J. Symbolic Computation (2001) **32**, 171–189
doi:10.1006/jsco.2001.0470
Available online at http://www.idealibrary.com on IDEAL®

Counting Points on Curves and Abelian Varieties Over Finite Fields

LEONARD M. ADLEMAN AND MING-DEH HUANG

Department of Computer Science, University of Southern California, Los Angeles, CA 90089-0781, U.S.A.

We develop efficient methods for deterministic computations with semi-algebraic sets and apply them to the problem of counting points on curves and Abelian varieties over finite fields. For Abelian varieties of dimension g in projective N space over $\mathbf{F}_q$, we improve Pila's result and show that the problem can be solved in $O((\log q)^{\delta})$ time where δ is polynomial in g as well as in N. For hyperelliptic curves of genus g over $\mathbf{F}_q$ we show that the number of rational points on the curve and the number of rational points on its Jacobian can be computed in $(\log q)^{O(g^2 \log g)}$ time.

1. Introduction

In this paper we develop efficient methods for deterministic computations with semi-algebraic sets and apply them to the problem of counting points on curves and Abelian varieties over finite fields. The general computational tools developed in this paper are specifically designed to circumvent the need for either factoring polynomials or solving polynomial equations. They make it possible to solve the counting problem completely deterministically and efficiently. Throughout the paper, time complexity will be measured in the number of arithmetic operations in the ground field over which an algebraic computational problem is defined.

The problem of counting points on curves and Abelian varieties over finite fields has drawn considerable interest in recent years. Schoof (1985) gave a deterministic polynomial time algorithm for the case of elliptic curves, and also applied to solve, for a fixed integer a, $x^2 \equiv a \pmod{p}$ in deterministic polynomial time on input primes p. The primality testing algorithm of Adleman and Huang (1992) involves a random polynomial time algorithm for counting rational points on the Jacobians of curves of genus 2 over finite fields. Pila (1990) showed that for a fixed curve over the rationals, the numbers of rational points on the reduction of the curve and its Jacobian modulo a prime can be computed in deterministic polynomial time. The result is applied to solve, for fixed l, $\Phi_l(x) \equiv 0 \pmod{p}$ in deterministic polynomial time on input primes p, where Φ_l denotes the l-th cyclotomic polynomial. More generally, Pila (1990) showed that when a g-dimensional Abelian variety A over a finite field of q elements is explicitly given as an irreducible closed set in projective N-space, with identity and addition morphism. The number of rational points on A can be computed in $O((\log q)^{\Delta})$ time, where Δ is a polynomial in g but exponential in N. Huang and Ierardi (1993) developed a randomized algorithm which on input a plane projective curve of degree n without non-ordinary multiple points over

0747–7171/01/090171 + 19 $35.00/0

a finite field of q elements, computes the number of rational points on the curve and the number of rational points on its Jacobian in expected time $O((\log q)^{\delta})$ where $\delta = n^{O(1)}$. We refer to Poonen (1996) for a more comprehensive survey on computational aspects of curves of genus at least 2.

For general Abelian varieties in the projective setting, we improve on the result of Pila and show that given an Abelian variety of dimension g in projective N space over $\mathbf{F}_q$, the problem can be solved in $O((\log q)^{\delta})$ time where δ is polynomial in g as well as in N. For hyperelliptic curves over finite fields we demonstrate that by dispensing with projective descriptions altogether but relying instead on semi-algebraic descriptions for the objects involved, an even better result can be achieved. We show that given a hyperelliptic curve C of genus g over $\mathbf{F}_q$ presented by an affine model $y^2 = f$ where $f \in k[x]$ is of degree $2g + 1$ without multiple roots, the number of rational points on C and the number of rational points on its Jacobian can be computed in $(\log q)^{O(g^2 \log g)}$ time.

2. Notation on Semi-algebraic Sets and Maps

We adopt the following notation. Let k be a field and let $t \in \mathbf{Z}_{>0}$. Then $A(k, t)$ denotes the affine t-space over k, $P(k, t)$ denotes projective t-space over k. For $f \in k[x_1, \ldots, x_t]$, $\mathrm{dg}(f)$ =degree of f.

Let $t \in \mathbf{Z}_{>0}$. A *semi-algebraic set* of type t over k is a set $S \subset A(k, t)$ for which there exist two finite sets of polynomials $P, N \subset k[x_1, \ldots, x_t]$ such that

$$S = \{\alpha \in A(k, t) : f(\alpha) = 0 \text{ for all } f \in P, g(\alpha) \neq 0 \text{ for all } g \in N\}.$$

$\hat{S} = \langle k, t, P, N\rangle$ is called a *description* of S. We define

$$\mathrm{dg}(\hat{S}) = \max\{\mathrm{dg}(f) : f \in P \cup N\}$$
$$n(\hat{S}) = \max\{\#P, \#N\}.$$

Let $s, t \in \mathbf{Z}_{>0}$. A *primitive semi-algebraic map* of type $\langle s, t\rangle$ over k is a map ϕ from a semi-algebraic set $S \subset A(k, s)$ to $A(k, t)$ for which there exist $f_1, g_1, \ldots, f_t, g_t \in k[x_1, \ldots, x_s]$ such that for all $\alpha \in S$, $g_i(\alpha) \neq 0$ for $i = 1, \ldots, t$, and

$$\phi(\alpha) = \left\langle \frac{f_1(\alpha)}{g_1(\alpha)}, \ldots, \frac{f_t(\alpha)}{g_t(\alpha)} \right\rangle.$$

Let $\hat{S}$ be a description of S. Then the tuple $\hat{\phi} = \langle k, s, t, \hat{S}, f_1, g_1, \ldots, f_t, g_t\rangle$ is called a *description* of ϕ. We define

$$\mathrm{dg}(\hat{\phi}) = \max\{\mathrm{dg}(f_1), \mathrm{dg}(g_1), \ldots, \mathrm{dg}(f_t), \mathrm{dg}(g_t), \mathrm{dg}(\hat{S})\}$$
$$n(\hat{\phi}) = n(\hat{S}).$$

Let $s, t \in \mathbf{Z}_{>0}$. Let $\phi_1, \phi_2, \ldots, \phi_v$ be primitive semi-algebraic maps over k of type $\langle s, t\rangle$ and domains $S_1, S_2, \ldots, S_v$, respectively, which are mutually disjoint. Let $S = \cup_{i=1}^{v} S_i$ and let Φ denote the map from S to $A(k, t)$ such that for all $\alpha \in S$ if $\alpha \in S_i$ then

$$\Phi(\alpha) = \phi_i(\alpha).$$

Then Φ is called a *semi-algebraic map* over k of type $\langle s, t\rangle$ with domain S and primitive maps $\phi_1, \phi_2, \ldots, \phi_v$. Let $\hat{\phi}_i$ be a description of ϕ_i for $i = 1, \ldots, v$. Then the tuple $\hat{\phi} = \langle k, s, t, \hat{\phi}_1, \ldots, \hat{\phi}_v\rangle$ is called a *description* of Φ. We define

$$\mathrm{dg}(\hat{\Phi}) = \max\{\mathrm{dg}(\hat{\phi}_i) : 1 \leq i \leq v\}$$

$$n(\hat{\Phi}) = \max\{n(\hat{\phi}_i) : 1 \leq i \leq v\}$$
$$r(\hat{\Phi}) = v.$$

In the following example we make use of the relation between subresultants and the extended Euclidean scheme to derive semi-algebraic descriptions for polynomial division and polynomial GCD. The semi-algebraic map for division of a degree m polynomial by a degree n polynomial has n primitive maps, each of degree $O(m+n)$, with domain defined by one inequality and no more than n equalities. The semi-algebraic map for the extended Euclidean scheme of a pair of polynomials A and B of degree m and n has no more than 2^n primitive maps, each of degree $O(m^3)$, with domain defined by $O(n)$ equalities and inequalities. The whole semi-algebraic description can be constructed in $2^n m^{O(m)}$ time. This result will be used in subsequent discussion. We refer to Ierardi and Kozen (1991) for the theory needed in the example.

Example 2.1. (Polynomial Division and GCD) Let k be a field. Given a pair of polynomials $A, B \in k[x]$, the Euclidean algorithm computes the sequence of polynomials $r_0 = A$, $r_1 = B$, $r_2, \ldots, r_l$, $r_{l+1} = 0$ such that for $i = 2, \ldots, l$, r_i is the remainder in dividing r_{i-2} by r_{i-1}, and the last non-zero remainder r_l is the GCD of A and B. We call $r_0, \ldots, r_{l+1}$ the *polynomial remainder sequence (PRS)* of A and B. Let $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, and $t_1 = 1$. For $i = 2$ to $l+1$, let q_i be the quotient so that

$$r_i = r_{i-2} - q_i r_{i-1},$$

let s_i and t_i be defined recursively by

$$s_i = s_{i-2} - q_i s_{i-1}, \qquad t_i = t_{i-2} - q_i t_{i-1}.$$

Then for $i = 2$ to $l+1$

$$s_i A + t_i B = r_i.$$

The collection of polynomials r_i, q_i, s_i and t_i is called the *extended Euclidean scheme* of A and B. We also let $r'_i = r_i/\alpha_i$, $s'_i = s_i/\alpha_i$, and $t'_i = t_i/\alpha_i$, where α_i denotes the leading coefficient of r_i.

Fix the degrees m and n of A and B for now and assume $m \geq n$. Let $A = \sum_{i=0}^m a_i x^i$ and $B = \sum_{i=0}^n b_i x^i$. The resultant matrix $\Phi(A,B)$ of A and B is an $m+n$ by $m+n$ matrix formed as follows. Let a denote the $(m+n)$-vector $col(a_m, \ldots, a_0, 0, \ldots, 0)$. Let $c(a) = col(0, a_m, \ldots, a_0, 0, \ldots, 0)$ denote the cyclic shift of a, $c^2(a)$ the cyclic shift of $c(a)$, and so on. Similarly b denotes the $(m+n)$-vector $col(b_n, \ldots, b_0, 0, \ldots, 0)$, $c(b)$ the cyclic shift of b, and so on. Then

$$\Phi(A,B) = [a, c(a), \ldots, c^{n-1}(a), b, c(b), \ldots, c^{m-1}(b)].$$

For $d = 0, \ldots, n-1$, let $\Phi_d(A,B)$ be the $m+n-2d$ by $m+n-2d$ matrix obtained from $\Phi(A,B)$ by deleting the last d columns of coefficients of A, the last d columns of coefficients of B, and the last $2d$ rows. We call $\Phi_d(A,B)$ the d-th *subresultant matrix* of A and B, and its determinant $\phi_d(A,B)$ the d-th *subresultant* of A and B.

