The arithmetic of Jacobian groups of superelliptic cubics

Abdolali Basiri, Andreas Enge, Jean-Charles Faugère, Nicolas Gürel

MATHEMATICS OF COMPUTATION
Volume 74, Number 249, Pages 389–410
S 0025-5718(04)01699-0
Article electronically published on July 20, 2004

THE ARITHMETIC OF JACOBIAN GROUPS OF SUPERELLIPTIC CUBICS

ABDOLALI BASIRI, ANDREAS ENGE, JEAN-CHARLES FAUGÈRE, AND NICOLAS GÜREL

Abstract. We present two algorithms for the arithmetic of cubic curves with a totally ramified prime at infinity. The first algorithm, inspired by Cantor's reduction for hyperelliptic curves, is easily implemented with a few lines of code, making use of a polynomial arithmetic package. We prove explicit reducedness criteria for superelliptic curves of genus 3 and 4, which show the correctness of the algorithm. The second approach, quite general in nature and applicable to further classes of curves, uses the FGLM algorithm for switching between Gröbner bases for different orderings. Carrying out the computations symbolically, we obtain explicit reduction formulae in terms of the input data.

1. Introduction

The success of elliptic curves in public key cryptography has created new interest in the arithmetic of other curves. Indeed, being able to properly represent elements of the associated group, the Jacobian, and to effectively realise the group law is the first prerequisite for implementing a cryptosystem based on a curve. The two simplest classes of curves, elliptic and hyperelliptic curves, which are quadratic covers of the projective line, are well studied. So the focus has shifted towards the next complex types of curves, cyclic Galois covers of the projective line, namely superelliptic curves, and more general curves, the C_{ab} curves [19]. All these curves have a unique, rational point at infinity, so that the rational part of their Jacobian group is isomorphic to the ideal class group of the coordinate ring of the curve.

In a cryptographic context, one is interested in curves defined over a finite field $\mathbb{F}_q$. Curve based cryptosystems may only be secure if their associated discrete logarithm problem is intractable. This requires the Jacobian order $N \approx q^g$ (where g denotes the genus of the curve) to be sufficiently large to be resistant against attacks with complexity $O(\sqrt{N})$. Using curves of genus greater than 1 allows us to decrease the size of the ground field for the same order of magnitude. Another necessary condition is that N be explicitly known and that it have a large prime factor. Recent progress on point counting methods allows us to obtain cryptographically suitable superelliptic curves over finite fields of small characteristic [14].

In the light of subexponential attacks on the discrete logarithm problem in hyperelliptic curves of large genus [1, 20, 9, 10, 8] and their analysis for small genus

Received by the editor July 18, 2002 and, in revised form, January 17, 2003.
2000 *Mathematics Subject Classification.* Primary 11G20, 14Q05, 14H40, 14H45, 68W30; Secondary 11T71, 13P10.
Key words and phrases. Superelliptic curve, C_{ab} curve, Jacobian, arithmetic, Gröbner basis.

in [13], it seems advisable to restrict the genus to at most 4 also in the case of other curves. Since even genus 4 curves are probably less secure than elliptic curves for the same group order, curves of genus 3 are the most attractive ones from a cryptographic point of view. With superelliptic and C_{ab} curves, a genus of 3 or 4 can only be realised if the curve is a cubic cover of the projective line.

Jacobians can be seen as divisor class groups, which by their very nature do not admit a unique representation for their elements. In the case of Jacobians of superelliptic or C_{ab} curves, however, a divisor class is canonically given by the divisor of smallest degree it contains, the so-called *reduced* representative (this is explained in more detail in Section 2). The core of their arithmetic therefore consists of the *reduction* process, transforming any group element into its equivalent reduced representative. The associated decision problem is, given an element of the Jacobian, to decide whether it is already reduced. A necessary but in general not sufficient condition for an ideal to be reduced is that its degree does not exceed the genus of the curve. In Section 3, we use the geometry of superelliptic curves to characterise reduced elements in genus 3 or 4. In particular, we show that for the type of ideals encountered most of the time, the constraint that their degrees do not exceed the genus is already a sufficient criterion for reducedness. We also prove that, unfortunately, this is no more the case for superelliptic curves of higher genus.

There are several general purpose algorithms for Jacobian arithmetic via effective versions of the Riemann–Roch theorem [17, 23, 16]. For superelliptic and C_{ab} curves, specific, more efficient algorithms are described in [2, 3, 12, 15, 5]. The closely related arithmetic of cubic curves with several points at infinity is treated in [22]. The algorithms use the representation of Jacobian elements by polynomials and rely on rather heavy techniques of symbolic computation like LLL, Hermite normal form and Gröbner basis computation. On a high level, these algorithms admit a unifying description; see Algorithm 5.1. In Section 5 of this article, we present two new reduction algorithms for cubic superelliptic and C_{ab} curves, which fit into this common framework. For the sake of conciseness, we limit the presentation to superelliptic cubics, indicating the necessary modifications for C_{ab} curves in Section 6.

Before developing the new algorithms, we exhibit a special class of ideals allowing a simplified polynomial representation, which is in fact not so special at all: assuming a uniform probability distribution over the elements of the Jacobian and that g is fixed and $q \to \infty$, then these "special" ideals occur with a probability of $1 - \frac{1}{q}O(1)$. Hence, we call these elements "typical".

Our first algorithm is inspired by the similarity between the representation of typical superelliptic and of hyperelliptic ideals. It generalises Cantor's reduction algorithm for hyperelliptic curves as described in [6] and, for characteristic 2, in [7]. The algorithm uses only basic polynomial arithmetic, on top of which it is easily implemented in a few lines of code. For general superelliptic cubics, it returns an ideal of degree at most g. In genus 3 and 4, this means that the output is indeed reduced according to our results of Section 3.

Our second approach is based on the FGLM algorithm of [11] for switching between Gröbner bases for different orderings. In our context, FGLM provides the link between the lexicographic and the C_{ab} order (cf. Definition 2.1). The technique we propose is in fact quite general and applies to arbitrary, also noncubic C_{ab}

curves. Carrying out all computations symbolically, one obtains explicit formulae for the reduced ideal in terms of the input ideal, operating on the polynomial representation. We derive such formulae for typical ideals of superelliptic curves of genus 3. Evidently, these formulae can be made completely explicit to obtain the coefficients of the output polynomials via straight line programs from the coefficients of the input polynomials, very much as in the case of elliptic curves. This also yields the precise number of operations in the base field. However, the results depend heavily on the exact layout of the computations. We briefly report on this approach in Section 6, leaving the details to [4].

2. Jacobians of superelliptic cubics

2.1. **Definitions and elementary properties.** Let K be a perfect field of characteristic different from 3 and $\overline{K}$ its algebraic closure. A *superelliptic cubic*, as introduced in [12], is an affine plane curve of the form

$$C = Y^3 - f$$

with $f \in K[X]$ of degree not divisible by 3 and at least 4 and without multiple roots in $\overline{K}$. The condition that the degree of f be not divisible by 3 implies that the curve is absolutely irreducible, the lack of multiple roots is equivalent with the nonsingularity of C. Notice that if the degree of f is larger than 4, then the projective closure of C has a singularity at infinity. However, it corresponds to a unique point ∞ on the nonsingular projective model of C.

Superelliptic curves are special cases of C_{ab} curves; cf. [19]. For coprime positive integers a and b, coprime to the characteristic of the ground field, a C_{ab} curve is defined by a nonsingular affine equation of the form

$$C = Y^a + \sum_{ia+jb<ab} c_{ij} X^i Y^j - X^b.$$

The *coordinate ring* of C is defined by $K[C] = K[X,Y]/(C)$, its *function field* $K(C)$ by the field of fractions of $K[C]$. Since C is nonsingular, $K[C]$ is the integral closure of $K[X]$ in $K(C)$.

We may define the same objects over the algebraic closure $\overline{K}$ of K. Then for a superelliptic cubic C, the field extension $\overline{K}(C)/\overline{K}(X)$ is Galois and its Galois group is generated by $\sigma : Y \mapsto \zeta^{-1}Y$ for a fixed primitive third root of unity ζ. In geometric terms, C is a cyclic cover of degree 3 of the projective line. By Hurwitz's formula, its genus is given by $g = \deg f - 1$.

The arithmetic object associated to the curve C is the K-rational part of its Jacobian or, equivalently, its divisor class group. A rational *prime divisor* of C is given by an orbit of points on C with coordinates in $\overline{K}$ under the action of $\mathrm{Gal}(\overline{K}/K)$ or, equivalently, by a discrete valuation of $K(C)$, and its degree is the number of points in the orbit. The group of K-rational divisors is the free abelian group over the prime divisors, with the degree function extended naturally, and of special interest is its degree zero part $\mathrm{Div}^0_K(C)$. Associating to a function in $K(C)$ its divisor of zeroes and poles with the appropriate multiplicities and noticing that it consists of orbits under $\mathrm{Gal}(\overline{K}/K)$, one defines the subgroup of principal divisors $\mathrm{Prin}_K(C)$ and finally the K-rational part of the Jacobian as $J_K(C) = \mathrm{Div}^0_K(C)/\mathrm{Prin}_K(C)$.

A C_{ab} curve has a unique infinite prime divisor ∞, which is furthermore rational of degree 1. This leads to the following definition.

Definition 2.1. Let C be a C_{ab} curve. The C_{ab} order of an element of $K(C)$ is given by the negative of its order at infinity. In particular, the C_{ab} order of X is a, that of Y is b, and that of an arbitrary polynomial can be obtained from these two values via the ultrametric triangle inequality.

The multiplicity of ∞ in a divisor is completely determined by the finite part of the divisor, and there is a bijective map between $\mathrm{Div}_K^0(C)$ and the divisors formed of only finite prime divisors, given by

$$\sum_{P\neq\infty} m_P P - \left(\sum_{P\neq\infty} m_P\right)\infty \leftrightarrow \sum_{P\neq\infty} m_P P.$$

To simplify the notation in the following, we always omit the multiplicity of ∞. For instance, the following definition is readily formulated in terms of divisors omitting the infinite prime divisor, since the notions of positivity and degree given therein refer only to the finite part.

