Fast arithmetic on hyperelliptic curves via continued fraction expansions

M. J. Jacobson, Jr.

Department of Computer Science, University of Calgary,
2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4
E-mail: jacobs@cpsc.ucalgary.ca

R. Scheidler*

Department of Mathematics and Statistics, University of Calgary,
2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4
E-mail: rscheidl@math.ucalgary.ca

A. Stein

Department of Mathematics, University of Wyoming
1000 E. University Avenue, Laramie, WY 82071-3036, USA
Email: astein@uwyo.edu

In this paper, we present a new algorithm for computing the reduced sum of two divisors of an arbitrary hyperelliptic curve. Our formulas and algorithms are generalizations of Shanks's NUCOMP algorithm, which was suggested earlier for composing and reducing positive definite binary quadratic forms. Our formulation of NUCOMP is derived by approximating the irrational continued fraction expansion used to reduce a divisor by a rational continued fraction expansion, resulting in a relatively simple and efficient presentation of the algorithm as compared to previous versions. We describe a novel, unified framework for divisor reduction on an arbitrary hyperelliptic curve using the theory of continued fractions, and derive our formulation of NUCOMP based on these results. We present numerical data demonstrating that our version of NUCOMP is more efficient than Cantor's algorithm for most hyperelliptic curves, except those of very small genus defined over small finite fields.

Keywords: Hyperelliptic curve, reduced divisor, continued fraction expansion, infrastructure, Cantor's algorithm, NUCOMP

*The research of the first two authors is supported by NSERC of Canada.

1. Introduction and Motivation

Divisor addition and reduction is one of the fundamental operations required for a number of problems and applications related to hyperelliptic curves. The group law of the Jacobian can be realized by this operation, and as such, applications ranging from computing the structure of the divisor class group to cryptographic protocols depend on it. Furthermore, the speed of algorithms for solving discrete logarithm problems on hyperelliptic curves, particularly of medium and large size genus, depend on a fast computation of the group law. There has been a great deal of work on finding efficient algorithms for this operation (see for instance [5]).

Cantor's algorithm [2] is a generic algorithm that allows this operation to be explicitly computed. It works by first adding the two divisors and subsequently reducing the sum. One drawback of this approach, and most algorithms derived from it, is that one has to deal with intermediate operands of double size. That is, while the basis polynomials of the two starting divisors and the final reduced divisor have degree at most g, where g is the genus of the curve, the divisor sum has a basis consisting of two polynomials whose degree is usually as large as $2g$, and reduction only gradually reduces the degrees back down to g. This greatly reduces the speed of the operation, and it is highly desirable to be able to perform divisor addition and reduction without having to compute with quantities of double size.

The group operation of the class group of positive definite binary quadratic forms, composition and reduction, suffers from the same problem of large intermediate operands. In 1988, Shanks [13] devised a solution to this problem, an algorithm he called NUCOMP. The idea behind this algorithm is to stop the composition process before completion and apply a type of intermediate reduction before computing the composed form. Instead of using the rather expensive continued fraction algorithm that produces the aforementioned intermediate operands of double size, the reduction is performed using the much less costly extended Euclidean Algorithm. The coefficients are only computed once the form is reduced or almost reduced. As a result, the sizes of the intermediate operands are significantly smaller, and the binary quadratic form produced by NUCOMP is very close to being reduced.

In [11], van der Poorten generalized NUCOMP to computing with ideals in the infrastructure of a real quadratic number field by showing how the relative generator corresponding to the output can be recovered. Jacobson and van der Poorten [6] presented numerical evidence for the efficiency

of their version of NUCOMP. They also sketched an adaptation of this method to arithmetic in the class group and infrastructure of a hyperelliptic curve. Their computational results indicated that their version of NUCOMP was more efficient than Cantor's algorithm for moderately small genera (between genus 5 and 10), and that the relative efficiency improved as both the genus and size of the ground field increase. However, a formal analysis and description of NUCOMP in the hyperelliptic curve setting was not provided.

Shanks's formulation of NUCOMP, as well as the treatments in [11] and [6], are based on the arithmetic of binary quadratic forms. In [8], the authors described NUCOMP in terms of ideal arithmetic in real quadratic number fields. They provided a clear and complete description of NUCOMP in terms of continued fraction expansions of real quadratic irrationalities and, in addition, showed how to optimize the formulas in this context.

In this paper, we provide a unified description of NUCOMP for divisor arithmetic on the three different possible models of a hyperelliptic curve: imaginary, real, and unusual [3]. We generalize the results in [8], describing and deriving NUCOMP in terms of continued fraction expansions in all three settings. Furthermore, we explain NUCOMP purely in terms of divisor arithmetic, also incorporating the infrastructure arithmetic of a real hyperelliptic curve. Our formulation of NUCOMP is complete and somewhat simpler than that in [6], and its relation to Cantor's algorithm is more clear. In addition, we prove its correctness and a number of related results, including the fact that the output is in most cases reduced, and is in the worst case only one step away from being reduced. The end result, supported by computational results, is that our improved formulation of NUCOMP offers performance improvements over Cantor's algorithm for even smaller genera than indicated in [6].

We begin in Sec. 2 with an overview of continued fractions, and explain divisor arithmetic on hyperelliptic curves and its connection to continued fractions in Sec. 3–Sec. 5. Based on this foundation, we describe divisor addition and reduction as well as NUCOMP in Sec. 6–Sec. 10. We conclude with numerical results in Sec. 11, including a discussion of the efficiency of our two different versions of NUCOMP as given in Sec. 9.

2. Continued Fraction Expansions

For brevity, we write the symbolic expression

$$s_0 + \cfrac{1}{s_1 + \cfrac{1}{\ddots \\ s_n + \cfrac{1}{\alpha_{n+1}}}}$$

as $[s_0, s_1, \ldots, s_n, \alpha_{n+1}]$. If we wish to leave the end of the expression undetermined, we simply write $[s_0, s_1, \ldots]$.

Let k be any field, $k[t]$ the ring of polynomials in the indeterminate t with coefficients in k, and $k(t)$ the field of rational functions in t with coefficients in k. It is well-known that the completion of $k(t)$ with respect to the place at infinity of $k(t)$ (corresponding to the discrete valuation "denominator degree minus numerator degree") is the field $k\langle t^{-1}\rangle$ of Puiseux series in t^{-1}; that is, any non-zero element in $k\langle t^{-1}\rangle$ is of the form

$$\alpha = \sum_{i=-\infty}^{d} a_i t^i \ ,$$

where $d \in \mathbb{Z}$, $a_i \in k$ for $i \leq d$, and $a_d \neq 0$. Define

$$\lfloor \alpha \rfloor = \sum_{i=0}^{d} a_i t^i \ , \qquad \mathrm{sgn}(\alpha) = a_d \ , \qquad \deg(\alpha) = d \ . \tag{2.1}$$

Also, define $\lfloor 0 \rfloor = 0$ and $\deg(0) = -\infty$.

Let $n \geq 0$, $s_0, s_1, \ldots, s_n$ a sequence of polynomials in $k[t]$, and $\alpha \in k\langle t^{-1}\rangle$ non-zero. Then the expression

$$\alpha = [s_0, s_1, \ldots, s_n, \alpha_{n+1}] \tag{2.2}$$

is referred to as the (*ordinary*) *continued fraction expansion* of α with *partial quotients* $s_0, s_1, \ldots, s_n$. It uniquely defines a Puiseux series $\alpha_{n+1} \in k\langle t^{-1}\rangle$ where $\alpha_0 = \alpha$ and $\alpha_{i+1} = (\alpha_i - s_i)^{-1}$ for $0 \leq i \leq n$. If we set

$$\begin{array}{l} A_{-2} = 0 \ , A_{-1} = 1 \ , A_i = s_i A_{i-1} + A_{i-2} \ , \\ B_{-2} = 1 \ , B_{-1} = 0 \ , B_i = s_i B_{i-1} + B_{i-2} \ , \end{array} \tag{2.3}$$

for $0 \leq i \leq n$, then $A_i/B_i = [s_0, s_1, \ldots, s_i]$ for $0 \leq i \leq n-1$. Since $A_i B_{i-1} - A_{i-1} B_i = (-1)^{i-1}$ for $-1 \leq i \leq n$, A_i and B_i are coprime for $-2 \leq i \leq n$.

If $s_i = q_i$ with $q_i = \lfloor \alpha_i \rfloor$ for $i \geq 0$, then Eq. (2.2) is the well-known *regular* continued fraction expansion of α. Here, the partial quotients $q_0, q_1, \ldots$

are uniquely determined by α, and $\deg(q_i) \geq 1$ for all $i \in \mathbb{N}$. The rational function $A_i/B_i = [q_0, q_1, \ldots, q_i]$ is the *i-th convergent* of α. This term is motivated by the well-known inequalities

$$\deg\left(\alpha - \frac{A_i}{B_i}\right) \leq -\deg(B_i B_{i+1}) < -2\deg(B_i) \tag{2.4}$$

for all $i \geq 0$. The following result is also well-known:

Lemma 2.1. *Let $\alpha \in k\langle t^{-1}\rangle$, $E, F \in k[t]$ with $\alpha F \neq 0$ and $\gcd(E, F) = 1$. If*

$$\deg\left(\alpha - \frac{E}{F}\right) < -2\deg(F) \ ,$$

then E/F is a convergent in the regular continued fraction expansion of α.

Throughout this paper, we reserve the symbols q_i and $\hat{q}_i$ for the quotients of a regular continued fraction expansion; for arbitrary partial quotients, we use the symbol s_i. To distinguish expansions of rational functions from those of Puiseux series, we henceforth use the convention that partial quotients and convergents relating to expansions of rational functions are equipped with a "$\hat{}$" symbol, whereas quantities pertaining to expansions of Puiseux series do not have this symbol.

One of the main ideas underlying NUCOMP is to approximate the regular continued fraction expansion of a Puiseux series by that of a rational function "close" to it. We then expect the convergents, and hence the two expansions, to agree up to a certain point:

Theorem 2.1. *Let $\alpha \in k\langle t^{-1}\rangle$ and $\hat{\alpha} \in k(t)$ be non-zero, and write $\hat{\alpha} = E/F$ with $E, F \in k[t]$. Let $\hat{q}_i$ $(0 \leq i \leq m)$ and $\hat{r}_i$ $(-1 \leq i \leq m)$ be the sequences of quotients and remainders, respectively, obtained by applying the Euclidean Algorithm to $\hat{\alpha}$; that is, $\hat{r}_{-2} = E$, $\hat{r}_{-1} = F$, $\hat{r}_{i-2} = \hat{q}_i \hat{r}_{i-1} + \hat{r}_i$ with $\hat{q}_i = \lfloor r_{i-2}/r_{i-1} \rfloor$ for $0 \leq i \leq m$, so $\hat{r}_{m-1} = \gcd(E, F)$ and $\hat{r}_m = 0$. If there exists $n \in \mathbb{Z}$, $-1 \leq n \leq m-1$, such that $2\deg(\hat{r}_n) > \deg(F^2(\alpha - \hat{\alpha}))$, then the first $n+2$ partial quotients in the regular continued fraction expansions of α and $\hat{\alpha}$ are equal.*

Proof. Let $\alpha = [q_0, q_1, \ldots, q_m, \ldots]$ be the regular continued fraction expansion of α. The regular continued fraction expansion of $\hat{\alpha}$ is obviously $\hat{\alpha} = [\hat{q}_0, \hat{q}_1, \ldots, \hat{q}_m]$. Then $A_i/B_i = [q_0, q_1, \ldots, q_i]$ and $\hat{A}_i/\hat{B}_i = [\hat{q}_0, \hat{q}_1, \ldots, \hat{q}_i]$ are the i-th convergents of α and $\hat{\alpha}$, respectively. We wish to prove that $q_i = \hat{q}_i$ for $0 \leq i \leq n+1$.

Suppose n as in the statement exists. If $n = -1$, then $2\deg(\hat{r}_{-1}) = 2\deg(F) > \deg(F^2(\alpha-\hat{\alpha}))$ implies $\deg(\alpha-\hat{\alpha}) < 0$, so $q_0 = \lfloor\alpha\rfloor = \lfloor\hat{\alpha}\rfloor = \hat{q}_0$.

Assume now inductively that $2\deg(\hat{r}_{n-1}) > \deg(F^2(\alpha-\hat{\alpha}))$ implies $q_i = \hat{q}_i$ for $0 \le i \le n$ and suppose that $2\deg(\hat{r}_n) > \deg(F^2(\alpha-\hat{\alpha}))$. Since the r_i are decreasing in degree for $-1 \le i \le m$, we have $2\deg(\hat{r}_{n-1}) > 2\deg(\hat{r}_n) > \deg(F^2(\alpha-\hat{\alpha}))$, so $q_i = \hat{q}_i$ for $0 \le i \le n$ by induction hypothesis, and we only need to show $q_{n+1} = \hat{q}_{n+1}$.

A simple induction argument yields $\hat{r}_i = (-1)^{i-1}(\hat{A}_i F - \hat{B}_i E)$ for $-2 \le i \le m$, so by assumption and Eq. (2.4),

$$\deg(\alpha-\hat{\alpha}) < 2\deg\left(\frac{\hat{r}_n}{F}\right) = 2\deg(\hat{A}_n - \hat{B}_n\hat{\alpha}) \le -2\deg(\hat{B}_{n+1}) \ .$$

It follows again from Eq. (2.4) that

$$\deg\left(\alpha - \frac{\hat{A}_{n+1}}{\hat{B}_{n+1}}\right) \le \max\left\{\deg(\alpha-\hat{\alpha}), \deg\left(\hat{\alpha} - \frac{\hat{A}_{n+1}}{\hat{B}_{n+1}}\right)\right\} < -2\deg(\hat{B}_{n+1}) \ .$$

Since $\gcd(\hat{A}_{n+1}, \hat{B}_{n+1}) = 1$, Lemma 2.1 implies that $\hat{A}_{n+1}/\hat{B}_{n+1} = A_j/B_j$ for some $j \ge 0$. If $j < n+1$, then $[q_{j+1}, \ldots, q_{n+1}] = 0$ which is a contradiction. If $j > n+1$, then similarly $[\hat{q}_{n+2}, \ldots, \hat{q}_j] = 0$, again a contradiction. Thus, $\hat{A}_{n+1}/\hat{B}_{n+1} = A_{n+1}/B_{n+1}$, and hence $q_{n+1} = \hat{q}_{n+1}$. □

Let $E, F \in k[t]$ be non-zero, and assume that $\deg(E) > \deg(F)$. Consider again the regular continued fraction expansion of the rational function $E/F = [\hat{q}_0, \hat{q}_1, \ldots, \hat{q}_m]$, where $m \ge 0$ is again minimal with that property. Set $\hat{\phi}_0 = E/F$ and $\hat{\phi}_{i+1} = (\hat{\phi}_i - \hat{q}_i)^{-1}$, so $\hat{q}_i = \lfloor\hat{\phi}_i\rfloor$ for $i \ge 0$. This continued fraction expansion corresponds to the Euclidean algorithm applied to E and F. We define

$$\begin{array}{l} b_{-1} = E \ , b_0 = F \ , \quad b_{i+1} = b_{i-1} - \hat{q}_i b_i \ , \\ a_{-1} = 0 \ , \ a_0 = -1 \ , a_{i+1} = a_{i-1} - \hat{q}_i a_i \ , \end{array} \tag{2.5}$$

so $\hat{q}_i = \lfloor b_{i-1}/b_i\rfloor$, for $0 \le i \le m$. Then $\hat{q}_i$ and b_{i+1} are the quotients and remainders, respectively, when dividing b_{i-1} by b_i. We have

$$b_{i-1} = \hat{q}_i\, b_i \ + \ b_{i+1} \quad , \quad \deg(b_{i+1}) < \deg(b_i) \quad (-1 \le i \le m) \ , \tag{2.6}$$

and the b_i strictly decrease in degree for $-1 \le i \le m+1$. Then m is minimal such that $b_{m+1} = 0$, so $b_m = \gcd(E, F)$.

As before, denote by $\hat{A}_i/\hat{B}_i = [\hat{q}_0, \hat{q}_1, \ldots, \hat{q}_i]$ the i-th convergents of $\hat{\phi}_0$ for $0 \le i \le m$. The quantities $\hat{A}_i, \hat{B}_i$ can be computed recursively by

$$\begin{array}{l} \hat{A}_{-2} = 0, \ \hat{A}_{-1} = 1, \ \hat{A}_i = \hat{q}_i\hat{A}_{i-1} + \hat{A}_{i-2} \quad (0 \le i \le m) \ , \\ \hat{B}_{-2} = 1, \ \hat{B}_{-1} = 0, \ \hat{B}_i = \hat{q}_i\hat{B}_{i-1} + \hat{B}_{i-2} \quad (0 \le i \le m) \ . \end{array} \tag{2.7}$$

Then induction yields $a_i = (-1)^{i-1}\hat{A}_{i-1}$ for $-1 \le i \le m+1$; in particular, we see that the a_i increase in degree for $-1 \le i \le m+1$. We also obtain

$$b_{-1} = (-1)^i(a_{i-1}b_i - a_i b_{i-1}) \qquad (0 \le i \le m+1)\ . \tag{2.8}$$

We require the following basic degree properties later on:

Lemma 2.2.

(a) $\deg(b_i) = \deg(b_{i-1}) - \deg(\hat{q}_i) \le \deg(b_{i-1}) - 1 \qquad (0 \le i \le m)$.
(b) $\deg(a_i) = \deg(a_{i-1}) + \deg(\hat{q}_{i-1}) \ge \deg(a_{i-1}) + 1 \qquad (1 \le i \le m+1)$.
(c) $\deg(b_i) \le \deg(b_{-1}) - i - 1 \qquad (-1 \le i \le m+1)$.
(d) $\deg(a_i) \ge i \qquad (0 \le i \le m+1)$.
(e) $\deg(a_i) + \deg(b_{i-1}) = \deg(b_{-1}) \qquad (0 \le i \le m+1)$.

Proof. Since $\deg(\hat{q}_i) \ge 1$ for $0 \le i \le m$ by Eq. (2.6), (a) and (b) follow from Eq. (2.5). Parts (c) and (d) can then be obtained from (a) and (b), respectively, using induction. Finally, since $\deg(a_i b_{i-1}) > \deg(a_{i-1}b_i)$ by (a) and (b), (e) now follows from Eq. (2.8). □

3. Hyperelliptic Curves

We employ an algebraic framework of hyperelliptic curves based on the treatments of function fields given in [12], [17], and [4], as opposed to a more geometric treatment. Let k be a finite field of order q. Following [3], we define a *hyperelliptic function field of genus* $g \in \mathbb{N}$ to be a quadratic extension of genus g over the rational function field $k(u)$, and a *hyperelliptic curve of genus* g *over* k to be a plane, smooth[a], absolutely irreducible, affine curve C over k whose function field $k(C)$ is hyperelliptic of genus g. The curve C and its function field are called *imaginary*, *unusual*, or *real*, if the place at infinity of $k(u)$ is ramified, inert, or split in $k(C)$, respectively. Then C is of the form

$$C : v^2 + h(u)v = f(u)\ , \tag{3.1}$$

where $f, h \in k[u]$, $h = 0$ if k has odd characteristic, h is monic if k has even characteristic, and every irreducible factor in $k[u]$ of h is a simple factor of f; in particular, f is squarefree if k has odd characteristic. Then the function field of C is $k(C) = k(u, v)$ and its *maximal order* is the integral domain $k[C] = k[u, v]$, the coordinate ring of C over k. The different signatures at infinity can easily be distinguished as follows:

[a] A hyperelliptic curve does have singularities at infinity if it is not elliptic, i.e. $g \ge 2$

(1) C is imaginary if $\deg(f) = 2g+1$, and if $\deg(h) \leq g$ if k has characteristic 2;
(2) C is unusual if the following holds: if k has odd characteristic, then $\deg(f) = 2g+2$ and $\operatorname{sgn}(f)$ is a non-square in k, whereas if k has characteristic 2, then $\deg(h) = g+1$, $\deg(f) = 2g+2$ and the leading coefficient of f is not of the form e^2+e for any $e \in k^*$.
(3) C is real if the following holds: if k has odd characteristic, then $\deg(f) = 2g+2$ and $\operatorname{sgn}(f)$ is a square in k, whereas if k has characteristic 2, then $\deg(h) = g+1$, and either $\deg(f) \leq 2g+1$, or $\deg(f) = 2g+2$ and the leading coefficient of f is of the form e^2+e for some $e \in k^*$.

