General Purpose Divisor Arithmetic Over Genus 2 Hyperelliptic Curves

---

Sebastian Lindner

Supervisor: Michael Jacobson

Motivation

Develop general purpose arithmetic in the Picard group over genus 2 hyperelliptic curves that is as efficient as possible.

We create new explicit formulas in terms of finite field operations to achieve this.

Some Applications

Algebra:

- General purpose algebra systems. (Sage,Magma,...)

Number Theory:

- Genus 2 and 3 analogs of the Sato-Tate conjecture that were originally formulated in the context of elliptic curves.

Our Contributions

Explicit formulas for computing general purpose divisor arithmetic over genus 2 ramified and split hyperelliptic curves.

- Explicit formulas work for any curve over any field.
- Require the least number of field operations all cases.
- Also specialized for characteristic 2 or not 2 fields

Setting - Hyperelliptic Curves

- Let C be described by the hyperelliptic equation

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

  C is a hyperelliptic curve over an algebraically closed field $\overline{k}$ when C is irreducible, and non singular over $\overline{k}$.

- C is a genus 2 curve when $Deg(f) = 5$ or $Deg(f) = 6$ and $Deg(h) \leq 3$

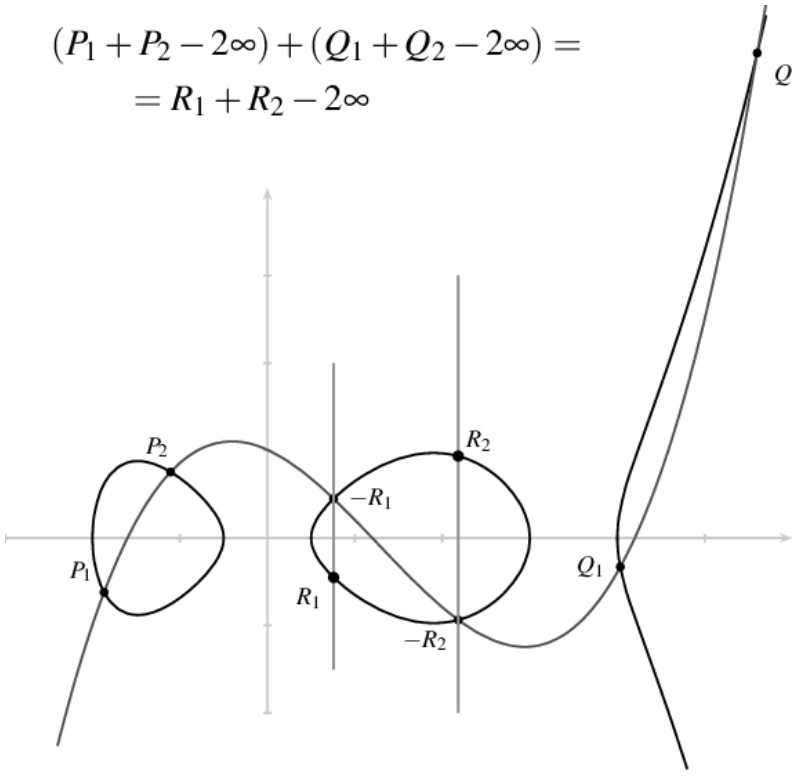
Setting - Ramified and Split Models

Generally:

- If $Deg(f) = 5$ then C is "ramified" and has one point at ∞.
- If $Deg(f) = 6$ then C has either 2 or 0 points at ∞.
  - If f_6 is a square when $h(x) = 0$ or $f_6 = s^2 + s$ for $s \in \overline{k}$ then C is "split" and has two points at infinity ∞_+, ∞_-
  - Otherwise C is "inert" and has no points at infinity.

Setting - Picard Group

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



- We use $Pic^0(C)$ the Picard group or degree zero divisor class group as our setting.

Unique Representations

Theorem

Let D_∞ be a rational degree 2 divisor and let $D \in Pic^0(C)$ be a divisor on the hyperelliptic curve C.

Then the divisor class $[D]$ has a unique representative in the Picard group of C of the form $[D_e - D_\infty]$, where D_e has no negative point coefficients and $deg(D_e) \leq 2$.

If C is **ramified**, then let $D_\infty = 2\infty$

If C is **split**, then let $D_\infty = \infty_+ + \infty_-$, and a "balanced representation" can be used, where n the number of extra copies of ∞_+ in D_e is kept track off, and $0 \leq n \leq 2$.

If C is **inert**, no unique representation for divisor classes has been figured out yet.

Mumford Representation

Let D_a be the affine part of D_e.

