IMPLICITIZATION OF RATIONAL PARAMETRIC EQUATIONS*

Xiao-Shan Gao† and Shang-Ching Chou

Department of Computer Sciences
The University of Texas at Austin
Austin, Texas 78712-1188

TR-90-34 November 1990

ABSTRACT

Based on the Gröbner basis method, we present algorithms for a complete solution of the following problems in the implicitization of a set of rational parametric equations. (1) To find a basis of the implicit prime ideal determined by a set of rational parametric equations. (2) To decide whether the parameters of a set of rational parametric equations are independent. (3) If the parameters of a set of rational parametric equations are not independent, to reparameterize the parametric equations so that the new parametric equations have independent parameters. (4) To compute the inversion maps of parametric equations, and as a consequence, to give a method to decide whether a set of parametric equations is proper. (5) In the case of algebraic curves, to find proper reparameterization for a set of improper parametric equations.

Keywords: Computer modeling, rational parametric equations, implicitization, inversion maps, independent parameters, proper parametric equations, Gröbner bases.

* The work reported here was supported in part by the NSF Grants CCR-8702108 and CCR-9002362.
† On leave from Institute of Systems Science, Academia Sinica, Beijing.

1. Introduction

For curves and surfaces, methods of converting parametric equations to their implicit form are of fundamental importance in computer modeling and computer graphics. Several methods to find the implicit equations and inversion maps for a set of parametric equations were given by various researchers. Sederberg was the first to address this problem using elimination theories [Sederberg, 1984]. [Arnon & Sederberg, 1984] appeared to be the first to address this problem using the Gröbner basis method. Buchberger solved this problem in more general cases using the Gröbner basis method [Buchberger, 1987]. A method to find the implicit approximation of parametric equations of curves and surfaces was presented in [Chuang & Hoffman, 1989]. Recently, a method to compute the image of parametric equations was given in [Wu, 1989] and [Li, 1989].

However, in more general cases, there are many problems untouched. For example, the parameters of a set of parametric equations might not be independent as shown by the following example. At first sight, one might think that the parametric equations

$$x = \frac{u+v}{u-v}, y = \frac{2v^2+2u^2}{(u-v)^2}, z = \frac{2v^3+6u^2v}{(u-v)^3} \tag{1.1}$$

represent a space surface. Actually, they represent a space curve, because let $t = \frac{u+v}{u-v}$, then the above parametric equations become

$$x = t,\ y = t^2 + 1,\ z = t^3 - 1.$$

For the above example, each point of the curve corresponds to infinitely many values of u and v. Hence the solution of the inversion problem here is not clear.

In this paper we will address the implicitization problem for rational parametric equations in a more general form. Our algorithms are based on the Gröbner basis method, a powerful toll in computer algebra [Buchberger, 1985] introduced by Buchberger in 1965.

We will show that each set of rational parametric equations determines a unique prime ideal which will be called the *implicit prime ideal* of the parametric equations. In [Buchberger, 1987], a method was given to compute a basis of the implicit prime ideal for a set of *polynomial* parametric equations. But a straight forward extension of Buchberger's method to the implicitization of *rational* parametric equations may not work (see Remark 3.6 below) because of the existence of base points. In [Kalkbrener, 1990], a method to find the implicit prime ideal for *rational* parametric equations of space curves and surfaces has been given. In this paper, by extending their methods we present a method of finding the prime ideal for general *rational* parametric equations. We also give a method to decide whether the parameters of a set of rational parametric equations are independent. If the parameters of the parametric equations are not independent, we can reparameterize them so that the new parametric equations have independent parameters.

If a set of parametric equations has independent parameters, we present a close form solution of the inversion problem in certain cases, i.e., we give a method to compute the

inversion maps of the parametric equations. As a consequence of our method, we can decide whether the parametric equations are proper, i.e., whether the implicit curves or surfaces are not multiply traced by the parametric equations [Faux and Pratt 1979].

If the parametric equations are not proper, naturally we would ask whether we can reparameterize them so that the new parametric equations are proper. In general cases, the answer is negative. However, in the case of algebraic curves, the existence of a proper reparametrization for the original improper parametric equations is guaranteed by Lüroth's theorem [Walker, 1950]. A constructive proof of Lüroth's theorem actually provides an algorithm to construct a set of proper parametric equations. Recently, Sederberg gave a method to find proper reparametrization for any set of improper parametric equations for algebraic curves [Sederberg 1986]. As an application of our method, we provide a new method to find a proper reparametrization for a set of improper parametric equations of an algebraic curve and our method does not need to randomly select sample points on the curve as Sederberg's algorithm does. In the case of algebraic surfaces, if the ground field K is the complex number field $\mathbf{C}$, then there always exists a proper reparametrization for the original improper parametric equations [Castelnuvo 1894]. However if the base field K is $\mathbf{Q}$ (the field of rational numbers) or $\mathbf{R}$ (the field of real numbers), this needs not to be the case [Segre 1951]. If the implicit variety determined by the parametric equations are of dimension > 2, then even for $K = \mathbf{C}$ there exist improper parametric equations that do not have a proper reparametrization [Artin & Mumford 1971].

