An elementary introduction to hyperelliptic curves*

Alfred J. Menezes† Yi-Hong Wu‡ Robert J. Zuccherato§

November 7, 1996

Abstract

This paper presents an elementary introduction to some of the theory of hyperelliptic curves over finite fields of arbitrary characteristic that has cryptographic relevance. Cantor's algorithm for adding in the jacobian of a hyperelliptic curve and a proof of correctness of the algorithm are presented.

Contents

*Published as Technical Report CORR 96-19, Department of C&O, University of Waterloo, Ontario, Canada, November 1996.

†Department of Discrete and Statistical Sciences, Auburn University, AL 36849, USA. Email: menezal@mail.auburn.edu.

‡Department of Discrete and Statistical Sciences, Auburn University, AL 36849, USA.

§Department of Combinatorics and Optimization, University of Waterloo, Ontario, Canada, N2L 3G1. Email: rjzucche@math.uwaterloo.ca.

1 Introduction

Hyperelliptic curves are a special class of algebraic curves and can be viewed as generalizations of elliptic curves. There are hyperelliptic curves of every genus $g \geq 1$. A hyperelliptic curve of genus $g = 1$ is an elliptic curve. Elliptic curves have been extensively studied for over a hundred years, and there is a vast literature on the topic; for example, see the books by Silverman [34, 35]. Originally pursued mainly for purely aesthetic reasons, elliptic curves have recently become an essential tool in several important areas of applications including coding theory (e.g., Driencourt and Michon [11] and van der Geer [15]); pseudorandom number generation (e.g., Kaliski [18]); number theory algorithms (e.g., Goldwasser and Kilian [16] and Lenstra [21]); and public-key cryptography (see Koblitz [19], Miller [27], and Menezes [25]).

On the other hand, the theory of hyperelliptic curves has not received as much attention by the research community. Most results concerning hyperelliptic curves which appear in the literature on algebraic geometry are couched in very general terms. For example, a common source cited in papers on hyperelliptic curves is Mumford's book [28]. However, the non-specialist will have extreme difficulty specializing (not to mention finding) the results in this book to the particular case of hyperelliptic curves. Another difficulty one encounters is that the theory in such books is usually restricted to the case of hyperelliptic curves over the complex numbers (as in Mumford's book), or over algebraically closed fields of characteristic not equal to 2. The recent book of Cassels and Flynn [6] is an extensive account on curves of genus 2. (Compared to their book, our approach is definitely "low-brow".) Recently, applications of hyperelliptic curves have been found to areas outside algebraic geometry. Hyperelliptic curves were a key ingredient in Adleman and Huang's random polynomial-time algorithm for primality proving [3]. Hyperelliptic curves have also been considered in the design of error-correcting codes [4], in integer factorization algorithms [22], and in public-key cryptography [20]. Hyperelliptic curves over finite fields of characteristic two are especially interesting for the purpose of implementing these codes and cryptosystems.

Charlap and Robbins [7, 8] presented an elementary introduction to elliptic curves. The purpose was to provide elementary self-contained proofs of some of the basic theory relevant to Schoof's algorithm [33] for counting the points on an elliptic curve over a finite field. The discussion was restricted to fields of characteristic not equal to 2 or 3. However, for practical applications, elliptic and hyperelliptic curves over characteristic two fields are especially attractive. This paper, similar in spirit to that of Charlap and Robbins, presents an elementary introduction to some of the theory of hyperelliptic curves over finite fields of arbitrary characteristic that has cryptographic relevance. For a general introduction to the theory of algebraic curves, consult Fulton's book [14].

2 Basic definitions and properties

Definition 1 (*hyperelliptic curve*) Let K be a field and let $\overline{K}$ be the algebraic closure of K. A *hyperelliptic curve C of genus g over K* ($g \geq 1$) is an equation of the form

$$C \ : \ v^2 + h(u)v = f(u) \text{ in } K[u,v], \tag{1}$$

where $h(u) \in K[u]$ is a polynomial of degree at most g, $f(u) \in K[u]$ is a monic polynomial of degree $2g+1$, and there are no solutions $(u,v) \in \overline{K} \times \overline{K}$ which simultaneously satisfy the equation $v^2 + h(u)v = f(u)$ and the partial derivative equations $2v + h(u) = 0$ and $h'(u)v - f'(u) = 0$.

A *singular point* on C is a solution $(u,v) \in \overline{K} \times \overline{K}$ which simultaneously satisfies the equation $v^2 + h(u)v = f(u)$ and the partial derivative equations $2v + h(u) = 0$ and $h'(u)v - f'(u) = 0$. Definition 1 thus says that a hyperelliptic curve does not have any singular points.

For the remainder of this paper it is assumed that the field K and the curve C have been fixed.

Lemma 2 Let C be a hyperelliptic curve over K defined by equation (1).

(i) If $h(u) = 0$, then $\text{char}(K) \neq 2$.

(ii) If $\text{char}(K) \neq 2$, then the change of variables $u \to u$, $v \to (v - h(u)/2)$ transforms C to the form $v^2 = f(u)$ where $\deg_u f = 2g+1$.

(iii) Let C be an equation of the form (1) with $h(u) = 0$ and $\text{char}(K) \neq 2$. Then C is a hyperelliptic curve if and only if $f(u)$ has no repeated roots in $\overline{K}$.

Proof.

(i) Suppose that $h(u) = 0$ and $\text{char}(K) = 2$. Then the partial derivative equations reduce to $f'(u) = 0$. Note that $\deg_u f'(u) = 2g$. Let $x \in \overline{K}$ be a root of the equation $f'(u) = 0$, and let $y \in \overline{K}$ be a root of the equation $v^2 = f(x)$. Then the point (x,y) is a singular point on C. Statement (i) now follows.

(ii) Under this change of variables, the equation (1) is transformed to

$$(v - h(u)/2)^2 + h(u)(v - h(u)/2) = f(u),$$

which simplifies to $v^2 = f(u) + h(u)^2/4$; note that $\deg_u(f + h^2/4) = 2g+1$.

(iii) A singular point (x,y) on C must satisfy $y^2 = f(x)$, $2y = 0$, and $f'(x) = 0$. Hence $y = 0$ and x is a repeated root of the polynomial $f(u)$. □

Definition 3 (*rational points, point at infinity, finite points*) Let L be an extension field of K. The *set of L-rational points on C*, denoted $C(L)$, is the set of all points $P = (x, y) \in L \times L$ which satisfy the equation (1) of the curve C, together with a special *point at infinity*[1] denoted ∞. The set of points $C(\overline{K})$ will simply be denoted by C. The points in C other than ∞ are called *finite points*.

Example 4 (*hyperelliptic curves over the reals*) The following are three examples of hyperelliptic curves over the field of real numbers. Each curve has genus $g = 2$ and $h(u) = 0$.

1. $C_1 : v^2 = u^5 + u^4 + 4u^3 + 4u^2 + 3u + 3 = (u+1)(u^2+1)(u^2+3)$. The graph of C_1 in the real plane is shown in Figure 1.

2. $C_2 : v^2 = u^5 + u^4 - u^2 - u = u(u-1)(u+1)(u^2+u+1)$. The graph of C_2 in the real plane is shown in Figure 2.

3. $C_3 : v^2 = u^5 - 5u^3 + 4u = u(u-1)(u+1)(u-2)(u+2)$. The graph of C_3 in the real plane is shown in Figure 3.

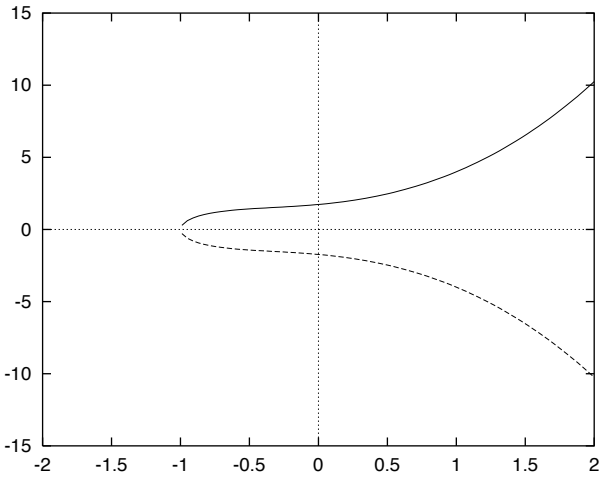

Figure 1: The hyperelliptic curve $C_1 : v^2 = u^5 + u^4 + 4u^3 + 4u^2 + 3u + 3$ over the real numbers.

Definition 5 (*opposite, special and ordinary points*) Let $P = (x, y)$ be a finite point on a curve C. The *opposite* of P is the point $\tilde{P} = (x, -y - h(x))$. (Note that $\tilde{P}$ is indeed on C.) We also define the opposite of ∞ to be $\widetilde{\infty} = \infty$ itself. If a finite point P satisfies $P = \tilde{P}$ then the point is said to be *special*; otherwise, the point is said to be *ordinary*.

[1]The point at infinity lies in the projective plane $P^2(K)$. It is the only projective point lying on the line at infinity that satisfies the homogenized hyperelliptic curve equation. If $g \geq 2$, then ∞ is a singular (projective) point which is allowed since $\infty \notin \overline{K} \times \overline{K}$.

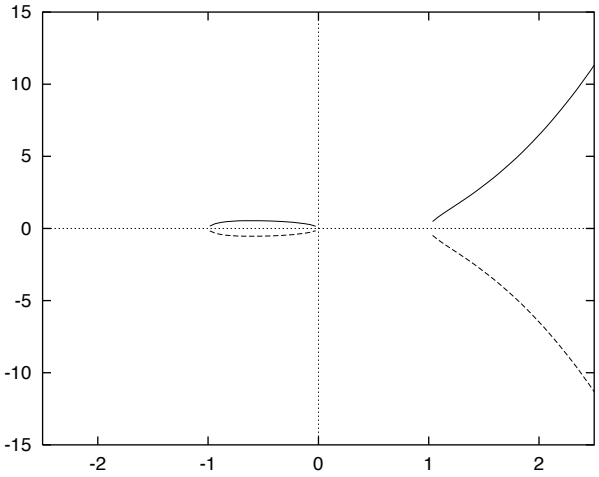

Figure 2: The hyperelliptic curve $C_2 : v^2 = u^5 + u^4 - u^2 - u$ over the real numbers.

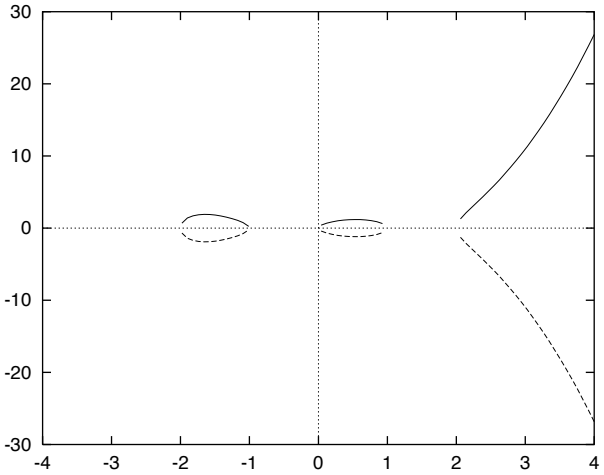

Figure 3: The hyperelliptic curve $C_3 : v^2 = u^5 - 5u^3 + 4u$ over the real numbers.

Example 6 (*hyperelliptic curve over* $\mathbb{Z}_7$) Consider the curve $C : v^2 + uv = u^5 + 5u^4 + 6u^2 + u + 3$ over the finite field $\mathbb{Z}_7$. Here, $h(u) = u$, $f(u) = u^5 + 5u^4 + 6u^2 + u + 3$ and $g = 2$. It can be verified that C has no singular points (other than ∞), and hence C is indeed a hyperelliptic curve. The $\mathbb{Z}_7$-rational points on C are

$$C(\mathbb{Z}_7) = \{\infty, (1,1), (1,5), (2,2), (2,3), (5,3), (5,6), (6,4)\}.$$

The point $(6,4)$ is a special point.

