Addition in the Jacobian of a Curve over a Finite Field

Emil J. Volcheck
Research Institute for Symbolic Computation
`volcheck@acm.org` — `http://acm.org/~volcheck`

Manuscript for a presentation given at the Oberwolfach conference, Computational Number Theory, *28 May – 3 June 1995. Preliminary version, last revised 15 July.*

Abstract

We describe a constructive procedure for adding points on the Jacobian of a curve (represented as the divisor class group) defined over a perfect ground field. For curves defined over a finite field or over the rationals, we present an algorithm that performs this construction.

Contents

1 Introduction **2**

2 Background **2**
2.1 Adjoints . . . 3
2.1.1 A Separating Variable . . . 3
2.1.2 The Conductor . . . 4
2.2 Addition and Reduction . . . 5

3 Methods **8**
3.1 Divisors . . . 8
3.1.1 Intersecting Curves . . . 8
3.1.2 Hamburger-Noether Expansions . . . 9
3.1.3 Operations on Divisors . . . 10
3.2 Algorithm . . . 10

4 Degree Bounds **11**

5 Examples **12**
5.1 Adjoint Divisor . . . 12
5.2 Addition . . . 13

1 Introduction

For an absolutely irreducible algebraic curve of genus g with a rational point, addition on the Jacobian variety of the curve can be represented in the divisor class group as the addition of divisors of degree g followed by a reduction operation, which yields a divisor of degree g equivalent to the sum. The Brill-Noether method of adjoints, first described by A. Brill and M. Noether in [3] and further developed by Noether in [16], provides a way to carry out this operation.

Huang and Ierardi gave a polynomial-time algorithm for addition in the case where the curve has only ordinary multiple points [13] and have further developed their methods in [14]. A fast algorithm for addition on hyperelliptic curves in normal form was described by Cantor [5]. For addition on a curve defined over the rationals with arbitrary singularities, an algorithm was presented in [25]. When the curve has only ordinary multiple points, this algorithm has better complexity than the Huang and Ierardi algorithm.

Coding theorists have also studied the method of adjoints for its applications to the algebraic-geometric codes due to Goppa. Dominique Le Brigand and J.J. Risler used the method of adjoints to construct a code whose parameters exceed the Gilbert-Varshamov bound [2]. These methods have been refined, and an algorithm for the construction of Goppa codes has been developed by G. Haché and D. Le Brigand [11]. Similar techniques have also been pursued by D. Polemi et al [19].

The method of adjoints makes use of certain key properties of curve adjoints. These properties have been generalized by Gorenstein to the case of curves defined over a perfect ground field [9]. We will show that the method of adjoints holds in this more general context and yields a theoretical algorithm, by which I mean a constructive procedure, for addition in the Jacobian of a curve over a perfect field. We present an algorithm, adapted from [25], to carry out the addition operation for curves defined over the rationals or over a finite field, which performs the constructions of the more general procedure.

2 Background

In this section, we describe how the Riemann Inequality can be applied to reduce the sum of two divisors. The proof we present of the Riemann Inequality utilizes the Brill-Noether method of adjoints. This method requires information about the singularities of a curve that is expressed by the adjoint divisor. We first look at how to determine the adjoint divisor based on its relationship to the conductor ideal.

We recall basic facts about function fields, including places, divisors, and separability. We refer the reader to Chevalley [6], Gorenstein [9], and Stichtenoth [22].

Given an absolutely irreducible curve $C : F(x, y) = 0$ defined over a perfect ground field k, we view the function field of C as the quotient field

K of the coordinate ring $\mathcal{O} = k[x, y]/\langle F(x, y)\rangle$. We define a *(closed) point* to be a complete conjugate set of (geometric) points, which corresponds to a maximal ideal in $\mathcal{O}$. The degree of a point is the degree of the residue field over k of its maximal ideal. By a *(closed) place*, we mean a complete conjugate set of (geometric) places, which corresponds to a valuation ring of K, which is centered at some point. The residue field of a place is a finite extension of the residue field of the point where it is centered. The degree of a place is the degree of its residue field over k. We identify each closed place with a prime divisor of the curve. A divisor is a finite formal sum of prime divisors with integer multiplicities of the form $\sum m_i P_i$. The degree of a divisor in this form is $\sum m_i \deg(P_i)$.

2.1 Adjoints

Perhaps the first detailed constructive procedure for computing the adjoints of a curve was given by M. Noether [16]. He applied the S-transformation, a particular kind of plane Cremona transformation, to simplify the singularities of a curve into ordinary multiple points. In this case, the adjoints can be easily computed. This transformation does not extend the ground field of the curve, because it simultaneously blows up conjugate sets of points. However his use of the transformation exponentially increases the degree of the proper transform because he applies it globally. A closer study of this approach was made in [25, Chap. 2] and [24].

Other ways to determine the adjoint divisor have been found recently. Polemi et al [17] calculate the adjoint divisor of a plane algebraic curve defined over a finite field by using an integral closure algorithm to construct a non-singular model of the curve. Haché & Le Brigand [11] and Polemi [18] describe how to compute the adjoint divisor of a curve over a finite field by resolving each singularity with quadratic transformations and then applying some relationship involving the conductor and/or differentials of the first kind. Sendra and Winkler [21] also compute the adjoints of a curve using quadratic transformations and apply this procedure to parametrizing rational curves.

