ADDITION IN JACOBIAN OF HYPERELLIPTIC CURVES

A Dissertation
by
Sandeep Sadanandan
CS03M031

Submitted in partial fulfillment of the requirements for the award of degree of

Master of Technology
in
Computer Science and Engineering
from
Indian Institute of Technology Madras, Chennai
within the framework of
DAAD-IIT Master Sandwich Program-2004
under the esteemed guidance of

Professor Ernst W Mayr
Dr. Peter Ullrich
Lehrstuhl für Effiziente Algorithmen
Institut für Informatik
Technische Universität München
Germany

Professor C Pandu Rangan
Theoretical Computer Science Laboratory
Dept. of Computer Science and Engineering
Indian Institute of Technology Madras
India

CERTIFICATE

This is to certify that the thesis entitled **Addition in Jacobian of Hyperelliptic Curves** by **Sandeep Sadanandan (CS03M031)**, submitted to the Indian Institute of Technology Madras, Chennai, India for partial fulfillment of the requirements for the award of **Master of Technology**, is a bona fide record of work carried out by him under our combined supervision. The contents of the thesis, in full or parts, have not been submitted to any other institute or university for the award of any degree or diploma.

Place: Chennai
Date : Prof. Dr. C Pandu Rangan

Place: München
Date : Prof. Dr. Ernst W Mayr

Place: München
Date : Dr. Peter Ullrich

ACKNOWLEDGEMENT

On successful completion of the dissertation I take this opportunity to thank all those involved directly or indirectly in its accomplishment.

I cannot express in few words my gratitude towards my supervisor Dr. Peter Ullrich who provided valuable guidence and support throughout the duration of this master thesis. This thesis would not have been possible without his help. I specially thank him for his infinite patience. The discussions I had with him were invaluable.

I thank Prof. Dr. Ernst W Mayr for accepting me as a post graduate student to work at the Chair for Efficient Algorithms.

I am indebted to Prof. Dr. C Pandurangan for giving me guidance and necessary support during the proceeding of this work at TU-M*ü*nchen. His timely advices and fatherly approach was always a great feeling. I also thank Prof. S Raman, Head of the Department, Dr. V Kamakoti, my faculty advisor and all other teachers at IIT Madras CSE department for facilitating my project work.

Many thanks to German Academic Exchange Service (Deutscher Akademischer Austausch Dienst) for providing me this opportunity to carry out this work at TU-M*ü*nchen. I thank all the nice people from the Center for International affairs, TU-M*ü*nchen for providing me with help and support in the initial part of my stay in M*ü*nchen.

Last but not least - my friends. On this occasion I not only thank them but also express my love for all my friends, in Germany and in India. They were always there for me.

Sandeep Sadanandan

M*ü*nchen, May 2005

It is better to do the right problem the wrong way than the wrong problem the right way.

- Richard Hamming.

Contents

Abstract

Rapid growth of electronic communication brought cyptography from military uses to the limelight in research community. The advent of small scale devices including handy and smart cards has given more importance to light-weight-cryptography.

This project is a study in the latest trend in cryptography - HECC(Hyper-Elliptic Curve Cryptography). An investigation in the existing methods of group operation in jacobian of a curve. A few attempts made to improve the present status of the field also are included.

Chapter 1

Introduction

Basic research is what I'm doing when

I don't know what I'm doing.

– Wernher Von Braun

1.1 The Scenario

Fast secure privacy!! This is what the world is after. Yes, better methods of doing cryptography. We need privacy with enough security and it should be fast. There are already many cryptosystems available which satisfy these requirements. But, new, emerging, small devices with very limited computing power, want to give more attention to public key cryptosystems. Other than RSA, most of the cryptosystems rely on the *discrete logarithm problem*[1]. The classical cryptosystems use DLP over multiplicative group of finite fields.

[1]Given an element g in a finite group G and another element $h \in G$, find an integer x such that $g^x = h$. Abbreviated as *DLP*

To have a cryptosystem based on a group if the group operations are fast, its order is easily computable, DLP is hard and the representations are compact. In 1987 Koblitz [10] introduced Elliptic Curve Cryptography(ECC). It is based on the discrete logarithm problem over the abelian group of points of the curve. The group of points has all the characteristics we need for cryptography. The advantages of using ECC were small-sized keys and easy generation of curves(groups). Also, there are no sub-exponential algorithms for ECDLP (Elliptic Curve DLP).

Later in 1989, Koblitz [11] introduced discrete logarithm based hyperelliptic cryptosystems which are over the Jacobian of hyperelliptic curves. Hyperelliptic curves are generalisations of elliptic curves. Here the advantage was again a good reduction in the keysize which eases the computation, still giving same level of security. Also, non-existence of sub-exponential algorithms. The smaller size of base field makes hyperelliptic curves a good choice for light weight cryptosystems.

The algorithm for group operation was given by Cantor [3]. In hyperelliptic curve cryptosystems, group operation is addition in the jacobian of the curve. The algorithm by Cantor [3] was the fastest algorithm for addition in the jacobian until in 2000, Harley algorithm [6, 5] was introduced. After that, there were many improvements and researches going on in the area of HECC. Hyperelliptic curve cryptosystems are the latest trend in cryptography. A comparison with respect to the keysize of RSA and HECC is given in the table 1.1. For more details about the mapping between the two, refer [20].

Unfortunately, in HECC, the algorithms for group operation are not as fast as in finite fields. For genus 1 hyperelliptic curves (elliptic curves) there are very fast algorithms. For larger genus curves, the algorithms for group operation are to be optimised to a much better level that to achieve the type of fast cryptosystems. That

Base Field	HECC-Keysize	RSA Equivalent
$F(2^{83})$	166	925
$F(2^{97})$	194	1325
$F(2^{113})$	226	1892
$F(2^{131})$	262	2681
$F(2^{149})$	298	3643
$F(2^{163})$	326	4517

Table 1.1: Keysize comparison: HECC (g = 2) Vs RSA

makes the study of HECC and the addition important.

1.2 Objectives

The objectives of the project can be listed as follows.

1. Study and understand the group laws of jacobian of hyperelliptic curves.
2. Investigate about the algorithms for addition in the jacobian.
3. Try to design some better algorithm.

This thesis, I am writing with one more objective in mind. I am trying to make this report a good point to start the studies about hyperelliptic curves - without much formal mathematics.

1.3 Overview

The following is an outline of the rest of the thesis.

- **Chapter 2: Mathematical Background**

In this chapter I try to explain the basic algebra and algebraic geometry needed for the rest of the book. By no way this is self contained. The major topics include the basics of groups - rings - fields in the algebra part. In the algebraic geometry part affine - projective spaces are introduced and their relation between each other as well. Basic details about algebraic curves, about coordinate rings - rational functions - Bezout's theorem - divisors - genus etc also. The end of the chapter just mentions about Riemann-Roch problem. I have not given most of the proofs of theorems and lemmas. The references given provide a better and detailed description of all the contents of the chapter.

- **Chapter 3: Hyperelliptic Curves**

From this chapter onwards, we move from general algebraic curves to the special types of curves on which are of our interest. Here we see the basic properties of hyperelliptic curves. A few examples - semi-reduced divisors - reduced divisors - jacobian - the group operation in the jacobian etc. Finally we see different types of representations of reduced divisors which are of more importance from the view point of computing world. The chapter makes the background needed for understanding the methods in addition in jacobian.

- **Chapter 4: Addition**

This chapter very briefly explains a few of the existing algorithms. Analysis and discussion are avoided. First of all, the chapter gives geometric concept of divisor addition in the jacobian. Then Cantor's algorithm - Harley's method - Lange's formulae etc are mentioned.

- **Chapter 5: Point Addition**

  This is where I discuss and explain the details of the algorithm devised by my team. The reduction algorithm in the chapter makes use of a probabilistic algorithm to find out the roots of polynomials.

- **Chapter 6: Addition using Chow Forms**

  This chapter discusses over another algorithm which is not complete. The basic idea is built for the addition algorithm. The details remain open still now. The method presented used a different type of divisor represetation which is very old in the literature. As all the researches were going on in a single type of representation, this was an attempt to see the problem from another viewpoint.

Rest of the thesis concludes the discussion and says about furthur work to be done.

1.4 Notation

We follow the notation of Fulton [4]. In the thesis, a reader can find many definitions, lemmas, theorems, facts and examples. Definitions, lemmas and theorems mean the same as in the common terminology. Facts are some truths which are not to be proved or just proofs are not given. They can be said to be similar to axioms. Some of them are theorems of which proofs are out of the scope of the thesis.

Chapter 2

Mathematical Background

"Young man, in mathematics you don't understand things,
you just get used to them."

– John von Neumann.

2.1 Abstract Algebra

Giving a background in abstract algebra is not an easy thing. It is always better to read **atleast** one book which gives you the basics of algebra. Atleast till the point where you can start to study more about field theory and Galois theory. A very good reference for the study of basic algebra is Herstein [7] and for field theory is Roman [18]. However, I give the definitions and results in abstract algebra which will be useful for our study of hyperelliptic curves. I believe that anybody who is reading this thesis is having enough background in *set theory*. So, here I start with groups.

2.1.1 Groups

Definition 1 (Group). A nonempty set G is said to be a group if in G there is defined an operation $\oplus$ such that it satisfies the following.

1. Closure: $a, b \in G$ implies $a \oplus b \in G$
2. Associativity: Given $a, b, c \in G$ then $a \oplus (b \oplus c) = (a \oplus b) \oplus c$
3. Existence of Identity: There exists a special element $\epsilon \in G$ such that $a \oplus \epsilon = \epsilon \oplus a = a$ for all $a \in G$. ϵ is called the *identity* element of G.
4. Inverse Element: For every $a \in G$ there exists an element $b \in G$ such that $a \oplus b = b \oplus a = \epsilon$. (We write b as a^{-1} and call it the *inverse* of a in G)

These four conditions are called *group axioms*.

We usually represent a group by $(G, *)$; where G is the group and $*$ is the group operation.

Example 2. $(\mathbb{Z}, +)$ is a group where $\mathbb{Z}$ is the integers and $+$ is the ordinary addition.

Definition 3 (Order). The number of element of a group is called the *order* of he group. if the order is finite, the group is said to be a finite group. Order of a group G is denoted as G.

But, for an element $a \in G$, the least positive number m such that $a^m = \epsilon$ is called the *order* of a in G.

Definition 4 (Abelian/Commutative Group). A group is an abelian[1] group if $a \oplus b = b \oplus a$ for all $a, b \in G$.

[1]The name comes from the great Norwegian mathematician Niels Henrik Abel

Definition 5 (Subgroup). A nonempty subset H of a group G is called a subgroup of G, if relative to the operation in G, H itself satisfies all the group axioms.

Example 6. H = {Even numbers} $\subset \mathbb{Z}$ $(H, +)$ is a group under ordinary addition.

Definition 7. A relation $\sim$ of a set G is called an equivalence relation if for all $a, b, c \in G$:

1. $a \sim a$.(Reflexive)
2. $a \sim b$ implies $b \sim a$.(Symmetric)
3. $a \sim b$ and $b \sim c$ implies $a \sim c$.(Transitive)

Definition 8 (Equivalence Class). If $\sim$ is an equivalence relation on G, then $[a]$, the equivalence class of a is defined by $[a] = \{b \in G \mid b \sim a\}$.

Lemma 9. If $\sim$ is an equivalence relation on G, then

1. G = $\bigcup_{a \in G}[a]$
2. $[a] \cap [b] \neq \phi$ equivalent to $[a] = [b]$

Proof:

Since $a \in [a]$, it is clear that $\bigcup_{a \in G}[a]$ = G.

Suppose that $[a] \cap [b] \neq \phi$. Let $c \in [a] \cap [b]$ So, $c \sim a$ since $c \in [a]$ and $c \sim b$ since $c \in [b]$. Again, $c \sim a$ implies $a \sim c$ because of symmetry. And $c \sim a$ and $c \sim b$ together imply $a \sim b$ (transitivity).

Hence $a \in [b]$. So, for all $x \in [a], x \sim a, a \sim b$ gives $x \sim b$. i.e, $[a] \subset [b]$. The same way we can prove that $[b] \subset [a]$.

ie, $[a] = [b]$.

ie, if $[a] \cap [b] \neq \phi$, $[a] = [b]$. Which is equivalent to $[a] \neq [b]$ implies $[a] \cap [b] = \phi$

Definition 10 (Coset). For a group G, for which H is a subgroup, and an element of G, then $gH = \{gh \mid h \text{ an element of } H\}$ is called the left coset of H in G, $Hg = \{hg \mid h$ an element of $H\}$ is called the right coset of H in G.

Theorem 11 (Lagrange's[2] Theorem). If G is a finite group and H is a subgroup of G, then $o(H) \mid o(G)$

Proof:

It is very easy to see that the relation $a \sim b$ iff $ab^{-1} \in H$ is an equivalence relation[3].

($aa^{-1} = \epsilon \in H$ so $a \sim a$. If $ab^{-1} \in H$, as $H \subset G$, $(ab^{-1})^{-1} \in H$ implies $ba^{-1} \in H$ i.e, $b \sim a$. The same way, if $ab^{-1} \in H$ and $bc^{-1} \in H$ implies $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$. So, $a \sim c$).

Also, we can see that $[a] = Ha = \{ha \mid h \in H\}$.

($ab^{-1} \in H$. Let $ab^{-1} = h$, *so,* $a = hb$. If $a = kb$; $k \in H, ab^{-1} = (kb)b^{-1} = k \in H$. So, $a \sim b$ iff $a \in Hb = \{hb \mid h \in H\}$. i.e, $[b] = Hb$.

