# Efficient Hyperelliptic Arithmetic Using Balanced Representation for Divisors

Steven Galbraith[1] Mike Harrison[2] David Mireles[1]

[1]Royal Holloway, University of London

[2]University of Sydney

May 22, 2008

# Overview

## Plane Models

We will consider a genus $g$ hyperelliptic curve $C$ defined over a field $k$ with $\mathrm{char}(k) \neq 2$. We can assume that $C$ is given by a plane model

$$C : y^2 = F(x),$$

where $F$ is a polynomial in $k[x]$ with no repeated roots.
If $P = (x, y)$ is a point on the curve, then $\overline{P} = (x, -y)$ also lies on the curve and is called hyperelliptic conjugate of $P$.

## Taxonomy

- If $\deg(F)$ is $2g + 1$, this is an imaginary model. $C$ will have 1 point at infinity.
- If $\deg(F)$ is $2g + 2$, this is a real model. $C$ will have 2 points at infinity.

## The divisor class group

- The *group of divisors* on $C$ is the group of finite formal sums $D = \sum n_i P_i$, for integers $n_i$ and points $P_i$ on $C(\bar{k})$. $\deg(D) = \sum n_i$.
- To every rational function $f$ in $C(\bar{k})^*$, one can associate a divisor

$$\operatorname{div}(f) = \sum_{P \in C(\bar{k})} \operatorname{ord}_P(f).$$

The set of divisors associated to all the functions in $C(\bar{k})^*$ forms the subgroup of principal divisors.
- The divisor class group of $C$ is the quotient group of the group of divisors modulo the subgroup of principal divisors. The class of $D$ will be denoted $[D]$.

## The divisor class group

- The *group of divisors* on $C$ is the group of finite formal sums $D = \sum n_i P_i$, for integers $n_i$ and points $P_i$ on $C(\overline{k})$.
  $\deg(D) = \sum n_i$.
- To every rational function $f$ in $C(\overline{k})^*$, one can associate a divisor

$$\operatorname{div}(f) = \sum_{P \in C(\overline{k})} \operatorname{ord}_P(f).$$

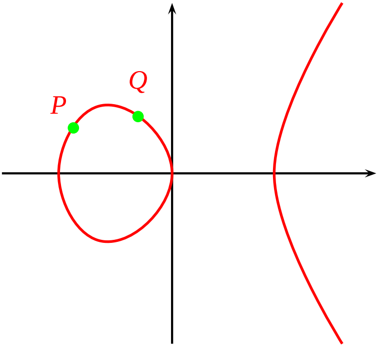
  The set of divisors associated to all the functions in $C(\overline{k})^*$ forms the subgroup of principal divisors.
- The divisor class group of $C$ is the quotient group of the group of divisors modulo the subgroup of principal divisors. The class of $D$ will be denoted $[D]$.

## The divisor class group

- The *group of divisors* on $C$ is the group of finite formal sums $D = \sum n_i P_i$, for integers $n_i$ and points $P_i$ on $C(\overline{k})$.
  $\deg(D) = \sum n_i$.
- To every rational function $f$ in $C(\overline{k})^*$, one can associate a divisor

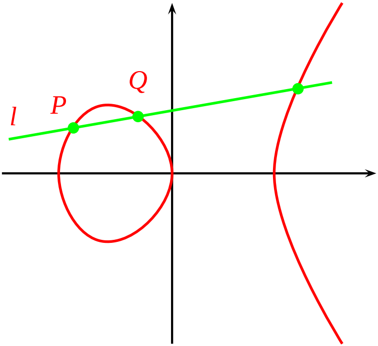
$$\operatorname{div}(f) = \sum_{P \in C(\overline{k})} \operatorname{ord}_P(f).$$

  The set of divisors associated to all the functions in $C(\overline{k})^*$ forms the subgroup of principal divisors.
- The divisor class group of $C$ is the quotient group of the group of divisors modulo the subgroup of principal divisors. The class of $D$ will be denoted $[D]$.



