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
Mathematics, Dept. 3036, University of Wyoming,
PO Box 3036, 1000 E. University Avenue, Laramie, WY 82071-3036, USA
E-mail: 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 Ref. 5).

Cantor's algorithm 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 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 Ref. 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 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 Refs. 11 and 6, are based on the arithmetic of binary quadratic forms. In Ref. 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. We generalize the results in Ref. 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 Ref. 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 Ref. 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

\[ s_0 + \frac{1}{s_1 + \frac{1}{s_2 + \ldots + \frac{1}{s_n + \frac{1}{\alpha_{n+1}}}}} \]

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 \(k(t^{-1})\) of Puiseux series in \(t^{-1}\); that is, any non-zero element in \(k(t^{-1})\) 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

\[ [\alpha] = \sum_{i=0}^{d} a_i t^i, \quad \text{sgn}(\alpha) = a_d, \quad \text{deg}(\alpha) = d. \]  \hspace{1cm} (2.1)

Also, define \([0] = 0\) and \(\text{deg}(0) = -\infty\).

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

\[ \alpha = [s_0, s_1, \ldots, s_n, \alpha_{n+1}] \]  \hspace{1cm} (2.2)

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

\[
\begin{align*}
A_{-2} &= 0, & A_{-1} &= 1, & A_i &= s_i A_{i-1} + A_{i-2}, \\
B_{-2} &= 1, & B_{-1} &= 0, & B_i &= s_i B_{i-1} + B_{i-2},
\end{align*}
\]  \hspace{1cm} (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 \(A_i B_{i-1} - A_{i-1} B_i = (-1)^i\) 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 \(q_i = [\alpha_i]\) for \(i \geq 0\), then Eq. (2.2) is the well-known \(\text{regular}\) continued fraction expansion of \(\alpha\). Here, the partial quotients \(q_0, q_1, \ldots\)
are uniquely determined by \( \alpha \), 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 \( \alpha \). This term is motivated by the well-known inequalities

\[
\deg \left( \alpha - \frac{A_i}{B_i} \right) \leq -\deg(B_iB_{i+1}) < -2\deg(B_i)
\]

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

**Lemma 2.1.** Let \( \alpha \in k\{t^{-1}\} \), \( E, F \in k[t] \) 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 \( \alpha \).

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 “\( \hat{\cdot} \)” 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 \( \alpha \in k\{t^{-1}\} \) 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 \( \hat{q}_{i} = [r_{i-2}/r_{i-1}] \) 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 \( \alpha \) and \( \hat{\alpha} \) are equal.

**Proof.** Let \( \alpha = [q_0, q_1, \ldots, q_m, \ldots] \) be the regular continued fraction expansion of \( \alpha \). 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 \( \alpha \) 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 $\hat{q}_0 = |\alpha| = |\hat{\alpha}| = \hat{q}_0$.

Assume now inductively that $2 \deg(\hat{r}_{n-1}) > \deg(F^2(\alpha - \hat{\alpha}))$ implies $\hat{q}_i = \hat{q}_i$ for $0 \leq i \leq n$ and suppose that $2 \deg(\hat{r}_n) > \deg(F^2(\alpha - \hat{\alpha}))$. Since the $r_i$ are decreasing in degree for $-1 \leq i \leq m$, we have $2 \deg(\hat{r}_{n-1}) > 2 \deg(\hat{r}_n) > \deg(F^2(\alpha - \hat{\alpha}))$, so $\hat{q}_i = \hat{q}_i$ for $0 \leq i \leq n$ 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 $-2 \leq i \leq m$, so by assumption and Eq. (2.4),

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

It follows again from Eq. (2.4) that

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

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 $j \geq 0$. If $j < n + 1$, then $[\hat{q}_{j+1}, \ldots, \hat{q}_{n+1}] = 0$ 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 $m \geq 0$ 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 $\hat{q}_i = [\hat{\phi}_i]$ for $i \geq 0$. This continued fraction expansion corresponds to the Euclidean algorithm applied to $E$ and $F$. We define

$$b_{-1} = E, \ b_0 = F, \ b_{i+1} = b_{i-1} - \hat{q}_i b_i, \ a_{-1} = 0, \ a_0 = -1, \ a_{i+1} = a_{i-1} - \hat{q}_i a_i ,$$

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

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

and the $b_i$ strictly decrease in degree for $-1 \leq i \leq m+1$. 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 $0 \leq i \leq m$. The quantities $\hat{A}_i, \hat{B}_i$ can be computed recursively by

$$\hat{A}_{-2} = 0, \ \hat{A}_{-1} = 1, \ \hat{A}_i = \hat{q}_i \hat{A}_{i-1} + \hat{A}_{i-2} \quad (0 \leq i \leq m) ,$$

$$\hat{B}_{-2} = 1, \ \hat{B}_{-1} = 0, \ \hat{B}_i = \hat{q}_i \hat{B}_{i-1} + \hat{B}_{i-2} \quad (0 \leq i \leq m) .$$


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

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

We require the following basic degree properties later on:

**Lemma 2.2.**

(a) $\deg(b_i) = \deg(b_{i-1}) - \deg(\tilde{q}_i) \leq \deg(b_{i-1}) - 1 \quad (0 \leq i \leq m).$

(b) $\deg(a_i) = \deg(a_{i-1}) + \deg(\tilde{q}_{i-1}) \geq \deg(a_{i-1}) + 1 \quad (1 \leq i \leq m + 1).$

(c) $\deg(b_i) \leq \deg(b_{-1}) - i - 1 \quad (-1 \leq i \leq m + 1).$

(d) $\deg(a_i) \geq i \quad (0 \leq i \leq m + 1).$

(e) $\deg(a_i) + \deg(b_{i-1}) = \deg(b_{-1}) \quad (0 \leq i \leq m + 1).$

**Proof.** Since $\deg(\tilde{q}_i) \geq 1$ for $0 \leq i \leq m$ 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 Refs. 12, 17, and 4, as opposed to a more geometric treatment. Let $k$ be a finite field of order $q$. Following Ref. 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, 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

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

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 hyperelliptic curve does have singularities at infinity if it is not elliptic, i.e. $g \geq 2$
8

(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 $\sgn(f)$ 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 $\sgn(f)$ 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 $k(C)_S$ 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,

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

where $k' = k(\sgn(v))$ 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 $k(u^{-1})$. 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

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

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 $\alpha$. 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 $D = \sum_p \nu_p(D)p$ where $p$ runs through all the places of $k(C)$ and $\nu_p(D) = 0$ for all but finitely many places $p$. The **support** $\text{supp}(D)$ of $D$ is the set of places for which $\nu_p(D) \neq 0$, and the **degree** of $D$ is $\deg(D) = \sum_p \nu_p(D)\deg(p)$; 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 uniquely written as a sum of two divisors

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

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

---

\(^b\)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 \( D \) denote the group of divisors of \( k(C) \), \( D^0 \) the subgroup of \( D \) of degree 0 divisors of \( k(C) \), and \( P \) the subgroup of \( D^0 \) of principal divisors of \( k(C) \), where we write the principal divisor of any \( \alpha \in k(C)^* \) as \( \text{div}(\alpha) \). Then the degree 0 divisor class group \( \text{Pic}^0 = D^0/P \) 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 \( D, D^0, P \), and hence to \( \text{Pic}^0 \). Note that \( N(D) = N(\overline{D}) \) and \( D + \overline{D} = \text{div}(N(D)) \) for any degree 0 divisor \( D \).

