Divisor Class Group Arithmetic on Non-hyperelliptic Genus 3 Curves

Evan MacNeil Michael J. Jacobson, Jr. Renate Scheidler

University of Calgary

macneil.evan@ucalgary.ca
jacobs@ucalgary.ca
rscheidl@ucalgary.ca

June 30, 2020

What We Did

- Produced fast explicit formulas fully describing $C_{3,4}$ curve arithmetic
- Formulas existed already for adding any two reduced divisors[1]
- Faster formulas existed, specialized to the "typical" case[2][3]
- We have improved upon both sets of formulas

[1] Arita, "An Addition Algorithm in Jacobian of $C_{3,4}$ Curve".

[2] F. Abu Salem and Khuri-Makdisi, "Fast Jacobian group operations for $C_{3,4}$ curves over a large finite field".

[3] Khuri-Makdisi, "On Jacobian group arithmetic for typical divisors on curves".

Why?

- Part of an ongoing project at UofC to fully describe divisor arithmetic on genus 3 curves
- Testing generalizations of elliptic curve conjectures to genus 3
  - Sato-Tate Conjecture
  - Birch and Swinnerton-Dyer Conjecture
  - and more ...
- L-series computations

Previous Work

Arita (2005)[4]

- Inputs: any two reduced divisors D, D'
- Output: the reduced divisor equivalent to $D + D'$
- Represent a divisor by the reduced Gröbner basis (RGB) of a polynomial ideal
- Classification of divisors of degree ≤ 6 into 20 types according to their RGB
- Very general, assumes $K = \mathbb{F}_q$ is large
- Might not terminate for some very small q
- Slow, computes redundant or unnecessary values

[4] Arita, "An Addition Algorithm in Jacobian of $C_{3,4}$ Curve".

Previous Work

Flon et al. (2008, preprint in 2004)[5]

- Inputs: two reduced, "typical", disjoint divisors $D + D'$
- Output: the reduced divisor equivalent to $D + D'$, or `error`
- Assumes $K = \mathbb{F}_q$ is large and $\operatorname{char} K > 5$

Khuri-Makdisi and Abu Salem (2007)[6] and Khuri-Makdisi (2018)[7]

- Improvement over above, and with $\operatorname{char} K > 3$
- Represent a divisor by two ideal generators (not an RGB)
- Previous state-of-the-art for typical case

[5] Flon, Oyono, and Ritzenthaler, "Fast addition on non-hyperelliptic genus 3 curves".
[6] F. K. Abu Salem and Khuri-Makdisi, "Fast Jacobian Group Operations for C3,4 Curves over a Large Finite Field".
[7] Khuri-Makdisi, "On Jacobian group arithmetic for typical divisors on curves".

$C_{3,4}$ Curves

$C_{3,4}$ **curve**: a non-singular algebraic plane curve over a (perfect) field K defined by a polynomial

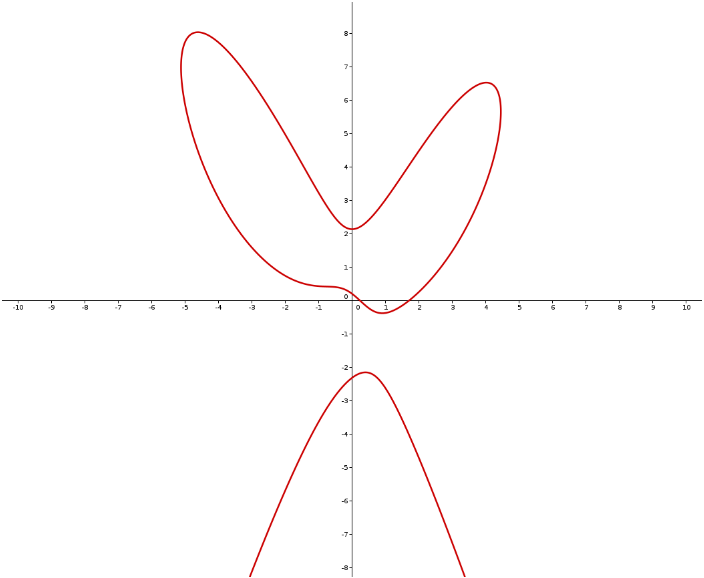
$$F = y^3 + x^4 + c_8xy^2 + c_7x^2y + c_6x^3 + c_5y^2 + c_4xy + c_3x^2 + c_2y + c_1x + c_0.$$