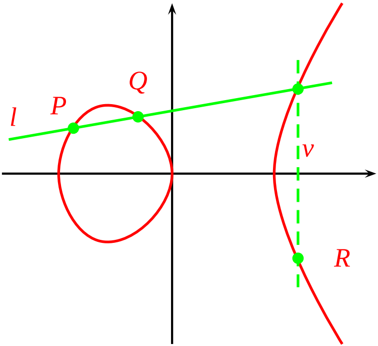

$$\operatorname{div}\left(\frac{l}{v}\right) = P + Q - R - \infty,$$

$$[P - \infty] + [Q - \infty] = [R - \infty]$$



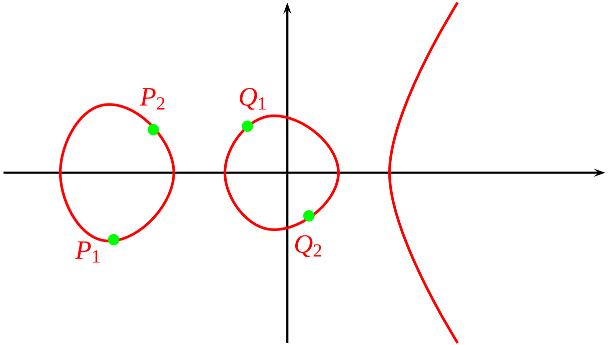

$$\operatorname{div}\left(\frac{l}{v}\right) = P + Q - R - \infty,$$

$$[P - \infty] + [Q - \infty] = [R - \infty]$$



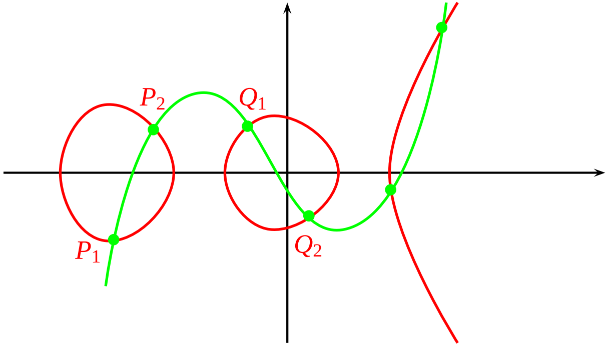

$$\operatorname{div}\left(\frac{l}{v}\right) = P + Q - R - \infty,$$

$$[P - \infty] + [Q - \infty] = [R - \infty]$$



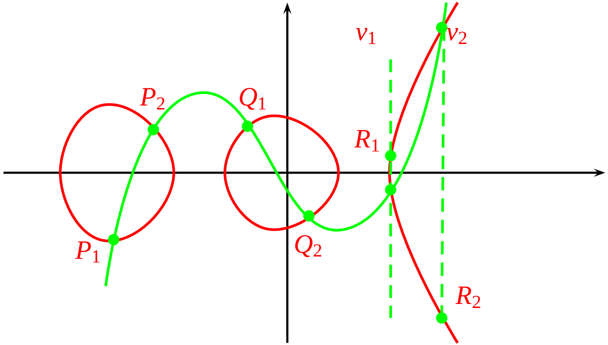

$$\operatorname{div}\left(\frac{y-p(x)}{v_1v_2}\right) = P_1 + P_2 + P_3 + P_4 - R_1 - R_2 - 2\infty,$$

