INDEPENDENT PARAMETERS, INVERSIONS AND PROPER PARAMETERIZATION*

Xiao-Shan Gao† and Shang-Ching Chou

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

TR-90-30 September 1990

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

† On leave from Institute of Systems Science, Academia Sinica, Beijing.

Independent Parameters, Inversions and Proper Parameterization*

Xiao-Shan Gao† and Shang-Ching Chou

Department of Computer Sciences
The University of Texas at Austin, Austin, Texas 78712 USA

Abstract. In this paper, we give a method to find a set of independent parameters as well as the implicit equations for a set of parametric equations. We also present a method to compute inversion maps of parametric equations with independent parameters and as a consequence, we can decide whether the parametric equations are proper. A new method to find proper parametric equations for rational algebraic curves is given. The problem of finding proper parametric equations for algebraic surfaces are also discussed.

Keywords. Computer modeling, parametric equations, inversion maps, independent parameters, proper parametric equations.

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

† On leave from Institute of Systems Science, Academia Sinica, Beijing.

1. Introduction

Methods of converting parametric equations to their implicit equations 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 have been presented. The first method is based on elimination theories [Sederberg, 1984]. The second method is based on Gröbner bases [Arnon & Sederberg, 1984] and [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, 1990] and [Li, 1990]. But the following example shows that in general case, the parameters may not be independent. At first sight, one may think that the parametric equations

$$x = u + v,\ y = u^2 + v^2 + 2uv - 1,\ z = u^3 + v^3 + 3u^2v + 3v^2u + 1 \tag{1.1}$$

represent a space surface. Actually, they represent a space curve, because let $t = u + v$, 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 concept of the inversion map here is not clear. This paper will address the implicitization problem for this kind of parametric equations.

In this paper, we give a method to find a group of independent parameters as well as the implicit equations for a set of parametric equations. We also present a method to compute the inversion map of parametric equations with independent parameters and as a consequence, we can decide whether the parametric equations are proper, i.e., whether the curves or surfaces are multiply traced by the parametric equations [Faux and Pratt 1979].

If the parametric equations are not proper, naturally we may ask whether we can reparameterize them so that the new parametric equations are proper. Generally speaking, the answer is negative. However, in the case of algebraic curve, this is true by Lüroth's theorem [Walker, 1950] and a constructive proof of Lüroth's theorem actually provides an algorithm to construct a set of proper parametric equations. Recently, Sederberg gives a new solution to the problem of finding proper parametric equations in the case of algebraic curves [Sederberg 1986]. In this paper, we shall show that as an application of our method, we can also find a proper reparametrization for a set of 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.

For the case of algebraic surfaces, if the ground field K is the complex 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 $\mathbf{Q}$ or $\mathbf{R}$ this need not to be the case [Segre 1951]. If the variety represented by the parametric equations are of dimension > 2 then even for $K = \mathbf{C}$ some improper parametric equations do not exist proper reparametrization [Artin & Mumford 1971]. As far as we know there exists no constructive proof for Castelnuvo's theorem. We show that by using a similar method for the case of curves, we can find proper parametric equations for certain kind of improper parametric equations of surfaces or variety of higher dimensions.

This paper is organized as follows. In section 2, we give some basic definitions and properties of parametric equations. We also give the main theorem of this paper. In section 3, we give a proof of the main theorem. In the appendix, we give a brief introduction to Ritt-Wu's decomposition algorithm which is the computation tool of our algorithm.

2. Preliminaries on Parametric Equations

Let K be a computable field of characteristic zero. 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 nonzero polynomials $P_1, ..., P_n, Q_1, ..., Q_n$ in $K[t_1, ..., t_m]$, we call

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

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. We can find polynomial sets PS_i and polynomials d_i, $i = 1, ..., t$, such that

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

Proof. It is obvious that

$$IM(P, Q) = \{(x_1, ..., x_n) \mid \exists t_1, \cdots \exists t_m (O_i(t)x_i - P_i(t) = 0 \wedge Q_i(t) \neq 0)\}.$$

Thus by a quantifier elimination theory for the field of algebraically closed field [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. Parametric equations of the form (2.1) are called parameter 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 in E^n whose dimension equals to the transendental degree of $K(P_1/Q_1, ..., P_n/Q_n)$ over K.

