Chapter 14

Conversion Between Implicit and Parametric Representations of Algebraic Varieties

Xiao-Shan Gao

In this chapter, we review algorithms for conversion between implicit and parametric representations of algebraic varieties with emphasis on the implicitization of rational parametric equations (abbr. RPEs). In the implicitization of RPEs, we will consider the following problems. (1) To find a basis for the implicit prime ideal determined by a set of RPEs. (2) To find a canonical representation for the image of a set of RPEs. (3) To decide whether the parameters of a set of RPEs are independent, and if not, to re-parameterize the RPEs so that the new RPEs have independent parameters. (4) To compute the inversion maps of a set of RPEs, and as a consequence, to decide whether a set of RPEs is proper. If the RPEs are not proper, find a proper re-parameterization for the given RPEs. (5) To decide whether a set of RPEs is normal. If it is not normal, find a normal re-parameterization of the given RPEs. In the parameterization of implicitly given varieties, we will discuss how to construct a hyperfurface that is biratinally to a given general variety and to find a set of RPEs of a plane curve if it is possible. We also propose several open problems for future research.

14.1 Introduction

There are two forms to represent algebraic curves or surfaces: the *implicit form* and the *parametric form.* For example, the unit circle can be given by an implicit algebraic equation:

$$x^2 + y^2 - 1 = 0,$$

or by a set of rational parametric equations (RPEs):

$$x = \frac{t^2 - 1}{t^2 + 1},\ y = \frac{2t}{t^2 + 1}. \tag{1.1}$$

Generally, *a set of RPEs* is as follows:

$$(1.2) \qquad x_1 = \frac{P_1(t_1, \ldots, t_m)}{Q_1(t_1, \ldots, t_m)}, \; \ldots, \; x_n = \frac{P_n(t_1, \ldots, t_m)}{Q_n(t_1, \ldots, t_m)}$$

where $t_1, \ldots, t_m$ are indeterminates and $P_1, \ldots, P_n$, $Q_1, \ldots, Q_n$ $(Q_i \neq 0)$ are polynomials in $\mathbf{Q}[t_1, \ldots, t_m]$. 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 (1.2).

It is well known that a set of RPEs can always be converted into a set of implicit equations. This conversion procedure is called *implicitization.* On the other hand, the inverse procedure, algorithms for *parameterization* of implicitly given algebraic varieties are much more difficult and are still not completely solved. Both implicitization and parameterization are classic topics in algebraic geometry. It has connections with the theory of resolvents, the theory of quantifier elimination, Lüroth's theorem, the computation of the genus, resolution of singularities, etc.

The recent extensive study of this problem is due to the fact that implicitization of RPEs is often used in *solid modeling.* It is recognized that both implicit and parametric representations for rational curves and surfaces have their advantages in solid modeling: The parametric form is best suited for generating points along a curve, whereas the implicit representation is most convenient for determining whether a given point lies on a specific curve. This motivates the search for a means of converting from one representation to the other.

Sederberg and Arnon are the first to discuss the implicitization problem using various resultant theories (Sederberg 1984) and (Arnon and Sederberg 1984). Methods of implicitization for *polynomial* parametric equations are presented in Buchberger (1987) and Shannon and Sweedler (1988) by using the Gröbner basis method. A method to find the implicit approximation of parametric equations of curves and surfaces is presented in Chuang and Hoffmann (1989). Implicitization problems for rational parametric surfaces are carefully studied in Hoffmann (1990), Chionh (1990) Kalkbrener (1990a), Manocha and Canny (1990). Methods of implicitization for general RPEs are presented in Ollivier (1989, 1990d), Kalkbrener (1990b); Gao and Chou (1991a, 1992a), Wang (1995b).

Most of the above work is to find the implicit ideal (see Section 14.3) of the RPEs, which is the most important but not all the tasks in the implicitization. A method for computing the image of RPEs is given in Wu (1989) and Li (1989). In Gao and Chou (1991a, 1992a), algorithms are presented to find a canonical representation for the image of a set of RPEs. Wang (1995b) gives another algorithm for image computation. In Gao and Chou (1991a, 1992a), the following problems are discussed. (1) To decide whether the parameters of a set of RPEs are independent, and if not, to re-parameterize the RPEs so that the new parametric equations have independent parameters. (2) To compute the inversion maps of a set of RPEs, and as a consequence, to decide whether the RPEs are proper. If the RPEs are not proper, find a proper re-parameterization. (3) To decide whether a set of RPEs is normal. If it is not normal, find a normal re-parameterization.

Finding parametric representation for implicitly given algebraic varieties is much more difficult than implicitization. Only a special class of algebraic varieties has parametric representations. Except the case of algebraic curves and surfaces, there is still no general methods for deciding whether a given algebraic variety has a parametric representation or not.

In Abhyankar and Bajaj (1988), classic results for finding RPEs are improved to provide an effective method of parameterization for plane curves. In Abhyankar and Bajaj (1989), a parameterization method for a special class of space curves has been provided. In Gao and Chou (1991b), the theory of resolvent from Ritt (1954) has been used to give a parameterization algorithm for any algebraic curves. This algorithm, though complete, needs to solve a system of algebraic equations which is a complicated task. Effective parameterization methods for plane curves have been proposed in Sendra and Winkler (1991).