Example 7 (*hyperelliptic curve over* $\mathbb{F}_{2^5}$) Consider the finite field $\mathbb{F}_{2^5} = \mathbb{F}_2[x]/(x^5+x^2+1)$, and let α be a root of the primitive polynomial x^5+x^2+1 in $\mathbb{F}_{2^5}$. The powers of α are listed in Table 1.

n	α^n	n	α^n	n	α^n
0	1	11	$\alpha^2+\alpha+1$	22	$\alpha^4+\alpha^2+1$
1	α	12	$\alpha^3+\alpha^2+\alpha$	23	$\alpha^3+\alpha^2+\alpha+1$
2	α^2	13	$\alpha^4+\alpha^3+\alpha^2$	24	$\alpha^4+\alpha^3+\alpha^2+\alpha$
3	α^3	14	$\alpha^4+\alpha^3+\alpha^2+1$	25	$\alpha^4+\alpha^3+1$
4	α^4	15	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$	26	$\alpha^4+\alpha^2+\alpha+1$
5	α^2+1	16	$\alpha^4+\alpha^3+\alpha+1$	27	$\alpha^3+\alpha+1$
6	$\alpha^3+\alpha$	17	$\alpha^4+\alpha+1$	28	$\alpha^4+\alpha^2+\alpha$
7	$\alpha^4+\alpha^2$	18	$\alpha+1$	29	α^3+1
8	$\alpha^3+\alpha^2+1$	19	$\alpha^2+\alpha$	30	$\alpha^4+\alpha$
9	$\alpha^4+\alpha^3+\alpha$	20	$\alpha^3+\alpha^2$	31	1
10	α^4+1	21	$\alpha^4+\alpha^3$		

Table 1: Powers of α in the finite field $\mathbb{F}_{2^5} = \mathbb{F}_2[x]/(x^5+x^2+1)$.

Consider the curve $C : v^2+(u^2+u)v = u^5+u^3+1$ of genus $g = 2$ over the finite field $\mathbb{F}_{2^5}$. Here, $h(u) = u^2+u$ and $f(u) = u^5+u^3+1$. It can be verified that C has no singular points (other than ∞), and hence C is indeed a hyperelliptic curve. The finite points in $C(\mathbb{F}_{2^5})$, the set of $\mathbb{F}_{2^5}$-rational points on C, are:

$$\begin{array}{cccccccc}
(0,1) & (1,1) & (\alpha^5,\alpha^{15}) & (\alpha^5,\alpha^{27}) & (\alpha^7,\alpha^4) & (\alpha^7,\alpha^{25}) & (\alpha^9,\alpha^{27}) & (\alpha^9,\alpha^{30}) \\
(\alpha^{10},\alpha^{23}) & (\alpha^{10},\alpha^{30}) & (\alpha^{14},\alpha^8) & (\alpha^{14},\alpha^{19}) & (\alpha^{15},0) & (\alpha^{15},\alpha^8) & (\alpha^{18},\alpha^{23}) & (\alpha^{18},\alpha^{29}) \\
(\alpha^{19},\alpha^2) & (\alpha^{19},\alpha^{28}) & (\alpha^{20},\alpha^{15}) & (\alpha^{20},\alpha^{29}) & (\alpha^{23},0) & (\alpha^{23},\alpha^4) & (\alpha^{25},\alpha) & (\alpha^{25},\alpha^{14}) \\
(\alpha^{27},0) & (\alpha^{27},\alpha^2) & (\alpha^{28},\alpha^7) & (\alpha^{28},\alpha^{16}) & (\alpha^{29},0) & (\alpha^{29},\alpha) & (\alpha^{30},0) & (\alpha^{30},\alpha^{16})
\end{array}$$

Of these, the points $(0,1)$ and $(1,1)$ are special.

3 Polynomial and rational functions

This section introduces basic properties of polynomial and rational functions which arise when they are viewed as functions on a hyperelliptic curve.

Definition 8 (*coordinate ring, polynomial function*) The *coordinate ring of C over K*, denoted $K[C]$, is the quotient ring

$$K[C] = K[u,v]/(v^2 + h(u)v - f(u)),$$

where $(v^2 + h(u)v - f(u))$ denotes the ideal in $K[u,v]$ generated by the polynomial $v^2 + h(u)v - f(u)$. Similarly, the *coordinate ring of C over $\overline{K}$* is defined as

$$\overline{K}[C] = \overline{K}[u,v]/(v^2 + h(u)v - f(u)).$$

An element of $\overline{K}[C]$ is called a *polynomial function* on C.

Lemma 9 The polynomial $r(u,v) = v^2 + h(u)v - f(u)$ is irreducible over $\overline{K}$, and hence $\overline{K}[C]$ is an integral domain.

Proof. If $r(u,v)$ were reducible over $\overline{K}$, it would factor as $(v - a(u))(v - b(u))$ for some $a, b \in \overline{K}[u]$. But then $\deg_u(a \cdot b) = \deg_u f = 2g + 1$ and $\deg_u(a + b) = \deg_u h \leq g$, which is impossible. □

Observe that for each polynomial function $G(u,v) \in \overline{K}[C]$, we can repeatedly replace any occurrence of v^2 by $f(u) - h(u)v$, to eventually obtain a representation

$$G(u,v) = a(u) - b(u)v, \quad \text{where } a(u), b(u) \in \overline{K}[u].$$

It is easy to see that the representation of $G(u,v)$ in this form is unique.

Definition 10 (*conjugate*) Let $G(u,v) = a(u) - b(u)v$ be a polynomial function in $\overline{K}[C]$. The *conjugate* of $G(u,v)$ is defined to be the polynomial function $\overline{G}(u,v) = a(u) + b(u)(h(u) + v)$.

Definition 11 (*norm*) Let $G(u,v) = a(u) - b(u)v$ be a polynomial function in $\overline{K}[C]$. The *norm* of G is the polynomial function $N(G) = G\overline{G}$.

The norm function will be very useful in transforming questions about polynomial functions in two variables into easier questions about polynomials in a single variable.

Lemma 12 (*properties of norm*) Let $G, H \in \overline{K}[C]$ be polynomial functions.

(i) $N(G)$ is a polynomial in $\overline{K}[u]$.

(ii) $N(\overline{G}) = N(G)$.

(iii) $N(GH) = N(G)N(H)$.

Proof. Let $G = a - bv$ and $H = c - dv$, where $a, b, c, d \in \overline{K}[u]$. [2]

(i) Now, $\overline{G} = a + b(h + v)$ and

$$\begin{aligned} N(G) = G \cdot \overline{G} &= (a - bv)(a + b(h + v)) \\ &= a^2 + abh - b^2 f \in \overline{K}[u]. \end{aligned}$$

(ii) The conjugate of $\overline{G}$ is

$$\begin{aligned} \overline{\overline{G}} &= (a + bh) + (-b)(h + v) \\ &= a - bv = G. \end{aligned}$$

Hence $N(\overline{G}) = \overline{G}\,\overline{\overline{G}} = \overline{G}G = N(G)$.

(iii) $GH = (ac + bdf) - (bc + ad + bdh)v$, and its conjugate is

$$\begin{aligned} \overline{GH} &= (ac + bdf) + (bc + ad + bdh)(h + v) \\ &= ac + bdf + bch + adh + bdh^2 + bcv + adv + bdhv \\ &= ac + bc(h + v) + ad(h + v) + bd(h^2 + hv + f) \\ &= ac + bc(h + v) + ad(h + v) + bd(h^2 + 2hv + v^2) \\ &= (a + b(h + v))(c + d(h + v)) \\ &= \overline{G}\,\overline{H}. \end{aligned}$$

Hence $N(GH) = GH\overline{GH} = GH\overline{G}\,\overline{H} = G\overline{G}H\overline{H} = N(G)N(H)$. □

Definition 13 (*function field, rational functions*) The *function field* $K(C)$ *of* C *over* K is the field of fractions of $K[C]$. Similarly, the *function field* $\overline{K}(C)$ *of* C *over* $\overline{K}$ is the field of fractions of $\overline{K}[C]$. The elements of $\overline{K}(C)$ are called *rational functions* on C.

Note that $\overline{K}[C]$ is a subring of $\overline{K}(C)$, i.e., every polynomial function is also a rational function.

Definition 14 (*value of a rational function at a finite point*) Let $R \in \overline{K}(C)$, and let $P \in C$, $P \neq \infty$. Then R is said to be *defined at* P if there exist polynomial functions $G, H \in \overline{K}[C]$ such that $R = G/H$ and $H(P) \neq 0$; if no such $G, H \in \overline{K}[C]$ exist, then R is *not defined* at P. If R is defined at P, the *value of* R *at* P is defined to be $R(P) = G(P)/H(P)$.

It is easy to see that the value $R(P)$ is well-defined, i.e., it does not depend on the choice of G and H. The following definition introduces the notion of the degree of a polynomial function.

[2] If not explicitly stated otherwise, the variable in all polynomials will henceforth be assumed to be u.

Definition 15 (*degree of a polynomial function*) Let $G(u,v) = a(u) - b(u)v$ be a non-zero polynomial function in $\overline{K}[C]$. The *degree* of G is defined to be

$$\deg(G) = \max[2\deg_u(a),\ 2g+1+2\deg_u(b)].$$

Lemma 16 (*properties of degree*) Let $G, H \in \overline{K}[C]$.

(i) $\deg(G) = \deg_u(N(G))$.

(ii) $\deg(GH) = \deg(G) + \deg(H)$.

(iii) $\deg(G) = \deg(\overline{G})$.

Proof.

(i) Let $G = a(u) - b(u)v$. The norm of G is $N(G) = a^2 + abh - b^2 f$. Let $d_1 = \deg_u(a(u))$ and $d_2 = \deg_u(b(u))$. By definition of a hyperelliptic curve, $\deg_u(h(u)) \leq g$ and $\deg_u(f(u)) = 2g+1$. There are two cases to consider:
Case 1: If $2d_1 > 2g+1+2d_2$ then $2d_1 \geq 2g+2+2d_2$, and hence $d_1 \geq g+1+d_2$. Hence

$$\deg_u(a^2) = 2d_1 \geq d_1 + g + 1 + d_2 > d_1 + d_2 + g \geq \deg_u(abh).$$

Case 2: If $2d_1 < 2g+1+2d_2$ then $2d_1 \leq 2g+2d_2$, and hence $d_1 \leq g + d_2$. Hence

$$\deg_u(abh) \leq d_1 + d_2 + g \leq 2g + 2d_2 < 2g + 2d_2 + 1 = \deg_u(b^2 f).$$

It follows that

$$\deg_u(N(G)) = \max(2d_1, 2g+1+2d_2) = \deg(G).$$

(ii) We have

$$\begin{aligned} \deg(GH) &= \deg_u(N(GH)),\ \text{by (i)} \\ &= \deg_u(N(G)N(H)),\ \text{by Lemma 12(iii)} \\ &= \deg_u(N(G)) + \deg_u(N(H)) \\ &= \deg(G) + \deg(H). \end{aligned}$$

(iii) Since $N(G) = N(\overline{G})$, we have $\deg(G) = \deg_u(N(G)) = \deg_u(N(\overline{G})) = \deg(\overline{G})$. □

Definition 17 (*value of a rational function at* ∞) Let $R = G/H \in \overline{K}(C)$ be a rational function.

(i) If $\deg(G) < \deg(H)$ then the value of R at ∞ is defined to be $R(\infty) = 0$.

(ii) If $\deg(G) > \deg(H)$ then R is *not defined* at ∞.

(iii) If $\deg(G) = \deg(H)$ then $R(\infty)$ is defined to be the ratio of the leading coefficients (with respect to the deg function) of G and H.

4 Zeros and poles

This section introduces the notion of a uniformizing parameter, and the orders of zeros and poles of rational functions.

Definition 18 (*zero, pole*) Let $R \in \overline{K}(C)^*$ and let $P \in C$. If $R(P) = 0$ then R is said to have a *zero* at P. If R is not defined at P then R is said to have a *pole* at P, in which case we write $R(P) = \infty$.

Lemma 19 Let $G \in \overline{K}[C]^*$ and $P \in C$. If $G(P) = 0$ then $\overline{G}(\tilde{P}) = 0$.

Proof. Let $G = a(u) - b(u)v$ and $P = (x, y)$. Then $\overline{G} = a(u) + b(u)(v + h(u))$, $\tilde{P} = (x, -y - h(x))$, and $\overline{G}(\tilde{P}) = a(x) + b(x)(-y - h(x) + h(x)) = a(x) - yb(x) = G(P) = 0$. □

Lemmas 20, 21 and 22 are used in Theorem 23 which establishes the existence of uniformizing parameters.

Lemma 20 Let $P = (x, y)$ be a point on C. Suppose that $G = a(u) - b(u)v \in \overline{K}[C]^*$ has a zero at P and that x is not a root of both $a(u)$ and $b(u)$. Then $\overline{G}(P) = 0$ if and only if P is a special point.

Proof. If P is a special point, then $\overline{G}(P) = 0$ by Lemma 19. Conversely, suppose that P is an ordinary point, i.e., $y \neq (-y - h(x))$. If $\overline{G}(P) = 0$ then we have:

$$\begin{aligned} a(x) - b(x)y &= 0 \\ a(x) + b(x)(h(x) + y) &= 0. \end{aligned}$$

Subtracting the two equations yields $b(x) = 0$, and hence $a(x) = 0$, which contradicts the hypothesis that x is not a root of both $a(u)$ and $b(u)$. Hence if $\overline{G}(P) = 0$ then P is special. □

Lemma 21 Let $P = (x, y)$ be an ordinary point on C, and let $G = a(u) - b(u)v \in \overline{K}[C]^*$. Suppose that $G(P) = 0$ and x is not a root of both $a(u)$ and $b(u)$. Then G can be written in the form $(u - x)^s S$, where s is the highest power of $(u - x)$ which divides $N(G)$, and $S \in \overline{K}(C)$ has neither a zero nor a pole at P.