$$[P_1 + P_2 - 2\infty] + [Q_1 + Q_2 - 2\infty] = [R_1 + R_2 - 2\infty].$$



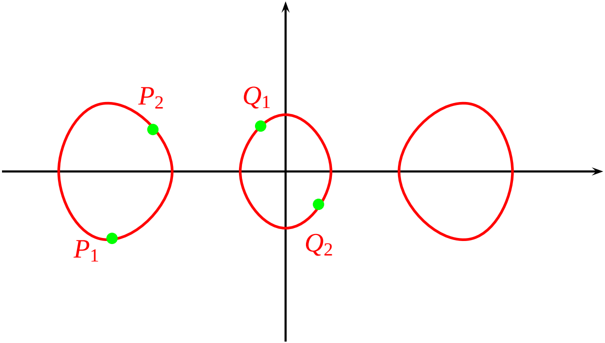

$$\operatorname{div}\left(\frac{y-p(x)}{v_1 v_2}\right) = P_1 + P_2 + P_3 + P_4 - R_1 - R_2 - 2\infty,$$

$$[P_1 + P_2 - 2\infty] + [Q_1 + Q_2 - 2\infty] = [R_1 + R_2 - 2\infty].$$



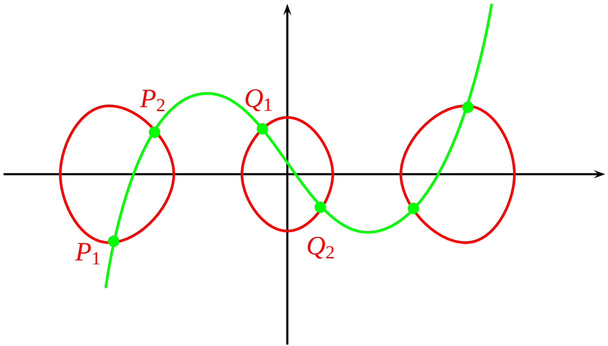

$$\operatorname{div}\left(\frac{y-p(x)}{v_1 v_2}\right) = P_1 + P_2 + P_3 + P_4 - R_1 - R_2 - 2\infty,$$

$$[P_1 + P_2 - 2\infty] + [Q_1 + Q_2 - 2\infty] = [R_1 + R_2 - 2\infty].$$



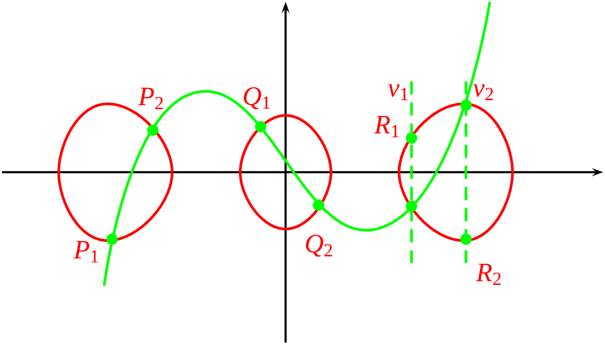

$$\operatorname{div}\left(\frac{y-p(x)}{v_1 v_2}\right) = P_1 + P_2 + P_3 + P_4 - R_1 - R_2 - \infty^+ - \infty^-,$$

$$[P_1+P_2-\infty^+-\infty^-]+[Q_1+Q_2-\infty^+-\infty^-] = [R_1+R_2-\infty^+-\infty^-].$$




$$\operatorname{div}\left(\frac{y-p(x)}{v_1 v_2}\right) = P_1 + P_2 + P_3 + P_4 - R_1 - R_2 - \infty^+ - \infty^-,$$

$$[P_1+P_2-\infty^+-\infty^-]+[Q_1+Q_2-\infty^+-\infty^-] = [R_1+R_2-\infty^+-\infty^-].$$




$$\operatorname{div}\left(\frac{y-p(x)}{v_1 v_2}\right) = P_1 + P_2 + P_3 + P_4 - R_1 - R_2 - \infty^+ - \infty^-,$$

$$[P_1 + P_2 - \infty^+ - \infty^-] + [Q_1 + Q_2 - \infty^+ - \infty^-] = [R_1 + R_2 - \infty^+ - \infty^-].$$

### Definition

A divisor $D = \sum n_i P_i$ is said to be *effective* if every coefficient $n_i$ is non-negative.