2.1.1 A Separating Variable

An element $z \in K$ for which $K/k(z)$ is separable, we call a *separating variable* (or *separating element*). Finding a separating variable allows us to compute the adjoint divisor using the technique described in the next section.

In characteristic zero, K/k is a separable extension, hence any element is a separating variable. Stichtenoth shows that even when k has characteristic p, K always has a separating variable, i.e. is separably generated over k (p. 128, Prop. III.9.2). Furthermore, he shows that any element $z \in K$ is a separating variable iff $z \notin K^p$. This implies the following corollary:

Corollary 1 *Either x or y is a separating variable for the extension K/k.*

Proof: K is generated over k by x and y. If neither x nor y were a separating variable, then together they would generate a proper subfield of K. $\square$

We can use the following criterion to recognize a separating variable: for $z \in K$, z is a separating variable iff $dz \neq 0$ [22, Prop. IV.1.8(c)]. Consider the completion at any place on the curve. Let t be a local parameter for the place and let an expansion $x = x(t),\ y = y(t)$, whose coefficients are in the residue field of the place, be given. If $dx/dt \neq 0$, then x is a separating parameter, otherwise y is a separating parameter.

2.1.2 The Conductor

For basic facts about the conductor and its relation to the adjoints of a curve, we refer to Gorenstein [9].

Let us also consider K as an extension of $k(x)$, for x a separating variable, that is, as the quotient field of $k(x)[y]/\langle F(x,y)\rangle$. Let $\bar{\mathcal{O}}$ be the integral closure of $\mathcal{O}$ in K. Let P be a point on the curve, and let $\{p_i\}$ denote the places centered at P with valuations v_i. Let $\mathcal{O}_P$ be the local ring of $\mathcal{O}$ at the point P and $\bar{\mathcal{O}}_P$ be its integral closure in K.

We introduce the discriminant, conductor, and different ideals for K. Let $\mathcal{C} = \{c \in \mathcal{O} : c\,\bar{\mathcal{O}} \subseteq \mathcal{O}\}$ be the conductor ideal of $\mathcal{O}$ in $\bar{\mathcal{O}}$ [1, p. 143]. The conductor is the largest ideal in $\bar{\mathcal{O}}$ that is still an ideal in $\mathcal{O}$. Locally we define the conductor at P to be $\mathcal{C}_P = \{c \in \mathcal{O}_P : c\,\bar{\mathcal{O}}_P \subseteq \mathcal{O}_P\}$.

We denote the discriminant ideal in $\mathcal{O}$ as $D = \langle F_y\rangle$. The different $\mathcal{D}$ is defined as the inverse of the complementary module to $\bar{\mathcal{O}}$. (see Lang [15, Ch. 3] or also [22, p. 81]). Since x is a separating element, we can use a property of the different that determines its divisor: $v_i(\mathcal{D}) = v_i(dx)$, for any place p_i of K [6, Thm. 7, p. 110]. Note that the valuation of an ideal is the minimum of the valuations of its elements.

The adjoint divisor at a point P, denoted Δ_P, is defined to be the divisor corresponding to $\mathcal{C}_P$, i.e. $\sum_i v_i(\mathcal{C}_P)\cdot p_i$. The adjoint divisor Δ of the curve is the sum of the adjoint divisors at each singular point. An adjoint is a polynomial that cuts out a multiple of the adjoint divisor on the curve, i.e. its intersection multiplicity with the curve is at least $v_i(\mathcal{C}_P)$ at every place p_i. The localization of $\mathcal{C}$ at P equals $\mathcal{C}_P$, so $v_i(\mathcal{C}) = v_i(\mathcal{C}_P)$ for a place p_i [9, p. 430].

To determine the adjoint divisor, we thus need to determine the order of the conductor at each place. We apply the following important relationship:

Proposition 2 *Let D, $\mathcal{C}$, and $\mathcal{D}$ denote the discriminant, conductor, and different ideals of K. Then in $\bar{\mathcal{O}}$, we have*

$$D = \mathcal{C}\cdot\mathcal{D}.$$

Proof: See [9, p. 435] or [12, p. 145]. $\square$

Let $t \in K$ be a local parameter for a place p_i of K. We can then write $x = x(t),\ y = y(t)$ in the completion of $\mathcal{O}$ at p_i. We evaluate the order of the different $\mathcal{D}$ at p_i by differentiating $x(t)$ with respect to t (see [22, Thm. IV.3.2(e) on p. 150]):

$$v_i(\mathcal{D}) = v_i(dx) = \mathrm{ord}_t\left(\frac{d}{dt}x(t)\right).$$

This argument gives us the following formula:

Proposition 3 *The order of the conductor ideal at p_i equals*

$$v_i(\mathcal{C}) = v_i(F_y) - \mathrm{ord}_t(dx/dt).$$

Roughly speaking, when we interpolate a polynomial through a regular point, we require one linear condition for each order of vanishing. At a regular point, the conductor is trivial. Interpolating a polynomial through a singularity causes difficulty in that we achieve a higher intersection multiplicity with fewer linear conditions. We can use the conductor to compensate for this difficulty in a way stated by Gorenstein [9, Theorem 10].