Let k be the number of distinct classes. We name them to be $Ha_1, Ha_2,$ $\ldots, Ha_k$. By Lemma 9 $\bigcup_{i=1}^{k} Ha_i = G$ and we know that $Ha_i \cap Ha_j = \phi$; $i \neq j$. Our claim is that $o(Ha_i) = o(H)$. If $ha_i = h'a_i$ by cancellation, $h = h'$. So the mapping is $1-1$. $G = \bigcup_{i=1}^{k} Ha_i$, $i \neq j \Rightarrow Ha_i \cap Ha_j = \phi$. This implies $o(G) = k \times o(H)$. Hence $o(H) \mid o(G)$.

Fact 12. If G is finite and $a \in G$, then $o(a) \mid G$ We can see this directly from definition 3 and Theorem 11.

Definition 13 (Homomorphism). Let G and G' be two groups then a mapping $\phi : G \to G'$ is called a homomorphism if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

[2]The name of the theorem comes from famous mathematician J L Lagrange

[3]For the ease of representation, we represent $a \oplus b$ as ab

If the homomorphism is a bijection, then it is called an isomorphism.

Definition 14 (Kernel). If ϕ is a homomorphism from G to G', then the kernel of ϕ is defined by $k\phi = \{a \in G \mid \phi(a) = \epsilon'\}$, and ϵ' is the identity element of G'.

Definition 15. Image of a subgroup H of G under ϕ is defined as $Im(H) = \{b \in G' \mid \exists a \in G \text{ such that } \phi(a) = b\}$.

Definition 16 (Normal Subgroup). A subgroup N of G is said to be normal subgroup iff $a^{-1}Na \subset N$ for every $a \in G$.

We denote this by $N \triangleleft G$.

Definition 17 (Factor group). If $N \triangleleft G$ and we define $a \sim b$ iff $ab^{-1} \in N$, we get a new set of equivalence classes. This set of equivalence classes is called the *factor group or quotient group* of G by N.

We have a symbol for this factor group is G/N.

Theorem 18. If $N \triangleleft G$, and

$\frac{G}{N} = \{[a] \mid a \in G\} = \{Na \mid a \in G\}$

Then G/N is a group relative to $[a][b] = [ab]$.

Proof:

Define $\psi : G \to G/N$ by $\psi(a) = [a]$. It's easy to see that it is a homomorphism. From the definition itself it is evident that the mapping is onto.

What is the kernel of the mapping? $K\psi = \{a \in G \mid \psi(a) = E\}$ where E us the unit of G/N. $E = [\epsilon] = N\epsilon = N$, $a \in K\psi$ iff $E = N = \psi(a) = Na$. But $Na = N$ says that $a = ea \in Na = N$ so, $K\psi \subset N$ similarly we can prove that $N \subset K\psi$.

Hence $K\psi = N$.

Theorem 19 (Homomorphism). Let $f : G \to G'$ be a homomorphism and N be a sub group of G with $N \subseteq ker(f)$. We then have a unique homomorphism $h : G/N \to G'$ such that $h \circ \phi = f$.

ie,

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \phi \downarrow & h \nearrow & \\ G/N & & \end{array}$$

Now we have come to a point where we can discuss the other three homomorphism theorems. I will state them one by one. I shall not give the proofs. For the proofs reader can refer to any of these books by Herstein [7, 8].

Theorem 20 (First Homomorphism Theorem). Let ϕ be a homomorphism of G *onto* to G' with kernel K. Then $G' \simeq G/K$, the isomorphism between these effected by the map.

$$\psi : G/K \to G'$$

defined by $\psi(Ka) = \phi(a)$.

Theorem 21 (Second Homomorphism Theorem). Let the map $\phi : G \to G'$ be a homomorphism of G *onto* G' with kernel K. If H' is a subgroup of G' and if

$$H = \{a \in G \mid \phi(a) \in H'\}$$

Then H is a subgroup of G, $H \supset K$ and $H/K \simeq H'$. Finally, if $H' \triangleleft G'$ then $H \triangleleft G$.

Theorem 22 (Third Homomorphism Theorem). If the map $\phi : G \to G'$ is a homomorphism of G *onto* G' with kernel K, then if $N' \triangleleft G'$ and $N = \{a \in G \mid \phi(a) \in N'\}$, we conclude that $G/N \simeq G'/N' \Leftrightarrow G/N \simeq (G/K)/(N/K)$

2.1.2 Rings and Fields

Definition 23 (Ring). Let R be a set on which two binary operations are defined, called addition and multiplication, and denoted by $+$ and $\cdot$. Then R is called a *ring* with respect to these operations if the following properties hold:

1. Closure: If $a, b \in R$, then the sum $a + b$ and the product $a \cdot b$ are uniquely defined and belong to R.

2. Associative law: For all $a, b, c \in R$, $a+(b+c) = (a+b)+c$ and $a\cdot(b\cdot c) = (a\cdot b)\cdot c$.

3. Commutative law: For all $a, b \in R$, $a + b = b + a$.

4. Distributive law: For all $a, b, c \in R$, $a\cdot(b+c) = a\cdot b+a\cdot c$ and $(a+b)\cdot c = a\cdot c+b\cdot c$.

5. Additive identity: The set R contains an additive identity element, denoted by 0, such that for all $a \in R$, $a + 0 = a$ and $0 + a = a$.

6. Additive inverse: For each $a \in R$, there exists an element $b \in R$ such that $a + b = 0$ and $b + a = 0$. The element b is called the additive inverse of a in R, and denoted by $-a$.

If $\cdot$ is also commutative, the ring is called a commutative ring. Otherwise an associative ring.

Definition 24 (Integral Domain). A commutative ring R is called an Integral Domain if $a \cdot b = 0$ implies $a = 0$ or $b = 0$. In other words, an integral domain is a commutative ring with NO zero divisors.

An element $0 \neq a \in R$ is called a zero divisors of there exists an element $b \neq 0 \in R$ such that $a \cdot b = 0$.

If there is an element $1 \in R$ such that for all $a \in R$, $1 \cdot a = a \cdot 1 = a$. We call R to be a ring with unit. It is necessary that $1 \neq 0$.

Definition 25 (Ideal). For a group we have subgroup. The same way, for a ring we have an Ideal. It is defined as below.

Let R be a ring, a non-empty subset I of R is called an ideal (two sided) if

1. I is an additive subgroup of R.
2. Given $r \in R$, $a \in I$, then $ra \in I$ and $ar \in I$.

Definition 26 (Homomorphism). Similar to group homomorphisms, we have homomorphisms in rings also.

A mapping $\phi : R \to R'$ of the ring R into the ring R' is a homomorphism if

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$

Definition 27 (Field). A ring R is called a field iff the following conditions are satisfied.

1. R is a ring with unit.
2. For all $a \neq 0 \in R$ there exists a $b \in R$ such that $a \cdot b = b \cdot a = 1$. This b is denoted as b^{-1}

3. R is commutative.

Or, we can say the same in other words.

1. $(R, +)$ is a commutative ring.

2. $(R^*, \cdot)$ is a commutative ring.$(R^* = R\backslash\{0\})$.

3. $\cdot$ is distributive over $+$.

2.1.3 Extension Field

Definition 28 (sub-field, extension field). If a field F is a subset of another field K with respect to the same operations in K, then F is called to a sub-field of K. And, K is an extension field of F.

Definition 29 (algebraic, minimal polynomial). Let K be an extension field of F. An element $a \in K$ is said to be algebraic over F if there exists a polynomial $f \in F[x]$ with $f(a) = 0$. The monic polynomial with minimal degree so that $f(a) = 0$ is called the minimal polynomial of a over F and denoted by f^a_{min}.

Definition 30 (Algebraic closure). A field K is said to be algebraically closed if every polynomial $f(x) \in K[x]$ has a zero in K. Such a polynomial splits into linear factors.

Sometimes, for a field F, all the polynomials in $F[x]$ have their zeros in K, an extension field of F. Then K is called the algebraic closure of F.

From the cryptographic perspective, all the details of algebra are not needed. In [12] Koblitz give an excellent tutorial of what is needed for our purpose.

2.2 Algebraic Geometry

In this section we will see the basics of algebraic geometry which are very essential for the rest of the thesis. For a better understanding of the details, the reader may refer to Fulton [4]. Also a very good explanation about projective space is given in the appendix of [19]. We directly start with the definitions and theorems.

Note: From here onwards, k is a field and K is its algebraic closure.

2.2.1 Affine Geometry

Definition 31 (Affine Space). $A^n(k)$ means the Cartesian product of k with itself n times. $A^n(k)$ is the set of n-tuples of elements of k. $A^n(k)$ is called n-dimensional affine space over k. Its elements are called points. Simply A^n means $A^n(K)$ where k is understood and K is its closure.

$A^1(k)$ is the affine line and A^2 is the affine plane.

The points in $A^n(k)$ are called the rational points of A^n.

Definition 32 (Zero of a polynomial). If $F \in k[x_1, x_2, \ldots, x_n]$, a point $P = (a_1, \ldots, a_n) \in A^n$ is a zero of F if $F(P) = F(a_1, \ldots, a_n) = 0$. The set of zeros of F is called the hyper-surface generated by F and is denoted by $V(F)$.

Definition 33 (Affine algebraic set). If S is any set of polynomials in $k[x_1, x_2, \ldots, x_n]$, then

$$V(S) = \{P \in A^n \mid F(P) = 0 \text{ for all } F \in S\}$$

$$V(S) = \bigcap_{F \in S} V(F)$$

A subset $X \in A^n$ is an affine algebraic set if $X = V(S)$ for some S.

Definition 34 (Affine variety). An affine algebraic set is called an affine variety if it cannot be written as a union of two smaller affine algebraic sets.

Or

It is an irreducible affine algebraic set. i.e, if $X = V(S)$ and the ideal generated by S is a prime ideal in $k[x_1, x_2, \ldots, x_n]$, then X is an affine variety.

2.2.2 Projective Geometry

Now we should see the definition of projective space. But, before the formal definition, we will see what it means.

We know that two different lines intersect at exactly one point. Is it always true? What happens if they are parallel?

In our case, we need any two lines to intersect - whether they are parallel or not. So we are trying to enlarge the plane so that they will intersect at infinity. For the same, we identify each point[4] $(x, y) \in A^2$ with points $(x, y, 1) \in A^3$. Every point $(x, y, 1)$ determines a unique line which passes through the origin and the point $(x, y, 1)$. Every line through $(0, 0, 0)$ which are in the place $z = 0$ are the points at infinity.

Definition 35 (Projective Space). Projective Space over k, written as $P^n(k)$ or simply P^n is defined to be the set of all lines through $(0, 0, \ldots, 0)$ in $A^{n+1}(k)$. Any point $x = (x_1, \ldots, x_{n+1}) \neq (0, \ldots, 0)$ determines a unique line namely $\{(\lambda x_1, \ldots, \lambda x_{n+1}) \mid \lambda \in k\}$.

[4]For ease of understanding we take A^2 and A^3. In general, we can take A^n and A^{n+1} with $(n+1)^{th}$ co-ordinate to be one.

Two points (x) and (y) are defined to be equivalent iff there is a nonzero $\lambda \in k$ such that

$$y_i = \lambda x_i \text{ for } i = 1, \ldots, n+1$$

One other way to identify P^n is as the set of equivalence classes of points in $A^{n+1} - \{0, \ldots, 0\}$.

Definition 36 (Homogeneous coordinates). Elements of P^n[5] will be called points. The equivalence classes of points are given by

$$(x_1, \ldots, x_{n+1}) \sim (\lambda x_1, \ldots, \lambda x_{n+1});\ \lambda, x_i \in k.$$

If a point $P \in P^n$ is determined by some $(x_1, \ldots, x_{n+1}) \in A^{n+1}$, we say that $(x_1, \ldots, x_{n+1})$ is a set of homogeneous coordinates for P. In fact, $(x_1, \ldots, x_{n+1})$ stands for an equivalence

Definition 37 (Homogeneous Polynomial). A homogeneous polynomial is a polynomial with all its terms are having the same degree.

Or formally,

$$F(\lambda x_1, \ldots, \lambda x_{n+1}) = \lambda^{deg(f)} F(x_1, \ldots, x_{n+1}) \text{ for all } \lambda \in K.$$

Definition 38 (Projective algebraic set, Projective variety). If S is any set of homogeneous polynomials in $k[x_1, x_2, \ldots, x_{n+1}]$,

$$V(S) = \{P \in P^n \mid F(P) = 0 \text{ for all } F \in S\}$$

[5] P^n means $P^n(K)$ when k is known and K is its closure

$$V(S) = \bigcap_{F \in S} V(F)$$

A subset $X \subseteq P^n$ is an projective algebraic set if $X = V(S)$ for some S.

A projective algebraic set is called an projective variety if it cannot be written as a union of two smaller projective algebraic sets.

Or

It is an irreducible projective algebraic set. i.e, if $X = V(S)$ and the ideal generated by S is a prime ideal in $k[x_1, x_2, \ldots, x_{n+1}]$, then X is an projective variety.

When $V(I)$ is a projective or affine variety then the polynomials in $I(V)$ are irreducible. Otherwise, the union of the factors of these polynomials form the same ideal, as the roots of the polynomials are the same. Now, the ideal formed is prime ideal. Suppose, for example that the ideal is generated by only one irreducible polynomial: $I(V) = F$. Then $GH \in (F) \Rightarrow G \in (F)$ or $H \in (F)$. In other words: F divides G or H.

