Appendix. An Elementary Introduction to Hyperelliptic Curves

by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato

This appendix is 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 is presented, along with a proof of its correctness.

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 are many books on the topic (for example, [Silverman 1986 and 1994], [Husemöller 1987], [Koblitz 1993], [Menezes 1993]).

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 1984]. However, the non-specialist will have 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 [Cassels and Flynn 1996] is an extensive account of curves of genus 2. (Compared to their book, our approach is definitely "low-brow".)

Recently, applications of hyperelliptic curves have been found in areas outside algebraic geometry. Hyperelliptic curves were a key ingredient in Adleman and Huang's random polynomial-time algorithm for primality proving [Adleman and Huang 1992]. Hyperelliptic curves have also been considered in the design of error-correcting codes [Brigand 1991], in the evaluation of definite integrals [Bertrand 1995], in integer factorization algorithms [Lenstra, Pila and Pomerance 1993], and in public-key cryptography (see Chapter 6 of the present book). Hyperelliptic

Authors' addresses: Alfred J. Menezes, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N1L 3G1, e-mail: ajmeneze@math.uwaterloo.ca; Yi-Hong Wu, Department of Discrete and Statistical Sciences, Auburn University, Auburn, AL 36849, USA; Robert J. Zuccherato, Entrust Technologies, 750 Heron Road, Ottawa, Ontario, Canada K1V 1A7, e-mail: robert.zuccherato@entrust.com.

curves over finite fields of characteristic two are particularly of interest when implementing codes and cryptosystems.

Charlap and Robbins [1988] 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 [Schoof 1985] 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 appendix, similar in spirit to the paper of Charlap and Robbins, presents an elementary introduction to some of the theory of hyperelliptic curves over finite fields of arbitrary characteristic. For a general introduction to the theory of algebraic curves, consult [Fulton 1969].

§ 1. Basic Definitions and Properties

Definition 1.1. Let $\mathbb{F}$ be a field and let $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$ (see Definition 1.8 of Chapter 3). A *hyperelliptic curve C of genus g over* $\mathbb{F}$ ($g \geq 1$) is an equation of the form

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

where $h(u) \in \mathbb{F}[u]$ is a polynomial of degree at most g, $f(u) \in \mathbb{F}[u]$ is a monic polynomial of degree $2g+1$, and there are no solutions $(u,v) \in \overline{\mathbb{F}} \times \overline{\mathbb{F}}$ 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 $(u,v) \in \overline{\mathbb{F}} \times \overline{\mathbb{F}}$ 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 1.1 thus says that a hyperelliptic curve does not have any singular points.

For the remainder of this paper it is assumed that the field $\mathbb{F}$ and the curve C have been fixed.

Lemma 1.1. *Let C be a hyperelliptic curve over $\mathbb{F}$ defined by equation* (1).

1) *If $h(u) = 0$, then* $\mathrm{char}(\mathbb{F}) \neq 2$.
2) *If* $\mathrm{char}(\mathbb{F}) \neq 2$, *then the change of variables $u \to u$, $v \to (v - h(u)/2)$ transforms C to the form $v^2 = f(u)$ where* $\deg_u f = 2g+1$.
3) *Let C be an equation of the form* (1) *with $h(u) = 0$ and* $\mathrm{char}(\mathbb{F}) \neq 2$. *Then C is a hyperelliptic curve if and only if $f(u)$ has no repeated roots in $\overline{\mathbb{F}}$.*

Proof.

1) Suppose that $h(u) = 0$ and $\mathrm{char}(\mathbb{F}) = 2$. Then the partial derivative equations reduce to $f'(u) = 0$. Note that $\deg_u f'(u) = 2g$. Let $x \in \overline{\mathbb{F}}$ be a root of the equation $f'(u) = 0$, and let $y \in \overline{\mathbb{F}}$ be a root of the equation $v^2 = f(x)$. Then the point (x,y) is a singular point on C. Statement 1) now follows.

2) 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 $\deg_u(f + h^2/4) = 2g + 1$.

3) 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 1.2. Let $\mathbb{K}$ be an extension field of $\mathbb{F}$. The *set of* $\mathbb{K}$*-rational points on* C, denoted $C(\mathbb{K})$, is the set of all points $P = (x, y) \in \mathbb{K} \times \mathbb{K}$ that satisfy the equation (1) of the curve C, together with a special *point at infinity** denoted ∞. The set of points $C(\overline{\mathbb{F}})$ will simply be denoted by C. The points in C other than ∞ are called *finite points.*

Example 1.1. The illustrations on the next page show two examples of hyperelliptic curves over the field of real numbers. Each curve has genus $g = 2$ and $h(u) = 0$.

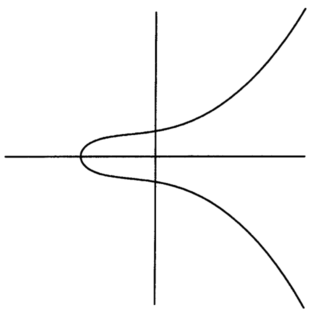
Definition 1.3. Let $P = (x, y)$ be a finite point on a hyperelliptic curve C. The *opposite* of P is the point $\widetilde{P} = (x, -y - h(x))$. (Note that $\widetilde{P}$ is indeed on C.) We also define the opposite of ∞ to be $\widetilde{\infty} = \infty$ itself. If a finite point P satisfies $P = \widetilde{P}$, then the point is said to be *special*; otherwise, the point is said to be *ordinary*.

