London Mathematical Society ISSN 1461–1570

FAST JACOBIAN GROUP OPERATIONS FOR $C_{3,4}$ CURVES OVER A LARGE FINITE FIELD

FATIMA K. ABU SALEM AND KAMAL KHURI-MAKDISI

This paper is dedicated to Richard P. Brent on the occasion of his sixtieth birthday.

Abstract

Let C be an arbitrary smooth algebraic curve of genus g over a large finite field $\mathbb{K}$. We revisit fast addition algorithms in the Jacobian of C due to Khuri-Makdisi (math.NT/0409209, to appear in *Mathematics of Computation*). The algorithms, which reduce to linear algebra in vector spaces of dimension $O(g)$ once $|\mathbb{K}| \gg g$ and which asymptotically require $O(g^{2.376})$ field operations using fast linear algebra, are shown to perform efficiently even for certain low genus curves. Specifically, we provide explicit formulae for performing the group law on Jacobians of $C_{3,4}$ curves of genus 3. We show that, typically, the addition of two distinct elements in the Jacobian of a $C_{3,4}$ curve requires 117 multiplications and 2 inversions in $\mathbb{K}$, and an element can be doubled using 129 multiplications and 2 inversions in $\mathbb{K}$. This represents an improvement of approximately 20% over previous methods.

1. *Introduction and background*

This article presents the fastest algorithms to date for arithmetic in the Jacobians of certain nonhyperelliptic genus 3 curves — specifically, $C_{3,4}$ curves over a very large finite field $\mathbb{K}$ that is not of characteristic 2 or 3. We attain this by adapting ideas from the asymptotically fastest algorithms known for general curves of large genus [9, 10]. Those algorithms boil down to linear algebra on matrices of size

$$O\big(g(1 + \log g / \log |\mathbb{K}|)\big) \times O(g),$$

where g is the genus of the curve; if $|\mathbb{K}|$ is large, the matrices will hence be of size $O(g) \times O(g)$. The complexity of those algorithms is thus $O(g^{2.376})$ using the current record for fast linear algebra.

Our results in this article illustrate how the asymptotic improvements introduced in [10], coupled with further new techniques, actually result in a significant speedup even for low genus curves that are slightly 'special' for their genus. However, fairly

The first author is supported in part by URB grant 788118, American University of Beirut.
Received 21 December 2006, revised 29 May 2007; *published* 7 August 2007.
2000 Mathematics Subject Classification 14Q05,14H40,14H45,11Y16
© 2007, Fatima K. Abu Salem and Kamal Khuri-Makdisi

special curves, such as hyperelliptic curves for example, are still probably better implemented using Cantor's algorithm or the general methods of [8], which have complexity $O(g^2)$ for curves of bounded gonality, but which have complexity $O(g^4)$ for 'most' curves of genus g.

Previous work on Jacobian group arithmetic for nonhyperelliptic genus 3 curves includes [2, 7], building on earlier work for curves of the form $y^3 = x^3 + \alpha x + \beta$ (see [3, 6]). The papers [2, 7] give slower algorithms for $C_{3,4}$ curves than ours, under the same hypotheses on $\mathbb{K}$. This article follows the lead introduced by [3], and adopted by [2, 6, 7], in that we present algorithms which are designed to work only for 'typical' (that is, sufficiently generic) elements of the Jacobian of C. Here, non-typical elements belong to a proper subvariety of the Jacobian, and so occur with frequency $O(1/|\mathbb{K}|)$, which means that they do not arise in practice. As in those previous articles, we also measure the complexity of our algorithms by counting only the number of multiplications and inversions that need to be performed in $\mathbb{K}$. This is reasonable, because in practical implementations of finite field arithmetic, addition and subtraction are much faster than multiplication or inversion, and inversion can take between 3 and 10 times as long as multiplication, as pointed out in [2]. Our approach requires 117 multiplications and 2 inversions in $\mathbb{K}$ to add a typical pair of distinct elements of the Jacobian; we abbreviate this complexity as $117M, 2I$. In contrast, the complexity of adding a typical pair of distinct elements in [7] is $145M, 2I$, while the complexity in [2] is $150M, 2I$. As for doubling a typical element of the Jacobian, our approach requires $129M, 2I$, as opposed to the doubling algorithm in [7], which needs $167M, 2I$, and to that in [2], which needs $174M, 2I$. Our algorithms and those of [7] actually compute first the negative of a sum of two elements of the Jacobian (respectively -2 times an element during doubling), and then invert the final result. The final inversion costs $7M$ in our approach, and $16M$ in [7] (as gathered from an inspection of their computer code). This final inversion is not needed if one wishes to compute a large multiple of an element of the Jacobian by the usual 'double and add' method; one can use instead the approach in [1], which uses the 'addflip' primitive $\xi, \xi' \mapsto -(\xi + \xi')$ (where ξ may equal ξ', for multiplication by -2) instead of the usual addition and doubling. Due to recent progress in index calculus methods for discrete logarithms (see [4], [5], and their references), it appears unlikely that the discrete logarithm problem in Jacobians of $C_{3,4}$ curves is worth using as a cryptographic primitive; the methods of this paper might still be useful for cover attacks on discrete logarithms of other curves.

For the general problem of computing effectively in Jacobians, our results in this article confirm the advantages of using the approach of [9, 10]. Even though we write down polynomials in this article, our algorithms work mainly via linear algebra in spaces of sections of line bundles, which we discuss here in the language of Riemann–Roch spaces $\mathcal{L}(D)$ associated to appropriate divisors on C. We perform almost no polynomial arithmetic, and instead use linear algebra on small matrices (essentially, 3×5 and 8×10, both explicitly and implicitly) which are often fairly structured. For example, our matrix may have two blocks that are almost in echelon form; hence an intelligent approach to Gaussian elimination produces efficient algorithms. We also optimise by hand any parts of the calculations that yield easily to an ad hoc trick, or to more systematic approaches. We hope that some of these methods can be useful elsewhere.

2. *Overview of our algorithms*

Consider a $C_{3,4}$ curve C of genus 3 over a large finite field $\mathbb{K}$ with $q = p^n$ elements. We assume that p, the characteristic of $\mathbb{K}$, is neither 2 nor 3 (similarly to [**2, 7**]; those articles also exclude characteristic 5). Let $P_\infty \in C$ denote the distinguished point at infinity and D a $\mathbb{K}$-rational divisor on C. Write $\mathcal{L}(D)$ for the Riemann–Roch space of rational functions on C with prescribed zeros and poles at D:

$$\mathcal{L}(D) = \{F \in \mathbb{K}(C) \mid (F) \geqslant -D\}.$$

Write $\mathcal{R}$ for the affine coordinate ring of $C - \{P_\infty\}$; hence $\mathcal{R} = \cup_{N \geqslant 0} \mathcal{L}(NP_\infty)$. By the definition of a $C_{3,4}$ curve, $\mathcal{R}$ is generated as a $\mathbb{K}$-algebra by two elements x, y whose valuations v_{P_∞} are given by

$$\begin{aligned} v_{P_\infty}(x) &= -3, \\ v_{P_\infty}(y) &= -4. \end{aligned}$$

The only relation between x and y is a $\mathbb{K}$-linear dependence $f(x,y) = 0$ between 1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3, $x^4 \in \mathcal{L}(12P_\infty)$. Thus, the affine coordinate ring of $C - \{P_\infty\}$ is $\mathcal{R} = \mathbb{K}[x,y]/(f(x,y))$. After a change of variables of the form

$$\begin{cases} x \mapsto u_1 x + u_2, \\ y \mapsto u_3 y + u_4 x + u_5, \end{cases} \qquad u_1, \ldots, u_5 \in \mathbb{K},\ u_1, u_3 \neq 0,$$

we can assume that the equation of the curve is

$$f(x,y) = y^3 - x^4 + p_2 x^2 y + p_1 xy + p_0 y + q_2 x^2 + q_1 x + q_0 = 0. \tag{1}$$

We further write $W^N = \mathcal{L}(NP_\infty)$; it is the subspace of $\mathcal{R}$ spanned by the monomials

$$\{x^i y^j \mid 3i + 4j \leq N\},$$

subject to the relation (1). To obtain a basis of W^N, we restrict ourselves to monomials with exponent pairs (i,j) with $j \leq 2$, or alternatively to pairs (i,j) with $i \leq 3$; this takes equation (1) into account. Note that

$$\begin{aligned} W^0 &= W^1 \\ &= W^2 = \mathbb{K} \cdot 1 \text{ is 1-dimensional,} \\ W^3 &= \mathbb{K} \cdot 1 + \mathbb{K} \cdot x \text{ is 2-dimensional,} \\ W^4 &= W^5 \\ &= \mathbb{K} \cdot 1 + \mathbb{K} \cdot x + \mathbb{K} \cdot y \text{ is 3-dimensional,} \end{aligned}$$

and for $N \geqslant 6$, W^N is $(N-2)$-dimensional.

