# Implicitization of Rational Parametric Equations*

XIAO-SHAN GAO
Institute of Systems Science, Academia Sinica, Beijing
SHANG-CHING CHOU
Department of Computer Science
Wichita State University,Wichita KS 67260, USA

21 January 1992

**Abstract**

Based on the Gröbner basis method, we present algorithms for a complete solution to the following problems in the implicitization of a set of rational parametric equations. (1) Find a basis of the implicit prime ideal determined by a set of rational parametric equations. (2) 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, reparameterize the parametric equations so that the new parametric equations have independent parameters. (4) Compute the inversion maps of parametric equations, and as a consequence, give a method to decide whether a set of parametric equations is proper. (5) In the case of algebraic curves, find a proper reparameterization for a set of improper parametric equations.

## 1 Introduction

For curves and surfaces, to transform their parametric equations to the implicit form are of fundamental importance in geometric modeling and computer graphics and many methods have been given to do this, see e.g. [Sederberg, 1984], [Arnon & Sederberg, 1984], [Chuang & Hoffmann, 1989], [Li, 1989], [Hoffmann, 1990], [Chionh, 1990], [Manocha & Canny, 1990], [Kalkbrener, 1990], and [Gao & Chou, 1991a,b]. However, in more general cases, many problems remain 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

*The work reported here was supported in part by the NSF Grants CCR-8702108 and CCR-917870.

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, since if we 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. Therefore, in the implicitization problem we should check whether the parameters of a set of parametric equations are independent, and if the parameters are not independent, reparameterize the parametric equations to make the new parameters independent.

In this paper we address the implicitization problem for rational parametric equations. Our algorithms are based on the Gröbner basis method, a powerful tool in computer algebra [Buchberger, 1985], which was introduced by Buchberger in 1965 to solve a system of polynomial equations and to determine whether a polynomial belongs to an ideal.

In [Buchberger, 1987] and [Shannon & Sweedler, 1988], a method was given to compute a basis of the implicit ideal (see Definition 2.2) for a set of *polynomial* parametric equations. But a straight forward extension of their method to the implicitization of *rational* parametric equations may not work (see the remark after Example 3.3.) because of the existence of base points. Various methods are designed to solve the implicitization problem for parametric equations with base points in the case of *rational surfaces* [Chionh, 1991], [Hoffmann, 1990], [Manocha & Canny, 1990]. In this paper, based on the Rabinowitsch's trick we present a method to find a basis of the implicit ideal for *general rational parametric equations* with or without base points. A similar method has also been presented independently in [Kalkbrener, 1990].

In the case of rational space surfaces, the independence of the parameters of parametric equations can be checked by counting the base points properly [Chionh, 1990]. In this paper, we present a method to decide the independence of the parameters in the general case. Furthermore, if the parameters of the parametric equations are not independent, we can reparameterize them so that the new parametric equations have independent parameters.

The inversion problem – given a point in the image of a set of parametric equations, to find a set of values for the parameters which corresponds to the given point – can be reduced to an equation solving problem [Buchberger, 1987]. In this paper, we present a method to find a closed form solution to the inversion problem, i.e., we give a method to compute the inversion maps of a set of parametric equations in the general form. As a consequence of our method, we can decide whether the parametric equations are proper or faithful, i.e.,

whether the implicit curves or surfaces are not multiply traced by the parametric equations. The inversion problem is also discussed in [Bajaj et al, 1988], section 6.2. Their method is for some special cases: (1) By using the Cramer's rule, the method only applies to faithful parametric equations. Our method can apply to more general cases (see Example 5.6). (2) Their method only applies to parametric equations with the same number of the parameters and parametric equations, because only in this case the "true image" of a hypersurface under the rational map defined by the parametric equations is also a hypersurface [Bajaj et al, 1988]. Most of the parametric equations used in geometric modeling fail to satisfy case (2).

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]. Sederberg gave a probabilistic method to find proper reparametrization for a set of improper parametric equations for algebraic curves [Sederberg 1986]. Manocha gave a deterministic method for improperly parametrized polynomial parametric equations [Manocha, 1990]. As an application of our method, we provide a deterministic method to find a proper reparametrization for a set of improper parametric equations of an algebraic curve. In the case of algebraic surfaces, if the base 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].

Finally, we remark that all the above tasks can be done by computing only one Gröbner basis. But in the case of *space rational surfaces* or in the more general case when the implicit variety is a hypersurface, the method based on computing the Gröbner basis is slow comparing with various specialized methods, e.g., the resultant methods [Bajaj et al, 1988], [Chionh, 1990], [Manocha et al, 1990] and the base conversion method [Hoffmann, 1990].

