Divisor Class Group Arithmetic on $C_{3,4}$ 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

Arita's Classification of Divisors[1]

Deg	Type	Gröbner Basis
0	0	1
1	11	$x + f_0$ $y + g_0$
2	21	$y + f_1x + f_0,$ $x^2 + g_1x + g_0$
	22	$x + f_0,$ $y^2 + g_2y + g_0$
3	31	$x^2 + f_2y + f_1x + f_0,$ $xy + g_2y + g_1x + g_0,$ $y^2 + h_2y + h_1x + h_0$
	32	$y + f_1x + f_0,$ $x^3 + g_3x^2 + g_1x + g_0$
	33	$x + f_0$
4	41	$xy + f_3x^2 + f_2y + f_1x + f_0,$ $y^2 + g_3x^2 + g_2y + g_1x + g_0,$ $x^3 + h_3x^2 + h_2y + h_1x + h_0$
	42	$x^2 + f_1x + f_0,$ $xy + g_2y + g_1x + g_0$
	43	$x^2 + f_2y + f_1x + f_0,$ $y^2 + g_4xy + g_2y + g_1x + g_0$
	44	$y + f_1x + f_0$

Deg	Type	Gröbner Basis
5	51	$y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0,$ $x^3 + g_4xy + g_3x^2 + g_2y + g_1x + g_0,$ $x^2y + h_4xy + h_3x^2 + h_2y + h_1x + h_0$
	52	$xy + f_3x^2 + f_2y + f_1x + f_0,$ $y^2 + g_3x^2 + g_2y + g_1x + g_0$
	53	$xy + f_3x^2 + f_2y + f_1x + f_0,$ $x^3 + g_5y^2 + g_3x^2 + g_2y + g_1x + g_0$
	54	$x^2 + f_2y + f_1x + f_0,$ $xy^2 + g_5y^2 + g_4xy + g_2y + g_1x + g_0$
6	61	$x^3 + f_5y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0,$ $x^2y + g_5y^2 + g_4xy + g_3x^2 + g_2y + g_1x + g_0,$ $xy^2 + h_5y^2 + h_4xy + h_3x^2 + h_2y + h_1x + h_0$
	62	$y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0,$ $x^3 + g_4xy + g_3x^2 + g_2y + g_1x + g_0$
	63	$y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0,$ $x^2y + g_6x^3 + g_4xy + g_3x^2 + g_2y + g_1x + g_0$
	64	$xy + f_3x^2 + f_2y + f_1x + f_0,$ $x^4 + g_6x^3 + g_5y^2 + g_3x^2 + g_2y + g_1x + g_0$
	65	$x^2 + f_2y + f_1x + f_0$

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

Riemann-Roch Spaces

Let D be a divisor and m a monomial in $K[C]$.
Define

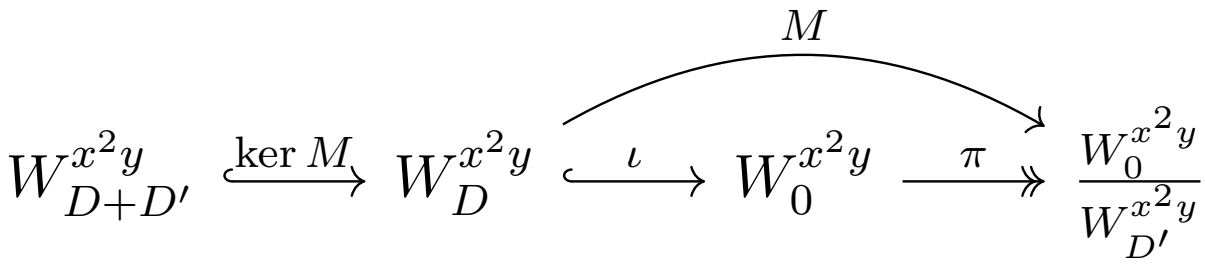
$$W_D^m := \mathcal{L}(-\operatorname{ord}_{P_\infty}(m)P_\infty - D) = \{f \in I_D \mid \operatorname{LM}(f) \leq m\}.$$

Given I_D and m, it is easy to find a basis for W_D^m.

Given W_D^m, it is easy to find generators for I_D (if m is sufficiently large).