Let D be an effective $\mathbb{K}$-rational divisor. Following the approach of [**9, 10**], we represent D by the space W_D^N defined by

$$W_D^N = \mathcal{L}(NP_\infty - D) \subset W^N$$

for some suitable positive integer N. If D is arbitrary of degree d, then we need to consider $N \geqslant d + 6$ (here, $6 = 2g$ for $g = 3$, the genus of the curve, to ensure that W_D^N is base-point free). However, for a typical divisor D, we can take $N = d + 4$ (here, $4 = g + 1$). Indeed, standard results from the theory of linear series on curves imply the following statement.

Proposition 2.1. *Let D be a typical effective $\mathbb{K}$-rational divisor of degree $d \geqslant 3$ on C. In particular, P_∞ does not belong to the support of D. Then*

$$\dim W_D^N = \begin{cases} 0 & \text{if } N \leq d+2, \\ N-d-2 & \text{if } N \geqslant d+2. \end{cases}$$

Furthermore, if $N \geqslant d+4$, then W_D^N is base-point free, and there exist two elements $F \in W_D^{d+3}$ and $G \in W_D^{d+4} - W_D^{d+3}$ that form a basis for the 2-dimensional subspace $W_D^{d+4} \subset W_D^N$, with the property that the only common vanishing of F and G occurs at D. In other words,

$$(F) = -(d+3)P_\infty + D + E,$$
$$(G) = -(d+4)P_\infty + D + E',$$

where E and E' are disjoint effective divisors.

Remark 2.2. Since F and G above vanish simultaneously only at D, we see that our basis $\{F, G\}$ for W_D^{d+4} is in fact an ideal generating set (an *IGS*) for D in the terminology of [10]. Thus, the ideal $\langle F, G\rangle = \mathcal{R}F + \mathcal{R}G$ of the affine coordinate ring $\mathcal{R}$ is the ideal of regular functions on $C - \{P_\infty\}$ vanishing on D. The quotient $\mathcal{A} = \mathcal{R}/\langle F, G\rangle$ is a d-dimensional $\mathbb{K}$-algebra describing the 'values' that a polynomial can take at the points of D. This makes sense even if the points of D are not all defined over $\mathbb{K}$, so long as the divisor D itself is $\mathbb{K}$-rational. Moreover, there is a $\mathbb{K}$-linear map

$$W^N/W_D^N \to \mathcal{A}$$

that is a bijection for $N \geqslant d+2$, for typical D with $d \geqslant 3$.

Remark 2.3. As mentioned above, a 'typical' divisor D is one that does not belong to a specific proper (hence at most $(d-1)$-dimensional) subvariety of the d-dimensional symmetric power $\mathrm{Sym}^d C$ parametrising the degree d effective divisors on C. For very large $q = |\mathbb{K}|$, the probability for a divisor D to be non-typical is $O(1/q)$. For enormous q, we do not expect ever to chance upon a non-typical divisor in our calculations. In case we do, it was already remarked in [2, 3] that we can then use a slower algorithm that works for all divisors. For example, we can use the larger space W_D^{d+6} instead of W_D^{d+4}, and adapt the algorithms accordingly.

We now discuss how we compute with typical elements of the Jacobian J of C. An element $\xi \in J(\mathbb{K})$ can be represented as the divisor class $[D - 3P_\infty]$ for some effective $\mathbb{K}$-rational divisor D with $\deg D = 3$. A typical class corresponds to a typical divisor D in a unique way. In turn, we represent D by a basis $\{F, G\}$ for the 2-dimensional space W_D^7. We can choose F and G to have the form

$$\begin{cases} F = x^2 + ay + bx + c & \in W_D^6 \subset W_D^7, \\ G = xy + dy + ex + f & \in W_D^7 - W_D^6. \end{cases} \tag{2}$$

Here $a \neq 0$ for typical divisors, and, for technical reasons, we also store the inverse a^{-1} along with the coefficients $a, b, \ldots, f \in \mathbb{K}$ in order to represent $\xi = [D - 3P_\infty]$.

Our addition algorithm begins with a typical pair $\xi, \xi' \in J(\mathbb{K})$ and computes their sum $\xi + \xi'$. Our doubling algorithm corresponds to the special case $\xi = \xi'$, in which case we compute $2\xi = \xi + \xi'$. In both cases, we first compute $\xi'' = -(\xi + \xi')$, the 'addflip' of the two elements in the terminology of [9, 10]. We then compute $\xi''' = -\xi''$. In practice, most of the use of Jacobian arithmetic will be to find a multiple $m \cdot \xi$ with $m \in \mathbb{Z}$. In that case, we can use the 'base -2 expansion' of [1] and only find the addflips ξ'' in the intermediate steps without any need for further negations.

We thus start with $\xi = [D - 3P_\infty]$ and $\xi' = [D' - 3P_\infty]$, with bases $\{F, G\}$ for W^7_D and $\{F', G'\}$ for $W^7_{D'}$. In our first phase (Steps 1 and 2 below) we produce a basis $\{F'', G''\}$ for $W^7_{D''}$, where $[D + D' + D'' - 9P_\infty] = 0$ in $J(\mathbb{K})$. Thus F'', G'' represent $\xi'' = [D'' - 3P_\infty] = -(\xi + \xi')$. In our second phase (Step 3 below), we find a basis $\{F''', G'''\}$ for $W^7_{D'''}$, where $[D'' + D''' - 6P_\infty] = 0$ in $J(\mathbb{K})$. At this point, F''', G''' represent $\xi''' = [D''' - 3P_\infty] = -\xi''$. Along the way, we also obtain the inverses $(a'')^{-1}$ and $(a''')^{-1}$ of the analogous coefficients in F'' and F'''. Here is a more detailed overview.

2.1. *Step* 1

This step comprises Sections 3–7 of this article. We first determine the space $W^{10}_{D+D'}$ along with its subspace $W^9_{D+D'}$. Since $D + D'$ is typical, we see that $\dim W^9_{D+D'} = 1$ and $\dim W^{10}_{D+D'} = 2$. Thus, there exists a basis $\{s, t\}$ for $W^{10}_{D+D'}$ of the form

$$\begin{aligned} s &= x^3 + s_1 y^2 + s_2 xy + s_3 x^2 + s_4 y + s_5 x + s_6 \\ &= 0x^2y + 1x^3 + \dots \qquad \in W^9_{D+D'} \subset W^{10}_{D+D'}, \\ t &= x^2y + t_1 y^2 + t_2 xy + t_3 x^2 + t_4 y + t_5 x + t_6 \\ &= 1x^2y + 0x^3 + \dots \qquad \in W^{10}_{D+D'} - W^9_{D+D'}, \end{aligned} \tag{3}$$

with $s_1, \dots, s_6, t_1, \dots, t_6 \in \mathbb{K}$. Our aim is thus to find s and t. Note that the principal divisor (s) has the form $(s) = D + D' + D'' - 9P_\infty$ for some effective $\mathbb{K}$-rational divisor D'' of degree 3. Hence, $[D + D' + D'' - 9P_\infty] = 0$, and $\xi'' = -(\xi + \xi')$, as desired.

Carrying out Step 1 depends on whether $D \neq D'$ (corresponding to addition) or $D = D'$ (corresponding to doubling).

2.1.1. *Point addition*

If $D \neq D'$, then D and D' typically have no point in common, in which case

$$W^{10}_{D+D'} = W^{10}_D \cap W^{10}_{D'}.$$

We find this intersection by looking for those elements of $W^{10}_{D'}$ that map to zero in the quotient ring $\mathcal{A} = \mathcal{R}/\langle F, G\rangle$ (hence such elements also vanish at D). We set up $\mathcal{A}$ in Section 3, compute how a basis for $W^{10}_{D'}$ maps to $\mathcal{A}$ in Section 4, and find the kernel of the map $(W^{10}_{D'} \to \mathcal{A})$ in Sections 6 and 7.

2.1.2. *Point doubling*

If $D = D'$, then we compute W^{10}_{2D} as the subspace of elements $L \in W^{10}_D$ whose differential dL also vanishes at D. This differs from the case of addition above only in computing a map $(W^{10}_D \to \mathcal{A}') : L \mapsto dL$ 'mod' $\langle F, G\rangle$, where $\mathcal{A}'$ is a 3-dimensional $\mathbb{K}$-vector space describing the 'values' that dL can take at the points of D. We describe this in Section 5, the analogue of Section 4 with respect to point addition. Thereafter, the remaining calculations in Sections 6 and 7 proceed similarly to the case of point addition.