It is a well-known result in algebraic geometry that an irreducible variety is birational to a hypersurface (Hartshorne 1977). Furthermore, a constructive proof of this result can be given based on, e.g., the theory of resolvent (Ritt 1954; Gao and Chou 1991b). Previous work on finding a plane curve birational to a space curve usually uses the technique of taking a projection of the space curve into a randomly selected direction and verifying that it is one-to-one (Abhyankar and Bajaj 1989; Garrity and Warren 1989; Kalkbrener 1990). The resolvent method is similar to the projection method and deals with the general case in a deterministic way.

By the results discussed in the preceding paragraph, we need only to find RPEs for hypersurfaces. As we have mentioned, there are several methods for parameterization of plane curves. Parameterization methods for surfaces were proposed by classical Italian geometers (Castelnuvo 1894) and studied recently in Schicho (1995). Parameterization methods for varieties with higher dimensions are still open (Eisenbud 1993).

Since an algebraic variety generally does not have parametric representations, an alternative way is to find an appropriate parametric representation for it at a local point using, e.g., Puisuix expansion (Alonso et al 1992 and Li 1996).

This chapter is a summary of the results about implicitization of RPEs and parameterization of algebraic varieties with emphasis on the implicitization. Also, we will mainly focus on the work done by Wu's group at MMRC including (Wu 1989; Li 1989; Gao and Chou 1991a, 1991b, 1992a, 1992b; Chou , Gao and Li 1994 and Wang 1995b). Other results are mentioned mainly for comparison purposes.

14.2 The implicit ideal of a set of RPEs

The *implicit ideal* of (1.2) is defined as

$$ID(P,Q) = \{P \in \mathbf{Q}[x_1,\ldots,x_n] \mid P(P_1/Q_1,\ldots,P_n/Q_n) \equiv 0\}.$$

Zero($ID(P,Q)$) is called the *implicit variety* of (1.2). It is clear that $ID(P,Q)$ is a prime ideal whose dimension equals the transcendental degree of $\mathbf{Q}(P_1/Q_1,\ldots,P_n/Q_n)$ over $\mathbf{Q}$.

14.2.1 A method based on Gröbner basis computation

For a set of RPEs of the form (1.2), let

$$F_i = Q_i x_i - P_i, \quad D_i = Q_i z_i - 1, \ i = 1,\ldots,n$$

where the z_i are new variables. Let

$$PS(P,Q) = Ideal(F_1,\ldots,F_n,D_1,\ldots,D_n)$$

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

Theorem 14.1 *The implicit ideal of (1.2) is* $PS(P,Q) \cap K[x_1,\ldots,x_n]$.

For a proofs, see (Ollivier 1989; Kalkbrener 1990b; Gao and Chou 1992a). With the help of the following Lemma and Theorem 14.1, we can compute a basis for the implicit ideal of (1.2) using the Gröbner basis method.

Lemma 14.2 *(Buchberger, 1985) Let GB be a Gröbner basis of an ideal $D \subset K[x_1, \ldots, x_n, y_1, \ldots, y_k]$ in the pure lexicographic order $x_1 < \ldots < x_n < y_1 < \ldots < y_k$, then $GB \cap K[x_1, \ldots, x_n]$ is a Gröbner basis of $D \cap K[x_1, \ldots, x_n]$.*

Example 14.3 *Consider the following RPEs:*

$$x = \frac{u+v}{u-v}, y = \frac{2v^2 + 2u^2}{(u-v)^2}, z = \frac{2v^3 + 6u^2v}{(u-v)^3}. \tag{2.1}$$

Let

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

Note that we can omit $(u-v)^2z_2 - 1$ and $(u-v)^3z_3 - 1$ 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

$$\{y - x^2 - 1, z - x^3 + 1, (x+1)v + (-x+1)u, 2uyz_1 + x + 1, 2vz_1 + x - 1\}. \tag{2.2}$$

By Theorem 14.1 and Lemma 14.2, a basis of the implicit ideal of (2.1) is $\{y - x^2 - 1, z - x^3 + 1\}$.

If $m = 1$, then the D_i can be deleted from $PS(P, Q)$, and Theorem 14.1 is still true. This is because that $gcd(P_i, Q_i) = 1$ implies resultant$(P_i, Q_i) = 1$. Thus, we get the same result as (Kalkbrener 1990a) for the implicitization of parametric equations of curves.

14.2.2 A method based on the characteristic set method

If it is difficult to compute the Gröbner basis in the above method, we may use a method based on the Wu-Ritt's characteristic set (abbr. CS) method to obtain a CS for the implicit ideal. Using the same notations introduced above, let $PS = \{F_1, \ldots, F_n\}$ and $DS = \{Q_1, \ldots, Q_n\}$. Since PS is of triangular form, we have

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

For the definition of $PD(PS)$, please see Chap 1of this book. By the CS method, we can find an irreducible ascending chain ASC under a new variable order $x_1 < \ldots < x_n < t_1 < \ldots < t_m$ such that

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

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

$$\begin{array}{l} A_1(x_1, \ldots, x_{d+1}), \ldots, A_{n-d}(x_1, \ldots, x_n), \\ B_1(x_1, \ldots, x_n, t_1, \ldots, t_{s+1}), \ldots, B_{m-s}(x_1, \ldots, x_n, t_1, \ldots, t_m) \end{array} \tag{2.3}$$

where $d + s = m$. The *parameter set* of ASC is $\{x_1, \ldots, x_d, t_1, \ldots, t_s\}$.

Theorem 14.4 *(Gao and Chou 1991a) The implicit ideal of (1.2) is $PD(A_1, \ldots, A_{n-d})$.*

An algorithm to compute a basis of $PD(A_1, \ldots, A_{n-d})$ can be found in Chou (1988), Gao and Chou (1993) and Wang (1992).