Proof. We can write

$$G = G \cdot \frac{\overline{G}}{\overline{G}} = \frac{N(G)}{\overline{G}} = \frac{a^2 + abh - b^2 f}{a + b(h + v)}.$$

Let $N(G) = (u - x)^s d(u)$, where s is the highest power of $(u - x)$ which divides $N(G)$ (so $d(u) \in \overline{K}[u]^*$ and $d(x) \neq 0$). By Lemma 20, $\overline{G}(P) \neq 0$. Let $S = d(u)/\overline{G}$. Then $G = (u - x)^s d(u)/\overline{G}$ and $S(P) \neq 0, \infty$. □

Lemma 22 Let $P = (x, y)$ be a special point on C. Then $(u - x)$ can be written in the form $(v - y)^2 \cdot S(u, v)$, where $S(u, v) \in \overline{K}(C)$ has neither a zero nor a pole at P.

Proof. Let $H = (v - y)^2$ and $S = (u - x)/H$, and note that $(u - x) = H \cdot S$. We will show that $S(P) \neq 0, \infty$. Since P is a special point, $2y + h(x) = 0$. Consequently, since P is not a singular point, we have $h'(x)y - f'(x) \neq 0$. Also, $f(x) = y^2 + h(x)y = y^2 + (-2y)(y) = -y^2$. Now,

$$H(u, v) = (v - y)^2 = v^2 - 2yv + y^2 = f(u) - h(u)v - 2yv + y^2.$$

Hence

$$\frac{1}{S(u, v)} = \left(\frac{f(u) + y^2}{u - x}\right) - v\left(\frac{h(u) + 2y}{u - x}\right). \tag{2}$$

Notice that the right hand side of (2) is indeed a polynomial function. Let $s(u) = H(u, y)$, and observe that $s(x) = 0$. Moreover, $s'(u) = f'(u) - h'(u)y$, whence $s'(x) \neq 0$. Thus $(u - x)$ divides $s(u)$, but $(u - x)^2$ does not divide $s(u)$. It follows that the right hand side of (2) is non-zero at P, and hence that $S(P) \neq 0, \infty$, as required. □

Theorem 23 (*existence of uniformizing parameters*) Let $P \in C$. Then there exists a function $U \in \overline{K}(C)$ with $U(P) = 0$ such that the following property holds: for each polynomial function $G \in \overline{K}[C]^*$, there exists an integer d and function $S \in \overline{K}(C)$ such that $S(P) \neq 0, \infty$ and $G = U^d S$. Furthermore, the number d does not depend on the choice of U. The function U is called a *uniformizing parameter* for P.

Proof. Let $G(u, v) \in \overline{K}[C]^*$. If P is a finite point, suppose that $G(P) = 0$; if $P = \infty$, suppose that $G(P) = \infty$. (If $G(P) \neq 0, \infty$, then we can write $G = U^0 G$ where U is any polynomial in $\overline{K}[C]$ satisfying $U(P) = 0$.) We prove the theorem by finding a uniformizing parameter for each of the following cases: (i) $P = \infty$; (ii) P is an ordinary point; and (iii) P is a special point.

(i) We first show that a uniformizing parameter for the point $P = \infty$ is $U = u^g/v$. First note that $U(\infty) = 0$ since $\deg(u^g) < \deg(v)$. Next, write

$$G = \left(\frac{u^g}{v}\right)^d \left(\frac{v}{u^g}\right)^d G,$$

where $d = -\deg(G)$. Let $S = (v/u^g)^d G$. Since $\deg(v) - \deg(u^g) = 2g + 1 - 2g = 1$ and $d = -\deg(G)$, it follows that $\deg(u^{-gd} G) = \deg(v^{-d})$. Hence $S(\infty) \neq 0, \infty$.

(ii) Assume now that $P = (x, y)$ is an ordinary point. We show that a uniformizing parameter for P is $U = (u - x)$; observe that $U(P) = 0$. Write $G = a(u) - b(u)v$. Let $(u - x)^r$ be the highest power of $(u - x)$ which divides both $a(u)$ and $b(u)$, and write

$$G(u, v) = (u - x)^r (a_0(u) - b_0(u)v).$$

By Lemma 21, we can write $(a_0(u) - b_0(u)v) = (u-x)^s S$ for some integer $s \geq 0$, and $S \in \overline{K}(C)$ such that $S(P) \neq 0, \infty$. Hence $G = (u-x)^{r+s} S$ satisfies the statement of the theorem with $d = r + s$.

(iii) Assume now that $P = (x, y)$ is a special point. We show that a uniformizing parameter for P is $U = (v - y)$; observe that $U(P) = 0$. By replacing any powers of u greater than $2g$ with the equation of the curve, we can write

$$G(u,v) = u^{2g} b_{2g}(v) + u^{2g-1} b_{2g-1}(v) + \cdots + u b_1(v) + b_0(v),$$

where each $b_i(v) \in \overline{K}[v]$. Replacing all occurrences of u by $((u-x)+x)$ and expanding yields

$$\begin{aligned} G(u,v) &= (u-x)^{2g} \overline{b}_{2g}(v) + (u-x)^{2g-1} \overline{b}_{2g-1}(v) + \cdots + (u-x)\overline{b}_1(v) + \overline{b}_0(v) \\ &= (u-x) B(u,v) + \overline{b}_0(v), \end{aligned}$$

where each $\overline{b}_i(v) \in \overline{K}[v]$, and $B(u,v) \in \overline{K}[C]$. Now $G(P) = 0$ implies $\overline{b}_0(y) = 0$, and so we can write $\overline{b}_0(v) = (v-y)c(v)$ for some $c \in \overline{K}[v]$. By the proof of Lemma 22 (see equation (2)), we can write $(u-x) = (v-y)^2 / A(u,v)$, where $A(u,v) \in \overline{K}[C]$ and $A(P) \neq 0, \infty$. Hence

$$\begin{aligned} G &= (v-y)\left[\frac{(v-y)B(u,v)}{A(u,v)} + c(v)\right] \\ &= \frac{(v-y)}{A(u,v)}\left[(v-y)B(u,v) + A(u,v)c(v)\right] \\ &\stackrel{\text{def}}{=} \frac{(v-y)}{A(u,v)} G_1(u,v). \end{aligned}$$

Now if $G_1(P) \neq 0$, then we are done by taking $S = G_1/A$. On the other hand, if $G_1(P) = 0$, then $c(y) = 0$ and we can write $c(v) = (v-y)c_1(v)$ for some $c_1 \in \overline{K}[v]$. Hence

$$\begin{aligned} G &= (v-y)^2\left[\frac{B(u,v)}{A(u,v)} + c_1(v)\right] \\ &= \frac{(v-y)^2}{A(u,v)}\left[B(u,v) + A(u,v)c_1(v)\right] \\ &\stackrel{\text{def}}{=} \frac{(v-y)^2}{A(u,v)} G_2(u,v). \end{aligned}$$

Again, if $G_2(P) \neq 0$ then we are done. Otherwise, the whole process can be repeated. To see that the process terminates, suppose that we have pulled k factors of $v - y$. There are two cases to consider.

(a) If k is even, say $k = 2l$, we can write

$$G = \frac{(v-y)^{2l}}{A(u,v)^l} D(u,v)$$

where $D \in \overline{K}[C]$. Hence $A^l G = (v-y)^{2l} D = (u-x)^l A^l D$, whence $G = (u-x)^l D$. Taking norms of both sides yields $N(G) = (u-x)^{2l} N(D)$. Hence $k \leq \deg_u(N(G))$.

(b) If k is odd, say $k = 2l+1$, we can write

$$G = \frac{(v-y)^{2l+1}}{A(u,v)^{l+1}} D(u,v)$$

where $D \in \overline{K}[C]$. Hence $A^{l+1} G = (v-y)^{2l+1} D = (u-x)^l A^l (v-y) D$, whence $AG = (u-x)^l (v-y) D$. Taking norms of both sides yields $N(AG) = (u-x)^{2l} N(v-y) N(D)$. Hence $2l < \deg_u(N(AG))$, and so $k \leq \deg_u(N(AG))$.

In either case, k is bounded by $\deg_u(N(AG))$ and so the process must terminate.

To see that d is independent of the choice of U, suppose that U_1 is another uniformizing parameter for P. Since $U(P) = U_1(P) = 0$, we can write $U = U_1^a A$ and $U_1 = U^b B$, where $a \geq 1$, $b \geq 1$, $A, B \in \overline{K}(C)$, $A(P) \neq 0, \infty$, $B(P) \neq 0, \infty$. Thus $U = (U^b B)^a A = U^{ab} B^a A$. Dividing both sides by U yields $U^{ab-1} B^a A = 1$. Substituting P in both sides of this equation tells us $ab - 1 = 0$. Hence $a = b = 1$. Thus $G = U^d S = U_1^d (A^d S)$, where $A^d S$ has neither a zero nor a pole at P. □

The notion of a uniformizing parameter is next used to define the order of a polynomial function at a point. An alternative definition from [20], which is more convenient to use for computational purposes, is given in Definition 26. Lemma 27 establishes that these two definitions are in fact equivalent.

Definition 24 (*usual definition of order of a polynomial function at a point*) Let $G \in \overline{K}[C]^*$ and $P \in C$. Let $U \in \overline{K}(C)$ be a uniformizing parameter for P, and write $G = U^d S$ where $S \in \overline{K}(C)$, $S(P) \neq 0, \infty$. The *order of* G *at* P is defined to be $\mathrm{ord}_P(G) = d$.

Lemma 25 Let $G_1, G_2 \in \overline{K}[C]^*$ and $P \in C$, and let $\mathrm{ord}_P(G_1) = r_1$, $\mathrm{ord}_P(G_2) = r_2$.

(i) $\mathrm{ord}_P(G_1 G_2) = \mathrm{ord}_P(G_1) + \mathrm{ord}_P(G_2)$.

(ii) Suppose that $G_1 \neq -G_2$. If $r_1 \neq r_2$ then $\mathrm{ord}_P(G_1 + G_2) = \min(r_1, r_2)$. If $r_1 = r_2$ then $\mathrm{ord}_P(G_1 + G_2) \geq \min(r_1, r_2)$.

Proof. Let U be a uniformizing parameter for P. By Definition 24, we can write $G_1 = U^{r_1} S_1$ and $G_2 = U^{r_2} S_2$, where $S_1, S_2 \in \overline{K}(C)$, $S_1(P) \neq 0, \infty$, $S_2(P) \neq 0, \infty$. Without loss of generality, suppose that $r_1 \geq r_2$.

(i) $G_1G_2 = U^{r_1+r_2}(S_1S_2)$, from which it follows that $\mathrm{ord}_P(G_1G_2) = r_1 + r_2$.

(ii) $G_1 + G_2 = U^{r_2}(U^{r_1-r_2}S_1 + S_2)$. If $r_1 > r_2$ then $(U^{r_1-r_2}S_1)(P) = 0$, $S_2(P) \neq 0, \infty$, and so $\mathrm{ord}_P(G_1+G_2) = r_2$. If $r_1 = r_2$ then $(S_1+S_2)(P) \neq \infty$ (although it may be the case that $(S_1 + S_2)(P) = 0$), and so $\mathrm{ord}_P(G_1 + G_2) \geq r_2$. □

Definition 26 (*alternate definition of order of a polynomial function at a point*) Let $G = a(u) - b(u)v \in \overline{K}[C]^*$ and $P \in C$. The *order of* G *at* P, denoted $\mathrm{ord}_P(G)$, is defined as follows:

(i) If $P = (x, y)$ is a finite point, then let r be the highest power of $(u - x)$ which divides both $a(u)$ and $b(u)$, and write $G(u, v) = (u-x)^r(a_0(u) - b_0(u)v)$. If $a_0(x) - b_0(x)y \neq 0$ then let $s = 0$; otherwise, let s be the highest power of $(u-x)$ which divides $N(a_0(u) - b_0(u)v) = a_0^2 + a_0b_0h - b_0^2f$. If P is an ordinary point, then define $\mathrm{ord}_P(G) = r + s$. If P is a special point, then define $\mathrm{ord}_P(G) = 2r + s$.

(ii) If $P = \infty$ then

$$\mathrm{ord}_P(G) = -\max[2\deg_u(a),\ 2g + 1 + 2\deg_u(b)].$$

Lemma 27 Definition 24 and Definition 26 are equivalent. That is, if the order function of Definition 26 is denoted by $\overline{\mathrm{ord}}$, then $\mathrm{ord}_P(G) = \overline{\mathrm{ord}}_P(G)$ for all $P \in C$ and $G \in \overline{K}[C]^*$.