### Definition

We say that an effective divisor $D = \sum_i P_i$ on a hyperelliptic curve $C$ is *semi-reduced* if $i \neq j$ implies $P_i \neq \overline{P}_j$. If the hyperelliptic curve $C$ has genus $g$, we say that a divisor $D$ on $C$ is *reduced* if it is semi-reduced, and has degree $d \leq g$. We will denote the degree of a divisor $D_i$ as $d_i$.

## Definition

A divisor $D = \sum n_i P_i$ is said to be *effective* if every coefficient $n_i$ is non-negative.

## Definition

We say that an effective divisor $D = \sum_i P_i$ on a hyperelliptic curve $C$ is *semi-reduced* if $i \neq j$ implies $P_i \neq \overline{P}_j$. If the hyperelliptic curve $C$ has genus $g$, we say that a divisor $D$ on $C$ is *reduced* if it is semi-reduced, and has degree $d \leq g$. We will denote the degree of a divisor $D_i$ as $d_i$.

### Theorem

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

### The base divisor

- If $C$ is given by an imaginary model, then $D_\infty = g\infty$.
- If $C$ is given by a real model denote its points at infinity as $\infty^+$ and $\infty^-$. Then
  - $D_\infty = \frac{g}{2}(\infty^+ + \infty^-)$ if $g$ is even.
  - $D_\infty = \frac{g+1}{2}\infty^+ + \frac{g-1}{2}\infty^-$ if $g$ is odd.

## Mumford's Representation

To every pair of polynomials $(u(x), v(x))$ such that

$$u(x) \quad \text{divides} \quad F(x) - v(x)^2, \tag{1}$$

we associate a divisor as follows

$$\text{If } u(x) = \prod_i (x - r_i), \text{ then } (u(x), v(x)) \mapsto \sum_i (r_i, v(r_i)).$$

We say that the polynomials $(u, v)$ are the Mumford representation of $D$, and denote this as $D = \operatorname{div}(u, v)$. Every affine semi-reduced divisor has a Mumford representation.

## Problem

Fix a degree $g$ divisor $D_\infty$. Given two effective degree $g$ divisors with reduced affine part $D_1$ and $D_2$, find an effective degree $g$ divisor $D_3$ with reduced affine part such that

$$[D_1 - D_\infty] + [D_2 - D_\infty] = [D_3 - D_\infty].$$

## Equivalently

To add the divisor classes $[D_1 - D_\infty]$ and $[D_2 - D_\infty]$, one calculates $D_3$ satisfying

$$[D_1 + D_2] = [D_3 + D_\infty].$$

1. Given the Mumford representation of $D_1$ and $D_2$, find the Mumford representation of $D_1 + D_2$.
2. From the Mumford representation of $D_1 + D_2$, find the appropriate $D_3$. This is done using the reduction algorithms.

## Reduction

Let $D_0 = \mathrm{div}(u_0, v_0)$ be a divisor of degree $d_0 \geq g+2$ ($d_0 \geq g+1$). By definition of the Mumford representation, the divisor of $y - v_0(x)$ has (generically) the form

$$\mathrm{div}(y - v_0(x)) = D_0 + D_1 - \frac{d_0 + d_1}{2}(\infty^+ + \infty^-),$$

where $D_1$ is an affine semi-reduced divisor. This implies

$$[D_0] = [\overline{D}_1 + \frac{d_0 - d_1}{2}(\infty^+ + \infty^-)].$$

The affine zeros of $y - v_0(x)$ are found solving $v_0(x)^2 - F(x) = 0$.