Example 14.5 *For the RPEs (2.1), let*

$$\begin{aligned} PS &= \{(v-u)x + v + u, (v-u)^2 y - 2v^2 - 2u^2, (v-u)^3 z + 2v^3 + 6u^2 v\} \\ DS &= \{u - v\}. \end{aligned}$$

Using the CS method under the pure lexicographical order $x < y < z < u < v < z_1$, we have $\mathrm{Zero}(PS/DS) = \mathrm{Zero}(PD(ASC))$ *where*

$$ASC = \{y - x^2 - 1, z - x^3 + 1, (x+1)v + (-x+1)u\}.$$

By Theorem 14.4, the implicit ideal of (2.1) is $PD(y - x^2 - 1, z - x^3 + 1)$, which is the ideal generated by $y - x^2 - 1$ and $z - x^3 + 1$.

14.2.3 Techniques of computation

Both Theorem 14.1 and Theorem 14.4 provide complete methods for finding a basis for the implicit prime ideal of a set of RPEs. But to compute the CS or the Gröbner basis is of very high complexity. For some parametric equations, we may use their special property to develop efficient algorithms. In what follows, we consider such a partial algorithm.

Consider a set of parametric equations for a space surface

$$x = \frac{P_1(t,s)}{Q_1(t,s)} \; y = \frac{P_2(t,s)}{Q_2(t,s)} \; z = \frac{P_3(t,s)}{Q_3(t,s)} \tag{2.4}$$

where P_i and Q_i are polynomials in $K[t,s]$. Let

$$F_1 = Q_1 x - P_1, F_2 = Q_2 y - P_2, F_3 = Q_3 z - P_3$$

The essential step in the implicitization is the triangulation of F_1, F_2, and F_3 by pseudo remainder sequences. We may use two tricks. First, we can use Collins' method or a similar result in the multi-polynomial case (Li 1987) to remove extraneous factors produced in the computation. Second, we may choose a "good" way to do pseudo divisions. The purpose is to keep the degrees of the polynomials occurring in the computation as low as possible. We shall explain this in the examples given below.

Theorem 14.6 *Suppose we obtain the following triangular from F_1, F_2 and F_3 under the variable order $x < y < z < s < t$*

$$g_1(x,y,z), g_2 = I_2(x,y,z)s - U_2(x,y,z), g_3 = I_3(x,y,z)t - U_3(x,y,z).$$

If $I_2(\eta)I_3(\eta) \not\equiv 0$ for $\eta = (\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3})$, then we have

(1) One irreducible factor of g_1, say f_1 satisfying $f_1(\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}) \equiv 0$), is the implicit equation of (2.4).

(2) Parametric equations (2.4) are proper and a set of inversion map is $t = \frac{U_2}{I_2}, s = \frac{U_3}{I_3}$.

Consider the following examples from (Hoffmann 1990).

Example 14.7 *Find the implicit ideal of the following RPEs.*

$$
\begin{array}{rl}
 & f_1 = z + (-9s + 15)t - 12s - 34 \\
\textit{(quadratic)} & f_2 = y + (s - 8)t - 6s^2 - 7 \\
 & f_3 = x - 3t^2 + (-s + 5)t - 4s^2 + 2s - 4, \\
 & f_1 = z - 2t^3 + (5s - 1)t + s^3 \\
\textit{(cubic)} & f_2 = y + (-s^2 + 3)t - 1 \\
 & f_3 = x + t^3 - 3st - s^3 - s, \\
 & f_1 = z + (3s^3 - 15s^2 + 15s)t^3 + (3s^3 + 18s^2 - 27s + 3)t^2 \\
\textit{(bi-cubic)} & +(-6s^3 - 9s^2 + 18s - 3)t + 3s^2 - 3s \\
 & f_2 = y - t^3 - 3t - 3s^3 + 6s^2 - 3s \\
 & f_3 = x - 3t^3 + 6t^2 - 3t - s^3 + 3s^2 - 6s + 1.
\end{array}
$$

The computation of the quadratic form is easy. To compute the cubic form, we first form the pseudo remainders $f_4 = \mathrm{prem}(f_1, f_2)$, $f_5 = \mathrm{prem}(f_1, f_3)$, $f_6 = \mathrm{prem}(f_2, f_3)$. Then f_6 and f_4 are polynomials in x, y, z, s such that $deg_s(f_6) = 5$ and $deg_s(f_4) = 9$. We compute sub-resultant remainder sequence of f_4 and f_6 to obtain a triangular form. For bi-cubic, we first form the pseudo remainders $f_4 = \mathrm{prem}(f_1, f_2)$, $f_5 = \mathrm{prem}(f_3, f_2)$, $f_6 = \mathrm{prem}(f_4, f_5)$, $f_7 = \mathrm{prem}(f_2, f_5)$, $f_8 = \mathrm{prem}(f_6, f_7)$, $f_9 = \mathrm{prem}(f_5, f_7)$. Then f_8 and f_9 are polynomials in x, y, z, s such that $deg_s(f_8) = 9$ and $deg_s(f_9) = 9$. We compute sub-resultant remainder sequence of f_4 and f_6 to obtain the triangular form. We can check that all the three examples satisfy the conditions in Theorem 14.6. Therefore, it is easy to obtain the implicit equation and the inversion maps for them.