Proof. If $P = \infty$, the proof of the lemma follows directly from the proof of Theorem 23(i). For the case P is an ordinary point, the proof of the lemma follows directly from Lemma 21 and the proof of Theorem 23(ii).
Suppose now that $P = (x, y)$ is a special point, and let $G = a - bv$. Let r be the highest power of $(u - x)$ which divides both $a(u)$ and $b(u)$, and write

$$G = (u - x)^r(a_0(u) - b_0(u)v) \stackrel{\mathrm{def}}{=} (u - x)^r H(u, v).$$

Let $\mathrm{ord}_P(H) = s$. Then, by Lemma 22,

$$\mathrm{ord}_P(G) \ = \ \mathrm{ord}_P((u - x)^r) + \mathrm{ord}_P(H) \ = \ 2r + s.$$

Now, since $v - y$ is a uniformizing parameter for P, we can write

$$H(u, v) = (v - y)^s A_1/A_2, \quad \text{where } A_1,\ A_2 \in \overline{K}[C],\ A_1(P) \neq 0,\ A_2(P) \neq 0.$$

Multiplying both sides by A_2 and taking norms yields

$$N(A_2)N(H) = (y^2 + h(u)y - f(u))^s N(A_1).$$

Now, $N(A_1)(x) \neq 0$ since $A_1(P) \neq 0$ and P is special (Lemma 19). Similarly, $N(A_2)(x) \neq 0$. Also, $u = x$ is a root of the polynomial $y^2 + h(u)y - f(u)$. Moreover, $u = x$ is not a double root of $y^2 + h(u)y - f(u)$ since $h'(x)y - f'(x) \neq 0$. It follows that $(u - x)^s$ is the highest power of $(u - x)$ which divides $N(H)$. Hence $\overline{\mathrm{ord}}_P(G) = 2r + s = \mathrm{ord}_P(G)$. □

Lemma 28 is a generalization of Lemma 19.

Lemma 28 Let $G \in \overline{K}[C]^*$ and $P \in C$. Then $\mathrm{ord}_P(G) = \mathrm{ord}_{\widetilde{P}}(\overline{G})$.

Proof. There are two cases to consider.

(i) Suppose $P = \infty$; then $\widetilde{P} = \infty$. By Definitions 26(ii) and 15, $\mathrm{ord}_P(G) = -\deg(G)$ and $\mathrm{ord}_{\widetilde{P}}(\overline{G}) = \mathrm{ord}_P(\overline{G}) = -\deg(\overline{G})$. By Lemma 16(iii), $\deg(G) = \deg(\overline{G})$. Hence $\mathrm{ord}_P(G) = \mathrm{ord}_{\widetilde{P}}(\overline{G})$.

(ii) Suppose now that $P = (x, y)$ is a finite point. Let $G = a(u) - b(u)v = (u-x)^r H(u, v)$, where r is the highest power of $(u-x)$ which divides both $a(u)$ and $b(u)$ and $H(u, v) = a_0(u) - b_0(u)v$. If $H(x, y) \neq 0$ then let $s = 0$; otherwise, let s be the highest power of $(u-x)$ which divides $N(H)$. Now, $\overline{G} = (u-x)^r \overline{H}$, where $\overline{H} = (a_0 + b_0 h) + b_0 v$. Recall that $H(P) = 0$ if and only if $\overline{H}(\widetilde{P}) = 0$. Since $(u-x)$ does not divide both $a_0 + b_0 h$ and b_0 (since otherwise, $(u-x) | a_0$), and s is the highest power of $(u-x)$ which divides $N(H) = N(\overline{H})$, it follows from Definition 26 that $\mathrm{ord}_{\widetilde{P}}(\overline{G}) = \mathrm{ord}_P(G)$. □

Theorem 29 Let $G \in \overline{K}[C]^*$. Then G has a finite number of zeros and poles. Moreover, $\sum_{P \in C} \mathrm{ord}_P(G) = 0$.

Proof. Let $n = \deg(G)$; then $\deg_u(N(G)) = n$. We can write

$$N(G) = G\overline{G} = (u - x_1)(u - x_2) \cdots (u - x_n),$$

where $x_i \in \overline{K}$, and the x_i are not necessarily distinct. The only pole of G is at $P = \infty$, and $\mathrm{ord}_\infty(G) = -n$. If x_i is the u-coordinate of an ordinary point $P = (x_i, y_i)$ on C, then $\mathrm{ord}_P(u - x_i) = 1$ and $\mathrm{ord}_{\widetilde{P}}(u - x_i) = 1$, and $(u - x_i)$ has no other zeros. If x_i is the u-coordinate of a special point $P = (x_i, y_i)$ on C, then $\mathrm{ord}_P(u - x_i) = 2$, and $(u - x_i)$ has no other zeros. Hence, $N(G)$, and consequently also G, has a finite number of zeros and poles, and moreover $\sum_{P \in C \setminus \{\infty\}} \mathrm{ord}_P(N(G)) = 2n$. But, by Lemma 28, $\sum_{P \in C \setminus \{\infty\}} \mathrm{ord}_P(G) = \sum_{P \in C \setminus \{\infty\}} \mathrm{ord}_P(\overline{G})$, and hence $\sum_{P \in C \setminus \{\infty\}} \mathrm{ord}_P(G) = n$. We conclude that $\sum_{P \in C} \mathrm{ord}_P(G) = 0$. □

Definition 30 (*order of a rational function at a point*) Let $R = G/H \in \overline{K}(C)^*$ and $P \in C$. The *order of R at P* is defined to be $\mathrm{ord}_P(R) = \mathrm{ord}_P(G) - \mathrm{ord}_P(H)$.

It can readily be verified that $\mathrm{ord}_P(R)$ does not depend on the choice of G and H, and that Lemma 25 and Theorem 29 are also true for non-zero rational functions.

5 Divisors

This section presents the basic properties of divisors and introduces the jacobian of a hyperelliptic curve.

Definition 31 (*divisor, degree, order*) A *divisor* D is a formal sum of points in C

$$D = \sum_{P \in C} m_P P, \quad m_P \in \mathbb{Z},$$

where only a finite number of the m_P are non-zero. The *degree* of D, denoted $\deg D$, is the integer $\sum_{P \in C} m_P$. The *order* of D at P is the integer m_P; we write $\mathrm{ord}_P(D) = m_P$.

The set of all divisors, denoted $\mathbf{D}$, forms an additive group under the addition rule:

$$\sum_{P \in C} m_P P + \sum_{P \in C} n_P P = \sum_{P \in C} (m_P + n_P) P.$$

The set of all divisors of degree 0, denoted $\mathbf{D}^0$, is a subgroup of $\mathbf{D}$.

Definition 32 (*gcd of divisors*) Let $D_1 = \sum_{P \in C} m_P P$ and $D_2 = \sum_{P \in C} n_P P$ be two divisors. The greatest common divisor of D_1 and D_2 is defined to be

$$\gcd(D_1, D_2) = \sum_{P \in C} \min(m_P, n_P) P - \left(\sum_{P \in C} \min(m_P, n_P) \right) \infty.$$

(Note that $\gcd(D_1, D_2) \in \mathbf{D}^0$.)

Definition 33 (*divisor of a rational function*) Let $R \in \overline{K}(C)^*$. The *divisor of* R is

$$\mathrm{div}(R) = \sum_{P \in C} (\mathrm{ord}_P R) P.$$

Note that if $R = G/H$ then $\mathrm{div}(R) = \mathrm{div}(G) - \mathrm{div}(H)$. Theorem 29 shows that the divisor of a rational function is indeed a finite formal sum and has degree 0.

Example 34 If $P = (x, y)$ is an ordinary point on C, then $\mathrm{div}(u - x) = P + \tilde{P} - 2\infty$. If $P = (x, y)$ is a special point on C, then $\mathrm{div}(u - x) = 2P - 2\infty$.

Lemma 35 Let $G \in \overline{K}[C]^*$, and let $\mathrm{div}(G) = \sum_{P \in C} m_P P$. Then $\mathrm{div}(\overline{G}) = \sum_{P \in C} m_P \tilde{P}$.

Proof. The result follows directly from Lemma 28. □

If $R_1, R_2 \in \overline{K}(C)^*$ then it follows from Lemma 25(i) that $\mathrm{div}(R_1 R_2) = \mathrm{div}(R_1) + \mathrm{div}(R_2)$.

Definition 36 (*principal divisor, jacobian*) A divisor $D \in \mathbf{D}^0$ is called a *principal divisor* if $D = \mathrm{div}(R)$ for some rational function $R \in \overline{K}(C)^*$. The set of all principal divisors, denoted $\mathbf{P}$, is a subgroup of $\mathbf{D}^0$. The quotient group $\mathbf{J} = \mathbf{D}^0/\mathbf{P}$ is called the *jacobian* of the curve C. If D_1, $D_2 \in \mathbf{D}^0$ then we write $D_1 \sim D_2$ if $D_1 - D_2 \in \mathbf{P}$; D_1 and D_2 are said to be *equivalent* divisors.

Definition 37 (*support of a divisor*) Let $D = \sum_{P \in C} m_P P$ be a divisor. The *support* of D is the set $\mathrm{supp}(D) = \{P \in C \mid m_P \neq 0\}$.

Definition 38 (*semi-reduced divisor*) A *semi-reduced divisor* is a divisor of the form $D = \sum m_i P_i - (\sum m_i)\infty$, where each $m_i \geq 0$ and the P_i's are finite points such that when $P_i \in \mathrm{supp}(D)$ then $\widetilde{P_i} \notin \mathrm{supp}(D)$, unless $P_i = \widetilde{P_i}$, in which case $m_i = 1$.

Lemma 39 For each divisor $D \in \mathbf{D}^0$ there exists a semi-reduced divisor D_1 ($D_1 \in \mathbf{D}^0$) such that $D \sim D_1$.

Proof. Let $D = \sum_{P \in C} m_P P$. Let (C_1, C_2) be a partition of the set of ordinary points on C such that (i) $P \in C_1$ if and only if $\widetilde{P} \in C_2$; and (ii) if $P \in C_1$ then $m_P \geq m_{\widetilde{P}}$. Let C_0 be the set of special points on C. Then we can write

$$D = \sum_{P \in C_1} m_P P + \sum_{P \in C_2} m_P P + \sum_{P \in C_0} m_P P - m\infty.$$

Consider the following divisor

$$D_1 = D - \sum_{P=(x,y) \in C_2} m_P \mathrm{div}(u - x) - \sum_{P=(x,y) \in C_0} \left\lfloor \frac{m_P}{2} \right\rfloor \mathrm{div}(u - x).$$

Then $D_1 \sim D$. Finally, by Example 34, we have

$$D_1 = \sum_{P \in C_1} (m_P - m_{\widetilde{P}}) P + \sum_{P \in C_0} \left(m_P - 2 \left\lfloor \frac{m_P}{2} \right\rfloor \right) P - m_1 \infty$$

for some $m_1 \in \mathbb{Z}$, and hence D_1 is a semi-reduced divisor. □

6 Representing semi-reduced divisors

This section describes a polynomial representation for semi-reduced divisors of the jacobian. It leads to an efficient algorithm for adding elements of the jacobian (see §8).

Lemma 40 Let $P = (x, y)$ be an ordinary point on C, and let $R \in \overline{K}(C)$ be a rational function which does not have a pole at P. Then for any $k \geq 0$, there are unique elements $c_0, c_1, \ldots, c_k \in \overline{K}$ and $R_k \in \overline{K}(C)$ such that $R = \sum_{i=0}^{k} c_i (u - x)^i + (u - x)^{k+1} R_k$, and where R_k does not have a pole at P.

Proof. There is a unique $c_0 \in \overline{K}$, namely $c_0 = R(x,y)$, such that P is a zero of $R - c_0$. Since $(u-x)$ is a uniformizing parameter for P, we can write $R - c_0 = (u-x)R_1$ for some (unique) $R_1 \in \overline{K}(C)$ with $\mathrm{ord}_P(R_1) \geq 0$. Hence $R = c_0 + (u-x)R_1$. The lemma now follows by induction. □

Lemma 41 Let $P = (x,y)$ be an ordinary point on C. Then for each $k \geq 1$, there exists a unique polynomial $b_k(u) \in \overline{K}[u]$ such that

(i) $\deg_u b_k < k$;

(ii) $b_k(x) = y$; and

(iii) $b_k^2(u) + b_k(u)h(u) \equiv f(u) \pmod{(u-x)^k}$.

Proof. Let $v = \sum_{i=0}^{k-1} c_i(u-x)^i + (u-x)^k R_{k-1}$ where $c_i \in \overline{K}$ and $R_{k-1} \in \overline{K}(C)$. Define $b_k(u) = \sum_{i=0}^{k-1} c_i(u-x)^i$. From the proof of Lemma 40, we know that $c_0 = y$, and hence $b_k(x) = y$. Finally, since $v^2 + h(u)v = f(u)$, reducing both sides modulo $(u-x)^k$ yields $b_k(u)^2 + b_k(u)h(u) \equiv f(u) \pmod{(u-x)^k}$. Uniqueness is easily proved by induction on k. □

The following theorem shows how a semi-reduced divisor can be represented as the gcd of the divisors of two polynomial functions.