There is a single projective point $P_\infty = (0 : 1 : 0)$ "at infinity".

Short form in $\operatorname{char} K \neq 2, 3$:

$$F = y^3 + x^4 + c_7x^2y + c_4xy + c_3x^2 + c_2y + c_1x + c_0.$$

$C: y^3 + x^4 - 5x^2y + 2xy - x^2 - 5y - 4x + 1 = 0$ over $\mathbb{R}$



Divisors

- A divisor D on C is a formal sum of points that is fixed under Galois automorphisms on $\overline{K}$.
- In the (degree zero) divisor class group $\mathrm{Div}_K^0(C)$, every divisor is linearly equivalent to one of the form

$$D = P_1 + \cdots + P_n - nP_\infty,$$

  where the P_i's are finite points.
- For simplicity, we refer to $n = \deg(D)$ as its degree.
- A divisor is reduced if n is minimal in its class.
- Each class has a unique reduced divisor.

Operations on Divisors

$$\text{Divisor class group of } C \simeq \text{Ideal class group of } K[C]$$

$$D \longleftrightarrow I_D$$

Represent a divisor D by the unique RGB of I_D.

Divisor	$A+B$	$\operatorname{lcm}(A,B)$	$\gcd(A,B)$	$\overline{A}$
Ideal	$I_A I_B$	$I_A \cap I_B$	$I_A + I_B$	$\langle f_{I_A} \rangle : I_A$

where f_{I_A} is the "smallest" element in the RGB of I_A.

lcm and $\gcd$ satisfy

$$A + B = \operatorname{lcm}(A,B) + \gcd(A,B).$$

The reduction of A is $\overline{\overline{A}}$.

High-level Algorithm

Given ideals I_D and $I_{D'}$, to compute the ideal of the reduced divisor D'' equivalent to $D + D'$,

1. Compute a RGB for $J = I_D I_{D'}$.
2. Compute a RGB for $J^* = f_J : J$.
3. Compute a RGB for $J^{**} = f_{J^*} : J^*$.

Then $J^{**} = I_{D''}$.

One can do two flips for less than the cost of one![8]

[8] Khuri-Makdisi, "On Jacobian group arithmetic for typical divisors on curves".

Addition

We generalize the previous state of the art to non-disjoint divisors.

- Khuri-Makdisi : $D + D'$ is retrieved by computing the kernel of a quotient of Riemann-Roch spaces.
- This works when D and D' are disjoint.
- More generally, the kernel gives $\mathrm{lcm}(D, D')$
- We handle non-disjoint cases by also computing $\gcd(D, D')$ via the image of the quotient and recursively computing

$$D + D' \equiv \overline{\overline{\mathrm{lcm}(D, D')}} + \gcd(D, D').$$

- We show that this recursion terminates.

Addition

We generalize to handle atypical divisors as well.

- We allow the size of the Riemann-Roch spaces to vary.
- Lower degree divisors may be represented by smaller spaces.
- Atypical divisors require larger spaces, relative to their degree.
- We derived explicit formulas for all atypical cases, including over finite fields of characteristic 2 and 3.

Addition

We also get runtime improvements in the typical case:

- We avoid computing two unnecessary values.
- We use an additional polynomial to represent I_D, a time-space tradeoff.
- We save an inversion operation at the cost of some multiplications.