Example 1.2. Consider the curve $C : v^2 + uv = u^5 + 5u^4 + 6u^2 + u + 3$ over the finite field $\mathbb{F}_7$. 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 $\mathbb{F}_7$-rational points on C are

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

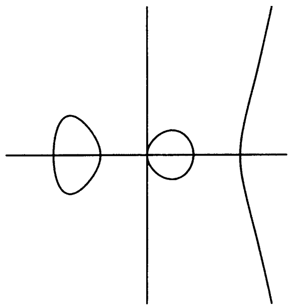
The point $(6, 4)$ is a special point.

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 below.



* The point at infinity lies in the projective plane $\mathbf{P}^2(\overline{\mathbb{F}})$. 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; this is allowed, since $\infty \notin \overline{\mathbb{F}} \times \overline{\mathbb{F}}$.

2) $C_2 : v^2 = u^5 - 5u^3 + 4u = u(u-1)(u+1)(u-2)(u+2)$. The graph of C_2 in the real plane is shown below.



Example 1.3. 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:

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

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

§ 2. Polynomial and Rational Functions

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

Definition 2.1. The *coordinate ring of* C *over* $\mathbb{F}$, denoted $\mathbb{F}[C]$, is the quotient ring

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

where $(v^2 + h(u)v - f(u))$ denotes the ideal in $\mathbb{F}[u, v]$ generated by the polynomial $v^2 + h(u)v - f(u)$.(See Example 4.1 in Chapter 3 for the definition of "quotient ring".) Similarly, the *coordinate ring of* C *over* $\overline{\mathbb{F}}$ is defined as

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

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

Lemma 2.1. *The polynomial* $r(u, v) = v^2 + h(u)v - f(u)$ *is irreducible over* $\overline{\mathbb{F}}$, *and hence* $\overline{\mathbb{F}}[C]$ *is an integral domain.*

Proof. If $r(u, v)$ were reducible over $\overline{\mathbb{F}}$, it would factor as $(v - a(u))(v - b(u))$ for some $a, b \in \overline{\mathbb{F}}[u]$. 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 $G(u, v) \in \overline{\mathbb{F}}[C]$, we can repeatedly replace any occurrence of v^2 by $f(u) - h(u)v$, so as to eventually obtain a representation

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

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

Definition 2.2. Let $G(u, v) = a(u) - b(u)v$ be a polynomial function in $\overline{\mathbb{F}}[C]$. 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 2.3 Let $G(u, v) = a(u) - b(u)v$ be a polynomial function in $\overline{\mathbb{F}}[C]$. The *norm* of G is the polynomial function $N(G) = G\overline{G}$.

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

Lemma 2.2. *Let* $G, H \in \overline{\mathbb{F}}[C]$ *be polynomial functions.*
1) $N(G)$ *is a polynomial in* $\overline{\mathbb{F}}[u]$.
2) $N(\overline{G}) = N(G)$.
3) $N(GH) = N(G)N(H)$.

Proof. Let $G = a - bv$ and $H = c - dv$, where $a, b, c, d \in \overline{\mathbb{F}}[u]$.*
1) Now, $\overline{G} = a + b(h + v)$ and

$$N(G) = G \cdot \overline{G} = (a - bv)(a + b(h + v)) = a^2 + abh - b^2 f \in \overline{\mathbb{F}}[u] \ .$$

2) The conjugate of $\overline{G}$ is

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

Hence $N(\overline{G}) = \overline{G}\,\overline{\overline{G}} = \overline{G}G = N(G)$.
3) $GH = (ac + bdf) - (bc + ad + bdh)v$, 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 2.4. The *function field* $\mathbb{F}(C)$ *of* C *over* $\mathbb{F}$ is the field of fractions of $\mathbb{F}[C]$. Similarly, the *function field* $\overline{\mathbb{F}}(C)$ *of* C *over* $\overline{\mathbb{F}}$ is the field of fractions of $\overline{\mathbb{F}}[C]$. The elements of $\overline{\mathbb{F}}(C)$ are called *rational functions* on C.

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

Definition 2.5. Let $R \in \overline{\mathbb{F}}(C)$, and let $P \in C$, $P \neq \infty$. Then R is said to be *defined at* P if there exist polynomial functions $G, H \in \overline{\mathbb{F}}[C]$ such that $R = G/H$ and $H(P) \neq 0$; if no such $G, H \in \overline{\mathbb{F}}[C]$ 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.

Definition 2.6. Let $G(u, v) = a(u) - b(u)v$ be a nonzero polynomial function in $\overline{\mathbb{F}}[C]$. The *degree* of G is defined to be

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

Lemma 2.3. *Let* $G, H \in \overline{\mathbb{F}}[C]$.
1) $\deg(G) = \deg_u(N(G))$.

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

2) $\deg(GH) = \deg(G) + \deg(H)$.
3) $\deg(G) = \deg(\overline{G})$.

Proof.
1) 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 the definition of a hyperelliptic curve, $\deg_u(h(u)) \le g$ and $\deg_u(f(u)) = 2g + 1$. There are two cases to consider:

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

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

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

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

It follows that

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

2) We have

$$\begin{aligned} \deg(GH) &= \deg_u(N(GH)) , \quad \text{by 1)} \\ &= \deg_u(N(G)N(H)) , \quad \text{by part 3) of Lemma 2.2} \\ &= \deg_u(N(G)) + \deg_u(N(H)) \\ &= \deg(G) + \deg(H) . \end{aligned}$$

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

Definition 2.7. Let $R = G/H \in \overline{\mathbb{F}}(C)$ be a rational function.
1) If $\deg(G) < \deg(H)$ then the value of R at ∞ is defined to be $R(\infty) = 0$.
2) If $\deg(G) > \deg(H)$ then R is *not defined* at ∞.
3) 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.