This paper is organized as follows. In section 2, we give some basic definitions and properties of parametric equations. In section 3, we give a method to compute a basis of the implicit prime ideal for a set of rational parametric equations. In section 4, we present a method to reparameterize a set of parametric equations (if its parameters are not independent) so that the parameters of the new parametric equations are independent. In section 5, we give a method to compute the inversion maps, and in the case of algebraic curves, give a method to find a set of proper parametric equations for a set of improper parametric equations. Section 6 is a summary of the paper.

2. Preliminaries on Parametric Equations

Let K be a computable field of characteristic zero, e.g., $\mathbf{Q}$. We use $K[x_1, ..., x_n]$ or $K[x]$ to denote the ring of polynomials in the indeterminates $x_1, ..., x_n$. Unless explicitly mentioned otherwise, all polynomials in this paper are in $K[x]$. Let E be a *universal extension* of K, i.e., an algebraic closed extension of K which contains sufficiently many independent indeterminates over K. For a polynomial set PS, let

$$Zero(PS) = \{x = (x_1, ..., x_n) \in E^n \mid \forall P \in PS, P(x) = 0\}.$$

For two polynomial sets PS and DS, we define

$$Zero(PS/DS) = Zero(PS) - \cup_{d \in DS} Zero(d).$$

Let $t_1, ..., t_m$ be indeterminates in E which are independent over K. For polynomials

$P_1, ..., P_n, Q_1, ..., Q_n$ in $K[t_1, ..., t_m]$ $(Q_i \neq 0)$, we call

$$x_1 = \frac{P_1}{Q_1}, \ ..., \ x_n = \frac{P_n}{Q_n} \tag{2.1}$$

a set of (rational) parametric equations. We assume that not all P_i and Q_i are constants and $gcd(P_i, Q_i) = 1$. The maximum of the degrees of P_i and Q_j is called the *degree* of (2.1). The image of (2.1) in E^n is

$$IM(P,Q) = \{(x_1, ..., x_n) \mid \exists t \in E^m (x_i = P_i(t)/Q_i(t))\}.$$

We have

Lemma 2.2. There is an algorithm to find polynomial sets $PS_1, ..., PS_t$ and polynomials $d_1, ..., d_t$ such that

$$IM(P,Q) = \cup_{i=1}^{t} Zero(PS_i/\{d_i\}). \tag{2.2.1}$$

Proof. It is obvious that $IM(P,Q) = \{(x_1, ..., x_n) \mid \exists t \in E^m (Q_i(t)x_i - P_i(t) = 0 \wedge Q_i(t) \neq 0)\}$. Thus by the quantifier elimination methods for algebraically closed fields (see, e.g., [Tarski, 1951] or [Wu, 1989]), we can find the PS_i and d_i such that (2.2.1) is correct. ∎

Definition 2.3. Let V be an irreducible variety of dimension $d > 0$ in E^n, then (2.1) is called a set of parametric equations of V (or (2.1) defines V) if

(1) $IM(P,Q) \subset V$; and

(2) $V - IM(P,Q)$ is contained in an algebraic set with dimension less than d.

Theorem 2.4. Each set of parametric equations of the form (2.1) defines a unique irreducible variety V in E^n whose dimension equals to the transendental degree of $K(P_1/Q_1, ..., P_n/Q_n)$ over K.

Proof. Let $I = \{F \in K[x] \mid F(P_1/Q_1, ..., P_n/Q_n) \equiv 0\}$, then I is a prime ideal with a generic point $\eta = (P_1/Q_1, ..., P_n/Q_n)$ and it is clear that $IM(P,Q) \subset Zero(I)$. We shall show that the irreducible variety $V = Zero(I)$ satisfies the condition of the theorem. We only need to prove $Zero(I) - IM(P,Q)$ is contained in an algebraic set of less dimension than the dimension of I. By (2.2.1), $IM(P,Q) = \cup_{i=1}^{t} Zero(PS_i/\{d_i\})$. Furthermore we can assume that for each PS_i, $Ideal(PS_i)$ (the ideal generated by PS_i) is a prime ideal and d_i is not in $Ideal(PS_i)$ by the decomposition theorem in algebraic geometry. Since $\eta \in IM(P,Q)$, η must be in some components, say in $Zero(PS_1/\{d_1\})$. Note that η is a generic point for I and $Zero(PS_1) \subset Zero(I)$, then $Ideal(PS_1) = I$. Hence $Zero(I) - IM(P,Q) = Zero(I \cup \{d_1\}) - \cup_{i=2}^{t} Zero(PS_i/\{d_i\})$. Thus $Zero(I) - IM(P,Q)$ is contained in $Zero(I \cup \{d_1\})$ the dimension of which is less than the dimension of I since d_1 is not contained in $I = Ideal(PS_1)$. Since η is a generic point of I, the dimension of I is equal to the transendental degree of $K(P_1/Q_1, ..., P_n/Q_n)$ over K. It is obvious that $Zero(I)$ is uniquely determined. ∎

By Theorem 2.4, a set of rational parametric equations of the form (2.1) defines a unique irreducible variety, hence a unique prime ideal in $K[x]$. We call this variety (or prime ideal) the *implicit variety* (*implicit prime ideal*) of (2.1).

3. The Computation of the Implicit Prime Ideal

For a set of rational parametric equations of the form (2.1), let

$$F_i = Q_i x_i - P_i, \quad D_i = Q_i z_i - 1, \ i = 1, ..., n. \tag{3.1}$$

where the z_i are new variables. Let

$$ID = Ideal(F_1, ..., F_n, D_1, ..., D_n) \tag{3.2}$$

i.e., the ideal generated by F_i and D_i in $K[t, x, z]$.