Theorem 4 *Let $\deg(\mathcal{C})$ denote the degree of the conductor $\mathcal{C}$ and let $\delta(\mathcal{C})$ denote the maximum number of linear conditions that $\mathcal{C}$ imposes on curves. Then*

$$\deg(\mathcal{C}) = 2\,\delta(\mathcal{C}).$$

Proof: See [9, Theorem 10].

Gorenstein also generalizes the genus formula in terms of the conductor:

Theorem 5 *The genus g of a curve of degree n equals*

$$g = \frac{1}{2}(n-1)(n-2) - \delta(\mathcal{C}).$$

Proof: See [9, Theorem 11].

These two relations play a key role in the method of adjoints.

2.2 Addition and Reduction

Given a polynomial $g(x, y)$, we define the intersection divisor $I_F(g)$ as the divisor $\sum m_i P_i$, where the P_i range over all places of intersection of the curve polynomial F with g, and m_i equals the intersection multiplicity of F with g at P_i. The principal divisor of a rational function g_1/g_2 is defined to be $\mathrm{div}(g_1/g_2) = I_F(g_1) - I_F(g_2)$. We say two divisors are equivalent when they differ by a principal divisor and write $D_1 \equiv D_2$. We refer to a divisor class as the equivalence class of a divisor. The quotient group of degree zero divisors modulo principal divisors is called the divisor class group (of degree zero divisors) or the Picard variety [10, Chap. 5].

We say a divisor D is effective (or non-negative) if the multiplicities m_i of its places P_i are non-negative. We write $D \geq 0$ to denote this. For divisors $D_1 = \sum m_i P_i$ and $D_2 = \sum n_i P_i$, we write $D_1 \geq D_2$ when $m_i \geq n_i$, for all i. For a divisor D, define the space of rational functions

$$\mathcal{L}(D) = \{g : \mathrm{div}(g) \geq -D\}.$$

We denote the dimension of $\mathcal{L}(D)$ as $\ell(D)$. This space corresponds to the space of all effective divisors equivalent to D.

The Abel-Jacobi map induces an isomorphism between the divisor class group and the Jacobian variety of the curve. Furthermore, the restriction of the Abel-Jacobi map to the g-fold symmetric product of the curve, which corresponds to divisors of degree g, is surjective and generically injective [10, p. 156, 185].

We assume the curve C has a rational point P_0. We represent addition of points on the Jacobian variety of a curve as formal addition of divisors of degree up to g, followed by a reduction operation which produces a divisor of degree up to g equivalent to the formal sum. More precisely, we identify any divisor D of degree m with the degree zero divisor $D - mP_0$. We seek an equivalent divisor D_1 that can be expressed in a reduced form $D_r - gP_0$. That we can always find a principal divisor to perform this reduction follows from the Riemann Inequality:

Theorem 6 (Riemann) *Given a curve C of genus g and degree n, and a divisor D of degree d, then*

$$\ell(D) \geq d - g + 1.$$

We will present a constructive proof but defer this for the moment in order to formally state the reduction procedure:

Proposition 7 *Given a divisor $D - mP_0$, where D has degree $m > g$, there is an equivalent divisor $D_1 = D_r - gP_0$, where D_r is effective and has degree g.*

Proof: Consider the divisor $S = D - (m-g)P_0$ of degree g. Apply the Riemann Inequality to find an f in $\mathcal{L}(S)$. Then

$$D_1 \leftarrow D + \operatorname{div}(f) = (m-g)P_0 + D_r,$$

where D_r is effective and has degree g since D and D_1 both have degree m. Then

$$D - mP_0 \equiv D_1 - mP_0 \equiv D_r - gP_0.$$

which gives the reduced form. □

Given two divisors each of degree g, we apply this reduction procedure to their sum, which has degree $2g$, and obtain a reduced equivalent divisor of degree g. We test whether two divisors D_1 and D_2 are equivalent by computing $\mathcal{L}(D_1 - D_2)$. We return to the proof of the Riemann Inequality.

Proof: We construct the space of functions $\mathcal{L}(D)$ and estimate its dimension. Our technique is similar to that used by Griffiths in the special case when the curve singularities are only ordinary double points [10, p. 112], however we apply Theorem 4 to handle arbitrary singularities.

Write the divisor D of degree d as a difference of effective divisors D^+ of degree d^+ and D^- of degree d^- such that $D = D^+ - D^-$ and $d = d^+ - d^-$.

Let $b(x, y)$ be an adjoint of degree m, not a multiple of the curve polynomial $F(x, y)$, for which

$$I_F(b) \geq D^+ + \Delta,$$

that is, b is an adjoint passing through D^+.

