Computing in the Jacobian of a Plane Algebraic Curve

(extended abstract)

Emil J. Volcheck
volcheck@acm.org
UCLA Dept. of Mathematics and
Center for Science and Art

Abstract

We describe an algorithm which extends the classical method of adjoints due to Brill and Noether for carrying out the addition operation in the Jacobian variety (represented as the divisor class group) of a plane algebraic curve defined over an algebraic number field K with arbitrary singularities. By working with conjugate sets of Puiseux expansions, we prove this method is rational in the sense that the answers it produces are defined over K. Given a curve with only ordinary multiple points and allowing precomputation of singular places, the running time of addition using this algorithm is dominated by M^7 coefficient operations in a field extension of bounded degree, where M is the larger of the degree and the genus of the curve.

1 Introduction

Every algebraic curve defines an abelian variety called the *Jacobian variety* (or Jacobian) of the curve. For example, elliptic curves are isomorphic to their Jacobian varieties. The classical chord-tangent method "adds" points on elliptic curves and hence describes the group operation. Computing in the Jacobian of curves has applications to the integration of algebraic functions [16], primality testing [1], and error-correcting codes [10, 19].

Davenport implemented an algorithm to test for torsion points on the Jacobians of a broad class of algebraic curves [7]. An efficient algorithm for computing in the Jacobian of a hyperelliptic curve was developed by Cantor [4], who also derived closed-form expressions to calculate multiples of points in the Jacobian of a hyperelliptic curve [5]. M.-D. Huang and D. Ierardi developed the first polynomial-time algorithm for computing in the Jacobian of a curve [12].

We present an algorithm for computing in the Jacobian of an algebraic curve defined over an algebraic number field K with arbitrary singularities. The theoretical basis for this algorithm was first described by Brill and Noether [2, sec. 5]. Our algorithm builds on Noether's algorithm for computing the adjoints of a curve [15], but it differs in one significant respect: we represent singularities using analytic rather than algebraic means.

Like Noether's algorithm, our algorithm is *rational* in the sense that it expresses an answer without a ground field extension. Unlike Noether's algorithm, our algorithm requires ground field extensions for intermediate calculations involving singularities. However any object or function we compute whose field of coefficients extends to K', a proper extension of K, is manipulated as part of a conjugate set, one invariant under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$.

We first apply one or more of Noether's S-transformations to the curve to simplify its singularities into ordinary multiple points without extending the ground field (a technique which applies equally well to the Huang & Ierardi algorithm) [20]. Following precomputation of singular places, our algorithm adds points on the Jacobian in time dominated by M^7 coefficient operations in a field extension of bounded degree, where M is the larger of the degree n and the genus g of the curve.

In this extended abstract, we outline only a special case of the algorithm that allows arbitrary input but assumes sets of points produced as intermediate steps during the calculation satisfy certain generic conditions. These conditions do not impose any practically significant restrictions. We briefly indicate how the constructions for the general case can be made. Full details of the algorithm and its correctness may be found in [21].

2 Background

We adapt some basic definitions and results from Chevalley [6], [21], and chapter 4 of Walker [22]. See Eisenbud and Harris [9] for background on schemes and the spectrum of a ring.

For $F(x, y)$ defined over a number field K, let $C : F(x, y) = 0$ denote the corresponding curve as a K-scheme, that is

$$C = \operatorname{Spec} K[x, y]/F(x, y).$$

We assume C has only ordinary multiple points and that F is absolutely irreducible. Let $\bar{\mathbb{Q}}$ be the algebraic closure of K. Then

$$\bar{C} = \operatorname{Spec} \bar{\mathbb{Q}}[x, y]/F(x, y)$$

denotes the curve C with ground field extended to $\bar{\mathbb{Q}}$.

Definition: A *Puiseux expansion* of $\bar{C}$ centered at the point (x_0, y_0) is a fractional power series

$$y(x) = y_0 + a_1(x - x_0)^{n_1/n} + a_2(x - x_0)^{n_2/n} + \cdots,$$

for which $F(x,\, y(x)) = 0$. The n, n_i are integers such that $0 < n,\ 0 < n_1 < n_2 < \cdots$, and no a_i vanish.

