94\omega^4 + 86\omega^3 + 62\omega^2 + 122\omega + 38);\\
w_2 = (&x^2 + (60\omega^5 + 8\omega^4 + 97\omega^3 + 64\omega^2 + 48\omega + 7)x + \omega^5 + 112\omega^4 + 73\omega^3 + 31\omega^2 + 108\omega + 7,\\
&(99\omega^5 + 4\omega^4 + 54\omega^3 + 69\omega^2 + 23\omega + 5)x + 71\omega^5 + 106\omega^4 + 88\omega^3 + 80\omega^2 + 104\omega + 70);\\
w_3 = (&x^2 + (6\omega^5 + 72\omega^4 + 9\omega^3 + 17\omega^2 + 50\omega + 112)x + 95\omega^5 + 20\omega^4 + 66\omega^3 + 27\omega^2 + 95\omega + 83,\\
&(43\omega^5 + 102\omega^4 + 75\omega^3 + 48\omega^2 + 114\omega + 78)x + 40\omega^5 + 63\omega^4 + 45\omega^3 + 9\omega^2 + 86\omega + 21);\\
w_4 = (&x^2 + (119\omega^5 + 97\omega^4 + 68\omega^3 + 111\omega^2 + 18\omega + 110)x + 60\omega^5 + 67\omega^4 + 81\omega^3 + 119\omega^2 + 31\omega + 1,\\
&(37\omega^5 + 82\omega^4 + 32\omega^3 + 9\omega^2 + 4\omega + 118)x + \omega^5 + 76\omega^4 + 113\omega^3 + 118\omega^2 + 13\omega + 83).
\end{aligned}$$

We can use w_2 to obtain

s_1 mod 27	s_2 mod 27
24	22

Example 19. *Consider $p = 127$ and the curve define by the equation*

$$y^2 = x^5 + 3x^3 + 6x^2 + 3x$$

over $\mathbb{F}_{p^6}$. We obtain that the 3-Sylow is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_{27} \times \mathbb{Z}_{243}$ with generators

$$\begin{aligned}
w_1 = (&x^2 + (101\omega^5 + 7\omega^4 + 7\omega^3 + 9\omega^2 + 68\omega + 114)x + 40\omega^5 + 75\omega^4 + 70\omega^3 + 69\omega^2 + 61\omega + 36, \\
&(111\omega^5 + 75\omega^4 + 73\omega^3 + 41\omega^2 + 73\omega + 6)x + 103\omega^5 + 93\omega^4 + 94\omega^3 + 76\omega^2 + 44\omega + 48) \\
w_2 = (&x^2 + (77\omega^5 + 113\omega^4 + 92\omega^3 + 31\omega^2 + 104\omega + 10)x + 85\omega^5 + 17\omega^4 + 44\omega^3 + 99\omega^2 + 16\omega + 36, \\
&(61\omega^5 + 67\omega^4 + 116\omega^3 + 37\omega^2 + 46\omega + 99)x + 2\omega^5 + 28\omega^4 + 64\omega^3 + 77\omega^2 + 111\omega + 74) \\
w_3 = (&x^2 + (118\omega^5 + 13\omega^4 + 124\omega^3 + 85\omega^2 + 19\omega + 25)x + 21\omega^5 + 49\omega^4 + 17\omega^3 + 106\omega^2 + 108\omega + 93, \\
&(100\omega^5 + 63\omega^4 + 47\omega^3 + 116\omega^2 + 23\omega + 14)x + 94\omega^5 + 58\omega^4 + 105\omega^3 + 76\omega^2 + 72\omega + 17) \\
w_4 = (&x^2 + (119\omega^5 + 120\omega^4 + 109\omega^3 + 9\omega^2 + 114\omega + 70)x + 43\omega^5 + 79\omega^4 + 23\omega^3 + 88\omega^2 + 58\omega + 43, \\
&(59\omega^5 + 75\omega^4 + 99\omega^3 + 95\omega^2 + 101\omega + 60)x + 6\omega^5 + 60\omega^4 + 108\omega^3 + 123\omega^2 + 94\omega + 84)
\end{aligned}$$

we can use w_3 to obtain

s_1 mod 27	s_2 mod 27
6	4

CHAPTER 7

Conclusion

The first four objectives of thesis were studied in Chapters 3 and 5 and the fifth objective was studied in 4 and 6 and the results were as follows:

In chapter 3, we obtained algorithms which allow to trisect any divisor in the Jacobian of a genus two hyperelliptic curve in odd characteristic. The techniques used by Gaudry-Schost in [8] solve system based in the $2D_1 = D_3 - D_1$ with the degrees of both sides balanced. We give in example 2 a case with a divisors D_3 of weight 1 where $2D_1 = D_3 - D_1$ is not balanced. Our technique of de-reduction allows works with equations not balanced and avoid denominators appearing in the addition formulas. We also show how to determine the field of definition of all the ℓ-section with $\ell \in \{3, 5, 7\}$ when the rank of $\mathrm{Jac(C)}(\mathbb{F}_q)[\ell]$ is strictly less than 4 and greater or equal to 1.

