DIVISOR CLASS GROUP ARITHMETIC ON NON-HYPERELLIPTIC GENUS 3 CURVES

EVAN MACNEIL, MICHAEL J. JACOBSON JR. AND RENATE SCHEIDLER

Abstract. We present novel explicit formulas for arithmetic in the divisor class group of a $C_{3,4}$ curve. Our formulas handle all cases of inputs and outputs without having to fall back on a generic method. We also improve on the most commonly occurring case by reducing the number of required field inversions to one at the cost of a small number of additional field operations, resulting in running times that are between 11 and 21% faster than the prior state-of-the-art depending on the field size, and even more for small field sizes when non-typical cases frequently arise.

1. Introduction

Computing in the divisor class group of an algebraic curve is a non-trivial component in computing L-series. L-series in turn are at the heart of the Sato-Tate conjecture and related conjectures. The Sato-Tate conjecture has been proved for elliptic curves with complex multiplication, but its analogues for other classes of algebraic curves remains open [14]. In order to test these conjectures for other curve families, it is desirable to have efficient algorithms to perform divisor class group arithmetic; see, for example, [7], [6], and [13].

Fast explicit formulas exist to perform divisor class group arithmetic for genus 1 and genus 2 curves. However, the picture for genus 3 curves is incomplete. Existing explicit formulas for arithmetic on the non-hyperelliptic genus 3 curves, the $C_{3,4}$ curves, were developed with cryptographic applications in mind, where the curves are defined over very large finite fields of characteristic greater than 3. A $C_{3,4}$ curve over such a field is isomorphic to one given by a short-form equation (see §2), yielding faster arithmetic. Moreover, with very high probability, one will only encounter "typical" divisors (see §2) and many degenerate cases need not be considered. When these assumptions are violated, one may fall back on slower divisor addition algorithms that work on any algebraic curve.

In [2], Arita specialized the algorithm for addition in the class group of a general $C_{a,b}$ curve in [1] to the $C_{3,4}$ case. He classified divisors of $C_{3,4}$ curves into 19 types based on the forms of their Gröbner bases representations. The method allows addition of divisors of any type, although it handles this in a recursive manner that does not terminate for some curves over very small finite fields; Arita was predominantly interested in the cryptographic setting over a large finite field where this does not present a problem. However, number theoretic applications require extensive curve arithmetic over far smaller finite fields.

Other algorithms are less general but much faster. In [8], the most recent of these, Khuri-Makdisi, building upon the work of Flon *et al.* [4] and Abu Salem and Khuri-Makdisi [11] assumed a $C_{3,4}$ curve defined by a short-form polynomial equation.

In addition to restricting to disjoint divisors without multiple points, they assume that divisors being added or doubled are typical. They represent divisors by a pair of polynomials of minimal degree and obtain sums of divisors by computing kernels of maps between vector spaces. This yields the most efficient explicit formulas, describing the operation as an optimized sequence of field operations instead of via polynomial arithmetic or linear algebra, for the typical case. Thus, prior to our work herein, the state-of-the-art for $C_{3,4}$ curves was the addition and doubling procedures of [11] and the reduction method of [8]. Both of these are limited to typical divisors; and one had to resort to general arithmetic for all other cases.

Our contribution is to marry the methods of Abu Salem/Khuri-Makdisi — who have the fastest explicit formulas to date — with the methods of Arita — whose formulas are the most general — in order to produce fast and fully general explicit formulas that cover all cases of $C_{3,4}$ curve arithmetic. This approach is facilitated by the fact that Salem/Khuri-Makdisi's representation of typical divisors resembles type 31 divisors from Arita's classification. Our algorithms work in full generality: the curve may be defined over a field of any size and any characteristic, including 0, 2, and 3 (our implementation only extends to finite fields), the curve equation may be in long or short form (see Section 2), divisors may be typical or atypical, non-disjoint, and have multiple points, and all our algorithms provably terminate.

We extend the approach of [11] for finding the kernel of the aforementioned matrix to computing its image as well and are thus able to handle atypical and non-disjoint divisors. We also improve on the state-of-the-art of [8, 11] for typical divisors. Fully general algorithms for adding, doubling, and reducing divisors are presented in §3, §4 and §5, respectively. These algorithms are used to develop fast explicit formulas in §6 that handle the most typical cases arising in $C_{3,4}$ curve divisor arithmetic, specifically, adding/doubling disjoint typical divisors on a curve in short form over a field of characteristic greater than 3. The operation counts of these formulas are summarized in Table 1.1, where I, M, S, A refer to the number of field inversions, multiplications, squarings, and additions in the base field of the curve[1]. Our formulas improve on the prior state-of-the-art by requiring only a single field inversion at the cost of a sufficiently small number of other field operations. Experiments confirm an overall running time speed-up by approximately 11–21% depending on the size of the field. Our algorithms are also used to produce explicit formulas for all atypical cases, including non-disjoint or atypical divisors and curves of arbitrary form and in any characteristic. These cases are so numerous that we choose instead to publish them in the form of Sage code on GitHub [9] and present their operation counts in §7.

TABLE 1.1. Comparison of operation counts in prior work

	Add				Double			
	I	M	S	A	I	M	S	A
Arita [2]	5	204	–	–	5	284	–	–
Flon et al [4]	2	148	15	–	2	165	20	–
Khuri-Makdisi/Abu Salem [8, 11]	2	97	1	132	2	107	3	155
This work	1	111	3	99	1	127	4	112

[1] Arita did not distinguish between field multiplications and squarings, and neither Arita nor Flon *et al.* counted field additions in their work.

By improving upon the typical case and completing the picture for the atypical cases, our results will have a significant impact on number theoretic computations heavy on arithmetic in the divisor class group of a $C_{3,4}$ curve. As in [14] for example, one may wish to take a curve over $\mathbb{Q}$, reduce it modulo all primes up to some bound, and compute the order of the divisor class group of that reduced curve. The improvement in the typical case remains significant over all the computations, while the completion of the atypical cases becomes more significant over the smaller fields, where one frequently encounters these atypical cases.

2. Preliminaries

Let K be a perfect field. A $C_{3,4}$ curve is a non-singular non-hyperelliptic projective curve C of genus 3 whose affine model is given by $F(x, y) = 0$ where $F \in K[x, y]$ is of the form

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

We denote the unique point at infinity on C by P_∞. When K has characteristic 0 or at least 5, the curve isomorphism $(x, y) \mapsto (x - a/4, y - (c_8/3)x + (ac_8 - 4c_5)/3)$, $a = (27c_6 - 9c_7c_8 + 2c_8^3)/27$ over K transforms the polynomial F to the short form

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

Let $\mathrm{Div}_K^0(C)$ denote the group of degree zero divisors on C defined over K. Elements of $\mathrm{Div}_K^0(C)$ are of the form

$$D = \sum_{P \in C(\bar{K}) - \{P_\infty\}} \mathrm{ord}_P(D)P - nP_\infty \ , \qquad n = \sum_{P \in C(\bar{K}) - \{P_\infty\}} \mathrm{ord}_P(D) \ ,$$

where the sum defining D is fixed under Galois automorphisms on $\bar{K}$. For brevity, we identify D with its finite part and refer to $n = \deg(D)$ as its degree. A divisor D is *effective* if $\mathrm{ord}_P(D) \geq 0$ for all $P \in C(\bar{K}) - \{P_\infty\}$ and *reduced* if in addition n is minimal among the degrees of all the divisors in the linear equivalence class of D. If D is reduced, then $\deg(D) \leq 3$. Every element of $\mathrm{Div}_K^0(C)$ is linearly equivalent to an effective divisor and to a unique reduced divisor in $\mathrm{Div}_K^0(C)$.