Because we work with an explicit coordinate representation, we need to distinguish between the curve as an algebraic set and as a scheme.

Definition: We refer to a (geometric) *point* of $\bar{C}$ to denote a point of $\bar{C}$ as an algebraic set. We refer to a *place* of $\bar{C}$ (resp. C) in the sense of Chevalley, to denote a closed point of $\bar{C}$ (resp. C) as a scheme. To avoid ambiguity, we may refer to a *K-place* of C and to a *$\bar{\mathbb{Q}}$-place* of $\bar{C}$.

Since C has only ordinary multiple points we can explicitly characterize a singular K-place as having the following simplified form:

Theorem 1 *Given a singular K-place at an ordinary multiple point, it has an expansion in the standard form*

$$x = x_0 + t,\ y = y_0 + \sum a_i t^i,$$

where $K \subseteq K_1 \subseteq K_2$ are fields such that

1. $K_1 = K(x_0, y_0)$ *is the coefficient field of the center point of the expansion, and*

2. $K_2 = K_1(a_1, a_2, \dots)$ *is the residue field of the expansion, which is formed by adjoining a root of the leading form of* $F(x, y)$ *at the center* (x_0, y_0)*.*

Let L *be the Galois closure of* K_2 *over* K*. Then the action* $\mathrm{Gal}(L/K)$ *fixes this set of Puiseux expansions. Any such set of expansions corresponds to one or more* K*-places.*

See Duval [8] for related work on conjugate expansions. Note that a place at a nonsingular point will also have the above form, but with the a_i in K_1.

Definition: The center point P of a K-place Q corresponds to the set of center points of the corresponding conjugate $\bar{\mathbb{Q}}$-places. We say the *residue field* of P is the extension K_1, in the notation of the above theorem. The *degree* of P is $[K_1 : K]$. The *residue field* of a singular place Q centered at P is K_2. We say the *degree* of Q is $[K_2 : K]$.

Definition: Let a place Q have the Puiseux expansion $y(x)$. We write the *order* of a polynomial $g(x, y)$ at Q as $\mathrm{ord}_Q(g)$, i.e. the order of $g(x, y(x))$.

We give definitions that lead up to the construction of the divisor class group. We follow section 2.7 of Griffiths [11].

Definition: A *divisor* D of a curve is a formal sum of places of the curve, $D = \sum n_i Q_i$, where only finitely many n_i are non-zero. Let q_i denote the degree of the place Q_i. Then the *degree* of D is $\sum n_i q_i$.

We have defined C as an affine curve and only consider finite places. To avoid the cumbersome transition to a projective curve, let us agree that places on the line at infinity will be made finite by an appropriate coordinate transformation as needed.

Definition: We define the *intersection divisor* $I_F(g)$ of a polynomial $g(x, y)$ with the curve $C : F(x, y) = 0$ as the formal sum

$$I_F(g) = \sum_Q \mathrm{ord}_Q(g)\, Q,$$

where the sum ranges over all places Q of C.

Note that if $g(x, y)$ has degree m and $F(x, y)$ has degree n, then by Bezout's theorem, the intersection divisor will have degree mn.

Definition: The *principal divisor* of a rational function $g(x,y)/h(x,y)$ on the curve C, written $\mathrm{div}(g/h)$ is defined to be the difference of intersection divisors

$$\mathrm{div}(g/h) = I_F(g) - I_F(h).$$

The degree of a principal divisor is zero because both intersection divisors have the same degree. We may assume that g and h have the same degree when neither has a place at infinity.

Definition: The *divisor class group* is the quotient of the group of divisors of degree zero modulo the group of principal divisors. When two divisors D_1 and D_2 differ by a principal divisor, then they are *equivalent* in the divisor class group and we write $D_1 \equiv D_2$. An equivalence class in the divisor class group is a *divisor class*.

Definition: Given two divisors $D_1 = \sum n_P\, P$ and $D_2 = \sum m_P\, P$, we write $D_1 \geq D_2$ when $n_P \geq m_P$ for all P. When all $n_P \geq 0$, we write $D_1 \geq 0$ and say D_1 is *effective*. We add divisors by adding the multiplicities of their places, so we write $D_1 + D_2 = \sum (n_p + m_p)P$.

