Improving Divisor Arithmetic Over Genus 2 Hyperelliptic Curves

Sebastian Lindner

Supervisor: Michael Jacobson

UNIVERSITY OF CALGARY

Motivation

Our goal is to make computation of divisor arithmetic in the divisor class group over genus 2 hyperelliptic curves fast as possible.

Divisor Class Group

○ Let C over F_q, described by

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

be an imaginary hyperelliptic curve of genus 2 where $h(x)$ has degree at most 2 and $f(x)$ is monic with degree 5.

○ A divisor D is a formal sum of points on C.

○ We use $Pic^0(C)$ the divisor class group, which is isomorphic to the Jacobian, as our setting.

○ Each divisor class over $\mathbb{F}_q$ can be represented uniquely in Mumford representation by two polynomials, and group law arithmetic in $Pic^0(C)$ is reduced to polynomial arithmetic.

Why do we care?

The most computationally intensive operation in Hyperelliptic Curve Cryptography (HECC) is scalar multiplication of a divisor D,

$$[n]D = D + D + D + \cdots + D, \ (n \text{ times.})$$

Efficient implementation of HECC relies on the ability to efficiently compute $[n]D$.

Multibase representations of numbers can be paired with fast divisor arithmetic to speed up scalar multiplication. For example using base 2 and 3 representations, we can take advantage fo fast divisor doubling and tripling:

$$57 = 2^5 + 2^4 + 2^3 + 2^0 \quad \text{vs} \quad 57 = 2^1 3^3 + 2^0 3^1$$

Current Work

We have overall improved on group law computations in previously submitted work, but our attempts at creating fast divisor triplings paired with multibase scalar multiplication algorithms were still lacking compared to doubling-add based scalar multiplication.

(Un)fortunately, after beating the group law to death, we have to turn to more sophisticated approaches in order to come by further improvements.

We focus on computations of compound operations called multiplication-by-l maps, with scalar multiplication in mind.

State of the Art

In their seminal paper, Doche, Icart and Kohel were able to computationally improve on doubling or tripling points through constructing elliptic curves that admit fast multiplication-by-2 and 3 maps, called **DIK curves**.

Moody expanded the same techniques to include fast multiplication-by-5 maps.

Goals

Our goal is to generalize DIK curves to the genus two setting.

DIK Curve Background

- Multiplication-by-l maps exist for all l and all elliptic curves via division polynomials, which require the evaluation of degree l^2 rational maps.
- For some select numbers l, it is possible for well chosen families of curves to “split” the multiplication-by-l map $[l]$ as the product of a degree l isogeny and its dual.
- Two applications of an l-isogeny (degree l rational map) computationally outperforms the application of a degree l^2 rational map in some cases, even for very small values for l.

Constructing DIK Curves

In order to amplify the impact of creating elliptic curves that have split multiplication-by-l maps, we wish to keep the construction of the curves as general as possible and make the maps as efficient as possible. The two main obstacles are:

1. Parametrize families of curves that admit l-isogenies with a curve equation dependent on some variable.
2. Describe efficient formulas to compute the l-isogenies and isogenous curve that makes up the split multiplication-by-l maps.

DIK Constructions

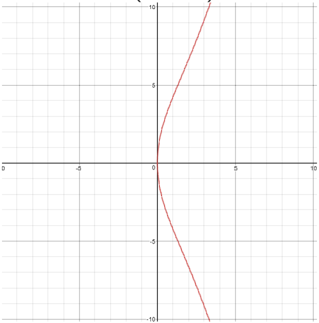
Given an elliptic curve E and the kernel of an l-isogeny G_l, it is easy to compute the rational maps defining $\phi_l \cdot \hat{\phi}_l P = [l]P$ along with the isogenous curve E_l using Velu's formulas.

The hard part is parametrizing the family of elliptic curves that admit an l-isogeny and therefor a split multiplication-by-l map.

This brings us to modular curves.

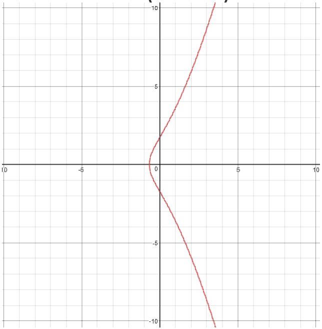
Examples of parametrized curves

$(l = 2)$



$$y^2 = x^3 + ux^2 + 16ux$$
$$(u = 1)$$

$(l = 3)$



$$y^2 = x^3 + 3u(x+1)^2$$
$$(u = 1)$$

Modular Curves

There exist modular curves X which have the following informal connection with elliptic curves:

$$\left\{ \begin{array}{c} \text{Information} \\ \text{on } X \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Information about the family} \\ \text{of elliptic curves that admit an} \\ l\text{-isogeny} \end{array} \right\}$$

There is one for every value l and they are denoted by $X_0(l)$. We use information about the $X_0(l)$ to create parametrized curve equations that encapsulate all elliptic curves admitting l-isogenies.