Proof. Let $I = \{F \in K[x] \mid F(P_1/Q_1, ..., P_n/Q_n) = 0\}$, 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 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), $IM(P,Q) = \cup_{i=1}^{l} Zero(PS_i/\{d_i\})$. Furthermore we can assume that each PS_i is a prime ideal and d_i is not in 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 $PS_1 = I$. Hence $Zero(I) - IM(P,Q) = Zero(I \cup \{d_1\}) - \cup_{i=2}^{l} Zero(PS_i/\{d_i\})$. 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 $I = PS_1$. 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. ∎

Definition 2.5. The parameters $t_1, ..., t_m$ of (2.1) are called independent if (2.1) define a variety of dimension m, or equivalently the transendental degree of $K(P_1/Q_1, ..., P_n/Q_n)$ over K is m.

Definition 2.6. *Inversion maps* for (2.1) are functions

$$t_1 = f_1(x_1, ..., x_n), ..., t_m = f_m(x_1, ..., x_n) \tag{2.6.1}$$

such that $x_i = P_i(f_1, ..., f_m)/Q_i(f_1, ..., f_m)$ on $IM(P,Q)$, i.e., functions which give the parameter values corresponding to points on the image of (2.1).

Definition 2.7. A set of parametric equations (2.1) for a variety V is called *proper* if there is a one to one correspondence between the points on V and the values of the t_i except for a subset of V and a subset of the E^m (where the t_i take values) both with lower dimensions than that of V.

The main result of this paper is

Main Theorem. For a set of parametric equations of the form (2.1),

(a) 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;

(b) if the parameters of (2.1) are independent, we can construct a set of inversion maps of the form (2.6.1) for (2.1), and (2.1) are proper if and only if the f_i are rational functions of $x_1, ..., x_n$;

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

3. A Proof of the Main Theorem

In this section, we shall use some results about Ritt-Wu's decomposition algorithm, a brief introduction of which can be found in the appendix of this paper.

3.1. The Independent Parameters

For a set of parametric equations

$$x_1 = \frac{P_1}{Q_1}, \ \ldots, \ x_n = \frac{P_n}{Q_n} \tag{3.1}$$

where P_i and Q_i are in $K[t_1, \cdots, t_m]$, let $PS = \{F_1, \cdots, F_n\}$ where $F_i = Q_i x_i - P_i$, $i = 1, ..., n$, $DS = \{Q_1, \cdots, Q_n\}$. It is obvious that

$$IM(P,Q) = \{(x_1, ..., x_n) \mid \exists (t_1, \cdots, t_m), (t_1, \cdots, t_m, x_1, \cdots, x_n) \in Zero(PS/DS)\} \tag{3.2}$$

Note that under the variable order $t_1 < \cdots < t_m < x_1 < \cdots < x_n$, $PS = \{F_1, \cdots, F_n\}$ is an irreducible asc chain in $K[t, x]$. By Theorem 4.3, $PD(PS)$ is a prime ideal of dimension m. Note that DS is the set of initials of the asc chain PS, then by (4.1.1) we have

$$Zero(PS/DS) = Zero(PD(PS)/DS).$$

Let ASC be a characteristic set of $PD(PS)$ under the variable order $x_1 < \cdots < x_n < t_1 < \cdots < t_m$. Since $PD(ASC) = PD(PS)$, we have

$$Zero(PS/DS) = Zero(PD(ASC)/DS). \tag{3.3}$$

ASC can be obtained by Theorem 4.6. By Theorem 4.3, ASC is irreducible with dimension m. Hence ASC contains n polynomials. Then by changing the order of the variables properly, we can assume ASC to be

$$\begin{array}{l} A_1(x_1, \cdots, x_{d+1}) \\ \cdots \\ A_{n-d}(x_1, \cdots, x_n) \\ B_1(x_1, \cdots, x_n, t_1, \cdots, t_{s+1}) \\ \cdots \\ B_{m-s}(x_1, \cdots, x_n, t_1, \cdots, t_m) \end{array} \tag{3.4}$$

where $d + s = m$. Note that the parameter set of ASC is $\{x_1, ..., x_d, t_1, ..., t_s\}$

Lemma 3.5. The transendental degree of $K' = K(P_1/Q_1, \cdots, P_n/Q_n)$ over K is $d = m - s > 0$.