Let $\mathcal{F}(m, n)$ denote the dimension (or degrees of freedom) of the space of polynomials of degree m which are not multiples of a fixed polynomial of degree n, that is,

$$\mathcal{F}(m, n) = \binom{m+2}{2} - \binom{m-n+2}{2}.$$

We must choose m large enough that

$$\mathcal{F}(m, n) > d^+ + \delta(\mathcal{C}). \tag{1}$$

Below in section 4, we calculate an upper bound on the smallest m which satisfies these properties in the case of adding two divisors each of degree g.

Next, we determine the divisor E for which $I_F(b) = D^+ + \Delta + E$. We refer to this as the residual divisor. We apply Bezout's Theorem to write the degree e of the residual divisor as

$$\deg(E) = e = mn - (d^+ + 2\,\delta(\mathcal{C})), \tag{2}$$

where we have also applied Theorem 4.

Let $r(x, y)$ be an adjoint of the same degree m, not a multiple of F, for which

$$I_F(r) \geq D^- + E + \Delta, \tag{3}$$

that is, an adjoint passing through $D^- + E$. The rational function r/b is in $\mathcal{L}(D)$ since

$$I_F(r) - I_F(b) \geq (D^- + E + \Delta) - (D^+ + \Delta + E).$$

So $\mathrm{div}(r/b) \geq -D$. If we let R denote the divisor of degree g for which $I_F(r) = D^- + E + \Delta + R$, then $\mathrm{div}(r/b) = R - D$.

The number of linear conditions which the requirement (3) imposes on r is no more than

$$d^- + e + \delta(\mathcal{C}) = mn - d - \delta(\mathcal{C}).$$

The number of degrees of freedom we have to choose r is thus at least

$$\mathcal{F}(m, n) - (mn - d - \delta(\mathcal{C})). \tag{4}$$

To simplify this expression, we point out a useful relationship in the following lemma:

Lemma 8

$$\mathcal{F}(m, n) - mn + g + \delta(\mathcal{C}) = 1.$$

Proof: Apply the genus formula (Theorem 5) to substitute $\frac{1}{2}(n-1)(n-2)$ for $g + \delta(\mathcal{C})$ and simplify. $\square$

To complete the proof of the Riemann Inequality, we simplify equation (4) by adding g, applying the lemma to simplify the expression to $d+1$, and subtracting g. Therefore, we have at least $d - g + 1$ degrees of freedom for r. $\square$

We now turn to explicit methods for the constructions we have discussed in this section.

3 Methods

We describe an algorithm that performs the constructions of the previous section. Our algorithm requires that we are able to perform polynomial arithmetic, calculate greatest common divisors, and factor univariate polynomials over towers of algebraic extensions of the ground field. Square-free factorization suffices if we apply lazy factorization techniques [7, 23], but we do not treat this technique here.

We restrict ourselves to the cases where the ground field is either the rationals or a finite field. Here we have all of the above operations, and all ground field extensions are separable. In principle, the algorithm is valid for any field k where we have the above operations. The algebraic closure $\bar{k}$ is perfect, and adjoints can also be computed as described above. However, to represent $\bar{k}$ we would dynamically form extensions of k which could be inseparable. We do not treat this more general setting here and intend to address this matter in future work.

3.1 Divisors

3.1.1 Intersecting Curves

Given two polynomials $F(x,y)$ and $G(x,y)$, we determine their intersection divisor $I_F(G)$ by first computing their resultant

$$r(x) = \mathrm{Res}_y(F, G).$$

We factor $r(x)$ into the product $\prod_i r_i(x)$. For each $r_i(x)$, we adjoin γ_i as a root of $r_i(x)$, then compute the gcd $p_i(\gamma_i, y)$ of $F(\gamma_i, y)$ and $G(\gamma_i, y)$ over $k(\gamma_i)$. Then we factor p_i into a product $\prod_j p_{ij}(\gamma_i, y)$. Each pair $(r_i(x), p_{ij}(x,y))$ represents a closed point. To determine intersections on the line at infinity, we homogenize with respect to a variable z, set $z = 0$, and take the gcd of the polynomials as homogeneous polynomials in two variables.

If we wish to find those closed points in the intersection of F with G which meet a third curve $H(x,y)$, then for each $r_i(x)$ with root γ_i, we calculate the gcd of $p_{ij}(\gamma_i, y)$ with $H(\gamma_i, y)$ over $k(\gamma_i)$. We find the infinite intersection points by homogenizing F, G, and H and taking their gcd on the line at infinity.

By choosing G and H to be the appropriate partial derivatives, we can determine the singular closed points of the curve.

When we refer to a point in explicit form, we mean, for a finite point, that we have an ideal $\langle a(x), b(x,y)\rangle$, where $a(x)$ and $b(x,y)$ are irreducible and as in the above form for $r_i(x)$ and $p_{ij}(x,y)$. To evaluate a polynomial at such a point, we reduce modulo $b(x,y)$ then modulo $a(x)$. We represent an infinite point as a homogeneous polynomial $a(x,y)$.

3.1.2 Hamburger-Noether Expansions

Hamburger-Noether expansions are a technique for determining a local parameter t and an expansion $x = x(t)$, $y = y(t)$ at the places of a curve in arbitrary characteristic [4, 20]. When the characteristic does not divide the ramification degree of the place, then a Hamburger-Noether expansion reduces to a Puiseux expansion.