Theorem 3.3. We use the same notations as above. The implicit prime ideal of (2.1) is $ID \cap K[x_1, ..., x_n]$.

Proof. By the proof of Theorem 2.4, the implicit prime ideal of (2.1) is

$$I = \{F \in K[x] \mid F(P_1/Q_1, ..., P_n/Q_n) \equiv 0\}.$$

For $B \in I$, replacing P_i/Q_i by $x_i - F_i/Q_i$ in $B(P_1/Q_1, ..., P_n/Q_n) = 0$ and clearing denominators, we have

$$(\prod_{i=1}^{n} Q_i^{k_i}) B(x_1, ..., x_n) = \sum_{j=1}^{n} C_j F_j \tag{3.3.1}$$

where $C_j \in K[x, t]$. Multiplying both sides of (3.3.1) by $G = \prod_{i=1}^{n} z_i^{k_i}$, we have

$$(\prod_{i=1}^{n} (z_i Q_i)^{k_i}) B(x_1, ..., x_n) = \sum_{j=1}^{n} G C_j F_j \tag{3.3.2}$$

Since $D_i = Q_i z_i - 1$, (3.3.2) shows that $B(x_1, ..., x_n)$ can be expressed as linear combination of F_i and D_i. Therefore B is in $ID \cap K[x]$. Thus we have proved $I \subset ID \cap K[x]$. To prove the other direction, let $P \in ID \cap K[x]$. Then we have

$$P = \sum_{i=1}^{n} C_i F_i + \sum_{j=1}^{n} B_j D_j$$

Setting $x_i = P_i/Q_i$ and $z_i = 1/Q_i$ in the above formula, we have $P(P_1/Q_1, ..., P_n/Q_n) = 0$, i.e., P is in I. This completes the proof. ∎

Using the following Lemma and Theorem 3.3, we can compute a basis for the implicit prime ideal of (2.1)

Lemma 3.4. (Lemma 6.8 in [Buchberger, 1985]) Let GB be a Gröbner basis of an ideal $ID \subset K[x_1,...,x_n,y_1,...,y_k]$ in the pure lexicographic order $x_1 < ... < x_n < y_1 < ... < y_k$, then $GB \cap K[x_1,...,x_n]$ is a Gröbner basis of $ID \cap K[x_1,...,x_n]$.

Example 3.5. For example (1.1), let

$$PS = \{(v-u)x+v+u, (v-u)^2y-2v^2-2u^2, (v-u)^3z+2v^3+6u^2v, (v-u)z_1-1\} \quad (3.5.1)$$

Under the pure lexicographical order $x < y < z < u < v < z_1$, the Gröbner basis of $Ideal(PS)$ is

$$\{y-x^2-1, z-x^3+1, (x+1)v+(-x+1)u, 2uyz_1+x+1, 2vz_1+x-1\} \quad (3.5.2)$$

By Theorem 3.3 and Lemma 3.4, a basis of the implicit prime ideal of (1.1) is $\{y-x^2-1, z-x^3+1\}$.

Remark 3.6. (a) The inequation part $D_i = 0$ (which is equivalent to $Q_i \neq 0$) is essential for Theorem 3.3 to be true. In Example 3.5, let $PS' = PS - \{(v-u)z_1-1\}$, then the Gröbner basis GB' of $Ideal(PS')$ is

$$\begin{aligned}
&(z+2)v^3+6uv^2+18u^2v+(-x^3+6x^2-18x+13)u^3\\
&((z+2)u)v^2+6u^2v+(-x^3+4x^2-8x+5)u^3\\
&(y-2)v^2-4uv+(-x^2+4x-3)u^2\\
&((z+2)u^2)v+(-x^3+2x^2-2x+1)u^3\\
&((y-2)u)v+(-x^2+2x-1)u^2\\
&(x+1)v+(-x+1)u\\
&(z-x^3+1)u^3\\
&(y-x^2-1)u^2
\end{aligned}$$

Note that $GB' \cap K[x] = \emptyset$.

(b) If $m = 1$, then the D_i can be deleted from PS in (3.2) and Theorem 3.3 is still true. This is because $gcd(P_i, Q_i) = 1$ implies that the resultant of P_i and Q_i is 1.

The following are some results about the properties of the Gröbner basis for a prime ideal which will be used in the next two sections. For $S \subset \{x_1,...,x_n\}$, we denote $K[S]$ to be the polynomial ring of the variables in S. A set of variables S is called *independent* modulo a prime ideal $I \subset K[x]$ if $I \cap K[S] = \{0\}$. It is known that if S is a maximal independent set modulo I then $|S|$ is the dimension of I [Gröbner, 1970]. A maximal set of independent variables for a prime ideal I is called a *parameter set* of I.

Lemma 3.7. Let I be a prime ideal with a parameter set S and P be a polynomial not in I, then there is a nonzero polynomial $Q \in K[S] \cap Ideal(I \cup \{P\})$.

Proof. It is a direct consequence of the dimension theorem (p48, [Hartshorne, 1977]). ∎

The *leading variable* of a nonconstant polynomial $P \in K[x]$ is the smallest $i \leq n$ such that $P \in K[x_1,...,x_i]$.