2.2.3 Affine and Projective spaces - Relation

We came up with the projective plane to enable any two lines to intersect at exactly one point. Now we should see how it happens. We know that a point $(x, y, z) \in P^2 \Leftrightarrow (x/z, y/z, 1) \in P^2 \Leftrightarrow (x, y) \in A^2$. Now, we should try to get the points at infinity by putting $z = 0$ in $(x, y, z) \in P^2$. We get a point at infinity of A^2. Using homogeneous coordinates and polynomials we can find the intersection of the lines (x, y, z) in the projective plane $z = 0$. The intersection represents the point at infinity of A^2 which will be the point of intersection of the lines under consideration. This sounds really absurd. But we define that all lines in the plane $z = 0$ and passing through origin

corresponds to directions in the affine space. So we can define the projective space as follows.

$$P^2 = A^2 \cup \{\text{set of directions in } A^2\}$$

So, all lines in the same direction will intersect at one of these points.

Now, how do we define it formally? We can define the set of direction in A^2 by P^1. So, $P^2 = A^2 \cup P^1$. Following represents the mapping between the two spaces.

$$\frac{\{[a,b,c] : a,b,c \text{ not all zero}\}}{\sim} \leftrightarrow A^2 \cup P^1$$

$$[a,b,c] \rightarrow \begin{cases} (a,b) \in A^2 & \text{if } c \neq 0 \\ [a,b] \in P^1 & \text{if } c = 0 \end{cases} \tag{2.1}$$

$$[x,y,1] \leftarrow (x,y) \in A^2 \tag{2.2}$$

$$[A,B,0] \leftarrow [A,B] \in P^2 \tag{2.3}$$

Definition 39 (Homogenisation and Dehomogenisation). $F \in k[x_1, \ldots, x_{n+1}]$ is called a form if it is a homogeneous polynomial and we define $F_* = F(x_1, \ldots, x_n, 1)$. This is called de-homogenisation.

If we have a polynomial in n variables, we can put $x_i = x_i/x_{n+1}$. This transformation gives F^* from F. This is called homogenisation.

Definition 40 (Algebraic Curve). An algebraic curve is always an algebraic variety of dimension equal to one. In two dimensional plane (P^2), a projective variety C is called an algebraic curve when $I(C)$, the ideal of $k[x_1, \ldots, x_{n+1}]$ which generates C,

consists of a single polynomial $\in k[x_1, \ldots, x_{n+1}]$ which is irreducible by definition.

We denote $V(I)$, [curve generated by ideal I] by C

$$C : F(x_1, \ldots, x_{n+1}) = 0 \in k[x_1, \ldots, x_{n+1}]$$

and $I(C) = F$.

From here onwards, C is an algebraic curve. Let it be $C : F(x_1, \ldots, x_n)$.

Definition 41 (Coordinate ring). Coordinate ring of C over k is the quotient ring given by

$$k[C] = k[x_1, \ldots, x_n]/I(C)$$

Similarly, the coordinate ring of C over K is defined as

$$K[C] = K[x_1, \ldots, x_n]/I(C)$$

An element of $K[C]$ is called polynomial function on C. they are polynomials modulo C.

Definition 42 (Function field and rational functions). The function field $k(C)$ of C over k is the field of fractions of $k[C]$. Similarly, $K(C)$ the function field of C over k is the field of fractions of $K[C]$.

$$K(C) = \left\{ \frac{G}{H} \mid G, H \in K[C], deg(G) = deg(H) \right\}$$

An element of $K[C]$ is called a rational function.

Definition 43 (Zeros and Poles). Let $R \in K(C)^*$ and $P \in C$. If $R(P) = 0$, then

R is said to have a zero at P. If R is not defined at P, then R has a pole at P. (We write $R(P) = \infty$)

Definition 44 (Uniformising parameter). Let $P \in C$. For all $G \in KC)^*$, there exist $T, S \in K(C)^*, m_P \in \mathbb{Z}$ such that,
$G = T^{m_P}S$ and $T(P) = 0$ and $S(P) \neq 0, \infty$.

The function T is called a uniformising parameter for P.

Definition 45 (Intersection multiplicity). Let $G, S \in K(C)$ and $P \in C$. Let $T \in K(C)$ be the uniformising parameter for P:
$G = T^{m_P}S$ and $T(P) = 0$ and $S(P) \neq 0, \infty$. Then m_P is the intersection multiplicity of G at P.

Theorem 46 (Bezout's Theorem). Let F and G be projective plane curves with degrees m an n respectively. Assume F and G have no common components. Then :

$$\sum_{P \in F \cap G} I(P) = mn$$

Where $I(P)$ is the intersection multiplicity at point P and $P \in F \cap G$ are the common points of F and G. i.e, the points of intersections.

Definition 47 (Order of Polynomial functions). The order of a polynomial function $G \in K[C]$ at a point $P \in C$ is the intersection multiplicity at that point and denoted by $ord_P(G)$.

Definition 48 (Order of rational functions). The order of a rational function $R = G/H \in K(C)$ at a point $P \in C$ is defined as: $ord_P(R) = ord_P(G) - ord_P(H)$.

2.3 Divisors

The ideals generated by the polynomial in function field is C are sub-varieties of C. i.e, the intersection of roots of $I(C)$ and a rational function. We name them as Divisor.

Definition 49 (Divisor). A divisor D is a formal sum of points $P \in C$:

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

with $m_P \in \mathbf{Z}$ and for all but finitely many $m_P = 0$.

The degree of D is the integer $deg(D) = \sum_{P \in C} m_p$.

The order of D at P is the integer $ord_P(D) = m_P$.

Definition 50 (support of a divisor). Let $D = \sum_{P \in C} m_P P$ be a divisor. The support of D is the set:

$$supp(D) = P \text{ in } C : mp \neq 0$$

Definition 51 (Addition of divisors). The divisors form a group under addition. The group of divisors of C are denoted by $Div(C)$. We can add two divisors as follows.

$$\sum_{P \in C} m_P P + \sum_{P \in C} n_P P = \sum_{P \in C} (m_P + n_P) P$$

The subgroup of $Div(C)$ with divisors of degree 0 is $Div^0(C)$.

Definition 52 (GCD of divisors.). Let $D_1 = \sum_{P \in C} m_P P$ and $D_2 = \sum_{P \in C} n_P P$

Then the $gcd(D_1, D_2)$ is defined by

$$gcd\left(\sum_{P\in C} m_P P, \sum_{P\in C} n_P P\right) = \sum_{P\in C} min(m_P, n_P)P$$

Definition 53 (Principal Divisor). Let $R = G/H \in K(C)$ and $G, H \in K[C]$. The divisor of a rational function R is called a principal divisor and defined as:

$$div(R) = \sum_{P\in C} ord_P(R)PP$$

By definition 48 we know that $div(R) = div(G) - div(H)$. We can see that $div(R) \in D^0$.

Definition 54 (Principal Divisor Group). The principal divisor group is defined by:

$$\mathbf{P} = \{Div(R) \mid R \in K(C)\}$$

We have,

$$\mathbf{P} \subset Div^0(C) \subset Div(C).$$

Definition 55 (Jacobian). The Jacobian of the curve C is defined by the quotient group:

$$J = J(C) = Div^0(C)/\mathbf{P}$$

Let $D_1, D_2 \in Div(C)$. We have the following equivalence relation on $Div(C)$:

$$D_1 \sim D_2 \Leftrightarrow D_1 - D_2 \in \mathbf{P}$$

Or equivalently:

$$D1 \sim D2 \Rightarrow \exists R \in K(C) : D1 = D2 + div(R)$$

2.4 Genus of a Curve

Before going directly to the genus of a curve, we should see a well celebrated problem. In fact, the solution to this problem gives the definition of genus.

For any divisor D, the set

$$L[D] = \{f \in K(C) \mid (f) + D \geq 0\} \cup 0$$

Where (f) is the principal divisor formed by f. $L(D)$ is the space of all rational functions with poles no worse than D^+ (points having positive order) and zeros of multiplicity atleast as specified by D^-.

$L(D)$ is a vector space over K The dimension of $L(D)$ is defined to be $\ell(D)$. The problem of finding the dimension of the vector space is the Riemann-Roch problem.

Theorem 56 (Riemann's Theorem.). There is a constant g such that $\ell(D) \geq deg(D) + 1 - g$ for all divisors D. The smallest such g is called the genus of C. g is always a non-negative integer.

The theorem stands as a definition for genus of a curve.

Chapter 3

Hyperelliptic Curves

Do not worry about your difficulties in Mathematics.

I can assure you mine are still greater.

– Albert Einstein (1879 - 1955)

3.1 Basics of Hyperelliptic Curves

Hyperelliptic curves are a class of algebraic curves. They can be seen as generalisations of elliptic curves. We classify them depending on the genus of the curve. For all genus, $g \geq one$ we have hyperelliptic curves. A detailed, simple and beautiful tutorial on Hyperelliptic Curves is available in [16].

Definition 57 (Hyperelliptic Curves). Let k be a field and K be the algebraic closure of k. A hyperelliptic curve C of genus g over k is defined by an equation of the form.

$$C : y^2 + h(x)y = f(x) \text{ in } k[x, y] \tag{3.1}$$

Where $h(x) \in k[x]$ is a polynomial of degree atmost g and $f(x)$ is a monic polynomial of degree $2g+1$ and there are no solutions $(x, y) \in K^2$ which simultaneously satisfy $y^2+h(x)y = f(x)$ and the partial derivatives $2y+h(x) = 0$ and $h'(x)ya-f'(x) = 0$. A singular point on C is a solution $(x, y) \in K^2$ which simultaneously satisfies all these conditions.

So, in other words, a hyperelliptic curve does not have any singular points.

Definition 58 (Rational points, Points at infinity, finite points). Let L be an extension field of k. The set of $L - rational$ points on C are denoted $C(L)$ is the set of points $P = (x, y) \in L \times L$ which satisfy the equation 3.1 of curve C together with a special point *at infinity* [1] denoted by ∞. The set of point $C(K)$ is simply denoted by C. The points in C other than ∞ are finite points.

Definition 59 (Opposite, special and ordinary points). Let $P = (x, y)$ be a finite point on C. The opposite point of P is the point $\widetilde{P} = (x, -y-h(x))$ (Note that $\widetilde{P}$ is indeed on C.). We also define the opposite of ∞ by $\widetilde{\infty} = \infty$ itself. If a finite point P satisfies $\widetilde{P} = P$, then it is called a special point. Otherwise P is an ordinary point.

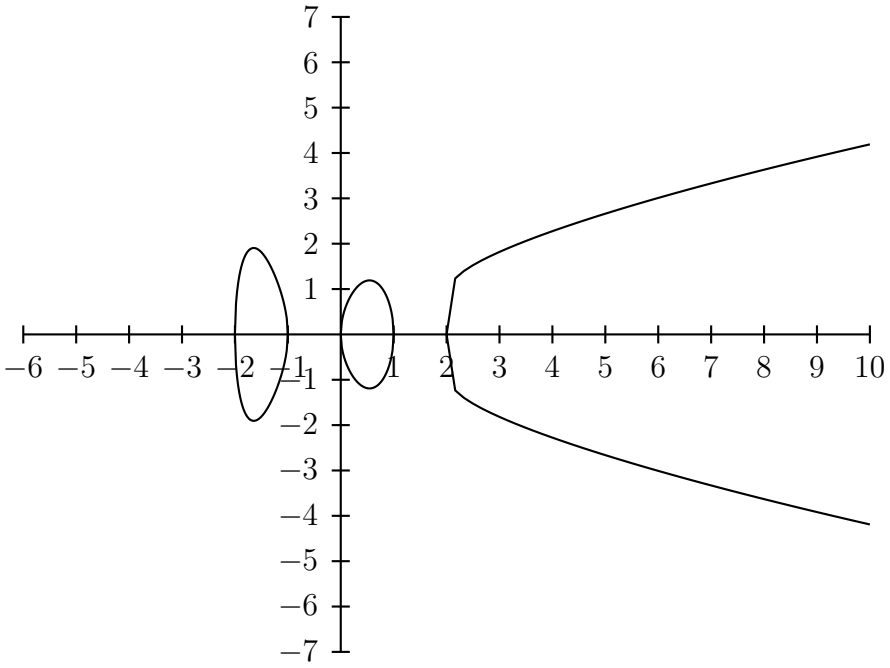
3.1.1 Examples

1. The figure shows a hyperelliptic curve over the R.

[1] point at infinity is in the projective plane $P^2(K)$.It is the only projective point lying on the line at ∞ that satisfies the homogenised hyperelliptic curves equation. If $g \geq two$ then ∞ is a singular point but allowed since $\infty \notin K \times K$

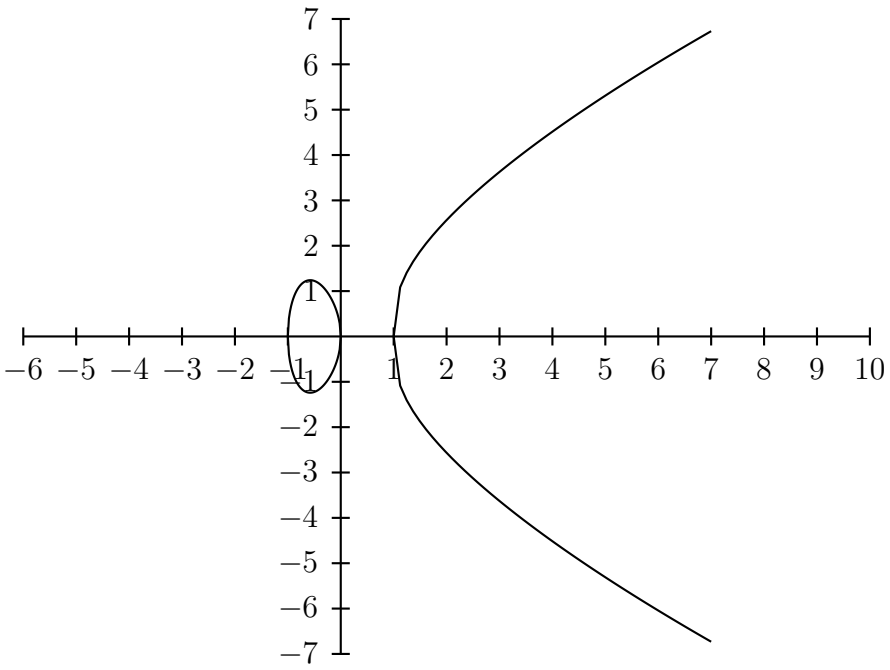
$$y^2 = (x-2)(x-1)x(x+1)(x+2)$$

In this example the genus of the curve is 2.