## Composition and reduction

- If the divisor $D = \text{div}(u, v)$ has degree at most $g + 1$, then reduction using $y - v(x)$ does not work.
- For instance if $D$ has degree $g + 1$, then $\deg(v) \leq g$, so $v^2 - F$ will have $2g + 2$ affine zeros, and we get another divisor of degree $g + 1$.
- We have cancelation in $v^2 - F$ if and only if the leading term of $p$ is $F_{2g+2}^{1/2} x^{g+1}$.
- The function $y - p(x)$ has different order at $\infty^+$ and $\infty^-$ if and only if the leading term of $p$ is $F_{2g+2}^{1/2} x^{g+1}$.

## Composition and reduction

- If the divisor $D = \mathrm{div}(u, v)$ has degree at most $g + 1$, then reduction using $y - v(x)$ does not work.
- For instance if $D$ has degree $g + 1$, then $\deg(v) \leq g$, so $v^2 - F$ will have $2g + 2$ affine zeros, and we get another divisor of degree $g + 1$.
- We have cancelation in $v^2 - F$ if and only if the leading term of $p$ is $F_{2g+2}^{1/2} x^{g+1}$.
- The function $y - p(x)$ has different order at $\infty^+$ and $\infty^-$ if and only if the leading term of $p$ is $F_{2g+2}^{1/2} x^{g+1}$.

## Composition and reduction

- If the divisor $D = \mathrm{div}(u, v)$ has degree at most $g+1$, then reduction using $y - v(x)$ does not work.
- For instance if $D$ has degree $g+1$, then $\deg(v) \leq g$, so $v^2 - F$ will have $2g+2$ affine zeros, and we get another divisor of degree $g+1$.
- We have cancelation in $v^2 - F$ if and only if the leading term of $p$ is $F_{2g+2}^{1/2} x^{g+1}$.
- The function $y - p(x)$ has different order at $\infty^+$ and $\infty^-$ if and only if the leading term of $p$ is $F_{2g+2}^{1/2} x^{g+1}$.

### This motivates

Let $H^+(x)$ be the polynomial with leading term $F_{2g+2}^{1/2}x^{g+1}$ such that $(H^+)^2 - F$ has minimal degree. Given $D = \mathrm{div}(u, v)$ of degree at most $g + 1$, use the polynomial

$$p(x) = H^+ + (v - H^+ \mod u)$$

to perform a reduction (This is a red$_\infty$ step).

### Generically

- If $D_0$ has degree $g$, then typically $[D_0] = [D_1 + (\infty^+ - \infty^-)]$.
- If $D_0$ has degree $g + 1$, then typically $[D_0] = [D_1 + \infty^+]$.

## This motivates

Let $H^+(x)$ be the polynomial with leading term $F_{2g+2}^{1/2}x^{g+1}$ such that $(H^+)^2 - F$ has minimal degree. Given $D = \mathrm{div}(u,v)$ of degree at most $g+1$, use the polynomial

$$p(x) = H^+ + (v - H^+ \mod u)$$

to perform a reduction (This is a red$_\infty$ step).

## Generically

- If $D_0$ has degree $g$, then typically $[D_0] = [D_1 + (\infty^+ - \infty^-)]$.
- If $D_0$ has degree $g+1$, then typically $[D_0] = [D_1 + \infty^+]$.

## This motivates

Let $H^+(x)$ be the polynomial with leading term $F_{2g+2}^{1/2}x^{g+1}$ such that $(H^+)^2 - F$ has minimal degree. Given $D = \mathrm{div}(u,v)$ of degree at most $g+1$, use the polynomial

$$p(x) = H^+ + (v - H^+ \mod u)$$

to perform a reduction (This is a $\mathrm{red}_\infty$ step).

## Generically

- If $D_0$ has degree $g$, then typically $[D_0] = [D_1 + (\infty^+ - \infty^-)]$.
- If $D_0$ has degree $g+1$, then typically $[D_0] = [D_1 + \infty^+]$.