For any two effective divisors $D, D' \in \mathrm{Div}_K^0(C)$, define

$$\mathrm{lcm}(D, D') = \sum_{P \in C(\bar{K}) - \{P_\infty\}} \max\{\mathrm{ord}_P(D), \mathrm{ord}_P(D')\}(P - P_\infty) \ ,$$

$$\gcd(D, D') = \sum_{P \in C(\bar{K}) - \{P_\infty\}} \min\{\mathrm{ord}_P(D), \mathrm{ord}_P(D')\}(P - P_\infty) \ .$$

Then $D + D' = \gcd(D, D') + \mathrm{lcm}(D, D')$.

There is a canonical isomorphism from $\mathrm{Div}_K^0(C)$ to the group of fractional $K[C]$-ideals, written as $D \mapsto I_D$, with inverse $I \mapsto \mathrm{div}(I)$. When D is effective, I_D is integral. If $g_1, g_2, \ldots \in K[C]$ are polynomials, then we write $\mathrm{div}(g_1, g_2, \ldots)$ in place of $\mathrm{div}(\langle g_1, g_2, \ldots \rangle)$.

In [2], Arita described a monomial order on $K[C]$ induced by the pole orders $\mathrm{ord}_{P_\infty}(x) = -3$ and $\mathrm{ord}_{P_\infty}(y) = -4$. Every ideal I of $K[C]$ has a unique reduced Gröbner basis with respect to this ordering that contains the *minimum polynomial* of I, i.e. the unique polynomial f_I in any Gröbner basis of I with the smallest leading monomial and leading coefficient 1. Under this isomorphism, we have the following correspondence between effective divisors and their associated $K[C]$-ideals:

Divisors	$D + D'$	$\operatorname{lcm}(D, D')$	$\gcd(D, D')$	$\overline{D}$	$D \leq D'$
Ideals	$I_D I_{D'}$	$I_D \cap I_{D'}$	$I_D + I_{D'}$	$f_{I_D} : I_D$	$I_D \supseteq I_{D'}$

Here, $f_{I_D} : I_D$ is the unique $K[C]$-ideal satisfying $I_D(f_{I_D} : I_D) = \langle f_{I_D} \rangle$, the principal ideal generated by f_{I_D}. The corresponding divisor $\overline{D} = \operatorname{div}(f_{I_D} : I_D)$ is the *flip* of D; it is equivalent to $-D$ and is reduced. It follows that D is reduced if and only if $D = \overline{\overline{D}}$, and $\overline{\overline{D}}$ is the *reduction* of D, i.e. the unique reduced divisor linearly equivalent to D. This gives rise to the following high-level algorithm for addition in the degree zero divisor class group of a $C_{3,4}$ curve, found also in [2]. Given two reduced divisors D and D', represented by the reduced Gröbner bases of their respective ideals I_D and $I_{D'}$, perform the following:

(1) Compute the reduced Gröbner basis of $J := I_D I_{D'}$.
(2) Compute the reduced Gröbner basis of $J^* := f_J : J$.
(3) Compute the reduced Gröbner basis of $J^{**} := f_{J^*} : J^*$.

Then $\operatorname{div}(J^{**})$ is the unique reduced divisor equivalent to $D + D'$. In [8], Khuri-Makdisi showed how to combine the last two steps into a single efficient step.

Following [8], an effective divisor D is said to be *semi-typical* if the reduced Gröbner basis of I_D consists of three polynomials, i.e. $I_D = \langle f, g, h \rangle$. A divisor is *typical* if it is semi-typical with $h \in \langle f, g \rangle$, where h is the generator with the largest pole order at infinity. A divisor that is not typical is called *atypical*. All typical divisors are semi-typical, but atypical divisors may or may not be semi-typical.

In [2], Arita classified all divisors of degree ≤ 6 into 19 types according to the leading monomials of their reduced Gröbner bases. Table 2.1 reproduces Arita's classification, along with a 20th type corresponding to the zero divisor. Note that a divisor of degree $d \leq 6$ is semi-typical if and only if it is of type 31, 41, 51, or 61, and a type 31 divisor D is typical if and only if f_2, the coefficient of y in f_{I_D}, is non-zero (see [8, Prop. 2.12]). The types of $\overline{D}$ and $\overline{\overline{D}}$ are determined by the type of D as summarized in Table 2.2. Examples of computing the type of $\overline{D}$ are found in §7.3 of [10]. A divisor is reduced if and only if it is of type 0, 11, 21, 22 or 31; in particular, all divisors of degree $d \leq 2$ are reduced.

3. Addition

In this section, we describe how to add two distinct reduced divisors. Analogous to [11], we make use of certain Riemann-Roch spaces. For any non-zero function $f \in K[C]$, denote by $\operatorname{LM}(f)$ the leading monomial of f. Let $m \in K[C]$ be a monomial and D an effective divisor in $\operatorname{Div}_K^0(C)$. Define

$$\begin{aligned} W^m &= \mathcal{L}(-\operatorname{ord}_{P_\infty}(m)P_\infty) &&= \{f \in K[C] \mid \operatorname{LM}(f) \leq m\} \ , \\ W_D^m &= \mathcal{L}(-\operatorname{ord}_{P_\infty}(m)P_\infty - D) &&= \{f \in I_D \mid \operatorname{LM}(f) \leq m\} \ = \ W^m \cap I_D \ . \end{aligned}$$

Given a reduced Gröbner basis for I_D, it is easy to construct an echelon basis for W_D^m by taking monomial multiples of the basis elements and removing all those that result in duplicate leading monomials. Given an echelon basis for W_D^m with m sufficiently large, a reduced Gröbner basis for I_D can be obtained by removing any basis element whose leading monomial is divisible by that of another basis element.

Now let D, D' be distinct reduced divisors of respective degrees $d = \deg(D)$ and $d' = \deg(D')$, with $d \geq d'$. Let m be the largest monomial appearing in the reduced Gröbner basis of any ideal I such that $\operatorname{div}(I)$ has degree $d + d'$. For example, if $d + d' = 6$, then the reduced Gröbner basis of an ideal of a type 64 divisor contains

Table 2.1. Arita's classification of divisors into types

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	$y + f_1x + f_0$
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	$x^2 + f_2y + f_1x + f_0$

Table 2.2. Divisor types and the type of their flip and double flip

Divisor	Type																			
D	0	11	21	22	31	32	33	41	42	43	44	51	52	53	54	61	62	63	64	65
$\overline{D}$	0	22	21	11	31	11	0	31	22	21	0	31	22	21	11	31	22	21	11	0
$\overline{\overline{D}}$	0	11	21	22	31	22	0	31	11	21	0	31	11	21	22	31	11	21	22	0

a polynomial with leading monomial $m = x^4$, and no other degree 6 divisor type has a larger monomial.