Definition 2.2. Let $D = \sum_{P\neq\infty} m_P P$ and $E = \sum_{P\neq\infty} n_P P$ be divisors. The coefficient $m_P = \mathrm{ord}_P D$ is called the *order* of D at P. The *greatest common divisor* of D and E is defined by

$$\gcd\left(\sum_{P\neq\infty} m_P P, \sum_{P\neq\infty} n_P P\right) = \sum_{P\neq\infty} \min(m_P, n_P) P.$$

We write $D \geq E$ if $m_P \geq n_P$ for all P and we say that D is *positive* or *effective* if $D \geq 0$, i.e., all $m_P \geq 0$. If α, $\alpha_1, \ldots, \alpha_n$ are functions in $K(C)$, we denote by $\mathrm{div}\,\alpha$ the principal divisor generated by α and we let $\deg\alpha = \deg(\mathrm{div}\,\alpha)$ and $\mathrm{ord}_P\,\alpha = \mathrm{ord}_P(\mathrm{div}\,\alpha)$. Finally, $\mathrm{div}(\alpha_1, \ldots, \alpha_n) = \gcd(\mathrm{div}\,\alpha_1, \ldots, \mathrm{div}\,\alpha_n)$.

By definition, the degree of a polynomial $\alpha \in K[C]$ is nothing but its C_{ab} order. Noticing that the C_{ab} order of X is a and that the number of conjugates of α over $K(X)$ is also a, it is easy to show that

$$\deg\alpha = \deg_X \mathrm{N}_{K(C)/K(X)}(\alpha).$$

Omitting ∞ in the notation of degree zero divisors, we have gone the first step towards the equivalent representation of the K-rational part of the Jacobian of C as the ideal class group of $K[C]$. Being the integral closure of $K[X]$ in $K(C)$, the coordinate ring $K[C]$ is the intersection of all valuation rings of $K(C)$ not extending the infinite valuation of $K(X)$. Hence, there is a one-to-one correspondence between finite prime divisors P of C and prime ideals $\mathfrak{p}$ of $K[C]$, which extends to degree zero divisors and the group of fractional ideals of $K[C]$ by homomorphism:

$$\begin{aligned} \sum m_P P &\leftrightarrow \prod \mathfrak{p}^{m_P}, \\ \mathrm{div}(\alpha_1, \ldots, \alpha_n) &\leftrightarrow \langle \alpha_1, \ldots, \alpha_n \rangle . \end{aligned}$$

Since principal divisors correspond to principal ideals, this homomorphism yields in fact an isomorphism between the Jacobian $J_K(C)$ and the ideal class group $\mathfrak{H}_K(C)$ of $K[C]$.

In the following, we switch freely between the divisor and the ideal representation. When providing criteria for reducedness in Section 3, which is essentially a geometric notion, it is more convenient to speak of divisors; the algorithms realising

the arithmetic given in Sections 4 and 5 are more readily formulated in terms of ideals.

Given a nonsingular affine curve with a unique point at infinity, which is moreover rational, it is shown in [12], Theorem 1, that each divisor class contains a unique positive divisor of minimal degree, which is at most g. The proof is based on the Riemann–Roch theorem. This minimal divisor and its corresponding ideal are called *reduced*, and the arithmetic in superelliptic Jacobians is realised by manipulating these reduced objects. Hence, in the remainder of this article, all divisors will be positive (i.e., all ideals will be integral), unless stated otherwise.

As mentioned in the introduction, we are mainly interested in curves of small genus, especially of genus 3 or 4. Thus, when giving asymptotic estimates in the following sections, it is understood that g is fixed and $q \to \infty$.

2.2. **Typical divisors.** It is a well-known fact from the theory of Dedekind rings that any integral ideal of $K[C]$ is generated by a polynomial in $K[X]$ and a second polynomial in $K[C]$. Thus, any reduced K-rational divisor D can be written as

$$D = \operatorname{div}(u, rY^2 + sY + t)$$

with u, r, s, $t \in K[X]$, $\deg r$, $\deg s$, $\deg t < \deg u \leq g$, $\gcd(u, r, s, t) = 1$.

The divisor D can also be written as the $K[X]$-module

$$D = [u_0, u_1 Y - v_1, Y^2 + v_2 Y + w_2].$$

This is exactly the Gröbner basis of the ideal for the lexicographic order or, equivalently, its Hermite normal form (HNF).

Recall that the isomorphisms of $K(C)/K(X)$ are given by $\{\mathrm{id}, \sigma, \sigma^2\}$ with $\sigma : Y \mapsto \zeta^{-1} Y$, which are extended to points and divisors via $(x, y)^\sigma = (x, \zeta y)$ so that $\operatorname{div}(f^\sigma) = (\operatorname{div} f)^\sigma$. The divisors D^σ and D^{σ^2} are called the *conjugates* of D. If D is a prime divisor such that $D = D^\sigma$, then D is called *ramified*. In particular, the ramified points are those with zero Y-coordinate.

The sum $D + D^\sigma + D^{\sigma^2}$ is the divisor of a polynomial in $K[X]$ (namely the norm of the corresponding ideal), so that $D^\sigma + D^{\sigma^2}$, which is a divisor in the opposite class of D, is K-rational even when K does not contain a primitive third root of unity and D^σ and D^{σ^2} are not rational themselves.

On hyperelliptic curves, which are degree 2 covers of the projective line, any reduced divisor can be written as $\operatorname{div}(u, Y - v)$. On superelliptic curves, such a simple form cannot always be obtained. For instance, if $P = (x, y)$, then

$$\operatorname{div}(X - x) = P + P^\sigma + P^{\sigma^2},$$

and the prime divisor P of degree 1 is represented by $\operatorname{div}(X - x, Y - y)$, while

$$P^\sigma + P^{\sigma^2} = \operatorname{div}\big(X - x, (Y - \zeta y)(Y - \zeta^2 y)\big) = \operatorname{div}(X - x, Y^2 + yY + y^2)$$

does not equal any $\operatorname{div}(u, Y - v)$. However, the simpler representation is still the typical case, as will be shown in Theorem 2.5, hence the following definition.

Definition 2.3. We call a divisor *typical* if it is of the form

$$\operatorname{div}(u, Y - v) \text{ with } u, v \in K[X], \deg v < \deg u \leq g \text{ and } u | v^3 - f.$$

Theorem 2.4. *Let D be a K-rational reduced divisor which does not contain a pair of conjugate prime divisors. In particular, it does not contain a ramified prime divisor with multiplicity greater than* 1. *Then D is typical.*

Proof. Let $D = \sum m_P P$ with distinct $P = (x_P, y_P) \in \overline{K} \times \overline{K}$ be as in the theorem. Then the x_P are all distinct, and u can be chosen as $\prod (X - x_P)^{m_P}$ of degree at most g and v of degree at most $\deg u - 1$ such that it interpolates the points P with the appropriate multiplicities m_P, which is equivalent to $u | v^3 - f$. The rationality of u and v follows easily from that of D. □

For the remainder of this section, we assume that $K = \mathbb{F}_q$ is a finite field and we examine more closely typical divisors. We show that all but a negligible proportion of the reduced divisors are of this form.

Theorem 2.5. *If $K = \mathbb{F}_q$ is finite and g is fixed, then the ratio of reduced typical divisors in the rational part $J_K(C)$ of the Jacobian is in $1 - \frac{1}{q} O(1)$. More precisely, this assertion even holds for reduced typical divisors with $\deg u = g$ and $\deg v = g-1$ that do not contain a ramified prime divisor.*

Assume a uniform probability distribution on reduced divisors. Consider the addition of divisors without reducing them, i.e., carrying out only the composition step of Section 4. Then with probability in $1 - \frac{1}{q} O(1)$, doubling a random reduced divisor or adding two independently chosen random reduced divisors yields a divisor of the form $\operatorname{div}(u, Y - v)$ with $\deg u = 2g$, $\deg v = 2g - 1$ and $u | v^3 - f$.

Proof. By Weil's theorem [24], the Jacobian $J_K(C)$ contains $q^g \left(1 \pm \frac{1}{\sqrt{q}} O(1)\right)$ elements. (This somewhat sloppy notation stands for $\left| |J_K(C)| - q^g \right| \in \frac{q^g}{\sqrt{q}} O(1)$.) Moreover, the number of points on C defined over $\mathbb{F}_{q^k}$ for some natural number k is in $q^k \left(1 \pm \frac{1}{q^{k/2}} O(1)\right) \subseteq q^k \left(1 \pm \frac{1}{\sqrt{q}} O(1)\right)$. Using Möbius inversion, one readily deduces that the number of prime divisors of degree k is in $\frac{1}{k} q^k \left(1 \pm \frac{1}{\sqrt{q}} O(1)\right) \subseteq O\left(q^k\right)$; that is, prime divisors of degree k behave basically like irreducible polynomials of degree k. As for polynomials, it thus follows that the number of divisors of degree at most k is in $q^k \left(1 \pm \frac{1}{\sqrt{q}} O(1)\right) \subseteq O\left(q^k\right)$.

As an upper bound on the number of Jacobian elements that do not have the required form, we now count the divisors of degree at most g that are not typical or are typical with polynomials u or v of too low degree or contain a ramified prime divisor. By the results of the previous paragraph, the number of divisors of degree at most g containing a pair of conjugate primes (or twice the same ramified prime) of degree i is in $O\left(q^i q^{g-2i}\right) \subseteq O\left(q^{g-1}\right)$. Summing up over the $O(1)$ possible values for i, we obtain by Theorem 2.4 that the number of nontypical divisors of degree at most g is in $O\left(q^{g-1}\right)$. The same kind of argumentation shows that the number of divisors of degree less than g or containing a ramified prime is in $O\left(q^{g-1}\right)$. Consider now typical divisors with $\deg u = g$ and $\deg v \leq g-2$. For any given such v, there is a constant number of possible u, so that the total number of such divisors is again in $O\left(q^{g-1}\right)$.

From the bound on the cardinality of the Jacobian we now deduce the desired ratio on well-behaved reduced divisors.