By Theorem 15.8 of Ierardi and Kozen (1991), $\phi_d(A,B) \neq 0$ if and only if $d = \mathrm{dg}(r_i)$ for some i, in which case the vector of coefficients of s'_i and t'_i forms the unique solution to $\Phi_d(A,B)X = col(0, \ldots, 0, 1)$. In particular the degree of the remainder r_2 in the division of $A = r_0$ by $B = r_1$ is d if and only if $\phi_d(A,B) \neq 0$ but $\phi_j(A,B) = 0$ for $j = d+1, \ldots, n-1$. In this case, the vector of coefficients of s'_2 and t'_2 forms the unique solution to $\Phi_d(A,B)X = col(0, \ldots, 1)$. This implies each coefficient α of s'_2 and t'_2 can be expressed as a quotient $q_\alpha(A,B)/\phi_d(A,B)$ where $q_\alpha(A,B)$ is a polynomial of degree no greater than $m+n$ in the coefficients of A and B. From $s_2 = 1$ and s'_2 the leading coefficient of r_2 can be determined, hence r_2, s_2, $t_2 = q_2$ can be determined. In this way we derive a semi-algebraic map for the division of a degree m polynomial by a degree n polynomial. The map has n primitive maps, corresponding to the n possible degrees for the remainder r_2. Each primitive map is of degree $O(m+n)$, with domain defined by one inequality and no more than n equalities.

Suppose $d_2 > d_3 > \cdots > d_l$ is the sequence of degrees corresponding to the non-zero polynomials in the PRS of A and B. Then $\phi_{d_i}(A,B) \neq 0$ for $i = 2,\ldots,l$, but $\phi_j(A,B) = 0$ for $j \neq d_2,\ldots,d_l$. In this case, s'_i, t'_i can be obtained by solving $\Phi_{d_i}(A,B)X = col(0,\ldots,0,1)$, hence each coefficient α of s'_i and t'_i can be expressed as a quotient $q_{i,\alpha}(A,B)/\phi_{d_i}(A,B)$ where $q_{i,\alpha}(A,B)$ is a polynomial of degree $O(m)$ in the coefficients of A and B. The same can be said of the coefficients of r'_i since $s'_iA+t'_iB = r'_i$. The leading coefficient α_i of r_i can be determined as follows (see Algorithm 15.1 of Ierardi and Kozen, 1991). Solving $\Phi_{d_i}(r'_{i-2}, r'_{i-1})X = col(0,\ldots,1)$ gives a constant b_i and a polynomial p_i such that $b_ir'_i = r'_{i-2} - p_ir'_{i-1}$. Then $\alpha_i = \alpha_0 b_2 b_4 \ldots b_i$ if i is even, and $\alpha_i = \alpha_1 b_3 b_5 \ldots b_i$ if i is odd. The constant b_i (and each coefficient of p_i) is expressed as the quotient of the form $q(r'_{i-2}, r'_{i-1})/\phi_{d_i}(r'_{i-2}, r'_{i-1})$ where $q(r'_{i-2}, r'_{i-1})$ is a polynomial of degree $O(m)$ in the coefficients of r'_{i-2} and r'_{i-1}, consequently s_i, t_i, r_i and q_i can be expressed rationally in the coefficients of A and B involving polynomials of degree $O(m^3)$. In this way we derive a semi-algebraic map for the extended Euclidean scheme of a pair of polynomials A and B of degree m and n. The map has no greater than 2^n primitive maps, each corresponding to a possible sequence of degrees of the non-zero polynomials in the PRS of A and B. Each primitive map is of degree $O(m^3)$ with a domain defined by $O(n)$ equalities and inequalities. The whole semi-algebraic description can be constructed in $2^n m^{O(m)}$ time.

3. Efficient Algorithms for Zero-dimensional Semi-algebraic Sets

In this section we develop efficient algorithms for counting the number of points in a zero-dimensional semi-algebraic set, and for constructing low-degree polynomial representation for the Frobenius endomorphism over a semi-algebraic set. The main results are stated in the following theorems.

Theorem 3.1. *There exists a deterministic algorithm and a $c \in \mathbf{Z}_{>0}$ which:*

(A) On input: a description $\langle k,t,P,N\rangle$ of a primitive zero-dimensional semi-algebraic set $S \subset A(k,t)$ over a field k with P, $N \subseteq k[x_1,\ldots,x_t]$,
(B) Outputs $|S|$,
(C) Halts within time $|P|^{O(t)}(d(|N|+1))^{O(t^2)}$ where $d = \max\{\mathrm{dg}(F) : F \in P \cup N\}$.

Let k be a finite field and $t \in \mathbf{Z}_{>0}$. Then $\phi(k,t)$ denotes the Frobenius map on $A(k,t)$.

Theorem 3.2. *There exists a deterministic algorithm and a $c \in \mathbf{Z}_{>0}$:*

(A) On input: a description $\langle k,t,P,N\rangle$ of a primitive zero-dimensional semi-algebraic set $S \subset A(k,t)$ over a finite field k of q elements with P, $N \subseteq k[x_1,\ldots,x_t]$, and an $e \in \mathbf{Z}_{>0}$,

(B) Outputs: g, $f_{i,1}, \ldots, f_{i,t} \in k'[x_1, \ldots, x_t]$, $i = 1, \ldots, e$, *where* k' *is an extension of* k, $\mathrm{dg}(g), \mathrm{dg}(f_{i,j}) \leq |S|(d'|N| + 1)$, *with* $d' = \max\{\mathrm{dg}(F) : F \in N\}$, *such that for all* $\alpha \in S$, $\phi^i(k,t)(\alpha) = \langle f_{i,1}(\alpha)/g(\alpha), \ldots, f_{i,t}(\alpha)/g(\alpha)\rangle$, *for* $i = 1, \ldots, e$,

(C) Halts within time $O(|P|^{ct}(d(|N|+1))^{ct^2} + et|S|^2 \log q)$ *where* $d = \max\{\mathrm{dg}(F) : F \in P \cup N\}$.

Remark. An extension k' is necessary only if the cardinality of k is less than $(t+1)|S|^2$.

3.1. preparatory results

Let k be a field and $n \in \mathbf{Z}_{>0}$. A *zero-dimensional cycle* Z of $P(k,n)$ is a formal sum $Z = \sum_{Q \in P(k,n)} n_Q Q$ where $n_Q \in \mathbf{Z}_{\geq 0}$ and $n_Q = 0$ for all but finitely many $Q \in P(k,n)$. Z is a simple cycle if n_Q is either zero or one for all points Q. The *support* of Z, denoted by supp(Z) is the set $\{Q \in P(k,n) : n_Q > 0\}$. The *Chow form* or *associated form* of Z is the polynomial

$$R(u_0, \ldots, u_n) = \prod_{Q=(x_0,\ldots,x_n) \in P(k,n)} (x_0 u_0 + \cdots + x_n u_n)^{n_Q},$$

for indeterminates $u_0, \ldots, u_n$. In defining the Chow form of a zero-dimensional cycle in $A(k,n)$, we identify $A(k,n)$ with the open neighborhood of $P(k,n)$ in which $x_0 \neq 0$.

Throughout "cycle" will mean zero-dimensional cycle. More general notions of Chow forms can be found in Chow (1950). A Chow form defined over a field k will be called a *k-rational Chow form.* It is known (Chow and van der Wareden, 1937; Chow, 1950) that a cycle is k-rational if and only if its Chow form is k-rational.

A Chow form can be used to produce a convenient parametrization of a zero-dimensional algebraic set, as shown in the following lemma which is adapted from Canny (1988).

Lemma 3.1. *Let* k *be a field,* $n \in \mathbf{Z}_{>0}$, *and* $R(u_0, \ldots, u_n)$, *the Chow form of a* k*-rational zero-dimensional cycle* $Z = \sum_Q n_Q Q$ *with* $Q \in A(k,n)$ *such that the points in supp(Z) have distinct first coordinates. Suppose* $\#k > |supp(Z)|^3$. *Then there exist polynomials* $R_1, \ldots, R_n \in k[x]$, *all of degree bounded by* $|supp(Z)|$, *such that* $supp(Z) = \{(\theta, R_2(\theta), \ldots, R_n(\theta)) : R_1(\theta) = 0\}$. *Moreover* $R_1, \ldots, R_n$ *can be constructed in time* $\mathrm{dg}(R)^{O(n)}$.

Proof. Let $S = supp(Z)$. Since

$$R(u_0, \ldots, u_n) = \prod_{Q=(\alpha_1,\ldots,\alpha_n) \in S} (u_0 + \alpha_1 u_1 + \cdots + \alpha_n u_n)^{n_Q}$$

and the points in S have distinct first coordinates, it follows that

$$R(t, -1, 0, \ldots, 0) = \prod_{Q=(\alpha_1,\ldots,\alpha_n) \in S} (t - \alpha_1)^{n_Q}.$$

Hence $R_1(t)$ is the square-free part of $R(t, -1, 0, \ldots, 0)$.

Next we construct $R_2(t)$, and the other R_is can be constructed similarly.

