Short Programs for functions on Curves

Victor S. Miller
Exploratory Computer Science
IBM, Thomas J. Watson Research Center
Yorktown Heights, NY 10598

May 6, 1986

Abstract

The problem of deducing a function on an algebraic curve having a given divisor is important in the field of indefinite integration. Indeed, it is the main computational step in determining whether an algebraic function posseses an indefinite integral. It has also become important recently in the study of discrete elliptic logarithms in cryptography, and in the construction of the new class of error-correcting codes which exceed the Varshamov-Gilbert bound. It can also be used to give a partial answer to a question raised by Schoof in his paper on computing the exact number of points on an elliptic curve over a finite field.

Heretofore, the best known algorithm for calculating such functions was exponential in the size of the input. In this paper I give an algorithm which is linear in the size of the input (if arithmetic in the field under consideration takes constant time). For this algorithm it is necessary to represent the function as a straight-line program, for representation as a rational function may be exponential in the size of the input.

1 Introduction

I recall some standard terminology from the theory of algebraic curves. There are many good references for this theory, for example [Ful69]. It contains all results quoted here. For simplicity in presentation I only work with plane curves, even though all of the results work for more general curves.

Definition 1 *Projective n-space over a field K: denoted by $\mathbf{P}^n(K)$ is the set of equivalence classes $\{(a_0, \ldots, a_n) \neq 0 | a_i \epsilon K\}$ where two vectors are equivalent if they are non-zero scalar multiples of one another. The equivalence class contataining $(a_0, \cdots, a_n)$ is denoted by $(a_0 : \cdots : a_n)$. The projective line is $\mathbf{P}^1$, and the projective plane is $\mathbf{P}^2$.*

Definition 2 *A* plane (projective) algebraic curve *is the set of solutions to a homogeneous polynomial $f(X, Y, Z)$ considered as points in boldP^1. The curve is* non-singular *if the three partial derivatives of f never vanish simultaneously.*

Definition 3 *The* function field *of the curve, C, is the set of functions from the curve to the projective line, which are given by rational functions of the coordinates and is denoted by $k(C)$.*

Definition 4 *A (geometric)* point*, P on C is a solution to the set of defining equations.*

Definition 5 *At each point, P, of the curve one can define the :hp2order, $v_P(f)$, of the function f at P: it is $n > 0$ if the function has a zero of order n at P, and is $-n < 0$ if the function has a pole of order n at P ($1/f$ has a zero of order n).*

Definition 6 *A* divisor *on a curve, C as being a formal sum of points on the curve with integral coefficients: $\sum_P a_P(P)$, where only finitely many of the a_P are $\neq 0$. Divisors will normally be denoted by script letters such as $\mathcal{A}$ or $\mathcal{B}$.*

Definition 7 *The* degree *of a divisor is the sum of its coefficients:* $\deg \mathcal{A} = \sum_P a_P$.

A function f has only a finite number of zeroes and poles. Therefore we may define

Definition 8 *The divisor of a function $f \neq 0$, denoted by (f) is $\sum_P v_P(f)(P)$.*

It is also true that $\deg(f) = 0$. The set of divisors of degree 0 is denoted by D_0. A divisor of a function is also called *principal*.

Definition 9 *Linear equivalence. If $\mathcal{A}$ and $\mathcal{B}$ are divisors we write $\mathcal{A} \sim \mathcal{B}$ if there is a function f such that $\mathcal{A} = \mathcal{B} + (f)$. Principal divisors are also called* linearly equivalent to 0*. The set of all such is denoted by D_ℓ. The group D_0/D_ℓ is known as the* Picard group *of C and is denoted by* $\text{Pic}(C)$.

Definition 10 *Genus. The genus g of a curve C is an integer ≥ 0, which is a measure of the curve's complexity.*

It, for example, is the number of "donut-holes" in the Riemann-surface of the curve if we are working over the complex numbers. See [Ful69] for an exact definition. For our purposes, we only need to know that $g \leq (n-1)(n-2)/2$ where n is the degree of the polynomial defining the curve. A curve whose genus is 1 is usually called an *elliptic curve*.