2.2. *Step* 2

This step comprises Sections 8 and 9 below. At this stage, we have a basis $\{s,t\}$ for $W^{10}_{D+D'}$ as in (3), which is typically an IGS for $D+D'$ as in Remark 2.2. Thus,

$$(s) = D + D' + D'' - 9P_\infty,$$
$$(t) = D + D' + E'' - 10P_\infty,$$

with D'' and E'' disjoint. We note that $sW^8 = W^{17}_{D+D'+D''}$ as in [9]. Taking a basis of monomials for W^8, we see that the following is a basis for sW^8:

$$\{s, xs, ys, x^2s, xys, y^2s\}.$$

We next compute $W^7_{D''}$. It is the 'quotient', as in [10], of $sW^8 = W^{17}_{D+D'+D''}$ by the IGS $\{s,t\}$ for $D+D'$:

$$\begin{aligned} W^7_{D''} &= sW^8 \div \{s,t\} \\ &= \{\ell \in W^7 \mid s\ell, t\ell \in sW^8\} \\ &= \{\ell \in W^7 \mid t\ell \in sW^8\}. \end{aligned} \tag{4}$$

Since W^7 has basis $\{1, x, y, x^2, xy\}$ and we have a basis for sW^8, the condition $t\ell \in sW^8$ amounts to finding a linear combination of t, xt, yt, x^2t, and xyt that is also a linear combination of s, xs, ys, x^2s, xys, and y^2s. Equivalently, we must determine the intersection of the 5- and 6-dimensional subspaces tW^7 and sW^8 inside W^{17}. This intersection will have a basis of the form $\{tF'', tG''\}$, where $\{F'', G''\}$ are a basis for the space $W^7_{D''}$ of solutions for ℓ in (4) above. Note that the intersection appears to take place in the 15-dimensional space W^{17} (where typical 5- and 6-dimensional spaces do not intersect), but actually occurs inside the 9-dimensional space $W^{17}_{D+D'}$, which contains (in fact, is generated by) the two subspaces tW^7 and sW^8. This reduces the amount of linear algebra that we need to perform. We formalise this in the following lemma.

LEMMA 2.4. *Let $\ell \in W^7$. Then $t\ell \in sW^8$ if and only if $t\ell \in sW^8 + W^9$. (This is equivalent to saying that $t\ell$ is congruent to an element of sW^8 in the quotient space W^{17}/W^9.)*

Proof. Trivially, $t\ell \in sW^8$ implies that $t\ell \in sW^8 + W^9$. To prove the converse, suppose that $t\ell = s\ell' + \ell''$, with $\ell' \in W^8$ and $\ell'' \in W^9$. Note that $t\ell, s\ell' \in W^{17}_{D+D'}$. Then, since $\ell'' \in W^9$, we obtain

$$\ell'' = t\ell - s\ell' \in W^9_{D+D'} = \mathbb{K} \cdot s,$$

and so we can write

$$t\ell - s\ell' = \alpha s, \qquad \alpha \in \mathbb{K},$$

from which we have

$$t\ell = (\ell' + \alpha)s \in sW^8,$$

as required.

Note incidentally that $sW^8 \cap W^9 = \mathbb{K}s$, so $\dim(sW^8 + W^9) = 6 + 7 - 1 = 12$. □

We conclude from the above discussion that we can obtain $F'', G'' \in W^7_{D''}$ as follows.

1. Denote F'' or G'' by $\ell = d_1 + d_2x + d_3y + d_4x^2 + d_5xy$. Here $\{d_4, d_5\} = \{0, 1\}$ in some order, and we must solve for d_1, d_2, d_3 such that $t\ell \in sW^8 + W^9$.
2. Find $\overline{C_1}, \ldots, \overline{C_5}$, the images of t, xt, yt, x^2t, xyt in the 3-dimensional quotient space $W^{17}/(sW^8 + W^9)$. (One can moreover see from Section 9 that a basis for this quotient space is given by the images of x^2y, xy^2, and x^2y^2.)
3. The three resulting equations $d_1\overline{C_1} + \ldots + d_5\overline{C_5} = 0$ allow us (in the typical case) to express d_1, d_2, d_3 in terms of d_4, d_5. We thus get a basis
$$\{(c'', b'', a'', 1, 0), (f'', e'', d'', 0, 1)\}$$
for the space $\{(d_1, \ldots, d_5) \mid d_1\overline{C_1} + \ldots + d_5\overline{C_5} = 0\}$. This corresponds to elements $F'' = c'' + b''x + a''y + x^2$ and $G'' = f'' + e''x + d''y + xy$ that form a basis for $W^7_{D''}$. The structure of the system of linear equations allows us to find $(a'')^{-1}$ along the way at minimal extra cost.

2.3. *Step* 3

This step comprises Section 10. At this point we have obtained our IGS $\{F'', G''\}$ for the divisor D'', where $\xi'' = [D'' - 3P_\infty] = -(\xi + \xi')$. We also know $(a'')^{-1}$. We now discuss how to negate this to obtain $\xi''' = -\xi'' = \xi + \xi'$. The divisor of F'' has the form $(F'') = D'' + D''' - 6P_\infty$ for some effective $\mathbb{K}$-rational divisor D''', and it follows that $\xi''' = [D''' - 3P_\infty]$. We thus seek the polynomials
$$F''' = x^2 + a'''y + b'''x + c''' \in W^6_{D'''},$$
$$G''' = xy + d'''y + e'''x + f''' \in W^7_{D'''},$$
that represent D''' and hence ξ'''. We easily observe that $F'' = F'''$, since $W^6_{D'''} = W^6_{D''} = W^6_{D''+D'''} = \mathbb{K}\cdot F''$. Hence $a''' = a''$, so we trivially know the inverse $(a''')^{-1}$.

It remains to find G'''. Analogously to (4) and to Lemma 2.4, we have $F''W^8 = W^{14}_{D''+D'''}$, and so
$$\begin{aligned} W^7_{D'''} &= F''W^8 \div \{F'', G''\} \\ &= \{\ell \in W^7 \mid G''\ell \in F''W^8\} \\ &= \{\ell \in W^7 \mid G''\ell \in F''W^8 + W^6\}. \end{aligned} \tag{5}$$
We thus have $G''G''' + F''H = 0$ for some $H \in W^8$. We can in principle carry out an analogous computation to Step 2, but this case is small enough that it is worth our while to carry out the calculation directly and to hand-optimise it to find G'''. We also find an explicit expression for H, which is useful in a different context that we encounter in Section 5.

3. *Preliminary to both point addition and doubling*

Consider the input $F = x^2 + ay + bx + c$ and $G = xy + dy + ex + f \in W^7_D$ representing a divisor D of degree 3. We know that $\langle F, G\rangle = \mathcal{R}F + \mathcal{R}G$ is the ideal of regular functions on $C - \{P_\infty\}$ vanishing at D. Our goal is to be able to compute in the algebra of 'values' of polynomials at D, given by
$$\mathcal{A} = \mathcal{R}/\langle F, G\rangle.$$

Since $\deg D = 3$, we have $\dim_{\mathbb{K}} \mathcal{A} = 3$. Given $u \in \mathcal{R}$, the element $\overline{u} \in \mathcal{A}$ denotes the reduction of u modulo $\langle F, G \rangle$.

Lemma 3.1. *A $\mathbb{K}$-basis for $\mathcal{A}$ is $\{\overline{1}, \overline{x}, \overline{y}\}$. Furthermore,*

$$\overline{x}^2 = -a\overline{y} - b\overline{x} - c\overline{1}, \tag{6}$$

$$\overline{xy} = -d\overline{y} - e\overline{x} - f\overline{1}, \tag{7}$$

$$\overline{y}^2 = -g\overline{y} - h\overline{x} - i\overline{1}, \tag{8}$$

where a, b, c, d, e and f are the coefficients of F and G, and

$$\begin{aligned} g &= a^{-1}\left(c + d(d-b)\right) + e, \\ h &= a^{-1}(ed - f), \\ i &= a^{-1}\left(ec + f(d-b)\right). \end{aligned} \tag{9}$$

Proof. Equations (6) and (7) reflect the fact that $F, G \in \langle F, G \rangle$. Equations (8) and (9) come from expanding $(y+e)F - (x+b-d)G \in \langle F, G \rangle$. Equations (6), (7) and (8) show that every element $\overline{u} \in \mathcal{A}$ can be written as a $\mathbb{K}$-linear combination of $\overline{1}, \overline{x}$ and $\overline{y}$. Since $\mathcal{A}$ is 3-dimensional, we obtain that $\overline{1}$, $\overline{x}$ and $\overline{y}$ are linearly independent. □

Given $u \in \mathcal{R}$, we represent its reduction $\overline{u} = \alpha\overline{1} + \beta\overline{x} + \gamma\overline{y} \in \mathcal{A}$ by the column vector

$$B_u = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} \in \mathbb{K}^3.$$

We then have the following proposition.