Theorem 42 Let $D = \sum m_i P_i - (\sum m_i)\infty$ be a semi-reduced divisor, where $P_i = (x_i, y_i)$. Let $a(u) = \prod (u - x_i)^{m_i}$. Let $b(u)$ be the unique polynomial satisfying: (i) $\deg_u b < \deg_u a$; (ii) $b(x_i) = y_i$ for all i for which $m_i \neq 0$; and (iii) $a(u)$ divides $(b(u)^2 + b(u)h(u) - f(u))$. Then $D = \gcd(\mathrm{div}(a(u)), \mathrm{div}(b(u) - v))$.
Notation: $\gcd(\mathrm{div}(a(u)), \mathrm{div}(b(u) - v))$ will usually be abbreviated to $\mathrm{div}(a(u), b(u) - v)$ or, more simply, to $\mathrm{div}(a, b)$.

Proof. Let C_1 be the set of ordinary points in $\mathrm{supp}(D)$, and let C_0 be the set of special points in $\mathrm{supp}(D)$. Let $C_2 = \{\tilde{P} : P \in C_1\}$. Then we can write

$$D = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - m\infty,$$

where $m_i, m \in \mathbb{Z}_{\geq 1}$.

We first prove that there does indeed exist a unique polynomial $b(u)$ which satisfies the conditions of the theorem. By Lemma 41, for each $P_i \in C_1$ there exists a unique polynomial $b_i(u) \in \overline{K}[u]$ satisfying (i) $\deg_u b_i < m_i$; (ii) $b_i(x_i) = y_i$; and (iii) $(u-x_i)^{m_i} | b_i^2(u) + b_i(u)h(u) - f(u)$. It can be easily verified that for each $P_i \in C_0$, $b_i(u) = y_i$ is the unique polynomial satisfying (i) $\deg_u b_i < 1$; (ii) $b_i(x_i) = y_i$; and (iii) $(u - x_i) | b_i^2(u) + b_i(u)h(u) - f(u)$. By the Chinese Remainder Theorem for polynomials, there is a unique polynomial $b(u) \in \overline{K}[u]$, $\deg_u b < \sum m_i$, such that

$$b(u) \equiv b_i(u) \pmod{(u-x_i)^{m_i}} \quad \text{for all } i.$$

It can now be verified that $b(u)$ satisfies conditions (i), (ii) and (iii) of the statement of the theorem.

Now,

$$\mathrm{div}(a(u)) = \mathrm{div}\left(\prod (u - x_i)^{m_i}\right) = \sum_{P_i \in C_0} 2P_i + \sum_{P_i \in C_1} m_i P_i + \sum_{P_i \in C_1} m_i \tilde{P}_i - (*)\infty.$$

And,

$$\mathrm{div}(b(u) - v) = \sum_{P_i \in C_0} t_i P_i + \sum_{P_i \in C_1} s_i P_i + \sum_{P_i \in C \setminus (C_0 \cup C_1 \cup C_2 \cup \{\infty\})} m_i P_i - (*)\infty,$$

where each $s_i \geq m_i$ since $(u - x_i)^{m_i}$ divides $N(b - v) = b^2 + hb - f$. Now, if $P = (x, y) \in C_0$, then $(u - x)$ divides $b^2 + bh - f$. The derivative of this polynomial evaluated at $u = x$ is

$$\begin{aligned} 2b(x)b'(x) + b'(x)h(x) + b(x)h'(x) - f'(x) &= b'(x)(2y + h(x)) + (h'(x)y - f'(x)) \\ &= h'(x)y - f'(x), \quad \text{since } 2y + h(x) = 0 \\ &\neq 0. \end{aligned}$$

Hence $u = x$ is a simple root of $N(b - v) = b^2 + bh - f$, and hence $t_i = 1$ for all i. Therefore

$$\gcd(a(u), b(u) - v) = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - m\infty = D,$$

as required. □

Note that the zero divisor is represented as $\mathrm{div}(1, 0)$. The next result follows from the proof of Theorem 42.

Lemma 43 Let $a(u), b(u) \in \overline{K}[u]$ be such that $\deg_u b < \deg_u a$. If $a | (b^2 + bh - f)$ then $\mathrm{div}(a, b)$ is semi-reduced.

7 Reduced divisors

This section defines the notion of a reduced divisor and proves that each coset of the quotient group $\mathbf{J} = \mathbf{D}^0/\mathbf{P}$ has exactly one reduced divisor. We can therefore identify each coset with its reduced divisor.

Definition 44 (*reduced divisor*) Let $D = \sum m_i P_i - (\sum m_i)\infty$ be a semi-reduced divisor. If $\sum m_i \leq g$ (g is the genus of C) then D is called a *reduced divisor*.

Definition 45 (*norm of a divisor*) Let $D = \sum_{P \in C} m_P P$ be a divisor. The *norm* of D is defined to be

$$|D| = \sum_{P \in C \setminus \{\infty\}} |m_P|.$$

Note that given a divisor $D \in \mathbf{D}^0$, the operation described in the proof of Lemma 39 produces a semi-reduced divisor D_1 such that $D_1 \sim D$ and $|D_1| \leq |D|$.

Lemma 46 Let R be a rational function in $\overline{K}(C)^*$. If R has no finite poles, then R is a polynomial function.

Proof. Let $R = G/H$, where $G, H \in \overline{K}[C]^*$. Then $R = \frac{G}{H} \cdot \frac{\overline{H}}{\overline{H}} = G\overline{H}/N(H)$, and so we can write $R = (a - bv)/c$, where $a, b, c \in \overline{K}[u]$, $c \neq 0$. Let $x \in \overline{K}$ be a root of c. Let $P = (x, y) \in C$ where $y \in \overline{K}$, and let $d \geq 1$ be the highest power of $(u - x)$ which divides c.

If P is ordinary, then $\mathrm{ord}_P(c) = \mathrm{ord}_{\widetilde{P}}(c) = d$. Since R has no finite poles, $\mathrm{ord}_P(a - bv) \geq d$ and $\mathrm{ord}_{\widetilde{P}}(a - bv) \geq d$. Now, since P and $\widetilde{P}$ are both zeros of $a - bv$, it is true that $a(x) = 0$ and $b(x) = 0$. It follows that $\mathrm{ord}_P(a) \geq d$ and $\mathrm{ord}_P(b) \geq d$. Hence $(u - x)^d$ is a common divisor of a and b, which can be cancelled with the factor $(u - x)^d$ of c.

Suppose now that P is special. Then $\mathrm{ord}_P(c) = 2d$. Since R has no finite poles, $\mathrm{ord}_P(a - bv) \geq 2d$. Then, as in part (iii) of the proof of Theorem 23, we can write

$$a - bv = \frac{(v - y)^{2d} D}{A^d},$$

where $A, D \in \overline{K}[C]^*$ and A satisfies $(v - y)^2 = (u - x)A$. Hence $a - bv = (u - x)^d D$. Again, the factor $(u - x)^d$ of $a - bv$ can be cancelled with the factor $(u - x)^d$ of c.

This can be repeated for all roots of c; it follows that R is a polynomial function. □

Theorem 47 For each divisor $D \in \mathbf{D}^0$ there exists a unique reduced divisor D_1 such that $D \sim D_1$.

Proof. (*Existence*) Let D' be a semi-reduced divisor such that $D' \sim D$ and $|D'| \leq |D|$ produced as in the proof of Lemma 39. If $|D'| \leq g$ then D' is reduced and we are done. Otherwise, let $P_1, P_2, \ldots, P_{g+1}$ be finite points in $\mathrm{supp}(D')$, not necessarily distinct. (A point P cannot occur in this list more than $\mathrm{ord}_P(D')$ times.) Let $\mathrm{div}(a(u), b(u))$ be the representation of the divisor

$$P_1 + P_2 + \cdots + P_{g+1} - (g + 1)\infty$$

as given by Theorem 42. Since $\deg_u(b) \leq g$, we have $\deg(b(u) - v) = 2g + 1$, and hence

$$\mathrm{div}(b(u) - v) = P_1 + P_2 + \cdots + P_{g+1} + Q_1 + \cdots + Q_g - (2g + 1)\infty$$

for some finite points $Q_1, Q_2, \ldots, Q_g$. Subtracting this divisor from D' gives a divisor D'', where $D'' \sim D' \sim D$ and $|D''| < |D'|$. We can now produce another semi-reduced divisor $D''' \sim D''$ such that $|D'''| \leq |D''|$. After doing this a finite number of times, we obtain a semi-reduced divisor D_1 with $|D_1| \leq g$, and we are done.[3]

[3]Algorithm 2 in Section 8 describes an efficient algorithm which, given a semi-reduced divisor $D = \mathrm{div}(a, b)$, finds a reduced divisor D_1 such that $D \sim D_1$; the algorithm only uses a and b.

(*Uniqueness*) Suppose that D_1 and D_2 are two reduced divisors with $D_1 \sim D_2$, $D_1 \neq D_2$. Let D_3 be a semi-reduced divisor with $D_3 \sim D_1 - D_2$ obtained as in the proof of Lemma 39. Since $D_1 \neq D_2$, there is a point P such that $\mathrm{ord}_P(D_1) \neq \mathrm{ord}_P(D_2)$. Suppose, without loss of generality, that $\mathrm{ord}_P(D_1) = m_1 \geq 1$, and either (i) $\mathrm{ord}_P(D_2) = 0$ and $\mathrm{ord}_{\widetilde{P}}(D_2) = 0$; or (ii) $\mathrm{ord}_P(D_2) = m_2$ with $1 \leq m_2 < m_1$; or (iii) $\mathrm{ord}_{\widetilde{P}}(D_2) = m_2$ with $1 \leq m_2 \leq m_1$. (If P is special then only (i) can occur.) In case (i), $\mathrm{ord}_P(D_3) = m_1 \geq 1$. In case (ii), $\mathrm{ord}_P(D_3) = (m_1 - m_2) \geq 1$. In case (iii), $\mathrm{ord}_P(D_3) = (m_1 + m_2) \geq 1$. In all cases, $\mathrm{ord}_P(D_3) \geq 1$, and so $D_3 \neq 0$. Also, $|D_3| \leq |D_1 - D_2| \leq |D_1| + |D_2| \leq 2g$. Let G be a rational function in $\overline{K}(C)^*$ such that $\mathrm{div}(G) = D_3$; since $D_1 \sim D_2$, and $D_3 \sim D_1 - D_2$, we know that D_3 is principal and hence such a function G exists. By Lemma 46, since G has no finite poles, it must be a polynomial function. Then $G = a(u) - b(u)v$ for some $a, b \in \overline{K}[u]$. Since $\deg(v) = 2g + 1$ and $\deg(G) = |D_3| \leq 2g$, we must have $b(u) = 0$. Suppose that $\deg_u(a(u)) \geq 1$, and let $x \in \overline{K}$ be a root of $a(u)$. Let $P = (x, y)$ be a point on C. Now, if P is ordinary, then both P and $\widetilde{P}$ are zeros of G, contradicting the fact that D_3 is semi-reduced. If P is special, then it must also be a zero of G of order at least 2, again contradicting the fact that D_3 is semi-reduced. Thus, $\deg_u(a(u)) = 0$ and so $D_3 = 0$, a contradiction. □

8 Adding reduced divisors

Let C be a hyperelliptic curve of genus g defined over a finite field K, and let J be the jacobian of C. Let $P = (x, y) \in C$, and let σ be an automorphism of $\overline{K}$ over K. Then $P^\sigma \stackrel{\text{def}}{=} (x^\sigma, y^\sigma)$ is also a point on C.

Definition 48 (*field of definition of a divisor*) A divisor $D = \sum m_P P$ is said to be *defined over* K if $D^\sigma \stackrel{\text{def}}{=} \sum m_P P^\sigma$ is equal to D for all automorphisms σ of $\overline{K}$ over K.

Note that if D is defined over K, it does not mean that each point in the support of D is a K-rational point. A principal divisor is defined over K if and only if it is the divisor of a rational function that has coefficients in K. The set $J(K)$ of all divisor classes in J that have a representative that is defined over K is a subgroup of J. Each element of $J(K)$ has a unique representation as a reduced divisor $\mathrm{div}(a, b)$, where $a, b \in K[u]$, $\deg_u a \leq g$, $\deg_u b < \deg_u a$, and hence $J(K)$ is in fact a finite abelian group. This section presents an efficient algorithm for adding elements in this group.