Lemma 3.8. Let GB be a Gröbner basis of a prime ideal I in the pure lexicographical order $x_1 < ... < x_n$, and S be the set of distinct leading variables of the polynomials in GB, then $T = \{x_1, ..., x_n\} - S$ is a set of parameters of I and hence I is of dimension $|T|$.

Proof. Induction on the number of variables n. If $n = 1$, it is trivial. Suppose the lemma is true for $n = k-1$. Let I be a prime ideal in $K[x_1, ..., x_k]$ with the Gröbner basis GB, then by Lemma 3.4, $I' = I \cap K[x_1, ..., x_{k-1}]$ is also a prime ideal and $GB' = GB \cap K[x_1, ..., x_{k-1}]$ is a Gröbner basis for I'. Let S' be the set of the distinct leading variables of the polynomials in GB', then by the induction hypotheses, $T' = \{x_1, ..., x_{k-1}\} - S'$ is a parameter set for I'. If $GB = GB'$ then $I = I'$. The result is obviously true in this case. Otherwise the set of leading variables of the polynomials in GB is $S = \{x_k\} \cup S'$. Let $P \in GB - GB'$, then P is not in I'. Note that I' is also a prime ideal in $K[x_1, ..., x_k]$ with a parameter set $T' \cup \{x_k\}$, then by Lemma 3.7, there is a $P' \in Ideal(I' \cup \{P\}) \subset I$ involving the variables in the parameter set of I', i.e., involving $T' \cup \{x_k\}$, alone. Thus x_k is algebraic dependent on T' modulo I which implies that $\{x_1, ..., x_n\} - S = T'$ is also a parameter set of I and I has the same dimension as I'. ∎

Lemma 3.9. Let GB be the reduced Gröbner basis of a zero-dimension prime ideal I under the pure lexicographical order $x_1 < ... < x_n$, then $GB = \{A_1, ..., A_n\}$ where A_i is a polynomial of $x_1, ..., x_i$ with a power of x_i as its leading term.

Proof. Denote $I_i = I \cap K[x_1, ..., x_i]$. By Lemma 3.8, $I_i - I_{i-1}$ is not empty. Let $P_i \in I$ be a polynomial in $I_i - I_{i-1}$ with least leading term. The leading term of P_i must be a power of x_i, for otherwise Let $P_i = C_{n_i} x_i^{n_i} + ... + C_0$ where the C_i are in $K[x_1, ..., x_{i-1}]$. Since C_{n_i} is not in I_{i-1}, by Lemma 3.7, $1 \in Ideal(I_{i-1} \cup \{C_{n_i}\})$ or equivalently, $1 = G + BC_{n_i}$ where $G \in I_{i-1}$. Then the leading term of $P_i' = BP_i + Gx_i^{n_i} \in I_i - I_{i-1}$ is $x_i^{n_i}$ which contradicts the selection of P_i. Thus C_{n_i} is in K. It is easy to show that $\{P_1, ..., P_n\}$ is a Gröbner basis of I. ∎

4. The Independent Parameters

We will use the notations introduced in (2.1), (3.1), and (3.2).

Definition 4.1. The parameters $t_1, ..., t_m$ of (2.1) are called independent if the implicit prime ideal of (2.1) is of dimension m, or equivalently the transendental degree of the field $K(P_1/Q_1, ..., P_n/Q_n)$ over K is m (by Theorem 2.4).

Lemma 4.2. ID and $ID \cap K[t, x]$ are prime ideals of dimension m.

Proof. Similar to the proof of Theorem 3.3, we have

$$ID = \{P \in K[t, x, z] \mid P(t_1, ..., t_m, P_1/Q_1, ..., P_n/Q_n, 1/Q_1, ..., 1/Q_n) \equiv 0\}$$

i.e., ID is a prime ideal with a generic point $(t_1, ..., t_m, P_1/Q_1, ..., P_n/Q_n, 1/Q_1, ..., 1/Q_n)$. Therefore, the dimension of ID is m. Similarly,

$$ID \cap K[t, x] = \{P \in K[t, x] \mid P(t_1, ..., t_m, P_1/Q_1, ..., P_n/Q_n) \equiv 0\}.$$

Therefore $ID \cap K[t, x]$ is also a prime ideal of dimension m. ∎

Let GB be a Gröbner basis of ID in the pure lexicographical order $x_1 < ... < x_n < t_1 < ... < t_m < z_1 < ... < z_n$. Since ID and $ID \cap K[t,x]$ have the same dimension (Lemma 4.2), by Lemma 3.8, each z_i must be the leading variable for some polynomials in GB. Thus without loss of generality we can assume the leading variables of the polynomials in GB be $x_{d+1}, x_{d+2}, ..., x_n, t_{s+1}, t_{s+2}, ..., t_m, z_1, ..., z_n$. Therefore, $\{x_1, ..., x_d, t_1, ..., t_s\}$ is a parameter set of the prime ideal ID and $d+s$ is the dimension of ID, i.e., $d+s=m$, by Lemma 4.2. For the same reason $\{x_1, ..., x_d\}$ is a parameter set of the ideal $ID \cap K[x]$ and the dimension of $ID \cap K[x]$ is d. Summing up, we have

Theorem 4.3. (a) The implicit prime ideal of (2.1) is of dimension $d > 0$. (b) The parameters of (2.1) are independent iff $s = 0$, i.e., each t_i occurs as the leading variable for some polynomials in GB.