Define \( D_S = \{ D_S \mid D \in D \} \), \( D^S = \{ D^S \mid D \in D \} \), \( P_S = P \cap D_S \), and \( P^S = P \cap D^S \). By Proposition 14.1, p. 243, of Ref. 12, there are exact sequences

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

\[
(0) \to (D^S \cap D^0)/P^S \to \text{Pic}^0 \to D_S/P_S \to \mathbb{Z}/f\mathbb{Z} \to (0), \tag{3.3}
\]

where \( f = \gcd(\deg(p) \mid p \in S) \), so \( f = 2 \) if \( C \) is unusual and \( f = 1 \) otherwise. If \( C \) is imaginary or unusual, then \( D^S \cap D^0 = P^S = 0 \), whereas if \( C \) is real, then \( D^S \cap D^0 = \langle \infty_1 - \infty_2 \rangle \) and \( P^S = \langle R(\infty_1 - \infty_2) \rangle \), where \( R \) is the order of the divisor class of \( \infty_1 - \infty_2 \) in \( \text{Pic}^0 \) 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 \( k[C]-\text{ideal} \) is a subset \( I \) of \( k(C) \) such that \( df \) is a \( k[C]-\text{ideal} \) for some non-zero \( d \in k[u] \). Let \( I \) denote the group of non-zero fractional \( k[C]-\text{ideals} \), \( H \) the subgroup of \( I \) of non-zero principal fractional \( k[C]-\text{ideals} \) (which we write as \( (\alpha) \) for \( \alpha \in k(C)^* \)), \( C = I/H \) the ideal class group of \( k(C) \), and \( h' = |C| \) the ideal class number of \( k(C) \). There is a natural isomorphism

\[
\Phi : D_S \to I, \quad D_S \mapsto \{ \alpha \in k(C)^* \mid \text{div}(\alpha)_S \geq D_S \} \tag{3.4}
\]

with inverse

\[
\Phi^{-1} : I \to D_S
\]

\[
f \mapsto D_S = \sum_{p \in S} m_p p \quad \text{where} \quad m_p = \min\{\nu_p(\alpha) \mid \alpha \in f \text{ non-zero}\}.
\]
The conjugate $\overline{f}$ of a fractional ideal $f$ is the image of $f$ under the conjugation map. If $f$ is non-zero, then the norm $N(f)$ of $f$ is simply $N(\Phi^{-1}(f))$, the norm of the finite divisor corresponding to $f$ under $\Phi^{-1}$, with $\Phi$ given by Eq. (3.4). Note that $\overline{f}$ is the principal fraction ideal generated by $N(f)$.

The isomorphism $\Phi$ extends to an isomorphism from the factor group $D_S/P_S$ onto the ideal class group $C$ (see p. 401 of Ref. 4 and Theorem 14.5, p. 247, of Ref. 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 $\Phi$ in Eq. (3.4) can further be extended to the group $D^0$, 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 $D^0 \rightarrow \mathcal{I}$.

### 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, $\Phi$ as given in Eq. (3.4) extends to an isomorphism from the subgroup of $D^0$ 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, $\Phi$ extends to an isomorphism from the subgroup of $D^0$ 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 \( C \), its order \( h' \), and the regulator \( R \) depend on the model of \( C \) (imaginary, unusual, or real), whereas the genus \( g \), the divisor groups \( D \), \( D^0 \) and \( P \), 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 Refs. 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 \(^*\) if there does not exist any subset \( U \subseteq \text{supp}(D_S) \) such that \( \sum_{p \in U} \nu_p(D_S)p \) 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 \( \Phi \), and refer to the polynomials \( Q \) and \( P \) as a basis of \( D_S \); note that \( N(D_S) = N(\mathfrak{a}) = \text{sgn}(Q)^{-1}Q \). 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

\(^*\)For geometric and ideal-independent definitions of the notions of semi-reduced and reduced divisors, see for example Refs. 2 or 5.
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 divisor classes, so we will have to allow divisors \( D \) with \( \deg(D_S) = g + 1 \) when representing elements in \( \text{Pic}^0 \). For simplicity, we will say that a degree 0 divisor \( D \) in a given class \( C \in \text{Pic}^0 \) has minimal norm if \( D \) is semi-reduced and \( \deg(N(E)) \geq \deg(N(D)) \) for every semi-reduced divisor \( E \in C \). 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 Ref. 2), and every degree 0 divisor class in \( \text{Pic}^0 \), and hence every ideal class in \( C \), 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 Ref. 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 identify a distinguished divisor of minimal norm in a given degree 0 divisor class are required.

### 4.3. Real Curves

By Proposition 4.1 of Ref. 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

---

\(^d\)The proposition as stated in Ref. 10 reads \( 0 \leq \nu_1(D) \leq g - \deg(D_S) \). The correct statement is \( 0 \leq \deg(D_S) + \nu_1(D) \leq g \).
in Pic\(^0\) is somewhat slower than 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.

Rather than examining degree 0 divisor classes, we now consider ideal classes of \(k(C)\). Recall that the isomorphism \(\Phi\) 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 \(\infty_1\) corresponding to \(\mathfrak{f}\); note that \(\mathfrak{f}\) is reduced if and only if \(D(\mathfrak{f})\) is reduced. Let \(C\) be any ideal class of \(k(C)\), and define the set \(R_C = \{D(a) \mid a \in C \text{ reduced}\}\).

By our above remarks, all the divisors in \(R_C\) 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, \(R_C\) is a finite set.

We now fix any reduced ideal \(a \in C\); for example, if \(C\) is the principal ideal class, then we always chose \(a = (1)\) to be the trivial ideal. Then for every \(b \in C\), there exists \(\alpha \in k(C)^*\) with \(b = (\alpha)a\); if \(a = (1)\), then \(\alpha\) is in fact a generator of \(b\). By multiplying \(\alpha\) 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 \(D(b)\) (with respect to \(D(a)\)) to be \(\delta(D(b)) = \deg(\alpha)\). It follows that the set \(R_C\) is ordered by distance, and if we set \(D_1 = D(a)\) and \(r_C = \#R_C\), then we can write

\[R_C = \{D_1, D_2, \ldots, D_{r_C}\}\]

and \(\delta_i = \delta(D_i)\), with \(0 = \delta_1 < \delta_2 < \cdots < \delta_{r_C} < R\). The set \(R_C\) is called the infrastructure of \(C\); we will motivate this term later on. Note that for any \(b \in C\), \(D(b)\) and \(D(\overline{b})\) both belong to \(R_C\), since \(b\) and \(\overline{b}\) are equivalent, and \(\delta(D(\overline{b})) = R + \deg(D(b)_S) - \delta(D(b))\) if \(b\) 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
\begin{equation}
S_{i+1} = \frac{f + hR_i - R_i^2}{S_i}, \quad R_{i+1} = h - R_i + \frac{R_i - h}{S_i} S_{i+1},
\end{equation}
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 $s_1 = [(R_0 - h)/S_1]$. Then for $i \in \mathbb{N}$:
\begin{equation}
S_{i+1} = S_{i-1} + s_i(R_{i-1} - R_i), \quad s_{i+1} = \frac{R_i - h}{S_{i+1}},
\end{equation}
\[ R_{i+1} = h - R_i + s_{i+1} S_{i+1} \equiv h - R_i \pmod{S_{i+1}}. \]
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 Refs. 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 $j \leq [\deg(S_0) - g]/2$ if $\deg(S_j) \leq g$ and $j \leq [\deg(S_0) - g - 1]/2$ 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{equation}
\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{equation}
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 $\text{sgn}(f)$, 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) ≤ 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) ≤ 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) ≤ 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 Ref. 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) ≤ 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 ∈ F_q where

\[ R_a = h − R + aS, \quad S_a = \frac{f + hR_a - R_a^2}{S}. \]  \hspace{1cm} (5.4)