Let $D_1 = \mathrm{div}(a_1, b_1)$ and $D_2 = \mathrm{div}(a_2, b_2)$ be two reduced divisors defined over K (so a_1, a_2, b_1, $b_2 \in K[u]$). Algorithm 1 finds a semi-reduced divisor $D = \mathrm{div}(a, b)$ with $a, b \in K[u]$, such that $D \sim D_1 + D_2$. Algorithm 2 reduces D to an equivalent reduced divisor D'. Notation: $b \bmod a$ denotes the remainder polynomial when b is divided by a.

Algorithms 1 and 2 were presented by Koblitz [20], and generalized earlier algorithms of Cantor [5] which assumed that $h(u) = 0$ and $\text{char}(K) \neq 2$. [4]

Algorithm 1
Input: Reduced divisors $D_1 = \text{div}(a_1, b_1)$ and $D_2 = \text{div}(a_2, b_2)$ both defined over K.
Output: A semi-reduced divisor $D = \text{div}(a, b)$ defined over K such that $D \sim D_1 + D_2$.

1. Use the extended Euclidean algorithm to find polynomials d_1, e_1, $e_2 \in K[u]$ where $d_1 = \gcd(a_1, a_2)$ and $d_1 = e_1 a_1 + e_2 a_2$.

2. Use the extended Euclidean algorithm to find polynomials d, c_1, $c_2 \in K[u]$ where $d = \gcd(d_1, b_1 + b_2 + h)$ and $d = c_1 d_1 + c_2(b_1 + b_2 + h)$.

3. Let $s_1 = c_1 e_1$, $s_2 = c_1 e_2$, and $s_3 = c_2$, so that

$$d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h). \tag{3}$$

4. Set

$$a = a_1 a_2 / d^2 \tag{4}$$

and

$$b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \bmod a. \tag{5}$$

Theorem 49 (*Algorithm 1 works*) Let $D_1 = \text{div}(a_1, b_1)$ and $D_2 = \text{div}(a_2, b_2)$ be semi-reduced divisors. Let a and b be defined as in equations (4) and (5). Then $D = \text{div}(a, b)$ is a semi-reduced divisor and $D \sim D_1 + D_2$.

Proof. We first verify that b is a polynomial. Using equation (3), we can write

$$\begin{aligned} \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} &= \frac{b_2(d - s_2 a_2 - s_3(b_1 + b_2 + h)) + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \\ &= b_2 + \frac{s_2 a_2(b_1 - b_2) - s_3(b_2^2 + b_2 h - f)}{d}. \end{aligned}$$

Since $d | a_2$ and $a_2 | (b_2^2 + b_2 h - f)$, b is indeed a polynomial.

[4] Koblitz did not provide proofs of correctness of the algorithms, and Cantor's proof contains some errors. In defining the polynomials $a(u)$ and $b(u)$ which represent the semi-reduced divisor $D = \sum_{P_i \in C} m_i P_i$ (for the case of hyperelliptic curves with $h(u) = 0$), Cantor incorrectly states that the condition that $a | (b^2 - f)$ is equivalent to the condition that $b - y_i$ be divisible by $(u - x_i)^{m_i}$ for all i (where $P_i = (x_i, y_i)$).

Let $b = (s_1a_1b_2 + s_2a_2b_1 + s_3(b_1b_2 + f))/d + sa$, where $s \in K[u]$. Now,

$$\begin{aligned} b - v &= \frac{s_1a_1b_2 + s_2a_2b_1 + s_3(b_1b_2 + f) - dv}{d} + sa \\ &= \frac{s_1a_1b_2 + s_2a_2b_1 + s_3(b_1b_2 + f) - s_1a_1v - s_2a_2v - s_3(b_1 + b_2 + h)v}{d} + sa \\ &= \frac{s_1a_1(b_2 - v) + s_2a_2(b_1 - v) + s_3(b_1 - v)(b_2 - v)}{d} + sa. \end{aligned} \tag{6}$$

From (6) it is not hard to see that $a|(b^2 + bh - f)$. Namely, $b^2 + bh - f$ is obtained by multiplying the left side of (6) by its conjugate: $(b-v)(b+v+h) = b^2+bh-f$. Thus, to see that $a|(b^2+bh-f)$ it suffices to show that a_1a_2 divides the product of $(s_1a_1(b_2-v)+s_2a_2(b_1-v)+s_3(b_1-v)(b_2-v))$ with its conjugate; this follows because $a_1|(b_1^2+b_1h-f) = (b_1-v)(b_1+v+h)$ and $a_2|(b_2^2 + b_2h - f) = (b_2 - v)(b_2 + v + h)$. Lemma 43 now implies that $\mathrm{div}(a, b)$ is a semi-reduced divisor.

We now prove that $D \sim D_1 + D_2$. There are two cases to consider.

(i) Let $P = (x, y)$ be an ordinary point. There are two subcases to consider.

(a) Suppose that $\mathrm{ord}_P(D_1) = m_1$, $\mathrm{ord}_{\widetilde{P}}(D_1) = 0$, $\mathrm{ord}_P(D_2) = m_2$, and $\mathrm{ord}_{\widetilde{P}}(D_2) = 0$, where $m_1 \geq 0$, $m_2 \geq 0$. Now, $\mathrm{ord}_P(a_1) = m_1$, $\mathrm{ord}_P(a_2) = m_2$, $\mathrm{ord}_P(b_1 - v) \geq m_1$, and $\mathrm{ord}_P(b_2 - v) \geq m_2$. If $m_1 = 0$ or $m_2 = 0$ (or both) then $\mathrm{ord}_P(d_1) = 0$, whence $\mathrm{ord}_P(d) = 0$ and $\mathrm{ord}_P(a) = m_1 + m_2$. If $m_1 \geq 1$ and $m_2 \geq 1$, then, since $(b_1 + b_2 + h)(x) = 2y + h(x) \neq 0$, we have $\mathrm{ord}_P(d) = 0$ and $\mathrm{ord}_P(a) = m_1 + m_2$.

From equation (6), it follows that

$$\mathrm{ord}_P(b - v) \geq \min\{m_1 + m_2, m_2 + m_1, m_1 + m_2\} = m_1 + m_2.$$

Hence $\mathrm{ord}_P(D) = m_1 + m_2$.

(b) Suppose that $\mathrm{ord}_P(D_1) = m_1$ and $\mathrm{ord}_{\widetilde{P}}(D_2) = m_2$, where $m_1 \geq m_2 \geq 1$. We have $\mathrm{ord}_P(a_1) = m_1$, $\mathrm{ord}_P(a_2) = m_2$, $\mathrm{ord}_P(d_1) = m_2$, $\mathrm{ord}_P(b_1-v) \geq m_1$, $\mathrm{ord}_P(b_2-v) = 0$, and $\mathrm{ord}_{\widetilde{P}}(b_2-v) \geq m_2$. The last inequality implies that $\mathrm{ord}_P(b_2+h+v) \geq m_2$, and hence $\mathrm{ord}_P(b_1+b_2+h) \geq m_2$ or $(b_1+b_2+h) = 0$. It follows that $\mathrm{ord}_P(d) = m_2$ and $\mathrm{ord}_P(a) = m_1 - m_2$.

From equation (6), it follows that

$$\mathrm{ord}_P(b - v) \geq \min\{m_1 + 0, m_2 + m_1, m_1 + 0\} - m_2 = m_1 - m_2.$$

Hence $\mathrm{ord}_P(D) = m_1 - m_2$.

(ii) Let $P = (x, y)$ be a special point. There are two subcases to consider.

(a) Suppose that $\mathrm{ord}_P(D_1) = 1$ and $\mathrm{ord}_P(D_2) = 1$. Then $\mathrm{ord}_P(a_1) = 2$, $\mathrm{ord}_P(a_2) = 2$, and $\mathrm{ord}_P(d_1) = 2$. Now, $(b_1+b_2+h)(x) = 2y+h(x) = 0$, whence $\mathrm{ord}_P(b_1+b_2+h) \geq 2$ or $(b_1 + b_2 + h) = 0$. It follows that $\mathrm{ord}_P(d) = 2$ and $\mathrm{ord}_P(a) = 0$. Hence $\mathrm{ord}_P(D) = 0$.

(b) Suppose that $\mathrm{ord}_P(D_1) = 1$ and $\mathrm{ord}_P(D_2) = 0$. Then $\mathrm{ord}_P(a_1) = 2$, $\mathrm{ord}_P(a_2) = 0$, whence $\mathrm{ord}_P(d_1) = \mathrm{ord}_P(d) = 0$ and $\mathrm{ord}_P(a) = 2$. Since $\mathrm{ord}_P(b_1 - v) = 1$, it follows from equation (6) that $\mathrm{ord}_P(b - v) \geq 1$. It can be inferred from equation (6) that $\mathrm{ord}_P(b - v) \geq 2$ only if $\mathrm{ord}_P(s_2a_2 + s_3(b_2 - v)) \geq 1$. If this is indeed the case, then $\mathrm{ord}_P(s_2a_2 + s_3(b_2 + h + v)) \geq 1$, and hence $\mathrm{ord}_P(s_2a_2 + s_3(b_1 + b_2 + h)) \geq 1$ (or $s_2a_2 + s_3(b_1 + b_2 + h) = 0$). It now follows from equation (3) that $\mathrm{ord}_P(d) \geq 1$, a contradiction. Hence $\mathrm{ord}_P(b - v) = 1$, whence $\mathrm{ord}_P(D) = 1$. □

Example 50 (*adding two reduced divisors*) Consider the hyperelliptic curve $C : v^2 + (u^2 + u)v = u^5 + u^3 + 1$ of genus $g = 2$ over the finite field $\mathbb{F}_{2^5}$ (see Example 7). $P = (\alpha^{30}, 0)$ is an ordinary point in $C(\mathbb{F}_{2^5})$ and the opposite of P is $\tilde{P} = (\alpha^{30}, \alpha^{16})$. $Q_1 = (0, 1)$ and $Q_2 = (1, 1)$ are special points in $C(\mathbb{F}_{2^5})$. The following are examples of computing the semi-reduced divisor $D = \mathrm{div}(a, b) = D_1 + D_2$, for sample reduced divisors D_1 and D_2 (see Algorithm 1).

(i) Let $D_1 = P + Q_1 - 2\infty$ and $D_2 = \tilde{P} + Q_2 - 2\infty$ be two reduced divisors. Then $D_1 = \mathrm{div}(a_1, b_1)$ where $a_1 = u(u + \alpha^{30})$, $b_1 = \alpha u + 1$, and $D_2 = \mathrm{div}(a_2, b_2)$ where $a_2 = (u + 1)(u + \alpha^{30})$, $b_2 = \alpha^{23}u + \alpha^{12}$.

1. $d_1 = \gcd(a_1, a_2) = u + \alpha^{30}$; $d_1 = a_1 + a_2$.
2. $d = \gcd(d_1, b_1 + b_2 + h) = u + \alpha^{30}$; $d = 1 \cdot d_1 + 0 \cdot (b_1 + b_2 + h)$.
3. $d = a_1 + a_2 + 0 \cdot (b_1 + b_2 + h)$.
4. Set $a = a_1a_2/d^2 = u(u + 1) = u^2 + u$, and

$$\begin{aligned} b &= \frac{1 \cdot a_1b_2 + 1 \cdot a_2b_1 + 0 \cdot (b_1b_2 + f)}{d} \bmod a \\ &\equiv 1 \pmod{a}. \end{aligned}$$

Check:

$$\begin{aligned} \mathrm{div}(a) &= 2Q_1 + 2Q_2 - 4\infty \\ \mathrm{div}(b - v) &= Q_1 + Q_2 + \sum_{i=1}^{3} P_i - 5\infty, \text{ where } P_i \neq Q_1, Q_2 \\ \mathrm{div}(a, b) &= Q_1 + Q_2 - 2\infty. \end{aligned}$$

(ii) Let $D_1 = P + Q_1 - 2\infty$ and $D_2 = Q_1 + Q_2 - 2\infty$. Then $D_1 = \mathrm{div}(a_1, b_1)$ where $a_1 = u(u + \alpha^{30})$, $b_1 = \alpha u + 1$, and $D_2 = \mathrm{div}(a_2, b_2)$ where $a_2 = u(u + 1)$, $b_2 = 1$.

1. $d_1 = \gcd(a_1, a_2) = u$; $d_1 = \alpha^{14} a_1 + \alpha^{14} a_2$.
2. $d = \gcd(d_1, b_1 + b_2 + h) = u$; $d = 1 \cdot u + 0 \cdot (b_1 + b_2 + h)$.
3. $d = \alpha^{14} a_1 + \alpha^{14} a_2 + 0 \cdot (b_1 + b_2 + h)$.
4. $a = (u + \alpha^{30})(u + 1)$; $b \equiv \alpha^{14} u + \alpha^{13} \pmod{a}$.