Proof. For (a), we only need to show $d > 0$. Since not all of P_i and Q_i are in K and $gcd(P_i, Q_i) = 1$, some x_i must dependent on the t effectively, i.e., we must have $d > 0$. Since $d + s = m$, the parameters of (2.1) are independent iff $d = m$, or $s = 0$. ∎

Theorem 4.4. If the parameters of (2.1) are not independent, we can find a set of new parametric equations

$$x_1 = P_1'/Q_1', \cdots, x_n = P_n'/Q_n' \tag{4.4.1}$$

which has the same implicit prime ideal as (2.1) and a set of independent parameters.

Proof. Use the notations introduced in the paragraph before Theorem 4.3. Then $\{ x_1, ..., x_d, t_1, ..., t_s \}$ $(d+s=m)$ is a parameter set for ID. Thus the ideal ID' generated by ID in

$$R = K(x_1, ..., x_d, t_1, ..., t_s)[x_{d+1}, ..., x_n, t_{s+1}, ..., t_m, z_1, ..., z_n]$$

is a prime ideal of zero dimension. By Lemma 3.9, a Gröbner basis of ID' under the pure lexicographical order $x_{d+1} < ... < x_n < t_{s+1} < ... < t_m < z_1 < ... < z_n$ is of the following form

$$\begin{aligned}
&A_1(x_{d+1}) \\
&\cdots \\
&A_{n-d}(x_{d+1}, ..., x_n) \\
&B_1(x_{d+1}, \cdots, x_n, t_{s+1}) \\
&\cdots \\
&B_{m-s}(x_{d+1}, \cdots, x_n, t_{s+1}, \cdots, t_m) \\
&C_1(x_{d+1}, ..., x_n, t_{s+1}, ..., t_m, z_1) \\
&\cdots \\
&C_n(x_{d+1}, ..., x_n, t_{s+1}, ..., t_m, z_1, ..., z_n)
\end{aligned} \tag{4.4.2}$$

where the leading term of each A_i (B_j and C_k) is a power of x_{d+i} (t_{s+j} and z_k) with coefficient 1. The coefficients of A_i, B_j and C_k are in $K(x_1, ..., x_d, t_1, ..., t_s)$. Let the least common divisor

of the denominators of the coefficients of the A_i, B_j, and C_k be M, then M is a polynomial of $x_1,...,x_d$ and $t_1,...,t_s$. Let $h_1,...,h_s$ be integers such that when replacing t_i by h_i, $i=1,...,s$, M becomes a nonzero polynomial M' of $x_1,...,x_d$. Let P_i' and Q_i' be polynomials obtained from P_i and Q_i by replacing t_i by h_i, $i=1,...,s$. In the next paragraph, we will show that $Q_i' \neq 0$. Thus we have obtained (4.4.1).

Let the implicit varieties defined by (4.4.1) and (2.1) be W and V respectively. We want to prove $W=V$. By the selection of h_i, it is clear that $W \subset V$. For each F_h, $h=1,...,n$, since $F_h \in ID'$, we have

$$F_h = \sum_{i=1}^{n-d} H_i A_i + \sum_{j=1}^{m-s} G_j B_j + \sum_{k=1}^{n} E_k C_k$$

where the H_i, G_j and E_k can be taken as ***polynomials*** in $K[t,x,z]$,because the leading terms of A_i, B_j, and C_k are powers of variables. Replacing t_i by h_i, $i=1,...,s$, in the above formula, we have

$$F_h' = \sum_{i=1}^{n-d} H_i' A_i + \sum_{j=1}^{m-s} G_j' B_j' + \sum_{k=1}^{n} E_k' C_k' \tag{4.4.3}$$

where $F_h' = Q_h' x_h - P_h'$. By the selection of h_i, B_j' and C_k' are well defined. Since $\{x_1,...,x_d\}$ is a parameter set of the implicit prime ideal whose zero set is V, there exists a generic zero $x_0=(x_1',...,x_n')$ of V such that $x_1',...,x_d'$ are independent variables over K. (It is easy to show that $A_1=0,...,A_{n-d}=0$ can determine such a generic zero.) Without loss of generality, we assume that the coefficients of B_j', as polynomials in R, have the form P/M' where P is a polynomial in $K[x_1,...,x_d]$ and M' is defined as the above paragraph. Then by the selection of the x_0, we can replace x by x_0 in B_j' and obtain a polynomial B_j''. B_j'' is a nonzero polynomial of $t_{s+1},...,t_j$ whose leading term is a power of t_j. Then $B_1''=0,...,B_{m-s}''=0$ can determine a set of solutions for $t_{s+1},...,t_m$. Let such a set of solutions be $t_{s+1}',...,t_m'$. Similarly, we can determine a set of solutions $z_1',...,z_n'$ for $z_1,...,z_n$ from $C_1',...,C_n'$. Now replacing x by x_0, t_i by t_i', $i=s+1,...,m$, and z_k by z_k', $k=1,...,n$, in (4.4.3), we have $Q_h''x_h' - P_h'' = 0$ where Q_h'' and P_h'' are obtained from Q_h' and P_h' by replacing t_i by t_i', $i=s+1,...,m$. Since $D_k = Q_k z_k - 1 \in ID'$, similar as above we can show that $Q_k'' z_k' - 1 = 0$. Thus $Q_k'' \neq 0$ (hence $Q_k' \neq 0$). Therefore we have $x_0 = (P_1''/Q_1'',...,P_n''/Q_n'')$, i.e., x_0 is in the image of (4.4.1) hence in W. This implies $V \subset W$. Thus we have proved $V=W$. Since V is of dimension d, by Theorem 4.3, the parameters $t_{s+1},...,t_m$ of (4.4.1) are independent. ∎