Put $L = \operatorname{lcm}(D, D')$ and $G = \gcd(D, D')$. The divisors L and G arise from the kernel and image, respectively, of the matrix M in the diagram below. Here, ι denotes inclusion and π is the natural projection.

$$\begin{tikzcd}
W^m_L \arrow[r, hook, "\ker M"] & W^m_D \arrow[r, hook, "\iota"] \arrow[rr, bend left, "M"] & W^m \arrow[r, two heads, "\pi"] & \frac{W^m}{W^m_{D'}} \arrow[r, two heads, "\operatorname{im} M"] & \frac{W^m_G}{W^m_{D'}}
\end{tikzcd}$$

A proof of this crucial result can be found in [10, Thm. 8.7]. This is a generalization of the addition procedure of [11], where the authors compute $\ker M$ for $m = x^2y$ only. This is sufficient when D and D' are disjoint (or equivalently, $G = 0$) and typical, but their approach fails otherwise. A larger bounding monomial m can handle atypical divisor sums, and computing the image $\operatorname{im} M$ allows non-disjoint input divisors D, D'.

The kernel and image of M are obtained by first computing the reduced row echelon form of M, denoted $\operatorname{RREF}(M)$, which in particular reveals the rank of M

as well as the dimensions of its kernel and image. If M has full rank, which is typically the case, then $G = 0$ and $\ker M$ produces a reduced Gröbner basis for $I_L = I_{D+D'}$. If M has rank 0, then $D' < D$, in which case we find the divisor A such that $D = D' + A$ and return $\overline{\overline{2D'}} + A$ via a call to the doubling algorithm in §4. Otherwise, we recursively compute the sum $\overline{\overline{L}} + G$. In this recursive call, one of the input divisors has degree strictly less than d', so this recursion terminates. Details of the algorithm and toy examples can be found in [10, Ch. 8].

4. Doubling

Doubling a reduced divisor D is similar to adding two distinct reduced divisors. Here, we find a (not necessarily reduced) divisor $A \neq D$ equivalent to D and compute the reduction $\overline{\overline{A + D}} = \overline{\overline{2D}}$ using the addition algorithm from §3. We describe an optimized approach for finding A that represents a significant improvement over the doubling method presented in [10, Ch. 9].

We begin with the most common case when D is a type 31 divisor. Let $\{f, g, h\}$ be a reduced Gröbner basis of its associated ideal I_D.

Lemma 4.1. *Let D be of type 31. Then there exist polynomials*

$$\begin{array}{lll} r = y + r_0 \ , & s = -(x + s_0) \ , & t = t_0 \ , \\ r' = x^2 + r'_2 y + r'_1 x + r'_0 \ , & s' = s'_0 \ , & t' = y + t'_0 \ , \\ r'' = r''_0 \ , & s'' = y + s''_0 \ , & t'' = x + t''_0 \end{array}$$

in $K[C]$ such that $rf + sg + th = 0$, $r'f + s'g + t'h = F$ and $r''f + s''g + t''h = 0$.

Proof. Explicit formulas for r, s, t, r', s', t' are given in Table 6.2. The polynomials $r'' = h_1$, $s'' = y - g_1 + h_2$ and $t'' = -x - g_2$, with g_1, g_2, h_1, h_2 as given in (6.1), are easily verified to satisfy the third identity. □

The quantities r'', s'', t'' are only auxiliary to the proof of Proposition 4.2. Put

$$A = \operatorname{div}(\tilde{f}, \tilde{g}, \tilde{h}) \quad \text{with} \quad \tilde{f} = st' - ts' \ , \quad \tilde{g} = tr' - rt' \ , \quad \tilde{h} = rs' - sr' \ . \tag{4.1}$$

Then the leading monomials of $\tilde{f}, \tilde{g}, \tilde{h}$ are xy, y^2, x^3, respectively, so A is of type 41 by Table 2.1. It is easy to verify that $f\tilde{g} = g\tilde{f}$ and $f\tilde{h} = h\tilde{f}$ in $K[C]$. It follows that $\tilde{f} I_D = f I_A$ and hence $\operatorname{div} f + A = \operatorname{div} \tilde{f} + D$, so A is equivalent to D.

The following proposition shows that A and D are typically disjoint. If not, we have $D \not\leq A$. Either way, we may add D and A using the addition algorithm from the previous section.

Proposition 4.2. *Let D be of type 31 and put $G = \gcd(D, A)$. If D is typical, then $G = 0$, otherwise G has degree 1.*

Proof. We have $\deg(G) \leq \deg(D) = 3$. Suppose $\deg(G) \geq 2$. Then $D - G$ and $A - G$ are equivalent divisors of degree ≤ 2. So these two divisors are reduced and hence equal, which is impossible since $\deg(D) \neq \deg(A)$. It follows that $\deg(G) \leq 1$.

Suppose $\deg(G) = 1$. Then $\deg(D - G) = 2$, $\deg(A - G) = 3$ and $\overline{\overline{D - G}} = \overline{\overline{A - D}}$, which by Table 2.2 forces $D - G$ to be of type 22 and $A - G$ to be of type 32. Let $x + a$ and $x + b$ be the minimum polynomials of I_G and I_{D-G}, respectively. Then $f = (x + a)(x + b) \in I_D$. Appealing to the form of I_D characterized in Table 2.1, f is the minimum polynomial of I_D and has a vanishing y-coefficient, so D is atypical.

Conversely, suppose that D is atypical. Referring to the quantities of Lemma 4.1, we have $t = -f_2 = 0$. Put $I = \langle r, s \rangle$. Then I is a prime ideal of degree 1. From (4.1), we see that $I_A \subseteq I$. A simple symbolic computation yields $f = st''$, $g = rt''$ and $h = r''s - s''r$, so $I_D \subseteq I$. It follows that $I_G = I_A + I_D \subseteq I$, so $\mathrm{div}(I) \leq G$, which in turn implies $\deg(G) \geq 1$, and hence $\deg(G) = 1$.

□

An optimization is possible when computing the kernel of M in

$$\begin{tikzcd}
W_L^m \arrow[r, hook, "\ker M"] & W_A^m \arrow[r, hook, "\iota"] \arrow[rr, bend left, "M"] & W^m \arrow[r, two heads, "\pi"] & \frac{W^m}{W_D^m} \arrow[r, two heads, "\mathrm{im}\, M"] & \frac{W_G^m}{W_D^m}
\end{tikzcd} .$$

The kernel consists of $K[C]$-linear combinations on $\{\tilde{f}, \tilde{g}, \tilde{h}\}$ that are in W_L^m. However, the following theorem shows that when D is typical, we may instead perform our computations on f, g, h. The latter have fewer monomials, so the resulting linear combinations are faster to generate.

