Computations with Parametric Equations*

Xiao-Shan Gao† and Shang-Ching Chou

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

Abstract. We present a complete method of implicitization for general rational parametric equations. We also present a method to decide whether the parameters of a set of parametric equations are independent, and if not, reparameterize the parametric equations so that the new parametric equations have independent parameters. We give a method to compute the 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 a proper reparameterization for a set of improper parametric equations of algebraic curves is presented.

1 Introduction

Methods of converting rational parametric equations to their implicit equations are of fundamental importance in computer modeling and computer graphics. Several methods to find the implicit equations for a set of rational parametric equations were presented. The first method was based on elimination theories [Sederberg, 1984]. The second method was based on Gröbner bases (see [Arnon & Sederberg, 1984], and in more general case [Buchberger, 1987]). The above methods are only complete for *polynomial* parametric equations. Complete methods to find the implicit equations of space curves and surfaces were presented in [Chuang & Hoffman, 1989], [Kalkbrener, 1990], and [Manocha & Canny, 1990]. Recently, a method to compute the *images* of parametric equations was given in [Wu, 1989] and [Li, 1989]. But the following kind of parametric equations is not considered in the above methods. The following example shows that in general case, the parameters of a set of parametric equation may not be

*The work reported here was supported in part by the NSF Grant CCR-8702108 and CCR-9002362.

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

independent. One might 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 solution of the inversion problem is not clear. This paper addresses the implicitization of this kind of *rational* parametric equations with *any dimensions*.

We show that each set of rational parametric equations determines a unique *implicit irreducible variety*. We give a method to find a set of polynomials the zero set of which is the implicit irreducible variety of the parametric equations. We also give a method to decide whether the parameters of a set of parametric equations are independent, and if not, reparameterize the parametric equations so that the new parametric equations have independent parameters. We present a close form solution to the inversion problem, i.e., we present a method to compute the inversion maps of parametric equations with independent parameters, and as a consequence, we can decide whether the parametric equations are *proper*, i.e., whether the implicit variety is not multiply traced by the parametric equations. If the parametric equations are not proper, naturally we might ask whether we can reparameterize them so that the new parametric equations are proper. The answer is negative in general. However, in the case of algebraic curves, this is true by Lüroth's theorem [Walker, 1950] and Sederberg presented a method to find proper parametric equations [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 improper parametric equations of an algebraic curve and our method does not need to randomly select sample points on the curve as Sederberg's method 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 [Castelnuovo 1894]. However if the base field K is $\mathbf{Q}$ or $\mathbf{R}$ this need not to be the case [Segre 1951]. For the complex case, it seems there is no algorithm to transform an improper parametric equations to a proper one. For some experiment results, see [Gao & Chou, 1990]. If the variety represented by the parametric equations are of dimension > 2, then even for $K = \mathbf{C}$ there are improper parametric equations that do not have proper reparametrization [Artin & Mumford 1971].

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

2 Preliminaries and the Main Result

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 nonzero polynomials $P_1, ..., P_n, Q_1, ..., Q_n$ in $K[t_1, ..., t_m]$, we call

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

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 *image* of (2.1) in E^n is

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

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 $IM(P, Q) = \{(x_1, ..., x_n) \mid \exists \tau \in E^m (Q_i(\tau)x_i - P_i(\tau) = 0 \wedge Q_i(\tau) \neq 0)\}$. Thus by the quantifier elimination theory for an algebraically closed field [Tarski, 1951] or [WU, 1989], we can find the PS_i and d_i such that (2.2.1) is correct. .QED.

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 if (1) $IM(P, Q) \subset V$; and (2) $V - IM(P, Q)$ is contained in an algebraic set with dimension less than d.

In Definition 2.3, we also say that (2.1) defines V, or V is the *implicit variety* of (2.1).