14.3 The images of a set of RPEs

Let $\mathbf{E}$ be an extension field $\mathbf{Q}$. The *image* of RPEs (1.2) in $\mathbf{E}^n$ is defined as

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

We might naturally guess that $\mathrm{Zero}(ID(P, Q)) = IM(P, Q)$. But this is not true. For instance, $(1, 0)$ is a point on the unit circle, but it is not in the image of (1.1). To compute the image of the RPEs, we need first to introduce the concept of projections.

Let PS and DS be polynomial sets in $\mathbf{Q}[x_1, \ldots, x_n, y_1, \ldots, y_m]$. The *projection* of $Z = \mathrm{Zero}(PS/DS)$ with $y_1, \ldots, y_m$, $\mathrm{Proj}_{y_1,\ldots,y_m} Z$ is defined as

$$\{(a_1, \ldots, a_n) \in \mathbf{E}^n \mid \exists (b_1, \ldots, b_m) \in \mathbf{E}^m, (a_1, \ldots, a_n, b_1, \ldots, b_m) \in Z\}.$$

If E is algebraic closed, Tarski's method (1951) for the real field can be used to compute the projection. In Heintz (1983) and Seidenberg (1956), direct methods for algebraic closed fields are presented. In Wu (1989), a method based on the CS method is proposed. It is a known result in logic that if an existential quantifier can be eliminated then there is a quantifier elimination theory for the theory of algebraic closed field (p. 83 (Shoenfield 1967)). Since the projection algorithm actually gives a method of eliminating existential quantifiers, it provides a complete method of quantifier elimination over the field of complex numbers. For details, see (Chou, Gao and Li 1994).

Theorem 14.8 *(Wu 1984a) Using the notations defined above, we can find polynomial sets PS_i and polynomials G_i, $i = 1, \ldots, k$ such that*

$$\text{Proj Zero}(PS/DS) = \cup_{i=1}^{k}\text{Zero}(PS_i/\{G_i\})$$

For RPEs (1.2), we have

$$IM(P, Q) = \text{Proj}_{t_1,\ldots,t_m}\text{Zero}(PS/QS) \tag{3.1}$$

where $PS = \{x_iQ_i - P_i(t), i = 1, \ldots, n\}$, and $QS = \{Q_i(t)), i = 1, \ldots, n\}$. As a direct consequence of (3.1) and Theorem 14.8, we have

Lemma 14.9 *There is an algorithm to find polynomial sets $PS_1, \ldots, PS_t$ and polynomials $D_1, \ldots, D_t$ such that*

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

The following result describes the relation between the image and the implicit variety of a set of RPEs and a canonical representation for the image (Chou, Gao and Li 1994).

Theorem 14.10 *Let V be the implicit variety of (1.2) 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.
(3) We can find irreducible asc chains ASC, ASC_i such that

$$IM(P, Q) = \text{Zero}(PD(ASC)) - \cup_{i=1}^{k}\text{Zero}(ASC_i/J_iD_i),$$

where J_i are the initial-products of ASC_i and D_i are polynomials. We also have: (a) $PD(ASC)$ is the implicit ideal of (1.2); (b) $\text{Zero}(ASC_i/J_iD_i) \subset \text{Zero}(PD(ASC))$.

Example 14.11 *Compute the image of (2.1), let $PS = \{(u^2+v^2-1)x - u^2+v^2-1, (u^2+v^2-1)y - 2uv, (u^2+v^2-1)z - 2u\}$, $DS = \{u^2+v^2-1\}$. Using a program based on Lemma 14.9, we have*

$$\text{Proj Zero}(PS/DS) =$$
$$\text{Zero}(z^2 - y^2 - x^2 + 1/z(x+1)(y^2+x^2-1)) \cup \text{Zero}(z, y, x+1).$$

We can find the following canonical form for the image.

$$\text{Zero}(z^2 - y^2 - x^2 + 1) - (\text{Zero}(z, y^2 + x^2 - 1/x + 1) \cup \text{Zero}(x + 1, z^2 - y^2/y)).$$

14.4 Independent parameters

The parameters $t_1, \ldots, t_m$ of RPEs (1.2) are called *independent* if the implicit ideal of (1.2) is of dimension m, or equivalently the transcendental degree of the field $\mathbf{Q}(P_1/Q_1, \ldots, P_n/Q_n)$ over $\mathbf{Q}$ is m.

Lemma 14.12 *Suppose that we have constructed (2.3). Then the transcendental degree of $K' = K(P_1/Q_1, \ldots, P_n/Q_n)$ over K is $d = m - s > 0$. Therefore, the parameters are independent iff $s = 0$.*

Theorem 14.13 *(Gao and Chou 1991a) If the parameters of (1.2) are not independent then one can find a set of new RPEs*

$$x_1 = P_1'/Q_1', \ldots, x_n = P_n'/Q_n' \tag{4.1}$$

which has the same implicit variety as (1.2) but with independent parameters.

Proof. Since (2.3) is irreducible, we may assume that the initials I_i of B_i in (2.3) and the initials J_j of A_j in (2.3) are polynomials in $x_1, \ldots, x_d, t_1, \ldots, t_s$. Since Q_i is not in $PD(F_1, \ldots, F_n) = PD(ASC)$, we can find a nonzero polynomial q_i in the parameters of ASC, i.e., $x_1, \ldots, x_d$ and $t_1, \ldots, t_s$, such that

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

Let $M = \prod_{i=1}^{m-s} I_i \cdot \prod_{j=1}^{n} q_j$. Then M is a polynomial of $x_1, \ldots, x_d, t_1, \ldots, t_s$. Let $h_1, \ldots, h_s$ be integers such that when replacing t_i by h_i, $i = 1, \ldots, s$, M becomes a nonzero polynomial of $x_1, \ldots, x_d$. Let P_i' and Q_i' be the polynomials obtained from P_i and Q_i by replacing t_i by h_i, $i = 1, \ldots, s$. Now we have obtained (4.1). ∎

The computation in the above theorem can be done with the Gröbner basis method (Gao and Chou 1992a).