2. The following figure shows a hyperelliptic curve of genus 1. In other words, this is an elliptic curve.

$$y^2 = (x-1)x(x+1)$$



3. The hyperelliptic curve given by the equation:

$$y^2 + xy = x^5 + 2x^4 + x^3 - 5x^2 + 10$$

(a) When the curve is defined over the finite field $\mathbb{Z}_{11}$, the valid points are:

$$(1,4), (1,6), (4,2), (4,5), (5,7), (5,10), (8,0)^*, (8,3), (9,5), (9,8)$$

The point which is starred is a special point.

(b) When the curve is defined over the finite field $\mathbb{Z}_7$, the valid points are:

$$(1,1), (1,5), (2,6), (3,5), (3,6), (4,4), (4,6), (5,3), (5,6), (6,4)$$

Here we can see that there are no special points.

Definition 60 (Coordinate ring and polynomial functions.). The definitions are same as the earlier ones.

Coordinate ring of C over k.

$$k[C] = k[x, y]/(y^2 + h(x)y - f(x))$$

Coordinate ring of C over K.

$$K[C] = K[x, y]/(y^2 + h(x)y - f(x))$$

Elements of $K[C]$ are called polynomial functions.

Definition 61 (Function field and rational functions). The function field $k(C)$ of C over k is the field of fractions of $k[C]$. Similarly, $K(C)$ the function field of C over k is the field of fractions of $K[C]$.

$$K(C) = \left\{ \frac{G}{H} \mid G, H \in K[C], deg(G) = deg(H) \right\}^{2}$$

An element of $K[C]$ is called a rational function.

3.2 Divisors

In the last chapter we have given all the definitions and primary details of divisors of an algebraic curve. Those are applicable for a divisor of hyperelliptic curves also.

But here I can provide you with a simple but good example.

Example 62. Let $P = (x_1, y_1)$ be a point on C. Then,

[2] the condition for degree is necessary iff G, H are from the homogeneous coordinate ring [4]

$$div(x - x_1) = \begin{cases} P + \widetilde{P} - 2\infty & \text{P is ordinary ,} \\ 2P + -2\infty & \text{P is special .} \end{cases}$$

$(x - x_1)$ is the line which is parallel to y axis and passes through the point $(x, 0)$. The y value of C for the value x_1 is y_1. The line passes through this point of the curve C. If the point P is an ordinary point, then there are two y values for the same x. These points correspond to P and $\widetilde{P}$.

Or

If P is a special point, its opposite also is the same point P and the line passes through it. So is the divisor.

3.2.1 Semi-Reduced Divisors

A semi-reduced divisor is a divisor of the form:

$$D = \sum_i m_i P_i - \left(\sum_i m_i \right) \infty$$

Where each $m_i \geq 0$ and all the P_i's are finite points such that if $P \in supp(D)$, then $\widetilde{P} \notin supp(D)$ unless P is special in which case $m_i = 1$.

Fact 63. For each divisor $D \in D^0$ there exists a semi-reduced divisor $D_1 (D_1 \in D^0)$ such that $D \sim D_1$.

3.2.2 Reduced Divisors

Definition 64 (Reduced Divisor). Let $D = \sum_i m_i P_i - (\sum_i m_i) \infty$ be a semi-reduced divisor. We call D to be a reduced divisor, if it satisfies the following property.

$$\sum m_i \leq g$$

Fact 65. For every divisor $D \in D^0$, there exists a unique reduced divisor D_1 such that $D \sim D_1$.

3.3 Jacobian of a Curve

In the last chapter we saw the definition of jacobian of a curve, here let us look into a little more details. We have defined $D^0 = \{\text{set of all divisors of degree } 0\}$. The set of divisors of rational functions form the principal divisors, $\mathbf{P \subset D^0}$. And the jacobian, J is the quotient group D^0/P. If $D_1, D_2 \in D^0$, $D_1 \sim D_2$ if $D_1 - D_2 \in P$. That is, $D_1 = D_2 + (f)$ for some $f \in K(C)$. By definition itself J is a group.

3.3.1 Group operation in Jacobian

What is the group operation in the jacobian? Ordinary addition itself is the group addition. The operation of divisor addition satisfies all the group axioms. But for the sake of a formal way we can say that it is the addition of two reduced divisors.

We know, J is a group of equivalence classes from the facts 63 and 65. we know that every divisor $\in J$ has an equivalent reduced divisor. In every class of J, there will be a unique reduced divisor. So, addition in the jacobian is the addition of two classes. We can represent the classes by the unique reduced divisor present in each class [3]. So, adding two classes boils down to adding two reduced divisors. Once we add two reduced divisors, we get either a reduced divisor or a semi-reduced divisor.

[3] this is similar to representing $\mathbb{Z}_p$ by the smallest positive numbers which can represent the class

If it is a reduced divisor it represents the resulting class. Or if it is a semi-reduced divisor, we can have the reduced divisor equivalent to the semi-reduced divisor to represent the resulting class.

Let $[D_1]$ and $[D_2]$ are the two classes to be added. And the result be $[D_3]$.

$$[D_1] + [D_2] = [D_3]$$

This is done by:

$$D_{1r} \oplus D_{2r} = D_{3r}$$

Where D_{1r} represents $[D_1]$, D_{2r} represents $[D_2]$ and D_{3r} represents $[D_3]$ and all D_{ir} are reduced divisors. And $\oplus$ stands for the addition of the divisors and then the reduction.

How do we do this in practice? For the addition in the jacobian, we have many algorithms available. They use different types of representations of the divisors. Before looking into the details of the algorithms, let us have a look to the different representations of divisors.

Definition 66 (k-rational Divisor). Let $P(x, y)$ be a point on C and σ be an automorphism of K over k. Then $P^\sigma = (x^sigma, y^sigma)$ also is a point on C.

A divisor $D = \sum m_P P$ is a k-rational divisor if $D^\sigma = \sum m_P P$ is equal to D for all automorphisms σ of K over k.

A divisor is k-rational does not mean that all the points are k-rational.

3.4 Representations of Divisors

3.4.1 Point Representation or Explicit Representation

This is the simplest form of representation. This is the representation which directly follows from the definition of the divisor word by word. Here, we represent the divisors just as the formal sum of points along with the order of points. If $P = (x_i, y_i)$ are the points in the support of the divisor and m_i's are the order of point P_i's respectively:

$$D = \sum_i m_i P_i$$

For computational purposes this form of representation is not advisable. One drawback of this form is that the values of x_i's and y_i's are in K which is the closure of the field k on which we have defined our curve.

3.4.2 Mumford Representation

This is the representation which is mostly used for the computing purposes. Once we state how is the representation, we will come to the advantages of this representation.

If we have a semi-reduced divisor, it can be represented by two polynomials. Let us see how is it.

let $D = \sum_i m_i P_i - (\sum m_i)\infty$

The two polynomial are:

1. $U(x) = \Pi(x - x_i)^{m_i}$: This is a monic polynomial of degree $\sum m_i$.

   In fact, this is a polynomial which has root having the same x-coordinate of the points in the support of the divisor. The multiplicities of the roots also is the same as the order of the corresponding point.

2. Here we have two cases.

   (a) If all the points P_i's are distinct.

$$V(x) = \sum_i y_i \left(\frac{\Pi_{j \neq i} (x - x_i)}{\Pi_{j \neq i} (x_i - x_j)} \right)$$

   $V(x)$ is the unique polynomial of maximum degree one less than degree of U. i.e, $deg(V) \leq deg(U) - 1$. Also, that $V(x_i) = y_i$ for all x_i.

   (b) If all the points are not distinct.

   We have to find out a V which satisfies the following condition along with the condition $V(x_i) = y_i$.

$$V(x) = \left[\begin{array}{c} \text{The unique polynomial of degree less than} \\ \sum_i m_i - 1 \text{ such that if multiplicity of } P_i = m_i \\ \left(\frac{d}{dx}\right)^j \left[V(x)^2 + V(x)h(x) - f(x)\right]_{x=x_i} = 0 \\ \text{for } 0 \leq j \leq m_i - 1 \end{array} \right]$$

   In other words, $V(x)$ is the unique polynomial such that:

$$(x - x_i)^{m_i} \mid (V(x)^2 + V(x)h(x) - f(x))$$

This, what we told above is given by the following theorem [16, 17].

Theorem 67. Let $D = \sum_i m_i P_i - (\sum m_i)\infty$ be a semi-reduced divisor. Where $P = (x_i, y_i)$ are the points and m_i are the order of the points respectively.

Let $a(x) = \Pi(x - x_i)^{m_i}$ and $b(x)$ be a unique polynomial which satisfies:

1. $deg(b(x)) \leq deg(a(x))$

2. $b(x_i) = y_i$ for all i for which $m_i \neq 0$

3. $a(x)$ divides $(b(x)^2 + b(x)h(x) - f(x))$

Then $D = gcd(div(a(x)), div(b(x) - y))$.

For proof of the theorem [16] and for more details of mumford representation refer [17].

Now we can see whether these polynomials $a(x)$ and $b(x)$ are constructible. $a(x)$ is easy. For $b(x)$:

1. $P = (x_i, y_i)$ is ordinary.

   Let $b(x) = \sum_i c_i(x - x_i)^{m_i}$ be the polynomial we need. It is easy to see that $b(x)$ satisfies the conditions. We have to find out the constants c_i's. From $b_i(x_i) = y_i$ we get c_0. Then $(b_i(x)^2 + b_i(x)h(x) - f(x)) = 0$ for $x = x_i$ and for all the $m_i - 1$ derivatives. This gives us enough equations to find out the constants.

2. $P = (x_i, y_i)$ is special. $(m_i = 1)$ Here we can directly see that $b_i(x_i) = y_i$ satisfies all the conditions.

Now, using Chinese Remainder Theorem [9] for polynomials, we can find a unique polynomial $b(x_i) \in k[x]$ which can represent the divisor along with $a(x)$.

$$b(x) \equiv b_i(x)(mod(x - x_i)^{m_i}) \text{ for all } i$$

The polynomials $a(x)$ and $b(x)$ together will represent the divisor.

The main advantage of this representation is that we can have the representation in $k[x]$. We need not bother about the closure of k. All the calculations also can be done in $k[x]$. This we will see later.

3.4.3 Chow Representation

Definition 68 (u-resultants). Let $F, G, H \in k[x, y, z]$ be three homogeneous polynomials of degrees f, g and h respectively with indeterminate coefficients. Their multi-variate resultant is a fixed polynomial (denoted $res(F, G, H)$) of degree fgh in the coefficients such that under any specialization σ of these coefficients, ${}^{\sigma}res(F, G, H)$ vanishes identically if and only if ${}^{\sigma}F$, ${}^{\sigma}G$ and ${}^{\sigma}H$ have common projective zeros.

Now, Let us replace H by $L(\bar{u})$ where $L(\bar{u})$ denotes the linear form $u_x x + u_y y * u_z z$ where u_x, u_y, u_z are new indeterminates. The u-resultant of F and G is $u - res(F, G)$ defined to be $res(F, G, L)$ which is a polynomial of degree fg in the indeterminate $(\bar{u})$.

$U - res(F, G)$ vanishes identically if and only if F and G have infinitely many common projective zeros.

If F and G have only a finite number of common zeros $P_1, \ldots, P_m$, then:

$$u - res(F, G) = R(u_x, u_y, u_z) = \Pi(x_i u_x + y_i u_y + z_i u_z)^{n_i}$$

Where $P = (x_i, y_i, z_i)$ and n_i is the intersection multiplicity at P_i. For more details of construction of $u - res$, refer [1, 2].

Now let us consider F to be C and G to be the divisor polynomial. We have all the P_i's and n_i's.

Definition 69 (Chow / Associated form). Let $D = \sum_i m_i P_i$ be an intersection cycle on C. Then the chow form or the associated form of D is the polynomial $R \in K[x, y, z]$ where

$$R((\bar{u})) = \Pi(x_i u_x + y_i u_y + z_i u_z)^{m_i}$$

Chow forms have a very important property which makes them attractive. The property is:

Fact 70. An intersection cycle D is $k - rational$ if and only if its chow form is $k - rational$. i.e, when $R \in k[(\bar{u})]$.

This is important because, for our purposes, we need only $k - rational$ divisors. So, we can again do all the computations in the base field itself rather than in K.

Chapter 4

Addition

"This principle is so perfectly general that no particular application of it is possible."