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 $\eta = (P_1/Q_1, ..., P_n/Q_n)$. Let $V = Zero(I)$, then it is clear that $IM(P, Q) \subset V$. We still need to prove that $V - IM(P, Q)$ is contained

in an algebraic set of less dimension than that of I. By (2.2.1), $IM(P,Q) = \cup_{i=1}^{t} Zero(PS_i/\{d_i\})$. Furthermore we can assume that each $Ideal(PS_i)$ (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 $Zero(PS_1) \subset V$, then $Ideal(PS_1) = I$. Hence $V - IM(P,Q) = Zero(I \cup \{d_1\}) - \cup_{i=2}^{t} Zero(PS_i/\{d_i\})$. Thus $V - IM(P,Q)$ 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 V is uniquely determined. .QED.

Definition 2.5. The parameters $t_1, ..., t_m$ of (2.1) are called *independent* if the parametric equation (2.1) defines a variety of dimension m, or

equivalently the transendental degree of $K(P_1/Q_1, ..., P_n/Q_n)$ over K is m (by Theorem 2.4).

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 $x_i = P_i(f_1, ..., f_m)/Q_i(f_1, ..., f_m)$, $i = 1, ..., n$, are true on $IM(P,Q)$, i.e., functions which give the parameter values corresponding to points on the image of (2.1).

Definition 2.7. (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 $a_i = P_i(\tau_1, ..., \tau_m)/Q_i(\tau_1, ..., \tau_m)$, $i = 1, ..., n$.

The following algorithmic theorem is the main result of this paper.

Main Theorem 2.8. For a set of parametric equations of the form (2.1),

(a) we can find a polynomial set PS such that $Zero(PS)$ is the implicit variety of (2.1);

(b) we can decide whether the parameters $t_1, ..., t_m$ 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

$$B_1(x_1, ..., x_n, t_1) = 0, B_2(x_1, ..., x_n, t_1, t_2) = 0, ..., B_m(x_1, ..., x_m, t_1, ..., t_m) = 0$$

which determine t_i as functions of $x_1, ..., x_n$. These functions are inversion maps of (2.1). Furthermore, (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.

3 A Proof of the Main Theorem

In this section, we will use some notions and results about Ritt-Wu's decomposition algorithm which can be found in the appendix of this paper.

3.1. The Implicit Variety and Independent Parameters

For a set of rational parametric equations of the form (2.1), let $PS = \{F_1, \cdots, F_n\}$ and $DS = \{Q_1, \cdots, Q_n\}$, where $F_i = Q_i x_i - P_i$, $i = 1, ..., n$. It is obvious that

$$IM(P,Q) = \{(x_1, ..., x_n) \mid \exists(\tau_1, \cdots, \tau_m) \in E^m \quad (\tau_1, \cdots, \tau_m, x_1, \cdots, x_n) \in Zero(PS/DS) \tag{3.1}$$

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 ascending chain* in $K[t, x]$. Thus by Theorem A.3 (i.e., Theorem A.3 in the Appendix), $PD(PS)$ (for the definition of PD, see the Appendix) is a prime ideal of dimension m. Note that DS is the set of initials of the polynomials in PS, then by (A.1.1) we have

$$Zero(PS/DS) = Zero(PD(PS)/DS). \tag{3.2}$$

By Theorem A.6 and (3.2), we can find an irreducible ascending chain ASC under the new variable order $x_1 < \cdots < x_n < t_1 < \cdots < t_m$ such that

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

ASC has the same dimension m as PS. Hence ASC contains n polynomials. Then by changing the order of the variables properly, we can assume ASC to be

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

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 (2.1), 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 depend on the t effectively. Hence $d = m - s > 0$. .QED.

By Definition 2.5, we have

Corollary 3.5.1. The parameters of (2.1) are independent iff $s = 0$.

Theorem 3.6. The implicit variety of (2.1) is $V = Zero(PD(A_1, \cdots, A_{n-d}))$.

Proof. By Theorem 2.4 and Lemma 3.5, (2.1) defines a variety W of dimension d. By (3.1) and (3.3), it is clear that $IM(P,Q) \subset V$. Then $W \subset V$. By Theorem A.3, V is also of dimension d. Therefore $V = W$. .QED.