Definition: For a divisor D, we write $\mathcal{L}(D)$ to denote the vector space of functions

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

Definition: A polynomial $G(x,y)$ satisfies the *adjoint condition* at an ordinary multiple point of order m when G has a singularity of order $m-1$ there. When C has only ordinary multiple points, G defines an *adjoint curve* (or simply an *adjoint*) of C when G satisfies the adjoint condition at every ordinary multiple point.

We introduce the following divisor notation to describe adjoint conditions and adjoint curves on a curve C with only ordinary multiple points.

Definition: Consider all singular places of C and their center points, which are conjugate sets of points. We label them as follows: let $\{P_i\}_{i=1}^{s}$ denote the sets of center points, which are ordinary multiple points of order m_i. Say P_i has degree p_i as a conjugate set. Let $\{S_{ij}\}_{j=1}^{t_i}$ be the singular places centered at P_i. Let $\{\Delta_i\}_{i=1}^{s}$ be the divisors defined by

$$\Delta_i = \sum_{j=1}^{t_i} (m_i - 1) S_{ij}$$

and having degree δ_i. The divisor Δ_i represents the adjoint condition at P_i. Let Δ be defined as $\Delta = \sum_{i=1}^{s} \Delta_i$ with degree $\delta = \sum_{i=1}^{s} \delta_i$. We say Δ is the *adjoint divisor* because the condition $I_F(G) \geq \Delta$ implies that $G(x, y)$ satisfies the adjoint condition.

3 Algorithm

In this section, we describe addition and reduction in the Jacobian. For further properties of the Jacobian, see Griffiths [11, chap. 5].

Let C be an absolutely irreducible degree n, genus g curve defined over a number field K. We assume that C has no singular points on the line at infinity and that C has a K-rational point. We designate this point as the *zero point* of the Jacobian and write it as P_0.

If we add divisors by simply adding the multiplicities of their places, then repeated additions would produce ever larger divisors, with no limit to their size. The Riemann Inequality [11, p. 112] provides a way to represent divisors in a reduced form, so that we can follow each formal addition by a reduction operation. The Riemann Inequality also provides a way to test whether two divisors are equivalent [21].

Theorem 2 (Riemann) *Let D be a divisor of degree d on the curve C. Then*

$$\dim \mathcal{L}(D) \geq d - g + 1.$$

Consider divisors $D_1 - gP_0$ and $D_2 - gP_0$, where D_1 and D_2 are effective of degree g. Let $D_3 - 2gP_0$ be their formal sum as divisors, where D_3 is effective of degree $2g$. We perform the following reduction. Consider the divisor $D_3' = D_3 - gP_0$ of degree g, and choose a rational function $g/h \in \mathcal{L}(D_3')$. Let D_3^r be the degree g effective divisor $D_3' + \operatorname{div}(g/h)$. Then $D_3 \equiv D_3^r - gP_0$. Because D_3^r has only degree g, compared to degree $2g$ of D_3, we have a more compact representation of the sum.

3.1 Generic Assumptions

When computing $\mathcal{L}(D)$ for a fixed D and performing a reduction, we will construct a residual divisor E and a reduced divisor R, which will generically satisfy certain properties. Note that only finitely many points on C are

1. singularities,
2. points with the same x-coordinate as a singularity,
3. points with the same x-coordinate as a place of D, or
4. points on the line at infinity.

Assumption 1 *We assume that neither the residual divisor nor the reduced divisor shall contain any of these "bad" points.*

We refer to the above conditions as A1.1 through A1.4.

A divisor will generically consist of distinct points with simple multiplicity. If two points of a divisor share x-coordinates, then that represents an unusual vertical coincidence. Hence we make the following additional assumptions, which we label A2.1 and A2.2:

Assumption 2 *We assume that the residual divisor and the reduced divisor together have no vertical coincidences (A2.1). Further, each divisor shall have only simple points (A2.2).*

Any of the cases covered by these assumptions represents a subspace of strictly lower dimension (a Zariski closed set) in the space of divisors. Hence, these cases seldom occur in practice.

3.2 Data and Procedures

We describe the primary data structures and basic procedures for our addition algorithm.