In some literature sources, unusual curves are counted among the imaginary ones, as there is a unique place in $k(C)$ lying above the place at infinity of $k(u)$ for both models. Note also that an unusual curve over k is real over a quadratic extension of k; whence the term "unusual".

It is well-known that the places of $k(u)$ are given by the monic irreducible polynomials in $k[u]$ together with the place at infinity of $k(u)$. Define S to be the set of places of $k(C)$ lying above the place at infinity of $k(u)$, and write $S = \{\infty\}$ if C is imaginary or unusual, and $S = \{\infty_1, \infty_2\}$ if C is real. Then the places of $k(C)$ are the prime ideals lying above the places of $k(u)$ (the *finite* places) together with the elements of S (the *infinite* places). To every place $\mathfrak{p}$ of $k(C)$ corresponds a normalized additive valuation $\nu_{\mathfrak{p}}$ on $k(C)$ and a discrete valuation ring $\mathcal{O}_{\mathfrak{p}} = \{\alpha \in k(C) \mid \nu_{\mathfrak{p}}(\alpha) \geq 0\}$; for brevity, we write $\nu_i = \nu_{\infty_i}$ $(i = 1, 2)$ if C is real. The *degree* $\deg(\mathfrak{p})$ of a place $\mathfrak{p}$ is the field extension degree $\deg(\mathfrak{p}) = [\mathcal{O}_{\mathfrak{p}}/\mathfrak{p} : k]$. Note that $\deg(\infty) = 1$ if C is imaginary, $\deg(\infty) = 2$ if C is unusual, and $\deg(\infty_1) = \deg(\infty_2) = 1$ if C is real. The *norm* of a finite place $\mathfrak{p}$ is the polynomial $N(\mathfrak{p}) = \mathfrak{P}^{\deg(\mathfrak{p})} \in k[u]$, where $\mathfrak{P}$ is the unique place of $k(u)$ lying below $\mathfrak{p}$.

For any place $\mathfrak{p}$ of $k(C)$, denote by $k(C)_{\mathfrak{p}}$ the completion of $k(C)$ with respect to $\mathfrak{p}$. Then it is easy to see that the completions $k(C)_S$ of $k(C)$ with respect to the places in S are, respectively,

$$k(C)_S = \begin{cases} k(C)_\infty = k\langle u^{-1/2}\rangle & \text{if } C \text{ is imaginary} , \\ k(C)_\infty = k'\langle u^{-1}\rangle & \text{if } C \text{ is unusual} , \\ k(C)_{\infty_1} = k(C)_{\infty_2} = k\langle u^{-1}\rangle & \text{if } C \text{ is real} , \end{cases}$$

where $k' = k(\operatorname{sgn}(v))$ is a quadratic extension of k. For C imaginary or unusual, the embedding of $k(C)$ into $k(C)_S$ is unique, whereas for the real case, we have two embeddings of $k(C)$ into $k\langle u^{-1}\rangle$. Here, we number the indices so that $\nu_1(v) \leq \nu_2(v)$, and choose the embedding with $\deg(\alpha) = -\nu_1(\alpha)$ for all $\alpha \in k(C)$.

To unify our discussion over all hyperelliptic models, we henceforth interpret elements in $k(C)$ as series in powers of u^{-1}, where in the imaginary case, the exponents of these powers are half integers. All degrees of function field elements are then taken with respect to u; more exactly, we set

$$\deg(\alpha) = \deg_u(\alpha) = \begin{cases} -\nu_\infty(\alpha)/2 & \text{if } C \text{ is imaginary} \quad , \\ -\nu_\infty(\alpha) & \text{if } C \text{ is unusual} \quad , \\ -\nu_1(\alpha) \;=\; -\nu_2(\overline{\alpha}) & \text{if } C \text{ is real} \quad , \end{cases}$$

for $\alpha \in k(C)$. Here, if $\alpha = a + bv \in k(C)$ with $a, b \in k(u)$, then $\overline{\alpha} = a - b(v + h)$ is the *conjugate* of α. Note that for imaginary curves, $\deg(\alpha)$ can be a half integer. The following properties are easily seen:

Lemma 3.1.

(a) If C is imaginary, then $\deg(v) = \deg(v + h) = g + 1/2$.
(b) If C is unusual or real with $\deg(f) = 2g+2$, *then* $\deg(v) = \deg(v+h) = g + 1$.
(c) If C is real and $\deg(f) \leq 2g+1$, *then* $\deg(v) = g+1$ *and* $\deg(v+h) = \deg(f) - (g + 1) \leq g$.

A *divisor*[b] is a formal sum $D = \sum_{\mathfrak{p}} \nu_{\mathfrak{p}}(D)\mathfrak{p}$ where $\mathfrak{p}$ runs through all the places of $k(C)$ and $\nu_{\mathfrak{p}}(D) = 0$ for all but finitely many places $\mathfrak{p}$. The *support* $\mathrm{supp}(D)$ of D is the set of places for which $\nu_{\mathfrak{p}}(D) \neq 0$, and the *degree* of D is $\deg(D) = \sum_{\mathfrak{p}} \nu_{\mathfrak{p}}(D) \deg(\mathfrak{p})$; this agrees with the notion of degree of a place. A divisor whose support is disjoint from S is a *finite* divisor. Every divisor D of $k(C)$ can be written uniquely as a sum of two divisors

$$D = D_S + D^S \quad \text{where } D_S \text{ is finite and } \mathrm{supp}(D) \subseteq S \quad .$$

The norm map extends naturally to all finite divisors D_S via $\mathbb{Z}$-linearity, and we can now define the norm of any divisor D to be $N(D) = N(D_S)$.

For two divisors D_1 and D_2 of $k(C)$, we write $D_1 \geq D_2$ if $\nu_{\mathfrak{p}}(D_1) \geq \nu_{\mathfrak{p}}(D_2)$ for all places $\mathfrak{p}$ of $k(C)$. With this notation, we see that $k[C]$ is the set of all $\alpha \in k(C)$ with $\mathrm{div}(\alpha)_S \geq 0$ and its unit group $k[C]^*$ consists of exactly those $\alpha \in k(C)$ with $\mathrm{div}(\alpha)_S = 0$.

[b] An equivalent geometric definition of a divisor (defined over k) that is frequently used in the literature on hyperelliptic curves is as follows: it is a formal sum $D = \sum_P \nu_P(D)P$ that is invariant under the Galois action of k, where P runs through all the points on C with coordinates in some algebraic closure of k. The degree of D is then simply $\sum_P \nu_P(D)$.

Let $\mathcal{D}$ denote the group of divisors of $k(C)$, $\mathcal{D}^0$ the subgroup of $\mathcal{D}$ of degree 0 divisors of $k(C)$, and $\mathcal{P}$ the subgroup of $\mathcal{D}^0$ of principal divisors of $k(C)$. Then the *degree 0 divisor class group* $\mathrm{Pic}^0 = \mathcal{D}^0/\mathcal{P}$ of $k(C)$ is a finite Abelian group whose order h is the *(degree 0 divisor) class number* of C.

Recall that the conjugation map on $k(C)$, arising from the hyperelliptic involution on C, maps each element $\alpha = a + bv \in k(C)$ with $a, b \in k(u)$ to $\overline{\alpha} = a - b(v + h)$. This map thus acts on all the finite places of $k(C)$ as well as on S via $\overline{\infty} = \infty$ if C is imaginary or unusual and $\overline{\infty}_1 = \infty_2$ if C is real. This action extends naturally to the groups $\mathcal{D}$, $\mathcal{D}^0$, $\mathcal{P}$, and hence to Pic^0. Note that $N(D) = N(\overline{D})$ and $D + \overline{D} = \mathrm{div}(N(D))$ for any degree 0 divisor D.

Define $\mathcal{D}_S = \{D_S \mid D \in \mathcal{D}\}$, $\mathcal{D}^S = \{D^S \mid D \in \mathcal{D}\}$, $\mathcal{P}_S = \mathcal{P} \cap \mathcal{D}_S$, and $\mathcal{P}^S = \mathcal{P} \cap \mathcal{D}^S$. By Proposition 14.1, p. 243, of [12], there are exact sequences

$$(0) \to k^* \to k[C]^* \to \mathcal{P}^S \to (0) \ , \tag{3.2}$$

$$(0) \to (\mathcal{D}^S \cap D^0)/\mathcal{P}^S \to \mathrm{Pic}^0 \to \mathcal{D}_S/\mathcal{P}_S \to \mathbb{Z}/f\mathbb{Z} \to (0) \ , \tag{3.3}$$

where $f = \gcd\{\deg(\mathfrak{p}) \mid \mathfrak{p} \in S\}$, so $f = 2$ if C is unusual and $f = 1$ otherwise. If C is imaginary or unusual, then $\mathcal{D}^S \cap D^0 = \mathcal{P}^S = 0$, whereas if C is real, then $\mathcal{D}^S \cap D^0 = \langle \infty_1 - \infty_2 \rangle$ and $\mathcal{P}^S = \langle R(\infty_1 - \infty_2) \rangle$, where R is the order of the divisor class of $\infty_1 - \infty_2$ in Pic^0 and is called the *regulator* of C. The principal divisor $R(\infty_1 - \infty_2)$ is the divisor of a fundamental unit of $k(C)$, i.e. a generator of the infinite cyclic group $k[C]^*/k^*$. For completeness, if C is imaginary or unusual, simply define the regulator of C to be $R = 1$.

A *fractional $k[C]$-ideal* is a subset $\mathfrak{f}$ of $k(C)$ such that $d\mathfrak{f}$ is a $k[C]$-ideal for some non-zero $d \in k[u]$. Let $\mathcal{I}$ denote the group of non-zero fractional $k[C]$-ideals, $\mathcal{H}$ the subgroup of $\mathcal{I}$ of non-zero principal fractional $k[C]$-ideals (which we write as (α) for $\alpha \in k(C)^*$), $\mathcal{C} = \mathcal{I}/\mathcal{H}$ the ideal class group of $k(C)$, and $h' = |\mathcal{C}|$ the ideal class number of $k(C)$. There is a natural isomorphism

$$\Phi : \mathcal{D}_S \to \mathcal{I}, \quad D_S \mapsto \{\alpha \in k(C)^* \mid \mathrm{div}(\alpha)_S \geq D_S\} \tag{3.4}$$

with inverse

$$\Phi^{-1} : \quad \mathcal{I} \to \mathcal{D}_S$$

$$\mathfrak{f} \mapsto D_S = \sum_{\mathfrak{p} \not\in S} m_{\mathfrak{p}} \mathfrak{p} \ \text{ where } m_{\mathfrak{p}} = \min\{\nu_{\mathfrak{p}}(\alpha) \mid \alpha \in \mathfrak{f} \text{ non-zero}\} \ .$$

The conjugate $\overline{\mathfrak{f}}$ of a fractional ideal $\mathfrak{f}$ is the image of $\mathfrak{f}$ under the conjugation map. If $\mathfrak{f}$ is non-zero, then the *norm* $N(\mathfrak{f})$ of $\mathfrak{f}$ is simply $N(\Phi^{-1}(\mathfrak{f}))$, the norm

of the finite divisor corresponding to $\mathfrak{f}$ under Φ^{-1}, with Φ given by Eq. (3.4). Note that $\mathfrak{f}\bar{\mathfrak{f}}$ is the principal fractional ideal generated by $N(\mathfrak{f})$.

The isomorphism Φ extends to an isomorphism from the factor group $\mathcal{D}_S/\mathcal{P}_S$ onto the ideal class group $\mathcal{C}$ (see p. 401 of [4] and Theorem 14.5, p. 247, of [12]). Thus, we have $h = Rh'/f$ by Eq. (3.3). The Hasse-Weil bounds $(\sqrt{q}-1)^{2g} \leq h \leq (\sqrt{q}+1)^{2g}$ imply $h \sim q^g$, and for real curves, we generally expect that h' is small and hence $R \approx h$. The isomorphism Φ in Eq. (3.4) can further be extended to the group $\mathcal{D}^0$, or a subgroup thereof, as follows.

3.1. *Imaginary Curves*

Since $\deg(\infty) = 1$ in this case, every degree 0 divisor of $k(C)$ can be written uniquely in the form $D = D_S - \deg(D_S)\infty$. Hence, every degree 0 divisor D is uniquely determined by D_S, and the isomorphism in Eq. (3.4) extends naturally to an isomorphism $\mathcal{D}^0 \to \mathcal{I}$.

3.2. *Unusual Curves*

Here, $\deg(\infty) = 2$, so every degree 0 divisor D of $k(C)$ can be written as $D = D_S - (\deg(D_S)/2)\infty$ and must have $\deg(D_S)$ even. Again, every degree 0 divisor D is uniquely determined by D_S. Thus, Φ as given in Eq. (3.4) extends to an isomorphism from $\mathcal{D}^0$ onto the group of fractional ideals whose norm have even degree.

3.3. *Real Curves*

If C is real, then $\deg(\infty_1) = \deg(\infty_2) = 1$, so every degree 0 divisor of $k(C)$ can be uniquely written in the form

$$D = D_S - \deg(D_S)\infty_2 + \nu_1(D)(\infty_1 - \infty_2) \ .$$

Hence, every degree 0 divisor D is uniquely determined by D_S and $\nu_1(D)$. Here, Φ extends to an isomorphism from the subgroup of $\mathcal{D}^0$ of degree 0 divisors D with $\nu_1(D) = 0$ onto $\mathcal{I}$.

We conclude this section with the observation that the choice of the transcendental element u determines the signature at infinity (ramified, inert, or split) and hence the set S of places lying above infinity. So the ideal class group $\mathcal{C}$, its order h', and the regulator R depend on the model of C (imaginary, unusual, or real), whereas the genus g, the divisor groups $\mathcal{D}$, $\mathcal{D}^0$ and $\mathcal{P}$, as well as the degree 0 divisor class group Pic^0 and its order h are model-independent.

4. Reduced Ideals and Divisors

Some of the material in this and the next section can be found in [2], [5], and [7]. As before, let $C : v^2 + h(u)v = f(u)$ be a hyperelliptic curve of genus g over a finite field k. The maximal order $k[C]$ of $k(C)$ is an integral domain and a $k[u]$-module of rank 2 with $k[u]$-basis $\{1, v\}$. The non-zero integral ideals in $k[C]$ are exactly the $k[u]$-modules of the form $\mathfrak{a} = k[u]\, SQ + k[u]\, S(P+v)$ where $P, Q, S \in k[u]$ and Q divides $f + hP - P^2$. Here, S and Q are unique up to factors in k^* and P is unique modulo Q. For brevity, write $\mathfrak{a} = S(Q, P)$. An ideal $\mathfrak{a} = S(Q, P)$ is *primitive* if $S \in k^*$, in which case we simply take $S = 1$ and write $\mathfrak{a} = (Q, P)$. A primitive ideal $\mathfrak{a}$ is *reduced* if $\deg Q \leq g$. The basis Q, P of a primitive ideal $\mathfrak{a} = (Q, P)$ is *adapted* if $\deg(P) < \deg(Q)$ and *reduced* if C is real and $\deg(P - h - v) < \deg(Q) < \deg(P + v)$; the latter is only possible if C is real. In practice, it is common to have reduced divisors given in adapted form for imaginary and unusual curves and in reduced (or possibly adapted) form for real curves.

A divisor D of $k(C)$ is *effective* if $D \geq 0$. An effective finite divisor D_S is *semi-reduced* [c] if there does not exist any subset $U \subseteq \mathrm{supp}(D_S)$ such that $\sum_{\mathfrak{p} \in U} \nu_{\mathfrak{p}}(D_S)\mathfrak{p}$ is the divisor of a polynomial in $k[u]$, and *reduced* if in addition $\deg(D_S) \leq g$. Under the isomorphism in Eq. (3.4), effective finite divisors of $k(C)$ map to integral $k[C]$-ideals, semi-reduced divisors to primitive ideals, and reduced divisors to reduced ideals. Analogous to the ideal notation, we write $D_S = (Q, P)$ for the semi-reduced divisor of $k(C)$ corresponding to the primitive $k[C]$-ideal $\mathfrak{a} = (Q, P)$ under Φ, and refer to the polynomials Q and P as a *basis* of D_S; note that $N(D_S) = N(\mathfrak{a}) = \mathrm{sgn}(Q)^{-1}Q$. It is easy to see that the conjugation map of $k(C)$ acts on semi-reduced and reduced divisors $D_S = (Q, P)$ via $\overline{D}_S = (Q, -P - h)$.

Up to now, we have only defined the notions of reduced and semi-reduced for finite divisors. We simply extend this notion to arbitrary degree 0 divisors of $k(C)$ by declaring a degree 0 divisor D to be (semi-)reduced if D_S is (semi-)reduced. We then say that a semi-reduced divisor D is in *adapted* or *reduced* form if D_S is given by an adapted or reduced basis, respectively.

We would like to represent degree 0 divisor classes via reduced divisors. In the imaginary case, this is well-known, but we repeat it briefly here for completeness; for the other two hyperelliptic curve models, it is less simple. In particular, for the unusual case, reduced divisors need not exist in some

[c] For geometric and ideal-independent definitions of the notions of semi-reduced and reduced divisors, see for example [2] or [5].

divisor classes, so we will have to allow divisors D with $\deg(D_S) = g + 1$ when representing elements in Pic^0. For simplicity, we will say that a degree 0 divisor D in a given class $\mathbf{C} \in \mathrm{Pic}^0$ has *minimal norm* if D is semi-reduced and $\deg(N(E)) \geq \deg(N(D))$ for every semi-reduced divisor $E \in \mathbf{C}$. We will see that if C is imaginary, unusual with g even, or real, then D will always be reduced, otherwise (C unusual and g odd), we have $\deg(N(D)) \leq g+1$.

4.1. *Imaginary Curves*

Here, it is well-known that reduced divisors are pairwise inequivalent (see [2]), and every degree 0 divisor class in Pic^0, and hence every ideal class in $\mathcal{C}$, has exactly one reduced representative.