Proposition 3.2. *Assume given F and G, as well as the inverse a^{-1}.*

(i) *For B_u defined as above, we have*

$$B_{xu} = T_x B_u, \qquad B_{yu} = T_y B_u,$$

where T_x and T_y are the matrices of multiplication by x and y on $\mathcal{A}$, with respect to the ordered basis $\{\overline{1}, \overline{x}, \overline{y}\}$:

$$T_x = \begin{pmatrix} 0 & -c & -f \\ 1 & -b & -e \\ 0 & -a & -d \end{pmatrix}, \qquad T_y = \begin{pmatrix} 0 & -f & -i \\ 0 & -e & -h \\ 1 & -d & -g \end{pmatrix}.$$

(ii) *We have the entries of T_x for free (that is, at a cost of $0M$); multiplying T_x by a vector B_u costs $6M$.*

(iii) *We can compute the entries of T_y using $7M$. Once we know T_y, multiplying $T_y \cdot B_u$ to get B_{yu} also costs $6M$.*

(iv) *If we do not already know T_y, we can obtain B_{yu} directly at a cost of $11M$.*

Proof. The proof of parts (i)–(iii) is immediate by inspecting (6)–(9) above. As for part (iv), we need to compute the reduction modulo $\langle F, G \rangle$ of $v = \alpha y + \beta xy + \gamma y^2$ in order to obtain B_{yu}. Now v is congruent to $w = v - \gamma a^{-1}(yF - xG)$, so we have

$$\begin{aligned} w &= \gamma a^{-1} f x + (\alpha - \gamma a^{-1} c) y + \gamma a^{-1} e x^2 + [\beta - \gamma a^{-1}(b-d)] xy \\ &= \delta x + \varepsilon y + \zeta x^2 + \eta xy \end{aligned}$$

where $\delta, \varepsilon, \zeta, \eta$ can be calculated using $5M$ (first find γa^{-1}).

Then the reduction modulo $\langle F, G\rangle$ of v is $w - \zeta F - \eta G$, whence

$$B_{yu} = \begin{pmatrix} 0 \\ \delta \\ \varepsilon \end{pmatrix} - \zeta \begin{pmatrix} c \\ b \\ a \end{pmatrix} - \eta \begin{pmatrix} f \\ e \\ d \end{pmatrix},$$

costing an additional $6M$. □

4. *First stage of addition of two distinct divisor classes: setting up a system of equations whose solution will determine $W^{10}_{D+D'}$*

Our input is now the descriptions of two typical degree 3 divisors D, D', given by pairs $F, G \in W^7_D$ and $F', G' \in W^7_{D'}$. In other words, we assume given the coefficients $a, \ldots, f$ and $a', \ldots, f'$ of $F = x^2 + ay + bx + c$, $G = xy + dy + ex + f$, $F' = x^2 + a'y + b'x + c'$, and $G' = xy + d'y + e'x + f'$, along with the inverses a^{-1} and $(a')^{-1}$. Our goal in this section is to determine a 3×5 matrix M whose five columns are respectively $B_{F'}$, $B_{xF'}$, $B_{yF'}$, $B_{G'}$ and $B_{xG'}$, in the notation of Section 3. The kernel of M will then correspond to $W^{10}_{D+D'}$ as follows: if $v = (c_1, c_2, c_3, c_4, c_5)^{\mathbf{T}}$ is a (column) vector in $\mathbb{K}^5$, then we identify it with the linear combination

$$L = (c_1 + c_2x + c_3y)F' + (c_4 + c_5x)G' \in \langle F', G'\rangle \cap W^{10} = W^{10}_{D'}.$$

Then $Mv = 0$ if and only if $\overline{L} = \overline{0}$ in $\mathcal{A}$, which is equivalent to

$$L \in \langle F, G\rangle \cap W^{10}_{D'} = W^{10}_{D+D'},$$

where the last equality follows from the fact that D and D' are disjoint.

Proposition 4.1. *Given F, G, F', G' and a^{-1} as above, we can compute the matrix M at a cost of $22M$.*

Proof. The first column $B_{F'}$ of M comes from

$$\begin{aligned} \overline{F'} &\equiv \overline{F' - F} \bmod \langle F, G\rangle \\ &= (a' - a)y + (b' - b)x + (c' - c). \end{aligned}$$

Hence we get the following result for free (that is, $0M$):

$$B_{F'} = \begin{pmatrix} c' - c \\ b' - b \\ a' - a \end{pmatrix}.$$

We similarly obtain the fourth column $B_{G'}$ of M for free:

$$B_{G'} = \begin{pmatrix} f' - f \\ e' - e \\ d' - d \end{pmatrix}.$$

We now compute the second and fifth columns $B_{xF'}$ and $B_{xG'}$ by noting the block matrix equation involving the matrix T_x of Proposition 3.2:

$$\left(B_{xF'} \mid B_{xG'}\right) = T_x \left(B_{F'} \mid B_{G'}\right).$$

Since the first column of T_x is $(0, 1, 0)^{\mathbf{T}}$, its interaction with the first row of $(B_{F'} \mid B_{G'})$ can be computed without any multiplication in $\mathbb{K}$. We must then multiply the 3×2 submatrix consisting of the second and third columns of T_x with the 2×2 submatrix consisting of the second and third rows of $(B_{F'} \mid B_{G'})$. This can be done at a cost of $11M$ using a Strassen's type multiplication on a 2×2 sub-block, which saves one multiplication over the 'naive' method. Finally, we use Proposition 3.2(iv) to compute the third column $B_{yF'}$ from $B_{F'}$ at a further cost of $11M$. This concludes the proof. □

5. *First stage of doubling a divisor class: setting up a system of equations whose solution will determine W^{10}_{2D}*

In this section, we take $D' = D$, so our input consists of two polynomials $F, G \in W^7_D$, where D is a typical degree 3 divisor. As before, we write $F = x^2 + ay + bx + c$ and $G = xy + dy + ex + f$, so our input consists of the coefficients $a, \dots, f$, as well as a^{-1}. Analogously to Section 4, we will construct a 3×5 matrix, which we also label as M, whose columns represent the 'reductions modulo $\langle F, G\rangle$' of the differential forms $dF, d(xF), d(yF), dG, d(xG)$. These differential forms are regular on $C - \{P_\infty\}$, so we really want the columns of M to represent the 'values' of $dF, \dots, d(xG)$ at the points of D, much in the same way that elements of the algebra $\mathcal{A}$ describe values at D.

As in Section 4, a column vector $v = (c_1, c_2, c_3, c_4, c_5)^{\mathbf{T}} \in \mathbb{K}^5$ represents

$$L = (c_1 + c_2 x + c_3 y)F + (c_4 + c_5 x)G \in \langle F, G\rangle \cap W^{10} = W^{10}_D.$$

This time, $Mv = 0$ if and only if the differential form $dL = c_1\, dF + c_2\, d(xF) + c_3\, d(yF) + c_4\, dG + c_5\, d(xG)$ vanishes at D. Since generically the points of D are distinct, this means that such an L vanishes to second order at the points of D, so we obtain that $Mv = 0$ if and only if $L \in W^{10}_{2D}$. Since, for example, $d(xF) = x\, dF + F\, dx$, and F vanishes at D, we see that the value of $d(xF)$ at D is the same as that of $x\, dF$, and so forth. Thus the columns of our matrix M can be taken to represent suitable 'reductions modulo $\langle F, G\rangle$':

$$\overline{dF}, \overline{x\, dF}, \overline{y\, dF}, \overline{dG}, \overline{x\, dG},$$

which we now proceed to explain. We write $d\mathcal{R}$ for the $\mathcal{R}$-module of differential forms on $C - \{P_\infty\}$; then $d\mathcal{R}$ is generated by dx and dy, with the sole relation $df = 0$ for $f(x, y)$ the equation of the curve in (1).

Lemma 5.1. *The $\mathcal{R}$-module $d\mathcal{R}$ is free of rank 1, and is generated by a differential form ω_0 such that*

$$dx = f_y \omega_0, \qquad dy = -f_x \omega_0, \tag{10}$$

where $f_y = \partial f/\partial y$ and $f_x = \partial f/\partial x$.

Proof. The relation $df = 0$ means that

$$f_x\, dx + f_y\, dy = 0. \tag{11}$$

Since C is nonsingular, f, f_x, and f_y have no common zeros over the algebraic closure $\overline{\mathbb{K}}$. We can therefore write

$$1 = r_1 f_x + r_2 f_y \qquad \text{for some } r_1, r_2 \in \mathcal{R}, \tag{12}$$

and we define

$$\omega_0 = r_2\, dx - r_1\, dy \in d\mathcal{R}.$$

Some algebra with (11) and (12) then implies equation (10). In particular, $dx, dy \in \mathcal{R}\omega_0$ so that ω_0 generates $d\mathcal{R}$ as an $\mathcal{R}$-module. To see that the annihilator of ω_0 is 0, one can argue directly from (11), (12) and the definition of ω_0, or one can use the fact that $d\mathcal{R}$ is a rank one projective module over the Dedekind domain $\mathcal{R}$, and is hence free, as it has a global generator ω_0. □

At this stage, we can state precisely what we mean by the reduction modulo $\langle F, G\rangle$ of the differential forms $dF, \dots, x\,dG$.