Theorem 4.3. *Let D be of type* 31*,* $L = lcm(D, A)$ *and* $G = \gcd(D, A)$*. Let* $a, b, c \in K[C]$*. Then* $af + bg + ch \in I_{2D-G}$ *if and only if* $a\tilde{f} + b\tilde{g} + c\tilde{h} \in I_L$*.*

Proof. We have $2D - G + \mathrm{div}(\tilde{f}) = L + D - A + \mathrm{div}(\tilde{f}) = L + \mathrm{div}(f)$. Since $f\tilde{g} = g\tilde{f}$ and $f\tilde{h} = h\tilde{f}$, the claim follows. □

If D is typical, then $I_{2D-G} = I_{2D}$ by Proposition 4.2.

Next, we provide analogous results for divisors D of types 11, 21, and 22. Here, $I_D = \langle f, g \rangle$.

Theorem 4.4. *Let D be of type* 11*,* 21*, or* 22*, and write* $I_D = \langle f, g \rangle$*. Then there exist non-zero polynomials* $\tilde{f}, \tilde{g} \in K[C]$ *such that* $f\tilde{g} + g\tilde{f} = F$ *and* $\tilde{f}\langle f, g \rangle = f\langle \tilde{f}, \tilde{g} \rangle$*. The divisor* $A = \mathrm{div}(\tilde{f}, \tilde{g})$ *is equivalent to D and* $\gcd(A, D) = 0$*. Finally, for any* $a, b \in K[C]$*, we have* $af + bg \in I_{2D}$ *if and only if* $a\tilde{f} + b\tilde{g} \in I_{A+D}$*.*

Proof. The first assertion follows from $F \in \langle f, g \rangle$. Since $f\tilde{g} = -g\tilde{f}$ in $K[C]$, we have $\tilde{f}\langle f, g \rangle = \langle f\tilde{f}, g\tilde{f} \rangle = \langle f\tilde{f}, f\tilde{g} \rangle = f\langle \tilde{f}, \tilde{g} \rangle$, so $\mathrm{div}(\tilde{f}) + D = \mathrm{div}(f) + A$. This identity also yields the last assertion, provided that $\gcd(A, D) = 0$.

Suppose first that D is of type 11. Then the leading monomials of f and g are x and y, respectively. A solution to $f\tilde{g} + g\tilde{f} = F$ then requires that the leading monomials of $\tilde{f}$ and $\tilde{g}$ are y^2 and x^3, respectively. Therefore $A = \mathrm{div}(\tilde{f}, \tilde{g})$ is a type 62 divisor. Suppose $\gcd(A, D) \neq 0$. Then $A - D$ would be a principal divisor of degree 5 which is impossible by Table 2.1.

Likewise, suppose D is of type 21. Then $A = \mathrm{div}(\tilde{f}, \tilde{g})$ is of type 43. Suppose $G = \gcd(A, D) \neq 0$. Since $A - G \equiv D - G$, we either have a degree 3 divisor that is equivalent to a degree 1 divisor, or a degree 2 divisor that is equivalent to 0, depending on the degree of G. Appealing to Table 2.1, we see that both cases are impossible. The case when D is of type 22 is similar. □

Our addition and doubling routines call one another, but this process terminates. The doubling routine terminates on all inputs except atypical type 31 divisors (Prop. 4.2), in which case we must add $\overline{\overline{L}} + G$ where $\deg G = 1$ and there is no need to subsequently double another type 31 divisor. Furthermore, the addition routine may call itself, but the degree of the smaller divisor strictly decreases, forcing it to eventually terminate.

5. Reduction

Reducing a divisor may be accomplished by flipping it twice, as was done in [2, 11]. However, in [8], it was shown that for typical degree 6 divisors, both flips can be combined into a single operation that is more efficient than even just the first flip. Below, we generalize this result to all typical and non-semi-typical divisors (of any degree). The remaining divisors, those that are semi-typical but atypical, are addressed in Theorem 5.2.

Theorem 5.1. *Let D be an effective divisor on C and let $\{u, v\}$ be any generating set for I_D such that u is the minimum polynomial of I_D. Then there exist polynomials $f, g \in K[C]$ such that $fv = gu$ in $K[C]$ and $\overline{\overline{D}} = \operatorname{div}(f, g)$.*

Proof. Let f be the minimum polynomial of the colon ideal $u : v$. Then there exists $g \in K[C]$ such that $fv = gu$ in $K[C]$. The divisor $A = \operatorname{div}(f, g)$ is equivalent to D since $uI_A = \langle fu, gu\rangle = \langle fu, fv\rangle = fI_D$. The minimality of u and f implies that A is reduced and is hence the reduction of D. □

In particular, Theorem 5.1 makes efficient reduction of all divisors listed in Table 2.1 straightforward, except for atypical semi-typical divisors, where I_D might be generated by no two of its Gröbner basis elements. Given $I_D = \langle u, v\rangle$, the type of $\overline{\overline{D}}$ is first read from Table 2.2. Then the leading monomials of f, g, with $I_{\overline{\overline{D}}} = \langle f, g\rangle$, are obtained from Table 2.1. The coefficients of f, g are now easily computed by equating coefficients in the relation $fv \equiv gu \pmod{F}$ and solving the resulting system of linear equations. Reduction of atypical semi-typical divisors is done via Theorem 5.2 which represents an improvement for type 41 and 51 divisors over the method presented in [10, Sec. 10.1].

Theorem 5.2. *Let D be an atypical semi-typical divisor, and write $I_D = \langle f, g, h\rangle$. Put $I = \langle f, g\rangle$. Then there exist K-rational points P, Q on C such that $\operatorname{div}(I) = D + (P - P_\infty)$ and $\overline{\overline{\operatorname{div}(I)}} = Q - P_\infty$.*

Proof. We have $\deg \operatorname{div}(I) = \dim_K(K[C]/I)$ and $\deg D = \dim_K(K[C]/I_D)$. Computing these dimensions for each atypical case using Table 2.1 (the dimensions are determined by the leading coefficients of f and g) yields $\deg \operatorname{div}(I) = \deg D + 1$ which establishes the existence of P.

Analogous to Lemma 4.1, there exist polynomials $r = x + r_0, s = y + s_1x + s_0 \in K[C]$ such that $fs + gr = F$ when D is of type 51 and $fs = gr$ otherwise. Since $\operatorname{div}(r, s)$ has degree 1, it is reduced and of the form $Q - P_\infty$. As in the proof of Theorem 5.1, we see that I is equivalent to $\langle r, s\rangle$, which is hence the reduction of $\operatorname{div}(I)$. □

Corollary 5.3. $\overline{\overline{D}} = (Q - P_\infty) + \overline{P - P_\infty}$.

Proof. By Theorem 5.2, $D = \operatorname{div}(I) - (P - P_\infty)$ and $\overline{\overline{\operatorname{div}(I)}} = Q - P_\infty$. The reduced divisor equivalent to $-(P - P_\infty)$ is $\overline{P - P_\infty}$. It follows that $\overline{\overline{D}}$ is equivalent to $(Q - P_\infty) + \overline{P - P_\infty}$. Since $\overline{\overline{D}}$ is reduced and both $\overline{\overline{D}}$ and $(Q - P_\infty) + \overline{P - P_\infty}$ have the same degree, they must both be reduced and therefore equal. □

Obtaining P amounts to finding polynomials $p = x + p_0$ and $q = y + q_1x + q_0$ such that $hp, hq \in I$. The polynomials r and s of Theorem 5.1 determine Q.