– George Polyá

We have come across all the pre-requisites for addition of divisors. In this chapter we will see how addition is done. There are different methods for addition. We will see them one by one.

4.1 Geometrically what is it?

We are concerned about the addition of reduced divisors of a genus g hyperelliptic curve. Consider that we have two reduced divisors, D_1 and D_2.

$$D_1 = \sum_i m_i P_i - \left(\sum_i m_i\right)\infty \quad \text{and} \quad D_2 = \sum_i m_i Q_i - \left(\sum_i m_i\right)\infty$$

where the P_i and Q_i are points on C.

The idea is to find out a curve which passes through the points P_i and Q_i with corresponding intersection multiplicities so that the intersection cycle of the curve will give $D_1 + D_2$. Let us draw that curve. We can see that this new curve will intersect with a few more points of C. Now we have to draw a new curve which passes through the opposites of the new intersections with the same multiplicities of their opposites [1]. This new intersection cycle is the resulting reduced divisor which is the desired sum $D_1 + D_2$

For ease of explanation, we will consider curve of genus 2. So we have:

$$D_1 = P_1 + P_2 - 2\infty \quad \text{and} D_2 = Q_1 + Q_2 - 2\infty$$

From geometry, we know that these points determine a unique cubic polynomial $b(x)$ which passes through them with respective multiplicities (in this case all multiplicities are 1). Substituting $b(x)$ for y in the equation of the hyperelliptic curve, we get:

$$b(x)^2 + b(x)h(x) = f(x) \tag{4.1}$$

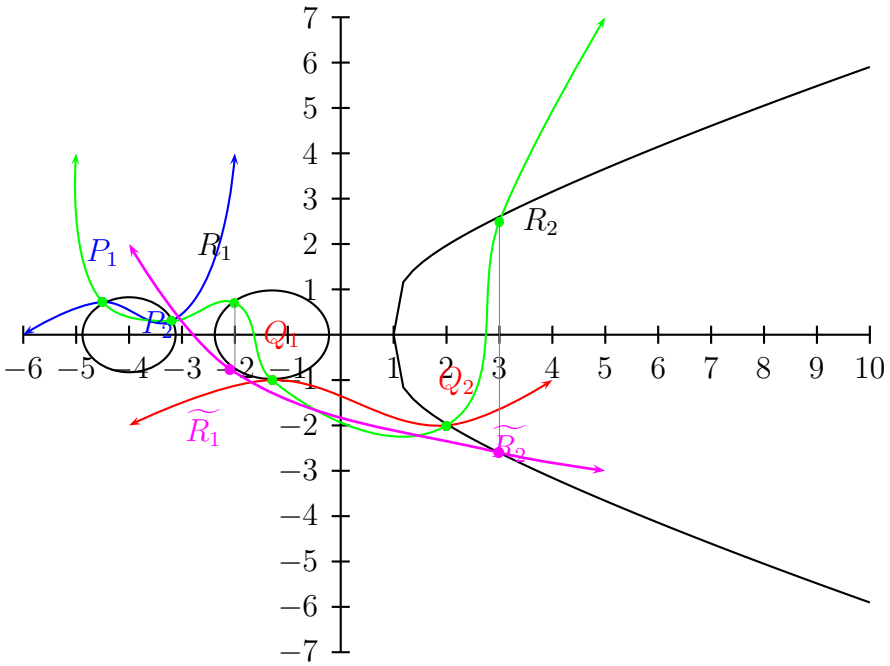
Solving the equation gives us 6 solutions (points on the curve) of which 4 of them are known to us. Let the new points to be R_1 and R_2. Then the new divisor $D_3 = \widetilde{R_1} + \widetilde{R_2} - 2\infty$ is the sum of D_1 and D_2.

4.1.1 Example

Here is the graph of the example mentioned above.

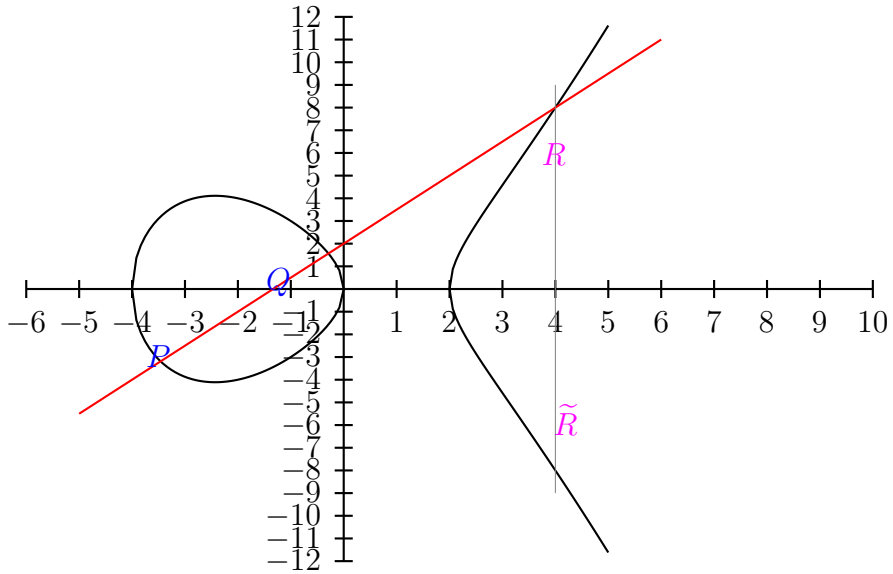
[1] The reason for this is to have an identity element [19]

Example 71. Blue and red lines are divisors D_1 and D_2 respectively. The new polynomial $b(x)$ is represented by the green curve. It intersects the hyperelliptic curve at points at six points including P_1 and P_2 of D_1, Q_1 and Q_2 of D_2 and the new points R_1 and R_2. Then we can calculate the opposites of these new points and get $\widetilde{R_1}$ and $\widetilde{R_2}$ respectively. The new curve (magenta) is the resultant divisor.



Example 72. We will see a more concrete example. Let us take a hyperelliptic curve of $g = 1$ which is an elliptic curve. How is the addition done in that case. As the genus is one, the reduced divisor is nothing but a single point P and also the multiplicity cannot exceed one. So our D_1 and D_2 are nothing but two points P and Q.

$$y^2 = (x-2)x(x+4)$$



We have the elliptic curve with points P and Q to be added together. We find out a line(curve) passing through them. This new line passes through the point R. Now we take the reflection of R on x-axis. The reflection $\widetilde{R}$ is the sum of P and Q.

4.2 Algebraic methods

In the last section we got a feel of how to add divisors. In the case of elliptic curves it was very easy. But in the general case, drawing a curve is not an easy thing. What we can do is that algebraically find out the equation of the curves/divisors. This is not very difficult. In fact, we can use the representations we saw in the last section. The one which is most popular is mumford representation. The polynomials $a(x)$ and $b(x)$ contains all about the divisors. Also there is a method which uses chow forms.

4.2.1 Cantor's Algorithm

In 1987 Cantor [3] came up with an algorithm for the addition of reduced divisors of hyperelliptic curves. The algorithm is known as Cantor's algorithm. As we have two

phases for addition of divisors, the algorithm also has two phases. Cantor's method uses mumford representation.

1. Composition : This is the phase in which we find out the new divisor which is the sum of the input divisors.

2. Reduction : In this phase we take prune out the parts which are not needed and take the inverse of the resulting one to get the result.

Composition

- **Input**: Reduced divisors $D_1 = div(a_1, b_1)$ and $D_2 = div(a_2, b_2)$ both defined over k.

- **Output**: A semi-reduced divisor $D = div(a, b)$ defined over k such that $D \sim D_1 + D_2$.

1. Use the extended Euclidean algorithm to find polynomials $d_1, e_1, e_2 \in k[u]$ where

$$d_1 = gcd(a_1, a_2) \text{ and } d_1 = e_1 a_1 + e_2 a_2$$

2. Use the extended Euclidean algorithm to find polynomials $d, c_1, c_2 \in K[u]$ where

$$d = gcd(d_1;\ b_1 + b_2 + h) \text{ and } d = c_1 d_1 + c_2(b_1 + b_2 + h)$$

3. Let $s_1 = c_1 e_1, s_2 = c_1 e_2$ and $s_3 = c_2$, so that

$$d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h) \tag{4.2}$$

4. Set

$$a = a_1 a_2 = d_2 \tag{4.3}$$

$$b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \bmod a \tag{4.4}$$

Again, I am not providing the proof. In fact, the proof given by Cantor contained a few errors and later when Koblitz gave the algorithm, he did not give any proof. But for the proof, readers can refer [12, 3, 16].

Reduction

Reduction part is comparatively simpler and easy to understand. Here also we skip the proof - for details [12, 3, 16]. But here, the algorithm is pretty clear that no one needs a proof to see that it is indeed correct.

Input: A semi-reduced divisor $D = div(a, b)$ defined over k.

Output: The (unique) reduced divisor $D' = div(a', b')$ such that $D' \sim D$.

1. Set

$$a' = (f - bh - b^2)/a \tag{4.5}$$

$$b' = (-h - b) \bmod a' \tag{4.6}$$

2. If $deg_x(a') \geq g$ then set $a \leftarrow a'$, $b \leftarrow b'$ and go to step 1.

3. Let c be the leading coefficient of a', and set $a' \leftarrow c^{-1}a'$

4. Output(a', b').

4.2.2 Other versions

As we told in the introduction, we are looking for faster addition in the jacobian of hyperelliptic curve. The method given above is a polynomial time algorithm. But when it comes to the number of micro-instructions needed in a processor, this version of the algorithm is too general to implement. So we have many different refined version of this algorithm or slight variants of this algorithm which is tailor made for different genus hyperelliptic curves.

Harley's Algorithm

In the year 2000, Rob Harley [6] came up with an algorithm which is very similar to the original Cantor's algorithm. The algorithm was optimised and made for genus two curves [5]. In the tailor made method for genus two curves, addition and doubling are handled separately. Finally the number of operations comes upto two inversions, three squarings and 24 multiplications for the genus 2 case.

Explicit formulae by Tanja Lange

In a recent paper published 2002, by Tanja Lange [14] she gives an explicit formulae for arithmetic on genus two curves over fields of even characteristic and for arbitrary curves. The formula is faster that all the methods which existed before that. It allows to obtain fast arithmetic on hyperelliptic curves of genus 2. The algorithm is a case by case analysis of different situation which can arise.

The method followed by Lange has inspired my team to investigate the things in a

similar way. The number of operations needed for the most difficult case come to be one inversion, three squarings and 22 multiplications for genus 2 hyperelliptic curves in her method.

Chapter 5

Point addition

Just because something doesn't do what you planned it to do doesn't mean it's useless.

– Thomas Alva Edison

In this chapter I shall explain the method developed by my team. This uses the explicit representation of divisors. The main advantage of the method is that the composition part is very efficient. The drawback is that the reduction part relies on a probabilistic algorithm rather than a deterministic one which is preferred.

5.1 Composition

As in Cantor's algorithm, we have two phases - composition and reduction. First we go for composition.

Input: Two reduced divisors D_1 and D_2 in standard form. (standard form is the $D = \sum_{P \in C} n_p P$ form of the divisor in explicit representation, the terms in the sum

are sorted in non-decreasing order of their x coordinate) Let them be:

$$D_1 = \alpha_1 P_1 + \alpha_2 P_2 + \cdots + \alpha_m P_m - (*)\infty$$

and

$$D_2 = \beta_1 Q_1 + \beta_2 Q_2 + \cdots + \beta_n Q_n - (*)\infty$$

As they are reduced divisors, $\sum_i \alpha_i$ and $\sum_j \beta_j$ are less than g.

Output: A semi-reduced divisor

$$D = \gamma_1 T_1 + \gamma_2 T_2 + \cdots + \gamma_s T_s - (*)\infty$$

Method: Our method is just like merging the divisors together. While merging them, we look for the conditions to decide the value of γ_i.

$i := j := k := 1$

while $k \leq m + n$

  if $i > m$

    $\gamma_k := \beta_j;\ T_k := Q_j;\ j := j + 1;$

  fi

  if $j > n$

    $\gamma_k := \alpha_i;\ T_k := P_i;\ i := i + 1;$

  fi

  if $P_i(x) < Q_j(x)$

$\gamma_k := \alpha_i;\ T_k := P_i;\ i := i + 1;$

fi

if $P_i(x) > Q_j(x)$

$\gamma_k := \beta_j;\ T_k := Q_j;\ j := j + 1;$

fi

if $P_i(x) = Q_j(x)$

if $(P_i(y) + Q_j(y) + h(x)) = 0$

if $P_i(y) = Q_j(y)$

$k := k - 1;$

else

$\gamma_k := \|\alpha_i - \beta_j\|$

if $\alpha_i > \beta_j$

$T_k := P_i;$

else

$T_k := Q_j;$

fi

if $\gamma_k = 0$

$k := k - 1;$

fi

fi

else if $P_i(y) = Q_j(y)$

$\gamma_k := \alpha_i + \beta_j;\ T_k := P_i;$

fi

fi

$i := i + 1;\ j := j + 1;$

fi

$k := k + 1;$

5.1.1 Details of the composition algorithm

We will go through all the conditions.

1. **while** $k \leq m + n$

   We have to go through all the points of both the divisors.

2. **if** $i > m$

   This **if** condition will be satisfied iff all the points from D_1 is already added to the result. So, we have to add the points Q_j from D_2 to the result. And, we can do it unconditionally.

   The same argument is valid for **if** $j > n$ with D_1 and D_2 interchanged their roles.