Modular Curves

A modular curve is defined as a quotient space of the complex upper half plane $\mathbb{H} = \{\delta \in \mathbb{C} \mid \mathrm{Im}(\delta) > 0\}$, under a subgroup of $SL_2(\mathbb{Z})$ denoted Γ :

$$X(\Gamma) = \mathbb{H}/\Gamma = \{\Gamma\delta \mid \delta \in \mathbb{H}\}.$$

The congruence subgroup of $SL_2(\mathbb{Z})$ for $X_0(l)$ is:

$$\Gamma_0(l) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \mod l \right\}.$$

And the modular curves are defined as:

$$X_0(l) = \mathbb{H}/\Gamma_0(l) = \{\Gamma_0(l)\delta \mid \delta \in \mathbb{H}\}$$

Connection between Modular and Elliptic Curves

- The modular curves $X_0(l)$ can be described algebraically.
- Points on the $X_0(l)$ correspond to pairs of j-invariants of l-isogenous elliptic curves.
- The modular curve theory presented is tied to complex numbers, but works over finite fields.

Modular Curves - Examples

Example

The curve equation for $X_0(2)$ is described by

$$F_2(X,Y) = -(XY)^2 + 1485(X+Y+27675)XY + (X+Y-54000)^3 = 0.$$

Every point (A,B) corresponds to two j-invariants of elliptic curves that are 2-isogenous to each other. Spanning over all X and Y parametrizes all elliptic curves the admit 2-isogenies.

What is $X_0(1)$?

Parametrizing families of elliptic curves

We can find curve equations for families of elliptic curves that have l-isogenies by looking at the relationship between rational functions that generate the function fields of $X_0(l)$, and the j-invariant which generates the j-line $X_0(1)$.

Genus Two Setting

All of the machinery surrounding constructing DIK curves generalizes to the genus two setting. We point out some important parts:

1. The Picard group of divisor classes in genus two is isomorphic to a dimension two principally polarized abelian variety.
2. All statements about isogenies for elliptic curves work in general for dimension two principally polarized abelian varieties.
3. The upper half plane generalizes to the two dimensional Siegel upper half plane

$$\mathbb{H}_2 = \{\tau \in Mat_2(\mathbb{C}) \mid \tau^T = \tau,\ Im(\tau) \text{ positive definite}\}.$$

Genus two Setting

4. Igusa invariants are the generalization of the j-invariant to the genus two setting. They play the same role as the j-invariant in finding explicit parametrizations of genus two curves with l-isogeny structure.

   The invariants are three algebraically independent rational functions defined on the two dimensional Siegel upper half plane, denoted by j_1, j_2, j_3.

Genus Two Setting

5. The modular group $SL_2(\mathbb{Z})$ generalizes to the *symplectic group*:

$$Sp_4(\mathbb{Z}) = \{M \in SL_4(\mathbb{Z}) \mid MJM^T = J\},$$

a subgroup of $SL_4(\mathbb{Z})$ where

$$J = \begin{pmatrix} 0 & 1_2 \\ -1_2 & 0 \end{pmatrix},$$

and 1_2 denotes the 2×2 identity matrix.

Genus Two Setting

6. The definition of the modular curve for the genus two setting is described as the quotient space

$$X^{(2)} = \mathbb{H}_2/\Gamma^{(2)},$$

   where $\Gamma^{(2)}$ is a congruence subgroup of $Sp_4(\mathbb{Z})$. When $\Gamma^{(2)} = Sp_4(\mathbb{Z})$, we get the generalization of the j-line from the genus one setting.

Looking forward - Genus 2

We anticipate taking the following steps in the genus 2 setting:

1. There are now three rational equations that need to be used in order to parametrize a family of genus two curves with l-isogeny structure. We must find the simplest way to parametrize a family of curves using three rational functions.
2. We then reduce the complexity of computing the multiplication-by-l maps by taking the general isogeny algorithms by D. Robert and others and specialize to our cases for l making the maps as simple as possible.

Thank you

Thank you