Doubling and Reducing

Doubling:

- The addition framework fails when adding identical divisors, $D + D$.
- We show how to find a suitable divisor $A \equiv D$ and add $D + A$ instead.
- A is quickly computed thanks to our RGB representation.
- All cases, including atypical cases and $\mathrm{char}\, K = 2, 3$, are handled explicitly.

Reducing:

- Khuri-Makdisi[9] shows how to efficiently reduce a typical degree 6 divisor.
- We generalize this to all divisors.

[9] Khuri-Makdisi, "On Jacobian group arithmetic for typical divisors on curves".

Improvements over Prior Work

Assuming $\mathrm{char}\, K > 5$, typical case

	Addition				Doubling			
	I	M	S	A	I	M	S	A
Arita	5	204	–	–	5	284	–	–
Flon et al.	2	148	15	–	2	165	20	–
Khuri-Makdisi	2	97	1	132	2	107	3	155
This work	1	111	3	99	1	127	4	112

Benchmark Methodology

We implemented our and Khuri-Makdisi's formulas in Sage and ran benchmark tests to see how many divisors each set of formulas could compute in 10 minutes.

Fix a prime p and randomly choose a $C_{3,4}$ curve C over $\mathbb{F}_p$. Randomly choose two divisors A, B on C.

Addition benchmark:

- Compute the Fibonacci-like sequence $D_1 = A$, $D_2 = B$, $D_{i+2} = D_{i+1} + D_i$, $i \geq 1$.

Doubling benchmark:

- Compute the sequence $D_1 = A$, $D_{i+i} = 2D_i$, $i \geq 1$.

Benchmark Results

We ran these benchmarks over several curves over byte-sized, word-sized, and large primes and totaled the results.

		Additions (millions)			Doublings (millions)		
p	#Trials	Us	K-M	Speedup	Us	K-M	Speedup
$\approx 2^{8}$	10	53.67	31.69	69.38%	48.16	39.15	23.00%
$\approx 2^{32}$	23	126.31	112.04	12.74%	120.83	108.49	11.37%
$\approx 2^{255}$	11	63.15	52.19	21.01%	56.80	48.40	17.36%

Conclusion

Main contributions

- Combine ideas from Arita/Khuri-Makdisi/Abu Salem
- Generalize to atypical cases
- Improvement in typical case
- Relax assumptions on C to handle $\operatorname{char} K = 2, 3$.
- Neatly handle non-disjointness with lcm and $\gcd$

Future Work

- Still possible to eliminate an inversion in some atypical cases.
- Ongoing work at UofC shows Shank's NUCOMP algorithm achieves savings in genus 3 *hyperelliptic* curve arithmetic.
- Can something NUCOMP-like be applied to $C_{3,4}$ curve arithmetic?

Thank You

Details and Sage implementation available at
`github.com/emmacneil/c34-curves`

- Abu Salem, Fatima K. and Kamal Khuri-Makdisi. "Fast Jacobian Group Operations for C3,4 Curves over a Large Finite Field". In: *LMS Journal of Computation and Mathematics* 10 (2007), pp. 307–328.
- Abu Salem, Fatima and Kamal Khuri-Makdisi. "Fast Jacobian group operations for $C_{3,4}$ curves over a large finite field". In: *LMS Journal of Computation and Mathematics* 10 (Nov. 2006).
- Arita, Seigo. "An Addition Algorithm in Jacobian of $C_{3,4}$ Curve". In: *IEICE Trans. Fundamentals* E88-A, NO.6 (2005), pp. 1589–1598.
- Flon, Stephane, Roger Oyono, and Christophe Ritzenthaler. "Fast addition on non-hyperelliptic genus 3 curves". In: *Algebraic Geometry and Its Applications*, pp. 1–28.
- Khuri-Makdisi, Kamal. "On Jacobian group arithmetic for typical divisors on curves". In: *Research in Number Theory* 4.1 (Jan. 2018), p. 3. ISSN: 2363-9555.