Example 14.14 *For Example 14.3, we have $d = 1, s = 1$; hence the parameters u and v are not independent. To re-parameterize (2.1), by Theorem 14.13, we have to compute M. Since* $\text{prem}(u - v, ASC) = 2u$ $M = 2(x + 1)u$, *selecting a value of u, say 1, 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 ideal as (2.1) and has an independent parameter v.

14.5 Inversion maps and proper parametric equations

The *inversion problem* is that given a point $(a_1, \ldots, a_n)$ on the image of (1.2), find a set of values $(\tau_1, \ldots, \tau_m)$ for the t such that

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

This 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.

Inversion maps for (1.2) are functions

$$t_1 = f_1(x_1, \ldots, x_n), \ldots, t_m = f_m(x_1, \ldots, x_n)$$

such that $x_i \equiv P_i(f_1, \ldots, f_m)/Q_i(f_1, \ldots, f_m)$ are true on the implicit variety V of (1.2) except for 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. RPEs (1.2) are called *proper* if for each $(a_1, \ldots, a_n) \in IM(P, Q)$ there exists only one $(\tau_1, \ldots, \tau_m) \in E^m$ such that $a_i = P_i(\tau_1, \ldots, \tau_m)/Q_i(\tau_1, \ldots, \tau_m)$, $i = 1, \ldots, n$. Let us assume that the parameters $t_1, \ldots, t_m$ of (1.2) are independent, i.e., $s = 0$. Then (2.3) becomes

$$\begin{array}{ll} & A_1(x_1, \ldots, x_{m+1}) \\ & \ldots \\ & A_{n-m}(x_1, \ldots, x_n) \\ (5.1) & B_1(x_1, \ldots, x_n, t_1) \\ & \ldots \\ & B_m(x_1, \ldots, x_n, t_1, \ldots, t_m) \end{array}$$

Theorem 14.15 *Using the above notations, we have*

(a) $B_i(x, t_1, \ldots, t_i) = 0$ determine t_i $(i = 1, \ldots, m)$ as functions of $x_1, \ldots, x_n$ which are a set of inversion maps for (1.2).

(b) (1.2) is proper if and only if $B_i = I_i t_i - U_i$ are linear in t_i for $i = 1, \ldots, m$, and if this is case, the inversion maps are

$$t_1 = U_1/I_1, \ldots, t_m = U_m/I_m$$

where the I_i and U_i are polynomials in $\mathbf{Q}[X]$.

Theorem 14.16 *(Gao and Chou 1991a) If $m = 1$ and RPEs (1.2) are not proper, we can find a new parameter $s = f(t_1)/g(t_1)$ where f and g are in $\mathbf{Q}[t_1]$ such that the re-parameterization of (1.2) in terms of s,*

$$x_1 = \frac{F_1(s)}{G_1(s)}, \ \ldots, \ x_n = \frac{F_n(s)}{G_n(s)} \tag{5.2}$$

are proper.

Proof. Let $K' = K(P_1/Q_1, \ldots, P_n/Q_n)$. Since $P_1(t_1) - Q_1(t_1)l = 0$ where $l = P_1(t_1)/Q_1(t_1) \in K'$, t_1 is algebraic over K'. Let $f(y) = a_r y^r + \ldots + a_0$ 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'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. To compute η, by Theorem 14.15, we can find an inversion map $B_1(x_1, \ldots, x_n, t_1) = 0$ of the curve. Then $B_1'(y) = B_1(P_1/Q_1, \ldots, P_n/Q_n, y) = 0$ 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 s can be obtained as follows. If B_1 is linear in t_1, nothing needs to be done. Otherwise let

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

where the b_i are in $\mathbf{Q}[x]$. By (1.2), b_i can also be expressed as rational functions $a_i(t_1)$, $i = 1, \ldots, r$. At least one of a_i/a_r, say a_0/a_r, is not an element in $\mathbf{Q}$. Let $s = a_0/a_r$. Eliminating t_1 from (1.2) and $a_r s - a_0$, we can get (5.2). Note that a_i comes from b_i by substituting x_j by P_j/Q_j, $j = 1, \ldots, n$, then $s = b_0/b_r$ is an inversion map of (5.2). ∎

Theorem 14.16 provides a new constructive proof for Lüroth's Theorem, i.e., we have

Proposition 14.17 *Let $g_1(t), \ldots, g_r(t)$ be elements of $\mathbf{Q}(t)$. Then we can find a $g(t) \in \mathbf{Q}(t)$ such that $\mathbf{Q}(g_1, \ldots, g_r) = \mathbf{Q}(g)$.*

Example 14.18 *Consider the parametric equations for a Bézier curve (Sederberg, 1986):*

$$x = \frac{8s^6-12s^5+32s^3+24s^2+12s}{s^6-3s^5+3s^4+3s^2+3s+1}$$
$$y = \frac{24s^5+54s^4-54s^3-54s^2+30s}{s^6-3s^5+3s^4+3s^2+3s+1}. \tag{5.3}$$

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*

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

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

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

To find a set of proper parametric equations for $g_1 = 0$, *by Theorem 14.16, we select a new parameter*

$$\begin{aligned} t_1 &= \frac{(7280y^2 + (-27006x - 125592)y - 174069x^2 + 598788x - 9767808)}{(15273x^2 + 1098792x - 9767808)} \\ &= \frac{s^2 + 1}{1 - s}. \end{aligned}$$

Eliminating s *from (5.3) and the above equation, we have*

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

which is a a set of proper parametric equations of $g_1 = 0$.