Proof. Since E_a = E + div((R_a+v)/S) for all a ∈ F_q, all E_a are equivalent to E. Furthermore, deg(R_a) ≤ g + 1 and hence deg(S_a) = g + 1, since the conditions on sgn(f) prevent cancellation of leading terms in the numerator of S_a. So it only remains to show that E 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 ∈ F_q and suppose that E_a = E or E_a = E_b for some b ∈ F_q \{a\}. We first claim that

S_a and S differ by a constant factor in F_q. \hspace{1cm} (5.5)

This is clear if E_a = E, so suppose E_a = E_b with b ∈ F_q, b ≠ a. Then S_a and S_b differ by a constant factor, and R_a ≡ R_b (mod S_a). By Eq. (5.4), R_a ≡ R_b (mod 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 F_q.

Next, we claim that

S divides 2R − h. \hspace{1cm} (5.6)

If E_a = E, then R ≡ R_a (mod S). On the other hand, R_a ≡ h − R (mod S) by Eq. (5.4), so R ≡ h − R (mod S), proving Eq. (5.6). Suppose now that E_a = E_b for some b ∈ 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 \( R_a = R + c_aS \). Substituting into Eq. (5.4) yields \( SS_a = f + hR - R^2 + c_aS(h - 2R - c_aS) \). 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 \( f' + hR' + R'(h - 2R) \), 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

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

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 \( \phi_0 \) 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 \( a_i \). The operation \( D_i \rightarrow D_{i+1} \) is referred to as a baby or reduction step.

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

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

Then $a_{i+1} = (\overline{\phi}_i^{-1})a_i$, and hence $a_i = (\overline{\theta}_i)a_1$, for $i \in \mathbb{N}$. Therefore, the ideals $a_i$ are all equivalent, so baby steps preserve ideal equivalence.

If we choose $s_i$ in Eq. (5.9) to be $s_i = q_i = [\phi_i]$, i.e. the quotient in the regular continued fraction expansion of $\phi_0$ in $k(C)$, then we have the baby steps

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

If $\deg(Q_i) > \deg(v)$, then $q_i = [P_i/Q_i]$. 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

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

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 $i \geq j$, $q_i \neq [P_j/Q_j]$, 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 $\deg(P_{i+1} - h - v) \leq g$, $\deg(P_{j+1} + v) = g + 1$, 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

$$q_i = \left\lfloor \frac{P_i + e_i v}{Q_i} \right\rfloor, \quad e_i = \begin{cases} 1 & \text{if } C \text{ real, } \deg(Q_i) = g + 1, \\ 0 & \text{otherwise}, \end{cases}$$

$$P_{i+1} = h - P_i + q_i Q_i, \quad Q_{i+1} = \frac{f + h P_{i+1} - P_{i+1}^2}{Q_i} .$$

(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 \( i \in \mathbb{N} \):

\[
q_i = \left\lceil \frac{P_i + [e_i v]}{Q_i} \right\rceil, \quad r_i \equiv P_i + [e_i v] \pmod{Q_i},
\]

\[
P_{i+1} = h + [e_i v] - r_i, \quad Q_{i+1} = Q_{i-1} + q_i(r_i - r_{i-1}).
\] (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 \( P_i + [e_i v] = q_i Q_i + r_i \) 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 \( D_1 = D(a) \) for some reduced ideal \( a \) of \( k(C) \), then we can generate the entire infrastructure \( \mathcal{R}_C = \{ D_i \mid 1 \leq i \leq r_C \} \) of the ideal class \( C \) containing \( a \). Here, \( D_i = D(a_i) \) where \( a_i = (\overline{a}_i) a \) with \( \overline{a}_i \) as in Eq. (5.10), so the distance of \( D_i \) is \( \delta_i = \deg(\overline{a}_i) \). In particular, \( \overline{a}_{r_C} \) is a fundamental unit of \( k(C) \) of positive degree, and \( \deg(\overline{a}_{r_C}) = R \) 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

\[
\delta_i = \deg(\overline{a}_i) = \deg(Q_{i-1}) - \deg(Q_0) + \sum_{j=1}^{i-1} \deg(q_j)
\] (5.15)

for \( i \in \mathbb{N} \). Since \( \overline{a}_i = (P_i - h - v)/Q_i = -Q_{i-1}/(P_i + v) \) and \( \delta_{i+1} - \delta_i = -\deg(\overline{a}_i) = \deg(P_i + v) - \deg(Q_{i-1}) = g + 1 - \deg(Q_{i-1}) \) 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 \( C \) 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.

\[
S = \gcd(Q', Q'', P' + P'' - h) = VQ' + WQ'' + X(P' + P'' - h),
\]

\[
Q = \frac{Q'Q''}{S^2},
\] (6.1)

\[
P = P'' + U \frac{Q''}{S} \quad \text{with} \quad U \equiv W(P' - P'') + XR'' \pmod{Q'/S},
\]
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 \( (D', D'') \rightarrow D' \oplus D'' \) 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 Ref. 2. Thus, the group operation on \( \text{Pic}^0 \) 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 \( \text{Pic}^0 \) via these distinguished representatives plus reduced representatives if they exist.

### 6.3. Real Curves

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

\[
\delta(D' \oplus D'') = \delta(D') + \delta(D'') - \delta \quad \text{with} \quad 0 \leq \delta \leq 2g .
\]  

(6.2)

Here, distances in the principal class are taken with respect to \( D_1 = 0 \), and distances in \( C \) with respect to some some suitable first divisor. The “error term” \( \delta \) in Eq. (6.2) is linear in \( g \) and hence very small compared to the two distances \( \delta(D') \) and \( \delta(D'') \). The quantity \( \delta \) 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 $l \leq \lceil g/2 \rceil$ 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 $D_{i+1} = (Q_i, P_i)$, $0 \leq i \leq l$, 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 $\phi$, one computes sequences of polynomials $a_i, b_i, c_i, d_i$ such that

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

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 $a_n, b_n, c_n, d_n$ 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 $Q'/\langle SU \rangle = [q_1, q_2, \ldots, q_{n+1}, \ldots]$. Note that $\deg(U) < \deg(Q'/\langle SU \rangle) \leq g$ (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 $Q'/\langle SU \rangle$ 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 $\text{sgn}(P'') \in k$ and $\text{sgn}(v) \notin k$ 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.