4.2. *Unusual Curves*

Again, reduced degree 0 divisors are pairwise inequivalent, and every degree 0 divisor class contains at most one reduced divisor. Those classes that do not contain any reduced divisor contain exactly $q + 1$ pairwise equivalent semi-reduced divisors D with $\deg(D_S) = g+1$ (see p. 183 of [1]). Note that this can only occur if g is odd, so in this case, the norm of a reduced divisor must have degree $\leq g-1$. Hence if g is even, then in complete analogy to the imaginary case, every divisor class does in fact have a unique representative. In order to represent divisor classes without reduced divisors, i.e. with $q+1$ pairwise equivalent divisors of minimal norm of degree $g + 1$, for g odd, a fast equivalence test or a systematic efficient way to identity a distinguished divisor of minimal norm in a given degree 0 divisor class are required.

4.3. *Real Curves*

By Proposition 4.1 of [10], every degree 0 divisor class of $k(C)$ contains a unique[d] reduced divisor D such that $0 \leq \deg(D_S) + \nu_1(D) \leq g$, or equivalently, $-g \leq \nu_2(D) \leq 0$. Using these reduced representatives for arithmetic in Pic^0 is somewhat slower that for imaginary curves, so we concentrate instead on reduced divisors $D = D_S - \deg(D_S)\infty_2$ with $\nu_1(D) = 0$. By the Paulus-Rück result cited above, these divisors are pairwise inequivalent, so every degree 0 divisor class of $k(C)$ contains at most one such reduced divisor.

[d]The proposition as stated in [10] reads "$0 \leq \nu_1(D) \leq g - \deg(D_S)$". The correct statement is "$0 \leq \deg(D_S) + \nu_1(D) \leq g$".

Rather than examining degree 0 divisor classes, we now consider ideal classes of $k(C)$. Recall that the isomorphism Φ defined in Eq. (3.4) can be extend to an isomorphism from the set $\{D \in \mathcal{D}^0 \mid \nu_1(D) = 0\}$ onto $\mathcal{I}$. For any non-zero fractional ideal $\mathfrak{f}$, set $D(\mathfrak{f}) = \Phi^{-1}(\mathfrak{f})$ to be the divisor with no support at ∞_1 corresponding to $\mathfrak{f}$; note that $\mathfrak{f}$ is reduced if and only if $D(\mathfrak{f})$ is reduced. Let $\mathbf{C}$ be any ideal class of $k(C)$, and define the set

$$\mathcal{R}_{\mathbf{C}} = \{D(\mathfrak{a}) \mid \mathfrak{a} \in \mathbf{C} \text{ reduced}\} \ .$$

By our above remarks, all the divisors in $\mathcal{R}_{\mathbf{C}}$ are reduced and pairwise inequivalent even though the corresponding ideals are all equivalent. Since the basis polynomials of a reduced divisor or ideal have bounded degree, $\mathcal{R}_{\mathbf{C}}$ is a finite set.

We now fix any reduced ideal $\mathfrak{a} \in \mathbf{C}$; for example, if $\mathbf{C}$ is the principal ideal class, then we always chose $\mathfrak{a} = (1)$ to be the trivial ideal. Then for every $\mathfrak{b} \in \mathbf{C}$, there exists $\alpha \in k(C)^*$ with $\mathfrak{b} = (\alpha)\mathfrak{a}$; if $\mathfrak{a} = (1)$, then α is in fact a generator of $\mathfrak{b}$. By multiplying α with a suitable power of a fundamental unit of $k(C)$, or equivalently, adding a suitable multiple of $R(\infty_1 - \infty_2)$ to its divisor, we may assume that $-R < \nu_1(\alpha) \leq 0$, or equivalently, $0 \leq \deg(\alpha) < R$. Then we define the *distance* of the divisor $D(\mathfrak{b})$ (with respect to $D(\mathfrak{a})$) to be $\delta(D(\mathfrak{b})) = \deg(\alpha)$. It follows that the set $\mathcal{R}_{\mathbf{C}}$ is ordered by distance, and if we set $D_1 = D(\mathfrak{a})$ and $r_{\mathbf{C}} = |\mathcal{R}_{\mathbf{C}}|$, then we can write

$$\mathcal{R}_{\mathbf{C}} = \{D_1, D_2, \ldots, D_{r_{\mathbf{C}}}\}$$

and $\delta_i = \delta(D_i)$, with $0 = \delta_1 < \delta_2 < \cdots < \delta_{r_{\mathbf{C}}} < R$. The set $\mathcal{R}_{\mathbf{C}}$ is called the *infrastructure* of $\mathbf{C}$; we will motivate this term later on. Note that if $\mathbf{C}$ is the principal class and $\mathfrak{b} \in \mathbf{C}$, $D(\mathfrak{b})$ and $D(\overline{\mathfrak{b}})$ both belong to $\mathcal{R}_{\mathbf{C}}$, and $\delta(D(\overline{\mathfrak{b}})) = R + \deg(D(\mathfrak{b})_S) - \delta(D(\mathfrak{b}))$ if $\mathfrak{b}$ is nontrivial.

5. Reduction and Baby Steps

We continue to assume that we have a hyperelliptic curve C given by Eq. (3.1). Our goal is to develop a unified framework for reduction on all hyperelliptic curves. We begin with the standard approach for reduction on imaginary curves — which we however apply to any hyperelliptic curve — and then link this technique to the traditional continued fractions method for real curves.

Starting with polynomials R_0, S_0 such that $\deg(R_0) < \deg(S_0)$ and S_0

dividing $f + hR_0 - R_0^2$, $\deg(S_0)$ even if C is unusual, the recursion

$$S_{i+1} = \frac{f + hR_i - R_i^2}{S_i} \ , \quad R_{i+1} = h - R_i + \left\lfloor \frac{R_i - h}{S_{i+1}} \right\rfloor S_{i+1} \ , \tag{5.1}$$

produces a sequence of semi-reduced, pairwise equivalent divisors $E_i = (S_{i-1}, R_{i-1})$, $i \in \mathbb{N}$. To avoid the costly full division in the expression for S_{i+1}, we can rewrite Eq. (5.1) as follows. Given S_0 and R_0, generate S_1 and R_1 using Eq. (5.1) and $s_1 = \lfloor (R_0 - h)/S_1 \rfloor$. Then for $i \in \mathbb{N}$:

$$\begin{aligned} S_{i+1} &= S_{i-1} + s_i(R_{i-1} - R_i) \ , \quad s_{i+1} = \left\lfloor \frac{R_i - h}{S_{i+1}} \right\rfloor \ , \\ R_{i+1} &= h - R_i + s_{i+1}S_{i+1} \equiv h - R_i \pmod{S_{i+1}} \ . \end{aligned} \tag{5.2}$$

Note that s_{i+1} and R_{i+1} are simply obtained by applying the division algorithm, i.e. $R_i - h = s_{i+1}S_{i+1} + (-R_{i+1})$ and $\deg(-R_{i+1}) < \deg(S_{i+1})$. Similar to [2] and [15], we derive the following properties.

Lemma 5.1.

(a) $\deg(R_i) < \deg(S_i)$ *for all* $i \geq 0$, *so all the* E_i *are in adapted form.*
(b) If $\deg(S_i) \geq g + 2$, *then* $\deg(S_{i+1}) \leq \deg(S_i) - 2$.
(c) If $\deg(S_i) = g + 1$, *then* $\deg(S_{i+1}) \leq g$ *if* C *is imaginary and* $\deg(S_{i+1}) = g + 1$ *if* C *is unusual or real. Hence, unless* C *is real,* E_{i+2} *has minimal norm.*
(d) There is a minimal index j *such that* $\deg(S_j) \leq \deg(v) < \deg(S_{j-1})$, *so unless* C *is real,* E_{j+1} *is the first of divisor of minimal norm. We have* $j \leq \lceil (\deg(S_0) - g)/2 \rceil$ *if* $\deg(S_j) \leq g$ *and* $j \leq \lceil (\deg(S_0) - g - 1)/2 \rceil$ *if* $\deg(S_j) = g + 1$.
(e) If C *is unusual, then* $\deg(S_i)$ *is even for all* $i \geq 0$.

Proof. (a) is obvious from Eq. (5.1). Since $\deg(h) \leq g + 1$, Eq. (5.1) and (a) imply

$$\begin{aligned} \deg(S_{i+1}) &= \deg(f + hR_i - R_i^2) - \deg(S_i) \\ &\leq \max\{\deg(f), \deg(S_i) + g, 2\deg(S_i) - 2\} - \deg(S_i) \ , \end{aligned} \tag{5.3}$$

yielding (b) and (c). Now (d) can easily be derived from (b) and (c). To see (e), note that if $\deg(R_i) \geq g + 1$, then $\deg(S_i) \geq g + 2$, so by Eq. (5.3), $\deg(S_{i+1}) = 2\deg(R_i) - \deg(S_i)$ (note that by the assumptions on $\mathrm{sgn}(f)$, there can never be cancellation in the numerator of S_{i+1} in the case where $\deg(R_i) = g + 1$), and if $\deg(R_i) \leq g$, then $\deg(S_{i+1}) = 2g + 2 - \deg(S_i)$. In either case, $\deg(S_{i+1})$ has the same parity as $\deg(S_i)$, so (e) is obtained by induction, since $\deg(S_0)$ was assumed to be even if C is unusual. □

Suppose $\deg(S_j) \leq \deg(v) < \deg(S_{j-1})$ as in part (d) of Lemma 5.1. If C is imaginary, or C is unusual with $\deg(S_j) \leq g$, then E_{j+1} is the unique reduced divisor in the class of D_1. If C is unusual and $\deg(S_j) = g+1$, (g odd), then the other q semi-reduced divisors equivalent to E_{j+1} whose norm have degree $g+1$ can be obtained from E_{j+1} as follows (see also [1] for the case where q is odd).

Proposition 5.1. *Let C given by Eq. (3.1) be unusual of odd genus g and $E = (S, R)$ a semi-reduced divisor with $\deg(R) \leq \deg(S) = g+1$. Then the $q+1$ divisors in the divisor class of E whose norm have degree $g+1$ are given by E and $E_a = (S_a, R_a)$ for $a \in \mathbb{F}_q$ where*

$$R_a = h - R + aS, \quad S_a = \frac{f + hR_a - R_a^2}{S} \ . \tag{5.4}$$

Proof. Since $E_a = E + \mathrm{div}((R_a + v)/S)$ for all $a \in \mathbb{F}_q$, all E_a are equivalent to E. Furthermore, $\deg(R_a) \leq g+1$ and hence $\deg(S_a) = g+1$, since the conditions on $\mathrm{sgn}(f)$ prevent cancellation of leading terms in the numerator of S_a. So it only remains to show that E and and all the E_a are pairwise distinct. To that end, we prove that equality among any two of these $q+1$ divisors leads to a sequence of divisibility conditions that yield a singular point on C.

So fix $a \in \mathbb{F}_q$ and suppose that $E_a = E$ or $E_a = E_b$ for some $b \in \mathbb{F}_q \backslash \{a\}$. We first claim that

$$S_a \text{ and } S \text{ differ by a constant factor in } \mathbb{F}_q \ . \tag{5.5}$$

This is clear if $E_a = E$, so suppose $E_a = E_b$ with $b \in \mathbb{F}_q$, $b \neq a$. Then S_a and S_b differ by a constant factor, and $R_a \equiv R_b \pmod{S_a}$. By Eq. (5.4), $R_a \equiv R_b \pmod{S}$, so since $\deg(R_a - R_b) = \deg(S_a) = \deg(S) = g+1$, we see that S_a and S must also differ by a constant factor in $\mathbb{F}_q$.

Next, we claim that

$$S \ \text{ divides } \ 2R - h \ . \tag{5.6}$$

If $E_a = E$, then $R \equiv R_a \pmod{S}$. On the other hand, $R_a \equiv h - R \pmod{S}$ by Eq. (5.4), so $R \equiv h - R \pmod{S}$, proving Eq. (5.6). Suppose now that $E_a = E_b$ for some $b \in \mathbb{F}_q$ distinct from a. Then S_a and S_b differ by a constant factor, so by Eq. (5.5), both differ from S by a constant factor. Now a simple calculation yields $S_a - S_b = (a-b)(2R - h - (a+b)S)$. Since $a \neq b$ and S divides the left hand side of this equality, S must again divide $2R - h$.

Our next assertion is that

$$S^2 \ \text{ divides } \ f + hR - R^2 \ . \tag{5.7}$$

By Eq. (5.4) and Eq. (5.6), $R_a \equiv h - R \equiv R \pmod{S}$. Since $\deg(R_a - R) \leq g + 1 = \deg(S)$, there exists $c_a \in \mathbb{F}_q$ with $R_a = R + c_a S$. Substituting into Eq. (5.4) yields $SS_a = f + hR - R^2 + c_a S(h - 2R - c_a S)$. By Eq. (5.5), S^2 divides the left hand side of this equality. Invoking Eq. (5.6), we obtain Eq. (5.7).

Our fourth and final claim is that

$$S \ \text{ divides } \ f' + hR' \ , \tag{5.8}$$

where f' denotes the derivative of f with respect to u; similarly for R'. To prove this claim, we simply observe that taking derivatives in Eq. (5.7) implies that S divides $f' + h'R + hR' - 2RR' = f' + hR' + R'(h - 2R)$, so Eq. (5.8) now follows from Eq. (5.6).

Now let r be a root of S in some algebraic closure of k. Then Eq. (5.6)–Eq. (5.8) easily imply that $(r, -R(r))$ is a singular point on C, a contradiction. So no two among the divisors E and E_a ($a \in \mathbb{F}_q$) can be be equal, proving the proposition. □

We now relate Eq. (5.1) to a regular continued fraction expansion, which is the usual approach to reduction on real curves. Let $P, Q \in k[u]$ with Q non-zero and Q dividing $f + hP - P^2$, and let $s_0, s_1, \ldots$ be a sequence of polynomials in $k[u]$. Set $P_0 = P$, $Q_0 = Q$, and

$$P_{i+1} = h - P_i + s_i Q_i, \quad Q_{i+1} = \frac{f + hP_{i+1} - P_{i+1}^2}{Q_i} \ , \tag{5.9}$$

for $i \geq 0$. If we set $\phi_i = (P_i + v)/Q_i$, then $\phi_{i+1} = (\phi_i - s_i)^{-1}$, so $\phi_0 = [s_0, s_1, \ldots, s_i, \phi_{i+1}]$ for all $i \geq 0$. Thus, Eq. (5.9) determines a continued fraction expansion of ϕ_0 in the completion $k(C)_S$. It is clear that Eq. (5.9) defines a sequence $D_i = (Q_{i-1}, P_{i-1})$ of semi-reduced divisors with corresponding primitive ideals $\mathfrak{a}_i$. The operation $D_i \to D_{i+1}$ is referred to as a *baby* or *reduction step*[e].

Set $\theta_1 = 1$ and $\theta_i = \prod_{j=1}^{i-1} \phi_j^{-1}$ for $i \geq 2$. Since $\phi_i \overline{\phi}_i = -Q_{i-1}/Q_i$, it is easy to see that $Q_0 \theta_i \overline{\theta}_i = (-1)^{i-1} Q_{i-1}$. Thus

$$\overline{\theta}_i = \prod_{j=1}^{i-1} \overline{\phi}_j^{-1} = (-1)^{i-1} \frac{Q_{i-1}}{Q_0 \theta_i} = (-1)^{i-1} \frac{Q_{i-1}}{Q_0} \prod_{j=1}^{i-1} \phi_j \ . \tag{5.10}$$

[e]Note that Eq. (5.4) is a special case of Eq. (5.9), with $s_i = a \in \mathbb{F}_q$. However, in this case, the recursion only alternates between E and E_a.

Then $\mathfrak{a}_{i+1} = (\overline{\phi_i^{-1}})\mathfrak{a}_i$ and hence $\mathfrak{a}_i = (\overline{\theta}_i)\mathfrak{a}_1$, for $i \in \mathbb{N}$. Therefore, the ideals $\mathfrak{a}_i$ are all equivalent, so baby steps preserve ideal equivalence.

If we choose s_i in Eq. (5.9) to be $s_i = q_i = \lfloor \phi_i \rfloor$, i.e. the quotient in the regular continued fraction expansion of ϕ_0 in $k(C)_S$, then we have the baby steps

$$q_i = \left\lfloor \frac{P_i + v}{Q_i} \right\rfloor,\ P_{i+1} = h - P_i + q_i Q_i,\ Q_{i+1} = \frac{f + hP_{i+1} - P_{i+1}^2}{Q_i}\ . \quad (5.11)$$

If $\deg(Q_i) > \deg(v)$, then $q_i = \lfloor P_i/Q_i \rfloor$. It is now easy to deduce that if j is as in part (d) of Lemma 5.1 and S_i, R_i are defined as in Eq. (5.1), then

$$q_i = \lfloor P_i/Q_i \rfloor \in k[u], \quad P_{i+1} = h - R_i, \quad Q_{i+1} = S_{i+1}\ , \quad (5.12)$$

for $0 \leq i < j$. Therefore, for this range of indices, Eq. (5.11) is equivalent to Eq. (5.1) and hence produces the same sequence of divisors. For imaginary and unusual curves, we will only consider baby steps as in Eq. (5.11) in the range $0 \leq i < j$. For C real, baby steps as in Eq. (5.11) can be performed beyond that range as well. However, for $i \geq j$, $q_j \neq \lfloor P_j/Q_j \rfloor$, so Eq. (5.12) is false. Here, if we use Eq. (5.11) to compute the sequence $D_{i+1} = (Q_i, P_i)$, starting with $i = j$, then D_{i+1} is reduced for $i > j$. We have $\deg(P_{j+1} - h - v) \leq g$, $\deg(P_{j+1} + v) = g + 1$, and for $i \geq j + 2$, $D_{i+1} = (Q_i, P_i)$ is in reduced form.

We now see that for all hyperelliptic curves, there exists an index $l \geq 0$ such that Eq. (5.11) repeatedly applied to $D_1 = (Q_0, P_0)$ produces a reduced divisor D_{l+1}, if one exists, after $l \leq \lceil (\deg(Q_0) - g)/2 \rceil$ steps. If C is unusual, g is odd, and the class of D_1 contains no reduced divisor, then Eq. (5.11) produces a divisor D_{l+1} whose norm has degree $g+1$ after $l \leq \lceil (\deg(Q_0) - g - 1)/2 \rceil$ steps. In the imaginary and unusual scenarios, we have $l = j$ with j as in part (d) of Lemma 5.1; for C real, we have $l = j + 1$. For $0 \leq i < l$, Eq. (5.11) is equivalent to

$$\begin{aligned} q_i &= \left\lfloor \frac{P_i + e_i v}{Q_i} \right\rfloor\ , \quad e_i = \begin{cases} 1 \text{ if } C \text{ real, } \deg(Q_i) = g+1, \\ 0 \text{ otherwise,} \end{cases} \\ P_{i+1} &= h - P_i + q_i Q_i, \quad Q_{i+1} = \frac{f + hP_{i+1} - P_{i+1}^2}{Q_i}\ . \end{aligned} \quad (5.13)$$

Again, the recursion in Eq. (5.13) can be made more efficient for $i \geq 1$, i.e. for all but the first baby step. Given Q_0 and P_0, we compute Q_1 and P_1 using Eq. (5.13). Then for $i \in \mathbb{N}$:

$$\begin{aligned} q_i &= \left\lfloor \frac{P_i + \lfloor e_i v \rfloor}{Q_i} \right\rfloor\ , \quad r_i \equiv P_i + \lfloor e_i v \rfloor \pmod{Q_i}\ , \\ P_{i+1} &= h + \lfloor e_i v \rfloor - r_i\ , \quad Q_{i+1} = Q_{i-1} + q_i(r_i - r_{i-1})\ . \end{aligned} \quad (5.14)$$

As before, the first line in Eq. (5.14) is equivalent to applying the division algorithm in order to compute polynomials q_i and r_i such that $P_i + \lfloor e_i v \rfloor = q_i Q_i + r_i$ and $\deg(r_i) < \deg(Q_i)$.