The result on the sum of two divisors is obtained in a similar fashion, making use moreover of a trivial generalisation of Theorem 2.4 to higher degree divisors. □

It is our aim in the present article to examine the arithmetic of typical divisors, sometimes imposing additional restrictions on their degrees, and to propose efficient algorithms for them. Whenever a divisor of a different form is encountered, which

in the light of Theorem 2.5 happens with a negligible probability, one may have recourse at a (presumably slower) generic addition method as described in [2, 3, 12, 15].

3. The geometry of reduced divisors

As for hyperelliptic curves, the addition in superelliptic Jacobians proceeds in two steps. In a first step, the two reduced divisors are simply added and yield a divisor of degree up to $2g$. In the second step, this divisor is reduced to the representative of minimal degree in its class.

Our new reduction algorithm of Section 5.1 outputs with high probability a typical divisor. Unlike for the result of the generic reduction of [12, 2, 3], however, there is a priori no guarantee that this divisor of degree at most g will be reduced. In this section, we thus examine the conditions under which a low degree divisor is reduced. To ease the presentation, we will henceforth consider all K-rational divisors as being decomposed over $\overline{K}$, so that instead of prime divisors we may speak of points. (The rationality of a divisor then means that it consists of complete orbits of points under $\mathrm{Gal}(\overline{K}/K)$, and the notion of reducedness does not depend on the field, K or $\overline{K}$, over which the divisor is interpreted.)

In hyperelliptic Jacobians, all typical divisors are reduced. Unfortunately, this is no more the case for superelliptic cubics, but at least in genus 3 and 4 the nonreduced typical divisors can be recognised quite easily via the following main theorem of this section.

Theorem 3.1. *A positive divisor of degree at most* 3 *on a superelliptic cubic of genus* 3 *is not reduced if and only if it consists of three collinear points. A positive divisor of degree at most* 4 *on a superelliptic cubic of genus* 4 *is not reduced if and only if it satisfies one of the following conditions:*

- *it contains a triplet of conjugate points;*
- *it consists of two pairs of conjugate points;*
- *it consists of four collinear points;*
- *it consists of four points T, U, V, W lying simultaneously on a parabola $Y-v$ with $v \in K[X]$ of degree* 2 *and an elliptic curve Y^2+sY+t with s, $t \in K[X]$, $\deg s \leq 1$ and $\deg t = 3$. Furthermore, the elliptic curve intersects the superelliptic curve exactly in these four points, three collinear points P_1^σ, P_2^σ and P_3^σ and their conjugates $P_1^{\sigma^2}$, $P_2^{\sigma^2}$ and $P_3^{\sigma^2}$. (Hereby, points designated by different letters may coincide, in which case the assertions remain correct even with the appropriate multiplicities.)*

Proof. We first show the necessity of the given conditions. Let thus $D \neq 0$ be a nonreduced positive divisor of degree at most g, and let D' with $\deg D' < \deg D$ be its reduced representative. Write

$$D' = \sum m_i P_i + \sum n_j (Q_j^\sigma + Q_j^{\sigma^2}),$$

$\mu = \sum m_i$, $\nu = \sum n_j$, $\deg D' = \mu + 2\nu$, where the P_i and Q_j all have different X-coordinates. Let $\beta \in K(X)$ be monic such that

$$\operatorname{div}\beta = \sum m_i (P_i + P_i^\sigma + P_i^{\sigma^2}) + \sum n_j (Q_j + Q_j^\sigma + Q_j^{\sigma^2}).$$

Since $\operatorname{div}\beta$ is positive, we even have $\beta \in K[X]$. Then

$$D - D' + \operatorname{div}\beta = D + \sum m_i (P_i^\sigma + P_i^{\sigma^2}) + \sum n_j Q_j$$

is principal and positive, whence

$$D + \sum m_i (P_i^\sigma + P_i^{\sigma^2}) + \sum n_j Q_j = \operatorname{div} \alpha$$

for some monic polynomial α. Write

$$\alpha = rY^2 + sY + t$$

with r, s, $t \in K[X]$, so that

$$\mathrm{N}(\alpha) = r^3 f^2 + (s^3 - 3rst)f + t^3. \tag{1}$$

By the statement after Definition 2.2, $\deg_X(\mathrm{N}(\alpha)) = \deg \alpha$, so that

$$\begin{aligned} \deg_X(\mathrm{N}(\alpha)) &= \max\{3\deg_X r + 2(g+1),\, 3\deg_X s + (g+1),\, 3\deg_X t\} \\ &= \deg D + 2\mu + \nu = \deg D + 2\deg D' - 3\nu \\ &\le \deg D + 2\deg D'. \end{aligned}$$

1. If $\deg D \le g-1$, then $\deg D' \le g-2$ and $\deg_X(\mathrm{N}(\alpha)) \le 3g-5$. Together with $\deg_X f = g+1$ and $g \in \{3,4\}$ this implies $r = 0$ and $\deg_X s \le 0$, i.e., $s \in \{0,1\}$. If $s = 1$, then $\operatorname{div}\alpha$ cannot contain a pair of conjugate points, whence $\mu = 0$, $\nu = \left\lfloor \frac{\deg D'}{2} \right\rfloor \le \left\lfloor \frac{g-2}{2} \right\rfloor \le 1$ and $\deg_X(\mathrm{N}(\alpha)) \le g-1+\left\lfloor \frac{g-2}{2} \right\rfloor \le g < \deg_X f$, a contradiction. If $s = 0$, then $\alpha = t$ is an element of $K[X]$ with zeroes including P_i^σ and Q_j, so that $\beta | \alpha$. Since $\deg D > \deg D'$ and $D = D' + \operatorname{div}\left(\frac{\alpha}{\beta}\right)$, we have $\deg_X \frac{\alpha}{\beta} \ge 1$, and D contains the divisor of a vertical line, i.e., a triplet of conjugate points.
2. Let now $\deg D = g$ and $r = 0$. We conclude from $\deg_X(\mathrm{N}(\alpha)) \le 3g-2$ that $\deg s \le 1$.

   If $s = 0$, then D contains the divisor of a vertical line as above.

   If $s = 1$, i.e., $\alpha = Y + t$, then as before $\operatorname{div}\alpha$ does not contain a pair of conjugate points, $\mu = 0$, $\nu \le \left\lfloor \frac{g-1}{2} \right\rfloor = 1$, $\deg_X(\mathrm{N}(\alpha)) \le g+1$ and $\deg_X t \le 1$. If $\nu = 0$, then $\beta = 0$ and $D = \operatorname{div}\alpha$, contradicting $\deg_X(\mathrm{N}(\alpha)) = \max\{\deg_X f, 3\deg_X t\} = \deg_X f = g+1$. So $\nu = 1$, $D' = Q^\sigma + Q^{\sigma^2}$ for some $Q = (x_Q, y_Q)$, and $\operatorname{div}(Y+t) = \operatorname{div}\alpha = D + Q$, whence D contains g collinear points.

   If $\deg_X s = 1$, the case $\mu = 0$ leads to $\deg_X(\mathrm{N}(\alpha)) \le g+1$ as in the previous paragraph, contradicting $\deg_X(s^3 f + t^3) \ge g+4$. Assume thus $\mu \ge 1$, and let $P = (x_P, y_P)$ be one of the P_i in D'. Then $s(x_P) = t(x_P) = 0$. (For unramified P, i.e., $y_P \ne 0$, this follows directly from $\alpha(P^\sigma) = \alpha(P^{\sigma^2}) = 0$. For ramified P, i.e., $y_P = 0$ and $P = P^\sigma$, recall that $\operatorname{ord}_P Y = 1$ and $\operatorname{ord}_P \alpha \ge 2$.) Hence $X - x_P | \alpha$ in $K[X,Y]$ and $P \le D$. This shows that $D - P$ reduces to $D' - P$ and by case 1, $D - P$ contains a triplet of conjugate points $Q + Q^\sigma + Q^{\sigma^2}$, so that $g = 4$, $D' = P$, $\beta = X - x_P$ and $\alpha = (X - x_P)(X - x_Q)$, a contradiction.
3. Finally let $\deg D = g$ and $r \ne 0$. Then $2g+2 \le 3\deg_X r + 2(g+1) \le \deg_X(\mathrm{N}(\alpha)) = \deg D + 2\deg D' - 3\nu \le \deg D + 2\deg D' \le 3g-2$ implies $g = 4$, equality in the previous chain of inequalities, i.e., $\nu = 0$, $\mu = 3$, $r = 1$, $D' = P_1 + P_2 + P_3$ with $P_i = (x_i, y_i)$, not necessarily distinct, $\alpha = Y^2 + sY + t$ and $\beta = (X - x_1)(X - x_2)(X - x_3)$. It follows now from $10 = \deg_X(\mathrm{N}(\alpha)) = \max\{10, 3\deg_X s + 5, 3\deg_X t\}$ that $\deg_X t \le 3$ and $\deg_X s \le 1$.

We proceed to show that $\beta | t - s^2$. Let $m \geq 1$ be such that $mP^\sigma + mP^{\sigma^2} \leq \operatorname{div}\alpha$ for $P = (x, y)$. If P is a ramification point, i.e., $y = 0$, then we deduce successively from $\operatorname{ord}_P Y = 1$ and $\operatorname{ord}_P \alpha \geq 2m \geq 2$ that $t(x) = 0$, $\operatorname{ord}_P t \geq 3$, $\operatorname{ord}_P(Y^2 + t) = 2$, $s(x) = 0$, $\operatorname{ord}_P s \geq 3$, $\operatorname{ord}_P \alpha = 2$ and $m = 1$. In particular, $(X - x)^m = X - x$ divides $t - s^2$ since the latter is zero in x. On the other hand, if P is not ramified, then $\operatorname{ord}_P Y = 0$, and $\operatorname{ord}_P(\alpha^\sigma) \geq m$, $\operatorname{ord}_P(\alpha^{\sigma^2}) \geq m$, which implies $m \leq \operatorname{ord}_P(\alpha^\sigma - \alpha^{\sigma^2}) = \operatorname{ord}_P(Y(Y - s)) = \operatorname{ord}_P(Y - s)$. Consider the function $\overline{\alpha} = (Y - s)^\sigma (Y - s)^{\sigma^2} = Y^2 + sY + s^2$. We have just shown that $mP^\sigma + mP^{\sigma^2} \leq \operatorname{div}\overline{\alpha}$, so that $mP^\sigma + mP^{\sigma^2} \leq \operatorname{div}(\alpha - \overline{\alpha}) = \operatorname{div}(t - s^2)$, which implies $(X - x)^m | t - s^2$ since P is unramified.