Example 4.5. In example (1.1), by (3.5.2), $\{x,u\}$ is a set of parameters of $Ideal(PS)$. Here $d=1, s=1$; hence the parameters u and v are not independent. To reparameterize (1.1), by Theorem 4.4, we need to compute the Gröbner basis of $Ideal(PS)$ in $K(x,u)[y,z,v,z_1]$ in the pure lexicographical order $y<z<v<z_1$. Such a Gröbner basis is

$$\{y-x^2-1, z-x^3+1, v+\frac{(-x+1)u}{(x+1)}, z_1+\frac{x+1}{2u}\}$$

Then the M in the proof of Theorem 4.4 is $2(x+1)u$. Selecting a value of u, say 1, which does not make M zero, we get a new parametric equation

$$x=\frac{v+1}{1-v}, y=\frac{2v^2+2}{(1-v)^2}, z=\frac{2v^3+6v}{(1-v)^3}$$

which has the same implicit prime ideal as (1.1) and has an independent parameter v.

5. Inversion Maps and Proper Parameterization

The inversion problem is that given a set of values $(a_1, ..., a_n)$ on the image of (2.1), find a set of values $(\tau_1, ..., \tau_m)$ for the t such that $a_i = P_i(\tau_1, ..., \tau_m)/Q_i(\tau_1, ..., \tau_m)$, $i = 1, ..., n$. The inversion problem can be reduced to an equation solving problem [Buchberger, 1987]. In the following, we show that in certain cases, we can find a closed form solution to the inversion problem.

Definition 5.1. *Inversion maps* for (2.1) are functions

$$t_1 = f_1(x_1, ..., x_n), ..., t_m = f_m(x_1, ..., x_n)$$

such that $x_i \equiv P_i(f_1, ..., f_m)/Q_i(f_1, ..., f_m)$ are true on the implicit variety V of (2.1) except a subset of V which has a lower dimension than that of V.

The inversion problem is closely related to whether a set of parametric equations is proper.

Definition 5.2. (2.1) is called *proper* if for each $(a_1, .., a_n) \in IM(P, Q)$ there exists only one $(\tau_1, ..., \tau_m) \in E^m$ such that $a_i = P_i(\tau_1, ..., \tau_m)/Q_i(\tau_1, ..., \tau_m)$, $i = 1, ..., n$.

Now we assume that the parameters $t_1, ..., t_m$ of (2.1) are independent, i.e., $s = 0$, then (4.4.2) becomes

$$\begin{aligned}
&A_1(x_{m+1}) \\
&\cdots \\
&A_{n-m}(x_{m+1}, \cdots, x_n) \\
&B_1(x_{m+1}, \cdots, x_n, t_1) \\
&\cdots \\
&B_m(x_{m+1}, \cdots, x_n, t_1, \cdots, t_m) \\
&C_1(x_{m+1}, \cdots, x_n, t_1 ..., t_m, z_1) \\
&\cdots \\
&C_n(x_{m+1}, \cdots, x_n, t_1 ..., t_m, z_1, ..., z_n)
\end{aligned} \tag{5.3}$$

Theorem 5.4. Using the same notations as above, we have

(a) $B_i(x, t_1, ..., t_i) = 0$ determine t_i $(i = 1, ..., m)$ as functions of $x_1, ..., x_n$ which are a set of inversion maps for (2.1).

(b) (2.1) is proper if and only if B_i are linear in t_i for $i = 1, ..., m$, and if this is case, the inversion maps are

$$t_1 = I_1/U_1, ..., t_m = I_m/U_m$$

where the I_i and U_i are polynomials in $K[X]$.

Proof. Similar to the proof of Theorem 4.4, let the least common divisor of the denominators of the coefficients of the A_i, B_j, and C_k be M, then M is a polynomial of $x_1, ..., x_d$. Let

$x' = (x'_1, ..., x'_n)$ be a zero on the implicit variety V of (2.1) such that $M(x') \neq 0$. Then similar to the proof of Theorem 4.4, we can show that $B_i(x', t_1, ..., t_i) = 0$, $i = 1, ..., m$, determine a set of values $t' = (t'_1, ..., t'_m)$ for the t_i and $C_k(x', t', z_1, ..., z_k) = 0$, $k = 1, ..., n$, determine a set of values $z' = (z'_1, ..., z'_n)$ for the z_i. Furthermore, (t', x', z') is a zero of ID (see (3.2)). Thus $F_h(t', x') = P_h(t')x'_h - Q_h(t') = 0$, i.e., $x'_h = P_h(t')/Q_h(t')$. Note that $Zero(M) \cap V$ has a lower dimension than that of V, we have proved (a).