3. **if** $P_i(x) < Q_j(x)$

   This **if** is true when the x coordinate of P_i is smaller than that of Q_j or we can say that the x coordinates are not the same. Two points with different xs do not have any effect on each other. So, we add the one which is having the lesser value for x coordinate.

   the same explanation stands for **if** $P_i(x) > Q_j(x)$

4. $P_i(x) = Q_j(x)$

   Both the x coordinates are the same. Here arise two cases.

(a) $P_i(y) + Q_j(y) + h(x) = 0$

This condition is satisfied when $P_i + Q_j = O$ i.e, $P_i = \widetilde{Q_j}$ This can happen when P_i is an ordinary point or a special point.

i. P_i is a special point.

From the condition, it is clear that $P_i = \widetilde{Q_j}$ and being a special point $\widetilde{P_i}$ is P_i itself. i.e, $P_i = Q_j = \widetilde{P_i} = \widetilde{Q_j}$. And from the definition we know that, the coefficients α_i and β_j are 1. If we have special points in a semi-reduced divisor, its coefficient will be either 0 or 1. Here, it cannot be 1. So, the algorithm skips the points.

ii. P_i is an ordinary point.

So is Q_j also. Here, both the points are opposites of each other. We have to take the the point which dominates. i.e, points will cancel out each other (since they are opposites of each other) and the one with larger coefficient will remain with a multiplicity of $abs(\alpha_i - \beta_j)$.

If α_i is larger than β_j, P_i will be there in the result. If α_i is smaller than β_j, Q_j will be there in the result. Otherwise, both of them will not be there in the result.

(b) $P_i(y) + Q_j(y) + h(x) \neq 0$ and $P_i(y) = Q_j(y)$

This means that $P_i \neq \widetilde{Q_j}$. Both have same x and y. So, $P_i = Q_j$ and is ordinary point. We have just to add their multiplicities together. i.e, $\gamma_k = \alpha_i + \beta_j$.

5. Increments and decrements.

We ought to adjust the indices i, j, k according to our decision to include or exclude the points.

5.1.2 Proof and equivalence to Cantor's composition

The proof that the algorithm is correct is there in the detailed construction of the algorithm. And it is clear that the result is a semi-reduced divisor.

For seeing the equivalence to Cantor's algorithm, we have to see different cases.

1. P is an ordinary point.

   (a) $P \in D_1$ and $P \in D_2$

   And with multiplicities α_i and β_j each. From Cantor's method we can see that in the result, the multiplicity of P is $\alpha_i + \beta_j$.

   In our method also the result is the same.

   (b) $P \in D_1$ and $\widetilde{P} \in D_2$

   And with multiplicities α_i and β_j each. From Cantor's method we can see that in the result, the point with larger multiplicity remains with the resultant order being the difference of α_i and β_j.

   The geometric version also gives the same result.

   (c) $P \in D_1$ and $P \notin D_2$ and $\widetilde{P} \notin D_2$.

   In this case the d calculated in Cantor's method cannot remove the point from the result and the result will contain P with the same multiplicity it has in D_1.

   Geometric version also gives the same result.

2. P is a special point.

   In this case, the coefficient of P will be always 1.

(a) $P \in D_1$ and $P \in D_2$

In Cantor's method, both have common point P with same multiplicity. Hence in the division step, the points will be removed from the result. Hence P will not be a part of the result.

The same happens with the geometric version.

(b) $P \in D_1$ and $P \notin D_2$ (W.L.G)

This is the same as case b when P is an ordinary point. The result is same as that of Cantor's algorithm.

Hence the divisor given by the merging method is **equivalent** to the divisor which is represented by the polynomials (a, b) of Cantor's algorithm which uses mumford representation.

5.2 Towards Mumford Representation

From the composition part it is clear that not in all cases we have to go through the reduction part. The composition part is the same for any special cases and general cases. But, here in the reduction part, we have taken the special case of g to be two. So, hyperelliptic curves of genus two are the only consideration in our reduction part.

5.2.1 Basic Idea about Conversion

Definition 73 (Weight of a divisor). Weight of a divisor is defined to be the degree of the divisor. Denoted by $W(D)$.

Here in our case, the maximum degree is two. So is the weight. There can happen different combinations of input divisors for composition part.

1. $W(D_1)$ is one, $W(D_2)$ is one. We are sure that the result of composition part is a reduced divisor. We can avoid the reduction part.

2. $W(D_1)$ is one, $W(D_2)$ is two. (without loss of generality, this includes $W(D_1)$ is two and $W(D_2)$ is one)

   The result can be of weight varying from one to three. If $W(D)$ is one or two reduction not needed. But if $W(D)$ is three, we have sub-cases.

   (a) $D = P_1 + P_2 + P_3$ all P's distinct

   (b) $D = 2P_1 + P_2$ two points with one having order two.

   (c) $D = 3P_1$ only a single point with order three.

3. $W(D_1)$ is two, $W(D_2)$ is two.

   In this case, the result can be of weight varying from one to four. If $W(D)$ is one or two reduction not needed. But if $W(D) \geq 2$ is, we have sub-cases to be reduced. If the weight of result is three, the sub-cases are listed above. If the weight is four, we have the following sub-cases:

   (a) $D = P_1 + P_2 + P_3 + P_4$ all P's distinct

   (b) $D = 2P_1 + P_2 + P_3$ three points with one point of order two.

   (c) $D = 2P_1 + 2P_2$ two points with order two each.

   (d) $D = 3P_1 + P_2$ three points with one point of order three.

   (e) $D = 4P_1$ a single point with order four.

In all the cases we have to use reduction, we have to find out new points which will be the reduced divisor. The approach we take is to convert the divisors into

mumford representation and then reduce them using Cantor's reduction phase and then find the new points. As a first step, we should find the mumford representation of the divisors.

5.2.2 Different cases in detail

All the cases which can arise are listed above. Now let's see how to handle them. In all of them, x-coordinates are known, hence finding the polynomial a is not difficult. In fact, $a(x) = (x - x_i)^{m_i}$. For finding the polynomial $b(x)$ there arise different cases.

1. $D = P_1 + P_2 + P_3$

   To find $b(x)$, we know the conditions. We have the y-coordinates also. We use the method given by Mumford [17] himself.

$$b(x) = \sum_{i=1}^{3} y_i \left(\frac{\Pi_{j \neq i} (x - x_i)}{\Pi_{j \neq i} (x_i - x_j)} \right)$$

$$\begin{aligned} b(x) &= y_1 \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)} \\ &\quad + y_2 \frac{(x - x_1)(x - x_3)}{(x2 - x_1)(x_2 - x_3)} \\ &\quad + y_3 \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)} \end{aligned}$$

2. $D = 2P_1 + P_2$

   Here in this case P_1 has an order of 2. We cannot use the method of Lagrange

to find out $b(x)$. The polynomial $b(x)$ is to be found using Chinese remainder theorem [9] from the polynomials which satisfy the condition at P_1 and P_2 each.

$$b_1(x) = c_2(x - x_1) + c_1$$

We can see that by applying the condition to the $b_1(x)$, all are satisfied. So, this is the polynomial for the point P_1. For P_2, the order is 1. Therefore,

$$b_2(x) = y_2$$

The values of c_1 and c_2 are unknown. The method to find out the values are explained in detail at the end of all the cases. The method is used by all the cases in general.

3. $D = 3P_1$

   In this case, there is only one point P_1 with order 3. From the previous case, it is easy to see that the polynomial is of the form:

$$b(x) = c_3(x - x_1)^2 + c_2(x - x_1) + c_1$$

   Again here also, the values of constants have to be computed. The general method is explained after all the cases.

4. $D = P_1 + P_2 + P_3 + P_4$

   All points are distinct. Lagrange's method can be employed.

$$b(x) = \sum_{i=1}^{4} y_i \left(\frac{\Pi_{j \neq i} (x - x_i)}{\Pi_{j \neq i} (x_i - x_j)} \right)$$

$$\begin{aligned} b(x) &= y_1 \frac{(x-x_2)(x-x_3)(x-x_4)}{(x_1-x_2)(x_1-x_3)(x_1-x_4)} \\ &+ y_2 \frac{(x-x_1)(x-x_3)(x-x_4)}{(x2-x_1)(x_2-x_3)(x_2-x_4} \\ &+ y_3 \frac{(x-x_1)(x-x_2)(x-x_4)}{(x_3-x_1)(x_3-x_2)(x_3-x_4)} \\ &+ y_4 \frac{(x-x_1)(x-x_2)(x-x_3)}{(x_4-x_1)(x_4-x_2)(x_4-x_3)} \end{aligned}$$

5. $D = 2P_1 + P_2 + P_3$

   It is evident from the previous cases that:

$$b_1(x) = c_2(x - x_1) + c_1$$

$$b_2(x) = y_2$$

$$b_3(x) = y_3$$

6. $D = 2P_1 + 2P_2$

   Using the same method as above:

$$b_1(x) = c_2(x - x_1) + c_1$$

$$b_2(x) = c_4(x - x_2) + c_3$$

7. $D = 3P_1 + P_2$

   Now it has very easy to see the polynomials we need without thinking much. Already computed ones are available.

$$b_1(x) = c_3(x - x_1)^2 + c_2(x - x_1) + c_1$$

   and

$$b_2(x) = y_2$$

8. $D = 4P_1$

   This case is the one which will take much of our computation. Here, $b(x)$ will be of the form:

$$b(x) = c_4(x - x_1)^3 + c_3(x - x_1)^2 + c_2(x - x_1) + c_1$$

   The values of c_1, c_2, c_3, c_4 are to be determined.

Now we can take the general case. For a point $P(x_k, y_k)$ having order n, the polynomial $b(x)$ will be of the form

$$b(x) = \sum_{i=1}^{n-1} c_i (x - x_k)^i$$

This should satisfy the conditions given by mumford representation. By default, it satisfies all the conditions except $((x-x_k)^n \mid (b^2+bh-f))$. By giving proper values for c_i's this condition must be satisfied. In the case of genus 2 curves, maximum value of n is 4. ie,

$$b(x) = c_4(x - x_1)^3 + c_3(x - x_1)^2 + c_2(x - x_1) + c_1$$

$$F : b^2 + bh - f$$

Replace $(x - x_1)$ by X_1.

$$\begin{aligned} F \quad : \quad & c_4^2 X_1^6 + c_3^2 X_1^4 + c_2^2 X_1^2 + c_1^2 \\ & + 2c_4c_3X_1^5 + 2c_4c_2X_1^4 + 2c_4c_1X_1^3 \\ & + 2c_3c_2X_1^3 + 2c_3c_1X_1^2 + 2c_2c_1X_1 - f \end{aligned} \tag{5.1}$$

$$\begin{aligned} F \quad : \quad & c_4^2 X_1^6 + 2c_4c_3X_1^5 + (c_3^2 + 2c_4c_2)X_1^4 \\ & + 2(c_4c_1 + c_3c_2)X_1^3 + (c_2 + 2c_3c_1)X_1^2 \\ & + 2c_2c_1X_1 + c_1^2 - f \end{aligned} \tag{5.2}$$

$$\begin{aligned}\frac{dF}{dx} = F' \quad : \quad & 6c_4^2X_1^5 + 10c_4c_3X_1^4 \\ & + 4(c_3^2 + 2c_4c_2)X_1^3 + 6(c_4c_1 + c_3c_2)X_1^2 \\ & + 2(c_2 + 2c_3c_1)X_1 + 2c_2c_1 - f' \end{aligned} \tag{5.3}$$

$$\begin{aligned}\frac{d^2F}{dx^2} = F'' \quad : \quad & 30c_4^2X_1^4 + 40c_4c_3X_1^3 \\ & + 12(c_3^2 + 2c_4c_2)X_1^2 + 12(c_4c_1 \\ & + c_3c_2)X_1 + 2c_2 + 4c_3c_1 - f'' \end{aligned} \tag{5.4}$$

$$\begin{aligned}\frac{d^3F}{dx^3} = F''' \quad : \quad & 120c_4^2X_1^3 + 120c_4c_3X_1^2 \\ & + 24(c_3^2 + 2c_4c_2)X_1 + 12(c_4c_1 \\ & + c_3c_2) - f''' \end{aligned} \tag{5.5}$$

By equating F, F', F'', F''' to zero and substituting $X_1 = 0$ (ie, put $x = x_1$), we get the values of constants as follows.

$$c_1 = y_1$$

$$c_2 = \frac{f'}{2c_1}$$

$$c_3 = \frac{f'' - 2c_2}{4c_1}$$

$$c_4 = \frac{f''' - 12c_3c_4}{12c_1}$$

From the equation of C we know that f is a function of x of degree $2g + 1$. In case genus $g = 2$, f is of degree 5. Let f be

$$f = f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x^1 + f_0$$

The polynomial $b(x)$ has to be calculated using Chinese remainder theorem. For that we can use the same method used by in [6] or [14]. The reduction algorithm is as follows:

5.3 Reduction

- **Input** : A semi-reduced divisor D in its explicit form. (output of composition phase)
- **Output** : A reduced divisor which is equivalent to the input.

1. Convert to mumford representation.
   (a) Depending on the weight of the divisor and the number of supports and their orders, find out which one of the above cases it falls to.
   (b) Find the polynomial $a(x)$ and $b(x)$ according to the calculations listed above.

2. Reduce

   (a) $a' = (b^2 + bh - f)/a$

   (b) $b' = (-b - h) \mod a'$

3. Convert back to explicit form.

   (a) Factorize a' : Uses probabilistic methods for root finding in finite fields.

   (b) Evaluate the value of b' at the values of x calculated in the last step.