Corollary 5.2. *Define the reduction of an element of $d\mathcal{R}$ to be its image in $\mathcal{A}' = d\mathcal{R}/\langle F, G\rangle d\mathcal{R}$. Then $\mathcal{A}'$ is a free $\mathcal{A}$-module of rank 1, generated by the reduction $\overline{\omega_0}$.*

We can in fact choose any generator $\overline{\omega}$ of $\mathcal{A}'$, not just $\overline{\omega_0}$. Our choice of $\overline{\omega}$ below was inspired by a careful reading of the formulae for doubling in [7]. This saves us several multiplications over using the generator $\overline{\omega_0}$.

Lemma 5.3. *For a typical divisor D, the following hold.*

(i) *The reduction $\overline{dF}$ generates the $\mathcal{A}$-module $\mathcal{A}'$.*

(ii) *There exist $G_1 \in W^7, H_1 \in W^8$ such that $FH_1 + GG_1 = 0$, and $\overline{G_1}$ is a unit in the ring $\mathcal{A}$.*

(iii) *There exists a generator $\overline{\omega} \in \mathcal{A}'$ such that*

$$\overline{dF} = \overline{G_1\omega}, \qquad \overline{dG} = -\overline{H_1\omega}. \tag{13}$$

Proof. The first assertion holds because F typically vanishes to order exactly one at each point of D, so dF is nonzero at the points of D. The second assertion comes from our results in Subsection 2.3 and Section 10 (replace $\{F'', G'', G''', H\}$ there by $\{F, G, G_1, H_1\}$; no circular reasoning is involved). The divisor of F is $(F) = D + D_1 - 6P_\infty$ for a 'complementary' divisor D_1 of D, which is typically disjoint from D. (In the original setting of Section 10, D''' was the complementary divisor of D''). Moreover, the only points where F and G_1 simultaneously vanish are typically those of D_1, since $\{F, G_1\}$ are an IGS for D_1 (indeed, they are a basis for $W^7_{D_1}$). Thus G_1 does not vanish at any point of D, so $\overline{G_1}$ is invertible in $\mathcal{A}$, as claimed. For the third assertion, the first part of equation (13) serves to define a generator $\overline{\omega}$ in light of parts (i) and (ii) above; the second part of (13) follows upon expanding the equation $d(FH_1 + GG_1) = 0$, reducing modulo $\langle F, G\rangle$, and cancelling $\overline{G_1}$. □

The upshot of the above discussion is that we can represent an element $\mathcal{A}'$, of the form $\overline{u\omega}$ with a unique $\overline{u} \in \mathcal{A}$, by the column vector $B_u \in \mathbb{K}^3$. In particular, we represent $\overline{dF} = \overline{G_1\omega}$ by B_{G_1}, and $\overline{dG} = \overline{-H_1\omega}$ by B_{-H_1}. Hence, we can take the columns of our matrix M to be

$$B_{G_1}, B_{xG_1}, B_{yG_1}, B_{-H_1}, B_{-xH_1}.$$

Proposition 5.4. *Given F, G, a^{-1}, the entries of the matrix M can be computed at a cost of $34M$.*

Proof. We first compute G_1 and H at a cost of $10M$, by Proposition 10.1(ii) (recall that we replace $\{F'', G'', G''', H\}$ there by $\{F, G, G_1, H_1\}$). For later use, we also compute the matrix T_y as in Proposition 3.2(iii). This costs us only a further $5M$, since we have already computed the expression $a^{-1}(c+d(d-b))$ as part of computing G_1, H_1 (when we computed $(a'')^{-1}\ell$ in the context of the proof of Proposition 10.1). As a result, we now have g, h, and i.

Our next step is to reduce G_1 and H_1 modulo $\langle F, G\rangle$, so as to obtain B_{G_1} and B_{H_1}; the extra negation to get B_{-H_1} costs nothing. We reduce $G_1 \equiv G_1 - G$ at no multiplicative cost, and since $G_1 - G \in \mathbb{K}\cdot 1 + \mathbb{K}\cdot x + \mathbb{K}\cdot y$ from our formulae for G_1 and G, we obtain B_{G_1} for free. As for H_1, our formulae give $H_1 = -y^2 + ax^2 +$ ($\mathbb{K}$-linear combination of $1, x, y$); hence by (8)

$$H_1 \equiv H_1 + y^2 + gy + hx + i - aF \in \mathbb{K}\cdot 1 + \mathbb{K}\cdot x + \mathbb{K}\cdot y$$

will be reduced. The only multiplication needed is to obtain aF, which costs $2M$ to obtain a^2, ac, since we have already found ab as part of finding G_1, H_1.

Finally, we multiply T_x by the 3×2 matrix $(B_{G_1} \mid B_{-H_1})$ to obtain B_{xG_1} and B_{-xH_1} at a cost of $11M$, as in the proof of Proposition 4.1; we also obtain $B_{yG_1} = T_y B_{G_1}$ at a cost of $6M$, by Proposition 3.2(iii). □

6. *Finding the kernel of M*

To find $W^{10}_{D+D'}$ in the case of addition, and W^{10}_{2D} in the case of doubling, we must now determine the kernel of our 3×5 matrix M from Sections 4 and 5, respectively. A vector

$$v = \begin{pmatrix} c_1 \\ \vdots \\ c_5 \end{pmatrix}$$

satisfying $Mv = 0$ corresponds in both cases to

$$L = c_1F' + c_2xF' + c_3yF' + c_4G' + c_5xG' \in W^{10}_{D+D'},$$

since $D = D'$ in the case of doubling. Our later calculations will be significantly simplified if we can find a basis $\{s, t\}$ for $W^{10}_{D+D'}$ of the following special 'monic' form:

$$\begin{aligned} s &= x^3 + (\mathbb{K}\text{-linear combination of } y^2, xy, x^2, y, x, 1) \\ &= 0x^2y + 1x^3 + \dots \quad \in W^{9}_{D+D'}\,, \\ t &= x^2y + (\mathbb{K}\text{-linear combination of } y^2, xy, x^2, y, x, 1) \\ &= 1x^2y + 0x^3 + \dots \quad \in W^{10}_{D+D'}\,. \end{aligned}$$

To do this, we actually find the kernel of a modification M' of M: if M has columns

$$\left(\begin{array}{c|c|c|c|c} K_1 & K_2 & K_3 & K_4 & K_5 \end{array} \right),$$

then M' has columns

$$\left(\begin{array}{c|c|c|c|c} K_1 & K_4 & K_3 - K_5 & K_2 & K_5 \end{array} \right).$$

Note that M' can be calculated from M without any field multiplications. In the case of addition, the columns of M' correspond to

$$\left(\begin{array}{c|c|c|c|c} \overline{F'} & \overline{G'} & \overline{yF' - xG'} & \overline{xF'} & \overline{xG'} \end{array} \right),$$

and a vector $(c'_1, \ldots, c'_5)^{\mathbf{T}} \in \ker M'$ corresponds to a combination

$$c'_1 F' + c'_2 G' + c'_3(yF' - xG') + c'_4(xF') + c'_5(xG') \in W^{10}_{D+D'};$$

an analogous statement holds in the case of doubling.

We shall see in Section 7 that the 'monic' element s comes from a kernel vector with $c'_5 = 0, c'_4 = 1$, while t comes from a kernel vector with $c'_5 = 1, c'_4 = 0$. We thus perform row reduction on M' so as to express the unknown cofficients c'_1, c'_2, c'_3 in terms of the free variables c'_4 and c'_5.

We write the entries of the modified matrix M' as:

$$M' = \begin{pmatrix} A_1 & B_1 & C_1 & D_1 & E_1 \\ A_2 & B_2 & C_2 & D_2 & E_2 \\ A_3 & B_3 & C_3 & D_3 & E_3 \end{pmatrix},$$

with rows $R_i = (A_i\ B_i\ C_i\ D_i\ E_i)$, $i = 1, 2, 3$.