Definition 11 *Linear system. The* linear system *of a divisor $\mathcal{A}$ is $L(\mathcal{A}) = \{0\} \cup \{f \epsilon k(C) | (f) + \mathcal{A} \geq 0\}$. It is easily seen that $L(\mathcal{A})$ is a vector space (in fact finite-dimensional). We denote $\ell(\mathcal{A}) = \dim L(\mathcal{A})$.*

Definition 12 *Support. The support* $\text{supp}\, \mathcal{A}$ *of a divisor $\mathcal{A}$ is the set $\{P | \mathcal{A}_P \neq 0\}$.*

2 The main algorithm

One of the fundamental problems in the theory of curves is to determine when a divisor of degree 0 is principal, and to construct a function whose divisor is the given divisor. In [Dav79]. Davenport gives an algorithm for this problem which does not always work for curves of genus > 1, and which is claimed to run in $\mathrm{O}(\lg A$ where A is the largest multiplicity of a zero or a pole at any point. This claim seems to be unjustified. The construction below gives a straight-line program instead of a ratio of two polynomials. This is in keeping with the spirit of [Kal85].

Algorithm 1 *Input:*

1. *An algebraic curve C of genus g*
2. *a fixed point Q on C*
3. *a divisor $\mathcal{A} = \sum_P a_P(P)$ of degree 0*

Output:

1. *A straight-line program for a function f on the curve*
2. *A divisor of the form $\mathcal{C} - g(Q)$ where $\deg \mathcal{C} = g$ and $\mathcal{C} \geq 0$.*

The divisor $\mathcal{C} - g(Q)$ will $= 0$ if and only if $\mathcal{A} \sim 0$. We will further have $\mathcal{A} = (f) + \mathcal{C} - g(Q)$. The length of this program is $\mathrm{O}(L)$ where $L = \sum_P \lg(|a_P| + 1)$ and the running time of the algorithm is $\mathrm{O}(L)$ arithmetic operations in the field of definition. The program gives the value **undefined** *on a set of points of size $\leq 2gL$.*

We use the following fundamental theorem:

Theorem 1 *The Riemann Theorem: Given a non-singular curve C, and a divisor $\mathcal{A}$, then*

$$\ell(\mathcal{A}) \geq \deg \mathcal{A} + 1 - g$$

with equality holding if $\deg \mathcal{A} > 2g - 2$.

Using the above we have

Lemma 1 *Any divisor $\mathcal{A}$ of degree 0 is equivalent to a divisor of the form $\mathcal{C} - g(Q)$, where $\deg \mathcal{C} = g$ and $\mathcal{C} \geq 0$.*

Proof: Using the Riemann Theorem we find that $\ell(\mathcal{A} + g(Q)) \geq 1$. Thus there is a function $f \neq 0$, $f \epsilon L(\mathcal{A} + g(Q))$. Now set $\mathcal{C} = (f) + \mathcal{A} + g(Q)$. It is readily seen that $\mathcal{C}$ has the desired properties. □

We use 1 to make calculations in the Picard Group, by representing each equivalence class by a divisor of the form $\mathcal{C} - g(Q)$. The fundamental point is that to calculate a representative for the sum of two such divisors takes $\mathrm{O}(g^3)$ field operations (basically the solution of a system of linear equations). We then write the divisor $\mathcal{A} = \sum_P a_P(P)$ as $\sum_P a_P((P) - (Q))$. We then can calculate a straight-line program of length $\leq 2\lg(|a_P| + 1)$ and a divisor $\mathcal{C} - g(Q)$ as above by means of the binary method of addition (or any other addition chain). The program will be undefined at most at all points of the supports of the divisors occuring in the intermediate steps. We then finish off by adding up all of the individual pieces, while multiplying the functions (this concatenates the straight-line programs with a multiplication in between).