Proof. By (3.1), the transendental degree of $K' = K(P_1/Q_1, \cdots, P_n/Q_n)$ over K is the maximal number of the independent quantities $x_1 = P_1/Q_1, ..., x_n = P_n/Q_n$, hence is d by (3.4). Since not all of P_i and Q_i are constants in K and $gcd(P_i, Q_i) = 1$, some x_i must dependent on the t effectively. Hence $d = m - s > 0$. ▮

By Definition 2.5, we have

Corollary 3.5.1. The parameters of (3.1) are independent iff $s = 0$.

Theorem 3.6. (3.1) defines the irreducible variety $V = Zero(PD(A_1, \cdots, A_{n-d}))$.

Proof. By Theorem 2.4 and Lemma 3.5, (3.1) defines a variety W of dimension d. By (3.2) and (3.3), it is clear that $IM(P,Q) \subset V$. Then $W \subset V$. By Theorem 4.3, V is also of dimension d. Therefore $V = W$. ▮

For example (1.1), let $HS = \{x - u - v, y - u^2 - v^2 - 2uv + 1, z - u^3 - v^3 - 3u^2v - 3v^2u - 1\}$. By Theorem 4.6, under the variable order $x < y < z < u < v$, we have $Zero(HS) = Zero(PD(ASC_1))$ where

$$ASC_1 = \{y - x^2 + 1, z - x^3 - 1, v + u - x\}. \tag{3.6.1}$$

By Theorem 3.6, (1.1) defines a curve $Zero(y - x^2 + 1, z - x^3 - 1)$. Note that $s = 1$, then the variable u and v are not independent.

Theorem 3.7. Use the same notations as above. If $s > 0$, we can find integers $h_1, ..., h_s$ such that

$$x_1 = P_1'/Q_1', \cdots, x_n = P_n'/Q_n' \tag{3.7.1}$$

defines the same irreducible variety as (3.1) and with independent parameters $t_{s+1}, ..., t_m$, where P_i' and Q_i' are polynomials obtained from P_i and Q_i by replacing t_i by h_i, $i = 1, ..., s$.

Proof. Suppose we already have (3.4). By Theorem 4.5, we can assume the initial I_i of B_i and the initial J_j of A_j in (3.4) are polynomials of the parameters of ASC, i.e., $x_1, ..., x_d, t_1, ..., t_s$. Since Q_i is not in $PD(F_1, ..., F_n) = PD(ASC)$, by Lemma 4.4 we can find a nonzero polynomial q_i of the parameters of ASC, i.e., $x_1, ..., x_d$ and $t_1, ..., t_s$, such that

$$q_i \in Ideal(A_1, ..., A_{n-d}, B_1, ..., B_{m-s}, Q_i). \tag{3.7.2}$$

Let $M = \prod_{i=1}^{m-s} I_i \cdot \prod_{j=1}^{n} q_j$, and $h_1, ..., h_s$ be integers such that when replacing t_i by h_i, $i = 1, ..., s$, M becomes a nonzero polynomial of $x_1, ..., x_d$.

We assume that (3.7.1) defines a variety W and (3.1) defines a variety V. By the selection of h_i, it is clear that the image of (3.7.1) is contained in the image of (3.1). Therefore, we have $W \subset V$ by Definition 2.3. Since (3.4) is a characteristic set of $PD(F_1, ..., F_n)$, for each F_k, by (4.1) we have

$$JF_k = \sum_{i=1}^{n-d} G_i A_i + \sum_{j=1}^{m-s} C_j B_j$$

where J is a product of powers of the initials of A_i and B_j. Hence J is a polynomial of $x_1, ..., x_d$ and $t_1, ..., t_s$. Replacing t_i by h_i, $i = 1, ..., s$, in the above formula, we have