Hence, $(D')^\sigma + (D')^{\sigma^2} \leq \operatorname{div}\alpha$ leads to $\beta | t - s^2$. We have furthermore shown that $D' = P_1 + P_2 + P_3 \leq \operatorname{div}(Y - s)$. Bézout's theorem now implies that $\operatorname{div}(Y - s) = P_1 + P_2 + P_3 + Q + R = D' + Q + R$ for two further points Q and R, which are not necessarily distinct from the others and from each other. Consider two subcases.

(a) If $\deg_X t \leq 2$, then $\beta | t - s^2$ implies $t = s^2$ and $\alpha = \overline{\alpha}$. This shows that $D = Q^\sigma + Q^{\sigma^2} + R^\sigma + R^{\sigma^2}$.

(b) Let now $\deg_X t = 3$, so that $\alpha = Y^2 + sY + s^2 + c\beta$ for some $c \in K^\times$ is an elliptic curve. Then

$$\begin{aligned} D &= \operatorname{div}\alpha + D' - \operatorname{div}\beta \\ &= \operatorname{div}\alpha + (\operatorname{div}(Y - s) - Q - R) - \operatorname{div}(c\beta) \\ &\leq \operatorname{div}\left(\frac{\alpha(Y - s)}{c\beta}\right) \\ &= \operatorname{div}\left(Y - s + \frac{f - s^3}{c\beta}\right). \end{aligned}$$

Notice that β divides $f - s^3 = \mathrm{N}(Y - s)$ in $K[X]$ since

$$\operatorname{div}\beta \leq \operatorname{div}(\mathrm{N}(Y - s)).$$

Furthermore, the degree of $v = s - \frac{f - s^3}{c\beta}$ in X is 2, so that $Y - v$ defines a parabola containing the points in D (with the corresponding multiplicities).

Hereby, $\operatorname{div}\alpha = D + P_1^\sigma + P_2^\sigma + P_3^\sigma + P_1^{\sigma^2} + P_2^{\sigma^2} + P_3^{\sigma^2}$, and P_1, P_2 and P_3 lie on the line $Y - s$. Hence, we are indeed in the last case of the theorem.

This shows the necessity of the conditions given in Theorem 3.1. That they are sufficient is easily seen by constructing the reducing functions as above. □

Corollary 3.2. *On a superelliptic cubic of genus* 3 *or of genus* 4*, a typical divisor* $\operatorname{div}(u, Y - v)$ *is reduced whenever* $\deg u < g$*, or* $\deg u = g$ *and* $\deg v = g - 1$.

Proof. Theorem 3.1 shows that a nonreduced divisor of degree at most g either contains a pair of conjugate points, in which case it is not typical, or it is of degree g, but its points can be interpolated by a polynomial $Y - v$ with $\deg v \leq g - 2$. □

The proof of Theorem 3.1 relies on the fact that between a nonreduced divisor of sufficiently low degree and its reduced representative of even lower degree, there is not enough "space" to squeeze the divisor of a higher degree rational function. As

has also been seen in the theorem, the geometry becomes noticeably more intricate in genus 4 than in genus 3, with more possible functions between the two divisors. In higher genus, there are even more possibilities, and the corollary becomes wrong already in genus 6, which is the next largest case since the degree of f must not be divisible by 3.

Theorem 3.3. *If $g \geq 6$ and the field of definition K is sufficiently large, then on a superelliptic cubic of genus g over K there are rational nonreduced typical divisors* $\operatorname{div}(u, Y - v)$ *with* $\deg u = g$ *and* $\deg v = g - 1$.

Proof. Choose a line $Y - s$ with $s \in K[X]$ of degree 1, not tangent to the superelliptic curve. By Bézout's theorem, it intersects the curve in $g+1$ points $P_1, \ldots, P_{g+1}$, none of which is infinite. Furthermore, as the line is neither vertical nor tangent, all the X-coordinates of the P_i are distinct. Select an additional point Q on the curve with a different X-coordinate. Then there is no univariate polynomial of degree less than $g-1$ interpolating $P_1, \ldots, P_{g-1}$ and Q, since the unique such polynomial interpolating $P_1, \ldots, P_{g-1}$ is s. Thus, $P_1 + \cdots + P_{g-1} + Q$ is typical of the form $\operatorname{div}(u, Y - v)$ with $\deg u = g$ and $\deg v = g - 1$, but it is not reduced since it is equivalent to $P_g^\sigma + P_g^{\sigma^2} + P_{g+1}^\sigma + P_{g+1}^{\sigma^2} + Q$ of degree $5 < g$. □

As a concrete example for genus 6 consider the curve

$$Y^3 - \left(X^7 - 3X^6 - \frac{257}{120}X^5 + 15X^4 - \frac{271}{24}X^3 - 3X^2 - \frac{467}{30}X + 27\right)$$

over any field of characteristic different from 2, 3, 5, 7, 587, 1446474881 and 12668272824090432149. The divisor

$$\operatorname{div}\left(X^6 - 3X^5 - 5X^4 + 15X^3 + 4X^2 - 12X,\right.$$
$$\left. Y - \left(\frac{7}{120}X^5 - \frac{7}{24}X^3 - \frac{23}{30}X + 3\right)\right)$$

decomposes as $P_1 + \cdots + P_5 + Q$ with $P_1 = (-2, 5)$, $P_2 = (-1, 4)$, $P_3 = (0, 3)$, $P_4 = (1, 2)$ and $P_5 = (2, 1)$ on the line $Y - (-X + 3)$ and $Q = (3, 7)$. The reduction of this divisor yields

$$Q + \operatorname{div}\left(X^2 - 3X + \frac{343}{120}, Y^2 + (-X + 3)Y + \left(-3X + \frac{737}{120}\right)\right).$$

Over $\mathbb{Q}$, the second term is a prime divisor, but it decomposes as described above over some algebraic extension.

The divisors constructed in the proof of Theorem 3.3 are still special and close to the nonreduced cases of Theorem 3.1 since even though their points cannot be interpolated by a small degree polynomial, they contain a subdivisor with this property. However, while this special property eases a general description for all genus, it is not really necessary, as illustrated by the following example.

Example 3.4. Consider the curve $Y^3 - f$ where f is the polynomial:

$$X^7 - 133925X^6 - 389893X^5 + 722500X^4 + 897144X^3 + 1012596X - 1344397,$$

over some field of characteristic different from 2, 3 and 11 in which the polynomial in X does not have a double root and consider the divisor

$$\operatorname{div}\Big(X^6+3X^5-5X^4-8X^3+X^2-9X+11,\\ Y-(2X^5+4X^4-14X^3+10X^2-5X+1)\Big).$$

This divisor reduces to

$$\operatorname{div}\Big(X^5-268141X^4+17974684859X^3+49468657057X^2\\ +46578236952X+15407791040,\\ Y-\Big(\frac{1}{88}X^3-\frac{67299}{44}X^2-\frac{251135}{88}X-\frac{15403}{11}\Big)\Big),$$

but it does not contain a subdivisor which can be written in the form $\operatorname{div}(u, Y-v)$ with $\deg v < \deg u - 1$.

This sporadic example has been found by constructing an FGLM matrix of lower than expected rank; cf. Section 5.2.

4. Composition

As in hyperelliptic Jacobians, two typical reduced ideals $\mathfrak{a}_1 = \langle u_1, Y - v_1\rangle$ and $\mathfrak{a}_2 = \langle u_2, Y - v_2\rangle$ are multiplied in two steps. The first step is the *composition*, in which a representation $\langle u, Y - v\rangle$ for the product $\mathfrak{a}_1\mathfrak{a}_2$ is sought. The second step *reduces* this ideal, which corresponds to a divisor of degree up to $2g$, to one of degree at most g.

Composing two typical divisors does not necessarily result in a typical divisor again. When both divisors contain the same ramified prime, or one contains a split prime P and the other one its conjugate P^σ, then the composed divisor contains a pair of conjugate primes; Theorem 2.4 does not apply, and the standard representation by two polynomials will usually contain a polynomial of degree 2 in Y. In the light of Theorem 2.5, this event occurs, however, with negligible probability, so that we may content ourselves with describing the typical case. A multiplication algorithm for ideals in more general form, but with coprime norms, is described in [22]; for the general case, see [5].

Theorem 4.1. *Let* $\mathfrak{a}_1 = \langle u_1, Y - v_1\rangle$ *and* $\mathfrak{a}_2 = \langle u_2, Y - v_2\rangle$ *be typical reduced ideals of* $K[C]$*, i.e.,* u_i*,* $v_i \in K[X]$*,* $\deg v_i < \deg u_i \le g$ *and* $v_i^3 - f = u_i w_i$ *for some* $w_i \in K[X]$*. Suppose that* $\gcd(u_1, u_2, v_1^2 + v_1v_2 + v_2^2) = 1$*, and let* s_1*,* s_2*,* $s_3 \in K[X]$ *be such that*

$$s_1u_1 + s_2u_2 + s_3(v_1^2 + v_1v_2 + v_2^2) = 1.$$

Let

$$\begin{aligned} u &= u_1u_2,\\ \tilde{v} &= v_1 + s_1u_1(v_2 - v_1) - s_3(v_1^3 - f),\\ v &= \tilde{v} \bmod u,\\ \mathfrak{a} &= \langle u, Y - v\rangle. \end{aligned}$$

Then $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}$*, and* $u | v^3 - f$.