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

If $C$ is unusual, $g$ is odd, and $\deg(Q) = g + 1$, 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.
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 $\hat{D}_1 = (\hat{Q}_{i-1}, \hat{P}_{i-1})$, $1 \leq i \leq m + 3$, obtained by choosing $s_i = \hat{q}_{i-1}$ in Eq. (5.9). That is

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

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

$$c_{-1} = \frac{Q''}{S}, \quad c_0 = \frac{P - P''}{b_{-1}}, \quad c_{i+1} = c_{i-1} - \hat{q}_i c_i,$$

$$d_{-1} = P' + P'' - h, \quad d_0 = \frac{d_{-1} b_0 - SR''}{b_{-1}}, \quad d_{i+1} = d_{i-1} - \hat{q}_i d_i,$$

(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 the two sequences. An easy induction yields

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

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

(7.7)

(7.8)

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

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

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

(7.9)

(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 $\hat{P}_0, \hat{Q}_0$, 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
\[ D_{i+1} = D_i r_{i+1}, \text{ for } 0 \leq i \leq n + 2 \] (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 \( P_0 = P_0 = P \), \( Q_0 = Q_0 = Q \), 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 \( \text{deg}(b_n) > N \), with \( N \) as in Eq. (7.3). Furthermore,

\[
\begin{align*}
q_i &= \hat{q}_{i-1} \quad (0 \leq i \leq n + 1), \\
\hat{P}_i &= \hat{P}_i \quad (0 \leq i \leq n + 2), \\
\hat{Q}_i &= \hat{Q}_i \quad (0 \leq i \leq n + 2).
\end{align*}
\]

**Proof.** We already observed that \( \text{deg}(b_{-1}) = \text{deg}(Q'/S) > N \), so since \( \text{deg}(b_i) \) decreases as \( i \) increases, there must exist \( n \geq -1 \) with \( \text{deg}(b_n) > N \). Since \( \text{deg}(b_{m+1}) = -\infty < N \), we must have \( n \leq m \). 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 \( q_i = \hat{p}_i/\hat{q}_i \) is the continued fraction expansion of \( \phi \) in a suitable field of Puiseux series; also, recall that \( \hat{\phi} = [\hat{q}_{i-1}, \hat{q}_0, \ldots, \hat{q}_m] \) where \( \hat{q}_{-1} = 0 \). We wish to apply\(^8\) Theorem 2.1 to \( \phi \) and \( \hat{\phi} \). Since \( \phi - \hat{\phi} = (P' + v)/Q \), we have \( \hat{b}_{i-1}^2 (\phi - \hat{\phi}) = Q' (P'' + v)/Q'' \). The definition of \( N \) implies \( 2N \geq \text{deg}(Q' (P'' + v)/Q'') \), so

\[
2 \text{deg}(b_n) > 2N \geq \text{deg} \left( \hat{b}_{i-1}^2 (\phi - \hat{\phi}) \right). \tag{7.11}
\]

Set\(^b\) \( \hat{r}_{-2} = U, \hat{r}_{-1} = Q'/S, \) and \( \hat{r}_i = \hat{r}_{i-2} - \hat{q}_{i-1} \hat{r}_{i-1} \) for \( 0 \leq i \leq m + 1 \). Then \( \hat{r}_i = b_i \) for \( -1 \leq i \leq m + 1 \), 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 \( 0 \leq i \leq n + 1 \). Now \( P_0 = P_0, Q_0 = Q_0, \) and

\(^8\)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.

\(^b\)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 \( \phi = [q_0, q_1, \ldots, q_m] \).
inductively by Eq. (5.11) and Eq. (7.5),

\[ P_{i+1} = h - P_i + q_i Q_i = h - \hat{P}_i + \hat{q}_{i-1} \hat{Q}_i = \hat{P}_{i+1} , \]

\[ Q_{i+1} = \frac{f + hP_{i+1} - P_{i+1}^2}{Q_i} = \frac{f + h\hat{P}_{i+1} - \hat{P}_{i+1}^2}{\hat{Q}_i} = \hat{Q}_{i+1} , \]

for \( 0 \leq i \leq n+1 \).

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

Since \( \text{deg}(b_i) \) 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

\[ \text{deg}(b_n) > N \geq \text{deg}(b_{n+1}) , \]  

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

\[ \hat{Q}_{i+1} = \left( -1 \right)^{i+1} \left( \frac{Q''}{b_{i-1}} \left( \frac{Q''}{b_{i-1}} + (h - 2P''a_{i-1}b_{i-1}) - SR''a_{i-1}^2 \right) \right) \]  

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

\[ u_i = \frac{Q''}{b_{i-1}S} \]  

\[ v_i = \frac{h - 2P''a_{i-1}b_i}{b_{i-1}} \]  

\[ w_i = \frac{SR''a_{i-1}^2}{b_{i-1}} \]  

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

\[ (-1)^{i+1} \hat{Q}_{i+1} = u_i + v_i + w_i \]  

(1 \leq i \leq m + 1) . 

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

\[ L = \text{deg}(Q''R'') = \text{deg}(f + hP'' - P''^2) = \text{deg}(P'' + v) + \text{deg}(P'' - h - v) . \]  

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

\[
\deg(v_i) = \deg(a_i) + \deg(b_i) + \deg(h - 2P'') - \deg(b_{-1}) = \deg(a_i) - \deg(a_{i+1}) + \deg(h - 2P'') \leq -1 + (g + 1) = g
\]

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

\[
\deg(w_i) = 2 \deg(a_i) + \deg(S) + \deg(R'') - \deg(b_{-1}) = \deg(b_{-1}) - 2 \deg(b_{i-1}) + \deg(S) + L - \deg(Q'') = L - \deg(u_{i-1})
\]

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

\[
\deg(u_i) = 2 \deg(b_i) + \deg(Q''/S) - \deg(b_{-1}) = \deg(Q''/Q') + 2 \deg(b_i) = M - 2N + 2 \deg(b_i)
\]

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),

\[
\deg(w_i) = L - \deg(u_{i-1}) < L - M \leq L - \deg(P'' + v) = \deg(P'' - h - v) .
\]

**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 (1) and (2) immediately follow from Eq. (8.3) as well as parts (a), (c), and (d) of Lemma 8.1. For part (3) 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

\[
q_{n+2} = \left\lfloor \frac{\hat{P}_{n+2} + e_{n+2}v}{Q_{n+2}} \right\rfloor \quad \text{with} \quad e_{n+2} = \begin{cases} 
1 \text{ if } C \text{ is real}, \\
0 \text{ if } C \text{ is imaginary}.
\end{cases}
\]

\[
P_{n+3} = h - \hat{P}_{n+2} + q_{n+2}\hat{Q}_{n+2} \quad \text{and} \quad Q_{n+3} = \frac{f + hP_{n+3} - P_{n+3}^2}{Q_{n+2}}.
\]

(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

\[
K = \deg(Q'') + \deg(Q') - g.
\]

(8.6)

Then we can determine \( D' \oplus D'' \) as follows.