## This motivates

Let $H^+(x)$ be the polynomial with leading term $F_{2g+2}^{1/2}x^{g+1}$ such that $(H^+)^2 - F$ has minimal degree. Given $D = \mathrm{div}(u, v)$ of degree at most $g+1$, use the polynomial

$$p(x) = H^+ + (v - H^+ \mod u)$$

to perform a reduction (This is a $\mathrm{red}_\infty$ step).

## Generically

- If $D_0$ has degree $g$, then typically $[D_0] = [D_1 + (\infty^+ - \infty^-)]$.
- If $D_0$ has degree $g+1$, then typically $[D_0] = [D_1 + \infty^+]$.

## Generical addition for even genus

- Given $[D_1 - D_\infty]$ and $[D_2 - D_\infty]$ find the Mumford representation of $D_1 + D_2$.
- Reduce until $[D_1 + D_2] = [D_3 + (g/2)(\infty^+ + \infty^-)]$.
- This is equivalent to $[D_1 - D_\infty] + [D_2 - D_\infty] = [D_3 - D_\infty]$.

## Generical addition for even genus

- Given $[D_1 - D_\infty]$ and $[D_2 - D_\infty]$ find the Mumford representation of $D_1 + D_2$.
- Reduce until $[D_1 + D_2] = [D_3 + (g/2)(\infty^+ + \infty^-)]$.
- This is equivalent to $[D_1 - D_\infty] + [D_2 - D_\infty] = [D_3 - D_\infty]$.

## Generical addition for even genus

- Given $[D_1 - D_\infty]$ and $[D_2 - D_\infty]$ find the Mumford representation of $D_1 + D_2$.
- Reduce until $[D_1 + D_2] = [D_3 + (g/2)(\infty^+ + \infty^-)]$.
- This is equivalent to $[D_1 - D_\infty] + [D_2 - D_\infty] = [D_3 - D_\infty]$.

## Odd genus

- Given $[D_1 - D_\infty]$ and $[D_2 - D_\infty]$ find the Mumford representation of $D_1 + D_2$.
- Reduce until $[D_1 + D_2] = [D_3' + (g-1)/2(\infty^+ + \infty^-)]$.
- Use composition-and-reduction to get $[D_3'] = [D_3 + \infty^+]$.
- Now $[D_1 + D_2] = [D_3' + (g+1)/2\infty^+ + (g-1)/2\infty^-]$.
- This is equivalent to $[D_1 - D_\infty] + [D_2 - D_\infty] = [D_3 - D_\infty]$.

## Odd genus

- Given $[D_1 - D_\infty]$ and $[D_2 - D_\infty]$ find the Mumford representation of $D_1 + D_2$.
- Reduce until $[D_1 + D_2] = [D_3' + (g-1)/2(\infty^+ + \infty^-)]$.
- Use composition-and-reduction to get $[D_3'] = [D_3 + \infty^+]$.
- Now $[D_1 + D_2] = [D_3' + (g+1)/2\infty^+ + (g-1)/2\infty^-]$.
- This is equivalent to $[D_1 - D_\infty] + [D_2 - D_\infty] = [D_3 - D_\infty]$.

## Odd genus

- Given $[D_1 - D_\infty]$ and $[D_2 - D_\infty]$ find the Mumford representation of $D_1 + D_2$.
- Reduce until $[D_1 + D_2] = [D_3' + (g-1)/2(\infty^+ + \infty^-)]$.
- Use composition-and-reduction to get $[D_3'] = [D_3 + \infty^+]$.
- Now $[D_1 + D_2] = [D_3' + (g+1)/2\infty^+ + (g-1)/2\infty^-]$.
- This is equivalent to $[D_1 - D_\infty] + [D_2 - D_\infty] = [D_3 - D_\infty]$.