D. Duval's procedures for representing Puiseux expansions in conjugate sets [7] carry over directly to Hamburger-Noether expansions over finite fields because all ground field extensions are separable. We sketch the technique. Each step of the Hamburger-Noether algorithm builds successive levels of the tree of singular places at a singular point. Each step requires finding a root of a characteristic polynomial obtained from the Newton Polygon. By factoring the characteristic polynomials and adjoining roots, we build a tree of expansions with a corresponding tree of towers of extensions. Upon termination of the algorithm, each leaf of the tree corresponds to a local nonsingular model of the curve at the place, a Hamburger-Noether expansion which determines the place, and a tower of extensions which is the residue field of the place.

Because all extensions of the residue field are separable, we can represent the expansions in conjugate sets, by taking the children of a node which correspond to distinct conjugate roots of the characteristic polynomial as conjugate partial expansions.

We shall refer to a place in explicit form as a representation of the place by a point in explicit form, a Hamburger-Noether expansion, and a representation of the residue field of the place as a sequence of minimal polynomials for each extension of the ground field. For a place on the line at infinity, we take an expansion with respect to an appropriate dehomogenization of the homogenized curve polynomial. To evaluate a polynomial at a place, we substitute the Hamburger-Noether expansion for x and y in t and reduce modulo the minimal polynomials for the residue field tower. The order of a polynomial at a place is then the order in t of the polynomial evaluated at that place, where we may need to compute additional terms of a Hamburger-Noether expansion for a singular place or of a Taylor expansion for a regular place.

The set of singular places can be represented as a forest of trees rooted at distinct singular points with residue field initially equal to the residue field of the point.

3.1.3 Operations on Divisors

Divisors are represented as formal sums of places in explicit form with multiplicities. Formal addition and subtraction of divisors means adding and subtracting their multiplicities.

When we interpolate a polynomial through a divisor D, we construct a polynomial $G(x, y)$ of undetermined coefficients, evaluate this polynomial at each place of D, impose linear conditions on G so that sufficiently many terms at each place vanish to satisfy $I_F(G) \geq D$ (where we compute further terms of the expansions as needed), and then solve this linear system. The evaluation procedure includes reducing modulo the tower of extensions of the residue field, so our linear system is over the ground field k, and our solutions for G will again be defined over the original ground field of the curve. The interpolation procedure is "rational" in this sense.

We need to be able to subtract an explicit divisor D from an (implicit) intersection divisor $I_F(G)$ when $I_F(G) \geq D$. To do so, we first form a polynomial $s_1(x)$ whose roots represent the x-coordinates of D with proper multiplicity. Then we form the resultant $s(x) = \mathrm{Res}_y(F, G)$ and divide by $s_1(x)$ to get $\bar{s}(x) = s/s_1$. Then we proceed as above to compute the intersection divisor of F with G over the roots of $\bar{s}(x)$. We factor $\bar{s}(x)$ into a product $\prod_i \bar{s}_i(x)$, adjoin roots $\bar{\gamma}_i$, and take the gcd of $F(\bar{\gamma}_i, y)$ with $G(\bar{\gamma}_i, y)$ over $k(\bar{\gamma}_i)$. Then we factor the gcds to obtain a representation for each closed point of the intersection.

For each closed point in this set, we identify the places at this point, compute the intersection multiplicity of each place in the intersection divisor (where we compute further terms of expansions as needed), and then subtract from the multiplicity of this place the multiplicity of this place in D (if it occurs). We remove places whose multiplicity drops to zero and form the divisor of those remaining.

3.2 Algorithm

We describe the algorithm for reducing the sum of two divisors of degree g, following the proof of the Riemann Inequality.

We begin by identifying the singular points and computing Hamburger-Noether expansions for each singular place. We identify a separating parameter by the method in subsection 2.1.1 and calculate the adjoint divisor as described in subsection 2.1.2. Note that to determine a separating parameter, we need look at no more than the first $v_P(F_y)$ terms of dx/dt or the first $v_P(F_x)$ terms of dy/dt at a place P with valuation v_P.

Given an explicit representation for two divisors D_1 and D_2, each of degree g, We will reduce their sum $D = D_1 + D_2$. First, we interpolate the polynomial $b(x, y)$ to satisfy $I_F(b) \geq A$, where $A = D + \Delta$. We subtract A from $I_F(b)$ as described above in subsection 3.1.3 to obtain the residual divisor E.

Then we determine a basis for the polynomials $\{r_i(x, y)\}$ which satisfy $I_F(r) \geq H$, where $H = g\, P_0 + E + \Delta$. The rational functions r_i/b form a basis for $\mathcal{L}(D - g\,P_0)$. We choose $r(x)$ to be a linear combination of the $r_i(x)$. We have always at least one choice for r, since $D - g\,P_0$ has degree g. We subtract H from $I_F(r)$ to obtain the divisor R corresponding to the reduced sum of D_1 and D_2.