**Proposition 8.1.** Let \( N, n, \) and \( K \) be given by 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 \( D' \oplus D'' = D_{n+3} \) if \( K \) is even. If \( K \) is odd, then \( D' \oplus D'' = D_{n+3} \) and only if \( \deg(Q_{n+2}) \leq g \), 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 (1) and (2) follow immediately from parts (1) and (3) of Corollary 8.1, respectively. For part (3) of the Proposition, we have \( M = \deg(P'' + v) = g + 1 \), so \( D' \oplus D'' = D_{n+3} \) if and only if \( \deg(Q_{n+2}) \leq g \), which by part (3) 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 \( \deg(P_{n+3}) \leq g \), whereas if \( C \) is real, then \( \deg(P_{n+3} - h - v) \leq g \). In either case, \( \deg(Q_{n+3}) \leq 2g + 1 - \deg(Q_{n+2}) = g \) by Eq. (8.5), so \( D_{n+4} \) is reduced.

\[\text{Remark 8.1.} \text{ We note that if } C \text{ is imaginary or real, } \deg(P'' + v) = g + 1, \text{ and } K \text{ as given in Eq. (8.6) is odd, then we will almost always have } D' \odot D'' = D_{n+4}, \text{ i.e. it is very unlikely that } D_{n+3} \text{ is reduced. In fact, under these conditions, if } D_{n+3} \text{ is reduced, then it is easy to show that } \deg(b_{n+1}) \leq N - 1 \text{ and } \deg(b_n) \geq N + 1, \text{ so } \deg(b_n) - \deg(b_{n+1}) \geq 2. \text{ (8.7)}\]

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 \( \delta = \delta(D') + \delta(D'') - \delta(D' \odot D'') \) using NUCOMP in the case where \( C \) is real, let \( a, a', a'' \) be the reduced ideals corresponding to the divisors \( D' \odot D'', D', D'' \), respectively. Then \( a = (S/\bar{a}a'a'') \) where \( \bar{a} = \bar{a}_i \) with \( a_1 = a'a'' \), \( a_i = a \), and \( i = n + 3 \) or \( n + 4 \) by Proposition 8.1. Setting \( d = \deg(S) - \deg(\bar{a}_n + 3) \), we obtain by Eq. (5.10), Eq. (6.1), and Theorem 7.1,

\[
d = \deg(S) - \left( \deg(Q_{n+2}) - \deg(Q_0) + \sum_{j=1}^{n+2} \deg(q_j) \right)
\]

\[
= \deg(Q') + \deg(Q'') - \deg(S) - \deg(\hat{Q}_{n+2}) - \sum_{j=0}^{n} \deg(\hat{q}_j) - \deg(q_{n+2}).
\]

If \( D' \odot D'' = D_{n+3} \), then \( \delta = d \), and if \( D' \odot D'' = D_{n+4} \), then \( \delta = d - \deg(q_{n+3}) \) with \( q_{n+3} = [(P_{n+3} + v)/Q_{n+3}] \), 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 \( D' \odot D'' = D_{n+3} \) 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' ⊕ D'' = D_{n+3} is reduced and n ≤ (g - 4)/2.
(b) If g is odd and C is unusual, then D' ⊕ D'' = D_{n+3} and n ≤ (g - 3)/2.
(c) If g is odd and C is imaginary or real, then D' ⊕ D'' = D_{n+4} and n ≤ (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' ⊕ D'' is reached after at most \([g/2]\) 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' ⊕ 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 \(\hat{P} = P_{n+2}\), 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 \(P_{n+2} = h - P_{n+1} + [P_{n+1}/Q_{n+1}]Q_{n+1}\), 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 $Q$ 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 $S_1 = \gcd(Q', Q'') = V_1Q' + W_1Q''$.

(b) If $S_1 = 1$ THEN $S := S_1 = 1, X := 0, W := W_1, \text{GOTO (d)}$.

(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 $U := W(P' - P'') + XR'' \pmod{b_{-1}}$. 
(2) IF \( \deg(Q') + \deg(Q'') - 2 \deg(S) \leq g + 1 \) THEN // at most one baby step

(a) Put
\[
\hat{Q} := \frac{QQ''}{S^2}, \quad \hat{P} := P' + U Q'' (\mod Q), \quad \hat{R} := \frac{f + hP - P^2}{Q}.
\]

(b) IF \( \deg(\hat{Q}) = g + 1 \) AND \( C \) is imaginary THEN
\[
\hat{Q} := \hat{R}, \quad \hat{P} := h - \hat{P} (\mod \hat{Q}), \quad \hat{R} := \frac{f + h\hat{P} - \hat{P}^2}{\hat{Q}}.
\]

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

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

(ii) \( \hat{q} := \left\lfloor (\hat{P} + v)/\hat{Q} \right\rfloor \)

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

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

(d) RETURN\((\hat{Q}, \hat{P}, \hat{R})\)

(3) // Now apply NUCOMP

(a) \( \hat{b}_0 := U, \hat{a}_{-1} := 0, \hat{a}_0 := 1 \).

(b) \( \hat{c}_{-1} := Q''/S, \hat{P} := P' + U\hat{Q''}/S, \hat{c}_0 := (P - P')/\hat{b}_{-1} \).

(c) \( \hat{d}_{-1} := P' + P'' - h, \hat{d}_0 := (\hat{d}_{-1}\hat{b}_0 - SR'')/\hat{b}_{-1} \).

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

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

(a) \( \hat{q}_i := [b_{i-1}/b_i], b_{i+1} := b_{i-1} (\mod b_i) \). // Division with remainder

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

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

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

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

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

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

(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, \( q_{i+1} := [P_{i+1}/Q_{i+1}] \)

ELSE \( q_{i+1} := [(P_{i+1} + v)/Q_{i+1}] \)

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. \( R_{i+2} := Q_{i+1} \).
sequences, we only compute forms, this idea is originally due to Atkin. Instead of computing all four
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 $g$. 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 $D' \odot D''$ 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 $U := W(P' - P'') + XR'' \pmod{b_{-1}}$.

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 $\text{deg}(\tilde{Q}) = g + 1$ AND $C$ is imaginary THEN

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

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

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

(ii) $\hat{q} := [\tilde{P} + v]/\tilde{Q}$.

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

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

(d) RETURN($\tilde{Q}, \tilde{P}, \tilde{R}$)

(3) // Now apply NUCOMP

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

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

(4) While $\text{deg}(b_i) > N$ do

(a) $\hat{q}_i := [b_{i-1}/b_i], b_{i+1} := b_{i-1} \mod b_i$. // Division with remainder

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

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

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

(a) $c_i := (b_iQ''/S + a_i(P' - P''))/b_{i-1}$.

(b) $d_{i-1} := (b_{i-1}(P'' - h) + a_{i-1}SR'')/b_{i-1}$.

(c) $X_i := b_{i-1}c_i, c_{i-1} := (X_1 + (-1)^i(P' - P''))/b_i$.

(d) $X_2 := ((P' + P'' - h) - X_2)/(-1)^{i-2}a_{i-1}$.

(e) $Q_{i+1} := (-1)^{i+1}(b_ic_i - a_id_i) \quad // Q_{i+1} = Q_{n+2}$.

(f) $P_{i+1} := (-1)^{i+1}(X_2 - X_1) + P'' \quad // P_{i+1} = P_{n+2}$.

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

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

i. IF $C$ is imaginary, $q_{i+1} := [P_{i+1}/Q_{i+1}]

\quad ELSE $q_{i+1} := [(P_{i+1} + v)/Q_{i+1}]

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 $\hat{Q} := Q_{i+1}, \tilde{P} := P_{i+1}, \tilde{R} := R_{i+1}$.