14.6 Normal RPEs

Generally speaking, the image of a set of RPEs is a quasi algebraic set. In this section, we discuss when the image of a set of parametric equations is an algebraic set.

RPEs (1.2) are called a set of *normal parametric equations* if $IM(P, Q)$ is the implicit variety of (1.2). As a consequence of Theorem 14.10, we have:

Theorem 14.19 *We can decide in a finite number of steps whether RPEs (1.2) are normal parametric equations.*

The method in Theorem 14.19, though complete, usually needs tedious computation. In what follows, we give some simple criteria for normal parameterization which can be used without any computational costs.

Theorem 14.20 *(Gao and Chou 1991b) Let*

$$y_1 = u_1(t)/v_1(t), \ldots, y_n = u_n(t)/v_n(t)$$

be parametric equations of an algebraic curve. If $degree(u_i) > degree(v_i)$ *for some* i, *they are normal parametric equations. As a consequence, a set of polynomial parametric equations of a curve is normal.*

If a set of parametric equations (1.2) is not normal, then naturally we will ask whether we can find a set of normal parametric equations which has the same implicit variety as (1.2). This problem is unsolved in general. But if the implicit variety of the parametric equation is a conic, then we have a solution to the above problem (Gao and Chou 1991b). As an example, we have

Example 14.21 *The image of the following parametric equations*

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

is $\mathrm{Zero}(x^2 + y^2 - 1)$*, i.e., (7.5.1) is a set of normal parametric equations for the unit circle. It is proved in Gao and Chou (1991b) that there exist no real coefficients normal quadratic parametric equations for the unit circle.*

14.7 Parameterization of algebraic varieties

Finding RPEs for algebraic varieties usually involves two steps:

1. To construct a hypersurface which is birational to the given irreducible variety and birational transformations between the hypersurface and the variety.

2. To find RPEs for the hypersurface obtained in the first step. A set of RPEs for the algebraic variety can be obtained from the RPEs of the hypersurface and the birational transformations.

There are complete results for the first step. The second step has been solved only for algebraic curves and surfaces.

14.7.1 The theory of resolvents

We will introduce a constructive proof for the following theorem (Hartshorne 1977) with the concept of resolvents (Ritt 1954).

Theorem 14.22 *Any irreducible variety of dimension r is birational to a hypersurface in E^{r+1}.*

A prime ideal distinct from (1) and (0) is called *nontrivial.* In what follows, we assume that ID is a nontrivial prime ideal in $K[x_1, \ldots, x_n]$. We can divide the x into two sets, $u_1, \ldots, u_q$ and $y_1, \ldots, y_p$, $p + q = n$, such that no nonzero polynomial of ID involves the u alone, while, for each $j = 1, \ldots, p$, there is a nonzero polynomial in ID involving y_j and the u alone. We call the u a *parameter set* of ID. A CS of ID, e.g., the minimal CS in Gao (1989), under the variable order $u_1 < \ldots < u_q < y_1 < \ldots < y_p$ is of the form

$$ASC = A_1(u, y_1), A_2(u, y_1, y_2), \ldots, A_p(u, y_1, \ldots, y_p)$$

where A_i is a polynomial involving y_i effectively and we also have $ID = PD(ASC)$. It is clear that the dimension of $ID = PD(ASC)$ is equal to the number of parameters of ID.

Lemma 14.23 *Let the notations be the same as above. Then for a new variable w, there exist polynomials $M_1, \ldots, M_p, G$ of the u, such that*

(1) two distinct zeros of ID with the u taking the same values for which G does not vanish give different values for $Q = M_1y_1 + \ldots + M_py_p$; and

(2) a CS of the prime ideal $ID_1 = Ideal(ID, w - Q)$ under the following variable order $u_1 < \ldots < u_q < w < y_1 < \ldots < y_p$ is of the form

$$A(u, w), A_1(u, w, y_1), \ldots, A_p(u, w, y_p)$$

where A is an irreducible polynomial in w and each A_i is linear in y_i.

For a proof of this result, see p85, (Ritt, 1954) or (Gao, 1991b) for general ideals. According to Ritt, we call the equation $A = 0$ a *resolvent* of ID.

Theorem 14.24 *Let ID be a prime ideal in $\mathbf{Q}[u_1, \ldots, u_q, y_1, \ldots, y_p]$ where the u are the parameters of ID, and let $A(u, w) = 0$ be a resolvent of ID. Then* $\mathrm{Zero}(ID)$ *is birational to the hypersurface* $\mathrm{Zero}(A)$.

Proof. Use the same notations as in Lemma 14.23. We define a morphism

$$MP_1 : \mathrm{Zero}(ID) \to \mathrm{Zero}(A)$$

by setting $MP_1(u_1, \ldots, u_q, y_1, \ldots, y_p) = (u_1, \ldots, u_q, M_1y_1 + \ldots + M_py_p)$ where the M_i are the same as in Lemma 14.23. By (2) of Lemma 14.23, we can assume $A_i = I_iy_i - U_i, i = 1, \ldots, p$ where I_i and U_i are polynomials in the u and w. We can further assume that I_i are free of w. We define another morphism

$$MP_2 : \mathrm{Zero}(A) \to \mathrm{Zero}(ID)$$

by setting $MP_2(u_1, \ldots, u_q, w) = (u_1, \ldots, u_q, U_1/I_1, \ldots, U_p/I_p)$. Let $I = \prod_{i=1}^p I_i$. Then MP_2 is well defined on $D_1 = \mathrm{Zero}(A) - \mathrm{Zero}(I)$. We can prove that MP_1 and MP_2 are birational transformations between the variety and the hypersurface. ∎

The following algorithm provides a constructive proof for Theorem 14.22.