To prove (b), first note that the $B_i = 0$ $(i = 1, ..., m)$ are the relations between the x and $t_1, ..., t_i$ in ID' which have the lowest degree in t_i. Also different solutions of $B_i = 0$ for the same x give same value for the x_i. Since (5.3) is a basis of a prime ideal ID', (b) comes from the fact that a point $x \in IM(P, Q)$ corresponds to one set of values for t_i iff B_i are linear in t_i, $i = 1, ..., m$. Let $B_i = I_i t_i - U_i$ where I_i and U_i are in $K[x]$ then the inversion maps are $t_i = U_i/I_i$, $i = 1, ..., m$. ∎

Theorem 5.4 gives a method to find the inversion maps and a method to decide whether the parametric equations are proper.

Remark. In the terminology of algebraic geometry, if (2.1) is proper, then the variety V defined by (2.1) is a rational variety, i.e., V is birational to E^m.

Theorem 5.5. If $m = 1$ and (2.1) is not proper, we can find a new parameter $s = f(t_1)/g(t_1)$ where f and g are in $K[t_1]$ such that the reparametrization of (2.1) in terms of s

$$x_1 = \frac{F_1(s)}{G_1(s)}, \ ..., \ x_n = \frac{F_n(s)}{G_n(s)} \tag{5.5.1}$$

are proper.

Proof. Since $m = 1$, (2.1) defines a curve C. Let $K' = K(P_1/Q_1, ..., P_n/Q_n)$ be the rational field of C. Note that $P_1(t_1) - Q_1(t_1)\lambda = 0$ where $\lambda = P_1(t_1)/Q_1(t_1) \in K'$, then t_1 is algebraic over K'. Let $f(y) = a_r y^r + ... + a_0$ be an irreducible polynomial $K'[y]$ for which $f(t_1) = 0$. Then at least one of a_i/a_r, say $\eta = a_s/a_r$, is not in K. By a proof of Lüroth's theorem (p149, [Walker, 1950]), we have $K' = K(\eta)$. This means that $x_i = P_i/Q_i$ can be expressed as rational functions of η and η also can be expressed as a rational function of $x_i = P_i/Q_i$, i.e., there is a one to one correspondence between the values of the $x_i = P_i/Q_i$ and η. Therefore η is the new parameter we seek. Now the only problem is how to compute the f.

By Theorem 5.4, we can find an inversion map $B_1(x_1, ..., x_n, t_1) = 0$ of the curve. Then B_1 is a relation between the x and t_1 with lowest degree in t_1 module the curve, in other words $B'_1(y) = B_1(P_1/Q_1, ..., P_n/Q_n, y) = 0$ is a polynomial in $K'[y]$ with lowest degree in y such that $B'_1(t_1) = 0$, i.e., $B'_1(y)$ can be taken as $f(y)$. So the s can be obtained as follows. If B_1 is linear in t_1 then (2.1) is already proper. We can take $s = t_1$. Otherwise let

$$B_1 = b_r t_1^r + \cdots + b_0$$

where the b_i are in $K[x]$. By (2.1), b_i can also be expressed as rational functions $a_i(t_1)$, $i = 1, ..., r$. At least one of a_i/a_r, say a_0/a_r, is not an element in K. Let $s = a_0/a_r$. Eliminating t_1 from (2.1) and $a_r s - a_0$, we can get (5.5.1). Note that a_i comes from b_i by substituting x_j by P_j/Q_j, $j = 1, ..., n$, then $s = b_0/b_r$ is an inversion map of (5.5.1). ∎

Theorem 5.5 provides a new constructive proof for Lüroth's Theorem, i.e., we have

Corollary 5.6. Let $g_1(t),...,g_r(t)$ be elements of $K(t)$, then we can find a $g(t) \in K(t)$ such that $K(g_1,...,g_r) = K(g)$.

Examples 5.7. Consider the parametric equations for a Bézier curve [Sederberg, 1986]:

$$x = \frac{8s^6 - 12s^5 + 32s^3 + 24s^2 + 12s}{s^6 - 3s^5 + 3s^4 + 3s^2 + 3s + 1} \tag{5.7.1}$$
$$y = \frac{24s^5 + 54s^4 - 54s^3 - 54s^2 + 30s}{s^6 - 3s^5 + 3s^4 + 3s^2 + 3s + 1}$$

Let $HS = \{(s^6 - 3s^5 + 3s^4 + 3s^2 + 3s + 1)x - (8s^6 - 12s^5 + 32s^3 + 24s^2 + 12s), (s^6 - 3s^5 + 3s^4 + 3s^2 + 3s + 1)y - (24s^5 + 54s^4 - 54s^3 - 54s^2 + 30s), (s^6 - 3s^5 + 3s^4 + 3s^2 + 3s + 1)z - 1\}$. Under the variable order $y < s < z$, the Gröbner basis of $Ideal(HS)$ in $K(x)[s, y, z]$ is

$g_1 = 224y^3 + (-2268x + 7632)y^2 + (-54x^2 - 1512x - 480384)y + 34263x^3 - 424224x^2 + 1200960x$

$g_2 = (15273x^2 + 1098792x - 9767808)s^2 + (7280y^2 + (-27006x - 125592)y - 174069x^2 + 598788x - 9767808)s - 7280y^2 + (27006x + 125592)y + 189342x^2 + 500004x$