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

$$IM(P, Q) = \cup_{i=1}^{t} Zero(PS_i/\{d_i\}). \tag{2.1.1}$$

*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., [Heintz, 1983] or [Wu, 1989]), we can find the $PS_i$ and $d_i$ such that (2.1.1) is correct. ∎

**Definition 2** *The implicit ideal of (2.1) is*

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

*Zero(I) is called the implicit variety of (2.1).*

It is clear that $I$ is a prime ideal whose dimension equals to the transcendental degree of $K(P_1/Q_1, ..., P_n/Q_n)$ over $K$. The following result gives the relation between the image and the implicit variety of a set of parametric equations.

**Theorem 3** *Let $V$ be the implicit variety of (2.1) and $d$ the dimension of $V$, then*

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

*(2) $V - IM(P,Q)$ is a quasi variety with dimension less than $d$. Furthermore, we can find this quasi variety.*

*Proof.* (1) is clear from the definitions. By (2.1.1), $IM(P,Q) = \cup_{i=1}^{t} Zero(PS_i/\{d_i\})$. We can further 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 $Ideal(PS_i)$. Let $I$ be the implicit ideal of (2.1). Since $\eta = (P_1/Q_1, ..., P_n/Q_n) \in IM(P,Q)$, $\eta$ must be in some components of $IM(P,Q)$, say in $Zero(PS_1/\{d_1\})$. Note that $\eta$ is a generic point for $V$ and $Zero(PS_1) \subset V$, then $Zero(PS_1) = V$ and $Ideal(PS_1) = I$. Hence $V - IM(P,Q) = Zero(I \cup \{d_1\}) - \cup_{i=2}^{t} Zero(PS_i/\{d_i\})$. Since $d_1$ is not in $I$, the dimension of $Zero(I \cup \{d_1\})$ is less than $d$. ∎

# 3 The Computation of Implicit Ideals

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 the $F_i$ and $D_i$ in $K[t, x, z]$.

**Theorem 4** *We use the same notations as above. The implicit ideal of (2.1) is $ID \cap K[x_1, ..., x_n]$.*

*Proof.* The implicit 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

$$(\prod_{i=1}^{n} Q_i^{k_i}) B(x_1, ..., x_n) = \sum_{j=1}^{n} C_j F_j \tag{3.1.1}$$

where $C_j \in K[x, t]$. Multiplying both sides of (3.1.1) by $G = \prod_{i=1}^{n} z_i^{k_i}$, we have

$$(\prod_{i=1}^{n} (z_i Q_i)^{k_i}) B(x_1, ..., x_n) = \sum_{j=1}^{n} G C_j F_j \tag{3.1.2}$$

Since $D_i = Q_i z_i - 1$, (3.1.2) shows that $B(x_1, ..., x_n)$ can be expressed as linear combination of $F_i$ and $D_i$. Therefore $B$ is in $ID \cap K[x]$. 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 $x_i = P_i/Q_i$, $z_i = 1/Q_i$ in the above formula, we have $P(P_1/Q_1, ..., P_n/Q_n) \equiv 0$, i.e., $P$ is in $I$. This completes the proof. ∎

Using the following Lemma and Theorem 3.1, we can compute a basis for the implicit ideal of (2.1)

**Lemma 5** *(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 6** *For parametric equations (1.1), let*

$$PS = \{(v-u)x+v+u, (v-u)^2y-2v^2-2u^2, (v-u)^3z+2v^3+6u^2v, (v-u)z_1-1\} \quad (3.3.1)$$

*Note that we can omit $(u-v)^2z_2 - 1, (u-v)^3z_3 - 1$ because of the appearance of $(v-u)z_1 - 1$. Under the pure lexicographical order $x < y < z < u < v < z_1$, the Gröbner basis of $Ideal(PS)$ is*

$$\{y-x^2-1, z-x^3+1, (x+1)v+(-x+1)u, 2uyz_1+x+1, 2vz_1+x-1\} \quad (3.3.2)$$

*By Theorem 3.1 and Lemma 3.2, a basis of the implicit ideal of (1.1) is $\{y - x^2 - 1, z - x^3 + 1\}$.*

**Remark** The inequation part $D_i = 0$ (which is equivalent to $Q_i \neq 0$) is essential for Theorem 3.1 to be true. In Example 3.3, let $PS' = PS - \{(v-u)z_1 - 1\}$, then the Gröbner basis $GB'$ of $Ideal(PS')$ is

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

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

The following are some well known 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 $I$. A maximal set of independent variables for a prime ideal $I$ is called a *parameter set* of $I$.