Framework for Addition

Abu Salem/Khuri-Makdisi (2007)[2]: If D and D' are disjoint, typical, reduced divisors:



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

Framework for Addition

Generalization for any distinct reduced divisors D, D' and monomial m:

$$W_L^m \xhookrightarrow{\ker M} W_D^m \xhookrightarrow{\iota} W_0^m \xrightarrow{\pi} \frac{W_0^m}{W_{D'}^m} \xrightarrow{\text{im } M} \frac{W_G^m}{W_{D'}^m}$$

where $L = \text{lcm}(D, D')$ and $G = \gcd(D, D')$

In general $D + D' = L + G$. Return

$$D + D' \equiv \overline{\overline{L}} + G.$$

Addition Example

Consider the $C_{3,4}$ curve $C : y^3 + x^4 + 1 = 0$ over $\mathbb{F}_{11}$.
Let D, D' be the typical divisors

$$I_D = \langle f, g, h \rangle \qquad I_{D'} = \langle f', g', h' \rangle$$
$$f = x^2 + 3y + 7x + 5 \qquad f' = x^2 + 6y + 3x - 2$$
$$g = xy + 2y + 2x + 9 \qquad g' = xy + 5y + 5x + 9$$
$$h = y^2 + 4y + 2x + 3 \qquad h' = y^2 - y - x + 5.$$

Addition Example

$$W_D^{x^4} = \mathrm{Span}\{f, g, h, xf, xg, xh, x^2 f\}$$

$$W_{D'}^{x^4} = \mathrm{Span}\{f', g', h', xf', xg', xh', x^2 f'\}$$

Compute $f, g, h, \ldots$ modulo $f', g', h', \ldots$. E.g.

$$\begin{aligned} \overline{f} &= f - f' \\ &= 8y + 4x + 7 \end{aligned}$$

$$M = \begin{pmatrix} 7 & 0 & 9 & 2 & 10 & 5 & 2 \\ 4 & 8 & 3 & 10 & 2 & 8 & 6 \\ 8 & 8 & 5 & 2 & 0 & 1 & 7 \end{pmatrix}$$

Addition Example

$$M_{\mathsf{rref}} = \begin{pmatrix} 1 & 0 & 6 & 0 & 6 & 9 & 2 \\ 0 & 1 & 7 & 0 & 9 & 8 & 10 \\ 0 & 0 & 0 & 1 & 6 & 4 & 5 \end{pmatrix}$$

$$\ker M = \begin{pmatrix} -6 & -6 & -9 & -2 \\ -7 & -9 & -8 & -10 \\ 1 & 0 & 0 & 0 \\ 0 & -6 & -4 & -5 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$I_L = \left\langle \begin{array}{l} h - 7g - 6f, \\ xg - 6xf - 9g - 6f, \\ xh - 4xf - 8g - 9f, \\ x^2 f - 5xf - 10g - 2f \end{array} \right\rangle$$

Numeric Addition Example

$$I_L = \left\langle \begin{array}{l} h - 7g - 6f, \\ xg - 6xf - 9g - 6f, \\ xh - 4xf - 8g - 9f, \\ x^2 f - 5xf - 10g - 2f \end{array} \right\rangle$$

$$= \left\langle \begin{array}{l} y^2 + 4xy + 5x^2 + 5y + x - 2, \\ x^2 y + 5x^3 - 3xy - 2x^2 - 3y - 4x - 1, \\ \cancel{xy^2 - 4x^3 - 5xy - 2x^2 + y + 3x + 4,} \\ \cancel{x^4 + 3x^2 y + 2x^3 - 3xy + x^2 - 4y - 4x - 1} \end{array} \right\rangle$$

L is a type 63 divisor.

Reduction Example

Recall $F = y^3 + x^4 + 1$ was the curve polynomial.

$$I_L = \left\langle \begin{array}{l} y^2 + 4xy + 5x^2 + 5y + x - 2, \\ x^2y + 5x^3 - 3xy - 2x^2 - 3y - 4x - 1 \end{array} \right\rangle$$
$$= \langle u, v \rangle$$

Generators for $\overline{\overline{L}}$ are known to have leading monomials y, x^2. Let

$$f'' = y + f_1''x + f_0''$$
$$g'' = x^2 + g_2''y + g_1''x + g_0''$$

and solve

$$f''v - g''u + g_2''F = 0.$$

Reduction Example

Equating coefficients gives a system of equations

$$\begin{aligned}
f_1'' &= -1 \\
g_2'' &= -5f_1'' + 5 && = -1 \\
g_1'' &= -4g_2'' - 3 && = 1 \\
f_0'' &= 3f_1'' + 4g_1'' + 5g_2'' + 7 && = 3 \\
g_0'' &= -5g_2'' - 3 && = 2
\end{aligned}$$

and

$$\begin{aligned}
I_{\overline{\overline{L}}} &= \left\langle y - x + 3,\ x^2 - y + x + 2 \right\rangle \\
&= \left\langle y - x + 3,\ x^2 + 5 \right\rangle .
\end{aligned}$$

Addition Formulas

First, compute the matrix M.
The right-most columns can be filled in later if we need them.

$$M = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & * & * \\ a_8 & a_9 & a_{10} & a_{11} & a_{12} & * & * \\ a_{15} & a_{16} & a_{17} & a_{18} & a_{19} & * & * \end{pmatrix}$$

$$\begin{array}{llll} a_1 = f_0 - f_0' & \dots & a_4 = -f_0' a_8 - g_0' a_{15} & \dots \\ a_8 = f_1 - f_1' & \dots & a_{11} = a_1 - f_1' a_8 - g_1' a_{15} & \dots \\ a_{15} = f_2 - f_2' & \dots & a_{18} = -f_1' a_8 - g_2' a_{15} & \dots \end{array}$$

Requires 18M+21A. Strassen's technique may also be applied.