§ 3. Zeros and Poles

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

Definition 3.1. Let $R \in \overline{\mathbb{F}}(C)$ be a nonzero rational function, 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 3.1. *Let $G \in \overline{\mathbb{F}}[C]$ be a nonzero polynomial function, and let $P \in C$. If $G(P) = 0$, then $\overline{G}(\widetilde{P}) = 0$.*

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

The next three lemmas are used in the proof of Theorem 3.1, which establishes the existence of uniformizing parameters.

Lemma 3.2. *Let $P = (x, y)$ be a point on C. Suppose that a nonzero polynomial function $G = a(u) - b(u)v \in \overline{\mathbb{F}}[C]$ has a zero at P, and suppose 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 3.1. Conversely, suppose that P is an ordinary point, i.e., $y \neq (-y - h(x))$. If $\overline{G}(P) = 0$ then we have:

$$a(x) - b(x)y = 0$$
$$a(x) + b(x)(h(x) + y) = 0 \ .$$

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

Lemma 3.3. *Let $P = (x, y)$ be an ordinary point on C, and let $G = a(u) - b(u)v \in \overline{\mathbb{F}}[C]$ be a nonzero polynomial function. 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 $(u - x)$ that divides $N(G)$, and $S \in \overline{\mathbb{F}}(C)$ 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 $(u - x)$ that divides $N(G)$ (so $d(u) \in \overline{\mathbb{F}}[u]$ and $d(x) \neq 0$). By Lemma 3.2, $\overline{G}(P) \neq 0$. Let $S = d(u)/\overline{G}$. Then $G = (u - x)^s S$ and $S(P) \neq 0, \infty$. □

Lemma 3.4. *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 $S(u, v) \in \overline{\mathbb{F}}(C)$ has neither a zero nor a pole at P.*

Proof. Let $H = (v - y)^2$ and $S = (u - x)/H$, so 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

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

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 nonzero at P, and hence that $S(P) \neq 0, \infty$, as required. □

Theorem 3.1. *Let $P \in C$. Then there exists a function $U \in \overline{\mathbb{F}}(C)$ with $U(P) = 0$ such that the following property holds: for each nonzero polynomial function $G \in \overline{\mathbb{F}}[C]$, there exist an integer d and a function $S \in \overline{\mathbb{F}}(C)$ 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 $G(u, v) \in \overline{\mathbb{F}}[C]$ be a nonzero polynomial function. 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 $\overline{\mathbb{F}}[C]$ satisfying $U(P) = 0$.) We prove the theorem by finding a uniformizing parameter for each of the following cases: 1) $P = \infty$; 2) P is an ordinary point; and 3) P is a special point.

1) We 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 $S(\infty) \neq 0, \infty$.

2) 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 3.3, we can write $(a_0(u) - b_0(u)v) = (u - x)^s S$ for some integer $s \geq 0$ and some $S \in \overline{\mathbb{F}}(C)$ such that $S(P) \neq 0, \infty$. Hence $G = (u - x)^{r+s} S$ satisfies the conclusion of the theorem with $d = r + s$.

3) 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 $b_i(v) \in \overline{\mathbb{F}}[v]$. Replacing all occurrences of u by $((u - x) + x)$ and expanding, we obtain

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

where each $\bar{b}_i(v) \in \overline{\mathbb{F}}[v]$, and $B(u,v) \in \overline{\mathbb{F}}[C]$. Now $G(P) = 0$ implies $\bar{b}_0(y) = 0$, and so we can write $\bar{b}_0(v) = (v-y)c(v)$ for some $c \in \overline{\mathbb{F}}[v]$. By the proof of Lemma 3.4 (see equation (2)), we can write $(u-x) = (v-y)^2/A(u,v)$, where $A(u,v) \in \overline{\mathbb{F}}[C]$ and $A(P) \neq 0, \infty$. Hence

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

Now if $G_1(P) \neq 0$, then we are done, since we can take $S = G_1/A$. 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 $c_1 \in \overline{\mathbb{F}}[v]$. 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 out 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 $D \in \overline{\mathbb{F}}[C]$. 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, we have $N(G) = (u-x)^{2l}N(D)$. 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 $D \in \overline{\mathbb{F}}[C]$. 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, we have $N(AG) = (u-x)^{2l}N(v-y)N(D)$. 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 $a \geq 1$, $b \geq 1$, $A, B \in \overline{\mathbb{F}}(C)$, $A(P) \neq 0, \infty$, $B(P) \neq 0, \infty$. Thus $U = (U^b B)^a A = U^{ab} B^a A$. Dividing both sides by U, we obtain $U^{ab-1} B^a A = 1$. If we substitute P in both sides of this equation, we see that $ab - 1 = 0$. 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 [Koblitz 1989], which is more convenient to use for computational purposes, is given in Definition 3.3. Lemma 3.6 establishes that these two definitions are in fact equivalent.

Definition 3.2. Let $G \in \overline{\mathbb{F}}[C]$ be a nonzero polynomial function, and let $P \in C$. Let $U \in \overline{\mathbb{F}}(C)$ be a uniformizing parameter for P, and write $G = U^d S$ where $S \in \overline{\mathbb{F}}(C)$, $S(P) \neq 0, \infty$. The *order of G at P* is defined to be $\mathrm{ord}_P(G) = d$.