We refer to a *parametrized conjugate set of points* to denote a set of points in the following parametrized form: $[r(t); \rho_1(t), \rho_2(t)]$. This represents the set of points $\{(\rho_1(\alpha), \rho_2(\alpha))\}$ for every root α of $r(t)$. For a place centered at a point of such a conjugate set, $r(t)$ generates the extension K_1 of Theorem 1.

A divisor can be represented as a list of quadruples, each quadruple containing an integer multiplicity, a parametrized conjugate set of points, a partial Puiseux expansion, and (for singular places) a factor of the leading form which generates the extension K_2 in the notation of Theorem 1.

We refer to the *coordinate polynomial* of a parametrized conjugate set of points to denote the polynomial whose roots are the x-coordinates of the individual geometric points with proper multiplicity. The coordinate polynomial of a place is the coordinate polynomial of its center point, and the coordinate polynomial of a divisor is the product (with proper multiplicity) of the coordinate polynomials for all its places.

We mention here but do not detail some basic procedures we need for the addition algorithm: calculating coordinate polynomials, calculating Puiseux expansions, evaluating a polynomial at a place, and interpolating a polynomial to vanish to a given positive multiplicity at a set of places on the curve. By modifying techniques of Sakkalis & Farouki [17] and Canny [3], we have an algorithm for representing an intersection divisor as a parametrized conjugate set of points. We refer to this operation as *parametrizing* the set of points and direct the reader to [21] for details.

3.3 Generic Algorithm

Given our generic assumptions, we now describe an algorithm `main` which will compute a reduction of a divisor down to g points.

Precomputation: [Singular places.] Compute coordinate polynomials for the singular points of C and for Δ and then parametrize the singularities. For each singular place Q with multiplicity δ_Q in the adjoint divisor Δ, compute the first δ_q terms of the Puiseux expansion at Q.

Input: the curve polynomial $F(x, y)$ of degree n; a (finite) divisor D of degree d greater than the genus g, written as a difference of two effective divisors $D^+ - D^-$ of degrees d^+ and d^-. Assume D^+ and D^- have no places in common.

Output: a basis for the functions of $\mathcal{L}(D)$ and a parametrized set of points representing an effective divisor of degree g equivalent to D.

Step 0: [Places of D.] For each place Q in D with multiplicity k, if Q is regular then compute the first k terms of the Puiseux expansion, else Q is singular and then compute an additional k terms of the expansion out to order $\delta_Q + k$. Compute the coordinate polynomials for D^+ and D^-.

Step 1: [Add the adjoint divisor to D^+, $A \leftarrow D^+ + \Delta$.] Iterate over all singular places Q, while adding the multiplicities of Q in D^+ and Δ and storing in A. Then add all regular places of D^+ to A.

Step 2: [Interpolate adjoints through D^+.] Construct a polynomial $b(x, y)$ of degree m with $I_F(b) \geq A$, where m is determined in section 4.1, by imposing linear conditions on a polynomial of undetermined coefficients and performing Gaussian elimination.

Step 3: [Subtract to find the residual divisor $E \leftarrow I_F(b) - A$.] Divide the coordinate polynomial for $I_F(b)$ by the coordinate polynomials for D^+ and Δ to get the coordinate polynomial $e(x)$ of the residual divisor E. We can parametrize E by computing the monic first subresultant $y - s(x)$ of $F(x, y)$ with $b(x, y)$, eliminating y, to obtain the parametrized conjugate set of points $[e(x); x, s(x)]$.

Step 4: [Add the adjoint divisor to D^- and E, $H \leftarrow D^- + E + \Delta$.] Iterate over all singular places Q, while adding the multiplicities of Q in D^- and Δ and storing in H. Then add the places of E and the regular places of D^- to H.

Step 5: [Interpolate adjoints through $E + D^-$.] Construct a basis of polynomials $r_i(x, y)$ of degree m such that $I_F(r_i) \geq H$, similar to Step 2. The rational functions r_i/b form a basis for $\mathcal{L}(D)$.

Step 6: [Reduce.] Choose some r from the space of the r_i. Similar to Step 3, subtraction occurs by dividing the coordinate polynomials of $I_F(r)$ by the coordinate polynomials for D^-, E, and Δ, and then parametrizing to get the reduced divisor R as a parametrized set.