For $a \in k$, let

$$F_a(t) = R(t, -a, -1, 0, \ldots, 0) = \prod_{Q=(\alpha_1,\ldots,\alpha_n) \in S} (t - a\alpha_1 - \alpha_2)^{n_Q}$$

and let $F(t)$ be the square-free part of

$$R(t,-1,1,0,\dots,0) = \prod_{Q=(\alpha_1,\dots,\alpha_n)\in S} (t-\alpha_1+\alpha_2)^{n_Q}.$$

Let

$$H_a(x,t) = F((a+1)x-t).$$

Then for $P=(\beta_1,\dots,\beta_n)\in S$, both $F_a(t)$ and $H_a(\beta_1,t)$ have $a\beta_1+\beta_2-t$ as a factor. We would like to choose an a such that for all $P=(\beta_1,\dots,\beta_n)\in S$ the GCD of $F_a(t)$ and $H_a(\beta_1,t)$ is $a\beta_1+\beta_2-t$. This will be true if for all $P=(\beta_1,\dots,\beta_n)$, $Q=(\alpha_1,\dots,\alpha_n)$, $R=(\gamma_1,\dots,\gamma_n)$ in S with $\alpha_2-\alpha_1\neq\beta_2-\beta_1$,

$$(a+1)\beta_1-\alpha_1+\alpha_2\neq a\gamma_1+\gamma_2.$$

For each choice of P,Q,R, all but one choice of a will work. So in $|S|^3$ many choices of as, at least one will work. To verify if a choice a works, we compute the first subresultant polynomial $G(x)$ of $H_a(x,t)$ and $F_a(t)$ with respect to the variable t, and check if the GCD of R_1 and G is 1. To justify this checking procedure we observe that for all $P=(\beta_1,\dots,\beta_n)\in S$, $G(\beta_1)$ is the first subresultant of $H_a(\beta_1,t)$ and $F_a(t)$. Since $H_a(\beta_1,t)$ and $F_a(t)$ have $a\beta_1+\beta_2-t$ as a common factor, it follows (see Theorem 15.8 of Ierardi and Kozen, 1991) that $G(\beta_1)\neq 0$ iff $H_a(\beta_1,t)$ and $F_a(t)$ have $a\beta_1+\beta_2-t$ as GCD. Recall that the polynomial R_1 has the first coordinates of all points of S as its roots. Hence a is good iff the GCD of R_1 and G is 1.

Assuming a good a is found, let A be the first subresultant matrix for $H_a(x,t)$ and $F_a(t)$ with respect to t. From Theorem 15.8 of Ierardi and Kozen (1991) it follows that by solving $AX=col(0,\dots,0,1)$ one gets the coefficients of some $h,f\in k[x][t]$ and $d\in k[x]$ such that $hH_a+fF_a=Gt-d$. For all $P=(\beta_1,\dots,\beta_n)\in S$,

$$h(\beta_1)H_a(\beta_1,t)+f(\beta_1)F_a(\beta_1,t)=G(\beta_1)t-d(\beta_1).$$

But since the GCD of $H_a(\beta_1,t)$ and $F_a(\beta_1,t)$ is $t-a\beta_1-\beta_2$, it follows that

$$c(t-a\beta_1-\beta_2)=G(\beta_1)t-d(\beta_1)$$

for some constant c. So

$$\beta_2=\frac{d(\beta_1)}{G(\beta_1)}-a\beta_1.$$

Since a is good and the GCD of G and R_1 is 1, there exist $b,Q\in k[t]$ such that

$$bG+QR_1=1.$$

So for all $P=(\beta_1,\dots,\beta_n)\in S$,

$$b(\beta_1)G(\beta_1)=1-R_1(\beta_1)Q(\beta_1)=1.$$

So

$$\beta_2=\frac{d(\beta_1)}{G(\beta_1)}-a\beta_1=d(\beta_1)b(\beta_1)-a\beta_1.$$

Hence we can set

$$R_2(t)=d(t)b(t)-at \bmod R_1(t).$$

The GCD and subresultant computation necessary can be done in a time polynomial in $\mathrm{dg}(R)$. The polynomials F_a and H_a can be constructed in $\mathrm{dg}(R)^{O(n)}$ time. The asserted bound on the complexity follows. □

Lemma 3.2. *Let k be a field and T be a finite set of $A(k,n)$. For all $a \in \bar{k}$, let L_a denote the affine linear map of $A(k,n)$ such that*

$$L_a(x_1, \ldots, x_n) = \left(\sum_{i=1}^{n} a^i x_i, x_2, \ldots, x_n \right).$$

Then in any set of $n|T|^2$ many elements of $\bar{k}$, there is at least one element a such that the first coordinates of the points in $L_a(T)$ are all distinct. Moreover given the Chow form R of a cycle Z with support T, such an a as well as the Chow form R_a of the cycle $L_a(Z)$ can be constructed in $\mathrm{dg}(R)^{O(n)}$ time.

Proof. For all distinct $\alpha, \beta \in T$, let $F_{\alpha,\beta}(x) = \sum_{j=1}^{n} (\alpha_j - \beta_j) x^j$. Then $L_a(\alpha)$ and $L_a(\beta)$ have the same first coordinate iff $F_{\alpha,\beta}(a) = 0$. As $F_{\alpha,\beta}$ has at most n roots, it follows that in any set of $n|T|^2$ many elements of $\bar{k}$, there is at least one element a such that the first coordinates of the points in $L_a(T)$ are all distinct.

Suppose $R(u_0, \ldots, u_n)$ is the Chow form of a cycle Z with support T, then the Chow form of the cycle $L_a(Z)$ is $R_a(u_0, \ldots, u_n) = R(z_0, \ldots, z_n)$ where $z_i = u_i + a^i u_1$ for $i \neq 1$ and $z_1 = a u_1$.

Construct an extension k' of k if necessary so that $\#k' \geq n\mathrm{dg}(R)^{2n} \geq n|T|^2$ and form a subset $A \subset k'$ of cardinality $n\mathrm{dg}(R)^{2n}$. (This can be done in $O(n\mathrm{dg}(R)^{2n})$ time.) For all $a \in A$, let $F_a(x) = R_a(x, -1, 0, \ldots, 0)$. Since the first coordinates of the points in $L_a(T)$ are all the roots of F_a, a correct choice of a in A is one whose corresponding F_a has maximum degree in its square-free part. Each F_a is formed in $O(\mathrm{dg}(R)^n)$ time. The result follows. □

Lemma 3.3. *Given the Chow form R of a k-rational cycle Z with support $T \subset A(k,n)$, and a polynomial $f \in k[x_1, \ldots, x_n]$, it can be checked in $\mathrm{dg}(R)^{O(n)} + \mathrm{dg}(f)^{O(n)}$ time whether $T \subset V(f)$.*

Proof. First apply Lemma 3.2 to find an $a \in \bar{k}$ such that the first coordinates of $L_a(T)$ are distinct, and construct the Chow form R_a for $L_a(T)$. Then apply Lemma 3.1 to R_a to construct univariate polynomials $R_1, \ldots, R_n$ such that $L_a(T) = \{(\alpha, R_2(\alpha), \ldots, R_n(\alpha)) : R_1(\alpha) = 0\}$. Now $T \subset V(f)$ iff $L_a(T) \subset L_a(V(f))$ iff $f_a(x, R_2(x), \ldots, R_n(x)) \equiv 0 \pmod{R_1(x)}$ where $f_a = f \circ L_a^{-1}$. The result follows. □

To construct a Chow form for a cycle defined by a set of polynomials, we will need the following result.

Lemma 3.4. *Let k be a field, $n \in \mathbf{Z}_{>0}$, and $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ with $d = \max\{\mathrm{dg} f_i : i = 1, \ldots, n\}$. Then there exists a deterministic algorithm which in $d^{O(n^2)}$ time constructs the k-rational Chow form of a zero-dimensional affine simple cycle Z such that:*

(1) supp(Z) includes all the isolated points in $V(f_1, \ldots, f_n)$,
(2) if $V(f_1, \ldots, f_n)$ is finite, then supp$(Z) = V(f_1, \ldots, f_n)$.

Proof. For $i = 1$ to n, let $F_i = x_0^{d_i} f(x_1/x_0, \ldots, x_n/x_n)$ be the homogenized f_i where $d_i = \mathrm{dg}(f_i)$, and let $G_i = t x_i^{d_i} + F_i$. Form the multivariate resultant $\hat{R}(u_0, \ldots, u_n, t)$ of $G_1, \ldots, G_n$ and $L = u_0 x_0 + \cdots + u_n x_n$ with respect to $x_0, \ldots, x_n$, and let $R(u_0, \ldots, u_n)$

be the least non-zero coefficient of $\hat{R}$ when written as a polynomial in t. Then by Ierardi (1989b) (see also Ierardi and Kozen, 1991 and the thesis of Ierardi, 1989a) $R(u_0, \ldots, u_n)$ is the Chow form of a cycle Z' where *supp*(Z') is a subset of $V(F_1, \ldots, F_n)$ and contains all the isolated points of $V(F_1, \ldots, F_n)$. Moreover R can be computed in $d^{O(n^2)}$ time. Note that when $V(f_1, \ldots, f_n)$ is finite, the affine part of *supp*(Z'), *supp*$(Z') \cap A(k, n)$, is exactly $V(f_1, \ldots, f_n)$. So it is sufficient to construct the Chow form $R_1(u_0, \ldots, u_n)$ of the simple affine cycle Z whose support is *supp*$(Z') \cap A(k, n)$. The Chow form $R_1(u_0, \ldots, u_n)$ of Z can be obtained from R as follows. Write $R(u_0, \ldots, u_n) = \sum_i r_i(u_1, \ldots, u_n) u_0^i$ and extract the GCD $r(u_1, \ldots, u_n)$ of the coefficient polynomials $r_i(u_1, \ldots, u_n)$. Then $F = R/r$ is the Chow form of a cycle Z_1 whose support is *supp*$(Z') \cap A(k, n)$, and R_1 is the square-free part of F which can be obtained as $R_1 = F/GCD(F, F')$, where F' is the partial derivative of F with respect to u_0. The result follows. □

Lemma 3.5. *Let k be a field and $n, m \in \mathbf{Z}_{>0}$. Let $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ with $d = \max\{\mathrm{dg} f_i : i = 1, \ldots, m\}$. Suppose $V(f_1, \ldots, f_m)$ is finite. Then $|V(f_1, \ldots, f_m)| \le d^n$. Moreover there exists a deterministic algorithm which constructs the k-rational Chow form of the simple cycle with support $V(f_1, \ldots, f_m)$ in $m^{O(n)} d^{O(n^2)}$ time.*

Proof. Without loss of generality assume that $f_1, \ldots, f_m$ are non-zero polynomials. Let $g_1 = f_1$. Inductively suppose $a_2, \ldots, a_j \in \bar{k}$ such that every component of $V(g_1, \ldots, g_j)$ is of co-dimension j in $A(k, n)$, where

$$g_i = \sum_{k=1}^{m} a_i^{k-1} f_k$$

for $i = 1, \ldots, j$.