Lemma 3.5. *Let $G_1, G_2 \in \overline{\mathbb{F}}[C]$ be nonzero polynomial functions, and let $P \in C$. Let* $\mathrm{ord}_P(G_1) = r_1$, $\mathrm{ord}_P(G_2) = r_2$.

1) $\mathrm{ord}_P(G_1 G_2) = \mathrm{ord}_P(G_1) + \mathrm{ord}_P(G_2)$.
2) *If $r_1 \neq r_2$, then* $\mathrm{ord}_P(G_1 + G_2) = \min(r_1, r_2)$. *If $r_1 = r_2$ and $G_1 \neq -G_2$, then* $\mathrm{ord}_P(G_1 + G_2) \geq r_2$.

Proof. Let U be a uniformizing parameter for P. By Definition 3.2, we can write $G_1 = U^{r_1} S_1$ and $G_2 = U^{r_2} S_2$, where $S_1, S_2 \in \overline{\mathbb{F}}(C)$, $S_1(P) \neq 0, \infty$, $S_2(P) \neq 0, \infty$. Without loss of generality, suppose that $r_1 \geq r_2$.

1) $G_1 G_2 = U^{r_1 + r_2}(S_1 S_2)$, from which it follows that $\mathrm{ord}_P(G_1 G_2) = r_1 + r_2$.
2) $G_1 + G_2 = U^{r_2}(U^{r_1 - r_2} S_1 + S_2)$. 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 $\mathrm{ord}_P(G_1 + G_2) \geq r_2$. □

We now give an alternate definition of the order of a polynomial function at a point.

Definition 3.3. Let $G = a(u) - b(u)v \in \overline{\mathbb{F}}[C]$ be a nonzero polynomial function, and let $P \in C$. The *order of G at P*, denoted $\mathrm{ord}_P(G)$, is defined as follows:

1) If $P = (x, y)$ is a finite point, then let r be the highest power of $(u - x)$ that 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 $(u - x)$ that divides $N(a_0(u) - b_0(u)v) = a_0^2 + a_0 b_0 h - b_0^2 f$. If P is an ordinary point, then define $\mathrm{ord}_P(G) = r + s$. If P is a special point, then define $\mathrm{ord}_P(G) = 2r + s$.
2) If $P = \infty$, then

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

Lemma 3.6. *Definitions 3.2 and 3.3 are equivalent. That is, if the order function of Definition 3.3 is denoted by* $\overline{\mathrm{ord}}$, *then* $\mathrm{ord}_P(G) = \overline{\mathrm{ord}}_P(G)$ *for all $P \in C$ and all nonzero $G \in \overline{\mathbb{F}}[C]$.*

Proof. If $P = \infty$, the lemma follows directly from the proof of part 1) of Theorem 3.1. For the case when P is an ordinary point, the lemma follows directly from Lemma 3.3 and the proof of part 2) of Theorem 3.1.

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

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

Let $\text{ord}_P(H) = s$. Then, by Lemma 3.4,

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

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

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

Multiplying both sides by A_2 and taking norms, we have

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

Now $N(A_1)(x) \neq 0$, since $A_1(P) \neq 0$ and P is special (Lemma 3.1). 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 $(u - x)$ that divides $N(H)$. Hence, $\overline{\text{ord}}_P(G) = 2r + s = \text{ord}_P(G)$. □

Lemma 3.7 is a generalization of Lemma 3.1.

Lemma 3.7. *Let $G \in \overline{\mathbb{F}}[C]$ be a nonzero polynomial function, and let $P \in C$. Then* $\text{ord}_P(G) = \text{ord}_{\widetilde{P}}(\overline{G})$.

Proof. There are two cases to consider.

1) Suppose $P = \infty$; then $\widetilde{P} = \infty$. By Definition 2.6 and part 2) of Definition 3.3, $\text{ord}_P(G) = -\deg(G)$ and $\text{ord}_{\widetilde{P}}(\overline{G}) = \text{ord}_P(\overline{G}) = -\deg(\overline{G})$. By part 3) of Lemma 2.3, $\deg(G) = \deg(\overline{G})$. Hence, $\text{ord}_P(G) = \text{ord}_{\widetilde{P}}(\overline{G})$.
2) 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 $(u - x)$ that 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 $(u - x)$ that 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 $(u - x)$ that divides $N(H) = N(\overline{H})$, it follows from Definition 3.3 that $\text{ord}_{\widetilde{P}}(\overline{G}) = \text{ord}_P(G)$. □

Theorem 3.2. *Let $G \in \overline{\mathbb{F}}[C]$ be a nonzero polynomial function. Then G has a finite number of zeros and poles. Moreover,* $\sum_{P \in C} \text{ord}_P(G) = 0$.