3.4 Rationality

We compute in ground field extensions without explicit factorization through the technique of passive or lazy factorization [8, 13, 18]. This procedure ensures that when we introduce a Galois extension K' of the ground field K for an intermediate calculation, then we work with a set invariant under $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$.

Here is one particularly useful application of lazy factorization to computing with places and parametrized conjugate set of points. Suppose we wish to explicitly compute places with their multiplicities in an intersection divisor $I_F(g)$. Let the parametrized set $P = [p(t); \pi_1(t), \pi_2(t)]$ represent the points of $I_F(g)$. We compute terms of the Puiseux expansion at P. If $I_F(g)$ has points at which $g(x, y)$ has different orders, then calculating enough terms will produce a lazy factorization of $p(t)$. This enables us to rationally separate the places of different multiplicities in $I_F(g)$ and represent them as distinct parametrized sets.

Our algorithm is rational in the following sense:

Theorem 3 *Let $C : F(x, y) = 0$ be defined over a number field K, and let D be a divisor. Then all objects constructed during algorithm* `main` *are composed of either places or polynomials or functions defined over K on the curve.*

Proof: The theorem follows by inspection of the description of `main`. We analyze the algorithm step-by-step.

We apply lazy factorization as we calculate partial expansions at places in the precomputation step and step 0. In step 0, we calculate the coordinate polynomials by taking resultants over K.

Step 1 is a formal addition of divisors of K-places, so A is a divisor of K-places.

The interpolation of step 2 performs evaluations at K-places and solves a linear system over K. Hence, $b(x, y)$ has coefficients in K.

The parametrization in step 3 uses a subresultant chain, which is calculated over K.

Steps 4,5, and 6 are rational by analogy with steps 1,2, and 3. □

3.5 Modular Calculations

Our algorithm adapts well for calculating modulo a large prime. Consider C to be defined over $\mathbb{F}_p$. Assuming C has only ordinary multiple points, all places are unramified. Since the ground field is perfect, all extensions of K are separable. These observations show that the basic procedures and operations of section 3.2 are valid modulo p, except for parametrization, which requires p to be large relative to n [14, 21]. Although the generic conditions of section

3.1 refer to an infinite ground field, when p is a 32-bit prime the ground field is sufficiently large for parametrization to work and for the generic conditions to almost always hold. We do not address the question of bad reduction of the Jacobian modulo p.

4 Complexity

To determine the complexity of this algorithm, we first bound the size of certain intermediate divisors calculated during the course of the algorithm, then we analyze the time required to carry out the computations. We use the notation $f \prec g$ to denote that functions f and g satisfy $f \leq Cg$ for some constant C and say f is dominated by g. We write $f \sim g$ to indicate that f and g are codominant.

4.1 The Residual Divisor

Theorem 4 *Let D be a divisor given as a difference of two effective divisors, $D = D^+ - D^-$, where D^+ is of degree d^+, D^- of degree d^-, and D of degree $d > g$, as per the input to* `main`*. Since $d^+ > d^-$, let us use $d_{\max}$ to denote d^+, which is the largest degree of the positive and negative parts. Let the N specified in* `main` *be set equal to nR, where $R = \lceil d_{\max}/n \rceil$. Then the size e of the residual divisor E computed by the algorithm* `main` *is dominated by N.*

Let M be $\max(n, d_{\max})$. Note that $M \sim N$ because $2M \geq N \geq M$. We obtain a more natural bound on e by using N rather than M. First we have two lemmas.

Lemma 5 *The number of singular places δ falls short of n^2 by an amount dominated by N, that is, $n^2 - \delta \prec N$.*

Proof: By the genus formula

$$n^2 - 3n + 2 = 2g + \delta,$$

so putting $n^2 - \delta$ together, we have

$$n^2 - \delta = 3n + 2g - 2.$$

The right-hand side is less than $5M$ since $g < d_{\max}$, hence it is also less than $5N$, which proves the lemma.

Let us define $\alpha(N) = n^2 - \delta$, where the N of $\alpha(N)$ serves to remind us that $\alpha(N) \prec N$.