$$J'F'_k = \sum_{i=1}^{n-d} G'_i A_i + \sum_{j=1}^{m-s} C'_j B'_j \tag{3.7.3}$$

where $F'_k = Q'_k x_k - P'_k$. By the selection of h_i, $J' \neq 0$ is a polynomial of $x_1, ..., x_d$. By Theorem 3.6, $V = Zero(PD(A_1, ..., A_{n-d}))$ has a generic zero $x_0 = (x'_1, ..., x'_n)$ such that $x'_1, ..., x'_d$ are independent variables over K. Let B''_i be obtained from B'_i by replacing the x by x_0. Since the initial I'_i of B'_i is a polynomial of $x_1, ..., x_d$, B''_i is a nonzero polynomial of $t_{s+1}, ..., t_i$ with with nonzero initials which are free of $t_{s+1}, ..., t_m$. Then $B''_1 = 0, ..., B''_{m-s} = 0$ have solutions for $t_{s+1}, ..., t_m$. Let such a set of solutions be $t'_{s+1}, ..., t'_m$. Now replacing x by x_0 and t_i by t'_i, $i = s+1, ..., m$ in (3.7.3), we have $J''F''_k = 0$. Since J' is polynomial of $x_1, ..., x_d$, $J'' \neq 0$ by the selection of x_0. Thus $F''_k = Q''_k x'_k - P''_k = 0$. Since q_i is a polynomial of $x_1, ..., x_d$ and $t_1, ..., t_s$, by (3.7.2) $Q''_k \neq 0$. Hence $x_0 = (P''_1/Q''_1, ..., P''_n/Q''_n)$ is in $IM(P', Q') \subset W$. As x_0 is a generic zero of V, we have $V \subset W$. We have proved $V = W$. Since (3.7.1) defines a variety of dimension d, by Corollary 3.5.1, the parameters $t_{s+1}, ..., t_m$ of (3.7.1) are independent. ▮

For Example (1.1), by (3.6.1), M in the proof of Theorem 3.7 is 1. Hence u can take any integers, say 1. (1.1) becomes

$$x = v + 1,\ y = v^2 + 2v,\ z = v^3 + 3v^2 + 3v + 2$$

which defines the same curve as (1.1) and has an independent parameter v.

3.2. Inversion Maps and Proper Parameterization

Now let us assume that the parameters $t_1, ..., t_m$ of (3.1) are independent, i.e., $s = 0$, then (3.4) becomes

$$\begin{array}{l} A_1(x_1, \cdots, x_{m+1}) \\ \cdots \\ A_{n-m}(x_1, \cdots, x_n) \\ B_1(x_1, \cdots, x_n, t_1) \\ \cdots \\ B_m(x_1, \cdots, x_n, t_1, \cdots, t_m) \end{array} \tag{3.8}$$

Theorem 3.9. Using the same notations as above, we have

(1) $B_i(x, t_1, ..., t_i) = 0$, $i = 1, ..., m$, determine t_i, $i = 1, ..., m$, as functions of $x_1, ..., x_n$ which are a set of inversion maps for (3.1).

(2) (3.1) are proper if and only if B_i are linear in t_i, $i = 1, ..., m$, and if this is true, 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 of the x.

Proof. Note that $B_i = 0$, $i = 1, ..., m$, are the relations between the x and $t_1, ..., t_i$ in $PD(PS)$ which has the lowest degree in t_i. Hence a set of solutions of t_i in terms of the x of the equations $B_i(x, t_1, ..., t_i) = 0$, $i = 1, ..., m$ gives a set of inversion maps for (3.1). The second conclusion of theorem 3.9 comes from the fact that a point x of the variety V defined by (3.1) corresponds to one set of parameter values if and only if 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 $t_i = U_i/I_i$, $i = 1, ..., m$. ∎

So we have a method to find the inversion maps and a method to decide whether the parametric equations are proper.

Remark From mathematical point of view if (3.1) are proper, then the variety V defined by (3.1) is a rational variety, i.e., V is birational to E^m.

Theorem 3.10. If $m = 1$ and (3.1) are 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 (3.1) in terms of s

$$x_1 = \frac{F_1(s)}{G_1(s)}, \ ..., \ x_n = \frac{F_n(s)}{G_n(s)} \tag{3.10.1}$$

are proper.

Proof. Since $m = 1$, (3.1) defines a curve C. Let $K' = K(P_1/Q_1, ..., P_n/Q_n)$ be the rational field of the curve 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 $f(x) = a_r x^r + ... + a_0$ be an irreducible polynomial over K' 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 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., η is the new parameter we seek. Now the only problem is how to compute the f.