(j) RETURN($\hat{Q}, \tilde{P}, \tilde{R}$).
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 $\deg(P'' - h - v) \leq g$; this is the case, for example, if $D''$ is given in reduced form. If $L$ is as in Eq. (8.4), then $L \leq 2g + 1$, and $L \leq g$ 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:

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

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 $\deg(\hat{Q}_{n+3}) = \deg(u_{n+1}) = g + 1$. 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

$$u'_i = \frac{Q''}{b_{-1}S}b_{i-1}b_i, \quad v'_i = \frac{h - 2P''}{b_{-1}}a_{i-1}b_i, \quad w'_i = \frac{SR''}{b_{-1}}a_{i-1}a_i, \quad (10.2)$$
for \(0 \leq i \leq m + 1\). Using Lemmas 2.2 and 8.1, we obtain
\[
\begin{align*}
\deg(u'_{n+2}) & \leq \deg(u_{n+1}) - 1 = (g + 1) - 1 = g, \\
\deg(v'_{n+2}) & \leq \deg(v_{n+1}) - 1 \leq g - 1, \\
\deg(w'_{n+2}) & \leq \deg(w_{n+2}) - 1 = L - \deg(u_{n+1}) - 1 = g - 1.
\end{align*}
\]

It follows that
\[
\deg(\hat{P}_{n+3} + v) = \deg(\hat{P}_{n+3} + P'' - h) - (P'' - h - v) \leq g.
\]

Proposition 10.2. Under the assumptions of Proposition 10.1, and with \(D_{n+4}\) given by Eq. (8.5), we have \(D_{n+4} \neq D_{n+4}\), 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 \(\hat{P}_{n+3} - P_{n+3} = sQ_{n+2}\) with \(s = \hat{q}_{n+1} - q_{n+2}\). Since \(\deg(Q_{n+2}) = g + 1\), 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 \(\hat{P}_{n+3} - P_{n+3} = sQ_{n+2}\). 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
\[
\hat{Q}_{n+2}(\hat{Q}_{n+3} - Q_{n+3}) = (f + h\hat{P}_{n+3} - \hat{P}_{n+3}^2) - (f + hP_{n+3} - P_{n+3}^2)
= (\hat{P}_{n+3} - P_{n+3})(h - \hat{P}_{n+3} - P_{n+3})
= s\hat{Q}_{n+2}(h - 2P_{n+3} - s\hat{Q}_{n+2}),
\]
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 \(\hat{a}_{n+3}, a_{n+4}\), and \(\hat{a}_{n+4}\) be the reduced ideals corresponding to \(\hat{D}_{n+3}, D_{n+4}\), and \(D_{n+4}\), respectively. Then \(\langle \hat{Q}_{n+2} \rangle a_{n+4} = (P_{n+3} + v)\hat{a}_{n+3}\) and \(\langle \hat{Q}_{n+2} \rangle \hat{a}_{n+4} = (\hat{P}_{n+3} + v)\hat{a}_{n+3}\). 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 \( \deg(P_{n+3} + v) = \deg(\hat{P}_{n+3} + v) \), we have \( \delta \geq 1 \). Furthermore, since \( \deg(P_{n+3} + v) = \deg(\hat{P}_{n+3} - h - v) = g + 1 \),

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

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\textsuperscript{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, Table 11.2, and Table 11.3 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.\textsuperscript{5} The results for characteristic 2 base fields are similar and have been omitted for brevity. 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 11.4, Table 11.5, and Table 11.6 contain the ratio of runtimes for binary exponentiation using Cantor’s algorithm as compared to that using
### Table 11.1. Exponentiation ratios (Alg 9.1 / Alg 9.2) over $F_p$, imaginary.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$2^8$</th>
<th>$2^{16}$</th>
<th>$2^{32}$</th>
<th>$2^{64}$</th>
<th>$2^{128}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0.8703</td>
<td>0.9471</td>
<td>0.9289</td>
<td>0.8834</td>
<td>0.9523</td>
</tr>
<tr>
<td>4</td>
<td>0.9610</td>
<td>0.9542</td>
<td>0.9266</td>
<td>0.9662</td>
<td>0.9503</td>
</tr>
<tr>
<td>6</td>
<td>0.9593</td>
<td>0.9550</td>
<td>0.9576</td>
<td>0.9647</td>
<td>0.9514</td>
</tr>
<tr>
<td>7</td>
<td>0.9754</td>
<td>0.9548</td>
<td>0.9631</td>
<td>0.9624</td>
<td>0.9787</td>
</tr>
<tr>
<td>8</td>
<td>0.9726</td>
<td>0.9663</td>
<td>0.9666</td>
<td>0.9660</td>
<td>0.9576</td>
</tr>
<tr>
<td>9</td>
<td>0.9751</td>
<td>0.9764</td>
<td>0.9840</td>
<td>0.9776</td>
<td>0.9760</td>
</tr>
<tr>
<td>10</td>
<td>0.9793</td>
<td>0.9708</td>
<td>0.9817</td>
<td>0.9724</td>
<td>0.9629</td>
</tr>
<tr>
<td>11</td>
<td>0.9653</td>
<td>0.9792</td>
<td>0.9854</td>
<td>0.9777</td>
<td>0.9987</td>
</tr>
<tr>
<td>12</td>
<td>0.9983</td>
<td>0.9969</td>
<td>0.9971</td>
<td>0.9875</td>
<td>0.9977</td>
</tr>
<tr>
<td>13</td>
<td>0.9851</td>
<td>1.0084</td>
<td>1.0000</td>
<td>0.9983</td>
<td>0.9993</td>
</tr>
<tr>
<td>14</td>
<td>1.0126</td>
<td>1.0039</td>
<td>1.0485</td>
<td>0.9988</td>
<td>0.9845</td>
</tr>
<tr>
<td>15</td>
<td>1.0143</td>
<td>1.0005</td>
<td>1.0102</td>
<td>1.0097</td>
<td>0.9913</td>
</tr>
<tr>
<td>16</td>
<td>1.0823</td>
<td>1.1033</td>
<td>1.1029</td>
<td>1.1017</td>
<td>1.0679</td>
</tr>
<tr>
<td>20</td>
<td>1.1003</td>
<td>1.1185</td>
<td>1.1137</td>
<td>1.1203</td>
<td>1.1103</td>
</tr>
<tr>
<td>30</td>
<td>1.0872</td>
<td>1.0908</td>
<td>1.0927</td>
<td>1.0895</td>
<td>1.1152</td>
</tr>
</tbody>
</table>