The sum of degree of the components in $V(g_1, \ldots, g_j)$ is bounded by $\mathrm{dg}(g_1) \ldots \mathrm{dg}(g_j) \le d^j$. (This follows inductively from Theorem 7.7, Chapter I of Hartshorne (1977). See also Lemma 2.20 of Ierardi (1989b).) In particular, the number of components in $V(g_1, \ldots, g_j)$ is bounded by d^j.

Fix for each component Z of $V(g_1, \ldots, g_j)$ such that Z is not contained in $V(f_1, \ldots, f_m)$ a point in $Z - V(f_1, \ldots, f_m)$. Let S_j be the set of all such points. For all $\alpha \in S_j$, let

$$h_\alpha(t) = \sum_{k=1}^{m} f_i(\alpha) t^{k-1}.$$

As there are no more than d^j components of $V(g_1, \ldots, g_j)$, the number of roots of $h = \prod_{\alpha \in S_j} h_\alpha$ is bounded by $(m-1)d^j$. Consequently, in any subset T_j of $\bar{k}$ of cardinality greater than $(m-1)d^j$, there is at least one element a_{j+1} such that $h(a_{j+1}) \ne 0$, hence $h_\alpha(a_{j+1}) \ne 0$ for all $\alpha \in S_j$. Let

$$g_{j+1} = \sum_{k=1}^{m} a_{j+1}^{k-1} f_k.$$

Then $g_{j+1}(\alpha) \ne 0$ for all $\alpha \in S_j$. Consequently the intersection of $V(g_{j+1})$ with any component Z of $V(g_1, \ldots, g_j)$ is either empty or of co-dimension one in Z. It follows that every component of $V(g_1, \ldots, g_{j+1})$ is of co-dimension $j+1$ in $A(k, n)$. By induction, $V(g_1, \ldots, g_n)$ is zero-dimensional with cardinality bounded by d^n. Since $V(f_1, \ldots, f_m) \subset V(g_1, \ldots, g_n)$, $V(f_1, \ldots, f_m) \le d^n$.

Let $S = V(g_1, \ldots, g_n) - V(f_1, \ldots, f_m)$. Then hence $\#(S \cup S_{n-1}) \leq d^n + d^{n-1}$. So a similar argument as before shows that in any subset T'_n of $\bar{k}$ of cardinality greater than $2(m-1)d^n$, there is at least one element b such that

$$\sum_{k=1}^{m} b^{k-1} f_k(\alpha) \neq 0$$

for all $\alpha \in S \cup S_{n-1}$. Let

$$g'_n = \sum_{k=1}^{m} b^{k-1} f_k.$$

Then $V(g_1, \ldots, g_{n-1}, g'_n)$ is zero-dimensional and since $g'_n(\alpha) \neq 0$ for all $\alpha \in S$,

$$V(g_1, \ldots, g_n) \cap V(g_1, \ldots, g_{n-1}, g'_n) = V(f_1, \ldots, f_m).$$

We now explain how such a sequence $a_2, \ldots, a_n$, and b can be found. Construct an extension k' of k if necessary so that k' has more than $2(m-1)d^n$ elements. (This can be done in $O(md^n)$ time.) Form subsets $T_1, \ldots, T_n, T'_n$ of k' so that $\#T_j > (m-1)d^j$ for $j = 1, \ldots, n$ and $\#T'_n > 2(m-1)d^n$. From the above discussion we see that there exist $a_1 \in T_1, \ldots, a_n \in T_n$, $b \in T'_n$ such that the corresponding $g_1, \ldots, g_n, g'_n$ satisfy $V(g_1, \ldots, g_n) \cap V(g_1, \ldots, g_{n-1}, g'_n) = V(f_1, \ldots, f_m)$. So for every choice $\alpha = (a_1, \ldots, a_n, b)$, construct the corresponding $g_1, \ldots, g_n, g'_n$. Apply the algorithm in Lemma 3.4 to $g_1, \ldots, g_n$ to construct the Chow form of the simple cycle associated with $V(g_1, \ldots, g_n)$, and similarly construct the Chow form of the simple cycle associated with $V(g_1, \ldots, g_{n-1}, g'_n)$. Then take the GCD of the two Chow forms. The resulting polynomial R_α is the Chow form of a simple affine cycle Z_α. We regard α as potentially good only if $supp(Z_\alpha) \subset V(f_1, \ldots, f_m)$. By Lemma 3.3 this can be checked in $md^{O(n)}$ time. Among the potentially good α, a good choice is one such that R_α has maximum degree. Such a good R_α is the Chow form of the simple cycle with support $V(f_1, \ldots, f_m)$ and is k-rational since the cycle it represents is k-rational. Each g_k involved can be computed in $O(md^n)$ time and there are altogether $m^{O(n)}d^{O(n^2)}$ such polynomials. There are $m^{O(n)}d^{O(n^2)}$ many applications of the algorithm in Lemma 3.4, each to a system of n polynomials of degree bounded by d. The total time complexity is $m^{O(n)}d^{O(n^2)}$. □

3.2. PROOFS OF THE MAIN THEOREMS

PROOF OF THEOREM 3.1. Let $S = S(k, t, P, N)$. Let $N = \{G_1, \ldots, G_m\}$ where $G_i \in k[x_1, \ldots, x_t]$ for $i = 1, \ldots, m$. Let $G = \prod_{i=1}^{m} G_i$. Let $H \in k[x_1, \ldots, x_t, z]$ be such that

$$H(x_1, \ldots, x_t, z) = zG(x_1, \ldots, x_t) - 1.$$

Let T be the set of zeros of the polynomials in P and H where the polynomials are considered to be in $k[x_1, \ldots, x_t, z]$. Then there is a one to one correspondence between S and T sending a point $(\alpha_1, \ldots, \alpha_t) \in S$ to a point $(\alpha_1, \ldots, \alpha_t, \beta) \in T$ where $\beta^{-1} = G(\alpha_1, \ldots, \alpha_t)$.

By Lemma 3.5, the Chow form $R(u_0, \ldots, u_{t+1})$ of the simple cycle Z with support T can be computed in $|P|^{O(t)}(d(|N|+1))^{O(t^2)}$ steps. The degree of R in u_0 is exactly $|T|$. □

PROOF OF THEOREM 3.2. We proceed with the Chow form R constructed in the proof of Theorem 3.1.

Let $n = t+1$, and $Z = \sum_{Q \in T} Q$. Apply Lemma 3.2 to find an $a \in \bar{k}$ such that the first coordinates of points in $L_a(Z)$ are distinct, and construct the Chow form R_a for $L_a(Z)$. This takes $\mathrm{dg}(R)^{O(n)}$ time.

Let $L = L_a$ and $R_L = R_a$. Then for $x = (x_1, \ldots, x_n) \in A(k,n)$, $L(x) = (\lambda(x), x_2, \ldots, x_n)$ where $\lambda(x) = \sum_{i=1}^n a^i x_i$, and $L^{-1}(x) = (\mu(x), x_2, \ldots, x_n)$ where $\mu(x) = a^{-1}x_1 + \sum_{i=2}^n a^{i-1} x_i$.

Apply Lemma 3.1 to R_L to compute polynomials R_i, $i = 1, \ldots, n$, all of degree bounded by $|T|$ such that $L(T) = \{(\theta, R_2(\theta), \ldots, R_n(\theta) : R_1(\theta) = 0\}$. This can be done in $\mathrm{dg}(R_L)^{O(t)} = |T|^{O(t)}$ steps.

Let $\phi = \phi(k, t+1)$. Let $\phi_L = L\phi L^{-1}$. For $x = (x_1, \ldots, x_n) \in L(T)$, $R_1(x_1) = 0$, $x_i = R_i(x_1)$ for $i = 2, \ldots, n$. So

$$\begin{aligned}\phi_L^i(x) &= L(\mu^{q^i}(x), x_2^{q^i}, \ldots, x_n^{q^i}) \\ &= L(r^{q^i}(x_1), R_2^{q^i}(x_1), \ldots, R_n^{q^i}(x_1))\end{aligned}$$

where $r(x_1) = \mu(x_1, R_2(x_1), \ldots, R_n(x_1))$. Let

$$\begin{aligned}G_{i,1} &= r^{q^i}(x_1) \bmod R_1(x_1) \\ F_{i,j} &= R_j^{q^i}(x_1) \bmod R_1(x_1), \qquad j = 2, \ldots, n.\end{aligned}$$

Each of these polynomials can be obtained by repeated squaring modulo $R_1(x_1)$ in $O(e \log q)$ multiplications and divisions of univariate polynomials of degree bounded by $|T|$. Then for $x = (x_1, \ldots, x_n) \in L(T)$,

$$\begin{aligned}\phi_L^i(x) &= L(G_{i,1}(x_1), F_{i,2}(x_1), \ldots, F_{i,n}(x_1)) \\ &= (F_{i,1}(x_1), F_{i,2}(x_1), \ldots, F_{i,n}(x_1))\end{aligned}$$

where $F_{i,1}(x_1) = \lambda(G_{i,1}(x_1), F_{i,2}(x_1), \ldots, F_{i,n}(x_1))$, and the $F_{i,j}$ are of degree bounded by $|T| = |S|$.