Suppose now that C is real. If we repeatedly apply Eq. (5.11), or equivalently, Eq. (5.14), starting with a reduced divisor $D_1 = D(\mathfrak{a})$ for some reduced ideal $\mathfrak{a}$ of $k(C)$, then we can generate the entire infrastructure $\mathcal{R}_{\mathbf{C}} = \{D_i \mid 1 \leq i \leq r_{\mathbf{C}}\}$ of the ideal class $\mathbf{C}$ containing $\mathfrak{a}$. Here, $D_i = D(\mathfrak{a}_i)$ where $\mathfrak{a}_i = (\overline{\theta}_i)\mathfrak{a}$ with $\overline{\theta}_i$ as in Eq. (5.10), so the distance of D_i is $\delta_i = \deg(\overline{\theta}_i)$. In particular, $\overline{\theta}_{r_{\mathbf{C}}}$ is a fundamental unit of $k(C)$ of positive degree, and $\deg(\overline{\theta}_{r_{\mathbf{C}}}) = R$ is the regulator of $k(C)$.

We conclude this section by showing how to compute the distances $\delta_i = \delta(D_i)$. By Eq. (5.10), the distance satisfies

$$\delta_i = \deg(\overline{\theta}_i) = \deg(Q_{i-1}) - \deg(Q_0) + \sum_{j=1}^{i-1} \deg(q_j) \tag{5.15}$$

for $i \in \mathbb{N}$. Since $\overline{\phi}_i = (P_i - h - v)/Q_i = -Q_{i-1}/(P_i + v)$ and $\delta_{i+1} - \delta_i = -\deg(\overline{\phi}_i) = \deg(P_i + v) - \deg(Q_{i-1}) = g + 1 - \deg(Q_{i-1})$ by Eq. (5.10), we have $1 \leq \delta_{i+1} - \delta_i \leq g$ if D_i is non-zero, and $\delta_{i+1} = g + 1$ if $D_i = 0$, in which case $\mathbf{C}$ is the principal class.

6. Giant Steps and the Idea of NUCOMP

As before, let C be given by Eq. (3.1), and let $D' = (Q', P'), D" = (Q'', P'')$ be two semi-reduced divisors of $k(C)$. Then it is well-known that there exists a semi-reduced divisor $D = (Q, P)$ in the divisor class of the sum $D' + D''$ that can be computed as follows.

$$\begin{aligned} S &= \gcd(Q', Q'', P' + P'' - h) = VQ' + WQ'' + X(P' + P'' - h) \ , \\ Q &= \frac{Q'Q''}{S^2} \ , \\ P &= P'' + U\,\frac{Q''}{S} \ \text{ with } \ U \equiv W(P' - P'') + XR'' \pmod{Q'/S} \ , \end{aligned} \tag{6.1}$$

where $U, V, W, X \in k[u]$, $\deg(U) < \deg(Q'/S)$, and $R'' = (f + hP'' - P''^2)/Q''$. Note that D is in adapted form if $\deg(P'') < \deg(Q)$.

Since S tends to have very small degree (usually $S = 1$), we expect $\deg Q \approx \deg Q' + \deg Q''$; in particular, even if D' and D'' have minimal norm, then D will generally not have minimal norm. We now apply repeated baby steps as in Eq. (5.14) to $P_0 = P$ and $Q_0 = Q$ until we obtain a divisor of minimal norm. The first divisor thus obtained is defined to be $D' \oplus D''$. The operation $(D', D'') \to D' \oplus D''$ is called a *giant step*.

6.1. *Imaginary Curves*

Here, $D' \oplus D''$ is the unique reduced divisor in the class of $D' + D''$, and the algorithm above is Cantor's algorithm [2]. Thus, the group operation on Pic^0 can be performed efficiently via reduced representatives.

6.2. *Unusual Curves*

In this case, if g is even, then everything is completely analogous to the imaginary setting. However, if g is odd, then $D' \oplus D''$ may or may not be reduced, so the set of reduced divisors is no longer closed under the operation $\oplus$. However, as mentioned earlier, if we could either perform fast equivalence testing, or efficiently and systematically identify a distinguished divisor D with $\deg(D_S) = g+1$ in every divisor class that contains no reduced divisor, then we could perform arithmetic in Pic^0 via these distinguished representatives plus reduced representatives if they exist.

6.3. *Real Curves*

Suppose D' and D'' are reduced, and $D' \in \mathcal{R}_{\mathbf{C}'}$, $D'' \in \mathcal{R}_{\mathbf{C}''}$ for suitable ideal classes $\mathbf{C}', \mathbf{C}''$ of $k(C)$. Then $D' \oplus D'' \in \mathcal{R}_{\mathbf{C}'\mathbf{C}''}$. In particular, if $\mathbf{C}''$ is the principal ideal class, then $D' \oplus D'' \in \mathcal{R}_{\mathbf{C}'}$, and we have

$$\delta(D' \oplus D'') = \delta(D') + \delta(D'') - \delta \quad \text{with} \quad 0 \le \delta \le 2g \ . \tag{6.2}$$

Here, distances in the principal class are taken with respect to $D_1 = 0$, and distances in $\mathbf{C}'$ with respect to some some suitable first divisor. The "error term" δ in Eq. (6.2) is linear in g and hence very small compared to the two distances $\delta(D')$ and $\delta(D'')$. The quantity δ in Eq. (6.2) can be efficiently computed as part of the giant step.

Suppose now that $D' = (Q', P')$ and $D'' = (Q'', P'')$ are two divisors of minimal norm. A giant step as described above finds the divisor $D' \oplus D''$ in two steps. First set $D_1 = (Q, P)$ with P and Q given by Eq. (6.1); Q and P have degree approximately $2g$, i.e. double size. Then apply repeated baby steps as in Eq. (5.14) to D_1 until the first divisor $D_{l+1} = D' \oplus D''$ of minimal norm is obtained; by Lemma 5.1, we have $l \le \lceil g/2 \rceil$ for all three curve models, so this takes at most $\lceil g/2 \rceil$ such steps. The reduction process produces a sequence of semi-reduced divisors $D_{i+1} = (Q_i, P_i)$, $0 \le i \le l$, via the continued fraction expansion of $\phi = (P+v)/Q = [q_0, q_1, \ldots, q_l, \phi_{l+1}]$. It slowly shrinks the degrees of the Q_i and P_i again to original size, reducing them by about 2 in each step by Lemma 5.1. The obvious disadvantage

of this method is that the polynomials Q_i, P_i have large degree while i is small, and are costly to compute.

NUCOMP is an algorithm for computing $D' \oplus D''$ that eliminates these costly baby steps on large operands. The idea of NUCOMP is to perform arithmetic on polynomials of much smaller degree. Instead of computing Q as well as the Q_i and P_i explicitly via the continued fraction expansion of ϕ, one computes sequences of polynomials a_i, b_i, c_i, and d_i such that

$$\begin{aligned} Q_i &= (-1)^i(b_{i-1}c_{i-1} - a_{i-1}d_{i-1}) \\ P_i &= (-1)^i(b_{i-2}c_{i-1} - a_{i-1}d_{i-2}) + P'' \ . \end{aligned}$$

Only two basis coefficients Q_{n+2} and P_{n+2} are evaluated at the end in order to obtain a divisor D_{n+3}. Here, the value of n is determined by the property that a_n, b_n, c_n, and d_n have approximately equal degree of about $g/2$. More exactly, we will have $l = n + 2$ or $n + 3$, i.e. $D' \oplus D'' = D_{n+3}$ or D_{n+4}.

The key observation is that $\hat{\phi} = U/(Q'/S)$, with U as given in Eq. (6.1), is a very good rational approximation of $\phi = (P+v)/Q$, and that the continued fraction expansion of $\hat{\phi}^{-1}$ is given by $Q'/(SU) = [q_1, q_2, \ldots, q_{n+1}, \ldots]$. Note that $\deg(U) < \deg(Q'/S) \leq g$ (or possibly $g+1$), so all quantities involved are of small degree. The polynomials a_i, b_i, c_i, and d_i are computed recursively along with the continued fraction expansion of $Q'/(SU)$ which is basically the extended Euclidean algorithm applied to Q'/S and U; in fact, the b_i are the remainders obtained in this Euclidean division process. Alternatively, only the a_i and b_i are computed recursively, and c_{n-1}, d_{n-1}, and d_n are then obtained from these two sequences; this approach turns out to employ polynomials of smaller degree (as c_0 and d_0 have large degree), but requires an extra full division by Q'/S. We describe the details of NUCOMP in the next two sections.

7. NUCOMP

Let $D' = (Q', P')$ and $D'' = (Q'', P'')$ be two divisors of minimal norm, and let P, Q, S, U be defined as in Eq. (6.1). We assume that

$$\deg(P'') \leq g + 1 < \deg(Q) \ . \tag{7.1}$$

The first inequality in Eq. (7.1) is equivalent to $\deg(P'' + v) \leq g + 1$, and holds if D'' is given in adapted or reduced form. While it can always be achieved by reducing P modulo Q, for example, we will see that this will generally not be necessary, i.e. usually NUCOMP outputs a divisor

$\hat{D} = (\hat{Q}, \hat{P})$ that again satisfies[f] $\deg(\hat{P}) \leq g+1$.

The second inequality in Eq. (7.1) is no great restriction, since if $\deg(Q) \leq g+1$, then $D = (Q, P)$ is at most one baby step away from having minimal norm, so one would simply compute $D' \oplus D''$ using one of the recursions in Section 5 and not use NUCOMP in this case. We now define

$$M = \max\{g\,, \deg(P'' + v)\} \in \frac{1}{2}\,\mathbb{Z}\ . \tag{7.2}$$

Note that $M \in \{g+1/2, g+1\}$ if C is imaginary, $M = \deg(P''+v) = g+1$ if C is unusual (since $\mathrm{sgn}(P'') \in k$ and $\mathrm{sgn}(v) \notin k$ can never cancel each other), and $M \in \{g, g+1\}$ if C is real. Furthermore, if D'' is given in adapted or reduced form, then $M = \deg(P''+v)$.

The quantity

$$N = \frac{1}{2}(\deg(Q') - \deg(Q'') + M) \in \frac{1}{4}\,\mathbb{Z} \tag{7.3}$$

will play a crucial role in our discussion. Since D'' is of minimal norm, we have $\deg(Q'') \leq M$ for all hyperelliptic curve models, so $N \geq \deg(Q')/2 > 0$. Furthermore, $N < \deg(Q'/S)$ by the second inequality in Eq. (7.1), so $N < g+1$. Usually, we expect N to be of magnitude $g/2$.

Let $Q'/SU = [\hat{q}_0, \hat{q}_1, \ldots, \hat{q}_m]$ be the regular continued fraction expansion of Q'/SU, where as usual, $m \geq 0$ is minimal. Setting $E = Q'/S$ and $F = U$, Eq. (2.5) defines sequences a_i, b_i for $-1 \leq i \leq m$, i.e.

$$\begin{array}{l} b_{-1} = Q'/S\ ,\, b_0 = U\ ,\quad b_{i+1} = b_{i-1} - \hat{q}_i b_i\ , \\ a_{-1} = 0\ ,\qquad a_0 = -1\ ,\, a_{i+1} = a_{i-1} - \hat{q}_i a_i\ . \end{array} \tag{7.4}$$

If we put $b_{-2} = U$ and $\hat{q}_{-1} = 0$, then for $i \geq -1$, the remainder sequence of the Euclidean algorithm applied to $\hat{\phi} = SU/Q'$ is the same as the one applied to $\hat{\phi}^{-1} = Q'/SU$ since $\deg(U) < \deg(Q'/S)$. The first step then simply reads $U = b_{-2} = 0 \cdot b_{-1} + b_0$. Since $Q'/SU = [\hat{q}_0, \hat{q}_1, \ldots, \hat{q}_m]$, we then see that the continued fraction expansion of $\hat{\phi}$ is $\hat{\phi} = [0, \hat{q}_0, \hat{q}_1, \ldots, \hat{q}_m]$.

Set $\hat{P}_0 = P$, $\hat{Q}_0 = Q$, and recall that $\hat{q}_{-1} = 0$. We investigate the sequence of semi-reduced divisors $\hat{D}_i = (\hat{Q}_{i-1}, \hat{P}_{i-1})$, $1 \leq i \leq m+3$, obtained by choosing $s_i = \hat{q}_{i-1}$ in Eq. (5.9). That is

$$\hat{P}_{i+1} = h - \hat{P}_i + \hat{q}_{i-1}\hat{Q}_i, \quad \hat{Q}_{i+1} = \frac{f + h\hat{P}_{i+1} - \hat{P}_{i+1}^2}{\hat{Q}_i}\ , \tag{7.5}$$

[f] If C is unusual, g is odd, and $\deg(\hat{Q}) = g+1$, then we expect $\deg(\hat{P}) \leq g+2$. However, in this situation, it suffices to assume $\deg(P'') \leq g+2$ as well. In order to avoid having to distinguish between too many different cases, we will henceforth ignore this scenario.

for $0 \leq i \leq m+1$. To facilitate the computation of $\hat{P}_i, \hat{Q}_i$, we proceed as in [8] and introduce two more sequences of polynomials c_i, d_i, $-1 \leq i \leq m+1$ as follows.

$$\begin{aligned} &c_{-1} = \frac{Q''}{S}, \qquad c_0 = \frac{P - P'}{b_{-1}}, \qquad c_{i+1} = c_{i-1} - \hat{q}_i c_i, \\ &d_{-1} = P' + P'' - h,\ d_0 = \frac{d_{-1} b_0 - S R''}{b_{-1}},\ d_{i+1} = d_{i-1} - \hat{q}_i d_i, \end{aligned} \tag{7.6}$$

for $0 \leq i \leq m$. We point out an interesting symmetry between the sequences b_i and c_i, $-1 \leq i \leq m+1$; namely, reversing the roles of D' and D'' in Eq. (6.1) results in a swap of these two sequences. An easy induction yields

$$c_i = \frac{1}{b_{-1}} \left(b_i \frac{Q''}{S} + a_i (P' - P'') \right) \ , \tag{7.7}$$

$$d_i = \frac{1}{b_{-1}} \left(b_i (P' + P'' - h) + a_i S R'' \right) \ , \tag{7.8}$$

for $-1 \leq i \leq m+1$. Using induction simultaneously on both formulas, we obtain

$$\hat{Q}_i = (-1)^i (b_{i-1} c_{i-1} - a_{i-1} d_{i-1}) \ , \tag{7.9}$$

$$\hat{P}_i = (-1)^i (b_{i-2} c_{i-1} - a_{i-1} d_{i-2}) + P'' \ , \tag{7.10}$$

for $0 \leq i \leq m+2$.

As outlined above, we wish to determine a point up to which the divisors $D_{i+1} = (Q_i, P_i)$ with $P_0 = P$, $Q_0 = Q$, and P_i, Q_i given by Eq. (5.13) or equivalently, by Eq. (5.11) or Eq. (5.14) are identical to the divisors $\hat{D}_{i+1} = (\hat{Q}_i, \hat{P}_i)$ with $\hat{P}_i, \hat{Q}_i$ given by Eq. (7.5) or equivalently, by Eq. (7.9) and Eq. (7.10). Clearly, $\hat{D}_1 = D_1$ by definition, so our goal is to find a maximal index $n \geq -1$ that guarantees $Q_i = \hat{Q}_i$ and $P_i = \hat{P}_i$, and hence $D_{i+1} = \hat{D}_{i+1}$, for $0 \leq i \leq n+2$ (see Theorem 7.1). Such an index will have to satisfy $n \leq m$ to ensure that the polynomials $\hat{Q}_i, \hat{P}_i$ as given in Eq. (7.5) are in fact defined. Our next task will then be to see how many baby steps if any we need to apply to the last divisor $D_{n+3} = (Q_{n+2}, P_{n+2})$ to obtain the divisor $D' \oplus D''$.

Theorem 7.1. *Let $D' = (Q', P')$, $D'' = (Q'', P'')$ be two divisors, and let P and Q be given by Eq. (6.1). Set $P_0 = \hat{P}_0 = P$, $Q_0 = \hat{Q}_0 = Q$, and define P_i, Q_i ($i \in \mathbb{N}$) by Eq. (5.11), $\hat{P}_i, \hat{Q}_i$ ($1 \leq i \leq m+2$) by Eq. (7.5), and b_i ($-1 \leq i \leq m+1$) by Eq. (7.4). Then there exists $n \in \mathbb{Z}$, $-1 \leq n \leq m$, such*

that $\deg(b_n) > N$, *with* N *as in Eq. (7.3). Furthermore,*

$$\begin{aligned} q_i &= \hat{q}_{i-1} \quad (0 \le i \le n+1) \ , \\ P_i &= \hat{P}_i \quad (0 \le i \le n+2) \ , \\ Q_i &= \hat{Q}_i \quad (0 \le i \le n+2) \ . \end{aligned}$$

Proof. We already observed that $\deg(b_{-1}) = \deg(Q'/S) > N$, so since $\deg(b_i)$ decreases as i increases, there must exist $n \ge -1$ with $\deg(b_n) > N$. Since $\deg(b_{m+1}) = -\infty < N$, we must have $n \le m$. So n as specified above exists and all the quantities $\hat{q}_{i-1}, \hat{P}_i, \hat{Q}_i$ above are in fact well-defined.

Set $\phi = (P+v)/Q$ and $\hat{\phi} = SU/Q'$. Then $\phi = [q_0, q_1, \ldots]$ with $q_i = (P_i + v)/Q_i$ is the continued fraction expansion of ϕ in a suitable field of Puiseux series; also, recall that $\hat{\phi} = [\hat{q}_{-1}, \hat{q}_0, \ldots, \hat{q}_m]$ where $\hat{q}_{-1} = 0$. We wish to apply[g] Theorem 2.1 to ϕ and $\hat{\phi}$. Since $\phi - \hat{\phi} = (P'' + v)/Q$, we have $b_{-1}^2(\phi - \hat{\phi}) = Q'(P'' + v)/Q''$. The definition of N implies $2N \ge \deg(Q'(P'' + v)/Q'')$, so

$$2\deg(b_n) > 2N \ge \deg\left(b_{-1}^2(\phi - \hat{\phi})\right) \ . \tag{7.11}$$

Set[h] $\hat{r}_{-2} = U$, $\hat{r}_{-1} = Q'/S$, and $\hat{r}_i = \hat{r}_{i-2} - \hat{q}_{i-1}\hat{r}_{i-1}$ for $0 \le i \le m+1$. Then $\hat{r}_i = b_i$ for $-1 \le i \le m+1$, so the $\hat{r}_i$ are the remainders when applying the Euclidean algorithm to $E = U$ and $F = Q'/S$. By Theorem 2.1, Eq. (7.11) implies that $q_i = \hat{q}_{i-1}$ for $0 \le i \le n+1$. Now $P_0 = \hat{P}_0$, $Q_0 = \hat{Q}_0$, and inductively by Eq. (5.11) and Eq. (7.5),

$$\begin{aligned} P_{i+1} &= h - P_i + q_i Q_i = h - \hat{P}_i + \hat{q}_{i-1}\hat{Q}_i = \hat{P}_{i+1} \ , \\ Q_{i+1} &= \frac{f + hP_{i+1} - P_{i+1}^2}{Q_i} = \frac{f + h\hat{P}_{i+1} - \hat{P}_{i+1}^2}{\hat{Q}_i} = \hat{Q}_{i+1} \ , \end{aligned}$$

for $0 \le i \le n+1$. □

Corollary 7.1. *With the notation of Theorem 7.1, we have* $D_i = \hat{D}_i$ *for* $1 \le i \le n+3$.