$g_3 = (488736x + 39071232)x + (33488y^2 + (-95718x + 1701432)y - 712134x^2 + 9970488x - 34187328)s + 27888y^2 + (-81210x + 1297128)y - 584109x^2 + 8885196x - 39071232$

By Theorem 3.3 and Theorem 5.5, (5.7.1) is a set of improper parametric equations for the curve $g_1 = 0$. To find a set of proper parametric equations for $g_1 = 0$, by Theorem 5.5, we select a new parameter

$$t_1 = \frac{(7280y^2 + (-27006x - 125592)y - 174069x^2 + 598788x - 9767808)}{(15273x^2 + 1098792x - 9767808)} = \frac{s^2 + 1}{1 - s} \tag{5.7.2}$$

Eliminating s from (5.7.2) and (5.7.1), we have

$$x = \frac{8t_1^3 + 12t_1^2 - 36t_1 + 16}{t_1^3 + 3t_1^2 - 3t_1}, y = \frac{-24t_1^2 + 78t_1 - 54}{t_1^3 + 3t_1^2 - 3t_1} \tag{5.7.3}$$

By Theorem 5.5, we can easily check that (5.7.3) is a set of proper parametric equations of $g_1 = 0$ with an inversion map (5.7.2).

6. Conclusions

The main results of this paper can be summaries as follows.

For a set of rational parametric equations of the form (2.1), we have

(a) We can find a basis for the implicit prime ideal of (2.1).

(b) We can decide whether the parameters $t_1,...,t_m$ are independent, and if not, reparameterize (2.1) such that the parameters of the new parametric equations are independent.

(c) If the parameters of (2.1) are independent, we can construct a set of polynomial equations

$$B_1(x_1,...,x_n,t_1)=0,...,B_m(x_1,...,x_n,t_1,...,t_m)=0$$

the solution of the t_i in terms of the x_i are the inversion maps of (2.1), and (2.1) is proper iff the B_i are linear in t_i, $i=1,...,m$.

(d) If $m=1$ and (2.1) is not proper, we can reparameterize (2.1) such that the new parametric equations are proper.

The general case of (d), i.e., to decide weather the implicit variety of (2.1) is rational (or equivalently, birational to E^k for some k), and if it is, to find a set of proper reparametrization for (2.1), is still open. For the case $m=2$, see [Gao & Chou, 1990] for some partial results.

Reference.

Arnon, D.S. and Sederberg, T.W. (1984), Implicit Equation for a Parametric Surface by Gröbner Bases, *Proc. 1984 MACSYMA User's Conference* (V.E. Golden ed.), General Electric, Schenectady, New York, 431–436.

Artin, M. and Mumford, D. (1972), Some Elementary Examples of Unirational Varieties Which Are Non-rational, *Proc. London Math. Soc.*, (3) 25, pp. 75-95.

Buchberger, B. (1985), Gröbner bases: an algorithmic method in polynomial ideal theory, *Recent Trends in Multidimensional Systems theory* (ed. N.K. Bose), D.Reidel Publ. Comp., 1985.

Buchberger, B. (1987), Applications of Gröbner Bases in Non-linear Computational Geometry, L.N.C.S. No 296, R.JanBen (Ed.), pp. 52-80, Springer-Verlag.

Castelnuvo, (1894), Sulla Rationalita della Involuzioni Pinae, *Math. Ann.*, 44, pp. 125-155.

Gao, X.S. and Chou, S.C. (1990), Independent Parameters, Inversions and Proper Parameterization, TR-90-30, Computer Sciences Department, The Univ. of Texas at Austin, September, 1990.

Chuang, J.H., and Hoffman, C.M. (1989), On Local Implicit Approximation and Its Applications, *ACM Tran. in Graphics*, 8(4), pp. 298–324.

Faux, I.D. and Pratt, M.J. (1979), *Computational Geometry for Design and Manufacture*, Ellis Horwood, Chichester.

Gröbner, W.(1970), *Algebraic Geometrie I, II*, Bibliographisches Institut, Mannheim.

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

Kalkbrener, M.(1990), Implicitization of Rational Parametric Curves and Surfaces, *Proc. of AAECC-8*,, ACM, New York.

Li, Z.M. (1989), Automatic Implicitization of Parametric Objects, *MM Research Preprints*, No4, Ins. of Systems Science, Academia Sinica.

Sederberg, T.W. (1986), Improperly Parametrized Rational Curves, *Computer Aided Geometric Design*, vol. 3, pp. 67-75, 1986.

Sederberg, T.W., Anderson, D.C. and Goldman, R.N. (1984), Implicit Representation of Parametric Curves and Surfaces, *Computer Vision, Graph, Image Proc.*, vol28 pp 72–84.

Segre, B. (1951), Sull Esistenza, Sia Nel Campo Rationale chenel Campo Reale, *Rend. Accad. Naz. Lincei* (8) 10, pp. 564–570.

Tarski, A, (1951), *A Decision Method for Elementary Algebra and Geometry*, Univ. of California Press, Berkeley, Calif., 1951.

Walker, R. (1950), *Algebraic Curves*, Princeton Univ. Press.

Wu, W.T. (1989), On a Projection Theorem of Quasi-Varieties in Elimination Theory *MM Research Preprints*, No. 4, Ins. of Systems Science, Academia Sinica.