## Odd genus

- Given $[D_1 - D_\infty]$ and $[D_2 - D_\infty]$ find the Mumford representation of $D_1 + D_2$.
- Reduce until $[D_1 + D_2] = [D_3' + (g-1)/2(\infty^+ + \infty^-)]$.
- Use composition-and-reduction to get $[D_3'] = [D_3 + \infty^+]$.
- Now $[D_1 + D_2] = [D_3' + (g+1)/2\infty^+ + (g-1)/2\infty^-]$.
- This is equivalent to $[D_1 - D_\infty] + [D_2 - D_\infty] = [D_3 - D_\infty]$.

## In the olden days

Previous authors used the base divisor $D_\infty = g\infty^+$ instead of the "balanced" divisor we proposed. We will show that this is slower than our approach.

## In the even genus case

Using a a balanced representation, we finished when we found $D_4$ such that

$$D_1 + D_2 \equiv D_4 + \frac{g}{2}(\infty^+ + \infty^-).$$

If we wanted to use $D_\infty = g\infty^+$ instead, we'd get

$$[D_1 - D_\infty] + [D_2 - D_\infty] = [D_4 - D_\infty] + \frac{g}{2}(\infty^- - \infty^+),$$

so $g/2$ extra $\mathrm{red}_\infty$ steps are needed to finish.

## In the even genus case

Using a a balanced representation, we finished when we found $D_4$ such that

$$D_1 + D_2 \equiv D_4 + \frac{g}{2}(\infty^+ + \infty^-).$$

If we wanted to use $D_\infty = g\infty^+$ instead, we'd get

$$[D_1 - D_\infty] + [D_2 - D_\infty] = [D_4 - D_\infty] + \frac{g}{2}(\infty^- - \infty^+),$$

so $g/2$ extra $\mathrm{red}_\infty$ steps are needed to finish.

## In the even genus case

Using a a balanced representation, we finished when we found $D_4$ such that

$$D_1 + D_2 \equiv D_4 + \frac{g}{2}(\infty^+ + \infty^-).$$

If we wanted to use $D_\infty = g\infty^+$ instead, we'd get

$$[D_1 - D_\infty] + [D_2 - D_\infty] = [D_4 - D_\infty] + \frac{g}{2}(\infty^- - \infty^+),$$

so $g/2$ extra $\mathrm{red}_\infty$ steps are needed to finish.

## In the odd genus case

Usinga a balanced representation, we finished when we found $D_4$ such that

$$D_1 + D_2 \equiv D_4 + \frac{g+1}{2}\infty^+ + \frac{g-1}{2}\infty^-.$$

If we wanted to use $D_\infty = g\infty^+$ instead, we'd get

$$[D_1 - D_\infty] + [D_2 - D_\infty] = [D_4 - D_\infty] + \frac{g-1}{2}(\infty^- - \infty^+),$$

so $(g-1)/2$ extra $\mathrm{red}_\infty$ steps are needed to finish.

## In the odd genus case

Usinga a balanced representation, we finished when we found $D_4$ such that

$$D_1 + D_2 \equiv D_4 + \frac{g+1}{2}\infty^+ + \frac{g-1}{2}\infty^-.$$

If we wanted to use $D_\infty = g\infty^+$ instead, we'd get

$$[D_1 - D_\infty] + [D_2 - D_\infty] = [D_4 - D_\infty] + \frac{g-1}{2}(\infty^- - \infty^+),$$

so $(g-1)/2$ extra $\mathrm{red}_\infty$ steps are needed to finish.

## In the odd genus case

Usinga a balanced representation, we finished when we found $D_4$ such that

$$D_1 + D_2 \equiv D_4 + \frac{g+1}{2}\infty^+ + \frac{g-1}{2}\infty^-.$$

If we wanted to use $D_\infty = g\infty^+$ instead, we'd get

$$[D_1 - D_\infty] + [D_2 - D_\infty] = [D_4 - D_\infty] + \frac{g-1}{2}(\infty^- - \infty^+),$$

so $(g-1)/2$ extra $\mathrm{red}_\infty$ steps are needed to finish.