For $x = (x_1, \ldots, x_t) \in T$,

$$\begin{aligned}\phi^i(x) &= L^{-1}\phi_L^i L(x) = L^{-1}\phi_L^i(\lambda(x), x_2, \ldots, x_n) \\ &= L^{-1}(F_{i,1}(\lambda(x)), \ldots, F_{i,n}(\lambda(x))) \\ &= (F'_{i,1}(x), \ldots, F'_{i,n}(x))\end{aligned}$$

where $F'_{i,1}(x) = \mu((F_{i,1}(\lambda(x)), \ldots, F_{i,n}(\lambda(x)))$, $F'_{i,j}(x) = F_{i,j}(\lambda(x))$ for $j = 2, \ldots, n$. The $F'_{i,j}$ are all of degree bounded by $|T|$.

Finally, a point $y = (y_1, \ldots, y_t) \in S$ corresponds to $(y, z) \in T$ where $zG(y) = 1$. It follows that

$$\phi^i(y) = (F'_{i,1}(y, G^{-1}(y)), \ldots, F'_{i,t}(y, G^{-1}(y))) = (f_{i,1}(y)/g(y), \ldots, f_{i,t}(y)/g(y))$$

for some g, $f_{i,1}, \ldots, f_{i,t} \in k'[x_1, \ldots, x_t]$, $i = 1, \ldots, e$, with $\mathrm{dg}(g), \mathrm{dg}(f_{i,j}) \le |S|(d'|N|+1)$ where $d' = \max\{\mathrm{dg}(F) : F \in N\}$.

Summing up the time in each part of the computation yields the bound $O(|P|^{ct}(d(|N|+1))^{ct^2} + et|S|^2 \log q)$ for some constant c. $\square$

4. Efficient Algorithms for Counting Points

In this section we apply the tools developed so far to construct the characteristic polynomial of the Frobenius endomorphism on an Abelian variety over a finite field, in particular the Jacobian variety of a hyperelliptic curve over a finite field. From the characteristic polynomial one gets immediately the number of rational points on the variety, and in the case where the Abelian variety is the Jacobian of a curve, the number of rational points on the curve, as well as the number of rational points on its Jacobian.

4.1. general strategy

Let A be an Abelian variety of dimension g defined over a finite field $\mathbf{F}_q$ where $q = p^m$ for some prime p and $m \in \mathbf{Z}_{>0}$. Let $F \in \mathbf{Z}[x]$ be the characteristic polynomial of the Frobenius endomorphism ϕ_A on A. Then F is monic of degree $2g$. As observed in Pila (1990), F is uniquely determined by F mod l for primes $l \leq (9g+3)\log q$. For all primes $l \neq p$, let $A[l]$ denote the set of l-torsion points on A. Then $A[l]$ is of dimension $2g$ over $\mathbf{F}_l$ and F mod l is the characteristic polynomial of ϕ_A acting on $A[l]$ as a linear automorphism. Consider $A[l]$ also as a module over the principal ideal domain $\mathbf{F}_l[t]$ where for all $Q \in A[l]$, $t(Q) = \phi_A(Q)$. For all monic irreducible polynomials $h \in \mathbf{F}_l[t]$ of degree no greater than $2g$, let $A[l]_h$ denote the submodule of $A[l]$ consisting of points in $A[l]$ killed by $h^i(t)$ for some $i > 0$. Then

$$A[l]_h \cong \bigoplus_{i=1}^{d} \frac{\mathbf{F}_l[t]}{h^{e_i}(t)}$$

for some d and some $e_1, \ldots, e_d$ with $e_1 \leq \cdots \leq e_d$. Suppose e is the largest integer such that h^e divides F mod l. Then

$$e = \sum_{i=1}^{d} e_i$$

hence

$$\#(A[l]_h) = \prod_{i=1}^{d} l^{e_i \mathrm{dg}(h)} = l^{e\mathrm{dg}(h)}.$$

Since $e \leq 2g$, it follows that $A[l]_h$ is the submodule killed by $h^s(t)$ where s is the largest integer e such that $e\mathrm{dg}(h) \leq 2g$. Consequently,

$$F \bmod l = \prod h^{e_h}$$

where h ranges over all irreducible polynomials in $\mathbf{F}_l[t]$ of degree no greater than $2g$ and e_h is such that $l^{e_h \mathrm{dg}(h)}$ is the cardinality of the kernel of $h^s(\phi_A)$ where s is the largest integer with $s\mathrm{dg}(h) \leq 2g$. Hence we are reduced to the following problem: given $H \in \mathbf{F}_l[t]$ of degree no greater than $2g$, to compute $\#(ker(H(\phi_A)))$ on $A[l]$.

4.2. improvement on Pila's result

Pila (1990) showed that an Abelian variety A of dimension g over a finite field k of q elements is explicitly given as a projective variety in $P(k, N)$ by:

- forms $F_1, \ldots, F_S \in k[x_0, \ldots, x_N]$ of maximum degree T that generate a radical ideal defining A as a closed subvariety of $P(k, N)$,
- an atlas for the addition morphism on A consisting of R charts involving forms of maximum degree D,

- the identity element E as a point in $P(k, N)$.

Then the characteristic polynomial of the Frobenius endomorphism can be constructed in $(\log(q))^{\Delta})$ time where Δ is polynomial in g, $\log R$, $\log D$, but exponential in N. Below we described how this result can be improved so that Δ depends polynomially in N.

Consider the problem of computing $\#ker(H(\phi))$ above. We follow the algorithm of Pila (1990), except that:[†]

- whenever a task is called for reducing a polynomial modulo a zero-dimensional affine ideal, we apply the algorithm in Theorem 3.2,
- whenever a task is called for counting the number of points in the zero set of a zero-dimensional affine ideal, we apply the algorithm in Theorem 3.1.

Hence following Pila (1990) we construct an atlas M_l for the l-morphism with $|M_l| \leq l^{2\log R}$ charts of degree $D_l \leq D^2 l^{1+\log D} \leq l^{O(\log D)}$, and for each i, $0 \leq i \leq N$, an affine ideal generated by at most $S + (N+1)|M_l|$ polynomials of degree at most $\max\{T, D_l\}$ whose zero set is the subset $A[l]_i$ of $A[l]$ in the i-th affine subspace of $P(k, N)$. The next step is to construct polynomials representing $\phi, \ldots, \phi^{2g}$ on $A[l]_i$ all of which with degree no greater than l^{2g}. However instead of following Pila (1990), we apply the algorithm in Theorem 3.2 to the algebraic set. This takes $O(\log q l^{4g+N^2(\log D+\log R)})$ time by Theorem 3.2. Then resuming the steps in Pila (1990) we eventually reduce the problem to computing the cardinality of the zero sets of $O(N^2)$ many zero-dimensional affine algebraic sets, each of at most $l^{O(g \log R)}$ many polynomials of degree no greater than l^{2g} and with no greater than l^{2g} points. However, instead of following Pila (1990) we apply the algorithm in Theorem 3.1 for the tasks. This takes for each ideal $l^{O(N^2(g+\log R))}$ time by Theorem 3.1. As in Pila (1990), these tasks calling for reduction of polynomials and counting of zero-dimensional algebraic sets dominate, in terms of time, the rest of the steps in the algorithm. Since $O(N^2 \log q)$ many such tasks are called for, a routine calculation shows that the running time is bounded by $(\log q)^{O(N^2(g+\log R+\log D))}$ which is polynomial in g, $\log D$, $\log R$, as well as N.

4.3. Counting points on hyperelliptic curves and Jacobians

Suppose the Abelian variety of interest is the Jacobian of a curve of genus g, a projective description required by Pila (1990) can in principle be constructed following Chow (1954). However the dimension N of the projective space where the Jacobian is realized as a projective variety can at least be exponential in g. Thus even the improved algorithm described above will take time $O(\log q^{\delta})$ where δ is exponential in g. To further improve the algorithm we will no longer insist on a projective description of the Jacobian, but will instead be content with semi-algebraic descriptions that can be realized in affine dimension $O(g)$. We will demonstrate how this can be done for the case of hyperelliptic curves and prove the following theorem.

Theorem 4.1. *There exists a deterministic algorithm which:*

[†] In Pila (1990) these tasks are handled by an ideal membership testing procedure which is far more time consuming.

(A) On input:

(1) a finite field k of q elements of characteristic different from two,
(2) a polynomial $f \in k[x]$ of degree $2g+1$ without multiple roots.

(B) Outputs:

(1) The number of k-rational points on the curve $y^2 = f$,
(2) The number of k-rational points on the Jacobian of the curve $y^2 = f$,
(3) The characteristic polynomial of the Frobenious endomorphism on the Jacobian of the curve $y^2 = f$.

(C) Halts within time $(\log q)^{O(g^2 \log g)}$.

We will need several elementary results concerning the degree bounds and the complexity of the composition of semi-algebraic maps. These results are summarized in Lemmas A.2, A.3, and A.4 of the Appendix.

4.3.1. semi-algebraic description for the Jacobian

We refer to Mumford (1984) for fundamental facts about hyperelliptic curves and their Jacobians.

Let $f \in \mathbf{F}_q[x]$ be of degree $2g+1$ without multiple roots. Then the curve C defined by $y^2 - f$ is hyperelliptic of genus g. The normalization X of C has one point ∞ at infinity which is $\mathbf{F}_q$-rational. The Jacobian J of X is isomorphic as a group to $\mathrm{Div}_0(X)/\mathrm{Div}_l(X)$ where $\mathrm{Div}_0(X)$ denotes the group of divisors of X of degree zero, and $\mathrm{Div}_l(X)$ denotes the group of divisors of functions on X.

Let ι denote the automorphism on C sending (x, y) to $(x, -y)$. For $m \geq 0$, let $\mathrm{Div}^{+m} = \{P_1 + \cdots + P_m : P_i \neq \infty \text{ for all } i, \text{ and } P_i \neq \iota P_j \text{ for } i \neq j\}$. A divisor in $\mathrm{Div}_0(X)$ is *reduced* if has the form $D - m\infty$ where $D \in \mathrm{Div}^{+m}$ for some $m \leq g$. Let $P = (a, b)$ be a point on C. Then $P + \iota P - 2\infty$ is in $\mathrm{Div}_l(X)$ since it is the divisor of the function $x - a$. This fact and the Riemann–Roch theorem imply that every divisor of degree zero is linearly equivalent to some reduced divisor (see, e.g. Cantor, 1987). Moreover since a non-constant function cannot have poles bounded by a divisor in Div^{+g} (Mumford, 1984), any two distinct reduced divisors cannot be linearly equivalent. Consequently every divisor class in $\mathrm{Div}_0(X)$ contains a unique reduced divisor. So let Div^+ be the disjoint unon of all Div^{+m} for $0 \leq m \leq g$. Then every point of J is uniquely represented by some $D \in \mathrm{Div}^+$. Hence we may identify J with Div^+.