4 Degree Bounds

In this section, we provide sharp bounds for the degree of the interpolated adjoints and of the residual divisor, which improve upon results in [25]. We do not provide a full complexity analysis here but refer to [25] for a complexity analysis in the case of a curve over the rationals whose singularities are ordinary multiple points.

To work with a residual divisor of degree as small as possible, we wish to choose the degree m of our interpolating polynomial $b(x,y)$ to be as small as possible and still satisfy equation (1) of section 2.2. Set U equal to $\lceil \frac{g+2}{n} \rceil$.

Proposition 9 *To reduce the sum of two divisors D_1 and D_2, each of degree g, an interpolating polynomial $b(x,y)$ of degree m must satisfy*

$$\mathcal{F}(m,n) > 2g + \delta(\mathcal{C}).$$

Choosing $m = n + U - 3$ always suffices.

Proof: We apply the genus formula to this condition to replace $g + \delta(\mathcal{C})$ by $\frac{1}{2}(n-1)(n-2)$ and simplify to get $n(m - n + 3) > g + 1$, hence

$$m > \frac{g+1}{n} + n - 3.$$

Thus we can take $m = U + n - 3$. □

We can now bound the size of the residual divisor.

Corollary 10 *The degree e of the residual divisor E is dominated by* $\max(n, g)$.

Proof: By equation (2) of section 2.2, and for $d^+ = 2g$, we have

$$\begin{aligned} e &= mn - 2g - 2\,\delta(\mathcal{C}) \\ &= (n + U - 3)n - (n-1)(n-2) \\ &= nU - 2, \end{aligned}$$

where we have applied the genus formula going to step 2. □

On elliptic curves, to add two points, we draw a line through the points and determine the residual third point on the line. Then we draw a second line through the residual point and the zero point to determine the third point on the line, which is the reduced sum. We can extend this analogy to curves of genus g by showing that we can choose the residual divisor E to have the form of a degree g divisor plus a multiple of the zero point.

Proposition 11 *We may choose the interpolating polynomial $b(x,y)$ so that the residual divisor E has the form $E' + kP_0$, where $k = e - g$ and E' has degree g.*

Proof: Consider again equation (1) of section 2.2. To impose an additional k linear conditions on our choice of b, the degree m must be large enough to satisfy

$$\mathcal{F}(m,n) > d^+ + \delta(\mathcal{C}) + (e-g).$$

Using equation (2) to substitute $mn - (d^+ + 2\,\delta(\mathcal{C}))$ for e, we simplify and shift terms to the left to get

$$\mathcal{F}(m,n) - mn + g + \delta(\mathcal{C}) > 0.$$

The left-hand side equals 1 by Lemma 8, hence we can always choose $b(x,y)$ to give us the desired form $E = E' + kP_0$. $\square$

Since the residual and reduced divisors each have degree dominated by $\max(n,g)$, this limits the number of additional terms of expansions that need to be computed during the course of the algorithm, apart from the initial work to determine the singular places and adjoint divisor.

Experimental evidence suggests that for curves over the rationals, over 80% of computing time is spent in determining the residual and reduced divisors. These operations are performed by taking gcds of polynomials of degree m and n over an extension of degree g. Recent work by M. Encarnación gives an improved complexity bound on this problem and significantly speeds up these calculations in practice [8].

5 Examples

5.1 Adjoint Divisor

We first consider two examples taken from [20, pp. 66 ff.] which demonstrate the method for computing the adjoint divisor at a place of a curve over a finite field. In both examples, we consider only the places at the origin, and the ground field is the finite field with two elements, GF(2).

Let $F(x,y) = y^2 + yx^4 + x^8 + x^{10}$. This curve has a pair of conjugate Puiseux expansions at the origin, $y = \delta x^4 + \cdots$, where δ satisfies $\delta^2 + \delta + 1 = 0$. There is no ramification, hence the different has order zero, i.e. x is a local parameter and separating variable, $dx/dx = 1$. The discriminant has order 4 since $F_y = x^4 + \cdots$. Hence the order of the adjoint divisor at each place is 4.

We can verify that the sum of adjoint orders is 8 by resolving the singularity at the origin through quadratic transformations. If e_i is the order of the singularity at the ith step, then $\sum e_i(e_i - 1)$ is the total order of the conductor at this singularity. Starting with $F = y^2 + yx^4 + x^8 + x^{10}$, we repeatedly substitute $y = xy$ and take the proper transform to get $y^2 + x^3y + x^6 + x^8$, then $y^2+x^2y+x^4+x^6$, then $y^2+xy+x^2+x^4$, and finally $y^2+y+1+x^2$, which has two non-singular points on the exceptional line. The original curve and each transform has order 2, for a total order of 8.

Next let $F(x,y) = y^4 + x^4 + x^2y^2 + x^7$. The singularity at the origin has conjugate Hamburger-Noether expansions

$$\begin{aligned} y &= \delta x + x^2 t \\ x &= t^2(1 + t^6 + \cdots), \end{aligned}$$

where δ satisfies $\delta^2+\delta+1 = 0$. Notice that $dx/dt \equiv 0$ since the characteristic is two, hence x is not a separating variable. Therefore we switch variables and consider the function field as the extension $K/k(y)$. We substitute to get an expansion for y in t as $y(t) = \delta t^2 + t^5 + \delta t^8 + \cdots$. Then since $F_x = x^6$, we have the order of the discriminant equal to 12. We differentiate $y(t)$ with respect to t to get order 4 for the different. Hence the conductor at each place has order $12 - 4 = 8$.