### Table 11.2. Exponentiation ratios (Alg 9.1 / Alg 9.2) over $F_p$, real.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$2^8$</th>
<th>$2^{16}$</th>
<th>$2^{32}$</th>
<th>$2^{64}$</th>
<th>$2^{128}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.6861</td>
<td>0.8747</td>
<td>0.9266</td>
<td>0.9572</td>
<td>0.8414</td>
</tr>
<tr>
<td>3</td>
<td>0.8379</td>
<td>0.9149</td>
<td>0.9413</td>
<td>0.9321</td>
<td>0.8907</td>
</tr>
<tr>
<td>4</td>
<td>0.9395</td>
<td>0.9647</td>
<td>0.9485</td>
<td>0.9582</td>
<td>0.9533</td>
</tr>
<tr>
<td>5</td>
<td>0.9294</td>
<td>0.9209</td>
<td>0.9335</td>
<td>0.9489</td>
<td>0.9681</td>
</tr>
<tr>
<td>6</td>
<td>0.9477</td>
<td>0.9397</td>
<td>0.9555</td>
<td>0.9523</td>
<td>0.9636</td>
</tr>
<tr>
<td>7</td>
<td>0.8635</td>
<td>0.9431</td>
<td>0.9466</td>
<td>0.9370</td>
<td>0.9460</td>
</tr>
<tr>
<td>8</td>
<td>0.9349</td>
<td>0.9667</td>
<td>0.9644</td>
<td>0.9860</td>
<td>0.9869</td>
</tr>
<tr>
<td>9</td>
<td>0.9549</td>
<td>0.9723</td>
<td>0.9683</td>
<td>0.9561</td>
<td>0.9859</td>
</tr>
<tr>
<td>10</td>
<td>0.9522</td>
<td>0.9963</td>
<td>0.9913</td>
<td>0.9820</td>
<td>0.9968</td>
</tr>
<tr>
<td>11</td>
<td>0.9540</td>
<td>0.9645</td>
<td>0.9854</td>
<td>0.9874</td>
<td>0.9966</td>
</tr>
<tr>
<td>12</td>
<td>0.9726</td>
<td>0.9872</td>
<td>0.9960</td>
<td>0.9809</td>
<td>0.9916</td>
</tr>
<tr>
<td>13</td>
<td>0.9806</td>
<td>0.9948</td>
<td>0.9926</td>
<td>0.9941</td>
<td>1.0191</td>
</tr>
<tr>
<td>14</td>
<td>0.9883</td>
<td>1.0125</td>
<td>1.0021</td>
<td>0.9989</td>
<td>1.0239</td>
</tr>
<tr>
<td>15</td>
<td>0.9807</td>
<td>0.9989</td>
<td>1.0117</td>
<td>1.0071</td>
<td>1.0229</td>
</tr>
<tr>
<td>16</td>
<td>1.0006</td>
<td>1.0156</td>
<td>1.1156</td>
<td>1.1109</td>
<td>1.1053</td>
</tr>
<tr>
<td>20</td>
<td>1.0968</td>
<td>1.1090</td>
<td>1.1164</td>
<td>1.1060</td>
<td>1.0847</td>
</tr>
<tr>
<td>30</td>
<td>1.0081</td>
<td>1.1088</td>
<td>1.1149</td>
<td>1.1058</td>
<td>1.0980</td>
</tr>
</tbody>
</table>

### Table 11.3. Exponentiation ratios (Alg 9.1 / Alg 9.2) over $F_p$, unusual.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$2^8$</th>
<th>$2^{16}$</th>
<th>$2^{32}$</th>
<th>$2^{64}$</th>
<th>$2^{128}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0.9175</td>
<td>1.0081</td>
<td>1.0101</td>
<td>1.0109</td>
<td>0.9715</td>
</tr>
<tr>
<td>4</td>
<td>0.9504</td>
<td>1.0289</td>
<td>1.0311</td>
<td>0.9607</td>
<td>0.9522</td>
</tr>
<tr>
<td>5</td>
<td>0.9684</td>
<td>0.9680</td>
<td>0.9853</td>
<td>0.9844</td>
<td>0.9730</td>
</tr>
<tr>
<td>6</td>
<td>0.9649</td>
<td>0.9626</td>
<td>0.9862</td>
<td>0.9731</td>
<td>0.9584</td>
</tr>
<tr>
<td>7</td>
<td>0.9816</td>
<td>0.9121</td>
<td>1.0139</td>
<td>0.9620</td>
<td>0.9745</td>
</tr>
<tr>
<td>8</td>
<td>0.9929</td>
<td>0.9867</td>
<td>0.9911</td>
<td>0.9886</td>
<td>0.9775</td>
</tr>
<tr>
<td>9</td>
<td>0.9938</td>
<td>0.9991</td>
<td>1.0131</td>
<td>0.9932</td>
<td>1.0047</td>
</tr>
<tr>
<td>10</td>
<td>1.0000</td>
<td>0.9982</td>
<td>0.9964</td>
<td>1.0017</td>
<td>0.9959</td>
</tr>
<tr>
<td>11</td>
<td>1.0000</td>
<td>1.0025</td>
<td>1.0103</td>
<td>1.0072</td>
<td>1.0228</td>
</tr>
<tr>
<td>12</td>
<td>1.0048</td>
<td>1.0046</td>
<td>1.0085</td>
<td>1.0014</td>
<td>1.0163</td>
</tr>
<tr>
<td>13</td>
<td>1.0060</td>
<td>1.0245</td>
<td>1.0243</td>
<td>1.0024</td>
<td>1.0086</td>
</tr>
<tr>
<td>14</td>
<td>0.9960</td>
<td>1.0245</td>
<td>1.0037</td>
<td>1.0070</td>
<td>1.0313</td>
</tr>
<tr>
<td>15</td>
<td>1.0094</td>
<td>1.0301</td>
<td>1.0376</td>
<td>1.0321</td>
<td>1.0448</td>
</tr>
<tr>
<td>16</td>
<td>1.1394</td>
<td>1.1789</td>
<td>1.1526</td>
<td>1.1262</td>
<td>1.1024</td>
</tr>
<tr>
<td>20</td>
<td>1.1014</td>
<td>1.1103</td>
<td>1.1209</td>
<td>1.1758</td>
<td>1.0840</td>
</tr>
<tr>
<td>30</td>
<td>1.0932</td>
<td>1.1047</td>
<td>1.1064</td>
<td>1.1018</td>
<td>1.0939</td>
</tr>
</tbody>
</table>

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. Once again, the data for $F_{2^n}$ are similar.
and have been omitted for brevity. The data clearly show that NUCOMP out-performs Cantor’s algorithm except for very small genera and finite field sizes, and that its relative performance improves as both the genus and finite field size increase. The findings are consistent with those presented in Ref. 6, but our improved versions of NUCOMP presented here out-perform Cantor’s algorithm for even smaller genera and finite field sizes than in Ref. 6.

Table 11.4. Exponentiation ratios (NUCOMP / Cantor) over $\mathbb{F}_p$, imaginary.

<table>
<thead>
<tr>
<th>$g$</th>
<th>$\log_2 p$ (prime)</th>
<th>$\log_2 p$ (imaginary)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1.296</td>
<td>1.000</td>
</tr>
<tr>
<td>3</td>
<td>1.062</td>
<td>1.070</td>
</tr>
<tr>
<td>4</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td>5</td>
<td>0.938</td>
<td>0.962</td>
</tr>
<tr>
<td>6</td>
<td>0.923</td>
<td>0.989</td>
</tr>
<tr>
<td>7</td>
<td>0.944</td>
<td>0.904</td>
</tr>
<tr>
<td>8</td>
<td>0.957</td>
<td>0.921</td>
</tr>
<tr>
<td>9</td>
<td>0.943</td>
<td>0.897</td>
</tr>
<tr>
<td>10</td>
<td>0.933</td>
<td>0.896</td>
</tr>
<tr>
<td>11</td>
<td>0.944</td>
<td>0.904</td>
</tr>
<tr>
<td>12</td>
<td>0.936</td>
<td>0.920</td>
</tr>
<tr>
<td>13</td>
<td>0.930</td>
<td>0.938</td>
</tr>
<tr>
<td>14</td>
<td>0.916</td>
<td>0.932</td>
</tr>
<tr>
<td>15</td>
<td>0.915</td>
<td>0.874</td>
</tr>
<tr>
<td>16</td>
<td>0.825</td>
<td>0.795</td>
</tr>
<tr>
<td>17</td>
<td>0.794</td>
<td>0.766</td>
</tr>
<tr>
<td>18</td>
<td>0.792</td>
<td>0.771</td>
</tr>
<tr>
<td>19</td>
<td>0.786</td>
<td>0.773</td>
</tr>
<tr>
<td>20</td>
<td>0.785</td>
<td>0.773</td>
</tr>
</tbody>
</table>

Table 11.5. Exponentiation ratios (NUCOMP / Cantor) over $\mathbb{F}_p$, real.