Following Mumford (1984) (see also Cantor, 1987), for $0 < m \leq g$, every $D = P_1 + \cdots + P_m \in \mathrm{Div}^{+m}$ is uniquely represented by a pair of polynomials (u, v) where $u(x) = \prod_{i=1}^{m}(x - x(P_i))$, and $v(x)$ is the uique polynomial of degree no greater than m such that $v(x(P_i)) = y(P_i)$ for all i and u divides $f - v^2$. Note that since no branch points (points with y-coordinates 0) can have multiplicity greater than one in D, the GCD of f and the first derivative of u must be one. We also note that the empty divisor corresponding to the identity of J is represented by the pair of polynomials $(1, 0)$.

Let $u, v \in \bar{k}[x]$ with $\mathrm{dg}(u) \leq g$ and $\mathrm{dg}(v) \leq g - 1$. Write $u = u_g x^g + \cdots + u_0$ and $v = v_{g-1}x^{g-1} + \cdots + v_0$. We identify the polynomial pair (u, v) with $(u_g, \ldots, u_0, v_{g-1}, \ldots, v_0) \in A(k, 2g+1)$. In this manner we identify $A(k, 2g+1)$ with the set of polynomial pairs (u, v) over k with $\mathrm{dg}(u) \leq g$ and $\mathrm{dg}(v) \leq g - 1$.

A polynomial pair $(u, v) \in A(k, 2g+1)$ represents a divisor in Div^{+m} iff u is monic of degree m and $\mathrm{dg}(v) \leq m-1$, and u divides $f - v^2$, and the GCD of f and the first derivative of u is one. Thus the set of polynomial pairs $(u, v) \in A(k, 2g+1)$ representing Div^{+m} acquires a primitive semi-algebraic description as follows. First of all such a (u, v) satisfies $u_g = \cdots = u_{m+1} = 0$, $u_m = 1$, and $v_{g-1} = \cdots = v_m = 0$. Treating the remaining u_i, v_j as indeterminates, let R be the remainder polynomial in dividing $f - v^2$ by u, and D be the resultant of the first derivative of u and f. Then $R = R_{m-1}(u_i, v_j)x^{m-1} + \cdots + R_0(u_i, v_j)$ where $R_k(u_i, v_j)$ are polynomials in the indeterminates u_is and v_js of degree $O(g)$, D is a polynomial in u_i and v_j of degree $O(g)$, and (u, v) represents some divisor in Div^{+m} if and only if $R_k(u_i, v_j) = 0$ for $k = 0, \ldots, m-1$ and $D(u_i, v_j) \neq 0$. In this manner Div^{+m} acquires a description as a primitive semi-algebraic set in the affine $2g+1$ space of degree and number of equations bounded by $O(g)$. The collection of descriptions of Div^{+m} as primitive semi-algebraic sets for $m = 0, \ldots, g$ constitutes a semi-algebraic description of Div^{+}, hence of J.

Cantor (1987) has given an algorithm for adding points on J. The algorithm on input two polynomial pairs (a_1, b_1), $(a_2, b_2) \in A(k, 2g+1)$ which represent reduced divisors D_1 and D_2, returns the polynomial pair $(a, b) \in A(k, 2g+1)$ which represents the reduced divisor linearly equivalent to $D_1 + D_2$. Cantor's algorithm consists of two subalgorithms: composition and reduction. Composition takes (a_1, b_1), (a_2, b_2) and produces a polynomial pair (a, b) representing the sum of D_1 and D_2. Reduction takes (a, b) and reduces it to a pair representing the reduced divisor linearly equivalent to $D_1 + D_2$.

[Composition]

(c1) Compute $d = \mathrm{GCD}(a_1, a_2, b_1 + b_2)$ and polynomials h_1, h_2 and h_3 such that $d = h_1 a_1 + h_2 a_2 + h_3(b_1 + b_2)$;

(c2) $a := (a_1 a_2)/d^2$;

(c3) $b := (h_1 a_1 b_2 + h_2 a_2 b_1 + h_3(b_1 b_2 + f))/d \bmod a$.

If $\mathrm{dg}(a) > g$ then perform the following:

[Reduction]

(r1) Computes the collection of polynomials r_i, q_i, s_i, t_i in an extended Euclidean scheme of a and b, where $r_0 = a$, $r_1 = b$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$ as in Example 2.1. Find the least $i \geq 2$ such that $\mathrm{dg}(r_i) \leq (\mathrm{dg}(a) + g)/2$. Then $c := r_i$; $d := t_i$;

(r2) $a_2 := \mathrm{GCD}(c, d)$; $a_1 := a/a_2$; $c_1 := c/a_2$; $d_1 := d/a_2$;

(r3) $a_3 := (c_1^2 - d_1^2 f)/a_1$ and compute d' so that $dd' \equiv 1 \pmod{a_3}$ (d' is in the extended Euclidean scheme of d and a_3);

(r4) Apply Composition to $(a_3, -d'c_1)$ and (a_2, b).

The composition and reduction phases each consist of no more than three extended GCD computations and a few polynomial additions, multiplications and divisions. It follows from Example 2.1 and Lemma A.3 that a semi-algebraic map $\Gamma_{k,f}$ for the algorithm can be derived, and its description $\hat{\Gamma}_{k,f}$ has $n(\hat{\Gamma}_{k,f}) = O(g)$, $r(\hat{\Gamma}_{k,f}) = 2^{O(g)}$ and $\mathrm{dg}(\hat{\Gamma}_{k,f}) = g^{O(1)}$. And $\hat{\Gamma}_{k,f}$ can be computed in $g^{O(g)}$ time. This is a semi-algebraic map representing the addition law on the Jacobian J.

4.3.2. semi-algebraic description for l-torsion

For all positive integers l, let Π_l denote the "multiplication by l" map in the sense that for all reduced divisors D, if (a,b) is the polynomial representation of D, then $\Pi_l(a,b)$ is the polynomial representation of the reduced divisor in the class of lD.

Let $\Gamma = \Gamma_{k,f}$. Let Δ be the semi-algebraic map over k with domain $A(k, 2g+1)$ such that for all $(a,b) \in A(k, 2g+1)$, $\Delta(a,b) = (a,b,a,b)$. Then $\Pi_2 = \Gamma \circ \Delta$, and for all $m \in \mathbf{Z}_{>1}$, $\Pi_{2^m} = \Gamma(\Pi_{2^{m-1}}, \Pi_{2^{m-1}})$. By Lemma A.3, we see inductively that for all $m \in \mathbf{Z}_{>0}$, there is a description $\hat{\Pi}_{2^m}$ of Π_{2^m} with

$$\mathrm{dg}(\hat{\Pi}_{2^m}) = g^{O(m)}, \qquad r(\hat{\Pi}_{2^m}) = 2^{O(mg)}, \qquad n(\hat{\Pi}_{2^m}) = O(mg),$$

and $\hat{\Pi}_{2^m}$ can be computed in $g^{O(mg)}$ time. It follows that for all positive integers l, a description $\hat{\Pi}_l$ of Π_l can be derived with $\mathrm{dg}(\hat{\Pi}_l) = l^{O(\log g)}$, $r(\hat{\Pi}_l) = l^{O(g)}$, and $n(\hat{\Pi}_l) = O(g \log l)$, and $\hat{\Pi}_l$ can be computed in $l^{O(g \log g)}$ time.

Let Ω be the semi-algebraic map with domain $A(k, 2g+1)$ such that for all $(a,b) \in A(k, 2g+1)$, $\Omega(a,b)$ is the polynomial representation of the identity of J.

For all rational primes l, let T_l be the set of all (a,b) representing l-torsion points in J. Then, in the notation of Lemma A.4, T_l is the union of all $\tau(\pi, \omega)$ where π is a component of Π_l and ω is a component of Ω. (See Lemma A.4 for the definition of τ.) From Lemma A.4 it follows that T_l is a semi-algebraic set and a description of it, $\hat{T}_l$, can be computed in $l^{O(g \log g)}$ time with $\mathrm{dg}(\hat{T}_{k,f,t,l}) = l^{O(\log g)}$, $n(\hat{T}_{k,f,t,l}) = O(g \log l)$ and $r(\hat{T}_{k,f,t,l}) = l^{O(g)}$.

4.3.3. kernel of $H(\phi)$

Fix a prime l different from the characteristic of k for now. Let $T = T_l$, and ϕ be the Frobenius map. From Theorem 3.2 it follows that for all $i \leq 2g$, there is a description $\hat{\phi^i}$ of ϕ^i on T such that $\mathrm{dg}(\hat{\phi^i}) = l^{O(g)}$, $r(\hat{\phi^i}) = l^{O(g)}$, $r(\hat{\phi^i}) = O(g \log l)$, and $\hat{\phi}, \ldots, \hat{\phi}^{2g}$ can be computed in $l^{O(g^2 \log g)} + l^{O(g)} \log q$ time. Let H be a polynomial in $\mathbf{F}_l[x]$ of degree no greater than $2g$. From Lemma A.3 it follows that the map $H(\phi)$ on T has a description $\hat{H}$ with $r(\hat{H}) = l^{O(g^2)}$, $\mathrm{dg}(\hat{H}) = l^{O(g)} g^{O(g)}$, $n(\hat{H}) = O(g^2 \log l)$, and $\hat{H}$ can be computed in $l^{O(g^2 \log g)}$ time, assuming $\hat{\phi}, \ldots, \hat{\phi}^{2g}$ are already computed. $ker(H(\phi))$ is the disjoint union of all $\tau(\eta, \omega)$ where η is a component of $H(\phi)$ and ω a component of Ω, each $\tau(\eta, \omega)$ being primitive semi-algebraic with a description of degree $l^{O(g)} g^{O(g)}$ and $O(g^2 \log l)$ many defining equalities and inequalities, and computable in $l^{O(g^2 \log g)}$ time by Lemma A.4. Hence we get a description of $ker(H(\phi))$ with $l^{O(g^2)}$ many primitive semi-algebraic sets, each with a degree and number of defining equalities and inequalities as described above. We then apply Theorem 3.1 to compute the cardinality of each of these primitive semi-algebraic sets. The total time complexity for computing $\#ker(H(\phi))$ is $l^{O(g^2 \log g)} + l^{O(g)} \log q$.