[g] Although the degrees in Theorem 2.1 are taken with respect to $u^{1/2}$ if C is imaginary, the statement still holds if degrees are taken with respect to u as is done here, since this only changes both sides of the degree inequality in Theorem 2.1 by a factor of 2.

[h] Note that the indices of the partial quotients $\hat{q}_i$ in the definition of the $\hat{r}_i$ are offset by 1 compared to the proof of Theorem 2.1 because here, the continued fraction in question is $\hat{\phi} = [\hat{q}_{-1}, \hat{q}_0, \hat{q}_1, \ldots, \hat{q}_m]$ (with $\hat{q}_{-1} = 0$), whereas in Theorem 2.1, it is $\hat{\phi} = [\hat{q}_0, \hat{q}_1, \ldots, \hat{q}_m]$.

Since $\deg(b_i)$ is a decreasing sequence for $-1 \leq i \leq m+1$, there exists a unique index n with $-1 \leq n \leq m$ such that

$$\deg(b_n) > N \geq \deg(b_{n+1}) \ , \tag{7.12}$$

with N as in Eq. (7.3). By Corollary 7.1, $D_i = \hat{D}_i$ for $1 \leq i \leq n+3$.

8. Giant Steps With NUCOMP

We now show that D_{n+3} is at most one baby step away from being reduced if C is imaginary or real, and always has minimal norm if C is unusual. Furthermore, D_{n+2} never has minimal norm. Note that this implies that if D_{n+3} actually has minimal norm, then $D_{n+3} = D' \oplus D''$.

Substituting Eq. (7.7) and Eq. (7.8) into Eq. (7.9) yields

$$\hat{Q}_i = \frac{(-1)^i}{b_{-1}} \left(\frac{Q''}{S} b_{i-1}^2 + (h - 2P'')a_{i-1}b_{i-1} - SR''a_{i-1}^2 \right) \tag{8.1}$$

for $0 \leq i \leq m+2$. For brevity, we define sequences of rational functions u_i, v_i, w_i via

$$u_i = \frac{Q''}{b_{-1}S} b_i^2 \ , \quad v_i = \frac{h - 2P''}{b_{-1}} a_i b_i \ , \quad w_i = \frac{SR''}{b_{-1}} a_i^2 \ , \tag{8.2}$$

for $-1 \leq i \leq m+1$, where as before, $R'' = (f + hP'' - P''^2)/Q''$. Then

$$(-1)^{i+1}\hat{Q}_{i+1} = u_i + v_i + w_i \qquad (1 \leq i \leq m+1) \ . \tag{8.3}$$

Note that u_i decreases and w_i increases in degree as i increases. Furthermore, u_i, v_i, w_i satisfy the following properties:

Lemma 8.1. *Let N and n be given by Eq. (7.3) and Eq. (7.12), respectively, and define*

$$\begin{aligned} L = \deg(Q''R'') &= \deg(f + hP'' - P''^2) \\ &= \deg(P'' + v) + \deg(P'' - h - v) \ . \end{aligned} \tag{8.4}$$

Then we have the following:

(a) $\deg(v_i) \leq g$ *for* $-1 \leq i \leq m+1$.
(b) $\deg(w_i) = L - \deg(u_{i-1})$ *for* $0 \leq i \leq m+1$.
(c) $\deg(u_{n+1}) \leq M < \deg(u_i)$ *for* $-1 \leq i \leq n$.
(d) $\deg(w_i) \leq \deg(P'' - h - v) - 1 \leq g$ *for* $-1 \leq i \leq n+1$.

Proof. Since $\deg(h - 2P'') \leq g + 1$, (a) can be derived using Lemma 2.2 (e) and (b), since

$$\begin{aligned}\deg(v_i) &= \deg(a_i) + \deg(b_i) + \deg(h - 2P'') - \deg(b_{-1}) \\ &= \deg(a_i) - \deg(a_{i+1}) + \deg(h - 2P'') \leq -1 + (g + 1) = g\end{aligned}$$

for $0 \leq i \leq m + 1$. The definition of u_{i-1} as well as Eq. (8.4) and part (e) of Lemma 2.2 imply

$$\begin{aligned}\deg(w_i) &= 2\deg(a_i) + \deg(S) + \deg(R'') - \deg(b_{-1}) \\ &= \deg(b_{-1}) - 2\deg(b_{i-1}) + \deg(S) + L - \deg(Q'') \\ &= L - \deg(u_{i-1})\end{aligned}$$

for $0 \leq i \leq m + 1$, whence follows (b). For (c), we note that

$$\begin{aligned}\deg(u_i) &= 2\deg(b_i) + \deg(Q''/S) - \deg(b_{-1}) \\ &= \deg(Q''/Q') + 2\deg(b_i) \\ &= M - 2N + 2\deg(b_i)\end{aligned}$$

for $-1 \leq i \leq m+1$. We then see from Eq. (7.2) and Eq. (7.3) that $\deg(u_i) \leq M$ if and only if $\deg(b_i) \leq N$. Part (c) now follows from Eq. (7.12). For (d), we note that $\deg(w_{-1}) = -\infty$, and for $0 \leq i \leq n + 1$, by Eq. (8.4), Eq. (7.2), and parts (b) and (c),

$$\begin{aligned}\deg(w_i) &= L - \deg(u_{i-1}) < L - M \\ &\leq L - \deg(P'' + v) = \deg(P'' - h - v) \ .\end{aligned}$$ □

Corollary 8.1. *Let N and n be given by Eq. (7.3) and Eq. (7.12), respectively. Then the following holds.*

(a) $\deg(Q_{i+1}) = \deg(u_i) \geq g + 2$ *for* $-1 \leq i \leq n$.
(b) $\deg(Q_{n+2}) \leq M + 1 \leq g + 1$.
(c) $\deg(Q_{n+2}) \leq g$ *if and only if* $\deg(b_{n+1}) < N$ *or* $M < g + 1$.

Proof. Parts (a) and (b) immediately follow from Eq. (8.3) as well as parts (a), (c), and (d) of Lemma 8.1. For part (c) of the Corollary, note that $\deg(u_{n+1}) = M - 2(N - \deg(b_{n+1}))$, so $\deg(Q_{n+2}) = g + 1$ if and only if $\deg(u_{n+1}) = g + 1$, which in turn holds if and only if $\deg(b_{n+1}) = N$ and $M = g + 1$. □

We now determine how to obtain the divisor $D' \oplus D''$ using NUCOMP. First, we recall that Eq. (7.5), or equivalently, Eq. (7.10) and Eq. (7.9), define a sequence of divisors $\hat{D}_{i+1} = (\hat{Q}_i, \hat{P}_i)$ for $0 \leq i \leq n + 2$. If C

is imaginary or real and $\deg(\hat{Q}_{n+2}) = g+1$, then we define the divisor $D_{n+4} = (Q_{n+3}, P_{n+3})$ where

$$\begin{aligned} q_{n+2} &= \left\lfloor \frac{\hat{P}_{n+2} + e_{n+2}v}{\hat{Q}_{n+2}} \right\rfloor \text{ with } e_{n+2} = \begin{cases} 1 \text{ if } C \text{ is real} \\ 0 \text{ if } C \text{ is imaginary} \end{cases}, \\ P_{n+3} &= h - \hat{P}_{n+2} + q_{n+2}\hat{Q}_{n+2}, \quad Q_{n+3} = \frac{f + hP_{n+3} - P_{n+3}^2}{\hat{Q}_{n+2}} . \end{aligned} \tag{8.5}$$

so P_{n+3} and Q_{n+3} are obtained by applying Eq. (5.13) to $P_{n+2} = \hat{P}_{n+2}$ and $Q_{n+2} = \hat{Q}_{n+2}$. For brevity, we define the integer

$$K = \deg(Q'') + \deg(Q') - g \ . \tag{8.6}$$

Then we can determine $D' \oplus D''$ as follows.

Proposition 8.1. *Let N, n, and K be given by Eq. (7.3), Eq. (7.12), and Eq. (8.6), respectively. Then the following holds.*

(a) If C is unusual, then $D' \oplus D'' = D_{n+3}$.
(b) If C is imaginary or real and $\deg(P''+v) < g+1$, then $D' \oplus D'' = \hat{D}_{n+3}$.
(c) If C is imaginary or real and $\deg(P''+v) = g+1$, then $D' \oplus D'' = \hat{D}_{n+3}$ if K is even. If K is odd, then $D' \oplus D'' = D_{n+3}$ and only if $\deg(Q_{n+2}) \le g$, or equivalently, $\deg(b_{n+1}) < N$, otherwise $D' \oplus D'' = D_{n+4}$.

Proof. Note that $\deg(P''+v) < g+1$ if and only if $M < g+1$, and $\deg(P''+v) = g+1$ if and only if $M = g+1$. We now use the definition of $D' \oplus D''$ and invoke Corollary 7.1. Then parts (a) and (b) follow immediately from parts (a) and (c) of Corollary 8.1, respectively. For part (c) of the Proposition, we have $M = \deg(P''+v) = g+1$, so $D' \oplus D'' = D_{n+3}$ if and only if $\deg(Q_{n+2}) \le g$, which by part (c) of Corollary 8.1 holds if and only if $\deg(b_{n+1}) < N$. Now if K is even, then $2N = K + 1 + 2(g - \deg(Q''))$ is an integer and odd, and $2\deg(b_n)$ is even, so we must have $\deg(b_{n+1}) < N$. If K is odd and $\deg(Q_{n+2}) = g+1$, then D_{n+3} is not reduced, so it suffices to prove that D_{n+4} is reduced.

To that end, note that by Eq. (8.5), $\deg(P_{n+3} - h - e_{n+2}v) < \deg(Q_{n+2}) = g+1$. If C is imaginary, then this implies $\deg(P_{n+3}) \le g$, whereas if C is real, then $\deg(P_{n+3} - h - v) \le g$. In either case, $\deg(Q_{n+3}) \le 2g + 1 - \deg(Q_{n+2}) = g$ by Eq. (8.5), so D_{n+4} is reduced. □

Remark 8.1. We note that if C is imaginary or real, $\deg(P''+v) = g+1$, and K as given in Eq. (8.6) is odd, then we will almost always have

$D' \oplus D'' = D_{n+4}$, i.e. it is very unlikely that D_{n+3} is reduced. In fact, under these conditions, if D_{n+3} is reduced, then it is easy to show that $\deg(b_{n+1}) \leq N-1$ and $\deg(b_n) \geq N+1$, so

$$\deg(b_n) - \deg(b_{n+1}) \geq 2 \ . \tag{8.7}$$

If $b_{n+1} = 0$, then $b_n = \gcd(Q'/S, U)$, so Eq. (8.7) would imply that Q'/S and U have a non-trivial common factor which is highly unlikely. If $b_{n+1} \neq 0$, then Eq. (8.7) implies $\deg(\hat{q}_{n+1}) \geq 2$. But all but the first partial quotient in a regular continued fraction expansion are expected to have degree 1 with very high probability.

To compute the relative distance $\delta = \delta(D') + \delta(D'') - \delta(D' \oplus D'')$ using NUCOMP in the case where C is real, let $\mathfrak{a}$, $\mathfrak{a}'$, $\mathfrak{a}''$ be the reduced ideals corresponding to the divisors $D' \oplus D''$, D', D'', respectively. Then $\mathfrak{a} = (S/\overline{\theta})\mathfrak{a}'\mathfrak{a}''$ where $\overline{\theta} = \overline{\theta}_i$ with $\mathfrak{a}_1 = \mathfrak{a}'\mathfrak{a}''$, $\mathfrak{a}_i = \mathfrak{a}$, and $i = n+3$ or $n+4$ by Proposition 8.1. Setting $d = \deg(S) - \deg(\overline{\theta}_{n+3})$, we obtain by Eq. (5.10), Eq. (6.1), and Theorem 7.1,

$$\begin{aligned} d &= \deg(S) - \left(\deg(Q_{n+2}) - \deg(Q_0) + \sum_{j=1}^{n+2} \deg(q_j) \right) \\ &= \deg(Q') + \deg(Q'') - \deg(S) - \deg(\hat{Q}_{n+2}) - \sum_{j=0}^{n} \deg(\hat{q}_j) - \deg(q_{n+2}) \ . \end{aligned}$$

If $D' \oplus D'' = D_{n+3}$, then $\delta = d$, and if $D' \oplus D'' = D_{n+4}$, then $\delta = d - \deg(q_{n+3})$ with $q_{n+3} = \lfloor (P_{n+3} + v)/Q_{n+3} \rfloor$, so $\deg(q_{n+3}) = g + 1 - \deg(Q_{n+3})$.

We now give upper bounds on the index n of Eq. (7.12).

Theorem 8.1. *Let N, n and K be defined by Eq. (7.3), Eq. (7.12) and Eq. (8.6), respectively. Then the following holds:*

(a) If K is even, then $n \leq (K-4)/2$ and $D' \oplus D'' = D_{n+3}$ is reduced.
(b) If K is odd, then we have the following:
  (a) If C is unusual, then $n \leq (K-5)/2$ and $D' \oplus D'' = D_{n+3}$.
  (b) If C is imaginary or real and $\deg(P'' + v) < g+1$, then $n \leq (K-3)/2$ and $D' \oplus D'' = D_{n+3}$.
  (c) If C is imaginary or real and $\deg(P'' + v) = g+1$, then $n \leq (K-5)/2$, and $D' \oplus D'' = D_{n+3}$ if and only if $\deg(b_{n+1}) < N$, otherwise $D' \oplus D'' = D_{n+4}$.

Proof. From Lemma 2.2 (c), Eq. (7.3), Eq. (7.12), and Eq. (8.6), we obtain

$$n \leq \deg(b_{-1}) - \deg(b_n) - 1 < \deg(Q') - N - 1 = \frac{1}{2}(K - M + g) - 1 \ .$$

If K is even, then as before, $\deg(b_{n+1}) < N$, which holds if and only if $\deg(Q_{n+2}) < M$, or equivalently, $\deg(Q_{n+2}) \leq g$. Thus, D_{n+3} is reduced, and we simply use $M \geq g$ to obtain $n < K/2 - 1$ and hence $n \leq (K-4)/2$.

Suppose now that K is odd. Then all the claims in Theorem 8.1 except for the bounds on n follow from Proposition 8.1. If $\deg(P'' + v) < g + 1$, then we again use $M \geq g$ to obtain $n \leq (K-3)/2$. If $\deg(P'' + v) = g + 1$ then $M = g+1$, yielding $n \leq (K-5)/2$. Note that this includes the unusual scenario. □

Remark 8.2. The bounds in Theorem (8.1) can also be derived as follows. If $D' \oplus D'' = D_{l+1}$, then by our remarks just before Eq. (5.13), $l \leq \lceil K/2 \rceil$ if $\deg(Q_l) \leq g$, and $l \leq \lceil (K-1)/2 \rceil$ if $\deg(Q_l) = g + 1$ for C unusual and g odd. Now distinguish between the cases $l = n + 2$ and $l = n + 3$ using Proposition 8.1.

In lieu of Remark 8.1, we see that in the imaginary and real cases, $D' \oplus D''$ can usually be found in $(K-4)/2$ "NUCOMP steps" if K is even and in either $(K-3)/2$ NUCOMP steps or $(K-5)/2$ NUCOMP steps plus one reduction step if K is odd. Furthermore, if D' and D'' have minimal norm, then we expect that $\deg(Q') = \deg(Q'')$. This degree will generally be equal to g if C is imaginary, unusual with g even, or real, and tends to be equal to $g + 1$ if C is unusual and g odd. In the latter case, we expect that the norm of $D' \oplus D''$ again has degree $g + 1$. We thus obtain the following Corollary:

Corollary 8.2. *Let N, n and K be defined by Eq. (7.3), Eq. (7.12) and Eq. (8.6), respectively, and assume that*

- $M = \deg(P'' + v) = g + 1$.
- $\deg(Q') = \deg(Q'') = g$ *if C is imaginary, unusual with g even, or real.*
- $\deg(Q') = \deg(Q'') = g + 1$ *if C is unusual and g odd.*
- $\deg(b_n) - \deg(b_{n+1}) = 1$.

Then the following holds:

(a) If g is even, then $D' \oplus D'' = D_{n+3}$ is reduced and $n \leq (g-4)/2$.
(b) If g is odd and C is unusual, then $D' \oplus D'' = D_{n+3}$ and $n \leq (g-3)/2$.
(c) If g is odd and C is imaginary or real, then $D' \oplus D'' = D_{n+4}$ and $n \leq (g-5)/2$.

Proof. Since $\deg(Q') = \deg(Q'')$, g has the same parity as K. If g is even, or g is odd and C is imaginary or real, then $\deg(Q') = \deg(Q'') = g$, so $K = g$. The bounds on n for these cases now again follow immediately from Theorem 8.1. If g is odd and C is unusual, then $K = 2(g+1) - g = g + 2$, so $(K-5)/2 = (g-3)/2$. □

In all three cases of Corollary 8.2, as pointed out in Sec. 6, $D' \oplus D''$ is reached after at most $\lceil g/2 \rceil$ steps; these are all NUCOMP steps except in case (c), where all but the last step are NUCOMP steps and the last step is a baby step.

Finally, recall our assumption Eq. (7.1) that $\deg(P'' + v) \leq g + 1$. We argue that if $D' \oplus D'' = (\hat{Q}, \hat{P})$, then we generally have $\deg(\hat{P}) \leq g + 1$ as well if C is imaginary or real. If $\hat{P} = P_{n+3}$, then we saw that $\deg(P_{n+3} - h - v) \leq g$, so $\deg(\hat{P}) \leq g$ if C is imaginary and $\deg(\hat{P}) \leq g+1$ if C is real. Suppose now that $\hat{P} = \hat{P}_{n+2}$, so $\deg(Q_{n+2}) \leq g$, implying $\deg(u_{n+1}) \leq g$ by Eq. (8.3) and Lemma 8.1. Since $\gcd(Q'/S, U)$ is very likely to have small degree (usually the gcd is 1), it is highly improbable that $b_{n+1} = 0$. Therefore, $\hat{q}_{n+1}$ is defined, and from part (a) of Lemma 2.2 and the definition of u_i, we see that

$$\deg(Q_{n+1}) = \deg(u_n) = 2\deg(\hat{q}_{n+1}) + \deg(u_{n+1}) \leq 2\deg(\hat{q}_{n+1}) + g \ .$$

It follows from Eq. (5.13) and part (a) of Corollary 8.1 that $P_{n+2} = h - P_{n+1} + \lfloor P_{n+1}/Q_{n+1} \rfloor Q_{n+1}$, so $\deg(P_{n+2}) \leq \deg(Q_{n+1}) - 1 \leq 2\deg(\hat{q}_{n+1}) + g - 1$. Since $\hat{q}_{n+1}$, as the partial quotient of a continued fraction expansion, is expected to have degree 1, we obtain $\deg(P_{n+2}) \leq g + 1$ with high probability.