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 $x_i \in \overline{\mathbb{F}}$, and the x_i are not necessarily distinct. The only pole of G is at $P = \infty$, and $\text{ord}_\infty(G) = -n$. If x_i is the u-coordinate of an ordinary point $P = (x_i, y_i)$ on C, then $\text{ord}_P(u - x_i) = 1$ and $\text{ord}_{\widetilde{P}}(u - x_i) = 1$, 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 $\text{ord}_P(u - x_i) = 2$, 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 $\sum_{P \in C \setminus \{\infty\}} \text{ord}_P(N(G)) = 2n$. But, by Lemma 3.7, $\sum_{P \in C \setminus \{\infty\}} \text{ord}_P(G) = \sum_{P \in C \setminus \{\infty\}} \text{ord}_P(\overline{G})$, and hence $\sum_{P \in C \setminus \{\infty\}} \text{ord}_P(G) = n$. We conclude that $\sum_{P \in C} \text{ord}_P(G) = 0$. □

Definition 3.4. Let $R = G/H \in \overline{\mathbb{F}}(C)$ be a nonzero rational function, and let $P \in C$. The *order of R at P* is defined to be $\text{ord}_P(R) = \text{ord}_P(G) - \text{ord}_P(H)$.

It can readily be verified that $\text{ord}_P(R)$ does not depend on the choice of G and H, and that Lemma 3.5 and Theorem 3.2 are also true for nonzero rational functions.

§ 4. Divisors

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

Definition 4.1. A *divisor* D is a formal sum of points on C

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

where only a finite number of the integers m_P are nonzero. 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 $\text{ord}_P(D) = m_P$.

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

Definition 4.2. 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

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

(Note that $\text{g.c.d.}(D_1, D_2) \in \mathbb{D}^0$.)

Definition 4.3. Let $R \in \overline{\mathbb{F}}(C)$ be a nonzero rational function. The *divisor of R* is

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

Note that if $R = G/H$ then $\mathrm{div}(R) = \mathrm{div}(G) - \mathrm{div}(H)$. Theorem 3.2 shows that the divisor of a rational function is indeed a finite formal sum and has degree 0.

Example 4.1. If $P = (x, y)$ is an ordinary point on C, then $\mathrm{div}(u-x) = P+\widetilde{P}-2\infty$. If $P = (x, y)$ is a special point on C, then $\mathrm{div}(u - x) = 2P - 2\infty$.

Lemma 4.1. *Let* $G \in \overline{\mathbb{F}}[C]$ *be a nonzero polynomial function, and let* $\mathrm{div}(G) = \sum_{P\in C} m_P P$. *Then* $\mathrm{div}(\overline{G}) = \sum_{P\in C} m_P \widetilde{P}$.

Proof. The result follows directly from Lemma 3.7. □

If $R_1, R_2 \in \overline{\mathbb{F}}(C)$ are nonzero rational functions, then it follows from part 1) of Lemma 3.5 that $\mathrm{div}(R_1R_2) = \mathrm{div}(R_1) + \mathrm{div}(R_2)$.

Definition 4.4. A divisor $D \in \mathbb{D}^0$ is called a *principal divisor* if $D = \mathrm{div}(R)$ for some nonzero rational function $R \in \overline{\mathbb{F}}(C)$. The set of all principal divisors, denoted $\mathbb{P}$, is a subgroup of $\mathbb{D}^0$. The quotient group $\mathbb{J} = \mathbb{D}^0/\mathbb{P}$ is called the *jacobian* of the curve C. If D_1, $D_2 \in \mathbb{D}^0$ then we write $D_1 \sim D_2$ if $D_1 - D_2 \in \mathbb{P}$; D_1 and D_2 are said to be *equivalent* divisors.

Definition 4.5. 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 4.6. 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 $P_i \in \mathrm{supp}(D)$ one has $\widetilde{P}_i \notin \mathrm{supp}(D)$, unless $P_i = \widetilde{P}_i$, in which case $m_i = 1$.

Lemma 4.2. *For each divisor* $D \in \mathbb{D}^0$ *there exists a semi-reduced divisor* $D_1 \in \mathbb{D}^0$ *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 1) $P \in C_1$ if and only if $\widetilde{P} \in C_2$; and 2) 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

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

Then $D_1 \sim D$. Finally, by Example 4.1, we have

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

for some integer $m_1 \geq 0$, and hence D_1 is a semi-reduced divisor. □

§ 5. 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 §7).

Lemma 5.1. *Let $P = (x, y)$ be an ordinary point on C, and let $R \in \overline{\mathbb{F}}(C)$ be a rational function that does not have a pole at P. Then for any $k \geq 0$, there are unique elements $c_0, c_1, \ldots, c_k \in \overline{\mathbb{F}}$ and $R_k \in \overline{\mathbb{F}}(C)$ such that $R = \sum_{i=0}^{k} c_i(u-x)^i + (u-x)^{k+1}R_k$, where R_k does not have a pole at P.*

Proof. There is a unique $c_0 \in \overline{\mathbb{F}}$, 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) $R_1 \in \overline{\mathbb{F}}(C)$ with $\text{ord}_P(R_1) \geq 0$. Hence $R = c_0+(u-x)R_1$. The lemma now follows by induction. □

In the next lemma, when we write "mod $(u-x)^k$", we mean modulo the ideal generated by $(u-x)^k$ in the subring of $\overline{\mathbb{F}}(C)$ consisting of rational functions that do not have a pole at P. Thus, the conclusion in Lemma 5.1 can be restated: $R \equiv \sum_{i=0}^{k} c_i(u-x)^k \pmod{(u-x)^{k+1}}$.

Lemma 5.2. *Let $P = (x, y)$ be an ordinary point on C. Then for each $k \geq 1$, there exists a unique polynomial $b_k(u) \in \overline{\mathbb{F}}[u]$ such that*
1) $\deg_u b_k < k$;
2) $b_k(x) = y$; *and*
3) $b_k^2(u) + b_k(u)h(u) \equiv f(u) \pmod{(u-x)^k}$.