4.3.4. characteristic polynomial

To summarize, on input $k = \mathbf{F}_q, f$, the following algorithm computes the characteristic polynomial F for the Frobenius endomorphism of the Jacobian of the curve with affine model $y^2 = f$.

```
(1) CALCULATE $\Gamma = \Gamma_{k,f}$.
(2) For all primes $l \in \mathbf{Z}_{>0}$ with $l \leq (9g+3)\log q$.
    (a) CALCULATE $T = T_l$.
    (b) For all monic irreducible polynomials $h \in \mathbf{Z}/l\mathbf{Z}[x]$ of degree no greater than $2g$:
        (i) Calculate $C_h = \sum_{\eta,\omega} \#(\tau(\eta,\omega))$, where $\eta$ ranges over all primitive maps in
            $h^s(\phi)$ with $s$ being the largest integer such that $s\mathrm{dg}(h) \leq 2g$, and $\omega$ ranges
            over all primitive maps in $\Omega$.
        (ii) Calculate $e_h = (\log_l(C_h))/\mathrm{dg}(h)$.
    (c) $F_l := \prod_{h \in I} h^{e_h}$ where $I$ is the set of all monic irreducible polynomials $h \in$
        $\mathbf{Z}/l\mathbf{Z}[x]$ of degree no greater than $2g$.
(3) Calculate $F$ by Chinese Remainder Theorem.
```

From the discussion above, it follows that the time for computing each C_h is $l^{O(g^2 \log g)} + l^{O(g)} \log q$. As there are no more than l^{2g} choices of h for each prime l, it follows that the total time complexity is $(\log q)^{O(g^2 \log g)}$.

Acknowledgements

The National Science Foundation supported this research through grants CCR-9403662 (LA) and, CCR-9412383, and CCR-9820778 (M-DH). A preliminary version of this paper appeared in Adleman and Huang (1996).

References

Adleman, L. M., Huang, M.-D. (1992). *Primality Testing and Abelian Varieties Over Finite Fields*, LNM **1512**. Berlin, Springer-Verlag.

Adleman, L. M., Huang, M.-D. (1996). Counting rational points on curves and Abelian varieties over finite fields. In *Proceedings of the 2nd Algorithmic Number Theory Symposium (ANTS II), Talence, France.*

Canny, J. (1988). Some algebraic and geometric problems in PSPACE. In *Proceedings of the 20th ACM Symposium on the Theory of Computing, Chicago, U.S.A.* New York, ACM Press.

Cantor, D. (1987). Computing in the Jacobian of a hyperelliptic curve. *Math. Comput.*, **V. 48**, 95–101.

Chow, W. L. (1950). On the defining field of a divisor in an algebraic variety. *Am. J. Math.*, **72**, 247–283.

Chow, W. L. (1954). The Jacobian variety of an Abelian variety. *Am. J. Math.*, **76**, 454–476.

Chow, W. L., van der Wareden, B. L. (1937). Zur algebraischen geometrie, IX, Über zugeordnete formen und algebraische systeme von algebraischen mannigfaltigkeiten. *Math. Annalen*, **113**, 692–704.

Hartshorne, R. (1977). *Algebraic Geometry.* Springer-Verlag.

Huang, M.-D., Ierardi, D. (1993). Counting points on curves over finite fields. *Proceedings of the 32nd IEEE Symposium on the Foundations of Computer Science, Palo Alto.*

Ierardi, D. (1989a). Quantifier elimination in the theory of an algebraically closed field. Ph.D. Thesis, Cornell University.

Ierardi, D. (1989b). Quantifier elimination in the theory of an algebraically closed field. In *Proceedings of the 21st ACM Symposium on Theory of Computing, Seattle, U.S.A.* New York, ACM Press.

Ierardi, D., Kozen, D. (1991). Parallel resultant computation. In *Synthesis of Parallel Algorithms.* Morgan Kaufman.

Mumford, D. (1984). *Tata Lectures on Theta II.* Boston, Birkhäuser.

Pila, J. (1990). Frobenius maps of Abelian varieties and finding roots of unity in finite fields. *Math. Comput.*, **55**, 745–763.

Poonen, B. (1996). Computational Aspects of curves of genus at least 2. In *Proceedings of the 2nd Algorithmic Number Theory Symposium (ANTS II), Talence, France.*

Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots mod P. *Math. Comput.*, **44**, 483–494.

Appendix A. Composition of Semi-algebraic Maps

We analyze the degree bounds and the complexity for the composition of semi-algebraic maps. The analysis is completely elementary. The time complexity of the algorithms in this section is measured in terms of the number of field operations in the specified ground field.

Lemma A.1. *Let k be a field and f_1,$g_1, \ldots, f_s, g_s \in k[x_1, \ldots, x_t]$ be of degree bounded by d. Then for $F \in k[x_1, \ldots, x_s]$ there exist A_F, $B_F \in k[x_1, \ldots, x_t]$ of degree bounded by $sd\mathrm{dg}(F)$ and computable in $O(s^{2t+1}d^{2t}\mathrm{dg}(F)^{s+2t+1})$ time, such that*

$$F\left(\frac{f_1(u)}{g_1(u)}, \ldots, \frac{f_s(u)}{g_s(u)}\right) = \frac{A_F(u)}{B_F(u)} \tag{A.1}$$

for all $u \in A(k,t)$ where $g_i(u) \neq 0$ for $i = 1, \ldots, s$.

Proof. Let

$$F = \sum_\alpha a_\alpha x_1^{\alpha_1} \ldots\ x_s^{\alpha_s} \in k[s]$$

where α ranges over all tuples $\alpha = (\alpha_1, \ldots, \alpha_s)$ with $\alpha_1 + \cdots + \alpha_s \leq \mathrm{dg}(F)$. Then for $u \in R$

$$F\left(\frac{f_1(u)}{g_1(u)}, \ldots, \frac{f_s(u)}{g_s(u)}\right) = \sum_\alpha a_\alpha \frac{f_1^{\alpha_1}\ \ldots\ f_s^{\alpha_s}(u)}{g_1^{\alpha_1}\ \ldots\ g_s^{\alpha_s}(u)}.$$

Reexpressing each term such that they acquire the common denominator $B_F(u)$ where $B_F = (g_1 \ldots g_s)^{\mathrm{dg}(F)}$, we derive

$$F\left(\frac{f_1(u)}{g_1(u)}, \ldots, \frac{f_s(u)}{g_s(u)}\right) = \frac{A_F(u)}{B_F(u)}$$

where $A_F \in k[x_1, \ldots, x_t]$ and $\mathrm{dg}(A_F)$,$\mathrm{dg}(B_F) \leq sd\mathrm{dg}(F)$. To bound the time complexity in computing A_F and B_F, we observe that multiplying two polynomials of degree m and n in l variables takes $O((nm)^l)$ operations. There are no more than $\mathrm{dg}(F)^s$ terms in F, and for each term we need no more than $s\mathrm{dg}(F)$ multiplications of a pair of polynomials in t variables of degree no more than $sd\mathrm{dg}(F)$. A routine calculation yields the bound $O(s^{2t+1}d^{2t}\mathrm{dg}(F)^{s+2t+1})$. □

Lemma A.2. (Composition of Primitive Semi-algebraic Maps) *There exists a deterministic algorithm which:*

(A) On input:

(1) a description $\hat{\psi}$ of a primitive semi-algebraic map ψ over a field k of type $\langle s,t\rangle$ with domain $S \subset A(k,s)$,

(2) for $i = 1, \ldots, z$, a description $\hat{\phi}_i$ of a primitive semi-algebraic map ϕ_i over k of type $\langle r, s_i\rangle$ with domain $R \subset A(k,r)$ and $\sum_{i=0}^z s_i = s$, such that $\hat{\phi}_i = \hat{\phi}_j$ if $\phi_i = \phi_j$.

(B) Outputs a description $\hat{\omega}$ of a primitive semi-algebraic map ω over k such that:

(1) ω is of type $\langle r,t\rangle$ with domain $D = \{u \in R : \langle\phi_1(u), \ldots, \phi_z(u)\rangle \in S\}$ such that $\omega(u) = \psi(\phi_1(u), \ldots, \phi_z(u))$ for all $u \in D$,

(2) $\mathrm{dg}(\hat{\omega}) = O(sd\mathrm{dg}(\hat{\psi}))$ *where* $d = \max\{\mathrm{dg}(\hat{\phi}_i) : i = 1, \ldots, z\}$,

(3) $n(\hat{\omega}) \leq n(\hat{R}) + n(\hat{S})$,

where $\phi'_1, \ldots, \phi'_m$ *are the distinct members of* $\{\phi_1, \ldots, \phi_z\}$.

(C) Halts within time $O((n(\hat{\psi}) + t)s^{r+1}d^r\mathrm{dg}(\hat{\psi})^{r+s+1})$.