Note that if C is unusual, then we may have $\deg(P_{n+2}) \leq g + 2$, but all the proofs in Sec. 8 can be easily adjusted to work for this case under the assumption $\deg(P'') \leq g + 2$. We omit the details of this reasoning.

If we impose stronger conditions than Eq. (7.1) on P'', then $\hat{P}$ need not satisfy the same conditions. For example, if D'' is given in adapted form, then $D' \oplus D''$ will usually not be in adapted form. Similarly, if C is real and D'' is in reduced form, then $D' \oplus D''$ will generally not be in reduced form. In this case, if the application requires the basis $\hat{Q}, \hat{P}$ to be of a particular form, then a suitable multiple of $\hat{Q}$ will need to be added to $\hat{P}$. However, we point out that in many applications, the above question does not even play a role. For example, if we apply NUCOMP repeatedly to a starting divisor $D'' = (Q'', P'')$, say to generate a "scalar product" $D'' \oplus D'' \oplus \cdots \oplus D''$ computed as part of a cryptographic protocol, then it is sufficient to ensure that $\deg(P'') \leq g + 1$ once at the beginning of the computation.

9. NUCOMP Algorithms

The basic strategy of the NUCOMP algorithm is as follows. Suppose we are given two divisors $D' = (Q', P')$ and $D'' = (Q'', P'')$ of minimal norm with $\deg(P'') \leq g+1$; for reasons of efficiency, we will also input the polynomials $R' = (f + hP' - P'^2)/Q'$ and $R'' = (f + hP'' - P''^2)/Q''$. Begin by computing S, U as in Eq. (6.1). If $\deg(Q') + \deg(Q'') - 2\deg(S) \leq g+1$, then the divisor $D = (Q, P)$ defined in Eq. (6.1) is at most one step away from having minimal norm, so simply compute Q and P as in Eq. (6.1) and, if necessary, apply one reduction step — Eq. (5.2) if C is imaginary or Eq. (5.14) otherwise — to $D = (Q, P)$ to obtain $D' \oplus D''$.

Suppose now that $\deg(Q') + \deg(Q'') - 2\deg(S) \geq g+2$. Then we simultaneously compute the sequences b_i, a_i, c_i, d_i for $-1 \leq i \leq n+1$; this is what we referred to as"NUCOMP steps" in the previous section. Finally, recover P_{n+2} and Q_{n+2} using Eq. (7.10) and Eq. (7.9) and, if necessary, apply one iteration of Eq. (5.14) to P_{n+2}, Q_{n+2} to obtain $D' \oplus D''$. We describe this method in algorithmic form below.

Algorithm 9.1. NUCOMP (original)
Input: (Q', P', R'), (Q'', P'', R'') *with* $Q'R' = f + hP' - P'^2$ *and* $Q''R'' = f + hP'' - P''^2$, *representing two semi-reduced divisors* D' *and* D'' *of minimal norm.*
Output: $(\hat{Q}, \hat{P}, \hat{R})$ *representing* $D' \oplus D''$ *with* $\hat{Q}\hat{R} = f + h\hat{P} - \hat{P}^2$.

(1) // Compute $D' + D''$

- *(a) Compute* $S_1, W_1 \in \mathbb{F}[u]$ *such that* $S_1 = \gcd(Q', Q'') = V_1 Q' + W_1 Q''$.
- *(b) IF* $S_1 = 1$ *THEN* $S := S_1 = 1$, $X := 0$, $W := W_1$, *GOTO (d).*
- *(c) Compute* $S, W_2, X \in \mathbb{F}[u]$ *such that* $S = \gcd(S_1, P' + P'' - h) = W_2 S_1 + X(P' + P'' - h)$. *Put* $W := W_1 W_2$.
- *(d) Put* $b_{-1} := Q'/S$ *and* $U :\equiv W(P' - P'') + XR'' \pmod{b_{-1}}$.

(2) IF $\deg(Q') + \deg(Q'') - 2\deg(S) \leq g+1$ *THEN // at most one baby step*

- *(a) Put*

$$\hat{Q} := \frac{Q'Q''}{S^2}, \quad \hat{P} := P'' + U\frac{Q''}{S} \pmod{Q}, \quad \hat{R} := \frac{f + hP - P^2}{Q} .$$

- *(b) IF* $\deg(\hat{Q}) = g+1$ *AND* C *is imaginary THEN*

$$\hat{Q} := \hat{R} , \quad \hat{P} := h - \hat{P} \pmod{\hat{Q}} , \quad \hat{R} := \frac{f + h\hat{P} - \hat{P}^2}{\hat{Q}} .$$

(c) *IF* $\deg(\hat{Q}) = g + 1$ *AND* C *is real THEN*

(i) *Put* $\tilde{P} := \hat{P}$, $\tilde{Q} := \hat{Q}$

(ii) $\tilde{q} := \lfloor (\tilde{P} + v)/\tilde{Q} \rfloor$.

(iii) $\hat{P} := h - \tilde{P} + \tilde{q}\tilde{Q}$.

(iv) $\hat{Q} := \hat{R} + \tilde{q}(\tilde{P} - \hat{P})$, $\hat{R} := \tilde{Q}$.

(d) *RETURN*(Q, P, R)

(3) *// Now apply NUCOMP*

(a) $b_0 := U$, $a_{-1} := 0$, $a_0 := 1$.

(b) $c_{-1} := Q''/S$, $P = P'' + UQ''/S$, $c_0 := (P - P')/b_{-1}$.

(c) $d_{-1} := P' + P'' - h$, $d_0 := (d_{-1}b_0 - SR'')/b_{-1}$.

(d) $i := 0$, $N := (\deg(Q') - \deg(Q'') + \max\{g, \deg(P'' + v)\})/2$.

(4) *While* $\deg(b_i) > N$ *do*

(a) $\hat{q}_i := \lfloor b_{i-1}/b_i \rfloor$, $b_{i+1} := b_{i-1} \pmod{b_i}$. *// Division with remainder*

(b) $a_{i+1} := a_{i-1} - \hat{q}_i a_i$.

(c) $c_{i+1} := c_{i-1} - \hat{q}_i c_i$.

(d) $d_{i+1} := d_{i-1} - \hat{q}_i d_i$.

(e) $i := i + 1$.

(5) *// Now* $i = n + 1$, *so* $\deg(b_{n+1}) \leq N < \deg(b_n)$.

(a) $Q_{i+1} := (-1)^{i+1}(b_i c_i - a_i d_i)$ *//* $Q_{i+1} = Q_{n+2}$.

(b) $P_{i+1} := (-1)^{i+1}(b_{i-1}c_i - a_i d_{i-1}) + P''$ *//* $P_{i+1} = P_{n+2}$.

(c) $R_{i+1} := (-1)^{i-1}(a_{i-1}d_{i-1} - b_{i-1}c_{i-1})$ *//* $R_{i+1} = R_{n+2} = Q_{n+1}$

(d) *IF* C *is imaginary or real and* $\deg(Q_{i+1}) = g + 1$ *THEN*

i. *IF* C *is imaginary,* $q_{i+1} := \lfloor P_{i+1}/Q_{i+1} \rfloor$
ELSE $q_{i+1} := \lfloor (P_{i+1} + v)/Q_{i+1} \rfloor$

ii. $P_{i+2} := h - P_{i+1} + q_{i+1}Q_{i+1}$.

iii. $Q_{i+2} := R_{i+1} + q_{i+1}(P_{i+1} - P_{i+2})$.

iv. $R_{i+2} := Q_{i+1}$.

v. $i := i + 1$.

(e) *put* $\hat{Q} := Q_{i+1}$, $\hat{P} := P_{i+1}$, $\hat{R} := R_{i+1}$.

(f) *RETURN*$(\hat{Q}, \hat{P}, \hat{R})$.

There is an alternative version of this algorithm that is aimed at keeping the size of the intermediate operands low. In the context of binary quadratic forms, this idea is originally due to Atkin. Instead of computing all four sequences, we only compute b_i, a_i for $-1 \leq i \leq n + 1$. Then compute c_{n+1}, d_n and d_{n+1} using Eq. (7.7) and Eq. (7.8), and finally, P_{n+2} and Q_{n+2} using Eq. (7.10) and Eq. (7.9). Since $N \approx g/2$, we expect b_n and b_{n+1}

to have approximate degree $g/2$. By Lemma 2.2 (e), we thus also expect $\deg(a_{n+1}) \approx g/2$, and Eq. (7.7) and Eq. (7.8) show that c_{n+1}, d_n and d_{n+1} also have approximate degree $g/2$. So all operands have very small degree; only the numerators in Eq. (7.7) for $i = n+1$ and Eq. (7.8) for $i = n$ and $i = n+1$ have degree $\approx 3g/2$. These degrees are much smaller than those of the numerators of c_0 and d_0 which are roughly $2g$. On the other hand, the computation of c_{n+1}, d_n and d_{n+1} requires three divisions by b_{-1}, compared to only two such divisions required for computing c_0 and d_0. We again present this technique algorithmically below.

Algorithm 9.2. NUCOMP (small operands)
Input: (Q', P', R'), (Q'', P'', R'') *with* $Q'R' = f + hP' - P'^2$ *and* $Q''R'' = f + hP'' - P''^2$, *representing two semi-reduced divisors* D' *and* D'' *of minimal norm.*
Output: $(\hat{Q}, \hat{P}, \hat{R})$ *representing* $D' \oplus D''$ *with* $\hat{Q}\hat{R} = f + h\hat{P} - \hat{P}^2$.

(1) // Compute $D' + D''$
  (a) Compute $S_1, W_1 \in \mathbb{F}[u]$ *such that* $S_1 = \gcd(Q', Q'') = V_1Q' + W_1Q''$.
  (b) IF $S_1 = 1$ *THEN* $S := S_1 = 1$, $X := 0$, $W := W_1$, *GOTO (d).*
  (c) Compute $S, W_2, X \in \mathbb{F}[u]$ *such that* $S = \gcd(S_1, P' + P'' - h) = W_2S_1 + X(P' + P'' - h)$. *Put* $W := W_1W_2$.
  (d) Put $b_{-1} := Q'/S$ *and* $U :\equiv W(P' - P'') + XR'' \pmod{b_{-1}}$.
(2) IF $\deg(Q') + \deg(Q'') - 2\deg(S) \le g + 1$ *THEN // at most one baby step*
  (a) Put

$$\hat{Q} := \frac{Q'Q''}{S^2}, \quad \hat{P} := P'' + U\frac{Q''}{S} \pmod{Q}, \quad \hat{R} := \frac{f + hP - P^2}{Q} .$$

  (b) IF $\deg(\hat{Q}) = g + 1$ *AND* C *is imaginary THEN*

$$\hat{Q} := \hat{R} , \quad \hat{P} := h - \hat{P} \pmod{\hat{Q}} , \quad \hat{R} := \frac{f + h\hat{P} - \hat{P}^2}{\hat{Q}} .$$

  (c) IF $\deg(\hat{Q}) = g + 1$ *AND* C *is real THEN*
    (i) Put $\tilde{P} := \hat{P}$, $\tilde{Q} := \hat{Q}$
    (ii) $\tilde{q} := \lfloor (\tilde{P} + v)/\tilde{Q} \rfloor$.
    (iii) $\hat{P} := h - \tilde{P} + \tilde{q}\tilde{Q}$.
    (iv) $\hat{Q} := \hat{R} + \tilde{q}(\tilde{\mathcal{P}} - P)$, $\hat{R} := \tilde{Q}$.
  (d) RETURN$(\hat{Q}, \hat{P}, \hat{R})$
(3) // Now apply NUCOMP

(a) $b_0 := U,\ \ a_{-1} := 0,\ \ a_0 := 1.$
(b) $i := 0,\ \ N := (\deg(Q') - \deg(Q'') + \max\{g, \deg(P'' + v)\})/2.$

(4) While $\deg(b_i) > N$ *do*

(a) $\hat{q}_i := \lfloor b_{i-1}/b_i \rfloor$, $b_{i+1} := b_{i-1} \pmod{b_i}$. *// Division with remainder*
(b) $a_{i+1} := a_{i-1} - \hat{q}_i a_i$.
(c) $i := i + 1$.

(5) // Now $i = n + 1$, *so* $\deg(b_{n+1}) \le N < \deg(b_n)$.

(a) $c_i := (b_i Q''/S + a_i(P' - P''))/b_{-1}$.
(b) $d_{i-1} := (b_{i-1}(P' + P'' - h) + a_{i-1}SR'')/b_{-1}$.
(c) $X_1 := b_{i-1}c_i$, $c_{i-1} := (X_1 + (-1)^i(P' - P''))/b_i$.
(d) $X_2 := (-1)^{i-1}a_i d_{i-1}$, $d_i := ((P' + P'' - h) - X_2)/(-1)^{i-2}a_{i-1}$.
(e) $Q_{i+1} := (-1)^{i+1}(b_i c_i - a_i d_i)$ *// * $Q_{i+1} = Q_{n+2}$.
(f) $P_{i+1} := (-1)^{i+1}(X_2 - X_1) + P''$ *// * $P_{i+1} = P_{n+2}$.
(g) $R_{i+1} := (-1)^{i-1}(a_{i-1}d_{i-1} - b_{i-1}c_{i-1})$ *// * $R_{i+1} = R_{n+2} = Q_{n+1}$
(h) IF C *is imaginary or real and* $\deg(Q_{i+1}) = g + 1$ *THEN*

i. *IF* C *is imaginary,* $q_{i+1} := \lfloor P_{i+1}/Q_{i+1} \rfloor$
ELSE $q_{i+1} := \lfloor (P_{i+1} + v)/Q_{i+1} \rfloor$
ii. $P_{i+2} := h - P_{i+1} + q_{i+1}Q_{i+1}$.
iii. $Q_{i+2} := R_{i+1} + q_{i+1}(P_{i+1} - P_{i+2})$.
iv. $R_{i+2} := Q_{i+1}$.
v. $i := i + 1$.

(i) put $\hat{Q} := Q_{i+1}$, $\hat{P} := P_{i+1}$, $\hat{R} := R_{i+1}$.
(j) RETURN$(\hat{Q}, \hat{P}, \hat{R})$.

10. An Extra Reduced Divisor

For real curves, if D_{n+3} is not reduced, then one can compute an alternative reduced divisor different from D_{n+4} under certain circumstances. Let C be a real hyperelliptic curve, and $\deg(P'' - h - v) \le g$; this is the case, for example, if D'' is given in reduced form. If L is as in Eq. (8.4), then $L \le 2g+1$, and $L \le g$ if D'' is in reduced form. Furthermore, $\deg(P''+v) = M = g + 1$, so by Proposition 8.1 (c), $D' \oplus D'' = D_{n+4}$ if and only if K as given in Eq. (8.6) is odd and $\deg(b_{n+1}) = N$; note that in this case, $b_{n+1} \neq 0$, so $\hat{q}_{n+1}$ and b_{n+2} are defined. So suppose that this is the case, and define a new divisor $\hat{D}_{n+4} = (\hat{Q}_{n+3}, \hat{P}_{n+3})$ as follows:

$$\hat{P}_{n+3} = h - \hat{P}_{n+2} + \hat{q}_{n+1}\hat{Q}_{n+2}, \quad \hat{Q}_{n+3} = \frac{f + h\hat{P}_{n+3} - \hat{P}_{n+3}^2}{\hat{Q}_i}\ , \quad (10.1)$$

i.e. $\hat{D}_{n+4}$ is obtained by applying Eq. (7.5) to $\hat{D}_{n+3} = (\hat{Q}_{n+2}, \hat{P}_{n+2})$ (or alternatively, by using Eq. (7.10) and Eq. (7.9) with $i = n+3$). We prove $\hat{D}_{n+4}$ is a reduced divisor that is almost always different from D_{n+4}.

Proposition 10.1. *Let C be real, $\deg(P'' - h - v) \leq g$, $\hat{D}_{n+3}$ not reduced, and $\hat{D}_{n+4} = (\hat{Q}_{n+3}, \hat{P}_{n+3})$ be given by Eq. (10.1). Then $\hat{D}_{n+4}$ is reduced.*

Proof. We have $\deg(\hat{Q}_{n+2}) = \deg(u_{n+1}) = g+1$. Then $\deg(u_{n+2}) \leq \deg(u_{n+1}) - 2 = g-1$ by Lemma 2.2 (a), $\deg(v_{n+2}) \leq g$ by Lemma 8.1 (a), and $\deg(w_{n+2}) = L - \deg(u_{n+1}) \leq g$ by Lemma 8.1 (b), since $L \leq 2g+1$. Thus, $\deg(\hat{Q}_{n+3}) \leq g$ by Eq. (8.3), so $\hat{D}_{n+4}$ is reduced. □

Before we can prove that $\hat{D}_{n+4} \neq D_{n+4}$ almost always, we first require a lemma.

Lemma 10.1. *Under the assumptions of Proposition 10.1, we have*

$$\deg(\hat{P}_{n+3} + v) \leq g \ .$$

Proof. Analogous to Eq. (8.1), we can derive

$$(-1)^{i+1}(\hat{P}_{i+1} + P'' - h) = u'_i + v'_i + w'_i$$

where

$$u'_i = \frac{Q''}{b_{-1}S} b_{i-1} b_i \ , \quad v'_i = \frac{h - 2P''}{b_{-1}} a_{i-1} b_i \ , \quad w'_i = \frac{SR''}{b_{-1}} a_{i-1} a_i \ ,$$

for $0 \leq i \leq m+1$. Using Lemmas 2.2 and 8.1, we obtain

$$\begin{aligned} \deg(u'_{n+2}) &\leq \deg(u_{n+1}) - 1 = (g+1) - 1 = g \ , \\ \deg(v'_{n+2}) &\leq \deg(v_{n+1}) - 1 \leq g - 1 \ , \\ \deg(w'_{n+2}) &\leq \deg(w_{n+2}) - 1 = L - \deg(u_{n+1}) - 1 = g - 1 \ . \end{aligned}$$

It follows that

$$\deg(\hat{P}_{n+3} + v) = \deg\Big((\hat{P}_{n+3} + P'' - h) - (P'' - h - v)\Big) \leq g \ . \qquad \square$$

Proposition 10.2. *Under the assumptions of Proposition 10.1, and with D_{n+4} given by Eq. (8.5), we have $\hat{D}_{n+4} \neq D_{n+4}$, provided $D_{n+4} \neq 0$.*

Proof. Recall that Eq. (8.5) yielded $\deg(P_{n+3} - h - v) \leq g$, so $\deg(P_{n+3} + v) = g+1$. Thus, by Lemma 10.1, $\deg(\hat{P}_{n+3} + v) \leq g < \deg(P_{n+3} + v)$. It follows that $\deg(P_{n+3}) = \deg(\hat{P}_{n+3}) = g+1$ and

$\hat{P}_{n+3} \neq P_{n+3}$. Now $\hat{P}_{n+3} - P_{n+3} = s\hat{Q}_{n+2}$ with $s = \hat{q}_{n+1} - q_{n+2}$. Since $\deg(\hat{Q}_{n+2}) = g+1$, we must have $s \in \mathbb{F}_q^*$.