In actual calculation one must proceed more explicitly: First calculate a basis for the space $L(3g(Q))$ in the form $f_1, \ldots, f_d$ where $\mathrm{ord}_Q(f_1) > \mathrm{ord}_Q(f_2) > \cdots > \mathrm{ord}_Q(f_d)$. When adding the two divisors $\mathcal{A} - g(Q)$ and $\mathcal{B} - g(Q)$ we first find $f \epsilon L(3g(Q) - \mathcal{A} - \mathcal{B})$. Define $\mathcal{C} = (f) + 3g(Q) - \mathcal{A} - \mathcal{B}$ then it is effective of degree g. Now find $h \epsilon L(2g(Q) - \mathcal{C})$, and set $\mathcal{D} = (h) + 2g(Q) - \mathcal{C}$. This divisor is also effective of degree g and $\mathcal{A} - g(Q) + \mathcal{B} - g(Q) = \mathcal{D} - g(Q) + (f/h)$. We further exploit the fact that there is a one-to-one correspondence between effective divisors and integral ideals of the ring of functions whose only poles are at Q. We represent each ideal by means of it Grobner Basis. In this way we avoid the necessity for root finding and factorization.

In the case of genus 1 we do not even need to do this. All zeroes and poles of intermediate divisors must be rational. If the curve is given in Weierstrass form $y^2 = x^3 + ax + b$ then $1, x, y$ form a basis of $L(3g(0))$. Finding the function f above amounts to finding the coefficients of the line $y = cx + d$ passing through the points $\mathcal{A}$ and $\mathcal{B}$.

3 Applications

In this section I discuss some applications of the above construction. The first is the calculation of the “Weil” e_N pairing.

Andre Weil [Wei46] introduced a pairing on points of finite order on elliptic curves in his first proof of the “Riemann Hypothesis” for curves over finite fields. Following are its definition and properties:

Definition 13 *Given an elliptic curve C and a non-negative integer N there is a unique function e_N defined on points of exponent N (P is of exponent N if $NP = 0$, it is of order N if N is an exponent and no smaller integer is). It has the following properties:*

1. *$e_N(P, Q)$ is an N-th root of unity.*
2. *Skew-symmetry: $e_N(P, Q) = e_N(Q, P) sup - 1$*
3. *Linearity: $e_N(P + R, Q) = e_N(P, Q) e_N(R, Q)$*
4. *Non-degeneracy: Given a point P of order N there is a point Q of order N such that $e_N(P, Q) \neq 1$.*

This pairing may be defined as follows (see [Lan73, pages 243–245]): If $\mathcal{A}$ is a divisor of order N in the divisor class group D_0/D_ℓ, then there is a function $f_\mathcal{A}$ such that $(f_\mathcal{A}) = N\mathcal{A}$. This function is defined up to multiplication by a constant. If f is any function, and $\mathcal{A} = \sum_P a_P(P)$ is a divisor of degree 0, then we define $f(\mathcal{A}) = \prod_P f(P)^{a_P}$. Note that this depends only on (f). If P and Q are points of exponent N, define f_P and f_Q as above. Then

$$e_N(P, Q) = f_\mathcal{A}(\mathcal{B})/f_\mathcal{B}(\mathcal{A})$$

where $\mathcal{A} \sim (P) - (0)$ and $\mathcal{B} \sim (Q) - (0)$ and whose support is disjoint. This is independent of the choice of $\mathcal{A}$ and $\mathcal{B}$. This yields:

Algorithm 2 *Calculation of e_N pairing Input:*

1. *An Elliptic Curve E*

2. *A natural number N*

3. *Two points P, Q on C of exponent N*

Output:

1. *The value $e_N(P, Q)$*

Method: First fix an addition chain $1 = a_1, \ldots, a_t = N$.