Proposition 6.1. *A basis for the kernel of M' can be obtained using $39M, 1I$.*

Proof. Apply row operations to the rows R_1, R_2, R_3. This transforms M' into the following echelon form with the same kernel:

$$\begin{pmatrix} A_1 & B_1 & C_1 & D_1 & E_1 \\ 0 & D & \sigma_1 & \sigma_2 & \sigma_3 \\ 0 & 0 & U & \sigma_4 & \sigma_5 \end{pmatrix}, \tag{14}$$

where the new rows are $R'_1 = R_1$, $R'_2 = A_1R_2 - A_2R_1$, $R'_3 = \Delta_{12}R_3 - \Delta_{13}R_2 + \Delta_{23}R_1$. Here the quantities Δ_{ij} are 2×2 minors coming from the first two columns of M', as given by the formulae below. This requires us to compute the following quantities at a cost of $21M$:

$$\begin{aligned} D = \Delta_{12} &= A_1B_2 - A_2B_1\,, \\ \Delta_{13} &= A_1B_3 - A_3B_1\,, \\ \Delta_{23} &= A_2B_3 - A_3B_2\,, \\ \sigma_1 &= A_1C_2 - A_2C_1\,, \\ \sigma_2 &= A_1D_2 - A_2D_1\,, \\ \sigma_3 &= A_1E_2 - A_2E_1\,, \\ U &= \Delta_{12}C_3 - \Delta_{13}C_2 + \Delta_{23}C_1\,, \\ \sigma_4 &= \Delta_{12}D_3 - \Delta_{13}D_2 + \Delta_{23}D_1\,, \\ \sigma_5 &= \Delta_{12}E_3 - \Delta_{13}E_2 + \Delta_{23}E_1\,. \end{aligned}$$

To perform back substitution, we need to obtain

$$A_1^{-1}, \qquad D^{-1}, \qquad \text{and} \qquad U^{-1}. \tag{15}$$

For this, we perform

$$Q_1 = A_1D, \qquad Q_2 = Q_1U, \qquad Q_3 = Q_2^{-1},$$
$$U^{-1} = Q_1Q_3, \qquad Q_4 = UQ_3, \qquad D^{-1} = A_1Q_4, \qquad A_1^{-1} = DQ_4,$$

so the inverses in (15) above can all be produced using $6M, 1I$. Back substitution performed on the matrix in (14) now costs a further $6M + 6M = 12M$ to find the two basis elements $(\alpha, \beta, \gamma, 1, 0)^{\mathbf{T}}$ and $(\delta, \varepsilon, \zeta, 0, 1)^{\mathbf{T}}$ of the kernel, corresponding to s and t. (Solve for γ, β, α, ζ, ε, δ in that order). □

7. *Finding s and t*

At this point, we have obtained a basis $\{v_1', v_2'\}$ for the kernel of M' of the form

$$v_1' = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ 1 \\ 0 \end{pmatrix},$$

corresponding to s, and

$$v_2' = \begin{pmatrix} \delta \\ \varepsilon \\ \zeta \\ 0 \\ 1 \end{pmatrix},$$

corresponding to t. The desired elements s and t are

$$\begin{cases} s = \alpha F' + \beta G' + \gamma(yF' - xG') + xF', \\ t\ = \delta F' + \varepsilon G' + \zeta(yF' - xG') + xG'. \end{cases}$$

(This includes the case of doubling, for which $F' = F$ and $G' = G$.) We now have the following.

PROPOSITION 7.1. *Given v_1' and v_2' as above, s and t can be obtained at a cost of $18M$.*

Proof. To calculate s and t using as few multiplications as possible, we illustrate the following steps for s (those for t follow similarly). We have

$$s = (\alpha + \gamma y)F' + (\beta - \gamma x)G' + xF',$$

where

$$F' = x^2 + a'y + b'x + c',$$
$$G' = xy + d'y + e'x + f'.$$

We now wish to expand s as a linear combination of the monomials x^3, y^2, xy, x^2, y, x, and 1. Write

$$\begin{aligned} s = (\alpha + \gamma y)x^2 + (\beta - \gamma x)xy + xF' \qquad & \text{(I)} \\ + (\alpha + \gamma y)(a'y + b'x + c) + (\beta - \gamma x)(d'y + e'x + f'). \qquad & \text{(II)} \end{aligned}$$

The terms in (I) do not involve any multiplication in K (note that the leading coefficient x^3 comes from xF'). The terms in (II) can be written as

$$\begin{aligned} (\alpha + \gamma y)b'x + (\beta - \gamma x)d'y \qquad & \text{(III)} \\ + (\alpha + \gamma y)(a'y + c) + (\beta - \gamma x)(e'x + f'), \qquad & \text{(IV)} \end{aligned}$$

where (III) requires $3M$ to form $\gamma(b'-d')xy+\alpha b'x+\beta d'y$ and (IV) requires $6M$ in total, using Karatsuba's method for each of the two terms. The total cost is thus $9M$ to find s.

Finding t also requires $9M$; the only essential difference is that xF' becomes xG' in the analogue of (I).

The total cost to find s and t is thus $18M$. Note from the computation that s and t are both monic in the sense that their 'leading' coefficient is 1, and that moreover the coefficient of x^3 in t is zero. □

8. *Calculating xt, yt, x^2t, xyt and xs, ys, x^2s, xys, y^2s*

We have now computed $s, t \in W^{10}_{D+D'}$. We let $s_1, \dots, s_6, t_1, \dots, t_6$ be the coefficients of s and t, as in equation (3) above. As we saw in Subsection 2.2, we now wish to find $F'', G'' \in W^7_{D''}$ via

$$\mathbb{K}F'' + \mathbb{K}G'' = \{\ell \in W^7 \mid \ell t \in sW^8 + W^9\}.$$

Thus, ℓ is a $\mathbb{K}$-linear combination of the basis $\{t, xt, yt, x^2t, xyt\}$ for tW^7 that is congruent to a $\mathbb{K}$-linear combination of the basis $\{s, xs, ys, x^2s, xys, y^2s\}$ for sW^8 in the quotient space W^{17}/W^9. We express these multiples of s and t in terms of the following ordered basis for W^{17}:

$$\{1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3, x^3y, x^2y^2, xy^3, y^4, x^3y^2\}. \tag{16}$$

To work in W^{17}/W^9, we need only the coefficients of the last eight monomials:

$$\{x^2y, xy^2, y^3, x^3y, x^2y^2, xy^3, y^4, x^3y^2\}. \tag{17}$$

Lemma 8.1. *Given s and t as above, producing the relevant coefficients of xt, yt, x^2t, xyt, xs, ys, x^2s, xys, and y^2s requires $2M$.*

Proof. Our choice of basis for W^{17} means that we use the equation of the curve (1) to eliminate all monomials x^iy^j with $i \geqslant 4$. Carrying this out for the multiples of s and t above, we obtain the matrix N given by

$$N=\begin{pmatrix}
t_6 & 0 & 0 & t_3q_0 & 0 & s_6 & q_0 & 0 & s_3q_0 & 0 & 0\\
t_5 & t_6 & 0 & t_3q_1 & 0 & s_5 & s_6+q_1 & 0 & q_0+s_3q_1 & 0 & 0\\
t_4 & 0 & t_6 & q_0+t_3p_0 & 0 & s_4 & p_0 & s_6 & s_3p_0 & q_0 & 0\\
t_3 & t_5 & 0 & t_6+t_3q_2 & 0 & s_3 & s_5+q_2 & 0 & s_6+q_1+s_3q_2 & 0 & 0\\
t_2 & t_4 & t_5 & q_1+t_3p_1 & t_6 & s_2 & s_4+p_1 & s_5 & p_0+s_3p_1 & s_6+q_1 & 0\\
t_1 & 0 & t_4 & p_0 & 0 & s_1 & 0 & s_4 & 0 & p_0 & s_6\\
0 & t_3 & 0 & t_5 & 0 & 1 & s_3 & 0 & s_5+q_2 & 0 & 0\\
1 & t_2 & t_3 & t_4+q_2+t_3p_2 & t_5 & 0 & s_2+p_2 & s_3 & s_4+p_1+s_3p_2 & s_5+q_2 & 0\\
0 & t_1 & t_2 & p_1 & t_4 & 0 & s_1 & s_2 & 0 & s_4+p_1 & s_5\\
0 & 0 & t_1 & t_3 & 0 & 0 & 1 & s_1 & s_3 & 0 & s_4\\
0 & 1 & 0 & t_2 & t_3 & 0 & 0 & 1 & s_2+p_2 & s_3 & 0\\
0 & 0 & 1 & t_1+p_2 & t_2 & 0 & 0 & 0 & s_1 & s_2+p_2 & s_3\\
0 & 0 & 0 & 0 & t_1 & 0 & 0 & 0 & 1 & s_1 & s_2\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & s_1\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

whose columns represent, in order, t, xt, yt, x^2t, xyt, s, xs, ys, x^2s, xys, and y^2s with respect to our full basis for W^{17} given in (16) above. However, since we only need the last eight rows of N to indicate the values in W^{17}/W^9, we only need to work with the matrix N' given by

$$N'=\begin{pmatrix} 1 & t_2 & t_3 & t_4+q_2+t_3p_2 & t_5 & 0 & s_2+p_2 & s_3 & s_4+p_1+s_3p_2 & s_5+q_2 & 0 \\ 0 & t_1 & t_2 & p_1 & t_4 & 0 & s_1 & s_2 & 0 & s_4+p_1 & s_5 \\ 0 & 0 & t_1 & t_3 & 0 & 0 & 1 & s_1 & s_3 & 0 & s_4 \\ 0 & 1 & 0 & t_2 & t_3 & 0 & 0 & 1 & s_2+p_2 & s_3 & 0 \\ 0 & 0 & 1 & t_1+p_2 & t_2 & 0 & 0 & 0 & s_1 & s_2+p_2 & s_3 \\ 0 & 0 & 0 & 0 & t_1 & 0 & 0 & 0 & 1 & s_1 & s_2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & s_1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