By Theorem 3.9, 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 $B_1'(x) = B_1(P_1/Q_1, ..., P_n/Q_n, x) = 0$ is a polynomial in $K'[x]$ with lowest degree in x such that $B_1'(t_1) = 0$, i.e., $B_1'(x)$ can be taken as f. So the s can be obtained as follows. If B_1 is linear in t_1 then (3.1) are 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 (3.1), 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 (3.1) and $a_r s - a_0$, we can get (3.10.1). Note that a_i comes from b_i by substituting x_j by P_j/Q_j, $j = 1, ..., n$, then $b_r s - b_0 = 0$ is an inversion map of (3.10.1). ∎

Theorem 3.10 also provides a new constructive proof for Lüroth's Theorem, i.e., we have

Corollary 3.11. 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 3.12. Consider the parametric equations for a Bézier curve [Sederberg, 1986]:

$$x = \frac{8s^6 - 12s^5 + 32s^3 + 24s^2 + 12s}{s^6 - 3s^5 + 3s^4 + 3s^2 + 3s + 1} \tag{3.12.1}$$
$$y = \frac{24s^5 + 54s^4 - 54s^3 - 54s^2 + 30s}{s^6 - 3s^5 + 3s^4 + 3s^2 + 3s + 1}$$

Let $HS = \{(s^6 - 3s^5 + 3s^4 + 3s^2 + 3s + 1)x - (8s^6 - 12s^5 + 32s^3 + 24s^2 + 12s), (s^6 - 3s^5 + 3s^4 + 3s^2 + 3s + 1)y - (24s^5 + 54s^4 - 54s^3 - 54s^2 + 30s)\}$ and $DS = \{s^6 - 3s^5 + 3s^4 + 3s^2 + 3s + 1\}$. By Theorem 4.6, under the variable order $x < y < s$, we have $Zero(HS/DS) = Zero(PD(ASC)/DS)$ where $ASC = \{f_1, f_2\}$ and

$f_1 = as^2 + bs + c$ with

$a = ((14388724x^2 + 1089290720x + 2205457984)y^2 + (-49736190x^3 - 2193776352x^2 + 44466793056x + 154797872640)y - 252381465x^4$
$-20654530164x^3 + 301488378048x^2 - 1030598219520x + 558403485696)$

$b = ((10771712x^2 + 872076352x + 1311063296)y^2 + (-31065888x^3 - 1942645344x^2 + 38282181504x + 95474718720)y - 227543904x^4$
$-15408517968x^3 + 233575488000x^2 - 835756710912x + 558403485696)$

$c = 4(904253x^2 + 54303592x + 223598672)y^2 + 6(-3111717x^3 - 41855168x^2 + 1030768592x + 9887192320)y - 24837561x^4 - 5246012196x^3 + 67912890048x^2 - 194841508608x$

$f_2 = 224y^3 + (-2268x + 7632)y^2 + (-54x^2 - 1512x - 480384)y + 34263x^3 - 424224x^2 + 1200960x$

By Theorem 3.5 and Theorem 3.9, (3.12.1) is a set of improper parametric equations for the curve $f_2 = 0$. To find a set of proper parametric equations for $f_2 = 0$, by Theorem 3.10, we select a new parameter

$$t = a/b = (s^2 + 1)/(1 - s). \tag{3.12.2}$$

Eliminating s from (3.12.1) and (3.12.2), we have

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

By Theorem 4.9, we can easily check that the above are a set of proper parametric equations of $f_2 = 0$ with an inversion map

$$s = \frac{32y^2 - (92x + 1768)y - 675x^2 + 8736x - 26688}{44y^2 + (-160x + 2504)y - 723x^2 + 9120x - 26688}.$$