Now choose T, U points on C at random until T and $T + P$ are distinct from a_iU and $a_i(U + Q)$ and U and $U + Q$ are distinct from a_iT and $a_i(T + P)$ for all i. This choice guarantees that the straight-line programs constructed below are defined at input values used. Set $\mathcal{A} = (T + P) - (T)$ and $\mathcal{B} = (U + Q) - (Q)$. Use 1 to construct straight-line programs for the functions $f_\mathcal{A}$ and $f_\mathcal{B}$. Now the number of pairs (T, U) which do not satisfy the two conditions above is $\leq 8tN_p$ where N_p is the total number of points on the curve in $GF(p)$. Because there always is an addition chain with $t \leq 2 \lg N$ we see that when $N \geq 256$ that the probability of success is $gt1/2$. We then set

$$e_N(P, Q) = \frac{f_\mathcal{A}(U + Q) f_\mathcal{B}(T)}{f_\mathcal{B}(T + P) f_\mathcal{A}(U)}$$

If one is willing to work a little harder, a deterministic algorithm for the Weil pairing with the same running time as above may be obtained. The main idea is to modify the straight line program to give the value of the function at all points. The program will no longer be straight-line, but will be allowed to have "case" statements. One handles zeroes and poles by representing the value there by a pair (α, n) with the property that $\alpha \neq 0$ and that the Laurent series of the function at the point P starts with αu^n where u is a uniformizer at P. Such functions may be multiplied without any problems: one multiplies their α's and adds their n's. If one uses this representation it is possible to dispense with the usual restriction that the divisors $\mathcal{A}$ and $\mathcal{B}$ above have disjoint supports.

One application of the e_N pairing is to give a partial answer to a question raised by Schoof [Sch85]. In that paper, Schoof gives a determinstic algorithm, polynomial in $\lg p$ for calculating the exact order of the group of points on an elliptic curve $\bmod p$. He points out that he does not determine the structure of the underlying group. It is known that this group is always either cyclic, or the product of two cyclic groups of orders d and e where $d|e$. I give a random algorithm which runs in expected time polynomial in $\lg p$ if the factorization of $\gcd(p-1, N)$ is known, where N is the order computed by Schoof's algorithm.

Algorithm 3

1. *Calculate* $N_p = N_0 N_1$ *where* $\gcd(N_0, N_1) = 1$*, and the set of prime divisors of* N_0 *is the same as the set of prime divisors of* $\gcd(p-1, N_p)$*.*
2. *Using the Euclidean Algorithm find* α *and* β *such that* $\alpha N_0 + \beta N_1 = 1$*.*
3. *Pick two points* P', Q' *on the curve* C*, and set* $P = \beta N_1 P'$*,* $Q = \beta N_1 Q'$*.*
4. *Find the exact order of* P *and* Q *(this is where we need the factorization). Say they are* m *and* n*.*
5. *Set* $r = \mathrm{lcm}(m, n)$*.*
6. *Set* $a = e_r(P, Q)$
7. *Find the exact order of* a*. Say it's* s*.*
8. *If* $rs = N$ *then stop, the orders of the two groups are* r *and* s*.*
9. *If not go to step 3.*

The analysis of the algorithm depends on the non-degeneracy of e_N, and its skew-symmetry. The probability of failure in the last step is $\mathrm{O}(\lg\lg^{-1} p)$.

References

[Dav79] James H. Davenport. *On the Integration of Algebraic Functions*, volume 102 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, 1979.

[Ful69] William Fulton. *Algebraic Curves.* W. A. Benjamin, Inc., New York, 1969.

[Kal85] Erich Kaltofen. Computing with polynomials given by straight-line programs i; greatest common divisors. In *Proc. 17th ACM Symp. Theory Comp.*, pages 131–142. ACM Press, 1985.

[Lan73] Serge Lang. *Elliptic Functions.* Addison-Wesley, Reading, 1973.

[Sch85] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, pages 483–494, 1985.

[Wei46] Andre Weil. Sur les fonctions algebriques a corps de constantes fini. *C. R. Academie des Sciences*, 1946.