6. Explicit Formulas for Typical Divisors

Here, we derive explicit formulas handling the most typical cases in $C_{3,4}$ arithmetic: adding disjoint type 31 divisors whose sum is typical, and doubling a typical type 31 divisor whose double is typical. If ever we detect that we are outside these cases, we may fall back on another series of explicit formulas.

Let D and D' be typical type 31 divisors, with respective associated ideals and Gröbner bases $I_D = \langle f, g, h\rangle$ and $\langle f', g', h'\rangle$, where

$$\begin{aligned} f &= x^2 + f_2 y + f_1 x + f_0 \ , & f' &= x^2 + f'_2 y + f'_1 x + f'_0 \ , \\ g &= xy + g_2 y + g_1 x + g_0 \ , & g' &= xy + g'_2 y + g'_1 x + g'_0 \ , \\ h &= y^2 + h_2 y + h_1 x + h_0 \ , & h' &= y^2 + h'_2 y + h'_1 x + h'_0 \ . \end{aligned} \tag{6.1}$$

The optimal choice of monomial in the addition and doubling algorithms of §3 and §4 is $m = x^2 y$. Bases for the vector spaces $W_D^{x^2y}$ and $W_{D'}^{x^2y}$ are $\{f, g, h, xf, xg\}$ and $\{f', g', h', xf', xg'\}$, respectively. The matrix

$$M = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}$$

for adding D and D' is constructed by reducing the former basis modulo the latter; e.g the reduction of f modulo $\{f', g', h', xf', xg'\}$ is $(f_2 - f'_2)y + (f_1 - f'_1)x + (f_0 - f'_0)$, so $a_1 = f_0 - f'_0$, $a_6 = (f_1 - f'_1)$, etc. Computing the first three columns requires only subtractions (counted as additions). The right two columns are given in terms of the first three by

$$\begin{pmatrix} a_4 & a_5 \\ a_9 & a_{10} \\ a_{14} & a_{15} \end{pmatrix} = \begin{pmatrix} 0 & -f'_0 & -g'_0 \\ 1 & -f'_1 & -g'_1 \\ 0 & -f'_2 & -g'_2 \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 \\ a_6 & a_7 & a_8 \\ a_{11} & a_{12} & a_{13} \end{pmatrix} .$$

For doubling D, we construct the divisor A defined in §4 using the polynomials defined in (4.1) and Lemma 4.1. Then the left three columns of the matrix M used in the computation of $D + A$ are the reductions of $\tilde{f}, \tilde{g}, \tilde{h}$ modulo f, g, h. Let $e_1 = -(f_1 + g_2)$ and $e_2 = r'_2 - f_2$. Then the left three columns of M are

$$\begin{pmatrix} t'_0 s_0 + s'_0 t_0 - g_0 & t'_0 r_0 + t_0(f_0 - r'_0) - h_0 & f_0 e_1 + g_0 e_2 - s'_0 r_0 - r'_0 s_0 \\ t'_0 - g_1 & t_0(f_1 + f_1) - h_1 & f_1(e_1 + s_0) + g_1 e_2 - r'_0 + f_0 \\ s_0 - g_2 & t'_0 - h_2 + r_0 - t_0 e_2 & f_2(e_1 - g_2) + r'_2(g_2 - s_0) - s'_0 \end{pmatrix} .$$

The right two columns relate to the first three as above, with D in place of D'.

If the first column is zero, then $D + D'$ (or $D + A$) is atypical and we must fall back on other formulas. Otherwise, we assume $a_1 \neq 0$ by swapping rows if necessary. Then elementary row operations convert M into row echelon form:

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} \longrightarrow \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ 0 & b_1 & b_2 & b_3 & b_4 \\ 0 & 0 & b_5 & b_6 & b_7 \end{pmatrix} .$$

If b_1 or b_5 are zero, then $D + D'$ (or $D + A$) either contains points of multiplicity exceeding 1 or is atypical. To avoid an expensive inversion operation, we compute a scalar multiple of the reduced row echelon form $\mathrm{RREF}(M)$ and defer the necessary inversion until later:

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ 0 & b_1 & b_2 & b_3 & b_4 \\ 0 & 0 & b_5 & b_6 & b_7 \end{pmatrix} \longrightarrow \begin{pmatrix} Z & 0 & 0 & A_1 & A_2 \\ 0 & Z & 0 & B_1 & B_2 \\ 0 & 0 & Z & C_1 & C_2 \end{pmatrix} .$$

Now $\ker(M) = \mathrm{Span}_K\{U, V\}$, where

$$U = Zxf - C_1h - B_1g - A_1f \ , \quad V = Zxg - C_2h - B_2g - A_2f \ .$$

Let $U = Zx^3 + U_5y^2 + \cdots + U_0$ and $V = Zx^2y + V_5x^2y + \cdots + V_0$. Formulas for the coefficients U_i, V_i are found in Table 6.3, although note that the constant coefficients U_0 and V_0 are not needed and therefore not computed. Let $u_0, \ldots, u_5, v_0, \ldots v_5$ be the coefficients of $u := U/Z$ and $v := V/Z$. To compute u_i, v_i, we will need the inverse of Z. However, we will also need the inverse of $f''_2 = u_5^2 + u_4 - v_5$ later on. We compute both inverses at once with only a single inversion using a variation of Montgomery's Trick. Formulas for $\zeta := Z^{-1}$ and $\tau := (f''_2)^{-1}$ are found in Table 6.3. We note that the intermediate value z_0 is equal to $Z^2f''_2$. If this is zero, then the sum is atypical and we fall back on other formulas. Once ζ is known, we compute $u_i = \zeta U_i$ and $v_i = \zeta V_i$ for $i = 1, \ldots, 5$.

Now $I_{D+D'}$ (or I_{2D}) is generated by $\{u, v\}$. We apply Theorem 5.1 and find polynomials $f'' = x^2 + f''_2y + f''_1x + f''_0$ and $g'' = xy + g''_3x^2 + g''_2y + g''_1x + g''_0$ satisfying $f''v \equiv g''u \pmod F$. We would then have to reduce g'' modulo f'' to eliminate the x^2 term in g''. Since $g''_3 = u_5$, this means subtracting u_5 times f'' from g''. We avoid this by instead finding $g'' = xy + g''_2y + g''_1x + g''_0$ such that $f''v \equiv (g'' + u_5f'')u \pmod F$, thereby saving a multiplication and a few additions.

The third polynomial in the Gröbner basis of $I_{D+D'}$ (or I_{2D}) is

$$h'' = \tau\left((y + g''_1)f'' - (x + f''_1 - g''_2)g''\right) .$$

Explicit formulas and operation counts for all the quantities above are given in Tables 6.1, 6.2, and 6.3.