If (3.1) defines a variety of dimension $d \geq 2$ then generally there is no proper reparametrization for improper parametric equations. However, the method used in Theorem 3.10 can be easily extend to the general case and are successful in many cases. Suppose, we already have (3.8) and B_i are not linear in t_i, $i = 1, ..., m$, then let

$$B_i = b_{i,r_i} t_i^{r_i} + ... + b_{i,0}$$

where $b_{i,j}$ are polynomials of the x and $t_1, ..., t_{i-1}$, $i = 1, ..., m$. Suppose $b_{i,s}/b_{i,r_i}$ are not elements in K. Let $s_i = b'_{i,s}/b'_{i,r_i}$ where $b'_{i,s}$ and b'_{i,r_i} are obtained from $b_{i,s}$ and b_{i,r_i} by replacing t_i by s_i, $i = 1, ..., m$. By Theorem 4.6, we can express x_i in terms of s_i. If x_i can be expressed as rational functions of s_i then s_i are a group of new parameters and $s_i = b'_{i,s}/b'_{i,r_i}$ are the inversion maps of the new parametric equations.

Example 3.13. Consider the following parametric equations.

$$(3.13.1). \qquad x = u^2 - v^2, \ y = 2uv, \ z = u^2 + v^2$$

Let $PS = \{x - u^2 + v^2, y - 2uv, z - u^2 - v^2\}$. By Theorem 4.6, under the variable order $x < y < z < u < v$ we have $Zero(PS) = Zero(PD(ASC))$ where

$$ASC = \{z^2 - y^2 - x^2, (2z - 2x)u^2 - y^2, 2uv - y\}$$

By Theorem 3.5 and Theorem 3.9, (3.13.1) is a set of improper parametric equations of the cone $z^2 = y^2 + x^2$. To find a proper parametric equation, using the method mentioned in the above paragraph, we select a group of new parameters

$$(3.13.2) \qquad s_1 = y^2/(2z - 2x), s_2 = y/2s_1$$

Using Theorem 4.6, we can express x, y and z in terms of s_1 and s_2,

$$x = s_1 - s_1 s_2^2, y = 2s_1 s_2, z = s_1 s_2^2 + s_1$$

which is a proper parametric equation of (3.13.1) with inversion maps (3.13.2).

Appendix 4. An Introduction to Ritt-Wu's Decomposition Algorithm

In this section, we give a brief introduction to Ritt-Wu's decomposition algorithm. A detailed description of the algorithm can be found in [Wu, 1984] or our new version [Chou & Gao, 1990]. The implementation of the algorithms in this paper is based on the new version.

Let P be a polynomial. The *class* of P, denoted by $class(P)$, is the largest p such that some x_p actually occurs in P. If $P \in K$, $class(P) = 0$. Let a polynomial P be of class $p > 0$. The coefficient of the highest power of x_p in P considered as a polynomial of x_p is called the *initial* of P. For polynomials P and G with $class(P) > 0$, let $prem(G; P)$ be the *pseudo remainder* of G wrpt P.

A sequence of polynomials $ASC = A_1, ..., A_p$ is said to be an *ascending* (ab. *asc) chain*, if either $r = 1$ and $A_1 \neq 0$ or $0 < class(A_i) < class(A_j)$ for $1 \leq i < j$ and A_k is of higher degree than A_m for $m > k$ in x_{n_k} where $n_k = class(A_k)$.

For an asc chain $ASC = A_1, ..., A_p$ such that $class(A_1) > 0$, we define the pseudo remainder of a polynomial G wrpt ASC inductively as

$$prem(G; ASC) = prem(prem(G; A_p); A_1, ..., A_{p-1}).$$

Let $R = prem(G; ASC)$, then from the computation procedure of the pseudo division procedure, we have the following important *remainder formula*:

$$JG = B_1A_1 + \cdots + B_pA_p + R \tag{4.1}$$

where J is a product of powers of the initials of the polynomials in ASC and the B_i are polynomials. For an asc chain ASC, we define

$$PD(ASC) = \{g \mid prem(g, ASC) = 0\}$$

By (4.1), a zero of ASC which does not annul the initials of the polynomial in ASC a zero of $PD(ASC)$. More precisely, we have

$$Zero(PD(ASC)) = Zero(ASC/J) \cup Zero(PD(ASC) \cup I) \tag{4.1.1}$$

where I is the initial set of ASC.