By way of contradiction, assume that $\hat{D}_{n+4} = D_{n+4} \neq 0$. Then Q_{n+3} and $\hat{Q}_{n+3}$ differ by a factor in k^*, and Q_{n+3} divides $\hat{P}_{n+3} - P_{n+3} = s\hat{Q}_{n+2}$. Since $s \in \mathbb{F}_q^*$, we see that Q_{n+3} divides $\hat{Q}_{n+2}$. By Eq. (8.5) and Eq. (10.1), we have

$$\begin{aligned}\hat{Q}_{n+2}(\hat{Q}_{n+3} - Q_{n+3}) &= (f + h\hat{P}_{n+3} - \hat{P}_{n+3}^2) - (f + hP_{n+3} - P_{n+3}^2) \\ &= (\hat{P}_{n+3} - P_{n+3})(h - \hat{P}_{n+3} - P_{n+3}) \\ &= s\hat{Q}_{n+2}(h - 2P_{n+3} - s\hat{Q}_{n+2}) \ ,\end{aligned}$$

so Q_{n+3} divides $h - 2P_{n+3}$. Now $D_{n+4} \neq 0$ forces Q_{n+3} to be non-constant. Let r be a root of Q_{n+3} in some algebraic closure of k. Then we can use reasoning analogous to the proof of Proposition 5.1 to infer that $(r, -P_{n+3}(r))$ is a singular point on C, a contradiction. □

Remark 10.1. Let $\hat{\mathfrak{a}}_{n+3}$, $\mathfrak{a}_{n+4}$ and $\hat{\mathfrak{a}}_{n+4}$ be the reduced ideals corresponding to $\hat{D}_{n+3}$, D_{n+4}, and $\hat{D}_{n+4}$, respectively. Then $(\hat{Q}_{n+2})\mathfrak{a}_{n+4} = (P_{n+3} + v)\hat{\mathfrak{a}}_{n+3}$ and $(\hat{Q}_{n+2})\hat{\mathfrak{a}}_{n+4} = (\hat{P}_{n+3} + v)\hat{\mathfrak{a}}_{n+3}$. If we now take distances with respect to some starting divisor and set $\delta_{n+4} = \delta(D_{n+4})$ and $\hat{\delta}_{n+4} = \delta(\hat{D}_{n+4})$, then we have $\delta_{n+4} = \hat{\delta}_{n+4} + \delta$ with

$$\delta = \deg(P_{n+3} + v) - \deg(\hat{P}_{n+3} + v) \ .$$

Since $\deg(P_{n+3} + v) = g + 1 > \deg(\hat{P}_{n+3} + v)$, we have $\delta \geq 1$. Furthermore, since $\deg(P_{n+3} + v) = \deg(\hat{P}_{n+3} - h - v) = g + 1$,

$$\frac{P_{n+3} + v}{\hat{P}_{n+3} + v} = \frac{(P_{n+3} + v)(\hat{P}_{n+3} - h - v)}{\hat{Q}_{n+2}Q_{n+3}} \ ,$$

and $\deg(Q_{n+3}) \geq 1$, we have $\delta \leq 2(g+1) - (g+1) - 1 = g$. In summary, $1 \leq \delta \leq g$, so D_{n+4} and $\hat{D}_{n+4}$ are not far from each other in the infrastructure of the appropriate ideal class. In general, we expect $\deg(Q_{n+3}) = g$ and hence $\delta = 1$, so D_{n+4} and $\hat{D}_{n+4}$ are neighbors.

11. Numerical Results

The following numerical experiments were performed on a Pentium IV 2.4 GHz computer running Linux. We used the computer algebra library NTL [14] for finite field and polynomial arithmetic and the GNU `C++` compiler version 3.4.3.

11.1. *Binary Exponentiation*

In order to test the efficiency of our versions of NUCOMP, we implemented routines for binary exponentiation using Cantor's algorithm in Eq. (6.1), NUCOMP (Algorithm 9.1), and NUCOMP with small operands (Algorithm 9.2). All three algorithms were implemented using real, imaginary, and unusual curves defined over prime finite fields $\mathbb{F}_p$ and characteristic 2 finite fields $\mathbb{F}_{2^n}$.

Table 11.1-11.5 contain the ratio of runtimes for binary exponentiation using Algorithm 9.1 (NUCOMP using recurrences to compute c_i and d_i) divided by the runtime using Algorithm 9.2 (NUCOMP using formulas to compute the final values of c_i and d_i). For each genus and field size listed, 1000 binary exponentiations were performed with random 100-bit exponents. The same 1000 exponents were used for both algorithms and for all genera and finite field sizes. The divisors produced by NUCOMP were normalized; adapted basis was used for imaginary and unusual curves and reduced basis was used for real curves [5]. The data clearly show that Algorithm 9.1 is more efficient that Algorithm 9.2 for $g < 10$ approximately, but that Algorithm 9.2 is ultimately more efficient as g grows.

Table 11.1. Exponentiation ratios (Alg 9.1 / Alg 9.2) over $\mathbb{F}_p$, imaginary.

g	$\log_2 p$								
	2	4	8	16	32	64	128	256	512
2	0.9839	0.9012	0.8983	0.9037	0.9038	0.8909	0.9110	0.9140	0.8976
3	0.8703	0.9471	0.9289	0.8934	0.9523	0.9659	0.9503	0.9568	0.9591
4	0.9619	0.9342	0.9266	0.9662	0.9503	0.9514	0.9634	0.9644	0.9672
5	0.9693	0.9550	0.9518	0.9576	0.9567	0.9474	0.9327	0.9341	0.9318
6	0.9754	0.9548	0.9631	0.9624	0.9378	0.9467	0.9413	0.9442	0.9434
7	0.9407	0.9530	0.9608	0.9561	0.9518	0.9532	0.9559	0.9592	0.9613
8	0.9726	0.9663	0.9666	0.9600	0.9576	0.9668	0.9785	0.9641	0.9671
9	0.9751	0.9764	0.9840	0.9776	0.9645	0.9760	0.9947	0.9710	0.9784
10	0.9793	0.9708	0.9817	0.9724	0.9629	0.9746	0.9976	0.9775	0.9864
11	0.9853	0.9792	0.9854	0.9877	0.9705	0.9839	1.0067	0.9875	0.9974
12	0.9983	0.9969	0.9971	0.9875	0.9777	0.9907	0.9924	0.9917	1.0023
13	0.9851	1.0084	1.0000	0.9963	0.9874	0.9993	0.9986	1.0024	1.0102
14	1.0126	1.0039	1.0049	0.9988	0.9845	1.0010	1.0003	1.0038	1.0130
15	1.0143	1.0085	1.0102	1.0097	0.9913	1.0079	1.0076	1.0103	1.0204
20	1.0823	1.1033	1.1029	1.1017	1.0670	1.1102	1.0568	1.0710	1.0866
25	1.1003	1.1185	1.1137	1.1203	1.1103	1.1187	1.0718	1.0988	1.0896
30	1.0872	1.0908	1.0927	1.0895	1.1152	1.1107	1.0839	1.0946	1.1129

Table 11.6–11.10 contain the ratio of runtimes for binary exponentiation using Cantor's algorithm as compared to that using the faster of Algorithm 9.1 or Algorithm 9.2. Again, for each genus and field size listed, 1000 binary exponentiations were performed with random 100-bit exponents. The same 1000 exponents were used for both algorithms and for all genera and finite field sizes. The data clearly show that NUCOMP outperforms Cantor's algorithm except for very small genera and finite field sizes, and that its relative performance improves as both the genus and

Table 11.2. Exponentiation ratios (Alg 9.1 / Alg 9.2) over $\mathbb{F}_p$, real.

	$\log_2 p$								
g	2	4	8	16	32	64	128	256	512
2	0.8661	0.8743	0.9368	0.9557	0.8414	0.8766	0.8830	0.8859	0.8761
3	0.8579	0.9149	0.9163	0.9216	0.8967	0.8996	0.8924	0.8761	0.8851
4	0.9395	0.9647	0.9485	0.9582	0.9533	0.9545	0.9633	0.9648	0.9694
5	0.9294	0.9209	0.9335	0.9489	0.9629	0.9661	0.9652	0.9695	0.9726
6	0.9477	0.9397	0.9595	0.9523	0.9636	0.9566	0.9499	0.9535	0.9570
7	0.8635	0.9431	0.9466	0.9370	0.9644	0.9606	0.9580	0.9586	0.9595
8	0.9349	0.9667	0.9684	0.9860	0.9869	0.9793	1.0003	0.9783	0.9781
9	0.9549	0.9723	0.9683	0.9561	0.9859	0.9818	0.9997	0.9774	0.9788
10	0.9522	0.9963	0.9913	0.9820	0.9968	0.9942	1.0116	0.9857	0.9962
11	0.9540	0.9645	0.9854	0.9874	0.9966	0.9975	0.9957	0.9902	0.9992
12	0.9726	0.9872	0.9960	0.9809	1.0166	1.0098	1.0058	1.0011	1.0130
13	0.9806	0.9948	0.9926	0.9941	1.0191	1.0148	1.0078	1.0018	1.0105
14	0.9883	1.0135	1.0023	0.9989	1.0239	1.0197	1.0171	1.0139	1.0237
15	0.9807	0.9989	1.0117	1.0071	1.0229	1.0226	1.0168	1.0127	1.0209
20	1.0995	1.1180	1.1156	1.1109	1.1063	1.1291	1.0692	1.0856	1.0932
25	1.0968	1.1090	1.1164	1.1060	1.0847	1.1100	1.0745	1.0784	1.0989
30	1.0981	1.1088	1.1149	1.1068	1.0980	1.1066	1.0863	1.0979	1.1258

Table 11.3. Exponentiation ratios (Alg 9.1 / Alg 9.2) over $\mathbb{F}_p$, unusual.

	$\log_2 p$								
g	2	4	8	16	32	64	128	256	512
2	0.9108	0.8800	0.8571	0.8910	0.8969	0.8896	0.9069	0.9082	0.9019
3	0.9175	1.0081	1.0161	1.0109	0.9715	0.9466	0.9658	0.9583	0.9649
4	0.9504	1.0290	1.0311	0.9967	0.9552	0.9542	0.9614	0.9603	0.9660
5	0.9684	0.9690	0.9853	0.9844	0.9730	0.9486	0.9475	0.9439	0.9491
6	0.9649	0.9626	0.9862	0.9731	0.9584	0.9471	0.9418	0.9368	0.9389
7	0.9816	1.0212	1.0139	0.9620	0.9854	0.9705	0.9868	0.9672	0.9724
8	0.9929	0.9867	0.9911	0.9980	0.9775	0.9666	0.9782	0.9590	0.9629
9	0.9938	0.9981	1.0131	0.9832	1.0047	0.9870	1.0063	0.9792	0.9899
10	1.0000	0.9982	0.9964	1.0017	0.9959	0.9834	0.9993	0.9729	0.9854
11	1.0000	1.0235	1.0103	1.0072	1.0228	1.0015	1.0012	0.9924	1.0058
12	1.0048	1.0046	1.0085	1.0014	1.0163	0.9956	0.9953	0.9851	0.9975
13	1.0000	1.0077	1.0243	1.0024	1.0362	0.9985	1.0101	1.0058	1.0184
14	0.9960	1.0245	1.0037	1.0070	1.0313	1.0101	1.0034	0.9958	1.0099
15	1.0094	1.0301	1.0370	1.0321	1.0448	1.0145	1.0176	1.0184	1.0264
20	1.1394	1.1789	1.1526	1.1262	1.1024	1.1000	1.0621	1.0671	1.0884
25	1.1014	1.1103	1.1209	1.1168	1.0860	1.1069	1.0716	1.0799	1.0981
30	1.0932	1.1047	1.1064	1.1018	1.0939	1.1108	1.0799	1.0885	1.1068

Table 11.4. Exponentiation ratios (Alg 9.1 / Alg 9.2) over $\mathbb{F}_{2^n}$, imaginary.

	$\log_2 p$								
g	2	4	8	16	32	64	128	256	512
2	0.9308	0.9002	0.8891	0.8889	0.8976	0.8744	0.9006	0.8880	0.8871
3	0.9622	0.9511	0.9547	0.9514	0.9446	0.9440	0.9600	0.9571	0.9585
4	0.9507	0.9395	0.9480	0.9507	0.9528	0.9592	0.9663	0.9613	0.9610
5	0.9682	0.9436	0.9396	0.9557	0.9443	0.9440	0.9396	0.9356	0.9343
6	0.9661	0.9544	0.9468	0.9528	0.9519	0.9530	0.9469	0.9474	0.9458
7	0.9819	0.9620	0.9674	0.9662	0.9681	0.9669	0.9611	0.9644	0.9622
8	0.9881	0.9663	0.9653	0.9693	0.9725	0.9780	0.9693	0.9691	0.9688
9	1.0071	0.9929	0.9868	0.9853	0.9920	0.9890	0.9807	0.9830	0.9820
10	1.0026	1.0011	0.9864	0.9917	0.9918	0.9891	0.9872	0.9878	0.9876
11	1.0205	0.9981	1.0046	1.0010	0.9947	0.9960	0.9960	0.9986	0.9964
12	1.0272	1.0124	1.0193	1.0137	1.0019	0.9984	1.0016	1.0042	1.0022
13	1.0341	1.0191	1.0311	1.0249	1.0116	1.0092	1.0118	1.0060	1.0148
14	1.0441	1.0311	1.0322	1.0242	1.0145	1.0081	1.0148	1.0181	1.0187
15	1.0504	1.0311	1.0415	1.0324	1.0208	1.0133	1.0190	1.0221	1.0216
20	1.1072	1.1263	1.1350	1.1218	1.1051	1.0890	1.0923	1.0893	1.0885
25	1.1624	1.1662	1.1724	1.1556	1.1337	1.1104	1.1119	1.1203	1.1146
30	1.1869	1.1797	1.1930	1.1826	1.1419	1.1375	1.1335	1.1337	1.1309

finite field size increase. The findings are consistent with those presented in [6], but our improved versions of NUCOMP presented here out-perform Cantor's algorithm for even smaller genera and finite field sizes than in [6].

Table 11.5. Exponentiation ratios (Alg 9.1 / Alg 9.2) over $\mathbb{F}_{2^n}$, real

	$\log_2 p$								
g	2	4	8	16	32	64	128	256	512
2	0.9249	0.8800	0.8630	0.8604	0.8649	0.8603	0.8816	0.8737	0.8725
3	0.8406	0.8562	0.8682	0.8670	0.8710	0.8910	0.8613	0.8745	0.8723
4	0.9331	0.9424	0.9480	0.9561	0.9524	0.9526	0.9561	0.9614	0.9618
5	0.9217	0.9480	0.9562	0.9596	0.9600	0.9526	0.9614	0.9668	0.9665
6	0.9471	0.9655	0.9548	0.9628	0.9574	0.9711	0.9444	0.9503	0.9504
7	0.9557	0.9580	0.9531	0.9511	0.9588	0.9574	0.9462	0.9512	0.9506
8	0.9765	0.9776	0.9781	0.9750	0.9819	0.9800	0.9711	0.9737	0.9759
9	0.9761	0.9709	0.9752	0.9799	0.9729	0.9705	0.9701	0.9701	0.9676
10	0.9891	1.0057	1.0019	0.9996	0.9970	0.9857	0.9868	0.9892	0.9952
11	0.9810	0.9962	1.0070	0.9997	0.9920	0.9849	0.9866	0.9905	0.9910
12	1.0080	1.0064	1.0220	1.0158	1.0081	0.9958	1.0006	1.0082	1.0085
13	1.0029	1.0162	1.0208	1.0120	1.0041	0.9845	1.0009	1.0093	1.0082
14	1.0243	1.0326	1.0379	1.0284	1.0162	0.9981	1.0093	1.0214	1.0215
15	1.0228	1.0329	1.0327	1.0270	1.0175	1.0016	1.0111	1.0182	1.0176
20	1.1270	1.1450	1.1401	1.1737	1.1256	1.0984	1.0998	1.0968	1.0937
25	1.1456	1.1565	1.1748	1.1471	1.0596	1.1021	1.1083	1.1207	1.1049
30	1.1672	1.1757	1.1822	1.1820	1.1477	1.1239	1.1288	1.1374	1.1328

Table 11.6. Exponentiation ratios (NUCOMP / Cantor) over $\mathbb{F}_p$, imaginary.

	$\log_2 p$								
g	2	4	8	16	32	64	128	256	512
2	1.0991	1.0504	1.0743	1.0432	0.9308	0.9141	0.9242	0.8847	0.8447
3	1.0662	1.0707	1.0609	1.0140	0.9523	0.9419	0.9008	0.8865	0.8652
4	1.0632	1.0607	1.0390	1.0158	0.9309	0.9286	0.9068	0.8582	0.8540
5	1.0766	1.0376	1.0350	1.0194	0.9120	0.9046	0.8865	0.8571	0.8642
6	1.0931	1.0462	1.0150	1.0056	0.8888	0.8963	0.8452	0.8594	0.8573
7	1.0235	0.9865	0.9679	0.9583	0.8692	0.8755	0.8310	0.8558	0.8586
8	0.9924	0.9349	0.9414	0.9268	0.8532	0.8697	0.8237	0.8500	0.8424
9	0.9557	0.9212	0.9212	0.9273	0.8405	0.8588	0.8144	0.8472	0.8420
10	0.9423	0.8975	0.8961	0.8910	0.8275	0.8451	0.8078	0.8402	0.8334
11	0.9538	0.8968	0.8981	0.9046	0.8128	0.8407	0.7921	0.8371	0.8333
12	0.9441	0.9043	0.8991	0.8918	0.8075	0.8332	0.8047	0.8278	0.8235
13	0.9361	0.9320	0.9035	0.9063	0.8060	0.7857	0.7995	0.8184	0.8148
14	0.9308	0.9038	0.8971	0.8981	0.7926	0.7821	0.8035	0.8184	0.8071
15	0.9135	0.8747	0.8704	0.8694	0.7851	0.7715	0.8043	0.8130	0.8059
20	0.8255	0.7956	0.7861	0.7989	0.7536	0.7242	0.7910	0.7843	0.7769
25	0.7949	0.7662	0.7693	0.7727	0.7208	0.7398	0.7854	0.7943	0.7759
30	0.7921	0.7714	0.7730	0.7716	0.7157	0.7372	0.7743	0.7616	0.7588

Table 11.7. Exponentiation ratios (NUCOMP / Cantor) over $\mathbb{F}_p$, real.