Lemma 6 *The degree m of the interpolating polynomial $b(x, y)$ need be no larger than $n + B$, where B is less than R.*

Proof: We must choose m large enough to satisfy

$$\binom{m+2}{2} - \binom{B+2}{2} \geq d^+ + \frac{1}{2}\delta.$$

Bound d^+ by $N = Rn$. Then multiply both sides of the equation by two, substitute $m = n + B$, and simplify the left-hand side:

$$n^2 + (2B+3)n \geq 2Rn + \delta.$$

Next, substitute $n^2 - \alpha(N)$ for δ:

$$n^2 + (2B+3)n \geq 2Rn + n^2 - \alpha(N).$$

The key step of this lemma is to cancel the n^2 terms from each side. We do so and then move the $2Rn$ term to the left-hand side.

$$(2B - 2R + 3)n + \alpha(N) \geq 0.$$

Since $\alpha(N) > 0$, this inequality is satisfied by the lowest value of B for which $2B - 2R + 3 \geq 0$. Solving for B, we have $B \geq R - 3/2$, or $B = R - 1$ since B is an integer. This proves the lemma.

Proof of Theorem: Again from the Riemann Inequality, we have

$$e = mn - d^+ - \delta,$$

so by neglecting d^+, which is positive, $e \leq mn - \delta$. Substituting $n + B$ for m, we have

$$mn - \delta = n^2 + Bn - \delta.$$

We rewrite $n^2 - \delta$ as $\alpha(N)$ to get $Bn + \alpha(N)$ on the right-hand side. Since $Bn < N$ and $\alpha(N) < 5N$, we have $e < 6N$, so $e \prec N$. $\square$

4.2 Operation Count

Now that we have some control over the size of the residual divisor, we count the coefficient operations of the main algorithm. We count each algebraic number calculation in extensions K_1 or K_2 (using the notation of Theorem 1) as one operation. Because our operation count neglects the size of integer coefficients and the degree of the intermediate ground field extensions, our estimate is best suited for modular calculations on curves with relatively few singularities (say $\delta \prec n$).

Theorem 7 *Allowing for precomputation of singular places, the time required for* `main` *is dominated by* N^6 *operations, where* $N = nR$ *and* $R = \lceil d_{\max}/n \rceil$.

Proof: We focus on the most expensive operations.

The interpolation in steps 2 and 5 is a Gaussian elimination which has a number of equations (linear conditions) dominated by N^2 and a number of unknowns dominated by N^2. The number of unknowns equals the number of undetermined coefficients of the interpolating polynomial of degree $m = n + R \prec N$. This gives complexity dominated by $(N^2)^2 N^2$ or N^6.

The most costly operation in the subtractions of steps 3 and 6 is parametrizing the residual divisor of size $\prec N$ points. The subresultant chain used for parametrization runs in time dominated by N^6 operations (see Loos [14]). □

4.3 Deterministic Complexity

We sketch techniques described in [21] to lift the generic assumptions.

Since singular points have an implicit representation using the partial derivatives of F, we may isolate any singular places in the residual or reduced divisors and handle them explicitly (A1.1).

In the case of any coordinate coincidences among D^+, D^-, Δ, E, or R, we may construct a coordinate transformation that eliminates these coincidences before parametrizing. This requires a resultant computation with complexity dominated by N^7. (A1.2, A1.3, A2.1).

Points at infinity can be made finite by a coordinate transformation (A1.4).

To detect multiple points in E or R, we compute sufficiently many terms of Puiseux expansions and then use lazy factorization as described in section 3.4 on rationality (A2.2).

This yields a deterministic complexity of addition of N^7, in contrast to the Huang & Ierardi algorithm which requires $n^{14}g^7$ [12].

Remark: The precomputation phase first requires parametrizing the singular points and then computing Puiseux expansions of each singular place. Let r equal the total number of (geometric) singular points. Parametrizing this set costs r^7 operations. Computing expansions at the singular places is dominated by n^8 operations [8, 21].

5 Example

In this section, we present an example of applying the generic algorithm `main` to adding divisors on a curve. 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 $D_1 = 2\cdot\Delta_1$ 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 $I_F(b) \geq D_1 + D_2 + \Delta_1 + \Delta_2$. This relationship imposes 10 linear conditions $(10 = 4+4+1+1)$ on the choice of $b(x, y)$ for which there are 15 degrees of freedom. This leaves 5 degrees of freedom to select $b(x, y)$. The b we choose has 15 terms with coefficients of up to 6 digits.