Check:

$$\begin{aligned} \mathrm{div}(a) &= 2Q_2 + P + \tilde{P} - 4\infty \\ \mathrm{div}(b - v) &= P + Q_2 + \sum_{i=1}^{3} P_i - 5\infty, \text{ where } P_i \neq P, \tilde{P}, Q_2 \\ \mathrm{div}(a, b) &= P + Q_2 - 2\infty. \end{aligned}$$

(iii) Let $D_1 = P + Q_1 - 2\infty$ and $D_2 = P + Q_2 - 2\infty$. Then $D_1 = \mathrm{div}(a_1, b_1)$ where $a_1 = u(u + \alpha^{30})$, $b_1 = \alpha u + 1$, and $D_2 = \mathrm{div}(a_2, b_2)$ where $a_2 = (u + \alpha^{30})(u + 1)$, $b_2 = \alpha^{14} u + \alpha^{13}$.

1. $d_1 = \gcd(a_1, a_2) = (u + \alpha^{30})$; $d_1 = 1 \cdot a_1 + 1 \cdot a_2$.
2. $d = \gcd(d_1, b_1 + b_2 + h) = 1$.
3. $d = (\alpha^{15} u + \alpha^4) a_1 + (\alpha^{15} u + \alpha^4) a_2 + \alpha^{15} \cdot (b_1 + b_2 + h)$.
4. $a = u(u + 1)(u + \alpha^{30})^2$; $b \equiv \alpha^{17} u^3 + \alpha^{26} u^2 + \alpha^2 u + 1 \pmod{a}$.

Check:

$$\begin{aligned} \mathrm{div}(a) &= 2P + 2\tilde{P} + 2Q_1 + 2Q_2 - 8\infty \\ \mathrm{div}(b - v) &= 2P + Q_1 + Q_2 + \sum_{i=1}^{2} P_i - 6\infty, \text{ where } P_i \neq P, \tilde{P}, Q_1, Q_2 \\ \mathrm{div}(a, b) &= 2P + Q_1 + Q_2 - 4\infty. \end{aligned}$$

Algorithm 2
Input: A semi-reduced divisor $D = \mathrm{div}(a, b)$ defined over K.
Output: The (unique) reduced divisor $D' = \mathrm{div}(a', b')$ such that $D' \sim D$.

1. Set

$$a' = (f - bh - b^2)/a \tag{7}$$

and

$$b' = (-h - b) \bmod a'. \tag{8}$$

2. If $\deg_u a' > g$ then set $a \leftarrow a'$, $b \leftarrow b'$ and go to step 1.

3. Let c be the leading coefficient of a', and set $a' \leftarrow c^{-1}a'$.

4. Output(a',b').

Theorem 51 (*Algorithm 2 works*) Let $D = \mathrm{div}(a, b)$ be a semi-reduced divisor. Then the divisor $D' = \mathrm{div}(a', b')$ returned by Algorithm 2 is reduced and $D' \sim D$.

Proof. Let $a' = (f - bh - b^2)/a$ and $b' = (-h - b) \bmod a'$. We show that

(i) $\deg_u(a') < \deg_u(a)$;

(ii) $D' = \mathrm{div}(a', b')$ is semi-reduced; and

(iii) $D \sim D'$.

The theorem then follows by repeated application of the reduction process (step 1 of Algorithm 2).

(i) Let $m = \deg_u a$, $n = \deg_u b$, where $m > n$, and $m \geq g + 1$. Then $\deg_u a' = \max(2g + 1, 2n) - m$. If $m > g + 1$, then $\max(2g + 1, 2n) \leq 2(m - 1)$, whence $\deg_u a' \leq m - 2 < \deg_u a$. If $m = g + 1$, then $\max(2g + 1, 2n) = 2g + 1$, whence $\deg_u a' = g < \deg_u a$.

(ii) Now, $f - bh - b^2 = aa'$. Reducing both sides modulo a' yields

$$f + (b' + h)h - (b' + h)^2 \equiv 0 \pmod{a'}$$

which simplifies to

$$f - b'h - (b')^2 \equiv 0 \pmod{a'}.$$

Hence $a' | (f - b'h - (b')^2)$. It follows from Lemma 43 that $\mathrm{div}(a', b')$ is semi-reduced.

(iii) Let $C_0 = \{P \in \mathrm{supp}(D) : P \text{ is special}\}$, $C_1 = \{P \in \mathrm{supp}(D) : P \text{ is ordinary}\}$, and $C_2 = \{\tilde{P} : P \in C_1\}$. Then, as in the proof of Theorem 42, we can write

$$D = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - (*)\infty.$$

Now,

$$\mathrm{div}(a) = \sum_{P_i \in C_0} 2P_i + \sum_{P_i \in C_1} m_i P_i + \sum_{P_i \in C_1} m_i \tilde{P}_i - (*)\infty$$

and

$$\mathrm{div}(b - v) = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} n_i P_i + \sum_{P_i \in C_1} 0\tilde{P}_i + \sum_{P_i \in C_3} s_i P_i - (*)\infty,$$

where $n_i \geq m_i$, C_3 is a set of points in $C \backslash (C_0 \cup C_1 \cup C_2 \cup \{\infty\})$, $s_i \geq 1$, and $s_i = 1$ if P_i is special. Since $b^2 + bh - f = N(b - v)$, it follows from Lemma 35 that

$$\mathrm{div}(b^2 + bh - f) = \sum_{P_i \in C_0} 2P_i + \sum_{P_i \in C_1} n_i P_i + \sum_{P_i \in C_1} n_i \tilde{P}_i + \sum_{P_i \in C_3} s_i P_i + \sum_{P_i \in C_3} s_i \tilde{P}_i - (*)\infty,$$

and hence

$$\begin{aligned}\operatorname{div}(a') &= \operatorname{div}(b^2+bh-f)-\operatorname{div}(a)\\ &= \sum_{P_i\in C_1'} t_iP_i + \sum_{P_i\in C_1'} t_i\tilde{P}_i + \sum_{P_i\in C_3} s_iP_i + \sum_{P_i\in C_3} s_i\tilde{P}_i - (*)\infty,\end{aligned}$$

where $t_i = n_i - m_i$ and $C_1' = \{P_i \in C_1 : n_i > m_i\}$. Now, $b' = -h - b + sa'$ for some $s \in \overline{K}[u]$. If $P_i = (x_i, y_i) \in C_1' \cup C_3$, then $b'(x_i) = -h(x_i) - b(x_i) + s(x_i)a'(x_i) = -h(x_i) - y_i$. Then, as in the proof of Theorem 42, it follows that

$$\operatorname{div}(b'-v) = \sum_{P_i\in C_1'} 0P_i + \sum_{P_i\in C_1'} r_i\tilde{P}_i + \sum_{P_i\in C_3} 0P_i + \sum_{P_i\in C_3} w_i\tilde{P}_i + \sum_{P_i\in C_4} z_iP_i - (*)\infty,$$

where $r_i \geq t_i$, $w_i \geq s_i$, $w_i = 1$ if $P_i \in C_3$ is special, and C_4 is a set of points in $C\backslash(C_1' \cup C_3 \cup \{\infty\})$. Hence

$$\begin{aligned}\operatorname{div}(a',b') &= \sum_{P_i\in C_1'} t_i\tilde{P}_i + \sum_{P_i\in C_3} s_i\tilde{P}_i - (*)\infty\\ &\sim -\sum_{P_i\in C_1'} t_iP_i - \sum_{P_i\in C_3} s_iP_i + (*)\infty\\ &= D - \operatorname{div}(b-v),\end{aligned}$$

whence $D \sim D'$. □

Note that all computations in Algorithms 1 and 2 take place in the field K itself (and not in any proper extensions of K). In Algorithm 1, if $\deg_u a_1 \leq g$ and $\deg_u a_2 \leq g$, then $\deg_u a \leq 2g$. In this case, Algorithm 2 requires at most $\lceil g/2 \rceil$ iterations of step 1.

Example 52 (*reducing a semi-reduced divisor*) Consider the hyperelliptic curve $C : v^2 + (u^2+u)v = u^5 + u^3 + 1$ of genus $g = 2$ over the finite field $\mathbb{F}_{2^5}$ (see Example 7). Consider the semi-reduced divisor $D = (0,1) + (1,1) + (\alpha^5, \alpha^{15}) - 3\infty$. Then $D = \operatorname{div}(a,b)$, where

$$a(u) = u(u+1)(u+\alpha^5) = u^3 + \alpha^2u^2 + \alpha^5u$$

and

$$b(u) = \alpha^{17}u^2 + \alpha^{17}u + 1.$$

Algorithm 2 yields

$$\begin{aligned}a'(u) &= u^2 + \alpha^{15}u + \alpha^{26},\\ b'(u) &= \alpha^{23}u + \alpha^{21}.\end{aligned}$$

Hence $D \sim \operatorname{div}(a',b') = (\alpha^{28}, \alpha^7) + (\alpha^{29}, 0) - 2\infty$.

9 Implementation of hyperelliptic curve cryptosystems

The Diffie-Hellman key exchange [10] is a protocol whereby two entities A and B can, by a sequence of transmissions over a public channel, agree upon a secret cryptographic key. The method is as follows. A and B first choose a (multiplicatively written) finite abelian group G and some element $\alpha \in G$. A then selects a random integer a and transmits α^a to B. B in turn selects a random integer b and transmits α^b to A. Both A and B can then determine α^{ab}, which is their shared secret key.

An eavesdropper C monitoring the transmission between A and B would know G, α, α^a, and α^b. The parameters G and α should be chosen so that it is computationally infeasible for C to then determine α^{ab}. Certainly, if C could compute either a or b, then C could determine α^{ab}. The problem of determining a given α and $\beta = \alpha^a$ is called the *discrete logarithm problem* in G. The integer a, which is unique if restricted to the range $[0, \text{order}(\alpha) - 1]$, is called the *discrete logarithm* of β to the base α. It is an open problem to decide whether or not determining α^{ab} is equivalent to computing discrete logarithms in G. Among the other cryptographic protocols whose security relies upon the discrete logarithm problem are the ElGamal public-key encryption and digital signature schemes [12], and the recently adopted U.S. Digital Signature Standard [29].

The best algorithms that are known for solving the discrete logarithm problem in an arbitrary group G are the exponential square root attacks (see McCurley [24]) that have a running time that is roughly proportional to the square root of the largest prime factor of l, where l is the order of α. Consequently, if G and α are chosen so that l has a large prime factor, then these attacks can be avoided.

Let $\mathbb{F}_q$ denote the finite field of order q, and let $q = p^m$ where p is the characteristic of $\mathbb{F}_q$. Diffie and Hellman originally proposed $G = \mathbb{F}_q^*$, the multiplicative group of $\mathbb{F}_q$, as a candidate for implementing the Diffie-Hellman key exchange. There are randomized subexponential-time algorithms known for computing logarithms in $\mathbb{F}_q$. (See Coppersmith, Odlyzko and Schroeppel [9] and Gordon [17] for the case q a prime, Odlyzko [30] for the case where $p = 2$, and Adleman and DeMarrais [1] for the general situation.) These algorithms are an asymptotic improvement over the general algorithms mentioned in the previous paragraph. For cryptographic purposes we are interested in groups for which subexponential algorithms for the corresponding discrete logarithm problem are not known. Additionally, for efficient and practical implementation, the group operation should be relatively easy to apply. The jacobian of a hyperelliptic curve defined over a finite field is one possibility for such a group.

To implement a discrete log cryptosystem using hyperelliptic curves, a suitable curve C and underlying finite field K must be selected. Desirable properties of the selected curve and field include the following:

1. Arithmetic in the underlying finite field K should be efficient to implement; finite fields of characteristic 2 appear to be the most attractive choice.

2. The order of the jacobian $J(K)$ of C, denoted $\#J(K)$, should be divisible by a large prime number. Given the current state of computer technology, a security requirement is that $\#J(K)$ be divisible by a prime number r of at least 45 decimal digits. In addition, to avoid the reduction attack of Frey and Rück [13] which reduces the logarithm problem in $J(K)$ to the logarithm problem in an extension field of $K = \mathbb{F}_q$, r should not divide $q^k - 1$ for all small k for which the discrete logarithm problem in $\mathbb{F}_{q^k}$ is feasible ($1 \leq k \leq 2000/(\log_2 q)$ suffices).

One technique for selecting a hyperelliptic curve and computing $\#J(K)$ is described next. Let J be the jacobian of the hyperelliptic curve C defined over $\mathbb{F}_q$, and given by the equation $v^2 + h(u)v = f(u)$. Let $\mathbb{F}_{q^n}$ denote the degree-n extension of $\mathbb{F}_q$, and let N_n denote the order of the (finite) abelian group $J(\mathbb{F}_{q^n})$. Denote by M_n the number of $\mathbb{F}_{q^n}$-rational points on C. Associated with C is the zeta-function, defined next.