	$\log_2 p$								
g	2	4	8	16	32	64	128	256	512
2	0.8943	1.1268	1.2192	1.2763	1.0659	1.0987	1.0872	1.0731	1.0835
3	1.0449	1.1497	1.1165	1.1330	1.0503	1.0515	1.0434	1.0376	1.0500
4	1.0745	1.1081	1.0932	1.0784	1.0169	1.0137	1.0150	0.9847	1.0060
5	1.0549	1.0659	1.0300	1.0570	0.9635	0.9771	0.9650	0.9664	0.9787
6	1.0507	1.0124	1.0350	1.0327	0.9444	0.9555	0.9243	0.9540	0.9569
7	0.9705	0.9525	0.9231	0.9209	0.9144	0.9309	0.8950	0.9289	0.9512
8	0.9724	0.9539	0.9426	0.9338	0.9094	0.9195	0.8816	0.9244	0.9254
9	0.9591	0.9179	0.9028	0.9023	0.8726	0.8876	0.8608	0.8913	0.9013
10	0.9105	0.9056	0.8818	0.8877	0.8625	0.8879	0.8642	0.8933	0.8955
11	0.9396	0.9043	0.9159	0.9145	0.8402	0.8596	0.8415	0.8836	0.8862
12	0.9668	0.9341	0.9149	0.9135	0.8356	0.8536	0.8512	0.8832	0.8745
13	0.9581	0.9128	0.8856	0.8942	0.8047	0.7877	0.8201	0.8637	0.8560
14	0.9596	0.9098	0.8782	0.8912	0.8051	0.7874	0.8205	0.8502	0.8471
15	0.9356	0.8696	0.8640	0.8670	0.7789	0.7656	0.8037	0.8425	0.8387
20	0.8065	0.7549	0.7519	0.7638	0.7463	0.7275	0.8110	0.8108	0.8008
25	0.7717	0.7303	0.7215	0.7186	0.6996	0.7124	0.7818	0.7842	0.7723
30	0.7651	0.7337	0.7270	0.7392	0.6873	0.7212	0.7687	0.7749	0.7801

11.2. *Key Exchange*

We also ran numerous examples of the key exchange protocols described in [7], again using both real and imaginary curves and $\mathbb{F}_p$ (p prime) and $\mathbb{F}_{2^n}$ as base fields. The genus of our curves ranged from 2 to 6 and the underlying

Table 11.8. Exponentiation ratios (NUCOMP / Cantor) over $\mathbb{F}_p$, unusual.

	$\log_2 p$								
g	2	4	8	16	32	64	128	256	512
2	1.0438	1.1079	1.0435	1.0444	0.9607	0.9345	0.9257	0.8955	0.8749
3	1.0500	1.0649	1.0506	1.0377	0.9102	0.8970	0.8815	0.8443	0.8417
4	1.1220	1.0905	1.0576	1.0565	0.9182	0.9301	0.9102	0.8782	0.8698
5	1.0824	1.0539	1.0030	1.0216	0.8861	0.8631	0.8382	0.8535	0.8465
6	1.1224	1.0404	1.0259	1.0419	0.9115	0.8951	0.8580	0.8769	0.8744
7	1.0081	0.9179	0.9309	0.9179	0.8604	0.8461	0.8158	0.8424	0.8312
8	0.9882	0.9695	0.9654	0.9900	0.8668	0.8647	0.8342	0.8627	0.8526
9	0.9340	0.8902	0.8883	0.8784	0.8286	0.8274	0.7986	0.8336	0.8274
10	0.9245	0.9151	0.9224	0.9308	0.8523	0.8396	0.8182	0.8484	0.8424
11	0.9641	0.9075	0.8642	0.8858	0.8033	0.8117	0.8016	0.8177	0.8164
12	0.9570	0.8997	0.8892	0.9055	0.8215	0.8265	0.8166	0.8258	0.8338
13	0.9615	0.8977	0.8662	0.8828	0.7821	0.7650	0.7964	0.8115	0.8026
14	0.9448	0.8719	0.8652	0.8858	0.7839	0.7699	0.8104	0.8328	0.8251
15	0.8945	0.8203	0.8111	0.8306	0.7663	0.7389	0.7822	0.7945	0.7858
20	0.8458	0.8234	0.8108	0.8250	0.7220	0.7456	0.8074	0.7927	0.7996
25	0.7964	0.7660	0.7606	0.7656	0.7252	0.7429	0.7942	0.7901	0.7822
30	0.7781	0.7591	0.7575	0.7622	0.7055	0.7307	0.7769	0.7766	0.7682

Table 11.9. Exponentiation ratios (NUCOMP / Cantor) over $\mathbb{F}_{2^n}$, imaginary.

	$\log_2 p$								
g	2	4	8	16	32	64	128	256	512
2	1.0068	0.9696	0.9498	0.9257	0.9185	0.8919	0.8824	0.8433	0.8205
3	0.9857	0.9757	0.9401	0.9244	0.9244	0.9251	0.8789	0.8951	0.8855
4	0.9725	0.9638	0.9448	0.9301	0.9056	0.9204	0.9285	0.9102	0.9110
5	0.9916	0.9705	0.9404	0.9360	0.9115	0.9153	0.9192	0.9035	0.9008
6	0.9632	0.9479	0.9248	0.9155	0.8915	0.9025	0.9132	0.9045	0.9035
7	0.9688	0.9248	0.9083	0.9050	0.8855	0.8761	0.9181	0.9161	0.9158
8	0.9305	0.9110	0.8928	0.8903	0.8866	0.9096	0.9263	0.9237	0.9247
9	0.9245	0.8985	0.8799	0.8902	0.8766	0.8926	0.9061	0.9079	0.9098
10	0.8890	0.8843	0.8809	0.8907	0.8715	0.8823	0.8937	0.8971	0.8996
11	0.8932	0.8695	0.8777	0.8780	0.8640	0.8776	0.8865	0.8938	0.8955
12	0.8744	0.8581	0.8621	0.8593	0.8666	0.8798	0.8811	0.8852	0.8905
13	0.8551	0.8623	0.8401	0.8469	0.8537	0.8696	0.8678	0.8759	0.8778
14	0.8407	0.8298	0.8202	0.8332	0.8492	0.8669	0.8676	0.8751	0.8802
15	0.8220	0.8171	0.8041	0.8173	0.8430	0.8609	0.8649	0.8750	0.8805
20	0.7449	0.7362	0.7399	0.7625	0.7950	0.8106	0.8316	0.8481	0.8536
25	0.7015	0.7089	0.7146	0.7263	0.7585	0.7847	0.8059	0.8174	0.8270
30	0.6744	0.7118	0.6993	0.7078	0.7419	0.7632	0.7839	0.7996	0.8131

Table 11.10. Exponentiation ratios (NUCOMP / Cantor) over $\mathbb{F}_{2^n}$, real.

	$\log_2 p$								
g	2	4	8	16	32	64	128	256	512
2	0.9277	1.0896	1.0930	1.0854	1.1152	1.0998	1.0653	1.0787	1.0661
3	0.8948	0.9597	0.9860	0.9622	0.9695	0.9791	0.9640	0.9824	0.9814
4	1.0213	1.0360	1.0375	1.0274	1.0267	1.0252	1.0289	1.0421	1.0440
5	0.9587	0.9672	0.9630	0.9505	0.9372	0.9295	0.9499	0.9516	0.9491
6	0.9989	0.9776	0.9743	0.9838	0.9718	0.9715	0.9689	0.9777	0.9790
7	0.9370	0.9193	0.9025	0.9126	0.8990	0.9041	0.9311	0.9413	0.9424
8	0.9534	0.9439	0.9222	0.9379	0.9365	0.9476	0.9650	0.9785	0.9842
9	0.9008	0.8771	0.8685	0.8928	0.8707	0.8727	0.8891	0.8954	0.8963
10	0.9053	0.8863	0.8854	0.9142	0.9098	0.9115	0.9252	0.9384	0.9491
11	0.8601	0.8518	0.8504	0.8713	0.8624	0.8595	0.8755	0.8838	0.8870
12	0.8878	0.8679	0.8589	0.8705	0.8938	0.9006	0.9154	0.9220	0.9301
13	0.8377	0.8230	0.8171	0.8281	0.8478	0.8476	0.8675	0.8729	0.8770
14	0.8393	0.8258	0.8206	0.8384	0.8659	0.8783	0.8863	0.8957	0.9031
15	0.7970	0.7775	0.7800	0.7942	0.8204	0.8423	0.8548	0.8594	0.8659
20	0.7221	0.7313	0.7312	0.7552	0.7968	0.8291	0.8311	0.8548	0.8638
25	0.6565	0.6298	0.6678	0.6954	0.7907	0.7356	0.7520	0.7756	0.8010
30	0.6576	0.6649	0.6722	0.6936	0.7353	0.7663	0.7823	0.8043	0.8187

finite field was chosen so that the size of the Jacobian (approximately q^g where the finite field has q elements) was roughly 2^{160}, 2^{224}, 2^{256}, 2^{384}, and 2^{512}. Assuming only generic attacks with square root complexity, these curves offer 80, 112, 128, 192, and 256 bits of security for cryptographic

protocols based on the corresponding discrete logarithm problem. NIST [9] currently recommends these five levels of security for key establishment in U.S. Government applications. Although the use of curves with genus 3 and larger for cryptographic purposes is questionable, we nevertheless included times for higher genus as our main goal is to provide a relative comparison between our formulation of NUCOMP with Cantor's algorithm.

For curves defined over $\mathbb{F}_p$, we chose a random prime p of appropriate length such that p^g had the required bit length, and for curves over $\mathbb{F}_{2^n}$ we chose the minimal value of n with gn greater than or equal to the required bit length. For each genus and finite field, we randomly selected 2000 curves and executed Diffie–Hellman key exchange twice for each curve, once using Cantor's algorithm and once using our version of NUCOMP (Algorithm 9.1). We used Algorithm 9.1 as opposed to Algorithm 9.2, because our previous experiments indicated that it is more efficient for low genus curves. The random exponents used had $160, 224, 256, 384$, and 512 bits, respectively, ensuring that the number of bits of security corresponds to the five levels recommended by NIST (again, considering only generic attacks). In order to provide a fair comparison, the same sequence of random exponents was used for each run of the key exchange protocol.

Table 11.11 contains the average CPU time in seconds for each version of the protocol using real and imaginary curves over $\mathbb{F}_p$ and $\mathbb{F}_{2^n}$. The columns labeled "Cantor" contain the runtimes when using Cantor's algorithm, and those labeled "NC" the runtimes when using NUCOMP. The times for any precomputations, as described in [7], are not included. We also give the ratios of the average time spent for key exchange using NUCOMP versus that using Cantor's algorithm in Table 11.12. Clearly, in almost all cases, NUCOMP offers a fairly significant performance improvement as opposed to Cantor's algorithm, even for genus as low as 2.

12. Conclusions

Our results indicate that NUCOMP does provide an improvement for divisor arithmetic in hyperelliptic curves except for the smallest examples in terms of genus and finite field size. They also show that both versions of NUCOMP, Algorithm 9.1 and Algorithm 9.2, are useful. Nevertheless, a careful complexity analysis and further numerical experiments are required to compare NUCOMP and Cantor's algorithm more precisely.

There are a number of possible improvements to NUCOMP that need to be investigated. For example, our remarks at the end of Sec. 8 indicate that basis normalization need not be done when NUCOMP is used as a

Table 11.11. Key exchange timings over $\mathbb{F}_p$ and $\mathbb{F}_{2^n}$ (in seconds).

Security level (in bits)	g	$\mathbb{F}_p$				$\mathbb{F}_{2^n}$			
		Imaginary		Real		Imaginary		Real	
		Cantor	NC	Cantor	NC	Cantor	NC	Cantor	NC
80	2	0.0322	0.0290	0.0324	0.0306	0.0320	0.0282	0.0282	0.0291
	3	0.0382	0.0350	0.0390	0.0363	0.0342	0.0320	0.0322	0.0317
	4	0.0492	0.0438	0.0487	0.0438	0.0443	0.0404	0.0403	0.0382
	5	0.0466	0.0435	0.0483	0.0444	0.0611	0.0601	0.0560	0.0563
	6	0.0124	0.0124	0.0123	0.0122	0.0737	0.0705	0.0667	0.0658
112	2	0.0562	0.0498	0.0554	0.0520	0.0585	0.0505	0.0511	0.0522
	3	0.0737	0.0649	0.0707	0.0660	0.0692	0.0627	0.0624	0.0636
	4	0.0723	0.0651	0.0730	0.0648	0.0691	0.0630	0.0622	0.0598
	5	0.0938	0.0875	0.0937	0.0867	0.0846	0.0822	0.0776	0.0781
	6	0.1182	0.1076	0.1171	0.1048	0.1032	0.0977	0.0946	0.0919
128	2	0.0667	0.0593	0.0663	0.0625	0.0692	0.0594	0.0598	0.0611
	3	0.0870	0.0771	0.0847	0.0790	0.0807	0.0732	0.0730	0.0734
	4	0.0904	0.0806	0.0906	0.0806	0.0791	0.0723	0.0697	0.0667
	5	0.1129	0.1044	0.1124	0.1037	0.0989	0.0957	0.0899	0.0909
	6	0.1354	0.1224	0.1318	0.1181	0.1192	0.1129	0.1090	0.1063
192	2	0.1439	0.1235	0.1375	0.1290	0.1620	0.1348	0.1369	0.1395
	3	0.1617	0.1436	0.1577	0.1480	0.1652	0.1484	0.1472	0.1486
	4	0.1832	0.1609	0.1793	0.1615	0.1743	0.1642	0.1537	0.1505
	5	0.2313	0.2114	0.2210	0.2069	0.2190	0.2147	0.1964	0.1985
	6	0.2247	0.2053	0.2242	0.2019	0.1912	0.1795	0.1726	0.1677
256	2	0.2517	0.2127	0.2303	0.2182	0.3037	0.2556	0.2540	0.2593
	3	0.2920	0.2538	0.2825	0.2633	0.3417	0.3129	0.3025	0.3106
	4	0.2875	0.2537	0.2771	0.2505	0.3015	0.2815	0.2664	0.2622
	5	0.3662	0.3375	0.3557	0.3341	0.3693	0.3599	0.3338	0.3344
	6	0.3968	0.3577	0.3792	0.3446	0.3555	0.3456	0.3185	0.3120

Table 11.12. Key exchange ratios over $\mathbb{F}_p$ and $\mathbb{F}_{2^n}$.

	g	Security level				
		80	112	128	192	256
$\mathbb{F}_p$ imaginary	2	0.8999	0.8869	0.8890	0.8585	0.8454
	3	0.9153	0.8804	0.8866	0.8882	0.8693
	4	0.8916	0.9004	0.8919	0.8781	0.8825
	5	0.9329	0.9332	0.9242	0.9140	0.9214
	6	0.9984	0.9102	0.9038	0.9135	0.9015
$\mathbb{F}_p$ real	2	0.9435	0.9383	0.9429	0.9383	0.9477
	3	0.9305	0.9342	0.9323	0.9384	0.9321
	4	0.9000	0.8867	0.8895	0.9008	0.9041
	5	0.9197	0.9255	0.9229	0.9363	0.9391
	6	0.9905	0.8947	0.8961	0.9007	0.9088
$\mathbb{F}_{2^n}$ imaginary	2	0.8800	0.8621	0.8579	0.8320	0.8417
	3	0.9364	0.9066	0.9074	0.8984	0.9157
	4	0.9132	0.9125	0.9144	0.9420	0.9336
	5	0.9829	0.9718	0.9677	0.9803	0.9744
	6	0.9558	0.9467	0.9475	0.9388	0.9722
$\mathbb{F}_{2^n}$ real	2	1.0334	1.0222	1.0225	1.0190	1.0206
	3	0.9855	1.0181	1.0067	1.0097	1.0270
	4	0.9493	0.9616	0.9567	0.9796	0.9840
	5	1.0046	1.0065	1.0112	1.0106	1.0016
	6	0.9870	0.9707	0.9753	0.9717	0.9796

component for binary exponentiation, because the degree of $\hat{P}$ will generally be at most $g + 1$ at the end of NUCOMP. Not performing normalization saves one division with remainder at the cost of the inputs to subsequent applications of NUCOMP having slightly larger degrees. In addition, the results in Sec. 10 indicate that in some cases, it is possible to perform one extra NUCOMP step to guarantee that the output of NUCOMP is reduced without having to perform a continued fraction step. Further investigation and analysis is required to determine which of these options is the most efficient in practice.

Our data also indicate that using NUCOMP is more efficient than Cantor's algorithm for cryptographic key exchange using low genus hyperelliptic curves, for both imaginary and real models, However, explicit formulas based on Cantor's algorithm have been developed for divisor arithmetic on curves of genus $2, 3$, and 4 (see [5] for a partial survey and references). NUCOMP, as presented in this paper, is generic in the sense that it works for any genus and as such does not compete in terms of performance with these explicit formulas. Given that NUCOMP out-performs Cantor's algorithm, it is conceivable that some of the ideas used in NUCOMP can be applied to improve the explicit formulas. This, as well as the open problems mentioned above, is the subject of on-going research.

References

[1] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen. *Math. Zeitschr.* **19** (1924), 153–206.
[2] D. G. Cantor, Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.* **48** (1987), 95–101.
[3] A. Enge, How to distinguish hyperelliptic curves in even characteristic. *Public-Key Cryptography and Computational Number Theory*. De Gruyter (Berlin), 2001, 49–58.
[4] H. Hasse, *Algebraic Number Theory*, Springer, Berlin 2002.
[5] M. J. Jacobson, Jr., A. J. Menezes, and A. Stein, Hyperelliptic curves and cryptography, in *High Primes and Misdemeanors: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Inst. Comm. **41**, American Mathematical Society, 2004, 255–282.
[6] M. J. Jacobson., Jr. and A. J. van der Poorten, Computational aspects of NUCOMP, *Proc. ANTS-V, Lect. Notes Comp. Sci.* **2369**, Springer (New York), 2002, 120–133.
[7] M. J. Jacobson, Jr., R. Scheidler, and A. Stein, Cryptographic protocols on real and imaginary hyperelliptic curves, submitted to *Advances Math. Comm.*, 2006.
[8] M. J. Jacobson, Jr., R. Scheidler and H. C. Williams, An improved real quadratic field based key exchange procedure. *J. Cryptology* **19** (2006), 211–239.
[9] National Institute of Standards and Technology (NIST), *Recommendation on key establishment schemes*, NIST Special Publication 800-56, January 2003.
[10] S. Paulus and H.-G. Rück, Real and imaginary quadratic representations of hyperelliptic function fields, *Math. Comp.* **68** (1999), 1233–1241.
[11] A. J. van der Poorten, A note on NUCOMP. *Math. Comp.* **72** (2003), 1935–1946.
[12] M. Rosen, *Number Theory in Function Fields*, Springer, New York 2002.
[13] D. Shanks, On Gauss and composition I, II. In *Proc. NATO ASI on Number Theory and Applications*, Kluwer Academic Press 1989, 163–204.

[14] V. Shoup, NTL: A library for doing number theory. Software, 2001. Available at `http://www.shoup.net.ntl`.
[15] A. Stein. Sharp upper bounds for arithmetics in hyperelliptic function fields. *J. Ramanujan Math. Soc.* **16** (2001), 1–86.
[16] A. Stein and H. C. Williams, Some methods for evaluating the regulator of a real quadratic function field. *Experiment. Math.* **8** (1999), 119–133.
[17] H. Stichtenoth, *Algebraic Function Fields and Codes*. Springer, Berlin 1993.