Remark. An algorithm to compute a basis of $PD(A_1, \cdots, A_{n-d})$ can be found in [Chou, Schelter & Yang, 1990]. Thus we have proved (a) of the Main Theorem 2.8.

For example (1.1), let $PS = \{x - u - v, y - u^2 - v^2 - 2uv + 1, z - u^3 - v^3 - 3u^2v - 3v^2u - 1\}$. By Theorem A.6, under the variable order $x < y < z < u < v$, we have $Zero(PS) = Zero(PD(ASC_1))$ 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. If the parameters of (2.1) are not independent, we can find a set of new parametric equations

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

which has the same implicit variety as (2.1) and with independent parameters.

Proof. By Theorem A.6, we can find (3.4) from (2.1). By Theorem A.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., of $x_1, ..., x_d, t_1, ..., t_s$. Since Q_i is not in $PD(F_1, ..., F_n) = PD(ASC)$, by Lemma A.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 $M = \prod_{i=1}^{m-s} I_i \cdot \prod_{j=1}^{n} q_j$. Then M is a polynomial of $x_1, ..., x_d, t_1, ..., t_s$. Let $h_1, ..., h_s$ be integers such that when replacing t_i by h_i, $i = 1, ..., s$, M becomes a nonzero polynomial of $x_1, ..., x_d$. Let P_i' and Q_i' be the polynomials obtained from P_i and Q_i by replacing t_i by h_i, $i = 1, ..., s$. Now we have obtained (3.7.1). The proof that (3.7.1) satisfies the condition is somewhat lengthy and can be found in [Gao & Chou, 1990]. .QED.

Remark. It is worth noting that almost all integer sets can be used to obtain the new parametric equations.

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. Then (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 (2.1) are independent, i.e., $s = 0$, then (3.4) becomes

$$A_1(x_1, \cdots, x_{m+1}), \cdots, A_{n-m}(x_1, \cdots, x_n)$$

$$B_1(x_1, \cdots, x_n, t_1), \cdots, B_m(x_1, \cdots, x_n, t_1, \cdots, t_m) \tag{3.8}$$

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

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

(b) (2.1) is 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 in $K[x]$.

Proof. Note that $B_i = 0$, $i = 1, ..., m$, are the relations between the x and $t_1, ..., t_i$ in $PD(PS)$ which have 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 (2.1). To prove (b), note that different solutions of $B_i = 0$ for the same x give same value for the x_i. Since (3.8) is irreducible, (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 $t_i = U_i/I_i$, $i = 1, ..., m$. .QED.

Remark. 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.

We have proved (c) of the Main Theorem 2.8, and (d) of the Theorem 2.8 can be summarized as the following theorem.

Theorem 3.10. 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

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

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 $P_1(t_1) - Q_1(t_1)lm = 0$ where $lm = P_1(t_1)/Q_1(t_1) \in K'$, then t_1 is algebraic over K'. Let $f(y) = a_r y^r + ... + a_0$ be an irreducible polynomial in $K'[y]$ 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 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 can also 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 $B_1'(y) = B_1(P_1/Q_1, ..., P_n/Q_n, y) = 0$ 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. Once $s = f(t_1)/g(t_1)$ has been found, the F_i and G_i can be computed easily. .QED.

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

Corollary 3.11. Let $g_1(t_1), ..., g_r(t_1)$ be elements of $K(t_1)$, then we can find a $g(t_1) \in K(t_1)$ such that $K(g_1, ..., g_r) = K(g)$.