Proof. Notice that the expression for $\tilde{v}$ is in fact symmetric in v_1 and v_2 since

$$\begin{aligned}\tilde{v} &= (1 - s_1u_1)v_1 + s_1u_1v_2 - s_3(v_1^3 - f)\\ &= (s_2u_2 + s_3(v_1^2 + v_1v_2 + v_2^2))v_1 + s_1u_1v_2 - s_3(v_1^3 - f)\\ &= s_2u_2v_1 + s_1u_1v_2 + s_3(v_1^2v_2 + v_1v_2^2 + f)\\ &= v_2 + s_2u_2(v_1 - v_2) - s_3(v_2^3 - f).\end{aligned}$$

We show first that $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a} = \langle u, Y - v\rangle = \langle u, Y - \tilde{v}\rangle$. The product $\mathfrak{a}_1\mathfrak{a}_2$ is given by $\langle u_1u_2, u_1(Y - v_2), u_2(Y - v_1), (Y - v_1)(Y - v_2)\rangle$, and it suffices to show that its four generators lie in $\mathfrak{a}$. This is trivial for $u_1u_2 = u$.

$$\begin{aligned}u_1(Y - v_2) &= u_1(Y - \tilde{v}) + u_1(\tilde{v} - v_2)\\ &= u_1(Y - \tilde{v}) + u_1(s_2u_2(v_1 - v_2) - s_3(v_2^3 - f))\\ &= u_1(Y - \tilde{v}) + u(s_2(v_1 - v_2) - s_3w_2);\end{aligned}$$

thus, $u_1(Y - v_2) \in \mathfrak{a}$, and the same argumentation applies to $u_2(Y - v_1)$. Concerning the last generator,

$$\begin{aligned}(Y - v_1)(Y - v_2) &= (Y - v_2)(Y - \tilde{v}) + (Y - v_2)(\tilde{v} - v_1)\\ &= (Y - v_2)(Y - \tilde{v}) + (Y - \tilde{v})(\tilde{v} - v_1) + (\tilde{v} - v_2)(\tilde{v} - v_1),\end{aligned}$$

and it suffices to show that $(\tilde{v} - v_1)(\tilde{v} - v_2) \in \mathfrak{a}$. This holds since $u_1|\tilde{v} - v_1$ and $u_2|\tilde{v} - v_2$, so that u divides the product.

We next show that $u|v^3 - f$. Let p be an irreducible polynomial and e_i such that $p^{e_i}||u_i$; thus $p^e||u$ for $e = e_1 + e_2$. If $e_1 = 0$, then $p^{e_2}|v_2^3 - f$ and $v \equiv v_2 \pmod{u_2}$ imply that $p^e|v^3 - f$; ditto for $e_2 = 0$. If $e_1, e_2 \geq 1$, assume without loss of generality that $e_2 \leq e_1$, so that $u_1^2 \equiv 0 \pmod{p^e}$. Furthermore, $v_1^3 \equiv f \equiv v_2^3 \pmod{p^{e_2}}$, and from $\gcd\left(u_1, u_2, \frac{v_1^3 - v_2^3}{v_1 - v_2}\right) = 1$ we deduce that $p^{e_2}|v_1 - v_2$. This in turn yields $1 \equiv s_3(v_1^2 + v_1v_2 + v_2^2) \equiv 3s_3v_1^2 \pmod{p^{e_2}}$. By the definition of v, we have

$$v \equiv v_1 - s_3u_1w_1 \pmod{p^e}.$$

Hence,

$$\begin{aligned}v^3 - f &\equiv v_1^3 - f - 3v_1^2s_3u_1w_1 \pmod{p^e}\\ &\equiv u_1w_1(1 - 3s_3v_1^2) \equiv 0 \pmod{p^e}\end{aligned}$$

since $p^{e_1}|u_1$ and $p^{e_2}|1 - 3s_3v_1^2$.

Notice now that the norms of $\mathfrak{a}_1$, $\mathfrak{a}_2$ and $\mathfrak{a}$ are given by u_1, u_2 and $u = u_1u_2$, respectively; this follows from the divisibility by the u_* of the norms of the $Y - v_*$, which are given by $v_*^3 - f$. The unique decomposability of ideals in Dedekind domains into prime ideals and $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$ then imply $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}$. □

We may specialise Theorem 4.1 to the situations of squaring an ideal or of multiplying two distinct ideals. By the analysis of Theorem 2.5, there is an overwhelming probability that in the first case the corresponding divisor does not contain a ramified prime divisor and that in the second case, if one divisor contains a prime P, then the other divisor contains none of its conjugates P, P^σ or P^{σ^2}. This leads to the following algorithms for composition.

Corollary 4.2 (Squaring/doubling)**.** *Let* $\mathfrak{a}_1 = \langle u_1, Y - v_1\rangle$ *be a typical reduced ideal with* $v_1^3 - f = u_1w_1$*, and suppose that* $\gcd(u_1, v_1) = 1$*. Write*

$$s_1u_1 + 3s_3v_1^2 = 1,$$

and let

$$\begin{aligned} u &= u_1^2, \\ t &= -s_3 w_1 \bmod u_1, \\ v &= v_1 + t u_1. \end{aligned}$$

Then $\mathfrak{a}_1^2 = \langle u, Y - v \rangle$.

Corollary 4.3 (Multiplying/adding)**.** *Let* $\mathfrak{a}_1 = \langle u_1, Y - v_1 \rangle$ *and* $\mathfrak{a}_2 = \langle u_2, Y - v_2 \rangle$ *with* $v_i^3 - f = u_i w_i$ *be two typical reduced ideals such that* $\gcd(u_1, u_2) = 1$*. Write*

$$s_1 u_1 + s_2 u_2 = 1,$$

and let

$$\begin{aligned} u &= u_1 u_2, \\ t &= s_1(v_2 - v_1) \bmod u_2, \\ v &= v_1 + t u_1. \end{aligned}$$

Then $\mathfrak{a}_1 \mathfrak{a}_2 = \langle u, Y - v \rangle$.

Notice that the intermediate reduction of t implies directly that v is reduced modulo u.

In the next section we need an algorithm for inverting an ideal in the class group; the following algorithm solves this problem by multiplying the two conjugate ideals.

Proposition 4.4 (Inverting/negating)**.** *Let* $\mathfrak{a} = \langle u, Y - v \rangle$ *with* $v^3 - f = uw$ *be a typical reduced ideal such that* $\gcd(u, w) = 1$*. Then*

$$\langle u \rangle \mathfrak{a}^{-1} = \langle u, Y^2 + vY + v^2 \rangle.$$

Proof. Carrying out similar computations as in the proof of Theorem 4.1 and using the fact that u and w are coprime, we obtain

$$\mathfrak{a}^{\sigma} \mathfrak{a}^{\sigma^2} = \langle u, \zeta^{-1} Y - v \rangle \langle u, \zeta^{-2} Y - v \rangle = \langle u, Y^2 + Yv + v^2 \rangle.$$

From $\mathfrak{a} \mathfrak{a}^{\sigma} \mathfrak{a}^{\sigma^2} = \langle u \rangle$ we then deduce the desired equality. □

5. Reduction

Reduction algorithms have been proposed by Arita for C_{ab} curves [2, 3] and Galbraith, Paulus and Smart for superelliptic curves [12]. Later, Harasawa and Suzuki noticed that these algorithms follow the same principle and generalised [12] to C_{ab} curves. All these algorithms can be synthesised as follows.

Algorithm 5.1 (Reduction)**.**
Input: *ideal* $\mathfrak{a}$ *of* $K[C]$
Output: *reduced ideal* $\mathrm{Red}(\mathfrak{a})$ *equivalent to* $\mathfrak{a}$

1. *Choose an integral ideal* $\mathfrak{b}$ *in the class of* $\mathfrak{a}^{-1}$*, such that* $\mathfrak{b} = u\mathfrak{a}^{-1}$ *for some* $u \in \mathfrak{a}$*.*
2. *Let* $e \neq 0$ *be the minimum of* $\mathfrak{b}$ *with respect to the* C_{ab} *order.*
3. *Put* $\mathrm{Red}(\mathfrak{a}) = e\mathfrak{b}^{-1} = \frac{e}{u}\mathfrak{a}$*.*

Arita represents ideals of $K[C]$ by their Gröbner bases with respect to the C_{ab} order and chooses u as the C_{ab} minimum of $\mathfrak{a}$. His approach relies on Buchberger's algorithm, whose complexity in the C_{ab} setting is not quite clear.

In [12] and [15], ideals are represented by their Hermite normal forms as $K[X]$-modules or, equivalently, by their Gröbner bases with respect to the lexicographic order. The natural choice for u is then the minimum with respect to this order. The minimum for the C_{ab} order can be computed via a variant of LLL for function fields due to Paulus [21].

In this section, we describe two new algorithms for realising the arithmetic in the Jacobians of superelliptic cubics. We hereby concentrate on typical ideals as introduced in Theorem 2.4. Sometimes, further restrictions as examined in Section 2.2 are imposed. In the rare case that the input or output data do not match these assumptions, one may have recourse in the more general, but presumably slower, algorithms of [2, 3, 12, 15].

Our first algorithm is inspired by Cantor's reduction of ideals in hyperelliptic function fields [6]; it turns out, however, that it can also be stated in terms of Algorithm 5.1.

The second approach follows the framework of Algorithm 5.1. Representing ideals by their lexicographic Gröbner bases, we use the algorithm of [11] to find the C_{ab} minimum. This method applies in complete generality to any C_{ab} curve. We carry out the symbolic computations explicitly for typical divisors in superelliptic cubics of genus 3, thus obtaining closed formulae for the reduced ideal in this case.

5.1. **Cantor reduction.** Taking into account the similarities between the typical representation of reduced divisors in hyperelliptic and superelliptic Jacobians, one might be tempted to generalize the well-known reduction algorithms of the hyperelliptic case (see [6, 18, 7]). However, this approach fails for Gauß reduction, which would amount to replacing $\operatorname{div}(u, Y - v)$ by

$$\operatorname{div}\left(\frac{f - v^3}{u}, Y - \left(v \bmod \frac{f - v^3}{u}\right)\right),$$

which is a divisor in the opposite class. Unfortunately, if we are in the typical case with $\deg u = 2g$ and $\deg v = 2g - 1$, the new divisor has a degree of $4g - 2$, which is even larger than $2g$. For polynomials v of unusually low degree, however, the approach does work.

The generalization of Cantor's algorithm as described in [6], and for the case of characteristic 2 in [7], is more successful due to an additional degree of freedom.