Proof. For $i = 1, \ldots, z$ let $\hat{\phi}_i = \langle k, r, s_i, \hat{R}, f_{i1}, g_{i1}, \ldots, f_{is_i}, g_{is_i}\rangle$ where $f_{ij}, g_{ij} \in k[x_1, \ldots, x_r]$ for $j = 1, \ldots, s_i$. Rename $f_{11}, \ldots, f_{zs_z}$ as $f_1, \ldots, f_s$ and $g_{11}, \ldots, g_{zs_z}$ as $g_1, \ldots, g_s$. Then for all $u \in R$

$$\langle \phi_1(u), \ldots, \phi_z(u)\rangle = \left\langle \frac{f_1(u)}{g_1(u)}, \ldots, \frac{f_s(u)}{g_s(u)} \right\rangle.$$

Let $\hat{R} = \langle P_R, N_R\rangle$ with $P_R, N_R \subset k[x_1, \ldots, x_r]$, and $\hat{S} = \langle P_S, N_S\rangle$ with $P_S, N_S \subset k[x_1, \ldots, x_s]$. For all $F \in P_S \cup N_S$, for all $u \in R$, from Lemma A.1 it follows that $F(\phi_1(u), \ldots, \phi_z(u)) = 0$ iff $A_F(u) = 0$. Consequently D is semi-algebraic with a description $\hat{D} = \langle P_D, N_D\rangle$ where $P_D = P_R \cup \{A_F : F \in P_S\}$ and $N_D = N_R \cup \{A_F : F \in N_S\}$, in particular $n(\hat{D}) \leq n(\hat{R}) + n(\hat{S})$, Moreover for $F \in P_S \cup N_S$, A_F is of degree $\leq sd\mathrm{dg}(\hat{\Psi})$ as $\mathrm{dg}(F) \leq \mathrm{dg}(\hat{\Psi})$ and can be computed in $O(s^{r+1}d^r\mathrm{dg}(\hat{\Psi})^{r+s+1})$ time.

Let $\hat{\psi} = \langle k, s, t, \hat{S}, H_1, T_1, \ldots, H_t, T_t\rangle$ where $H_k, T_k \in k[x_1, \ldots, x_s]$ for $k = 1, \ldots, t$. Let $u \in D$, then

$$\psi(\phi_1, \ldots, \phi_z)(u) = \langle y_1(u), \ldots, y_t(u)\rangle$$

where

$$y_k(u) = \frac{H_k(\phi_1(u), \ldots, \phi_z(u))}{T_k(\phi_1(u), \ldots, \phi_z(u))}$$

for $k = 1, \ldots, t$. By Lemma A.1

$$H_k(\phi_1(u), \ldots, \phi_z(u)) = \frac{A_{H_k}(u)}{B_{H_k}(u)}$$

$$T_k(\phi_1(u), \ldots, \phi_z(u)) = \frac{A_{T_k}(u)}{B_{T_k}(u)}$$

with A_{H_k}, A_{T_k}, B_{H_k}, $B_{T_k} \in k[x_1, \ldots, x_r]$ of degree $\leq 2sd\mathrm{dg}(\hat{\Psi})$, and computable in $O(s^{r+1}d^r\mathrm{dg}(\hat{\Psi})^{r+s+1})$ time. Let $F_{k1} = A_{H_k}B_{T_k}$ and let $F_{k2} = B_{H_k}A_{T_k}$. Then $y_k(u) = \frac{F_{k1}(u)}{F_{k2}(u)}$. Let $\hat{\omega} = \langle k, r, t, \hat{D}, F_{11}, F_{12}, \ldots, F_{t1}, F_{t2}\rangle$. Then $\hat{\omega}$ is a description of ω with $\mathrm{dg}(\hat{\omega}) = O(sd\mathrm{dg}(\hat{\psi}))$ where $d = \max\{\mathrm{dg}(\hat{\phi}_i) : i = 1, \ldots, z\}$ And $\hat{\omega}$ can be computed in $O((n(\hat{\psi}) + t)s^{r+1}d^r\mathrm{dg}(\hat{\psi})^{r+s+1})$ time. □

Lemma A.3. (Composition of Semi-algebraic Maps) *There exists a deterministic algorithm which:*

(A) On input:

(1) a description $\hat{\Psi}$*of a semi-algebraic map* Ψ *over a field* k *of type* $\langle s, t\rangle$ *with domain* $S \subset A(k, s)$,

(2) for $i = 1, \ldots, z$, *a description* $\hat{\Phi}_i$ *of a semi-algebraic map* Φ_i *over* k *of type* $\langle r, s_i\rangle$ *with domain* $R \subset A(k, r)$ $\sum_{i=0}^{z} s_i = s$, *such that* $\hat{\Phi}_i = \hat{\Phi}_j$ *if* $\Phi_i = \Phi_j$.

(B) Outputs a description $\hat{\Omega}$ *of a semi-algebraic map* Ω *over* k *such that:*

(1) Ω *is of type* $\langle r,t\rangle$ *with domain* $D=\{x\in R:\langle\Phi_1(x),\dots,\Phi_z(x)\rangle\in S\}$ *such that for all* $u\in D$, $\Omega(u)=\Psi(\Phi_1(u),\dots,\Phi_z(u))$,

(2) $r(\hat{\Omega})=r(\hat{\Psi})r(\hat{\Phi}'_1)\dots r(\hat{\Phi}'_m)$,

(3) $\mathrm{dg}(\hat{\Omega})=O(sd\mathrm{dg}(\hat{\Psi}))$ *where* $d=\max\{\mathrm{dg}(\hat{\Phi}_i):i=1,\dots,z\}$,

(4) $n(\hat{\Omega})\leq n(\hat{\Psi})+\sum_{i=1}^{m}n(\hat{\Phi}'_i)$,

where $\Phi'_1,\dots,\Phi'_m$ *are the distinct members of* $\{\Phi_1,\dots,\Phi_z\}$.

(C) Halts within time $O(r(\hat{\Psi})r(\hat{\Phi}'_1)\dots r(\hat{\Phi}'_m)(n(\hat{\Psi})+t)s^{r+1}d^r\mathrm{dg}(\hat{\Psi})^{r+s+1})$.

PROOF. Let Σ be the set of all $\langle\phi_1,\dots,\phi_z\rangle$ where ϕ_i is a component of Φ_i for $i=1,\dots,z$ such that if $\Phi_i=\Phi_j$ then $\phi_i=\phi_j$. For all $\sigma=\langle\phi_1,\dots,\phi_z\rangle\in\Sigma$, let $R_\sigma=\cap_{i=1}^{z}R_i$ where R_i is the domain of ϕ_i for $i=1,\dots,z$. Let $\hat{R}_i=\langle P_{R_i},N_{R_i}\rangle$ be a description of R_i for $i=1,\dots,z$. Then R_σ is a semi-algebraic set with a description $\hat{R}_\sigma=\langle P_{R_\sigma},N_{R_\sigma}\rangle$ where $P_{R_\sigma}=\cup_{i=1}^{z}P_{R_i}$ and $N_{R_\sigma}=\cup_{i=1}^{z}N_{R_i}$. In particular $n(\hat{R}_\sigma)\leq\sum_{i=1}^{m}n(\hat{\Phi}'_i)$. Moreover R is the disjoint union of all R_σ with $\sigma\in\Sigma$. Let ψ be a component of Ψ with domain S_ψ. Then applying Lemma A.2 to ψ and the restrictions of $\phi_1,\dots,\phi_z$ to R_σ we obtain a description $\hat{\omega}_{\psi,\sigma}$ for the primitive semi-algebraic map $\omega_{\psi,\sigma}=\psi(\phi_1,\dots,\phi_z)$ with domain

$$\{x\in R_\sigma:\langle\phi_1(x),\dots,\phi_z(x)\rangle\in S_\psi\}.$$

We note that $n(\hat{\omega}_{\psi,\sigma})\leq n(\hat{S}_\psi)+n(\hat{R}_\sigma)\leq n(\hat{\psi})+\sum_{i=1}^{m}n(\hat{\Phi}'_i)$. The collection of all $\omega_{\psi,\sigma}$ with ψ a component of Ψ and ϕ_i a component of Φ_i, for $i=1,\dots,z$, forms a semi-algebraic map Ω with domain

$$\{x\in R:\langle\phi_1(x),\dots,\phi_z(x)\rangle\in S\},$$

and number of components $r(\hat{\Psi})r(\hat{\Phi'_1})\dots r(\hat{\Phi'_m})$. The rest of the assertion follows easily from Lemma A.2. □

LEMMA A.4. *Let* k *be a field. Let* ϕ *be a primitive semi-algebraic map over* k *of type* $\langle s,t\rangle$ *with domain* R. *Let* ψ *be a primitive semi-algebraic map over* k *of type* $\langle s,t\rangle$ *with domain* S. *Let* $\tau(\phi,\psi)=\{\alpha:\alpha\in R\ \&\ \alpha\in S\ \&\ \phi(\alpha)=\psi(\alpha)\}$. *Then* $\tau(\phi,\psi)$ *is a semi-algebraic set over* k. *Moreover, suppose* $\hat{\phi}$, $\hat{\psi}$ *are descriptions of* ϕ *and* ψ *such that*

$$\hat{\phi}=\langle k,s,t,\hat{R},f_1,g_1,\dots,f_t,g_t\rangle$$
$$\hat{\psi}=\langle k,s,t,\hat{S},h_1,q_1,\dots,h_t,q_t\rangle$$

where $\hat{R}=\langle P_R,N_R\rangle$ *with* $P_R,N_R\subset k[x_1,\dots,x_s]$, *and* $\hat{S}=\langle P_S,N_S\rangle$ *with* $P_S,N_S\subset k[x_1,\dots,x_s]$. *Then* $\tau(\phi,\psi)$ *has a description* $\langle M,Q\rangle$ *where*

$$M=P_R\cup P_S\cup\{f_iq_i-h_ig_i:1\leq i\leq t\}$$
$$Q=N_R\cup N_S.$$

PROOF. It is easy to see that $R\cap S$ is semi-algebraic with representative $\langle P_R\cup P_S,N_R\cup N_S\rangle$. For $x\in R\cap S$, $\phi(x)=\psi(x)$ iff $f_i(x)/g_i(x)=h_i(x)/q_i(x)$ for all $i=1,\dots,t$ iff $(f_iq_i-h_ig_i)(x)=0$ for $i=1,\dots,t$, and the lemma follows. □

Received 25 August 1997
Accepted 4 April 2001