Table 6.1. Construction of matrix M — typical addition

Addition	12M+17A
Input: $I_D = \langle f, g, h\rangle$, $I_{D'} = \langle f', g', h'\rangle$ $f = x^2 + f_2y + f_1x + f_0$ $\quad f' = x^2 + f'_2y + f'_1x + f'_0$ $g = xy + g_2y + g_1x + g_0$ $\quad g' = xy + g'_2y + g'_1x + g'_0$ $h = y^2 + h_2y + h_1x + h_0$ $\quad h' = y^2 + h'_2y + h'_1x + h'_0$ Output: $M_{\mathrm{add}} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}$	
Compute elements a_i of M_{add}	12M+17A
$a_1 = f_0 - f'_0$ $\quad a_2 = g_0 - g'_0$ $\quad a_3 = h_0 - h'_0$ $\quad a_6 = f_1 - f'_1$ $a_7 = g_1 - g'_1$ $\quad a_8 = h_1 - h'_1$ $\quad a_{11} = f_2 - f'_2$ $\quad a_{12} = g_2 - g'$ $a_{13} = h_2 - h'_2$ $\quad a_4 = -f'_0a_6 - g'_0a_{11}$ $\quad a_5 = -f'_0a_7 - g'_0a_{12}$ $a_9 = a_1 - f'_1a_6 - g'_1a_{11}$ $\quad a_{10} = a_2 - f'_1a_7 - g'_1a_{12}$ $a_{14} = -f'_2a_6 - g'_2a_{11}$ $\quad a_{15} = -f'_2a_7 - g'_2a_{12}$ If $a_1 = a_6 = a_{11} = 0$, then abort. If $a_1 = 0$ is zero but $a_6 \neq 0$ or $a_{11} \neq 0$, then swap rows so $a_1 \neq 0$.	

Table 6.2. Construction of matrix M — typical doubling

Doubling	28M+1S+41A
Input: $I_D = \langle f, g, h\rangle$ $f = x^2 + f_2y + f_1x + f_0, \quad g = xy + g_2y + g_1x + g_0$ $h = y^2 + h_2y + h_1x + h_0$ Output: $M_{\text{doub}} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}$	
Compute polynomials $r = y + r_0, s = -(x + s_0), t = t_0$ such that $rf + sg + th = 0$	1A
$r_0 = g_1 \quad s_0 = f_1 - g_2 \quad t_0 = -f_2$	
Compute polynomials $r' = x^2 + r_2'y + r_1'x + r_0'$, $s' = s_0', t' = y + t_0'$ such that $r'f + s'g + t'h = F$	2M+1S+7A
$r_2' = c_7 - f_2 \qquad r_1' = -f_1 \quad t_0' = -h_2 - f_2r_2'$ $s_0' = c_4 - h_1 + f_1(f_2 - r_2') \quad r_0' = c_3 + f_1^2 - f_0$	
Compute reductions $\overline{\tilde{f}} = \tilde{f}_2y + \tilde{f}_1x + \tilde{f}_0$, $\overline{\tilde{g}} = \tilde{g}_2y + \tilde{g}_1x + \tilde{g}_0$, $\overline{\tilde{h}} = \tilde{h}_2y + \tilde{h}_1x + \tilde{h}_0$	14M+25A
$e_1 = -f_1 - g_2 \qquad e_2 = r_2' - f_2$ $\tilde{f}_2 = s_0 - g_2 \qquad \tilde{f}_1 = t_0' - g_1$ $\tilde{f}_0 = t_0's_0 + s_0't_0 - g_0 \qquad \tilde{g}_2 = t_0' - h_2 + r_0 - t_0e_2$ $\tilde{g}_1 = t_0(f_1 + f_1) - h_1 \qquad \tilde{g}_0 = t_0'r_0 + t_0(f_0 - r_0') - h_0$ $\tilde{h}_2 = f_2(e_1 - g_2) + r_2'(g_2 - s_0) - s_0'$ $\tilde{h}_1 = f_1(e_1 + s_0) + g_1e_2 - r_0' + f_0$ $\tilde{h}_0 = f_0e_1 + g_0e_2 - s_0'r_0 - r_0's_0$	
Compute matrix M_{doub}	12M+8A
$a_1 = \tilde{f}_0 \qquad a_2 = \tilde{g}_0 \qquad a_3 = \tilde{h}_0 \qquad a_6 = \tilde{f}_1 \qquad a_7 = \tilde{g}_1$ $a_8 = \tilde{h}_1 \qquad a_{11} = \tilde{f}_2 \qquad a_{12} = \tilde{g}_2 \qquad a_{13} = \tilde{h}_2$ $a_4 = -f_0a_6 - g_0a_{11} \qquad a_5 = -f_0a_7 - g_0a_{12}$ $a_9 = a_1 - f_1a_6 - g_1a_{11} \quad a_{10} = a_2 - f_1a_7 - g_1a_{12}$ $a_{14} = -f_2a_6 - g_2a_{11} \qquad a_{15} = -f_2a_7 - g_2a_{12}$ If $a_1 = a_6 = a_{11}$, then abort. If $a_1 = 0$ but $a_6 \neq 0$ or $a_{11} \neq$, then swap rows so $a_1 \neq 0$.	

Table 6.3. Computing $\ker M$

Computing $\ker M$	1I+99M+3S+72A
Input: $I_D = \langle f, g, h\rangle$, M $f = x^2 + f_2y + f_1x + f_0, \quad g = xy + g_2y + g_1x + g_0$ $h = y^2 + h_2y + h_1x + h_0$ $M = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}$ Output: $I_{D+D'} = \langle f'', g'', h''\rangle$ (or $I_{2D} = \langle f'', g'', h''\rangle$) $f'' = x^2 + f_2''y + f_1''x + f_0'', \quad g'' = xy + g_2''y + g_1''x + g_0''$ $h'' = y^2 + h_2''y + h_1''x + h_0''$	
Compute row echelon form of M	21M+12A
$d_1 = a_1a_{12} - a_2a_{11} \qquad d_2 = a_6a_{12} - a_7a_{11}$ $b_1 = a_1a_7 - a_2a_6 \qquad b_5 = b_1a_{13} - d_1a_8 + d_2a_3$ $b_2 = a_1a_8 - a_3a_6 \qquad b_6 = b_1a_{14} - d_1a_9 + d_2a_4$ $b_3 = a_1a_9 - a_4a_6 \qquad b_7 = b_1a_{15} - d_1a_{10} + d_2a_5$ $b_4 = a_1a_{10} - a_5a_6$	