Theorem 5.2. *Let the sequences of polynomials r_i, s_i and t_i such that $r_i = s_i u + t_i v$ be obtained from applying the extended Euclidian algorithm to u and v. Assume that we have $\gcd(r_i, t_i) = 1$. Let*

$$\begin{aligned} u' &= \frac{t_i^3 f - r_i^3}{u}, \\ v' &= r_i (t_i^{-1} \bmod u'). \end{aligned}$$

Then $\operatorname{div}(u', Y - v')$ is a divisor in the class opposite to $\operatorname{div}(u, Y - v)$.

Remark. Notice that by [7], Lemma 7, $\gcd(r_i, t_i) = 1$ happens with probability in $1 - \frac{1}{q} O(1)$ for any value of i. We then have

$$\gcd(t_i, u') \mid \gcd(t_i, t_i^3 f - r_i^3) \mid \gcd(t_i, r_i)^3 = 1,$$

so that the inverse of t_i modulo u' does indeed exist.

Proof of Theorem 5.2. Let $\sim$ denote equivalence of divisors.

$$\begin{aligned}
\operatorname{div}(u, Y - v) &= \operatorname{div}(u, t_i Y - t_i v) \text{ since } \gcd(t_i, u) \mid \gcd(t_i, r_i) = 1 \\
&= \operatorname{div}(u, t_i Y - r_i) \text{ since } t_i v \equiv r_i \pmod{u} \\
&\sim -(\operatorname{div}(t_i Y - r_i) - \operatorname{div}(u, t_i Y - r_i)) \\
&= -\operatorname{div}(u', t_i Y - r_i) \quad (*) \\
&= -\operatorname{div}(u', Y - r_i(t_i^{-1} \bmod u')).
\end{aligned}$$

For the step marked by $(*)$ notice that $\mathrm{N}(t_i Y - r_i) = t_i^3 f - r_i^3 = uu'$, so that $\operatorname{div}(t_i Y - r_i) = \operatorname{div}(uu', t_i Y - r_i)$. Let $x \in \overline{K}$ be a root of uu' corresponding to some point $P = (x, y)$ in $\operatorname{div}(t_i Y - r_i)$. Then $t_i(x) \neq 0$, since otherwise $r_i(x) = 0$, contradicting $\gcd(t_i, r_i) = 1$. Thus, $y = \frac{r_i(x)}{t_i(x)}$. Assume first that $y \neq 0$, which implies that P^σ and P^{σ^2} are not contained in $\operatorname{div}(t_i Y - r_i)$. Hence, if $(X - x)^k || uu'$, then the multiplicity of P^{σ^m} in $\operatorname{div}(t_i Y^{\sigma^n} - r_i)$ is k if $m = n$ and zero otherwise. On the other hand, if $y = 0$, then $r_i(x) = 0$, $\operatorname{ord}_P r_i \geq 3$, $\operatorname{ord}_P Y = 1$, and $t_i(x) \neq 0$ imply $\operatorname{ord}_P(t_i Y - r_i) = 1$. This shows that $k = 1$, and exactly one of u and u', say u, is divisible by $X - x$. The corresponding divisor $\operatorname{div}(u, t_i Y - r_i)$ contains P with multiplicity 1; the other one does not contain P. This shows that indeed $(*)$ holds. □

To obtain a reduction, the degree of the new divisor must be smaller than that of the original one. This is the case if i can be chosen such that

$$\max\{3 \deg_X r_i, 3 \deg_X t_i + (g+1)\} - \deg_X u < \deg_X u.$$

As in Cantor's algorithm, a suitable index i exists provided that the degrees of the remainder sequence in the Euclidian algorithm behave typically, i.e., decrease by 1 in each step. If there are larger jumps, then the algorithm may fail as in the case of hyperelliptic curves.

Theorem 5.3. *Let* $\operatorname{div}(u, Y - v)$ *be a divisor with* $\deg_X u \geq g$, $\deg_X v = \deg_X u - 1$ *and* $u | v^3 - f$. *Suppose that* $r_i = s_i u + t_i v$ *with* $\deg_X r_i = \deg_X u - 1 - i$ *and* $\deg_X t_i = i$. *Let* i_0 *be the closest integer to* $\frac{3 \deg_X u - g - 4}{6}$. *If* u', v' *are computed from* i_0 *as in Theorem 5.2, then* $\operatorname{div}(u', Y - v')$ *is a divisor in the opposite class of* $\operatorname{div}(u, Y - v)$. *If* $\deg_X u \geq g + 2$, *then* $\deg u' < \deg u$; *if* $\deg_X u \in \{g, g+1\}$, *then* $\deg u' = g$.

Proof. Define the function d by

$$d(i) = \max\{2 \deg_X u - 3 - 3i, 3i + g + 1 - \deg_X u\},$$

that is, by the degree of the divisor after one step of the reduction process in Theorem 5.2 with r_i and t_i. Since d is the maximum of a strictly decreasing and a strictly increasing linear function, it is minimized by $i_{\min} = \frac{3 \deg_X u - g - 4}{6}$, where the two linear functions admit the same value, if real arguments are permitted. The value in this point is given by $d(i_{\min}) = \frac{1}{2} \deg_X u + \frac{g}{2} - 1$, which satisfies $d(i_{\min}) = g - 1$ for $\deg_X u = g$, $d(i_{\min}) = g - \frac{1}{2}$ for $\deg_X u = g + 1$ and $d(i_{\min}) \leq \deg_X u - 2$ for $\deg_X u \geq g + 2$.

If only integral arguments are taken into account, then d takes its minimum in one of the neighbouring integers of $i_{\min}$. Letting i be one of them, the slopes -3 and $+3$ of the linear functions imply that $d(i) = d(i_{\min}) + 3|i - i_{\min}|$, so that the minimum is indeed attained for the closest integer i_0 to $i_{\min}$. Furthermore,

since $|i_0 - i_{\min}| \leq \frac{1}{2}$, we obtain $d(i_0) \leq \left\lfloor g - 1 + \frac{3}{2} \right\rfloor = g$ for $\deg_X u = g$ and $d(i_0) \leq \left\lfloor \deg_X u - 2 + \frac{3}{2} \right\rfloor = \deg_X u - 1$ for $\deg_X u \geq g + 2$. For $\deg_X u = g + 1$, this argument yields only $d(i_0) \leq g + 1$. However, in this case, i_0 equals $\frac{2g-1}{6}$ which cannot be half-integral since g is different from -1 modulo 3, so that in fact $\frac{1}{6} \leq |i_0 - i_{\min}| < \frac{1}{2}$ and $d(i_0) = g$. A similar argument shows that $|i_0 - i_{\min}| = \frac{1}{3}$ and $d(i_0) = g$ if $\deg_X u = g$. □

Theorem 5.4. *Let $g \in \{3, 4\}$, and assume the typical behavior of the remainder degrees of the Euclidian algorithm. Then two applications for $g = 3$, respectively four applications for $g = 4$, of the reduction process of Theorem 5.2 to a divisor $\operatorname{div}(u, Y - v)$ with $\deg u = 2g$ and $\deg v = 2g - 1$ yield the reduced divisor in the same class.*

Proof. If $g = 3$, then by Theorem 5.3, the first reduction step yields a divisor of degree 4 in the opposite class and the second one a divisor of degree 3 in the same divisor class. The first three steps in genus 4 transform the divisor of degree 8 to divisors of degree 6, 5 and 4, respectively, the latter of which lies in the opposite divisor class. So a fourth step is needed to obtain a divisor in the original class. By Corollary 3.2, these divisors are indeed reduced. □

Remarks.

1. Proposition 4.4 provides a simple way of computing the negative of a divisor class. However, the output is neither in typical form nor reduced. Theorem 5.3 and Corollary 3.2 show that in genus 3 or 4, one application of the algorithm to a divisor suffices to obtain the reduced representative in the opposite class.
2. If the genus of the superelliptic curve is larger than 4, then Theorem 5.3 still applies, and the algorithm will (with overwhelming probability) output a divisor of degree g. However, as seen in Section 3, this divisor need not necessarily be the reduced representative of the class. Nevertheless, the algorithm may be used for the intermediate steps of the multiplication of a divisor by a scalar. To assure reducedness of the final output, one may then use another algorithm for the last reduction step.
3. The algorithm can be interpreted as a specialisation of Algorithm 5.1. All but the last reduction step correspond to the computation of $\mathfrak{b}$.

Example 5.5. Consider the curve $Y^3 - f$ where f is the polynomial

$$X^4 + 391X^3 + 1300X^2 + 1583X + 1905$$

over the field $\mathbb{F}_{2003}$ and the ideal $\mathfrak{a} = \langle u, Y - v \rangle$ with

$$\begin{aligned} u &= X^6 + 420X^5 + 1293X^4 + 1420X^3 + 1149X^2 + 419X + 1538, \\ v &= 1559X^5 + 775X^4 + 1541X^3 + 162X^2 + 368X + 1864. \end{aligned}$$

The first step of the Cantor algorithm determines $\mathfrak{a}_1 = \langle u_1, Y - v_1 \rangle$ in the class of $\mathfrak{a}^{-1}$. Using Theorem 5.3, the polynomials u_1 and v_1 are computed with $i_0 = 2$ as

$$\begin{aligned} u_1 &= 1757 \left(X^4 + 294X^3 + 521X^2 + 374X + 1973 \right), \\ v_1 &= 1768X^3 + 349X^2 + 274X + 972. \end{aligned}$$

We need a second step with $i_0 = 1$, which yields $\operatorname{Red}(\mathfrak{a}) = \langle u', Y - v' \rangle$ with

$$\begin{aligned} u' &= 879 \left(X^3 + 1123X^2 + 428X + 1166 \right), \\ v' &= 1543X^2 + 882X + 921. \end{aligned}$$

5.2. **FGLM reduction.** The FGLM algorithm of [11] is an efficient method for switching between Gröbner bases for different orders. Since the first element of a Gröbner basis is the minimum of the ideal, an early abort solves the second step of Algorithm 5.1. We explain the principles of the algorithm applied to curves, illustrating them by the concrete case of superelliptic cubics. All computations may be carried out symbolically, which can be used to obtain explicit formulae for the reduced ideal in terms of the coefficients of the input polynomials.