Proof. We apply Lemma 5.1 to $R(u, v) = v$. Let $v = \sum_{i=0}^{k-1} c_i(u-x)^i + (u-x)^k R_{k-1}$, where $c_i \in \overline{\mathbb{F}}$ and $R_{k-1} \in \overline{\mathbb{F}}(C)$. Define $b_k(u) = \sum_{i=0}^{k-1} c_i(u-x)^i$. From the proof of Lemma 5.1, we know that $c_0 = y$, and hence $b_k(x) = y$. Finally, since $v^2 + h(u)v = f(u)$, if we reduce both sides modulo $(u-x)^k$ we obtain $b_k(u)^2 + b_k(u)h(u) \equiv f(u) \pmod{(u-x)^k}$. Uniqueness is easily proved by induction on k. □

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

Theorem 5.1. *Let $D = \sum m_i P_i - (\sum m_i)\infty$ be a semi-reduced divisor, where $P_i = (x_i, y_i)$. Let $a(u) = \prod(u-x_i)^{m_i}$. There exists a unique polynomial $b(u)$ satisfying:* 1) $\deg_u b < \deg_u a$; 2) $b(x_i) = y_i$ *for all i for which $m_i \neq 0$; and* 3) *$a(u)$ divides $(b(u)^2 + b(u)h(u) - f(u))$. Then $D = \text{g.c.d.}(\text{div}(a(u)), \text{div}(b(u) - v))$.*

Notation: $\text{g.c.d.}(\text{div}(a(u)), \text{div}(b(u) - v))$ will usually be abbreviated to $\text{div}(a(u), b(u) - v)$ or, more simply, to $\text{div}(a, b)$.

Proof. Let C_1 be the set of ordinary points in $\text{supp}(D)$, and let C_0 be the set of special points in $\text{supp}(D)$. Let $C_2 = \{\widetilde{P} : P \in C_1\}$. 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 are positive integers.

We first prove that there exists a unique polynomial $b(u)$ which satisfies the conditions of the theorem. By Lemma 5.2, for each $P_i \in C_1$ there exists a unique polynomial $b_i(u) \in \overline{\mathbb{F}}[u]$ satisfying 1) $\deg_u b_i < m_i$; 2) $b_i(x_i) = y_i$; and 3) $(u - x_i)^{m_i} | b_i^2(u) + b_i(u)h(u) - f(u)$. It can easily be verified that for each $P_i \in C_0$, $b_i(u) = y_i$ is the unique polynomial satisfying 1) $\deg_u b_i < 1$; 2) $b_i(x_i) = y_i$; and 3) $(u - x_i) | b_i^2(u) + b_i(u)h(u) - f(u)$. By the Chinese Remainder Theorem for polynomials (see Exercise 3 in §3 of Chapter 3), there is a unique polynomial $b(u) \in \overline{\mathbb{F}}[u]$, $\deg_u b < \sum m_i$, such that

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

It can now be verified that $b(u)$ satisfies conditions 1), 2) and 3) of the theorem.

Next,

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

In addition,

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

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

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

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

$$\text{g.c.d.}(a(u), b(u) - v) = \sum_{P_i \in C_0} P_i + \sum_{P_i \in C_1} m_i P_i - m\infty = D ,$$

as required. □

Note that the zero divisor is represented as div$(1, 0)$. The next result follows from the proof of Theorem 5.1.

Lemma 5.3. *Let* $a(u), b(u) \in \overline{\mathbb{F}}[u]$ *be such that* $\deg_u b < \deg_u a$. *If* $a | (b^2 + bh - f)$, *then* div(a, b) *is semi-reduced.*

§ 6. Reduced Divisors

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

Definition 6.1. 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 6.2. 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 $D \in \mathbb{D}^0$, the operation described in the proof of Lemma 4.2 produces a semi-reduced divisor D_1 such that $D_1 \sim D$ and $|D_1| \leq |D|$.

Lemma 6.1. *Let R be a nonzero rational function in $\overline{\mathbb{F}}(C)$. If R has no finite poles, then R is a polynomial function.*

Proof. Let $R = G/H$, where G, H are nonzero polynomial functions in $\overline{\mathbb{F}}[C]$. 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 $a, b, c \in \overline{\mathbb{F}}[u]$, $c \neq 0$. Let $x \in \overline{\mathbb{F}}$ be a root of c. Let $P = (x, y) \in C$ where $y \in \overline{\mathbb{F}}$, and let $d \geq 1$ be the highest power of $(u - x)$ that 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 $a - bv$, we have $a(x) = 0$ 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, and it can be canceled 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 3) of the proof of Theorem 3.1, we can write

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

where A and D are nonzero polynomial functions in $\overline{\mathbb{F}}[C]$, 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 canceled 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 6.1. *For each divisor $D \in \mathbb{D}^0$ 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 $|D'| \leq |D|$ (see the proof of Lemma 4.2). 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 $\mathrm{supp}(D')$. The points P_i are not necessarily distinct, but 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

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

given by Theorem 5.1. 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.