Compute $Z \cdot \mathrm{RREF}(M)$	18M+6A
$Y = a_1b_1 \quad e_1 = b_3b_5 - b_2b_6 \quad Z = Yb_5 \quad e_2 = b_4b_5 - b_2b_7$ $A_1 = b_1(a_4b_5 - b_6a_3) - a_2e_1 \quad B_1 = a_1e_1 \quad C_1 = Yb_6$ $A_2 = b_1(a_5b_5 - b_7a_3) - a_2e_2 \quad B_2 = a_1e_2 \quad C_2 = Yb_7$	
Compute $\ker(M)$	18M+14A
$U_1 = Zf_0 - C_1h_1 - B_1g_1 - A_1f_1 \quad U_2 = -C_1h_2 - B_1g_2 - A_1f_2$ $V_1 = Zg_0 - C_2h_1 - B_2g_1 - A_2f_1 \quad V_2 = -C_2h_2 - B_2g_2 - A_2f_2$ $U_3 = Zf_1 - A_1 \; U_4 = Zf_2 - B_1 \quad U_5 = -C_1$ $V_3 = Zg_1 - A_2 \; V_4 = Zg_2 - B_2 \quad V_5 = -C_2$	
Compute $\zeta = Z^{-1}, \tau = (f''_2)^{-1}$	1I+5M+2S+3A
$z_0 = U_5^2 + Z(U_4 - V_5) \quad z_1 = Zz_0 \quad z_2 = z_1^{-1} \quad z_3 = Zz_2$ $\zeta = z_0z_2 \qquad \tau = Z^2z_3$	
Compute $u_1, \ldots, u_5, v_1, \ldots, v_5$	10M
$u_1 = \zeta U_1 \quad u_2 = \zeta U_2 \quad u_3 = \zeta U_3 \quad u_4 = \zeta U_4 \quad u_5 = \zeta U_5$ $v_1 = \zeta V_1 \quad v_2 = \zeta V_2 \quad v_3 = \zeta V_3 \quad v_4 = \zeta V_4 \quad v_5 = \zeta V_5$	
Compute f'', g'', h''	27M+1S+37A
$f''_2 = u_5^2 + u_4 - v_5 \qquad r_0 = u_5(f''_2 + u_4 - c_7) + u_3 - v_4$ $r_1 = f''_2(f''_2 - u_4) \qquad g''_1 = r_1 - u_5(u_3 + r_0) + v_3$ $g''_2 = -u_4u_5 + v_4 - r_0 + \tau(u_4r_0 - u_5g''_1 - u_2) \qquad f''_1 = r_0 + g''_2$ $f''_0 = -c_7(r_1 + g''_2u_5) + u_5(f''_2u_3 + f''_1u_4 - c_4 + u_2)$ $\qquad + g''_2u_3 + g''_1u_4 - f''_2v_3 - f''_1v_4 + u_1 - v_2$ $g''_0 = u_5(c_3 - f''_0 - u_1 - f''_1u_3) - g''_1u_3 + f''_1v_3 + v_1$ $h''_0 = \tau(f''_0g''_1 - g''_0r_0) \qquad h''_1 = \tau(g''_1g''_2 - g''_0)$ $h''_2 = g''_1 + \tau(f''_0 - g''_2r_0)$	

7. Implementation and Testing

A Sage implementation of $C_{3,4}$ curve arithmetic based on the algorithms in this paper is available at [9]. This implementation includes optimized addition and doubling subroutines `fast_add_31_31`, `fast_add_31_31_high_char`, `fast_double_31`, and `fast_double_31_ high_char`. The high characteristic versions assume that the curve equation is given in short form and implement the formulas in Tables 6.1, 6.2, and 6.3. The other versions implement similar formulas with no assumptions on the coefficients c_5, c_6, and c_8. The optimized subroutines assume the typical cases described in §6. When any of these assumptions are violated, an exception is thrown, and a less-optimized subroutine is called instead.

The less-optimized subroutines are nonetheless implemented via explicit formulas. These include addition subroutines for every pair of reduced divisor types (e.g. `add_31_21`), a doubling subroutine for every reduced divisor type (e.g. `double_31`), and a reduction subroutine for every unreduced divisor type (e.g. `reduce_61`).

Addition subroutines, given input divisors D and D', compute $L = \mathrm{lcm}(D, D')$ and $G = \gcd(D, D')$ by computing the kernel and image of a matrix as described in §3. If $G = 0$, then the reduction of L is computed via the appropriate subroutine and $\overline{\overline{L}}$ is returned. Otherwise $\overline{\overline{L}}$ and G are added by calling another addition subroutine. The cost of evaluating $D + D'$ depends on the type of L. Costs are given in Table 7.1a for the cases when $G = 0$. When $G > 0$, one or more recursive calls must be made. A full analysis of the cost in these cases was not done, due to the large number of sub-cases that can occur.

Doubling subroutines, given an input divisor D, find generators for a divisor A equivalent to D, and compute $G = \gcd(A, D)$ and $2D - G$ as outlined in §4. We recursively compute $\overline{\overline{2D-G}} + G$. The cost depends on the type of $2D - G$, if $G = 0$, and if a recursive call must be made. Table 7.1b contains the costs for the cases where $G = 0$. Here, "t" and "a" under the type column refer to typical and atypical divisors, respectively.

Table 7.1. Operation counts for $C_{3,4}$ arithmetic

(a) Addition

	Op count				Type
Subroutine	I	M	S	A	of L
add_11_11	1	3	0	4	21
add_11_11	0	1	0	3	22
add_21_11	1	13	0	14	31
add_21_11	0	12	0	17	32
add_21_21	2	68	1	58	41-t
add_21_21	2	67	0	58	41-a
add_21_21	1	27	0	19	42
add_21_21	1	39	0	32	43
add_21_21	0	12	0	9	44
add_21_22	2	40	1	41	41-t
add_21_22	2	39	0	41	41-a
add_21_22	0	2	0	2	42
add_22_11	1	5	0	5	31-a
add_22_11	0	1	0	3	33
add_22_22	1	11	0	17	43
add_31_11	2	43	1	49	41-t
add_31_11	2	22	0	49	41-a
add_31_11	0	6	0	10	42
add_31_11	1	16	0	32	43
add_31_21	2	80	1	77	51-t
add_31_21	2	78	1	74	51-a
add_31_21	1	35	1	33	52
add_31_21	1	57	1	51	53
add_31_21	1	43	1	41	54
add_31_22	2	69	0	64	51-t
add_31_22	2	67	0	61	51-a
add_31_22	1	24	0	20	52
add_31_22	1	46	0	38	53
add_31_22	1	36	0	29	54
fast_add_31_31 _high_char	1	111	3	99	61-t
fast_add_31_31	1	114	2	102	61-t
add_31_31	2	127	0	110	61-a
add_31_31	1	69	0	54	62
add_31_31	1	85	0	67	63
add_31_31	1	94	0	75	64
add_31_31	0	32	0	28	65

(b) Doubling

	Op count				Type of
Subroutine	I	M	S	A	$2D - G$
double_11	1	15	1	20	21
double_11	0	8	1	13	22
double_21	2	86	1	85	41-t
double_21	2	85	0	85	41-a
double_21	1	50	0	47	42
double_21	1	60	0	60	43
double_21	0	7	0	12	44
double_22	1	22	0	22	42
double_22	1	25	0	29	43
fast_double_31 _high_char	1	127	4	112	61
fast_double_31	1	138	2	130	61
double_31	2	159	0	156	61-t
double_31	2	152	0	149	61-a
double_31	1	94	0	90	62
double_31	1	110	0	103	63
double_31	1	119	0	111	64
double_31	0	57	0	64	65

(c) Reduction

	Op count			
Subroutine	I	M	S	A
reduce_32	0	8	0	11
reduce_33	0	0	0	0
reduce_41t	1	23	1	28
reduce_41a	1	22	0	28
reduce_42	0	0	0	1
reduce_43	0	6	0	11
reduce_44	0	0	0	0
reduce_51t	1	24	0	32
reduce_51a	1	22	0	29
reduce_52	0	1	0	3
reduce_53	0	12	0	14
reduce_54	0	7	0	10
reduce_61t	1	35	0	46
reduce_61a	1	28	0	39
reduce_62	0	2	0	5
reduce_63	0	8	0	13
reduce_64	0	12	0	21
reduce_65	0	0	0	0

Our operation counts for the high characteristic formulas compare to the previous state-of-the-art in [8] as follows:

	Addition	Doubling
Khuri-Makdisi [8]	2I+97M+1S+132A	2I+107M+3S+155A
This work	1I+111M+3S+99A	1I+127M+4S+112A

These counts include a trade-off of one inversion for several multiplications. An inversion is generally considered to be as expensive as 80 multiplications, depending on implementation and environment details [3, 5]. However, we note also that our formulas significantly decrease the number of additions required, and that the total number of field operations in both of our formulas is less than that of [8]. Over large fields such as those considered in [8], additions are generally considered to have negligible cost compared to multiplications and inversions, but in number theoretic computations such as [13] over smaller (typically word-sized) primes, this has been observed to not be the case.