Let $K[C]$ be the coordinate ring of a curve and $\mathfrak{b}$ an ideal of $K[C]$. Consider $K[C]/\mathfrak{b}$ as a K-vector space with the natural basis $B = (b_1, \dots, b_k)$ formed by reduced monomials modulo $\mathfrak{b}$, ascending with respect to the first order. It is understood that the monomials are also reduced modulo the curve equation C.

In the context of Algorithm 5.1, we have $\mathfrak{a} = \langle u, Y - v\rangle$ with $\deg u = 6$ and we let $\mathfrak{b} = u\mathfrak{a}^{-1} = \langle u, Y^2 + vY + v^2\rangle$ by Proposition 4.4. The Gröbner basis of $\mathfrak{b}$ with respect to the lexicographic order is given by

$$[u, uY, Y^2 + vY + (v^2 \bmod u)],$$

whence

$$B = (1, X, X^2, X^3, X^4, X^5, Y, YX, YX^2, YX^3, YX^4, YX^5)$$

and $k = 12$.

Similarly, let $B' = (b'_1, \dots, b'_{k+1})$ be formed from the first $k+1$ monomials, again reduced modulo the curve equation and ascending with respect to the second order. In our case, we are interested in the $C_{3,4}$ order, so that

$$B' = (1, X, Y, X^2, XY, Y^2, X^3, YX^2, Y^2X, X^4, YX^3, Y^2X^2, X^5).$$

As $|B'| = |B| + 1$, the b'_i are K-linearly dependent in $K[C]/\mathfrak{b}$. Notice that any nontrivial linear relation $\sum \lambda_i b'_i = 0$ means that $b = \sum \lambda_i b'_i$ is an element of $\mathfrak{b}$. The ordering of B' implies that the second order of b equals that of the last b'_i with $\lambda_i \neq 0$. The minimum of $\mathfrak{b}$ with respect to the second order can thus be obtained by constructing B' incrementally, that is, adding the b'_i one by one, until the set becomes linearly dependent. This leads to the following algorithm.

Algorithm 5.6 (Minimum by FGLM)**.**
Input: $\mathfrak{b}$, B *and* B'
Output: $i \leq |B'|$ *and* $\lambda_1, \dots, \lambda_{i-1}$ *s.t.* $b'_i - \sum_{j=1}^{i-1} \lambda_j b'_j$ *is the minimum of* $\mathfrak{b}$ *w.r.t. the second order*

1. $M \leftarrow$ *empty matrix,* $i \leftarrow 0$
2. **while** $\operatorname{rank} M = i$
   - $i \leftarrow i + 1$
   - *write* $b'_i = \sum_{j=1}^{k} \mu_{ij} b_j$
   - *add* $(\mu_{i1}, \dots, \mu_{ik})$ *as a new row to* M
3. *compute* $\lambda_1, \dots, \lambda_{i-1}$ *s.t.* $b'_i = \sum_{j=1}^{i-1} \lambda_j b'_j$

Before applying the algorithm to our case, we fix some notation which will be used throughout this and the following section.

Notation 5.7. For $u \in K[X]$ and $\alpha \in K[X, Y]$ we denote by $\delta_u(\alpha)$ the quotient and by $\varphi_u(\alpha)$ the remainder in $K[X, Y]$ of α divided by u. When no confusion is possible, we omit the subscript u.

We now apply Algorithm 5.6 symbolically to the ideal $\mathfrak{b} = \langle u, Y^2 + vY + \varphi(v^2)\rangle$ of a superelliptic cubic of genus 3, where u is monic of degree 6. After the first six iterations, the matrix looks as follows. A subscript i indicates the coefficient of X^i of a polynomial, and an entry "$*$" stands for some element of K.

	1	X	X^2	X^3	X^4	X^5	Y	XY	X^2Y	X^3Y	X^4Y	X^5Y
1	1	0	0	0	0	0	0	0	0	0	0	0
X	0	1	0	0	0	0	0	0	0	0	0	0
Y	0	0	0	0	0	0	1	0	0	0	0	0
X^2	0	0	1	0	0	0	0	0	0	0	0	0
XY	0	0	0	0	0	0	0	1	0	0	0	0
Y^2	$*$	$*$	$*$	$-\varphi(v^2)_3$	$-\varphi(v^2)_4$	$-\varphi(v^2)_5$	$*$	$*$	$-v_2$	$-v_3$	$-v_4$	$-v_5$

If we had $\deg(v) \leq 1$, then we would obtain a linear dependency and $Y^2 + vY + \varphi(v^2)$ would be the minimum of $\mathfrak{b}$. In the typical case, where $\deg(v) = 5$, we continue. The next interesting situation arises after adding XY^2, which is not an element of B.

	1	X	X^2	X^3	X^4	X^5	Y	XY	X^2Y	X^3Y	X^4Y	X^5Y
X^3	0	0	0	1	0	0	0	0	0	0	0	0
X^2Y	0	0	0	0	0	0	0	0	1	0	0	0
XY^2	$*$	$*$	$*$	$*$	$-\varphi(Xv^2)_4$	$-\varphi(Xv^2)_5$	$*$	$*$	$*$	$-\varphi(Xv)_3$	$-\varphi(Xv)_4$	$-\varphi(Xv)_5$

The algorithm could only stop here if (v_4, v_5) and $(\varphi(Xv)_4, \varphi(Xv)_5)$ were linearly dependent, i.e., if

$$\det \begin{pmatrix} v_4 & v_5 \\ \varphi(Xv)_4 & \varphi(Xv)_5 \end{pmatrix} = 0.$$

Notice that since $\varphi(Xv) = Xv - v_5 u$, this determinant equals v_5^2 times the coefficient of X^4 of $u \bmod v$. For a typical remainder sequence in the Euclidian algorithm, however, we expect this coefficient to be different from zero. After three further iterations we obtain a square matrix, which we expect to be nonsingular (we will see later that otherwise the reduced ideal would have a norm of degree less than 3).

	1	X	X^2	X^3	X^4	X^5	Y	XY	X^2Y	X^3Y	X^4Y	X^5Y
X^4	0	0	0	0	1	0	0	0	0	0	0	0
X^3Y	0	0	0	0	0	0	0	0	0	1	0	0
X^2Y^2	$*$	$*$	$*$	$*$	$*$	$-\varphi(X^2v^2)_5$	$*$	$*$	$*$	$*$	$-\varphi(X^2v)_4$	$-\varphi(X^2v)_5$
X^5	0	0	0	0	0	1	0	0	0	0	0	0

Solving the linear system, we compute a quadratic polynomial $t = t_2X^2 + t_1X + t_0$ and the minimum

$$\begin{aligned} e &= tY^2 + \left(\varphi(tv)_3X^3 + \varphi(tv)_2X^2 + \varphi(tv)_1X + \varphi(tv)_0\right)Y + \varphi(tv^2) \\ &= tY^2 + \left(\varphi(tv) \bmod X^4\right)Y + \varphi(tv^2). \end{aligned}$$

We show now that in fact

$$e = tY^2 + \varphi(tv)Y + \varphi(tv^2),$$

or, otherwise said, that $\varphi(tv)$ is of degree at most 3. As an element of $\mathfrak{b} = [u, uY, Y^2 + vY + \varphi(v^2)]$ with leading term tY^2, e can be written as a linear combination $tY^2 + tvY + t\varphi(v^2) + q_1uY + q_2u$. So its coefficient in Y is given by $tv + q_1u$. Computing the C_{ab} degrees of all terms, one finds that e can only be the minimum if its coefficient in Y equals $\varphi(tv)$.

The concrete value of t is given as follows. (Notice that t is only defined up to a constant factor; we choose it to be monic.)

$$\begin{aligned} t_1 &= \frac{v_4v_3 - v_2v_5 - u_5v_4^2 + v_4u_5^2v_5 - u_4u_5v_5^2 + u_3v_5^2}{v_5v_3 - u_4v_5^2 - v_4^2 + v_4u_5v_5} \\ t_0 &= \frac{v_5u_4 + u_5v_4 - v_3 - u_5^2v_5}{v_5} + \frac{v_5u_5 - v_4}{v_5}\, t_1\,. \end{aligned}$$

As a side note, t is (up to a constant factor) the multiplier of v obtained after applying two steps of the extended Euclidian algorithm to u and v, that is, $\beta u + tv = r$ with r of degree 3. This is specific to the case of genus 3.

Our aim is now to derive an expression for $\mathrm{Red}(\mathfrak{a})$ in the form $\langle u', Y - v'\rangle$. First, we show how to compute u'. By Algorithm 5.1, we have $\mathrm{Red}(\mathfrak{a}) = \frac{e}{u}\mathfrak{a} = \langle e, \tilde{e}\rangle$ with $\tilde{e} = e(Y - v)/u$. We let u' be the norm of $\mathrm{Red}(\mathfrak{a})$, given by

$$\frac{\mathrm{N}(e)\,\mathrm{N}(\mathfrak{a})}{\mathrm{N}(u)} = \frac{\mathrm{N}(e)}{u^2} = \frac{t^3f^2 + (\varphi(tv)^3 - 3t\varphi(tv)\varphi(tv^2))f + \varphi(tv^2)^3}{u^2},$$

where $\mathrm{N}(e)$ is computed from (1). Recall that the degree of $\mathrm{N}(e)$ equals the C_{ab} order of e, so that it is 15, and u' is of degree 3. If we succeed in finding an element $Y - v'$ of $\mathrm{Red}(\mathfrak{a})$ with $v' \in K[X]$, then $\langle u', Y - v'\rangle$ is an ideal contained in $\mathrm{Red}(\mathfrak{a})$ of the same norm, so that these two ideals are equal. Furthermore, u' divides automatically the norm $f - (v')^3$ of $Y - v'$.

Remark. If the FGLM Algorithm 5.6 had found a minimum e before the last step, then the degree of $\mathrm{N}(e)$ would be less than 15, and we would find an element u' in $\mathrm{Red}(\mathfrak{a})$ of degree less than 3. This shows that in the typical case, the matrix constructed by FGLM is of maximal rank, and the minimum is found in the last step only, an argumentation that easily generalises to other curves.