## Divisor inversion

It is important to be able to invert elements in a group (window methods, signed representations, etc).

Using our representation, this can be done with 0 or 1 $\mathrm{red}_\infty$ steps.

- If the genus is even, then $D_\infty = \overline{D_\infty}$.
- If the genus is odd, then $D_\infty = \overline{D_\infty} + (\infty^+ - \infty^-)$.

Using $g\infty^+$ as base divisor, it takes $g$ applications of $\mathrm{red}_\infty$.

- If $D_\infty = g\infty^+$, then $D_\infty = \overline{D_\infty} + g(\infty^+ - \infty^-)$.

## Divisor inversion

It is important to be able to invert elements in a group (window methods, signed representations, etc).
Using our representation, this can be done with 0 or 1 $\mathrm{red}_\infty$ steps.

- If the genus is even, then $D_\infty = \overline{D_\infty}$.
- If the genus is odd, then $D_\infty = \overline{D_\infty} + (\infty^+ - \infty^-)$.

Using $g\infty^+$ as base divisor, it takes $g$ applications of $\mathrm{red}_\infty$.

- If $D_\infty = g\infty^+$, then $D_\infty = \overline{D_\infty} + g(\infty^+ - \infty^-)$.

## Divisor inversion

It is important to be able to invert elements in a group (window methods, signed representations, etc).
Using our representation, this can be done with 0 or 1 $\mathrm{red}_\infty$ steps.

- If the genus is even, then $D_\infty = \overline{D_\infty}$.
- If the genus is odd, then $D_\infty = \overline{D_\infty} + (\infty^+ - \infty^-)$.

Using $g\infty^+$ as base divisor, it takes $g$ applications of $\mathrm{red}_\infty$.

- If $D_\infty = g\infty^+$, then $D_\infty = \overline{D_\infty} + g(\infty^+ - \infty^-)$.

## Comparison

In a genus 2 curve if $S = M$ and $I = 4M$ then balanced representations give a saving of around 15% for addition and 13% for doubling (if $I = 30M$ the savings become 62% and 58% respectively).

| | Imaginary | Balanced | Non-balanced |
|---|---|---|---|
| Addition | 1I, 2S, 22M | 1I, 2S, 26M | 2I, 4S, 30M |
| Doubling | 1I, 5S, 22M | 1I, 4S, 28M | 2I, 6S, 32M |
| Inversion | 0 | 0 | 2I, 4S, 8M |

Table: Operation counts for genus 2 arithmetic.

## Remarks

- The analogue of a baby-step in the imaginary model is addition of $P - \infty$.
- If the genus is even and the points at infinity are not rational, baby-steps are not necessary.
- Implemented in Magma V2.12, July 2005.
- One can efficiently implement pairings on hyperelliptic curves given by a real model (upcoming article with S. Galbraith and X. Lin ).

## Remarks

- The analogue of a baby-step in the imaginary model is addition of $P - \infty$.
- If the genus is even and the points at infinity are not rational, baby-steps are not necessary.
- Implemented in Magma V2.12, July 2005.
- One can efficiently implement pairings on hyperelliptic curves given by a real model (upcoming article with S. Galbraith and X. Lin ).

## Remarks

- The analogue of a baby-step in the imaginary model is addition of $P - \infty$.
- If the genus is even and the points at infinity are not rational, baby-steps are not necessary.
- Implemented in Magma V2.12, July 2005.
- One can efficiently implement pairings on hyperelliptic curves given by a real model (upcoming article with S. Galbraith and X. Lin ).

## Remarks

- The analogue of a baby-step in the imaginary model is addition of $P - \infty$.
- If the genus is even and the points at infinity are not rational, baby-steps are not necessary.
- Implemented in Magma V2.12, July 2005.
- One can efficiently implement pairings on hyperelliptic curves given by a real model (upcoming article with S. Galbraith and X. Lin ).

## Questions?

Thank you for your attention