Definition 53 (*zeta function*) Let C be a hyperelliptic curve defined over $\mathbb{F}_q$, and let $M_r = \#C(\mathbb{F}_{q^r})$ for $r \geq 1$. The *zeta-function* of C is the power series

$$Z_C(t) = \exp\left(\sum_{r \geq 1} M_r \frac{t^r}{r}\right).$$

The following are some well-known facts (e.g., see [23]) about the zeta-function.

Theorem 54 (*properties of the zeta-function*) Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$, and let $Z_C(t)$ be the zeta-function of C.

(i) $Z_C(t) \in \mathbb{Z}(t)$. More precisely, we have

$$Z_C(t) = \frac{P(t)}{(1-t)(1-qt)} \tag{9}$$

where $P(t)$ is a polynomial of degree $2g$ with integer coefficients. Moreover, $P(t)$ has the form:

$$\begin{aligned} P(t) = 1 + a_1 t + \cdots + a_{g-1} t^{g-1} + a_g t^g + \\ q a_{g-1} t^{g+1} + q^2 a_{g-2} t^{g+2} + \cdots + q^{g-1} a_1 t^{2g-1} + q^g t^{2g}. \end{aligned} \tag{10}$$

(ii) $P(t)$ factors as

$$P(t) = \prod_{i=1}^{g} (1 - \alpha_i t)(1 - \overline{\alpha}_i t), \tag{11}$$

where each α_i is a complex number of absolute value $\sqrt{q}$, and $\overline{\alpha}_i$ denotes the complex conjugate of α_i.

(iii) $N_n = \#J(\mathbb{F}_{q^n})$ satisfies

$$N_n = \prod_{i=1}^{g} |1 - \alpha_i^n|^2, \tag{12}$$

where $|\ |$ denotes the usual complex absolute value.

In order to compute N_n, it thus suffice to (i) determine the coefficients $a_1, a_2, \ldots, a_g$ of $P(t)$, hence determining $P(t)$; (ii) factor $P(t)$ thus determining the α_i; (iii) compute N_n via equation (12). Now, multiplying both sides of equation (9) by $(1-t)(1-qt)$ yields

$$P(t) = (1-t)(1-qt)Z_C(t).$$

Taking logarithms of both sides and then differentiating with respect to t yields

$$\frac{P'(t)}{P(t)} = \sum_{r \geq 0} (M_{r+1} - 1 - q^{r+1})t^r.$$

By equating coefficients of $t^0, t^1, \ldots, t^{g-1}$ of both sides, we see that the first g values $M_1, M_2, \ldots, M_g$ suffice to determine the coefficients $a_1, a_2, \ldots, a_g$ and, hence, N_n.

The following procedure summarizes the technique for computing N_n in the case $g = 2$.

1. By exhaustive search, compute M_1 and M_2.
2. The coefficients of $Z_C(t)$ are given by $a_1 = M_1 - 1 - q$ and $a_2 = (M_2 - 1 - q^2 + a_1^2)/2$.
3. Solve the quadratic equation $X^2 + a_1 X + (a_2 - 2q) = 0$, to obtain two solutions γ_1 and γ_2.
4. Solve $X^2 - \gamma_1 X + q = 0$ to obtain a solution α_1, and solve $X^2 - \gamma_2 X + q = 0$ to obtain a solution α_2.
5. Then $N_n = |1 - \alpha_1^n|^2 \cdot |1 - \alpha_2^n|^2$.

The following bounds on the order N_n of the jacobian are an immediate corollary of Theorem 54(iii).

Corollary 55 Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$, and let $N_n = \#J(\mathbb{F}_{q^n})$. Then

$$(q^{n/2} - 1)^{2g} \leq N_n \leq (q^{n/2} + 1)^{2g}.$$

Hence, $N_n \approx q^{ng}$.

Example 56 (*selecting a hyperelliptic curve*) Consider the following hyperelliptic curve C of genus 2 defined over $\mathbb{F}_2$:

$$C \ : \ v^2 + v = u^5 + u^3 + u.$$

By exhaustive search, we find $M_1 = 3$ and $M_2 = 9$; hence $a_1 = 0$ and $a_2 = 2$. The solutions of $X^2 - 2 = 0$ are $\gamma_1 = \sqrt{2}$ and $\gamma_2 = -\sqrt{2}$. Solving $X^2 - \sqrt{2}X + 2 = 0$ yields $\alpha_1 = (\sqrt{2} + \sqrt{6}i)/2$; solving $X^2 + \sqrt{2}X + 2 = 0$ yields $\alpha_2 = (-\sqrt{2} + \sqrt{6}i)/2$. Hence

$$N_n = |1 - \alpha_1^n|^2 \cdot |1 - \alpha_2^n|^2 = \begin{cases} 2^{2n} + 2^n + 1, & \text{if } n \equiv 1, 5 \pmod 6, \\ (2^n + 2^{n/2} + 1)^2, & \text{if } n \equiv 2, 4 \pmod 6, \\ (2^n - 1)^2, & \text{if } n \equiv 3 \pmod 6, \\ (2^{n/2} - 1)^4, & \text{if } n \equiv 0 \pmod 6. \end{cases}$$

For $n = 101$,

$$N_{101} = 6427752177035961102167848369367185711289268433934164747616257,$$

and its prime factorization is

$$N_{101} = 7 \cdot 607 \cdot 151276822241373525586440300526410583932437477852063185399 3.$$

Hence N_{101} is divisible by a 58-decimal digit prime r. However, since r divides $(2^{101})^3 - 1$, the Frey-Rück attack tells us that C offers no more security that a discrete log system in $\mathbb{F}_{2^{303}}$. Hence the curve C is not suitable for cryptographic applications.

10 Future work

There are several areas of research that need to be pursued before hyperelliptic curve cryptosystems may be adopted in practical applications.

1. The most important issue is with regards to the security of hyperelliptic curve cryptosystems. More precisely, the security relies upon the *hyperelliptic curve discrete logarithm problem* (HCDLP) which is the following: given a hyperelliptic curve C over a finite field K, and given reduced divisors $D_1, D_2 \in J(K)$, determine a positive integer l such that $D_2 = lD_1$, provided that such an integer exists.

   If the order of the divisor D_1 is divisible by a large prime factor r, then the best algorithm known for the HCDLP is an exponential one and takes $O(\sqrt{r})$ steps. However, for special hyperelliptic curves, it may be possible to reduce the HCDLP to the DLP in a small extension finite field. Since there are subexponential-time algorithms known for the DLP, this will yield a subexponential-time algorithm for the HCDLP; hyperelliptic curves for which such reductions exist offer no significant advantages over finite fields for the implementation of discrete log cryptosystems.

Such a reduction was accomplished for the genus 1 hyperelliptic curves (or elliptic curves) by Menezes, Okamoto and Vanstone [26]. Frey and Rück [13] extended this reduction to more general classes of abelian varieties. The reduction is efficient for some classes of hyperelliptic curves; the implications of the Frey-Rück reduction to hyperelliptic curve cryptography need to be fully explored.

Adleman, DeMarrais and Huang [2] recently discovered an algorithm for HCDLP which takes subexponential time if the genus g of the curve is large. More precisely, if the curve is defined over $\mathbb{Z}_p$, then the genus g should satisfy $\log p \leq (2g+1)^{0.98}$. Interestingly, the algorithm is worse than exhaustive search if specialized to the $g = 1$ case. It would be interesting to implement this algorithm, and to better understand why it is inefficient when the genus is small.

2. It could be useful to classify the isomorphism classes of hyperelliptic curves over finite fields, in order to know how many essentially different choices of curves there are.

3. Further research needs to be done on the efficient implementation of the addition rule in the jacobian. A more efficient algorithm may arise by considering a different form of the defining equation or by restricting the genus to certain values (e.g., when $g = 1$, the equation has a simple form). Cantor [5] described a reduction algorithm that is asymptotically faster than Algorithm 2. Petersen [31] presented an algorithm for addition in the jacobian when $g = 2$ which is comparable to that of Cantor's.

4. Another method for selecting a suitable hyperelliptic curve is to select at random a defining equation over a *large* finite field K, and compute $\#J(K)$ directly. Pila [32] presented a generalization of Schoof's algorithm for computing the characteristic polynomial $P(t)$ of the Frobenius endomorphism of an abelian variety defined over a finite field in deterministic polynomial time. In the case that the variety is the jacobian of an algebraic curve C defined over F_q, the number of F_q–rational points on C is then easily recovered. Pila's algorithm, as it applies to hyperelliptic curves, should be studied further and implemented.

Acknowledgements

The authors would like to thank Doug Leonard for his helpful comments that led to the simplification of several proofs.

References

[1] L. Adleman and J. DeMarrais, "A subexponential algorithm for discrete logarithms over all finite fields", *Mathematics of Computation*, **61** (1993), 1-15.

[2] L. Adleman, J. DeMarrais and M. Huang, "A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields", Algorithmic Number Theory, Lecture Notes in Computer Science, **877** (1994), 28-40.

[3] L. Adleman and M. Huang, *Primality Testing and Abelian Varieties over Finite Fields*, Lecture Notes in Mathematics, **1512**, Springer-Verlag, Berlin, 1992.

[4] D. Le Brigand, "Decoding of codes on hyperelliptic curves", *Eurocode '90*, Lecture Notes in Computer Science, **514** (1991), Springer-Verlag, 126-134.

[5] D. Cantor, "Computing in the jacobian of a hyperelliptic curve", *Mathematics of Computation*, **48** (1987), 95-101.

[6] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge University Press, 1996.

[7] L. Charlap and D. Robbins, *An Elementary Introduction to Elliptic Curves*, CRD Expository Report No. 31, Institute for Defense Analysis, Princeton, December 1988.

[8] L. Charlap and D. Robbins, *An Elementary Introduction to Elliptic Curves II*, CRD Expository Report No. 34, Institute for Defense Analysis, Princeton, December 1988.

[9] D. Coppersmith, A. Odlyzko and R. Schroeppel, "Discrete logarithms in $GF(p)$", *Algorithmica*, **1** (1986), 1-15.

[10] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, **22** (1976), 644-654.

[11] Y. Driencourt and J. Michon, "Elliptic codes over a field of characteristic 2", *Journal of Pure and Applied Algebra*, **45** (1987), 15-39.

[12] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, **31** (1985), 469-472.

[13] G. Frey and H. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", *Mathematics of Computation*, **62** (1994), 865-874.

[14] W. Fulton, *Algebraic Curves*, Benjamin, New York, 1969.

[15] G. van der Geer, "Codes and elliptic curves", in *Effective Methods in Algebraic Geometry*, Birkhäuser, 1991, 159-168.

[16] S. Goldwasser and J. Kilian, "Almost all primes can be quickly certified", *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, 316-329, 1986.

[17] D.M. Gordon, "Discrete logarithms in $GF(p)$ using the number field sieve", *Siam Journal on Discrete Mathematics*, **6** (1993), 124-138.

[18] B. Kaliski, "A pseudorandom bit generator based on elliptic logarithms", *Advances in Cryptology – CRYPTO '86*, Lecture Notes in Computer Science, **293** (1987), Springer-Verlag, 84-103.

[19] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, **48** (1987), 203-209.

[20] N. Koblitz, "Hyperelliptic cryptosystems", *Journal of Cryptology*, **1** (1989), 139-150.

[21] H.W. Lenstra, "Factoring integers with elliptic curves", *Annals of Mathematics*, **126** (1987), 649-673.

[22] H.W. Lenstra, J. Pila and C. Pomerance, "A hyperelliptic smoothness test. I", *Philosophical Transactions of the Royal Society of London A*, **345** (1993), 397-408.

[23] J. van Lint and G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, Birkhäuser-Verlag, Basel, Germany, 1988.

[24] K. McCurley, "The discrete logarithm problem", *Cryptology and Computational Number Theory*, Proceedings of Symposia in Applied Mathematics, **42** (1990), 49-74.

[25] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, Boston, 1993.

[26] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *IEEE Transactions on Information Theory*, **39** (1993), 1639-1646.

[27] V. Miller, "Uses of elliptic curves in cryptography", *Advances in Cryptology – Proceedings of Crypto '85*, Lecture Notes in Computer Science, **218** (1986), Springer-Verlag, 417-426.

[28] D. Mumford, *Tata Lectures on Theta II*, Birkhäuser, Boston, 1984.

[29] National Institute for Standards and Technology, "Digital signature standard", FIPS Publication 186, 1993.

[30] A. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance", *Advances in Cryptology – Proceedings of Eurocrypt '84*, Lecture Notes in Computer Science, **209** (1985), Springer-Verlag, 224-314.

[31] M. Petersen, "Hyperelliptic cryptosystems", Technical report, University of Aarhus, Denmark, 1994.

[32] J. Pila, "Frobenius maps of abelian varieties and finding roots of unity in finite fields", *Mathematics of Computation*, **55** (1990), 745-763.

[33] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p", *Mathematics of Computation*, **44** (1985), 483-494.

[34] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1985.

[35] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.