To find a polynomial in $\mathrm{Red}(\mathfrak{a})$ which is linear in Y, we define $w \in K[X]$ by $\frac{v^3 - f}{u}$ and develop

$$\tilde{e} = -\delta(tv)Y^2 + (v\delta(tv) - \delta(tv^2))Y + (v\delta(tv^2) - tw).$$

A polynomial combination of e and $\tilde{e}$ eliminates Y^2 and yields

$$\tilde{v} = t\tilde{e} - \delta(tv)e = \tilde{v}_1 Y - \tilde{v}_0$$

with

$$\begin{aligned} \tilde{v}_1 &= t\,\delta(tv^2) - \delta(tv)(\varphi(tv) + tv), \\ \tilde{v}_0 &= -t^2w + tv\,\delta(tv^2) + \delta(tv)\varphi(tv^2). \end{aligned}$$

Substituting $\delta(tv)$ and $\delta(tv^2)$, we find the alternative expression

$$\tilde{v}_1 = \frac{\varphi(tv)^2 - t\varphi(tv^2)}{u},$$

which shows that $\tilde{v}_1$ is of degree (at most) 1. In the typical case, we expect it to be invertible modulo u', so that $v' = (\tilde{v}_1)^{-1}\tilde{v}_0$. Notice that $(\tilde{v}_1)^{-1}$ is easily computed symbolically.

Example 5.8. We resume Example 5.5, applying the explicit FGLM formulae. The minimum with respect to the C_{ab} order in $\mathfrak{b}$ is given by

$$e = tY^2 + (tv \bmod u)Y + (tv^2 \bmod u),$$

where $t = 1328X^2 + 911X + 1446$. Then

$$\begin{aligned} \frac{\mathrm{N}(e)}{u^2} &= 1513\left(X^3 + 1123X^2 + 428X + 1166\right), \\ \tilde{v} &= (1465X + 536)\,Y + 1783X^2 + 1510X + 570, \\ v' &= 1543X^2 + 882X + 921. \end{aligned}$$

6. Further results

During this article we focus on the typical behaviour of divisors in superelliptic Jacobians, occurring virtually all the time. Of course, it is possible to adapt the algorithms to treat nontypical cases as well. The FGLM method, for instance, actually becomes simpler, since the matrix does not have full rank any more and the minimum is found earlier.

Carrying out the computations of the FGLM algorithm symbolically, we have obtained explicit reduction formulae relating the coefficients of the output polynomials to those of the input polynomials. In the following table, we provide the number of multiplications and inversions in the ground field needed by the different algorithms to reduce a typical ideal of degree 6 in the Jacobian of a genus 3 superelliptic curve. The numbers should not be taken literally, since they are subject to considerable variations depending on the polynomial arithmetic used and the exact arrangement of the computations. They are rather meant to convey a vague idea on how the algorithms behave. We describe our implementations of the new algorithms in more detail in [4].

	formulae	Cantor	following [12]
mul.	150	200	510
inv.	6	10	10

The described algorithms generalise without difficulty to $C_{3,b}$ curves. Completing the cube, we can assume that such a curve is given by an equation of the form

$$C = Y^3 + hY - f$$

with $\deg f = b$ and $\deg h \leq \left\lfloor \frac{2b}{3} \right\rfloor$. The formulae for Cantor reduction (cf. Theorem 5.2) then become

$$\begin{aligned} u' &= \frac{t_i^3 f - t_i^2 r_i h - r_i^3}{u}, \\ v' &= r_i (t_i^{-1} \bmod u). \end{aligned}$$

Notice that the degree restriction on h implies that Theorem 5.3 remains valid, whence the same number of reduction steps is needed as for superelliptic curves.

Acknowledgments

Our motivation for examining reducedness criteria for superelliptic ideals stems from intensive discussions with Pierrick Gaudry, to whom we are most indebted. We thank Mark Bauer for interesting discussions on C_{ab} curves. Thanks to Guillaume Hanrot and François Morain for their careful reading of the manuscript. The second author gratefully acknowledges being supported by a fellowship within the postdoctoral program of the German Academic Exchange Service (DAAD). This research was partially supported by the French Ministry of Research — ACI Cryptocourbes.

References

[1] Leonard M. Adleman, Jonathan DeMarrais, and Ming-Deh Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In Leonard M. Adleman and Ming-Deh Huang, editors, *Algorithmic Number Theory — ANTS-I*, volume 877 of *Lecture Notes in Computer Science*, pages 28–40, Berlin, 1994. Springer-Verlag. MR96b:11078

[2] Seigo Arita. Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log based public key cryptosystems. *IEICE Transactions*, J82-A(8):1291–1299, 1999. In Japanese. English translation in the proceedings of the Conference on The Mathematics of Public Key Cryptography, Toronto 1999.

[3] Seigo Arita. An addition algorithm in Jacobian of C_{ab} curves. *Discrete Applied Mathematics*, 130(1):13–31, 2003.

[4] Abdolali Basiri, Andreas Enge, Jean-Charles Faugère, and Nicolas Gürel. Implementing the arithmetic of $C_{3,4}$ curves. In Duncan Buell, editor, *Algorithmic Number Theory — ANTS-VI*, Lecture Notes in Computer Science, Berlin, 2004. Springer-Verlag, vol. 3076, pp. 87–101.

[5] Mark L. Bauer. The arithmetic of certain cubic function fields. *Mathematics of Computation*, 73(245):387–413, 2004.

[6] David G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Mathematics of Computation*, 48(177):95–101, 1987. MR88f:11118

[7] Andreas Enge. The extended Euclidian algorithm on polynomials, and the computational efficiency of hyperelliptic cryptosystems. *Designs, Codes and Cryptography*, 23(1):53–74, 2001. MR2002e:94096

[8] Andreas Enge. A general framework for subexponential discrete logarithm algorithms in groups of unknown order. In A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel, and J. A. Thas, editors, *Finite Geometries*, volume 3 of *Developments in Mathematics*, pages 133–146, Dordrecht, 2001. Kluwer Academic Publishers.

[9] Andreas Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. *Mathematics of Computation*, 71(238):729–742, 2002. MR2003b:68083

[10] Andreas Enge and Pierrick Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta Arithmetica*, 102(1):83–103, 2002. MR2002k:11225

[11] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16:329–344, 1993. MR94k:68095

[12] Steven D. Galbraith, Sachar Paulus, and Nigel P. Smart. Arithmetic on superelliptic curves. *Mathematics of Computation*, 71(237):393–405, 2002. MR2002h:14102

[13] Pierrick Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In Bart Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 19–34, Berlin, 2000. Springer-Verlag. MR2001b:94028

[14] Pierrick Gaudry and Nicolas Gürel. An extension of Kedlaya's point counting algorithm to superelliptic curves. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 480–494, Berlin, 2001. Springer-Verlag. MR2003h:11159

[15] Ryuichi Harasawa and Joe Suzuki. Fast Jacobian group arithmetic on C_{ab} curves. In Wieb Bosma, editor, *Algorithmic Number Theory — ANTS-IV*, volume 1838 of *Lecture Notes in Computer Science*, pages 359–376, Berlin, 2000. Springer-Verlag. MR2002f:11073

[16] Florian Heß. Computing Riemann–Roch spaces in algebraic function fields and related topics. *Journal of Symbolic Computation*, 33(4):425–445, 2002. MR2003j:14032

[17] Ming-Deh Huang and Doug Ierardi. Efficient algorithms for the Riemann–Roch problem and for addition in the Jacobian of a curve. *Journal of Symbolic Computation*, 18:519–539, 1994. MR96h:14077

[18] Neal Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1:139–150, 1989. MR90k:11165

[19] Shinji Miura. Linear codes on affine algebraic curves. *IEICE Transactions*, J81-A:1398–1421, 1998. In Japanese. English summary by Ryutaroh Matsumoto available at `http://www.rmatsumoto.org/cab.html`.

[20] Volker Müller, Andreas Stein, and Christoph Thiel. Computing discrete logarithms in real quadratic congruence function fields of large genus. *Mathematics of Computation*, 68(226):807–822, 1999. MR99i:11119

[21] Sachar Paulus. Lattice basis reduction in function fields. In J. P. Buhler, editor, *Algorithmic Number Theory — ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 567–575, Berlin, 1998. Springer-Verlag. MR2000i:11193

[22] Renate Scheidler. Ideal arithmetic and infrastructure in purely cubic function fields. *Journal de Théorie des Nombres de Bordeaux*, 13:609–631, 2001. MR2002k:11209

[23] Emil Volcheck. Computing in the Jacobian of a plane algebraic curve (extended abstract). In Leonard M. Adleman and Ming-Deh Huang, editors, *Algorithmic Number Theory — ANTS-I*, volume 877 of *Lecture Notes in Computer Science*, pages 221–233, Berlin, 1994. Springer-Verlag. MR96a:14033

[24] André Weil. Sur les courbes algébriques et les variétés qui s'en déduisent. In *Courbes algébriques et variétés abéliennes*. Hermann, Paris 1971, 1948. MR10:262c

Laboratoire d'Informatique de Paris 6 (CNRS/UMR 7606), 4 place Jussieu, 75252 Paris Cedex 05, France

E-mail address: basiriab2@yahoo.com

Current address: Department of Mathematics and Computer Sciences, Damghan University of Sciences, Damghan, Iran

INRIA Futurs and Laboratoire d'Informatique (CNRS/FRE 2653), École polytechnique, 91128 Palaiseau Cedex, France

E-mail address: enge@lix.polytechnique.fr

URL: http://www.lix.polytechnique.fr

Laboratoire d'Informatique de Paris 6 (CNRS/UMR 7606), 4 place Jussieu, 75252 Paris Cedex 05, France

E-mail address: jcf@calfor.lip6.fr

URL: http://www-calfor.lip6.fr

INRIA Futurs and Laboratoire d'Informatique (CNRS/FRE 2653), École polytechnique, 91128 Palaiseau Cedex, France

E-mail address: gurel@lix.polytechnique.fr

URL: http://www.lix.polytechnique.fr