4. Reproduce the new divisor in standard form.

5.4 Analysis

5.4.1 Composition

As we can see the while loop executes $m+n$ times, which is less than $2g$. We dont have any multiplications also except for the computation of $h(x)$. That we can calculate in g multiplications and g additions.

The operations in total are

Additions:

$g + g + 2g$ (for incrementing i, j, k)

g (in calculating $h(x)$)

2 ($Pi_y + Qj_y + h(x)$)

2 (like ai - bj and decrementing k)

ie, 5g + 4 additions.

Multiplications:

g^2 (for calculating $h(x)$)

Generally, additions are not considered to be expensive operations. Hence, the algorithm takes only g^2 multiplications. When the polynomial $h(x)$ is a constant polynomial, there will be no multiplications needed.

5.4.2 Reduction

Reduction is the subtle part of the whole algorithm. There are 3 different parts for the reduction phase.

1. Conversion to mumford representation.

   In this part we have explicit formulae for the polynomial $b(x)$. But the constants are to be calculated. In their calculation the derivatives of $f(x)$ has to be computed. This part of the algorithm is $O(g)$.

2. Reduction.

   Here, the explicit methods of Lange [14] can be employed. Hence we have the exact number of operations needed for different cases. They depend on the degree of $b(x)$. For details see section 4 of [14].

3. Root finding.

   This part employs a probabilistic algorithm to factorise the polynomial $a(x)$. The probabilistic algorithm is too expensive that it is of $O(n^4)$ where n is the size of the base field. Next step is to evaluate $b(x)$ at the new points. This computation will take maximum of four multiplications.

Details of finding roots in finite fields will be given in any Number Theory books. You can see the algorithm in section 2 of [13].

5.4.3 Pros and Cons

One of the advantage is that the composition algorithm is one of the simplest and needs very less computation. Unfortunately, the algorithm as a whole has more drawbacks than advantages. I shall give them as follows

1. Reduction is very expensive.

   The reduction step which is of $O(n^4)$ where n is the size of the base field, is very expensive. Also that it is probabilistic which takes more time to compute.

2. Operations are not in k.

   The operations cannot be done in k. As the values of coordinates are in a quadratic extension of k. The size of operands are of double the size of the base field. This reduces the speed of the algorithm by a great extent.

Chapter 6

Addition using Chow Forms

"The art of doing mathematics consists in finding that special case which contains all the germs of generality."

– David Hilbert

How to represent a divisor in chow form is given in section 3.4.3. This chapter gives the algorithm for divisor addition which adds two divisors given in their chow form. In the chapter, the curve under consideration is of genus two. First part of the chapter gives a sketch of composition algorithm. Later, the chapter takes the reader to more specific details of the algorithm for genus two hyperelliptic curves and gives a sketch of how the reduction to be done.

6.1 Composition

As the inputs for the algorithm are reduced divisors, they are of maximum weight two. And from section 3.4.3, the chow representation of a divisor $D = \sum_i m_i P_i$ is:

$$R = \Pi(x_i u_x + y_i u_y + z_i u_z)^{m_i}$$

There for R will be a multi-variate polynomial of maximum degree two (genus 2). A divisor can be of degree one or of degree two. A divisor of degree one is as follows:

$$R = (x_i u_x + y_i u_y + u_z)$$

and a divisor of degree two is as follows.

$$R_1 = x_1 x_2 u_x^2 + y_1 y_2 u^2 + u_z^2 + (x_1 y_2 + x_2 y_1) u_x u_y + (x_1 + x_2) u_x u_z + (y_1 + y_2) u_y u_z$$

Definition 74 (Opposite/Inverse of a divisor). If R is a divisor given in its chow form, we can define the opposite of R to be $\widetilde{R}$ as follows:

$$\widetilde{R} = \begin{cases} R \text{ with coefficient of } u_y \text{ term negated} & \text{if } degree(R) = 1 \\ R \text{ with coefficient of } u_y u_z \text{ term negated} & \text{if } degree(R) = 2 \end{cases}$$

In all the practical cases, the value of z is 1.

The basic idea of the composition is given in the next subsection. Subsection after that gives the complete algorithm.

6.1.1 Basic Idea

As in the case of reduction in point addition, here many different cases arise. These different cases which may arise are listed below.

1. No common points. $gcd(R_1, R_2) = 1$.

The divisors R_1 and R_2 have no common points. This can be checked by calculating the *gcd*. Three sub-cases arise:

(a) R_1 and R_2 have one pair of opposite points.

This can be found out by calculating $gcd(R_1, \widetilde{R_2})$. If $gcd(R_1, \widetilde{R_2}) = R_3$ of degree one, then result, R is:

$$R = \frac{R_1 R_2}{R_3 \widetilde{R_3}}$$

(b) Both the pairs are opposites.

Here $gcd(R_1, \widetilde{R_2})$ will be of degree two. Then the result must be zero divisor. i.e, 1

(c) No opposite pairs.

By seeing $gcd(R_1, \widetilde{R_2})$ is 1, we can understand that we are in this sub-case. The result is $R = R_1 R_2$.

2. One common point. $gcd(R_1, R_2) = R_3$ of degree one.

Here also sub-cases arise:

(a) Common point is special. $R_3 = \widetilde{R_3}$.

i. The other points are separate.

If $gcd(R_1, \widetilde{R_2}) = R_4$ is same as R_3 then one common special point and other points are separate. Result R will be:

$$R = \frac{R_1 R_2}{R_3 \widetilde{R_3}}$$

ii. The other points are opposites of each other.

If $gcd(R_1, \widetilde{R_2}) = \widetilde{R_2} = R_1$ then, one common special point and other points are opposite. Result R will be 1:

(b) Common point is not special. $R_3 \neq \widetilde{R_3}$.

i. The other points are separate. $gcd(R_1, R_2) = R_3$ of degree 0.

The result R is:

$$R = R_1 R_2$$

ii. The other points are opposites of each other. $gcd(R_1, R_2) = R_4 \neq R_3$ of degree one.

$$R = \frac{R_1 R_2}{R_4 \widetilde{R_4}}$$

3. Two common points. $gcd(R_1, R_2) = R_3 = R_1 = R_2$ of degree two.

(a) One pair special. $gcd(R_1, \widetilde{R_2}) = R_4$ of degree one.

The special points will cancel out. The result will be:

$$R = \frac{R_1 R_2}{R_4 \widetilde{R_4}}$$

(b) Both pairs special. $gcd(R_1, \widetilde{R_2}) = R_4$ of degree two.

Both the pairs will cancel out each other. And the result will be zero divisor. $R = 1$.

(c) None of the common points are special. $gcd(R_1, \widetilde{R_2}) = R_4$ is of degree 0.

Nothing to be cancelled out. All the points add up to the result R.

$$R = R_1 R_2$$

The details listed above are the main structure of the algorithm. The problems we face are the calculation of multi-variate *gcd* and that too very frequently. This problem can be avoided by careful handling of the cases and careful comparisons of the coefficients. The detailed algorithm is given in next section.

6.1.2 The Algorithm

The algorithm itself is divided into three major parts depending on the three combination of weights of the divisors.

- **Input:** The inputs for the algorithm are the chow forms of reduced divisors. Let us call them a and b. Both of them are multi-variate polynomials.
- **Output:** The output of the algorithm also is chow form of a divisor. But the divisor is either reduced or semi-reduced. The result is named as R.

Case I : $degree(a) = 1$ **and** $degree(b) = 1$**.**

comment: $a = x_1 u_x + y_1 u_y + u_z$

comment: $b = x_3 u_x + y_3 u_y + u_z$

if $x_1 = x_3$

  if $y_1 = y_3$

    comment: This means they are opposites of each other

$R = 1$

comment: Result is zero divisor

else

comment: Not opposites nor special point. Must be same non-zero points

$R = a.b$

fi

else

comment: No common x

$R = a.b$

fi

The result R is reduced divisor.

Case II: $degree(a) = 1$ **and** $degree(b) = 2$**.**

comment: Here the polynomials will be of the following form.

$$a = x_1 u_x + y_1 u_y + u_z$$

$$b = b_1 u_x^2 + b_2 u_y^2 + b_3 u_z^2 + b_4 u_x u_y + b_5 u_x u_z + b_6 u_y u_z$$

$$\begin{aligned} b_1 &= x_3 x_4 & b_4 &= x_3 y_4 + x_4 y_3 \\ b_2 &= y_3 y_4 & b_5 &= x_3 + x_4 \\ b_3 &= 1 & b_6 &= y_3 + y_4 \end{aligned}$$

if $x_1(b_5 - x_1) = b_1$

comment: x_1 is a common x

if $y_1(b_6 - y_1) = b_2$

comment: y coordinate also is common.

comment: But which y? - y_3 or y_4? Let $x_1 = x_3$.

comment: Then y_3 can be either y_1 or $-y_1$.

if $y_1 = 0$

comment: The common point is special

$R = b/a$

comment: We can do it without division

$R = (b_5 - x_1)u_x + (b_6 - y_1)u_y + u_z$

else

comment: Common point is not special

$R = ab$

comment: No short cuts

fi

else

comment: $y_3 = -y_1$

comment: Cancel them out

$R = (ab)/(a\widetilde{a}) = b/\widetilde{a}$

comment: this also without real division we can do

$R = (b_5 - x_1)u_x + (b_6 + y_1)u_y + u_z$

fi

else

comment: No common x coordinate

$R = ab$

fi

Case III: $degree(a) = 2$ **and** $degree(b) = 2$**.**

Comment: Here the polynomials will be of the following form.

$$a = a_1u_x^2 + a_2u_y^2 + a_3u_z^2 + a_4u_xu_y + a_5u_xu_z + a_6u_yu_z$$

$$\begin{aligned} a_1 &= x_1x_2 & a_4 &= x_1y_2 + x_2y_1 \\ a_2 &= y_1y_2 & a_5 &= x_1 + x_2 \\ a_3 &= 1 & a_6 &= y_1 + y_2 \end{aligned}$$

$$b = b_1u_x^2 + b_2u_y^2 + b_3u_z^2 + b_4u_xu_y + b_5u_xu_z + b_6u_yu_z$$

$$\begin{aligned} b_1 &= x_3x_4 & b_4 &= x_3y_4 + x_4y_3 \\ b_2 &= y_3y_4 & b_5 &= x_3 + x_4 \\ b_3 &= 1 & b_6 &= y_3 + y_4 \end{aligned}$$

We just calculate a few more constants:

$$a_7 = a_5 \times a_6 = x_1y_1 + x_2y_2 + x_1y_2 + x_2y_1$$

$$a_8 = a_7 - a_4 = x_1y_1 + x_2y_2$$

Similarly b_7 and b_8.

if $a_1 = b_1$

comment: $x_1x_2 = x_3x_4$

if $a_5 = b_5$

comment: $x_1 + x_2 = x_3 + x_4$

comment: Two common x coordinates

if $a_2 = b_2$

comment: $y_1y_2 = y_3y_4$ They can be opposites

if $a_6 = b_6$

comment: y's are common in both pairs

if $a_2 = 0$

comment: Atleast one y is zero

if $a_6 = 0$

comment: Both y's are zeros

comment: Cancel each other

$R = 1$

else

comment: Other pair is same but nonzero

comment: Cancel out the special point

$R = \frac{ab}{gcd(a,\widetilde{b})gcd(\widetilde{a},b)}$

comment: We can have manage without calculating gcd

comment: $a_8 = x_2y_2$

comment: $2a_8 = 2x_2y_2 = x_2y_4 + x_4y_2 = R_4$

comment: $a_6 = y_2$

comment: $2a_6 = R_6, a_6^2 = R_2$

comment: $a_9 = (a_8/a_6) = x_2$

comment: $2a_9 = R_5, a_9^2 = R_1$

comment: In 1M, 2S, 1I - we have reduced divisor R

fi

comment: End of $a_6 = 0$

else

comment: None of the y's are zeros

$R = ab$

fi

comment: End of $a_2 = b_6$

else

comment: y's are not same

comment: Only option is they are opposites

comment: They cancel out each other

$R = 1$

fi

comment: End of $a_6 = b_6$

else

comment: $a_2 \neq b_2$ i.e, $y_1y_2 \neq y_3y_4$

comment: a_2 nor b_2 can be 0. Because 0 comes in pairs

comment: It must be $y_1y_2 = -y_3y_4$

comment: One common and other pair opposite

$R = \frac{ab}{gcd(a,\widetilde{b})gcd(\widetilde{a},b)}$

comment: $a_8 + b_8 = x_1y_1 + x_3y_3 = R_4$

comment: $a_6 + b_6 = 2y_1 = R_6$

comment: $(R_6/2)^2 = y_1y_3 = R_2$

comment: $R_4/y_1 = 2x_1 = R_5$

comment: $(R_5/2)^2 = x_1x_3 = R_1$

comment: In 2M, 2S, 1I we have R

fi

comment: End of $a_2 = b_2$

else

comment: $x_1x_2 = x_3x_4, x_1 + x_2 \neq x_3x_4$

comment: If $x_1x_2 \neq 0$ all of them are different

if $a_1 \neq 0$

comment: $x_1x_2 = x_3x_4 \neq 0$

comment: x_1, x_2, x_3, x_4 all separate

$R = ab$

else

comment: One x is common and is zero

comment: To be dealt in the next case

$Consider\_next\_case$.