We can verify that the total of the adjoint orders at the origin is equal to 16 by applying quadratic transformations again to resolve the singularity. Starting with $F = y^4 + x^4 + x^2y^2 + x^7$, we obtain $y^4 + y^2 + x^3 + 1$. We translate $y = y + \delta$ to get $y^4 + y^2 + x^3$, then $x^2y^4 + y^2 + x$. Hence we have an order 4 singularity which separates into two order 2 singularities. The total order is $4(4-1) + 2 + 2 = 16$.

5.2 Addition

We present an example of adding divisors on a curve over the rationals. The calculations were carried out in `Maple`.

The curve C specified by the polynomial,

$$\begin{aligned} F(x,y) &= -8 + 4\,y + 2\,y^2 - 3\,y^3 + 82\,y^4 \\ &\quad -81\,y^5 + 2\,xy^3 - 2\,xy^4 + 8\,x^2 \\ &\quad -4\,x^2y + x^2y^3 - 2\,x^4 + x^4y, \end{aligned}$$

has two singular places, Δ_1 and Δ_2. The places are centered at the conjugate set of points $\{(-\alpha, 0),\ (\alpha, 0)\}$, where $\alpha^2 - 2 = 0$. The places Δ_1 and Δ_2 form two ordinary double points over a ground field extension to $\mathbb{Q}(\alpha)$. The expansions of F at Δ_1 and Δ_2 respectively begin with $y = 2\alpha\,(x-\alpha) + (4\alpha\, - 1)\,(x-\alpha)^2 + \cdots$ and $y = -2\alpha\,(x-\alpha) + (4\alpha\, + 1)\,(x-\alpha)^2 + \cdots$. We assign the zero point of this curve, P_0 to be $(1,1)$. Let P_1 and P_2 be the points $(-2,1)$ and $(3,-1)$ on the curve.

In this example, we add the two divisors $D_1 = 2{\cdot}\Delta_2$ plus $D_2 = 2{\cdot}P_1{+}2{\cdot}P_2$. Each of D_1 and D_2 has total degree 4, so their sum has degree 8, which we reduce to a divisor of degree 4. We compute expansions up to order 4 at P_0 and up to order 2 at P_1 and P_2.

We compute the space of functions $\mathcal{L}(D)$ for $D = D_1 + D_2 - 4\cdot P_0$. First we interpolate $b(x,y)$ of degree 4 such that $I_F(b) \geq D_1 + D_2 + \Delta_1 + \Delta_2 + 4\cdot P_0$. This relationship imposes 14 linear conditions ($14 = 4 + 4 + 1 + 1 + 4$) on the choice of $b(x,y)$ for which there are 15 degrees of freedom. This leaves one degree of freedom for b, and after making it primitive, b has 15 terms of degree 4 in x and y with coefficients of up to 13 digits.

According to Bezout's theorem, b meets F in $4\cdot 5 = 20$ places. The resultant $s(x)$ eliminating y of F with b has degree 20. After dividing this by the coordinate polynomials for $D_1, D_2, \Delta_1, \Delta_2, 4 \cdot P_0$, which have a product $s_1(x)$ of degree 16 corresponding to the 16 places they represent ($16 = 4+4+2+2+4$), we have an irreducible degree 4 polynomial $\bar{s}(x)$ for the x-coordinates of the divisor E', where the whole residual $E = E' + 4 \cdot P_0$. The polynomial $\bar{s}(x)$ has degree 4 in x with integer coefficients up to 66 digits. We adjoin a root γ of $\bar{s}(x)$ and take the gcd of $F(\gamma, y)$ with $b(\gamma, y)$ over $\mathbb{Q}(\gamma)$. The gcd is monic of degree 1 in y, degree 3 in x, with rational coefficients of up to degree about 130 in numerator and denominator.

Next we interpolate $r(x, y)$ of degree 4 such that $I_F(r) \geq E' + 8 \cdot P_0 + \Delta_1 + \Delta_2$. Again we start with 15 degrees of freedom for the choice of r, but this relationship imposes 14 linear conditions ($14 = 4 + 8 + 1 + 1$), leaving only one degree of freedom for r. This implies the dimension of $\mathcal{L}(D)$ is one. This $r(x, y)$ is degree 4 in both x and y, with 15 terms and integer coefficients of up to 34 digits.

We have again that r meets F in 20 places, so we take the resultant $s(x)$ of F with r, eliminating y, divide by the x-coordinate polynomial $s_1(x)$ for $E', 8 \cdot P_0, \Delta_1, \Delta_2$ of degree 16 ($16 = 8 + 4 + 2 + 2$) leaving $\bar{s}(x)$ of degree 4. This polynomial has degree 4 in x with integer coefficients up to 110 digits. We adjoin a root γ of $\bar{s}(x)$ and take the gcd of $F(\gamma, y)$ with $r(\gamma, y)$ over $\mathbb{Q}(\gamma)$. The gcd is monic of degree 1 in y, degree 3 in x, with rational coefficients of up to about 180 digits in numerator and denominator. This gcd and $\bar{s}(x)$ represent the reduced sum of the divisors.