This shows that we only need to compute the multiples $t_3 \cdot p_2$ and $s_3 \cdot p_2$, thereby proving our result. □

9. *Finding F'', G'' that span the subspace $W^7_{D''}$*

We refer to the columns of N' above as

$$N' = \left(\; C_1 \; \middle| \; C_2 \; \middle| \; C_3 \; \middle| \; \dots \; \middle| \; C_{11} \; \right).$$

We now need to find a linear combination of the first five columns $C_1, \dots, C_5$ of N', corresponding to a basis for the image of tW^7 in W^{17}/W^9, which belongs to the span of the last six columns $C_6, \dots, C_{11}$ of N', corresponding to the image of sW^8 in W^{17}/W^9. Let V denote the 5-dimensional subspace of $\mathbb{K}^8$ spanned by the columns $C_6, \dots, C_{11}$ (of course, the zero column C_6 is irrelevant), and let $\mathcal{T}$ denote the set of columns $\{C_1, \dots, C_5\}$: we thus want to find combinations of columns of $\mathcal{T}$ that map to zero in the 3-dimensional quotient $\mathbb{K}^8/V$. This quotient can be identified with the subspace $V' \subset \mathbb{K}^8$ given by

$$V' = \left\{ (\alpha, \beta, 0, 0, \gamma, 0, 0, 0)^{\mathbf{T}} \mid \alpha, \beta, \gamma \in \mathbb{K} \right\},$$

since V and V' are complementary subspaces. Our first goal is then to reduce the columns of $\mathcal{T}$ modulo V, so as to obtain elements $\overline{C_1}, \dots, \overline{C_5} \in V'$ with

$$C_i \equiv \overline{C_i} \bmod V, \qquad \overline{C_i} = \begin{pmatrix} \alpha_i \\ \beta_i \\ 0 \\ 0 \\ \gamma_i \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad i = 1, \dots, 5.$$

After that, we will need to determine the kernel of the 3×5 matrix

$$M'' = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 \\ \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_5 \end{pmatrix}$$

to obtain F'' and G''.

Lemma 9.1. *Given the matrix N', the columns of $\mathcal{T}$ can be reduced modulo V to produce the columns of the matrix M'', at a total cost of* $19M$.

Proof. As a preliminary calculation, we find elements D_8, D_{10}, and D_{11} of V, corresponding respectively to $ys - s_1xs = (y - s_1x)s$, $x(y - s_1x)s$, and $y(y - s_1x)s$. This will aid us in reducing columns of $\mathcal{T}$ modulo V. We have:

$$D_8 = C_8 - s_1C_7 = \begin{pmatrix} s_3 - s_1(s_2 + p_2) \\ s_2 - s_1^2 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

$$D_{10} = C_{10} - s_1C_9 = \begin{pmatrix} s_5 + q_2 - s_1(s_4 + p_1 + s_3p_2) \\ s_4 + p_1 \\ -s_1s_3 \\ s_3 - s_1(s_2 + p_2) \\ s_2 + p_2 - s_1^2 \\ 0 \\ 1 \\ 0 \end{pmatrix},$$

$$D_{11} = C_{11} - s_1C_{10} = \begin{pmatrix} -s_1(s_5 + q_2) \\ s_5 - s_1(s_4 + p_1) \\ s_4 \\ -s_1s_3 \\ s_3 - s_1(s_2 + p_2) \\ s_2 - s_1^2 \\ 0 \\ 1 \end{pmatrix}.$$

Calculating D_8, D_{10} and D_{11} costs $6M$, as we already know s_3p_2 from N', so it suffices to calculate

$$s_1(s_2 + p_2), \quad s_1^2, \quad s_1(s_4 + p_1 + s_3p_2), \quad -s_1s_3, \quad -s_1(s_5 + q_2), \quad -s_1(s_4 + p_1).$$

It is clear that V is spanned by $\{C_7, D_8, C_9, D_{10}, D_{11}\}$. We now compute the reduction of columns of $\mathcal{T}$ modulo V.

First, note that

$$\overline{C_1} = C_1 \in V'$$

which comes at no cost, so we obtain

$$\begin{pmatrix} \alpha_1 \\ \beta_1 \\ \gamma_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Second,

$$\overline{C_2} = C_2 - D_8 \in V'$$

which also comes at no cost, so that

$$\begin{pmatrix} \alpha_2 \\ \beta_2 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} t_2 - s_3 + s_1(s_2 + p_2) \\ t_1 - s_2 + s_1^2 \\ 0 \end{pmatrix}.$$

Third, we have

$$\overline{C_3} = C_3 - t_1 C_7 \in V',$$

costing $2M$ to calculate $t_1 C_7$, and hence

$$\begin{pmatrix} \alpha_3 \\ \beta_3 \\ \gamma_3 \end{pmatrix} = \begin{pmatrix} t_3 - t_1(s_2 + p_2) \\ t_2 - t_1 s_1 \\ 1 \end{pmatrix}.$$

Fourth and fifth, note that

$$C_4 - D_{10} = \begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad \text{with } m_i \in \mathbb{K},\ i = 1, \ldots, 5,$$

$$C_5 - D_{11} = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ 0 \\ 0 \end{pmatrix}, \qquad \text{with } z_i \in \mathbb{K},\ i = 1, \ldots, 6,$$

so that

$$C_5 - D_{11} - z_6 C_9 = \begin{pmatrix} \ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \\ \ell_5 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad \text{with } \ell_i \in \mathbb{K},\ i = 1, \ldots, 6.$$

Hence our desired reductions are

$$\begin{aligned} \overline{C_4} &= C_4 - D_{10} - m_4 D_8 - m_3 C_7, \\ \overline{C_5} &= C_5 - D_{11} - z_6 C_9 - \ell_4 D_8 - \ell_3 C_7, \end{aligned}$$

which ensures that $\overline{C_4}$ and $\overline{C_5}$ belong to V'. We require $4M$ to find $z_6 C_9$, which allows us to calculate the vectors $C_4 - D_{10}$ and $C_5 - D_{11} - z_6 C_9$. The expressions

$m_4D_8+m_3C_7$ and $\ell_4D_8+\ell_3C_7$ can now be obtained simultaneously as the matrix product

$$\left(\begin{array}{c|c} C_7 & D_8 \end{array}\right)\begin{pmatrix} m_3 & \ell_3 \\ m_4 & \ell_4 \end{pmatrix}.$$

The entries of C_7 and D_8 are mostly zeros and ones, and the only part of the above matrix product that involves nontrivial multiplications in $\mathbb{K}$ is the top 2×2 submatrix multiplication

$$\begin{pmatrix} s_2+p_2 & s_3-s_1(s_2+p_2) \\ s_1 & s_2-s_1^2 \end{pmatrix}\begin{pmatrix} m_3 & \ell_3 \\ m_4 & \ell_4 \end{pmatrix}. \tag{18}$$

This costs $7M$ using Strassen's technique. At this point we need no further multiplications to produce $\overline{C_4}$ and $\overline{C_5}$.

Adding up the costs to produce all of $\overline{C_1},\dots,\overline{C_5}$ concludes the proof. □

Lemma 9.2. *Given s and t, the columns of $\mathcal{T}$ can be obtained and reduced modulo V, thereby obtaining the matrix M'', at a total cost of $20M$. (In other words, we can save one multiplication compared to using Lemmas 8.1 and 9.1.)*

Proof. We claim that the two multiplications t_3p_2 from Lemma 8.1 and $s_1(s_4+p_1+s_3p_2)$ from Lemma 9.1 can be replaced with a single multiplication. To see this, observe that these two multiplications are used only when we calculate the first coefficient m_1 in the column vector $C_4-D_{10}=(m_1,m_2,m_3,m_4,m_5,0,0,0)^{\mathbf{T}}$. Now rearrange

$$\begin{aligned} m_1 &= t_4+q_2+t_3p_2-s_5-q_2+s_1(s_4+p_1+s_3p_2) \\ &= t_4-s_5+s_1(s_4+p_1)+(t_3+s_1s_3)p_2. \end{aligned}$$

Since we have already computed $s_1(s_4+p_1)$ and s_1s_3 during Lemma 9.1, we see that we can replace the two multiplications t_3p_2 and $s_1(s_4+p_1+s_3p_2)$ by the single multiplication $(t_3+s_1s_3)p_2$. This concludes our proof. □

The following proposition now allows us to find the desired polynomials

$$\begin{aligned} F'' &= x^2+a''y+b''x+c'', \\ G'' &= xy+d''y+e''x+f''. \end{aligned}$$