fi

comment: End of $a_1 = 0$

fi

comment: End of $a_5 = b_5$

else

if $res(x^2 - a_5x + a_1, x^2 - b_5x + b_1) = 0$

comment: One common x coordinate

if $a_2 = b_2$

comment: $y_1y_2 = y_3y_4$

if $a_6 = b_6$

comment: Same factorisation - common y's

if $a_2 = 0$

comment: Atleast one y is zero

if $a_6 = 0$

comment: Both y's are zero

comment: Cancel out the common special point

$R = (ab)/(gcd(a, b))^2$

comment: $a_9 = a_5 + b_5 = 2x_1 + x_2 + x_4$

comment: $a_{10} = a_5 - b_5 = x_2 - x_4 \neq 0$

comment: $a_{11} = a_9 \times a_{10} = 2a_1 - 2b_1 + x_2^2 - x_4^2$

comment: $a_{12} = a_{11} - 2a_1 + 2b_1 = x_2^2 - x_4^2$

comment: $a_{13} = a_{12}/a_{11} = x_2 + x_4 = R_5$

comment: $a_{14} = (a_{10}a_{13})(a_{13}a_{10})/4 = x_2x_4 = R_1$

comment: All other coefficients are zeros

comment: In 2M, 1I R is calculated

else

comment: One pair is 0. Cancel or add?

if $a_4 = b_4$

comment: Common x has zero y's

$R = (ab)/(gcd(a,b))^2$

comment: $a_6 + b_6 = R_6$

comment: $a_6 \times b_6 = R_2$

comment: $T_1 = a_5 \times b_6 - a_4 = x_2 y_4$

comment: $T_2 = a_6 \times b_5 - b_4 = x_4 y_2$

comment: $T_1 + T_2 = R_4$

comment: $(T_1 T_2)/R_2 = x_2 x_4 = R_1$

comment: $(T_1 + T_2)/a_6 = x_2 + x_4 = R_5$

comment: In 3M and 2I, R is calculated

else

$R = ab$

fi

comment: End of $a_4 = b_4$

fi

comment: End of $a_6 = 0$

else

comment: No zeros at all

comment: Here $a_2 = b_2 \neq 0$

$R = ab$

fi

comment: End of $a_2 = b_2 = 0$

else

comment: $a_6 \neq b_6$

if $a_2 = 0$

comment: b_2 also is 0.

comment: Common x has y equal 0 or y_1

if $a_4 = b_4$

comment: First case: y equal 0

$R = (ab)/(gcd(a, b))^2$

comment: We can find R_1 and R_5 using a previous method

comment: $a_6 + b_6 = R_6$

comment: $a_6 \times b_6 = R_2$

comment: $(a_5 b_6) + (b_5 + a_6) - a_4 - b_4 = R_4$

comment: Here we need 5M and 1I

else

$R = ab$

fi

comment: End of $a_4 = b_4$

else

comment: No y is zero

comment: Only thing remaining is to cancel common x's

$R = (ab)/(gcd(a, b))^2$

comment: The same method used above can be used

comment: $y_2 = (a_8 + b_8)/(x_2 - x_4)$

comment: $x_2 - x_4$ calculated in the previous one

comment: $-y_2^2 = R_2$

comment: Other constants are zeros

comment: Here we need 5M and 1I

fi

comment: End of $a_2 = 0$

fi

comment: $a_6 = b_6$ End.

else

comment: $a_2 \neq b_2$

if $a_6 = b_6$

comment: $y_1 + y_2 = y_3 + y_4$

comment: $y_1 = y_3 \Rightarrow y_2 = y_4 \Rightarrow a_2 = b_2 \Rightarrow Contradiction$

comment: $y_1 = -y_3$

$R = (ab)/(gcd(a, b))^2$

comment: Same methods of calculations

else

$R = \frac{ab}{gcd(a,\widetilde{b})gcd(\widetilde{a},b)}$

comment: As in the cases above. We get the result in a few steps

fi

fi

else

comment: No common x coordinate

comment: Multiply them together and then reduce

$R = ab$

fi

Many of the cases arise can be computed with the coefficients. A few of the cases give semi-reduced divisors. Hence we need a reduction algorithm also.

6.2 Reduction

Before going to the idea of reduction I should define a few things which are needed in this section. We know that all the points in our curve are non-singular points. A non-singular point is sometimes called a simple point.

Definition 75 (Simple divisor, Very Simple divisor). Let $D = \sum_i m_i P_i$ be a divisor of C which is rational over K. We will say that D is simple if each P_i is simple point of C. D is very simple if, in addition, each $m_i = \pm 1$.

Definition 76 (Good Line). A line L is goof for D if for every $Q \in L \cap C$

1. Q is simple.
2. $Q \notin D$
3. L is not tangent to C at Q.

A finite set of lines $\mathcal{L}$ is good for D on C if every line $L \in \mathcal{L}$ is good for D on C.

Lemma 77 (Implicit Simplification Lemma). Let D be a divisor in which all points are affine. Let $S = D = \sum_j m_j Q_i$ be a divisor such that $supp(D) \cap supp(S) = \phi$. We can construct a k-rational polynomial G such that (1) G is a product of linear forms, (2) $(G) = D + A$ where A is a very simple affine divisor, and (3) every factor L of G is good for S on C.

We can see that the new very simple divisor A is an equivalent to D. The construction of G needs one invertible linear transformation :
$\phi : A^2 \rightarrow A^2$. For details of the method [1, 2]. There is no direct connection between this lemma and our requirement. But this lemma gives something which is very similar to what we need. It is in a very general case where even singular points can exist.

From this lemma and related theorems and methods, we have to refine out a method for the special cases of our small problems.

The method has not been refined from the general method available for all types of curves. The things to be done and to be resolved are listed below.

1. To make sure that $degree(A) \leq degree(D)$.

   The lemma states just that we can construct a polynomial having the property of giving an equivalent very simple divisor for D. But if the weight of the new equivalent created is larger than that of D, our purpose cannot be served. It has to be studied and proved. Otherwise a new construction is to be devised - which is a tailor made method for our special cases.

2. Can we make the transformation general?

   The affine transformation ϕ which is used for the construction of the new polynomial G must be given a general form so that deciding on the transformation is to be done one and only once. Repeating a search for an optimal transformation can be time consuming.

3. What happens if the result must contain points with order more than one.

   From the lemma, we know that A, the new equivalent divisor is a very simple divisor. i.e, the order/multiplicity of all points is one. But in our addition in the jacobian its very usual to get reduced divisors which consist of points with multiplycity 2. (Eg: $D = 2P_1$). Again here we have to change the construction method so that the restriction on the resulting equivalent divisor is taken away.

The three problems to be resolved are remaining as open problems whose solution may lead to better algorithms in addition in the jacobian of hyperelliptic curves.

Chapter 7

Results, Conclusion and Further Work

"Not too fast

Not too slow"

– L Armstrong

In the chapters 5 and 6 we saw the new methods developed by my team. It was very evident that the composition phase was fairly easy to both understand and also to design. The reduction part stays as a hurdle even now. In this chapter let us have a look towards the results.

7.1 Results

7.1.1 Point Addition

Composition

The algorithm given for composition is general. But practically for cryptography we need only those curves of genus either *two* or *three*. Also in most of the cases, $h(x)$ will be zero.

1. Genus 2

   - $h \neq 0$

     Here as we saw in the chapter 5, we have g^2 multiplications along with $5g + 4$ additions which are very cheap.

Additions	$5 \times 2 + 4 = 14$
Multiplications	$2^2 = 4$

   - $h = 0$

     Just with 14 additions the composition phase will be over.

2. Genus 3

   - $h \neq 0$

     This is similar to the genus 2 case.

Additions	$5 \times 3 + 4 = 19$
Multiplications	$3^2 = 9$

   - $h = 0$

     Again, there are no multiplications. Just 19 additions are the only operations in the composition phase.

Case (Common x)	Worst subcase	Necessity of reduction.
Two	2M, 2S and 1I	Most subcases dont need.
One	5M and 2I	50% needs reduction
None		All must be reduced

Table 7.1: Cases of chow composition and number of operations

Reduction

As a matter of probability we can take that only 50% of the additions only will need to go through the reduction step. In the reduction step, we cannot in precise tell the number of operations needed for computation. But there are very fast implementations available for root finding in finite fields. Their existence makes the algorithm worth enough to give a try.

The details of the reduction part we have already seen in the last part of chapter 5.

7.1.2 Chow Representation Addition

Using the chow representation, we have only designed the composition part. The basic idea for reduction part is laid. More work has to be done with the reduction part. Here I shall give an account of the number of operation needed in the major three cases which can occur. See Table 7.1. Again, for the details refer chapter 6.

Whether reduction is to be used or not is decided in the beginning itself by just comparing the coefficients of the chow forms. Hence we can directly do the reduction part without wasting our resources in composition.

As of now the method is good provided that a good reduction method has to be designed.

7.2 Conclusion

In the project, a study of hyperelliptic curves was done. Also a detailed investigation in the methods used to do arithmetic in the jacobian of hyperelliptic curves was done. A study on different represetation of divisors of hyperelliptic curves was also done.

I am able to see that only one of the represetations is deeply explored by the researchers in this area. The other two represetations are almost un-explored. From what we have seen in the thesis, explicit representation does not seem to have much future because, the explicit representation needs the arithmetic to be done in the closure of the base field. The future of the addition lies in the other two represenations:

1. Mumford Representation
2. Chow Form Represenation

Why mumford representation seems to be better than any other representations? One reason is very clear. There was not enough research done in the other representation. In a recent paper by Tanja Lange [15], she uses projective coordinates. In fact, chow forms use projective coordinates with $z = 1$ always.

In my opinion enough study has not been done in chow forms. The non-availability of the literature itself is a proof for that.

In the table 7.2 a comparison of the two representations is given in the perspective of addition in the jacobian of hyperelliptic curves.

7.3 Further Work

1. Implementation.

Mumford Representation	Chow Representation
Uses two polynomials a and b. Both polynomials are $\in k[x]$.	Representation uses a single multivariate polynomial. The polynomial is $\in k[x, y]$.
For genus 2 curves, the representation needs five variables to be stored.	The represetation takes five variables to represent a divisor of a genus 2 curve.
Generic type of representation.	For divisors of different weights the representation varies.
Very efficient algorithms exist for computation.	Not many good methods are available.

Table 7.2: Different Representations: A Comparison

The obvious work to be done is the implementation of the algorithms. Comparisons between differnt methods available and the new ones also must be done. A rough estimate says that the implementation will take about two to three months.

2. Pipelining.

   The method of point addition is in a form such that pipelining can be tried out. While the composition phase is going on itself, the calculation of derivatives of f can be done. The step of factorisation is the only step which we cannot pipeline because of the probabilistic algorithm.

3. More about Chow forms.

   A detailed study about chow forms must be done so as to make the reduction part more clear. It must be seen whether the affine transformation can be generalised for all types of hyperelliptic curves. The work must be seen from a practical perspective rather than from the theoretical point of view.

Bibliography

[1] Ming-Deh A. Huang, Doug Ierardi, Efficient Algorithms for the Riemann-Roch Problem and for Addition in the Jacobian of a Curve. Journal of Symbolic Computation 1994, v. 18 i. 6 p. 519 - 539.

[2] Ming-Deh Huang, Doug Ierardi, Efficient algorithms for the Riemann-Roch problem and for addition in the Jacobian of a curve (extended abstract), Proceedings of the 32nd annual symposium on Foundations of computer science, p.678-687, September 1991, San Juan, Puerto Rico.

[3] D. G. Cantor, Computing in the Jacobian of a hyperelliptic curve, Mathematics of Computation 48 (1987), 95-101.

[4] W. Fulton, Algebraic curves. Addison-Wesley 1989.

[5] P. Gaudry and R. Harley, Counting points on hyperelliptic curves over finite fields, ANTS-IV, Springer-Verlag, LNCS 1838, 313-332, 2000.

[6] R. Harley *adding.text, doubling.c*, `http://cristal.inria.fr/~harley/hyper`, 2000.

[7] I. N. Herstein, Abstract Algebra, Macmillan, 1986.

[8] I. N. Herstein, Topics in Algebra, 2nd ed. New York: Wiley, 1975.

[9] D. E. Knuth, TAOCP - 2, Seminumerical Algorithms, Third Edition, Addison-Wesley, 1997.

[10] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, Vol. 48, 1987, 203-209.

[11] N. Koblitz, Hyperelliptic cryptosystems, Journal of Cryptology, Vol. 1, 1989, 139-150.

[12] N. Koblitz, Algebraic Aspects of Cryptography, Algorithms and Computation in Mathematics Vol. 3, Springer-Verlag, New York, 1998.

[13] N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, Berlin, 1994.

[14] Tanja Lange, Efficient Arithmetic on Genus 2 Hyperelliptic Curves over Finite Fields via Explicit Formulae. `http://eprint.iacr.org/2002/121.pdf`.

[15] Tanja Lange, Inversion-Free Arithmetic on Genus 2 Hyperelliptic Curves. `eprint.iacr.org/2002/147.ps`.

[16] Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato. An elementary introduction to hyperelliptic curves. `www.math.uiuc.edu/~handuong/crypto/menezes_wu_zuccherato.pdf`.

[17] Mumford, D. Tata Lectures on Theta. II. Boston, MA: Birkhuser, 1984.

[18] S. Roman, Field Theory, Series: Graduate Texts in Mathematics, Vol. 158

[19] J.H. Silverman and J. Tate, "Rational Points on Elliptic Curves", Springer, 1992.

[20] C. C. Thomas, Analysis of FPGA-based Hyperelliptic Curve Cryptosystems. `www.cs.umd.edu/clancy/docs/thesis.pdf`.