To verify that our results represent an improvement over the previous state-of-the-art, we implemented the formulas from [11] and [8] in Sage and ran benchmark tests as follows. Given a prime p, choose a random $C_{3,4}$ curve C over $\mathbb{F}_p$ (with defining polynomial in short form) and two random divisors D_1 and D_2 on C. Details on random divisor generation are given in Section 12.2 of [10]. We counted how many terms in the Fibonacci-like sequence $D_{i+2} = D_{i+1} + D_i$, $i \geq 1$ (for addition) and the sequence $D_{i+1} = 2D_i$, $i \geq 1$ (for doubling) each algorithm is able to compute in 10 minutes. We chose to run these tests over the first 23 primes greater than 2^{28}, as primes on this order are of interest in number theoretic applications (see [14], for example), and because degenerate cases are so rare that we can strictly compare our formulas to those of [11] and [8]. Any time we encountered a degenerate case, we began a new trial with a different curve and initial divisors. In the tens of millions of divisors we added, this only occurred a few times. Our algorithm computed 126,310,162 additions as compared to 112,041,012 using the algorithm from [8], for a speedup of 12.74%. Similarly, our algorithm computed 120,827,482 doublings as compared to 108,489,487 for a speedup of 11.37%.

This benchmark was repeated over the first 11 primes larger than 2^{255}, where we found a more significant speed-up, likely due to the increasing cost of inverting in large finite fields. Our algorithm computed 63,151,623 additions versus 52,185,141 using the algorithm from [8], for a speedup of 21.01%. Similarly, our algorithm computed 56,795,783 doublings as compared to 48,395,712 for a speedup of 17.36%.

We found the most significant speed-up over very small primes, where atypical cases are frequently encountered and our explicit formulas are much faster than generic arithmetic. Over the ten largest primes under 2^8, we compared our formulas against those of [11] and [8], falling back on Sage's generic ideal arithmetic for cases not handled by those papers. Our algorithm computed 53,670,222 additions as compared to 31,685,426 using the algorithm from [8], for a speedup of 69.38%, and 48,156,514 doublings as compared to 39,152,564 for a speedup of 23.00%.

Correctness testing was accomplished by a combination of unit testing and random testing. Unit tests were constructed testing every branch of code in the addition, doubling, and reduction subroutines. These subroutines were also tested via hundreds of thousands of random inputs and the results were compared against Sage's vetted ideal arithmetic.

8. Conclusion

By generalizing the techniques of Abu Salem and Khuri-Makdisi [11] to atypical divisors as classified by Arita [2], we provided a fully general framework for efficient divisor arithmetic on $C_{3,4}$ curves. Taken together with our additional improvements to the setting of typical divisors, we obtain speedups of between 11- and 21-%

depending on the field size, and even more for small fields were atypical cases arise more frequently.

There is room for further speed advances in $C_{3,4}$ curve arithmetic, and work on this topic is ongoing. In our formulas for atypical divisors, addition/doubling and reduction are performed separately. Savings could be effected by combining these into a single optimized subroutine, as was done in §6 for the typical case. It may also be possible to eliminate all inversions using an analogue of projective coordinates, but this likely would not help with number-theoretic computations where frequent equality tests of divisors are required

Arithmetic on $C_{3,4}$ curves continues to be significantly more expensive than arithmetic on genus 3 hyperelliptic curves. Preliminary results indicate that Shanks' NUCOMP algorithm [12] achieves significant savings in the latter setting, which raises the question whether a NUCOMP-like idea may be applied to $C_{3,4}$ curve arithmetic as well.

References

[1] Seigo Arita. Algorithms for computations in Jacobian group of $C_{a,b}$ curve and their application to discrete-log-based public key cryptosystems. *Conference on the Mathematics of Public Key Cryptography*, pages 165–175, 1999.

[2] Seigo Arita. An addition algorithm in Jacobian of $C_{3,4}$ curve. *IEICE Trans. Found.*, E88-A, NO.6:1589–1598, 2005.

[3] Erik Dahmen, Katsuyuki Okeya, and Daniel Schepers. Affine precomputation with sole inversion in elliptic curve cryptography. In Josef Pieprzyk, Hossein Ghodosi, and Ed Dawson, editors, *Information Security and Privacy*, pages 245–258, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[4] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler. Fast addition on non-hyperelliptic genus 3 curves. In *Algebraic geometry and its applications, Proceedings of the first SAGA conference, Ser. Number theory and its applications*, volume 4, pages 1–28. World Sci. Publ., 2008.

[5] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography.* Springer-Verlag, 2004.

[6] David Harvey, Maike Massierer, and Andrew S. Sutherland. Computing L-series of geometrically hyperelliptic curves of genus three. *LMS J. Comput. Math.*, 19(suppl. A):220–234, 2016.

[7] Kiran S. Kedlaya and Andrew V. Sutherland. Computing L-series of hyperelliptic curves. In *Algorithmic Nnumber Theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 312–326. Springer, Berlin, 2008.

[8] Kamal Khuri-Makdisi. On Jacobian group arithmetic for typical divisors on curves. *Research in Number Theory*, 4, no. 1, article 3, 2018.

[9] Evan MacNeil. c34-curves. `https://github.com/emmacneil/c34-curves`, 2019.

[10] Evan MacNeil. Divisor Class Group Arithmetic on $C_{3,4}$ Curves. Master's thesis, University of Calgary, Canada, 2019. `https://github.com/emmacneil/c34-curves/blob/master/thesis-pdf/ucalgary_2020_macneil_evan.pdf`.

[11] Fatima Abu Salem and Kamal Khuri-Makdisi. Fast Jacobian group operations for $C_{3,4}$ curves over a large finite field. *LMS J. Comput. Math.*, 10:307–328, 11 2007.

[12] Daniel Shanks. On Gauss and composition i, ii. In *Proc. NATO ASI on Number Theory and Applications*, pages 163–204. Kluwer Academic Press, 1989.

[13] Andrew V. Sutherland. Fast Jacobian arithmetic for hyperelliptic curves of genus 3. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *The Open Book Ser.*, pages 425–442. Math. Sci. Publ., Berkeley, CA, 2019.

[14] Andrew V. Sutherland. Sato-Tate distributions. In *Analytic methods in arithmetic geometry*, volume 740 of *Contemp. Math.*, pages 197–248. Amer. Math. Soc., Providence, RI, 2019.