Balanced representation for divisors and Explicit Formula in Real Hyperelliptic Curves

Monireh Rezai Rad

University of Calgary

ECC 2012 Mexico, Queretaro
October 29, 2012

Hyperelliptic Curves

A hyperelliptic curve of genus g over a finite field $\mathbb{F}_q$ is a non-singular, irreducible equation of the form

$$C: \ y^2 + h(x)y = f(x)$$

where $h, f \in \mathbb{F}_q[x]$ satisfy certain conditions.
For example, $h(x) = 0$ if $char(\mathbb{F}_q) \neq 2$.

Imaginary and Real Model

Hyperelliptic curves come in two models:

- Imaginary Model
  - f monic and $deg(f) = 2g + 1$,
  - $deg(h) \leq g$ if q even.
- Real Model
  - If q odd: f monic and $deg(f) = 2g + 2$,
  - If q even: h monic and $deg(h) = g + 1$,
    - f monic and $deg(f) \leq 2g + 1$, or
    - $deg(f) = 2g + 2$, and $sgn(f) = e^2 + e, (e \in F_q^*)$.

The imaginary model has one point ∞ at infinity.
The real model has two points at infinity, ∞ and $\bar{\infty}$.

Divisors and Jacobian

A **divisor** D is a formal sum of points in C

$$D = \sum_{P \in C} n_P P \ , \ n_P \in \mathbb{Z}$$

where all $n_P = 0$, except for finitely many.

The divisor class group or the **Jacobian**, $Cl^0(C)$, is defined to be the quotient group of a certain subgroup of $Div(C)$ modulo the principal divisors.

Each class in the Jacobian has a representative called **reduced** divisor.

Each reduced divisor can be represented by two polynomials (u, v), namely the Mumford representation.

Balanced Divisors

Definition: D_∞ is a degree g effective divisor defined as below:
- If g is even then $D_\infty = \frac{g}{2}(\infty^+ + \infty^-)$.
- If g is odd then $D_\infty = \frac{g+1}{2}\infty^+ + \frac{g-1}{2}\infty^-$.

Proposition: Let C be a real hyperelliptic curve and $D \in \mathrm{Div}^0(C$ then $[D]$ has a unique representative in $Cl^0(C)$ of the form $[D_0 - D_\infty]$, where D_0 is an effective divisor of degree g whose affine part is reduced.

Definition: Let D_1 and D_2 be two divisors. we say that the numbers ω^+ and ω^- are counterweights for D_1 and D_2 if

$$D_1 \equiv D_2 + \omega^+\infty^+ + \omega^-\infty^-$$

we denote the set of such a pair of ω^+ and ω^- by $\omega(D_1, D_2)$.

Arithmetic in Real model Using Balanced Divisors

Algorithm 1. Composition
Input: Semi-reduced affine divisors $D_1 = (u_1, v_1)$, and $D_2 = (u_2, v_2)$.
Output: A semi-reduced affine divisor $D_3 = (u, v)$ and a pair (ω^+, ω^-) such that $(\omega^+, \omega^-) \in \omega(D_1 + D_2, D_3)$.

Algorithm 2 Reduction
Input: A semi-reduced affine divisor $D_0 = (u_0, v_0)$ with $d_0 \geq g + 2$.
Output: A semi-reduced affine divisor $D_1 = (u_1, v_1)$, and a pair of (ω^+, ω^-), such that $d_1 < d_0$ and $(\omega^+, \omega^-) \in \omega(D_0, D_1)$.

Baby Step

Algorithm 3. Composition at Infinity and Reduction
Input: A semi-reduced affine divisor $D_0 = (u_0, v_0)$ of degree $d_0 \leq g + 1$.
Output: A reduced affine divisor $D_1 = (u_1, v_1)$ and a pair of integers (ω^+, ω^-) such that $(\omega^+, \omega^-) \in \omega(D_0, D_1)$.

- $v' := H^{\pm} + ((v_0 - H^{\pm}) \bmod u_0)$.
- $u_1 := \frac{v'^2 + hv' - f}{u_0}$ made monic.
- $v_1 := -h - v' \bmod u_1$.
- **if** H^+ was used **then**
  $(\omega^+, \omega^-) := (d_0 - g - 1, g + 1 - d_1)$.
- **else if** H^- was used **then**
  $(\omega^+, \omega^-) := (g + 1 - d_1, d_0 - g - 1)$.
  end if
- **return** (u_1, v_1) and (ω^+, ω^-).

$H^+ = \lfloor y \rfloor$ and $H^- = -\lfloor y \rfloor - h$

Explicit Formula

In this section we introduce a method named explicit formula for real hyperelliptic curves of genus 2. Thus in the hyperelliptic curve

$$C: \; y^2 + h(x)y = f(x)$$

$h(x) = h_3x^3 + h_2x^2 + h_1x + h_0$ is a degree 3, and
$f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x^1 + f_0$ is a degree 6 polynomial.

$$H^+ = y_3x^3 + y_2x^2 + y_1x + y_0$$

By plug in H^+) in the C we will have:

$$\left\{ \begin{array}{l} y_3^2 + h_3y_3 = f_6 \\ y_2 = (f_5 - y_3h_2)/(2y_3 + h_3) \\ y_1 = (f_4 - y_3h_1 - y_2(y_2 + h))/(2y_3 + h_3) \\ y_0 = (f_3 - y_3h_0 - y_2(2y_1 + h_1) - y_1h_2)/(2y_3 + h_3) \end{array} \right\}$$

Explicit Formula for Baby step

We can show that v must be in the forms
$v = -(y_3 + h_3)x^3 + -(y_2 + h_2)x^2 + v_1 x + v_0$ or
$v = y_3 x^3 + y_2 x^2 + v_1 x + v_0$.
$u = x^2 + u_1 x + u_0$ or $u = x + u_0$.

By plug in them in the algorithm 3 we can compute u' and v' in the worth case in 1 inversion, 6 Multiplication.

Thank you for your attention!