For an asc chain $ASC = A_1, ..., A_p$, we make a renaming of the variables. If A_i is of class m_i, we rename x_{m_i} as y_i, other variables are renamed as $u_1, ..., u_q$, where $q = n - p$. The variables $u_1, ..., u_q$ are called a *parameter set* of ASC. ASC is said to be an *irreducible ascending chain* if A_1 is irreducible, and for each $i \le p$ A_i is an irreducible polynomial of y_k in $K_{i-1}[y_i]$ where $K_{i-1} = K(u)[y_1, ..., y_{i-1}]/D$ where D is the ideal generated by $(A_1, ..., A_{i-1})$ in $K(u)[y_1, ..., y_{i-1}]$.

Definition 4.2. The dimension of an irreducible ascending chain $ASC = A_1, ..., A_p$ is defined to be $DIM(ASC) = n - p$.

Thus $DIM(ASC)$ is equal to the number of parameters of ASC. The following results are needed in this paper.

Theorem 4.3. *ASC is an irreducible ascending chain iff $PD(ASC)$ is a prime ideal with dimension $DIM(ASC)$.*

Proof. See [Wu, 1984]. ▮

A characteristic set of a polynomial ideal D is an ascending chain ASC in D such that for all $P \in D$ $prem(P, ASC) = 0$. Theorem 4.3 says that an ideal is prime iff it has a characteristic set which is irreducible.

Lemma 4.4. Let ASC be an irreducible asc chain with parameters $u_1, ..., u_q$. If Q is a polynomial not in $PD(ASC)$, then we can find a nonzero polynomial P in the u alone such that $P \in Ideal(ASC, Q)$ (i.e., the ideal generated by Q and the polynomials in ASC).

Proof. See [Wu, 1984]. ▮

Theorem 4.5. Let ASC be an irreducible asc chain with parameters $u_1, ..., u_q$, we can find an irreducible asc chain ASC' such that $PD(ASC) = PD(ASC')$ and the initials of the polynomials in ASC' are polynomials of the u.

Proof. Let $ASC = \{A_1, ..., A_p\}$ and $I_i = int(A_i)$. By Lemma 4.4, for each i we can find a polynomial P_i of y_i and the u and polynomials Q_k $(k = 1, ..., i)$ such that $P_i = \sum_{k=1}^{i-1} Q_k A_k + Q_i I_i$. We assume that A_i is of degree d_i in y_i. Let $A_i' = Q_i A_i + (\sum_{k=1}^{i-1} Q_k A_k) y_i^{d_i}$, then $ASC' = \{A_1, A_2', ..., A_p'\}$ is an asc chain such that the initials of A_i' are polynomials of the u. Note that the degrees of A_i' in y_i are the same as the degrees of A_i in y_i, then ASC' is also a characteristic set of $PD(ASC)$, i.e., $PD(ASC') = PD(ASC)$ and ASC' is irreducible by Theorem 4.3. ∎

Let PS be a polynomial set. For an algebraic closed extension field E of K, 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

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

Then we have the following Ritt–Wu's decomposition algorithm.

Theorem 4.6. For finite polynomial sets PS and DS, we can either detect the emptiness of $Zero(PS/DS)$ or find irreducible asc chains ASC_i, $i = 1, ..., l$, such that

$$Zero(PS/DS) = \cup_{i=1}^{l} Zero(PD(ASC_i)/DS)$$

The decompositions satisfies (a). the initials of the polynomials of ASC_i, denoted by J_i, are polynomials of the parameters of ASC_i; (b). there are no $i \neq j$ such that $PD(ASC_i) \subset PD(ASC_j)$; and (c). $prem(d, ASC_i) \neq 0$ for all $d \in DS$ and $i = 1, ..., l$.

Proof. See [Chou & Gao, 1990]. ∎

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

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

Chou, S.C. and Gao, X.S. (1990), Ritt-Wu's Decomposition Algorithm and Geometry Theorem Proving, *10th International Conference on Automated Deduction*, M.E. Stickel (Ed.) pp 207–220, Lect. Notes in Comp. Sci., No. 449, Springer-Verlag.

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.

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

Sederberg, T.W. (1986), Improperly Paramatrized 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, Gragh, 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.

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

Wu, W.T. (1984), Basic Principles of Mechanical Theorem Proving in Elementary Geometries, *J. Sys. Sci. & Math. Scis.*, 4(1984), 207 –235, Re-published in *J. Automated Reasoning*, 1986.

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.