Example 3.12. Consider the following parametric equations

$$x = \frac{t^4 - 4t^2 + 1}{t^4 + 1},\ y = \frac{2\sqrt{2}(-t^3 + t)}{t^4 + 1}. \tag{3.12.1}$$

Let $PS = \{(t^4+1)x-(t^4-4t^2+1), (t^4+1)y-2\sqrt{2}(-t^3+t)\}$, $DS = \{t^4+1\}$, and by Theorem A.6, under the variable order $x < y < t$ we have $Zero(PS/DS) = Zero(PD(ASC))$ where

$$ASC = \{y^2 + x^2 - 1, \sqrt{2}(x-1)t^2 - 2yt - \sqrt{2}x + \sqrt{2}\}.$$

By Theorem 3.5 and Theorem 3.9, the implicit variety of (3.12.1) is the unit circle $y^2 + x^2 - 1 = 0$ and (3.12.1) is not proper. An inversion map of (3.12.1) can be found by solving the following equation

$$\sqrt{2}(x-1)t^2 - 2yt - \sqrt{2}x + \sqrt{2} = 0$$

e.g., $t = (y - \sqrt{y^2 + 2(x-1)^2})/(\sqrt{2}x - \sqrt{2})$. To find a set of proper parametric equations for the unit circle, by Theorem 3.10 we select a new parameter $s = y/(x-1) = (t^2-1)/(\sqrt{2}t)$. Expressing x and y in terms of s using Theorem A.6, we have

$$x = (s^2 - 1)/(s^2 + 1), \quad y = 2s/(s^2 + 1)$$

which is a set of proper parametric equations for the unit circle with inversion map $s = y/(x-1)$.

References

[1] rnon, 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.

[2] rtin, 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] uchberger, 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.

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

[5] hou, 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.

[6] hou, S.C., W.F. Schelter and Yang, J.G., (1990) An Algorithm for Constructing Gröbner Bases from Characteristic Sets, *Algorithmic*, 5, 147–154.

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

[8] ao, 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.

[9] alkbrener, M.(1990), Implicitization of Rational Parametric Curves and Surfaces, *Proc. of AAECC-8,*, ACM press, New York.

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

[11] anocha, D. and Canny J. F. (1990), Implicitizing Rational Parametric Surfaces, UCB/CSD, September.

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

[13] ederberg, 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.

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

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

[16] alker, R. (1950), *Algebraic Curves*, Princeton Univ. Press.

[17] u, W.T. (1984), Basic Principles of Mechanical Theorem Proving in Elementary Geometries, *J. Sys. Sci. & Math. Scis.*, 4(1984), 207 –235, Republished in *J. Automated Reasoning*, 1986.

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

Appendix. Some Results about Ritt-Wu's Decomposition Algorithm

A detailed description of Ritt-Wu's Decomposition algorithm can be found in [Wu, 1984]. The implementation of the algorithms in this paper is based on a new version of the decomposition algorithm in [Chou & Gao, 1990].

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 $p = 1$ 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 $ASC = A_1, ..., A_p$ with $class(A_1) > 0$, the pseudo remainder of a polynomial G wrpt ASC is defined 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*:

$$JG = B_1A_1 + \cdots + B_pA_p + R \tag{A.1}$$

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 (A.1), a zero of ASC which does not annul the initials of the polynomials in ASC is a zero of $PD(ASC)$. More precisely, we have

$$Zero(PD(ASC)) = Zero(ASC/J) \bigcup \cup_{d \in J} Zero(PD(ASC) \cup \{d\}) \tag{A.1.1}$$

where J is the set of initials of the polynomials in 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 $i \leq p$ A_i is an irreducible polynomial of y_i 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 A.2. The dimension of an irreducible ascending chain $ASC = A_1, ..., A_p$ is defined to be $DIM(ASC) = n - p$.

Theorem A.3. ([Wu, 1984]) If ASC is an irreducible ascending chain then $PD(ASC)$ is a prime ideal with dimension $DIM(ASC)$.

Lemma A.4. ([Wu, 1984]) 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).

Theorem A.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. It is a direct consequence of Lemma A.4. .QED.

Theorem A.6. (Ritt–Wu's decomposition algorithm) 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). there are no $i \neq j$ such that $PD(ASC_i) \subset PD(ASC_j)$; and (b). $prem(d, ASC_i) \neq 0$ for all $d \in DS$ and $i = 1, ..., l$.

Proof. See [Chou & Gao, 1990]. .QED.