Addition Formulas

$$M \to \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & * & * \\ 0 & b_1 & b_2 & b_3 & b_4 & * & * \\ 0 & b_7 & b_8 & b_9 & b_{10} & * & * \end{pmatrix}$$

$$\to \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & * & * \\ 0 & b_1 & b_2 & b_3 & b_4 & * & * \\ 0 & 0 & c_1 & c_2 & c_3 & * & * \end{pmatrix} = M_{\mathsf{ref}}$$

$$b_1 = a_1a_9 - a_2a_8 \qquad c_1 = b_1b_8 - b_2b_7$$

$$b_2 = a_1a_{10} - a_3a_8 \qquad c_2 = b_1b_9 - b_3b_7$$

$$\ldots = \ldots \qquad \ldots = \ldots$$

Requires 22M+11A

Addition Formulas

Supposing $a_1, b_1 \neq 0$ and $c_1 = 0$,

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & * & * \\ 0 & b_1 & b_2 & b_3 & b_4 & * & * \\ 0 & 0 & 0 & c_2 & c_3 & * & * \end{pmatrix} \to \begin{pmatrix} 1 & 0 & -r_0 & 0 & -s_0 & * & * \\ 0 & 1 & -r_1 & 0 & -s_1 & * & * \\ 0 & 0 & 0 & 1 & -s_2 & * & * \end{pmatrix} = M_{\mathsf{rref}}$$

$$\begin{aligned} A &= a_1 b_1 & s2 &= -\gamma c_3 \\ B &= A c_2 & r1 &= -\beta b_2 \\ \delta &= 1/B & s1 &= -\beta(b_3 s_2 + b_4) \\ \alpha &= \delta b_1 c_2 & r0 &= -\alpha(a_2 r_1 + a_3) \\ \beta &= \delta a_1 c_2 & s0 &= -\alpha(a_2 s_1 + a_4 s_2 + a_5) \\ \gamma &= \delta A \end{aligned}$$

Requires 1I+16M+4A

Additions Formulas

The $I_L = \langle u, v \rangle$ where

$$u = h + r_1 g + r_0 f \qquad = y^2 + u_4 xy + \cdots + u_0$$
$$v = xg + s_2 xf + s_1 g + s_0 f \qquad = x^2 y + v_6 x^3 + v_4 xy + \cdots + v_0$$

$$u_0 = f_0 r_0 + g_0 r_1 + h_0 \qquad v_0 = f_0 s_0 + g_0 s_1$$
$$u_1 = f_1 r_0 + g_1 r_1 + h_1 \qquad v_1 = f_1 s_0 + g_1 s_1 + f_0 s_2 + g_0$$
$$u_2 = f_2 r_0 + g_2 r_1 + h_2 \qquad v_2 = f_2 s_0 + g_2 s_1$$
$$u_3 = r_0 \qquad v_3 = s_0 + f_1 s_2 + g_1$$
$$u_4 = r_1 \qquad v_4 = s_1 + f_2 s_2 + g_2$$
$$v_6 = s_2$$

Requires 6M+7A

Solving $f''v - g''u + g_2''F = 0$

Let $f'' = y + f_1''x + f_0''$ and $g'' = x^2 + g_2''y + g_1''x + g_0''$. Equating coefficients in $f''v - g''u - g_2F = 0$ gives the system

$$
\begin{aligned}
(x^3y) \quad & f_1 - u_4 + v_6 = 0 \\
(x^4) \quad & f_1v_6 + g_2 - u_3 = 0 \\
(xy^2) \quad & c_8g_2 - g_2u_4 - g_1 + v_4 = 0 \\
(x^2y) \quad & c_7g_2 - g_2u_3 - g_1u_4 + f_1v_4 + f_0 - u_2 + v_3 = 0 \\
(y^2) \quad & c_5g_2 - g_2u_2 - g_0 + v_2 = 0
\end{aligned}
$$

and 6 more equations.

Total: 1I+70M+61A, after reducing g'' modulo f''.

Thank You

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

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.

Possible Discussion

- How common are $C_{3,4}$ curves in the wild?
- Relative costs of field operations
- Future Work (NUCOMP?)