Algorithm 14.25 *Let $PS = \{f_1, \ldots, f_s\}$ be a polynomial set in $K[x]$. The algorithm decides whether $V =$* $\mathrm{Zero}(PS)$ *is an irreducible variety, and if it is, finds an irreducible polynomial H such that V is birational to the hypersurface* $\mathrm{Zero}(H)$.

Step 1. By Wu-Ritt zero decomposition algorithm, we have an irredundant decomposition

$$V = \mathrm{Zero}(PS) = \cup_{i=1}^m \mathrm{Zero}(ASC_i/I_i).$$

V is an irreducible variety if there exists one component, say, $\mathrm{Zero}(ASC_1/I_1)$, such that $DIM(ASC_1) > DIM(ASC_i)$ and $\mathrm{Zero}(ASC_i/I_i) \subset \mathrm{Zero}(PD(ASC_1))$ for $i > 1$. We have that $V = \mathrm{Zero}(PD(ASC_1))$.

Step 2. Let $ASC_1 = A_1, \ldots, A_p$. We make a renaming of the variables. If A_i is of class m_i, we rename x_{m_i} as y_i, the other variables are renamed as $u_1, \ldots, u_q$, where $q = n - p$.

Step 3. Let $\lambda_1, \ldots, \lambda_p, w$ be new indeterminates and let $ID = Ideal(PD(ASC_1), w - Q)$ where $Q = \lambda_1y_1 + \ldots + \lambda_py_p$. ID is a prime ideal in $K(u, \lambda, w, y)$ with parameters u and λ. Let

$$R(u, \lambda, w), R_1(u, \lambda, w, y_1), \ldots, R_p(u, \lambda, w, y_p) \tag{7.1}$$

be a CS of ID. As the λ are indeterminates, by (1) of Lemma 14.23, R_i are linear in y_i.
Step 4. By Wu-Ritt zero decomposition algorithm, under the variable order $u < \lambda < w < y_1 < \ldots < y_p$ we have

$$\mathrm{Zero}(ASC_1 \cup \{w - Q'\}) = \cup_{i=1}^{t} \mathrm{Zero}(PD(ASC_i')).$$

There only exists one component in the above decomposition, say $\mathrm{Zero}(PD(ASC_1'))$, on which the u and λ are algebraically independent and ASC_1' is a CS of ID. For convenience, we assume that ASC_1' is (7.1).
Step 5. We can assume that for each $1 \le i \le p$, the initial I_i of R_i involves u and λ alone. Let $D = I \prod_{i=1}^{p} I_i$ where I is the initial of R. Then D is a polynomial in u and λ.
Step 6. Let $a_1, \ldots, a_p$ be integers for which D becomes a nonzero polynomial in the u when each λ_i is replaced by a_i. Then for $\lambda_i = a_i, i = 1, \ldots, p$, (7.1) becomes

$$R', R_1', \ldots, R_p' \tag{7.2}$$

where R and R' have the same degree in w, and y_i occurs in R_i' effectively.
Step 7. We can prove that R' is an irreducible polynomial in w, and (7.2) is a CS of $ID'' = Ideal(PD(ASC_1), w - a_1 y_1 - \ldots - a_p y_p)$. Hence R' is a resolvent of $PD(ASC_1)$, and $\mathrm{Zero}(R')$ is birational to $\mathrm{Zero}(PS)$. The birational transformations can be obtained as in Theorem 14.24. ▮

In practice, we may use a probability approach by randomly selecting p integers $a_1, \ldots, a_p$ in Step 5. The success probability of the selection of the integers is one.

14.7.2 Parameterization of algebraic curves

An irreducible algebraic curve $C = \mathrm{Zero}(PS)$ (where $PS \subset K[X]$) is called *rational* if it has a set of RPEs. By the the resolvent theory, we need only to find a set of RPEs for $f(x, y) = 0$. The following method for parameterization of $f(x, y) = 0$ is based on Theorem 14.26 and Lüroth's theorem (Walker 1950).

Theorem 14.26 *Let $x = u(t)/w(t), y = v(t)/w(t)$ be a set of proper parametric equations for a plane curve $f(x, y) = 0$. We assume $gcd(u, v, w) = 1$. Then the degree of f is equal to the degree of the parametric equations.*

Algorithm 14.27 *Let $f(x, y)$ be an irreducible polynomial. The algorithm decides whether $f(x, y) = 0$ is a rational irreducible algebraic curve, and if it is, finds a set of RPEs for C.*

Step 1. By Lüroth's theorem, a rational curve always has a set of proper parametric equations (Walker 1950). By Theorem 14.26, if $f(x, y) = 0$ is rational then it has a set of parametric equations of degree d. Let

$$x = u(t)/w(t), y = v(t)/w(t)$$

where $u(t) = u_d t^d + \ldots + u_0$, $v(t) = v_d t^d + \ldots + v_0$, and $w(t) = w_d t^d + \ldots + w_0$ for indeterminates u_i, v_i, and w_i.
Step 2. Replacing x and y by $u(t)/w(t)$ and $v(t)/w(t)$ in $f(x, y) = 0$ respectively and clearing denominators, we obtain a polynomial Q in t whose coefficients are polynomials in u_i, v_i and w_i. Let the set of coefficients of Q as a polynomial of t be $HS = \{P_1, \ldots, P_h\}$.