**Lemma 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 8** *Let $GB$ be a Gröbner basis of a prime ideal $I$ in the 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.* See [Kredel et al, 1989]. ∎

**Lemma 9** *Let $GB$ be the reduced Gröbner basis of a zero-dimension prime ideal $I$ in 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.* See Proposition 5.5 and 5.9 in [Gianni et al, 1988]. ∎

**Lemma 10** *Let $GB$ be the reduced Gröbner basis of a prime ideal $I$ under the lexicographical order $x_1 < ... < x_n$, and $S$ be the parameter set of $I$, then the Gröbner basis of the ideal generated by $I$ in $K(S)[T]$, $(T = \{x_1, ..., x_n\} - S)$, is $\{P \mid$ for each $x_{i_0}$ in $T$, $P \in GB$ is the least polynomial with $x_{i_0}$ as its leading variable $\}$.*

*Proof.* It is a consequence of Lemma 3.4. ∎

# 4 The Independent Parameters

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

**Definition 11** *The parameters $t_1, ..., t_m$ of (2.1) are called independent if the implicit ideal of (2.1) is of dimension $m$, or equivalently the transcendental degree of $K(P_1/Q_1, ..., P_n/Q_n)$ over $K$ is $m$ (by Theorem 2.3).*

**Lemma 12** *$ID$ and $ID \cap K[t, x]$ are prime ideals of dimension $m$.*

*Proof.* Similar to the proof of Theorem 3.1, 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 $(t_1, ..., t_m, P_1/Q_1, ..., P_n/Q_n, 1/Q_1, ..., 1/Q_n)$ as a generic point. 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 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 3.5, 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 13** *(a) The implicit 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 14** *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 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 3.6 and Lemma 3.7, a Gröbner basis of $ID'$ under the lexicographical order $x_{d+1} < ... < x_n < t_{s+1} < ... < t_m < z_1 < ... < z_n$ can be found and is of the following form

$$A_1(x_{d+1})$$

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

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 $M$ be the least common divisor of the denominators of the coefficients of the $A_i$, $B_j$, and $C_k$, 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 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 $D_k = Q_k z_k - 1 \in ID'$, similarly 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 15** *In example (1.1), by (3.3.2),* $\{x, u\}$ *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

**Definition 16** 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 or faithful.

**Definition 17** *(2.1) is called* proper *if, except a subset of* $IM(P, Q)$ *which has lower dimension, 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

$$\begin{array}{l} A_1(x_{m+1}) \\ \cdots \\ A_{n-m}(x_{m+1}, \cdots, x_n) \end{array}$$

$$
\begin{array}{l}
B_1(x_{m+1}, \cdots, x_n, t_1) \\
\cdots \\
B_m(x_{m+1}, \cdots, x_n, t_1, \cdots, t_m) \\
C_1(x_{m+1}, \cdots, x_n, t_1 ..., t_m, z_1) \\
\cdots \\
C_n(x_{m+1}, \cdots, x_n, t_1 ..., t_m, z_1, ..., z_n)
\end{array} \tag{5.1}
$$

**Theorem 18** *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*

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

*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)) which implies that $Q_i(t') \neq 0$. 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 (5.1) is a basis of a zero dimensional prime ideal $ID'$, for a generic zero $x'$ on the implicit variety $V$, $B_i(x', t_1, ..., t_i) = 0$, $i = 1, ..., m$, have no repeated roots for the $t_i$. Therefore 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 5.3 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 19** *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 $s$*

$$x_1 = \frac{F_1(s)}{G_1(s)}, \ ..., \ x_n = \frac{F_n(s)}{G_n(s)} \tag{5.4.1}$$

*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 $\eta$ and $\eta$ 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 $\eta$. Therefore $\eta$ is the new parameter we seek. Now the only problem is how to compute the $f$.