Proposition 9.3. *Given s and t, the polynomials F'' and G'', as well as the inverse $(a'')^{-1}$, can be obtained using $31M, 1I$.*

Proof. Recall that the columns of M'' represent the reductions of each of t, xt, yt, x^2t and xyt modulo the multiples of s via the 'reduction modulo V' described above. Hence, by Lemma 9.2, the matrix M'' can be obtained using $20M$, and has the form

$$M''=\begin{pmatrix} 1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ 0 & \beta_2 & \beta_3 & \beta_4 & \beta_5 \\ 0 & 0 & 1 & \gamma_4 & \gamma_5 \end{pmatrix}.$$

In anticipation of our next step, we compute γ_4^{-1} and β_2^{-1} using $3M, 1I$ (that is, we find $\beta_2\cdot\gamma_4$, invert it, and multiply the inverse separately with each of β_2 and γ_4). We can now find two vectors

$$\begin{cases} v_1'' = (c'', b'', a'', 1, 0)^{\mathbf{T}}, \\ v_2'' = (f'', e'', d'', 0, 1)^{\mathbf{T}}, \end{cases}$$

that span the kernel of M'' using back substitution, requiring a further $8M$. Those give us the coefficients of the polynomials F'' and G''. Note that $a'' = -\gamma_4$, and so we know its inverse thanks to our previous anticipatory step. □

10. *Negating the final result, and an application to Section 5*

As mentioned in Subsection 2.3, our final result representing $\xi''' = -\xi'' = \xi + \xi'$ will be a pair $\{F''', G'''\}$, with $F''' = F''$ and $G''' = xy + d'''y + e'''x + f''' \in W^7_{D'''}$ that satisfies $G''G''' + F''H = 0$ for some $H \in W^8$. We can then in principle find G''' by a procedure analogous to that in Sections 8 and 9, by working modulo W^6, which is analogous to how we previously dropped some rows from the matrix N to get N'. If we furthermore need to find H, as is the case in Proposition 5.4, we can do something similar by dropping one fewer row at the start, thereby working modulo W^4. (We invite the reader to check that this extra 'precision' is required exactly to obtain the constant term of H.)

We, however, preferred to find the following solution by a direct calculation:

$$\begin{aligned} G''' &= xy + (b'' - d'')y - (\ell(a'')^{-1} + m)x \\ &\qquad + [md'' + (\ell(a'')^{-1} + e'')(d'' - b'') + a''(a''b'' - p_1) - f''], \\ H &= -y^2 + a''x^2 + \ell(a'')^{-1}y - a''b''x \\ &\qquad + [(\ell(a'')^{-1} + m)e'' + a''(b''^2 - c'' - q_2)], \end{aligned} \tag{19}$$

where

$$\begin{aligned} m &= e'' + a''(a'' + p_2), \\ \ell &= c'' + (d'' - b'')d''. \end{aligned}$$

This can be verified without setting up a system of linear equations; instead, note that our expressions for G''', H satisfy $G''G''' + F''H \in \mathbb{K} \cdot x + \mathbb{K} \cdot y + \mathbb{K} \cdot 1 = W^4$ (taking into account equation (1) of our curve). However, any combination of F'' and G'' vanishes at D'', so $G''G''' + F''H \in W^4_{D''} = 0$, since D'' is typical.

Thus our result is as follows.

Proposition 10.1. *Given F'', G'' and $(a'')^{-1}$, let F''', G''' represent the negative in the Jacobian; then $F''' = F''$, and we obtain $(a'')^{-1} = (a''')^{-1}$ for free.*

(i) *It costs $7M$ to compute G''' as given by the above formulae.*

(ii) *It costs $10M$ to compute both G''' and H, satisfying $G''G''' + F''H = 0$.*

Proof. First compute m and ℓ, then compute $\ell(a'')^{-1}$ and $a''b''$, and then compute the remaining coefficients of G''' (and of H, if needed) using the above expressions. □

11. *Conclusion*

We now assemble all the parts to obtain the main result of our paper.

Theorem 11.1. *In the Jacobian of a $C_{3,4}$ curve defined over a large finite field $\mathbb{K}$, point addition can be performed on typical elements using* 117 *field multiplications and* 2 *field inversions. Point doubling can be performed on typical elements using* 129 *field multiplications and* 2 *field inversions.*

Proof. For point addition, add up the costs of Propositions 4.1, 6.1, 7.1, 9.3, and 10.1(i). For point doubling, add up the costs of Propositions 5.4, 6.1, 7.1, 9.3, and 10.1(i). □

In terms of the number of multiplications required, our results represent improvements of 19.3% for addition and 22.8% for doubling (compared to [**7**]), and of 22% for addition and 25.8% for doubling (compared to [**2**]). All the algorithms require two inversions in $\mathbb{K}$ per group operation in the Jacobian.

Appendix A. *Implementation*

We have included a complete implementation in Magma of our algorithms as an appendix to this article. The files can be found at:

http://www.lms.ac.uk/jcm/10/lms2006-049/appendix-a/.

The list of files is as follows.

- The file `curve.magma` contains the code for our algorithms, as well as a sample set of values over the finite field $\mathbb{K}$ whose cardinality $|\mathbb{K}|$ is the first prime above 10^8. Larger values of $|\mathbb{K}|$ pose no problem, but then elements of $\mathbb{K}$ will appear less legible in a printout. The sample set of values includes two data structures `FG` and `FG2` representing the divisors D and D' of our algorithms.
- The file `sample_run_output.txt` contains a sample run of our addition and doubling algorithms on the divisors D and D' defined in `curve.magma`. We verify that the results are correct using the built-in operations in Magma for ideals in polynomial algebras.
- The file `sample_run_input.magma` is the input that was used to produce the output above.

Acknowledgement. The second author would like to thank K. and C. Adal for providing computer access and an agreeable work environment during the summer of 2006, when the author's usual office was inaccessible.

References

1. Roberto Avanzi, Gerhard Frey, Tanja Lange and Roger Oyono, 'On using expansions to the base of -2', *Int. J. Comput. Math.* 81 (2004) 403–406. 308, 311

2. Abdolali Basiri, Andreas Enge, Jean-Charles Faugère and Nicolas Gürel, 'Implementing the arithmetic of $C_{3,4}$ curves', *Algorithmic number theory—ANTS VI*, Lecture Notes in Comput. Sci. 3076 (Springer, Berlin, 2004) 87–101. 308, 309, 310, 327

3. Abdolali Basiri, Andreas Enge, Jean-Charles Faugère and Nicolas Gürel, 'The arithmetic of Jacobian groups of superelliptic cubics', *Math. Comp.* 74 (2005) 389–410 (electronic). 308, 310

4. Claus Diem, 'An index calculus algorithm for plane curves of small degree', *Algorithmic number theory—ANTS VII*, Lecture Notes in Comput. Sci. 4076 (Springer, Berlin, 2006) 543–557. 308

5. Claus Diem and Emmanuel Thomé, 'Index calculus in class groups of non-hyperelliptic curves of genus three', preprint, 2006, http://www.math.uni-leipzig.de/~diem/preprints/non-he-genus3.ps ; *J. Cryptology*, to appear. 308

6. Stéphane Flon and Roger Oyono, 'Fast arithmetic on Jacobians of Picard curves', *Public key cryptography—PKC 2004*, Lecture Notes in Comput. Sci. 2947 (Springer, Berlin, 2004) 55–68. 308

7. Stéphane Flon, Roger Oyono and Christophe Ritzenthaler, 'Fast addition on non-hyperelliptic genus 3 curves', preprint, 2004, http://www.math.uwaterloo.ca/~royono/Quartic.html , http://www.exp-math.uni-essen.de/~oyono/Quartic.html . 308, 309, 317, 327

8. Florian Hess, 'Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern', PhD thesis, Technische Universität Berlin, 1999, http://www.math.tu-berlin.de/~kant/publications/diss/hess.pdf . 308

9. Kamal Khuri-Makdisi, 'Linear algebra algorithms for divisors on an algebraic curve', *Math. Comp.* 73 (2004) 333–357 (electronic), http://arxiv.org/abs/math.NT/0105182 . 307, 308, 309, 311, 312

10. Kamal Khuri-Makdisi, 'Asymptotically fast group operations on Jacobians of general curves', preprint (2004), *Math. Comp.*, to appear, http://arxiv.org/abs/math.NT/0409209 . 307, 308, 309, 310, 311, 312

Fatima K. Abu Salem fa21@aub.edu.lb
http://www.cs.aub.edu.lb/fa21/

Computer Science Department
American University of Beirut
P. O. Box 11-0236
Beirut
Lebanon

Kamal Khuri-Makdisi kmakdisi@aub.edu.lb
http://people.aub.edu.lb/~kmakdisi/

Mathematics Department and
Center for Advanced Mathematical Sciences
American University of Beirut
P. O. Box 11-0236
Beirut
Lebanon