According to Bezout's theorem, b meets F in $4 \cdot 5 = 20$ places. The coordinate polynomials of $I_F(b)$ have degree 20. After dividing these coordinate polynomials by the coordinate polynomials for $D_1, D_2, \Delta_1, \Delta_2$, which have a product of degree 12 corresponding to the 12 places they represent ($12 = 4+4+2+2$), we have degree 8 coordinate polynomials for the residual divisor E.

We pass b and both these polynomials to the parametrization routine which returns the parametrization $[r(x); \rho_1(x), \rho_2(x)]$, where r has degree 8 and integer coefficients of up to 28 digits, and ρ_1 and ρ_2 have degree 7 and rational coefficients with numerator and denominator of up to 136 digits.

Next we interpolate $r(x, y)$ of degree 4 such that $I_F(r) \geq E + 4 \cdot P_0 + \Delta_1 + \Delta_2$. Again we start with 15 degrees of freedom for the choice of r, but this relationship imposes 14 linear conditions ($14 = 8 + 4 + 1 + 1$), leaving only one degree of freedom for r. That is, 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 25 digits.

We have again that r meets F in 20 places, so we divide the coordinate polynomials of $I_F(r)$ by the coordinate polynomials for $E, 4 \cdot P_0, \Delta_1, \Delta_2$ of degree 16 ($16 = 8 + 4 + 2 + 2$) leaving coordinate polynomials of degree 4. We pass r and these degree 4 coordinate polynomials to the parametrization routine which returns the parametrization $[s(x); \sigma_1(x), \sigma_2(x)]$, where $s(x)$ has degree 4 with integer coefficients of up to 102 digits, and σ_1 and σ_2 have degree 3 with rational coefficients of up to 182 digits in both numerator and denominator. This parametrized set of points represents the reduced sum of $D_1 + D_2$ in the divisor class group.

Acknowledgement

I would like to acknowledge the help of my advisor Prof. David Cantor and the support I received from the National Security Agency as a Graduate Student Researcher under grant NSA MDA 904-88-H2031 (Cantor-Hales).

References

[1] Leonard M. Adleman and Ming-Deh A. Huang. *Primality Testing and Abelian Varieties over Finite Fields*, volume 1512 of *Lecture Notes in Mathematics*. Springer Verlag, 1992.

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

[3] John Canny. Some algebraic and geometric computations in PSPACE. In *Proceedings of the ACM Symposium on the Theory of Computation*, pages 460–467, 1988.

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

[5] David G. Cantor. On the analogue of the division polynomials for hyperelliptic curves. To appear in *Journal für die reine und angewandte Mathematik*, 1994.

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

[7] James Harold Davenport. *On the Integration of Algebraic Functions*, volume 102 of *Lecture Notes in Computer Science*. Springer Verlag, 1981.

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

[9] David Eisenbud and Joe Harris. *Schemes: the Language of Modern Algebraic Geometry*. Wadsworth and Brooks/Cole, 1992.

[10] V. D. Goppa. *Geometry and Codes*, volume 24 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers, 1988.

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

[12] 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.

[13] Lars Langemyr. Algorithms for a multiple algebraic extension. In Teo Mora and Carlo Traverso, editors, *Methods in Algebraic Geometry, Proceedings of MEGA 1990*, pages 235–248. Birkhäuser, 1991.

[14] Rüdiger Loos. Computing in algebraic extensions. In B. Buchberger, G. E. Collins, and R. Loos, editors, *Computer Algebra: Symbolic and Algebraic Computation*. Springer Verlag, 1983.

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

[16] R. H. Risch. The problem of integration in finite terms. *Transactions of the AMS*, 139:167–189, 1969.

[17] Takkis Sakkalis and Rida Farouki. Singular points of algebraic curves. *Journal of Symbolic Computation*, 9:405–421, 1990.

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

[19] M. A. Tsfasman and S. G. Vladut. *Algebraic Geometric Codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers, 1991.

[20] 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.

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

[22] Robert J. Walker. *Algebraic Curves*. Springer-Verlag, 1978.