Algorithm 2 in §7 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 4.2. 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 1) $\mathrm{ord}_P(D_2) = 0$ and $\mathrm{ord}_{\widetilde{P}}(D_2) = 0$, or 2) $\mathrm{ord}_P(D_2) = m_2$ with $1 \leq m_2 < m_1$, or 3) $\mathrm{ord}_{\widetilde{P}}(D_2) = m_2$ with $1 \leq m_2 \leq m_1$. (If P is special, then 3) cannot occur.) In case 1), $\mathrm{ord}_P(D_3) = m_1 \geq 1$. In case 2), $\mathrm{ord}_P(D_3) = (m_1 - m_2) \geq 1$. In case 3), $\mathrm{ord}_P(D_3) = (m_1 + m_2) \geq 1$. 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 nonzero rational function in $\overline{\mathbb{F}}(C)$ 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 6.1, since G has no finite poles, it must be a polynomial function. Then $G = a(u) - b(u)v$ for some $a, b \in \overline{\mathbb{F}}[u]$. 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 $x \in \overline{\mathbb{F}}$ 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. □

§ 7. Adding Reduced Divisors

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

Definition 7.1. A divisor $D = \sum m_P P$ is said to be *defined over* $\mathbb{F}$ if $D^\sigma \stackrel{\text{def}}{=} \sum m_P P^\sigma$ is equal to D for all automorphisms σ of $\overline{\mathbb{F}}$ over $\mathbb{F}$.

A principal divisor is defined over $\mathbb{F}$ if and only if it is the divisor of a rational function that has coefficients in $\mathbb{F}$. The set $\mathbb{J}(\mathbb{F})$ of all divisor classes in $\mathbb{J}$ that have a representative that is defined over $\mathbb{F}$ is a subgroup of $\mathbb{J}$. Each element of $\mathbb{J}(\mathbb{F})$ has a unique representation as a reduced divisor $\operatorname{div}(a, b)$, where $a, b \in \mathbb{F}[u]$, $\deg_u a \le g$, $\deg_u b < \deg_u a$; and hence $\mathbb{J}(\mathbb{F})$ is in fact a finite abelian group. This section presents an efficient algorithm for adding elements in this group.

Let $D_1 = \operatorname{div}(a_1, b_1)$ and $D_2 = \operatorname{div}(a_2, b_2)$ be two reduced divisors defined over $\mathbb{F}$ (that is, a_1, a_2, b_1, $b_2 \in \mathbb{F}[u]$). Algorithm 1 finds a semi-reduced divisor $D = \operatorname{div}(a, b)$ with $a, b \in \mathbb{F}[u]$, 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 in [Koblitz 1989]. They generalize earlier algorithms in [Cantor 1987], in which it was assumed that $h(u) = 0$ and $\operatorname{char}(\mathbb{F}) \ne 2$.

Algorithm 1

INPUT: Semi-reduced divisors $D_1 = \operatorname{div}(a_1, b_1)$ and $D_2 = \operatorname{div}(a_2, b_2)$, both defined over $\mathbb{F}$.

OUTPUT: A semi-reduced divisor $D = \operatorname{div}(a, b)$ defined over $\mathbb{F}$ such that $D \sim D_1 + D_2$.

1) Use the Euclidean algorithm (see §3 of Chapter 3) to find polynomials d_1, e_1, $e_2 \in \mathbb{F}[u]$ where $d_1 = \text{g.c.d.}(a_1, a_2)$ and $d_1 = e_1 a_1 + e_2 a_2$.
2) Use the Euclidean algorithm to find polynomials d, c_1, $c_2 \in \mathbb{F}[u]$ where $d = \text{g.c.d.}(d_1, b_1 + b_2 + h)$ 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 7.1. *Let $D_1 = \operatorname{div}(a_1, b_1)$ and $D_2 = \operatorname{div}(a_2, b_2)$ be semi-reduced divisors. Let a and b be defined as in equations* (4) *and* (5). *Then $D = \operatorname{div}(a, b)$ 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

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

Since $d|a_2$ and $a_2|(b_2^2+b_2h-f)$, b is indeed a polynomial.

Let $b=(s_1a_1b_2+s_2a_2b_1+s_3(b_1b_2+f))/d+sa$, where $s\in\mathbb{F}[u]$. 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 $\big(s_1a_1(b_2-v)+s_2a_2(b_1-v)+s_3(b_1-v)(b_2-v)\big)$ with its conjugate; and 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 5.3 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.

1) Let $P=(x,y)$ be an ordinary point. There are two subcases to consider.
   a) Suppose that $\mathrm{ord}_P(D_1)=m_1$, $\mathrm{ord}_{\tilde{P}}(D_1)=0$, $\mathrm{ord}_P(D_2)=m_2$, and $\mathrm{ord}_{\tilde{P}}(D_2)=0$, 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 $\mathrm{ord}_{\tilde{P}}(D_2)=m_2$, 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 $\mathrm{ord}_{\tilde{P}}(b_2-v)\geq m_2$. 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, $\mathrm{ord}_P(D)=m_1-m_2$.

2) 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 either $\mathrm{ord}_P(b_1+b_2+h)\geq 2$ 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 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 7.1. 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 1.3). $P = (\alpha^{30}, 0)$ is an ordinary point in $C(\mathbb{F}_{2^5})$, and the opposite of P is $\widetilde{P} = (\alpha^{30}, \alpha^{16})$. $Q_1 = (0, 1)$ 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).