In chapter 4, we showed how to compute symbolic trisection polynomial for Jacobians of genus 2 curves over finite field $\mathbb{F}_q$ of odd characteristic. Since the size of the polynomials involved prohibits direct computation, this computation is done via interpolation techniques, taking advantage of several properties of the trisection polynomials (weighted homogeneity, knowledge of the form of leading and constant terms in one of the variables). As was indicated by our experiments, these polynomials can be used to improve the efficiency of trisection algorithms, which may then be used to obtain faster point counting algorithms.

In chapter 5 we complete the study of trisection in characteristic two. The supersingular cases were addressed in [17]. The bottleneck in the case of trisection for non-supersingular genus 2 curves in characteristic 2 is the largest size of the polynomials involved compared with the supersingular case. We used techniques studied in chapter 4 to obtain symbolic trisection polynomial for Jacobians of genus 2 curves over binary field.

Finally in chapter 6 we show how to generalize the algorithms to explicit 2-power torsion of genus 2 curves over finite fields [16] for the case of ℓ-power torsion. These can be used because there exists implementations of ℓ-section for $\ell \in \{2, 3, 5, 7\}$ in odd characteristic and ℓ-section for $\ell \in \{2, 3\}$ in characteristic two. We present explicit algorithms for the computation of the 3-Sylow subgroup. These algorithms may be used to improve the choice of ℓ-torsion divisors of index ℓ^k used in Schoof-like algorithms.

Bibliography

[1] P. Birkner and N. Thériault, *Faster halvings in genus 2*, Selected Areas in Cryptography 2008, LNCS **5381** (2008), 1–17.

[2] J. Canon, W. Bosma and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[3] D. Cantor, *Computing in the Jacobian of a Hyperelliptic Curve*, Mathematics of Computation **48** 95–101, (1987).

[4] D. Cantor, *On the analogue of the division polynomial for hyperelliptic curves*, J. Reine Angew. Math. **447** , 91-145,(1994).

[5] G. Cardona, E. Nart and J. Pujolàs, *Curves of genus two over fields of even characteristic*, Math. Z. 250 (2005) number 1, 177–201.

[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 (Boca Raton). Chapman & Hall/CRC, Boca Raton (2005).

[7] P. Gaudry and E. Schost, *Construction of secure random curves of genus 2 over prime fields*, Eurocrypt, 3027, 239-256, (2004).

[8] P. Gaudry and E. Schost, *Genus 2 point counting over prime fields*, Journal of Symbolic Computation, 47, 4, 368-400, (2012).

[9] P. Gaudry and E. Schost, *Modular equations for hyperelliptic curves*, Mathematics of Computation, 74, 429-454, (2005).

[10] T. Lange and M. Stevens: *Efficient Doubling for Genus Two Curves over Binary Field.* Selected Areas in Cryptography SAC 2004, LNCS, 3357. 170181 (2005).

[11] T. Ishiguro, K. Matsuo, *Fields of definition of torsion points on the Jacobians of genus 2 hyperelliptic curves over finite fields*, Proc. of SCIS2010, IEICE Japan, 2D4-6, January 2010

[12] I. Kitamura, M. Katagi and T. Takagi, *A complete divisor class halving algorithm for hyperelliptic curve cryptosystems of genus two*, LNCS **3574** , 146–157,(2005).

[13] J. Miret, R. Moreno, A. Rio and M. Valls, *Computing the ℓ-power torsion of an elliptic curve over a finite field*, Mathematics of Computation **78** number 267 (2009), 1767–1786.

[14] J. Miret, R. Moreno, J. Pujolàs and A. Rio, *Halving for the* 2*-Sylow subgroup of genus* 2 *curves over binary fields*, Finite Fields Appl. **15** (2009), 569–579.

[15] J. Miret, J. Pujolàs and A. Rio, *Bisection for genus* 2 *curves in odd characteristic*, Proceedings of the Japan Academy– Series A **85** , 55–61.(2009)

[16] J. Miret, J. Pujolàs and A. Rio, *Explicit 2-Power Torsion of Genus* 2 *Curves over Finite Fields*, Advances in Mathematics of Communications **4** number 2 , 155–165,(2010).

[17] J. Miret, J. Pujolàs and N. Thériault, *Trisection for supersingular genus 2 curves in characteristic 2*, Advances in Mathematics of Communications **8**, num. 4, 375–387 (2014).

[18] J. Pujolàs, E. Riquelme and N. Thériault, *Trisection for non-supersingular genus 2 curves in characteristic 2*, International Journal of Computer Mathematics, DOI: 10.1080/00207160.2015.1059935.

[19] E. Riquelme, *Trisection for genus* 2 *curves in odd characteristic*, Applicable Algebra in Engineering Communication and Computing DOI:10.1007/s00200-015-0282-3.

[20] H. Verdure, *Factorisation patterns of division polynomials*, Proc. Japan Acad. Ser. A Math. Sci. **80** num. 5, 79-82 (2004)

[21] https://dl.dropboxusercontent.com/u/50859627/TrisecAAECC/TorsionAAECC.txt

[22] https://dl.dropboxusercontent.com/u/50859627/TrisecAAECC/trisection2AAECC.txt

[23] https://dl.dropboxusercontent.com/u/50859627/TrisecAAECC/trisection1AAECC.txt

[24] https://dl.dropboxusercontent.com/u/50859627/TrisecAAECC/orbitas.txt