By Theorem 5.3, 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 (5.4.1). 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 (5.4.1). ∎

Theorem 5.4 provides a new constructive proof for Lüroth's Theorem, i.e., we have

**Corollary 20** *Let $g_1(t), ..., g_r(t)$ be elements of $K(t)$, then we can find a $g(t) \in K(t)$ such that $K(g_1, ..., g_r) = K(g)$.*

**Example 21** *Consider the parametric equations for a Bézier curve [Sederberg, 1986]:*

$$\begin{aligned} x &= \tfrac{8s^6-12s^5+32s^3+24s^2+12s}{s^6-3s^5+3s^4+3s^2+3s+1} \\ y &= \tfrac{24s^5+54s^4-54s^3-54s^2+30s}{s^6-3s^5+3s^4+3s^2+3s+1} \end{aligned} \tag{5.6.1}$$

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

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

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

$q_3 = (488736x+39071232)z+(33488y^2+(-95718x+1701432)y-712134x^2+9970488x-34187328)s+27888y^2+(-81210x+1297128)y-584109x^2+8885196x-39071232$

Since (5.6.1) defines a plane curve, by Theorem 3.1 and Theorem 5.4, (5.6.1) is a set of improper parametric equations for the curve $g_1 = 0$. An inversion map of (5.6.1) can be obtained by solving $g_2 = 0$ as a quadratic equation of $s$. To find a set of proper parametric equations for $g_1 = 0$, by Theorem 5.4, we select a new parameter

$$t_1 = \frac{(7280y^2 + (-27006x - 125592)y - 174069x^2 + 598788x - 9767808)}{(15273x^2 + 1098792x - 9767808)} = \frac{s^2+1}{1-s} \tag{5.6.2}$$

Eliminating $s$ from (5.6.2) and (5.6.1), we have

$$x = \frac{8t_1^3 + 12t_1^2 - 36t_1 + 16}{t_1^3 + 3t_1^2 - 3t_1}, y = \frac{-24t_1^2 + 78t_1 - 54}{t_1^3 + 3t_1^2 - 3t_1} \tag{5.6.3}$$

By Theorem 5.4, we can easily check that (5.6.3) is a set of proper parametric equations of $g_1 = 0$ with an inversion map (5.6.2).

# 6 Conclusions

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

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

(b) We can decide whether the parameters $t_1, ..., t_m$ of (2.1) are independent, and if not, reparameterize (2.1) so 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. In the case $m = 2$, see [Gao & Chou, 1991b] for further discussions.

# References


[1] 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.), New York, 431–436.

[2] 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.

[3] Bajaj, C., Garrity, T. and Warren, J. (1988). On the Applications of multi-equational resultants, Tech. Report CSD-TR-826, Dep. of Comp. Sci., Purdue University, 1988.

[4] 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.

[5] 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.

[6] Castelnuvo, (1894). Sulla Rationalita della Involuzioni Pinae, *Math. Ann.*, 44, pp. 125–155.

[7] Chionh, E.W. (1990). *Base Points, Resultants, and the Implicit Representation of Rational Surfaces*, Phd Thesis, The Univ. of Waterloo.

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

[9] Gao, X.S. and Chou, S.C. (1991a). On the Normal Parameterization of Curves and Surfaces, *The International Journal of Computational Geometry & Applications*, vol. 1, p.125-136, 1991, World Science Press.

[10] Gao, X.S. and Chou, S.C. (1991b). Computations with Parametric Equations, *Proc. of ISSAC'91*, ACM Press, New York, pp.122-127.

[11] Gianni, P., Trager, B. and Zacharias, G. (1988). Gröbner Bases and Primary Decomposition of Polynomial Ideals, *J. of Symbolic Computation*, vol.6, pp. 149–168.

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

[13] Heintz, J. (1983). Definability and Fast Quantifier Elimination in Algebraically Closed Fields, Theoretic Computing Science, 24, 239–278.

[14] Hoffmann, C.M. (1990). Algebraic and Numeric Techniques for Offsets and Blends, in *Computations of Curves and Surfaces*, (eds. W. Dahman), p.499-529, Kluwer Academic Publishers.

[15] Kalkbrener, M.(1990). Three Contributions to Elimination Theory, Phd Thesis, RISC, Kepler Unin. of Linz, Austria.

[16] Kredel, H. and Weipfenning, V. (1989). Computing dimension and independent sets for polynomial ideals, *J. Symb. Comp.*, 6(2&3),p.213-248, 1988.

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

[18] Manocha, D. (1990). Regular Curves and Proper Parametrizations, *Proc. of ISSAC-90*, p.271-276, ACM Press.

[19] Manocha, D. and Canny J. F. (1990). Implicitizing Rational Parametric Surfaces, Tech. Report, UCB/CSD, September, The univ. of California at Berkeley.

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

[21] 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.

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

[23] Shannon, S. and Sweedler, M. (1988). Using Gröbner Bases to Determine Algebraic Membership, *J. Symbolic Computation*, 6, p. 267-273.

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

[25] 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.