<table>
<thead>
<tr>
<th>$g$</th>
<th>$\log_2 p$ (prime)</th>
<th>$\log_2 p$ (imaginary)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1.296</td>
<td>1.000</td>
</tr>
<tr>
<td>3</td>
<td>1.062</td>
<td>1.070</td>
</tr>
<tr>
<td>4</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td>5</td>
<td>0.938</td>
<td>0.962</td>
</tr>
<tr>
<td>6</td>
<td>0.923</td>
<td>0.989</td>
</tr>
<tr>
<td>7</td>
<td>0.944</td>
<td>0.904</td>
</tr>
<tr>
<td>8</td>
<td>0.957</td>
<td>0.921</td>
</tr>
<tr>
<td>9</td>
<td>0.943</td>
<td>0.897</td>
</tr>
<tr>
<td>10</td>
<td>0.933</td>
<td>0.896</td>
</tr>
<tr>
<td>11</td>
<td>0.944</td>
<td>0.904</td>
</tr>
<tr>
<td>12</td>
<td>0.936</td>
<td>0.920</td>
</tr>
<tr>
<td>13</td>
<td>0.930</td>
<td>0.938</td>
</tr>
<tr>
<td>14</td>
<td>0.916</td>
<td>0.932</td>
</tr>
<tr>
<td>15</td>
<td>0.915</td>
<td>0.874</td>
</tr>
<tr>
<td>16</td>
<td>0.825</td>
<td>0.795</td>
</tr>
<tr>
<td>17</td>
<td>0.794</td>
<td>0.766</td>
</tr>
<tr>
<td>18</td>
<td>0.792</td>
<td>0.771</td>
</tr>
<tr>
<td>19</td>
<td>0.786</td>
<td>0.773</td>
</tr>
<tr>
<td>20</td>
<td>0.785</td>
<td>0.773</td>
</tr>
</tbody>
</table>

11.2. Key Exchange

We also ran numerous examples of the key exchange protocols described in Ref. 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 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 \( g^n \) 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 11.7 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 Ref. 7, are not included. We also give the

---

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

<table>
<thead>
<tr>
<th>genus</th>
<th>( \log_2 p )</th>
<th>8</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
<th>256</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1.0438</td>
<td>1.0179</td>
<td>1.0423</td>
<td>1.0444</td>
<td>0.9607</td>
<td>0.9345</td>
<td>0.9257</td>
</tr>
<tr>
<td>3</td>
<td>1.0500</td>
<td>1.0649</td>
<td>1.0566</td>
<td>1.0665</td>
<td>0.9182</td>
<td>0.9301</td>
<td>0.9102</td>
</tr>
<tr>
<td>4</td>
<td>1.1220</td>
<td>1.0539</td>
<td>1.0030</td>
<td>0.9216</td>
<td>0.8601</td>
<td>0.8631</td>
<td>0.8382</td>
</tr>
<tr>
<td>5</td>
<td>1.1224</td>
<td>1.0484</td>
<td>1.0259</td>
<td>1.0419</td>
<td>0.9115</td>
<td>0.8951</td>
<td>0.8580</td>
</tr>
<tr>
<td>6</td>
<td>1.0081</td>
<td>0.9179</td>
<td>0.9305</td>
<td>0.9175</td>
<td>0.9004</td>
<td>0.8461</td>
<td>0.8158</td>
</tr>
<tr>
<td>7</td>
<td>0.9882</td>
<td>0.9605</td>
<td>0.9654</td>
<td>0.9900</td>
<td>0.8686</td>
<td>0.8477</td>
<td>0.8342</td>
</tr>
<tr>
<td>8</td>
<td>0.9340</td>
<td>0.8902</td>
<td>0.8883</td>
<td>0.8784</td>
<td>0.8266</td>
<td>0.8274</td>
<td>0.7986</td>
</tr>
<tr>
<td>9</td>
<td>0.9245</td>
<td>0.9151</td>
<td>0.9224</td>
<td>0.9308</td>
<td>0.8523</td>
<td>0.8396</td>
<td>0.8182</td>
</tr>
<tr>
<td>10</td>
<td>0.9641</td>
<td>0.9075</td>
<td>0.8642</td>
<td>0.8858</td>
<td>0.8033</td>
<td>0.8117</td>
<td>0.8016</td>
</tr>
<tr>
<td>11</td>
<td>0.9570</td>
<td>0.8997</td>
<td>0.8892</td>
<td>0.9055</td>
<td>0.8215</td>
<td>0.8265</td>
<td>0.8166</td>
</tr>
<tr>
<td>12</td>
<td>0.9615</td>
<td>0.8977</td>
<td>0.8662</td>
<td>0.8828</td>
<td>0.7821</td>
<td>0.7550</td>
<td>0.7964</td>
</tr>
<tr>
<td>13</td>
<td>0.9448</td>
<td>0.8719</td>
<td>0.8652</td>
<td>0.8858</td>
<td>0.7839</td>
<td>0.7699</td>
<td>0.8104</td>
</tr>
<tr>
<td>14</td>
<td>0.8945</td>
<td>0.8203</td>
<td>0.8111</td>
<td>0.8306</td>
<td>0.7663</td>
<td>0.7389</td>
<td>0.7822</td>
</tr>
<tr>
<td>15</td>
<td>0.8458</td>
<td>0.8234</td>
<td>0.8108</td>
<td>0.8250</td>
<td>0.7220</td>
<td>0.7456</td>
<td>0.8074</td>
</tr>
<tr>
<td>16</td>
<td>0.7964</td>
<td>0.7660</td>
<td>0.7598</td>
<td>0.7556</td>
<td>0.7252</td>
<td>0.7429</td>
<td>0.7942</td>
</tr>
<tr>
<td>17</td>
<td>0.7781</td>
<td>0.7591</td>
<td>0.7575</td>
<td>0.7622</td>
<td>0.7055</td>
<td>0.7387</td>
<td>0.7769</td>
</tr>
</tbody>
</table>
Table 11.7. Key exchange timings over $F_p$ and $F_{2^n}$ (in seconds).

<table>
<thead>
<tr>
<th>Security level (in bits)</th>
<th>$F_p$</th>
<th>$F_{2^n}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Imaginary</td>
<td>Real</td>
</tr>
<tr>
<td>80</td>
<td>0.0242</td>
<td>0.0590</td>
</tr>
<tr>
<td></td>
<td>0.0382</td>
<td>0.0530</td>
</tr>
<tr>
<td></td>
<td>0.0409</td>
<td>0.0438</td>
</tr>
<tr>
<td></td>
<td>0.0466</td>
<td>0.0435</td>
</tr>
<tr>
<td></td>
<td>0.0124</td>
<td>0.0124</td>
</tr>
</tbody>
</table>

Table 11.8. Key exchange ratios over $F_p$ and $F_{2^n}$.

<table>
<thead>
<tr>
<th>Security level</th>
<th>$F_p$</th>
<th>$F_{2^n}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Imaginary</td>
<td>Real</td>
</tr>
<tr>
<td>80</td>
<td>0.0325</td>
<td>0.0490</td>
</tr>
<tr>
<td>128</td>
<td>0.0682</td>
<td>0.0553</td>
</tr>
<tr>
<td>256</td>
<td>0.1439</td>
<td>0.1033</td>
</tr>
</tbody>
</table>

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 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 Ref. 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