The gcd calculations required 146 and 163 seconds respectively for the `evala(Gcd ...)` calculations in `Maple` running on a DECStation 5240. The `SACLIB` implementation of the gcd techniques previously mentioned [8] require less than a second for comparable computations.

Acknowledgements

I would like to acknowledge the support of the Austrian Science Foundation (Fonds zur Förderung der wissenschaftlichen Forschung) for this research through a Lise Meitner Postdoctoral Fellowship, project M–00153MAT

I would also like to thank Mark Encarnación, Gaétan Haché, Michal Mňuk, Paul Pedersen, and Josef Schicho for valuable discussions.

References

[1] Shreeram S. Abhyankar. *Algebraic Geometry for Scientists and Engineers*, volume 35 of *Mathematical Surveys and Monographs*. American Mathematical Society, 1990.

[2] D. Le Brigand and J.J. Risler. Algorithme de Brill-Noether et codes de Goppa. *Bulletin de la société mathématique de France*, 116:231–253, 1988.

[3] A. Brill and M. Noether. Über die algebraischen Functionen und ihre Anwendung in der Geometrie. *Mathematische Annalen*, 7:269–310, 1874.

[4] Antonio Campillo. *Algebroid Curves in Positive Characteristic*, volume 813 of *Lecture Notes in Mathematics*. Springer Verlag, 1980.

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

[6] Claude Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable*, volume 6 of *Mathematical Surveys*. American Mathematical Society, 1951.

[7] Dominique Duval. Rational puiseux expansions. *Compositio Mathematica*, 70:119–154, 1989.

[8] Mark J. Encarnación. Computing greatest common divisors of polynomials over algebraic number fields. To appear in the *Journal of Symbolic Computation*.

[9] Daniel Gorenstein. An arithmetic theory of adjoint plane curves. *Transactions of the AMS*, 72:414–436, 1952.

[10] Phillip A. Griffiths. *Introduction to Algebraic Curves*. American Mathematical Society, 1989.

[11] Gaétan Haché and Dominique Le Brigand. Effective construction of algebraic geometry codes. Technical Report 2267, INRIA-Rocquencourt, May 1994. available through ftp at `ftp.inria.fr`.

[12] Erich Hecke. *Vorlesungen über die Theorie der algebraischen Zahlen*. Akademische Verlagsgesellschaft, 1923. reprinted by Chelsea Publishing.

[13] Ming-Deh Huang and Doug Ierardi. Efficient algorithms for the Riemann-Roch problem and for addition in the Jacobian of a curve. In *IEEE 32nd Annual Symposium on Foundations of Computer Science*, pages 678–687, 1991.

[14] Ming-Deh Huang and Doug Ierardi. Efficient algorithms for the Riemann-Roch problem and for addition in the Jacobian of a curve. *Journal of Symbolic Computation*, 18(6):pp. 519–539, December 1994.

[15] Serge Lang. *Algebraic Number Theory*. Springer-Verlag, 1986.

[16] Max Noether. Rationale Ausführung der Operationen in der Theorie der algebraischen Functionen. *Mathematische Annalen*, Band 23:311–358, 1884.

[17] D. Polemi, M. Hassner, O. Moreno, and C. Williamson. A computer algebra algorithm for the adjoint divisor. In *Proceedings of the IEEE International Symposium on Information Theory*, page 358, 1993. San Antonio, Texas, USA.

[18] Despina Polemi. Computing the adjoint divisor over finite fields. obtained by email, contact `polemid@snyfarva.cc.farmingdale.edu`.

[19] Despina Polemi, Carlos J. Moreno, and Oscar J. Moreno. Search and construction of good a.g. codes. obtained by email, contact `polemid@snyfarva.cc.farmingdale.edu`.

[20] Marc Rybowicz. Calcul de parametrisation de courbes algebriques: Les developpements de Hamburger-Noether. Technical Report RR 798-M, TIM3/Institut national de polytechnique Grenobles, December 1989. obtained by email, contact `Marc.Rybowicz@unilim.fr`.

[21] J. Rafael Sendra and Franz Winkler. Symbolic parametrization of curves. *Journal of Symbolic Computation*, 12:607–631, 1991.

[22] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Universitext. Springer Verlag, 1993.

[23] Jeremy Teitelbaum. The computational complexity of the resolution of plane curve singularities. *Mathematics of Computation*, 54(190):797–837, 1990.

[24] Emil J. Volcheck. Noether's S-transformation simplifies curve singularities rationally: a local analysis. In G. Gonnet, editor, *Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation.* Association for Computing Machinery, 1993.

[25] Emil J. Volcheck. *Resolving Singularities and Computing in the Jacobian of a Plane Algebraic Curve.* PhD thesis, UCLA, 1994.