1) Let $D_1 = P + Q_1 - 2\infty$ and $D_2 = \widetilde{P} + Q_2 - 2\infty$ 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) $d_1 = \mathrm{g.c.d.}(a_1, a_2) = u + \alpha^{30}$; $d_1 = a_1 + a_2$.
   2) $d = \mathrm{g.c.d.}(d_1, b_1 + b_2 + h) = u + \alpha^{30}$; $d = 1 \cdot d_1 + 0 \cdot (b_1 + b_2 + h)$.
   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:

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

2) 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) $d_1 = \mathrm{g.c.d.}(a_1, a_2) = u$; $d_1 = \alpha^{14}a_1 + \alpha^{14}a_2$.
   2) $d = \mathrm{g.c.d.}(d_1, b_1 + b_2 + h) = u$; $d = 1 \cdot u + 0 \cdot (b_1 + b_2 + h)$.
   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:

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

3) 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) $d_1 = \text{g.c.d.}(a_1, a_2) = (u + \alpha^{30})$; $d_1 = 1 \cdot a_1 + 1 \cdot a_2$.
2) $d = \text{g.c.d.}(d_1, b_1 + b_2 + h) = 1$.
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:

$$\text{div}(a) = 2P + 2\widetilde{P} + 2Q_1 + 2Q_2 - 8\infty$$

$$\text{div}(b - v) = 2P + Q_1 + Q_2 + \sum_{i=1}^{2} P_i - 6\infty \ , \quad \text{where} \quad P_i \neq P, \widetilde{P}, Q_1, Q_2$$

$$\text{div}(a, b) = 2P + Q_1 + Q_2 - 4\infty \ .$$

Algorithm 2

INPUT: A semi-reduced divisor $D = \text{div}(a, b)$ defined over $\mathbb{F}$.
OUTPUT: The (unique) reduced divisor $D' = \text{div}(a', b')$ such that $D' \sim D$.
1) Set

$$a' = (f - bh - b^2)/a$$

and

$$b' = (-h - b) \bmod a' \ .$$

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 7.2. *Let $D = \text{div}(a, b)$ be a semi-reduced divisor. Then the divisor $D' = \text{div}(a', b')$ 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

1) $\deg_u(a') < \deg_u(a)$;
2) $D' = \text{div}(a', b')$ is semi-reduced; and
3) $D \sim D'$.

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

1) 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 $\deg_u a' = g < \deg_u a$.
2) Now $f - bh - b^2 = aa'$. Reducing both sides modulo a', we obtain

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

which simplifies to

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

Hence $a' | (f - b'h - (b')^2)$. It follows from Lemma 5.3 that $\text{div}(a', b')$ is semi-reduced.

3) Let $C_0 = \{P \in \text{supp}(D) : P \text{ is special}\}$, $C_1 = \{P \in \text{supp}(D) : P \text{ is ordinary}\}$, and $C_2 = \{\widetilde{P} : P \in C_1\}$, so that

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

Then, as in the proof of Theorem 5.1, we can write

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

and

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

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 4.1 that

$$\begin{aligned}
&\text{div}(b^2 + bh - f) \\
&\quad = \sum_{P_i \in C_0} 2P_i + \sum_{P_i \in C_1} n_i P_i + \sum_{P_i \in C_1} n_i \widetilde{P}_i + \sum_{P_i \in C_3} s_i P_i + \sum_{P_i \in C_3} s_i \widetilde{P}_i - (*)\infty \ ,
\end{aligned}$$

and hence

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

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 $s \in \mathbb{F}[u]$. 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 5.1, it follows that

$$\begin{aligned}
&\text{div}(b' - v) \\
&\quad = \sum_{P_i \in C_1'} 0P_i + \sum_{P_i \in C_1'} r_i \widetilde{P}_i + \sum_{P_i \in C_3} 0P_i + \sum_{P_i \in C_3} w_i \widetilde{P}_i + \sum_{P_i \in C_4} z_i P_i - (*)\infty \ ,
\end{aligned}$$

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,

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

whence $D \sim D'$. □

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

Example 7.2. 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 Examples 1.3 and 7.1). Consider the semi-reduced divisor $D = (0,1) + (1,1) + (\alpha^5, \alpha^{15}) - 3\infty$. Then $D = \operatorname{div}(a, b)$, where

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

and

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

Algorithm 2 yields

$$a'(u) = u^2 + \alpha^{15}u + \alpha^{26} \ ,$$

$$b'(u) = \alpha^{23}u + \alpha^{21} \ .$$

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

Exercises

1. Verify that the curves C in Examples 1.2 and 1.3 have no singular points (except for ∞).

2. Let $R \in \mathbb{F}(C)$ be a non-zero rational function, and let $P \in C$. Prove that $\operatorname{ord}_P(R)$ does not depend on the representation of R as a ratio of polynomial functions (see Definition 3.4).

3. Prove Lemma 5.3.

4. Let C be the curve in Example 1.2. Find the divisor of the polynomial function $G(u, v) = v^2 + uv + 6u^4 + 6u^3 + u^2 + 6u$.

5. Let C be the curve in Example 1.2. Find the polynomial representation for the semi-reduced divisor $D = 2(2,2) + 3(5,3) + (1,1) + (6,4)$.

6. Let C be the curve in Example 1.2. Use Algorithm 1 to compute $D_3 = \operatorname{div}(a_3, b_3) = D_1 + D_2$, where $D_1 = \operatorname{div}(u^2+6, 2u+6)$ and $D_2 = \operatorname{div}(u^2+4u+2, 4u+1)$. Check your work by computing these divisors explicitly.

7. Let C be the curve in Example 1.2. Consider the semi-reduced divisor $D = \operatorname{div}(u^7 + 2u^6 + 3u^5 + 6u^3 + 4u + 5, 5u^6 + 5u^5 + 6u^4 + 4u^3 + 5u^2 + 4)$. Use Algorithm 2 to find the reduced divisor equivalent to D.