D_a portion of a divisor class can be represented with two polynomial $[u, v]$ where:

- u relates to the x-coordinates of points in the support of D
- $deg(v) < deg(u)$ where $u \mid f - vh(x) - v^2$ exactly. (meaning v interpolates the points)
- representation is unique when $deg(u) \leq 2$

What about infinite parts?

Ramified curves: The infinite part of D_e does not need adjustments and D_a is a unique representation of $[D]$.

Split curves: D_a is not unique by previous theorem.

- Sometimes requires adjustments by ∞_+ or ∞_- after composition to get $0 \leq n \leq 2$.
- Using $D_\infty = \infty_+ + \infty_-$ guarantees no adjustments are needed when computing typical composition of full degree divisors.
- Furthermore, a minimal number of adjustments are required for non-typical compositions.

Polynomial Algorithms for Composition

For $[u_{1+2}, v_{1+2}] = [u_1, v_1] + [u_2, v_2]$:

Compose:

- Compute $u' = u_1 u_2$, and v' where v' interpolates points of u'.

Reduce:

- v' intersects C at extra points, so

$$u_{1+2} = (f - hv' - (v')^2)/u', \quad v_{1+2} = -v' - h \mod u_{1+2}$$

Approaches:

- Cantor's: Requires a GCD computation to find polynomial s such that $su + v = v'$.
- Geometric: Solve a $g \times g$ system of equations to find v'.
- Otherwise approaches are similar, the costs differ based on pre-computed values.

Our Approach

Hybrid: We solve a linear system of equations to compute s instead of using GCD in Cantor's composition allowing to skip a direct computation of v'.

Results in:

- Reuse of computations from solving s, makes skipping direct computation of v' viable, saving additions/multiplications.
- Varying improvements apply to both ramified and split curves.

General Purpose Considerations

Cases: Dedicated explicit formulas are required for:

- Typical cases (doubling, addition, tripling and double-add)
- Non-typical cases of composing degenerate divisors and,
- Non-typical cases where there is a non-trivial intersection between the affine supports

Over split curves, we explicitly combine adjustments with composition for degenerate and non trivial intersection cases.

Results

Our ramified curve formulas have the same or lower field operation counts in all cases.

Our split curve formulas thus far also improve on previous best.

We are first to analyze addition counts. Field operations are denoted by:

- M = multiplications,
- S = squares,
- A = additions,
- C = curve constant multiplications

Non-typical cases occur rarely, we do not include these in the tables.

Ramified Curve Typical Cases

Any Characteristic																
	DBL				ADD				DA				TRPL			
Previous Work	**M**	**S**	**A**	**C**	**M**	**S**	**A**	**C**	**M**	**S**	**A**	**C**	**M**	**S**	**A**	**C**
Lange(2005)	23	5	52	3	22	3	41	-	-	-	-	-	-	-	-	-
This work	21	5	47	3	21	2	33	-	51	7	65	2	49	7	78	3
Not Even Characteristic																
	DBL				ADD				DA				TRPL			
Previous Work	**M**	**S**	**A**	**C**	**M**	**S**	**A**	**C**	**M**	**S**	**A**	**C**	**M**	**S**	**A**	**C**
Lange(2005)	22	5	32	-	22	3	32	-	-	-	-	-	-	-	-	-
Fan(2007)	-	-	-	-	-	-	-	-	56	7	54	-	-	-	-	-
Costello(2012)**	20	6	41	-	18	4	32	-	-	-	-	-	-	-	-	-
This work	21	5	26	-	21	2	24	-	49	5	45	-	47	7	48	-
Even Characteristic																
	DBL				ADD				DA				TRPL			
Previous Work	**M**	**S**	**A**	**C**	**M**	**S**	**A**	**C**	**M**	**S**	**A**	**C**	**M**	**S**	**A**	**C**
Lange(2005)	22	5	33	1	22	3	33	-	-	-	-	-	-	-	-	-
This work	20	5	27	1	20	3	27	-	47	6	47	2	45	7	47	3

Split Curve Typical Cases

Any Characteristic								
	DBL				**ADD**			
Previous Work	**M**	**S**	**A**	**C**	**M**	**S**	**A**	**C**
Jacobson(2010)	30	3	73	19	27	2	42	7
This work	30	3	67	19	27	2	39	7
Not Even Characteristic								
	DBL				**ADD**			
Previous Work	**M**	**S**	**A**	**C**	**M**	**S**	**A**	**C**
Jacobson(2010)	26	6	42	-	26	3	34	-
This work	26	6	37	-	24	4	33	-

Future Work

- Finish developing all split curve formulas.
- Graduate

Sorry

Sorry