Step 3. Curve $f = 0$ has a set of RPEs iff HS has a set of zeros such that when the coefficients of $u(t)$, $v(t)$ and $w(t)$ are replaced by the zeros, u/w and v/w are not constants in K. By Step 4, we can decide whether there exist such zeros of HS.
Step 4. Let $DS_1 = \{u_i w_j - u_j w_i \mid i, j = 0, \ldots, d\}$, $DS_2 = \{v_i w_j - v_j w_i \mid i, j = 0, \ldots, d\}$. Then $f = 0$ is rational iff $HD = \mathrm{Zero}(HS) - (\mathrm{Zero}(DS_1) \cup \mathrm{Zero}(DS_2))$ is not empty, and if it is not empty, each zero of HD provides a set of parametric equations for $f = 0$. ▮

In Step 6, we need to solve a system of algebraic equations. There are many methods for doing this. We can use, e.g., the method based on Wu-Ritt CS method (Wu 1987). For the implementation of this algorithm, please refer Chap.24.

14.8 Conclusions

For a set of RPEs of the form (1.2), the following results are summarized.

1. We can find a basis for the implicit ideal of (1.2).
2. We can compute the image of (1.2) and represent the image as a canonical form.
3. We can decide whether the parameters $t_1, \ldots, t_m$ are independent, and if not, re-parameterize (1.2) such that the parameters of the new parametric equations are independent.
4. If the parameters of (1.2) are independent, we can construct equations
$$B_1(x_1, \ldots, x_n, t_1) = 0, \ldots, B_m(x_1, \ldots, x_n, t_1, \ldots, t_m) = 0$$
the solution of the t_i in terms of the x_i are the inversion maps of (1.2), and (1.2) is proper iff the B_i are linear in t_i, $i = 1, \ldots, m$.
5. If $m = 1$ and (1.2) is not proper, we can re-parameterize (1.2) such that the new parametric equations are proper. In general, to find a set of proper re-parameterization for (1.2) is still open.
6. We can decide whether a set of parametric equations is normal. We can also find a normal re-parameterization for a set of non-normal parametric equations of conics. The general case for this problem is still open.
7. We can construct a hypersurface which is birational to a given irreducible variety and birational transformations between the hypersurface and the variety.
8. We can find a set of RPEs for a plane curve if it exists. The problem of finding a set of RPEs for a hypersurfaces of dimension higher than two is still open.

References.

Abhyankar, S. S. and Bajaj, C. (1988): Automatic parameterization of rational curves and surfaces, III: algebraic plane curves, *Comp. Aided Geo. Design*, **5**, 309-321.
Abhyankar, S. S. and Bajaj, C. (1989): Automatic parameterization of rational curves and surfaces, IV: algebraic space curves, *ACM Tran. in Graphics*, **8**(4), 325-333.

Alonso, M. E., Mora, T., Niesi, G. and Raimondo, M. (1992): Local parameterization of space curves at singular points, *Proc. of IWMM*, pp. 135–166, Beijing, International Academic Press.

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, pp. 431–436.

Buchberger, B. (1985): Grobner 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**, 125–155.

Chionh, E. W., (1990): *Base points, resultants, and the implicit representation of rational surfaces*, Phd Thesis, The Univ. of Waterloo.

Chuang, J. H. and Hoffman, C. M. (1989): On local implicit approximation and its applications, *ACM Tran. in Graphics*, **8**(4), 298–324.

Chou, S. C. (1988): *Mechanical geometry theorem proving*, D.Reidel Publishing Company, Dordrecht, Netherlands.

Chou, S. C. and Gao, X. S. (1990a): Ritt-Wu's decomposition algorithm and geometry theorem proving, *CADE'10*, M.E. Stickel (Ed.) pp 207–220, Lect. Notes in Comp. Sci., No. 449, Springer-Verlag, 1990.

Chou, S. C. and Gao, X. S. (1992b): An algebraic system based on the characteristic method, *Proc. of International Workshop on Mathematics Mechanization*, Beijing, International Academic Publishers, pp.1–17, 1992.

Chou, S.C., Gao, X.S. and Li, Z.M. (1994): Computations with Rational Parametric Equations, *Computer Mathematics*, pp.86-111, World Scientific Pub., River Edg. NJ.

Collins, G. E. (1975): Quantifier elimination for real closed fields by cylindrical algebraic decomposition, *Lect. Notes Comp. Sci.*, No. 33, pp. 134–183, Springer-Verlag.

Eisenbud D. (1991): Open problems in computational algebraic geometry, in *Cortona 1991* and *Proc. of Symp. Math*, Vol 34, pp. 49–70, 1993.

Faux, I. D. and Pratt, M. J. (1979): *Computational geometry for design and manufacture*, Ellis Horwood, Chichester.

Farouki, R. T. and Neff, C. A. (1989): Automatic parsing of degenerate quadric-surface intersections, *ACM Trac. on Graphics*, **8**(3).

Gao X. S. (1989): The Minimal Characteristic Basis of a Polynomial Ideal, *J. Sys. Sci. and Math Sci.*, **2**, 236–242.

Gao, X. S. (1991b): On the theory of resolvents and its applications, *MM-Research Preprints*, No.6, 1991, Inst. of Systems Science, Academia Sinica, pp.79-93.

Gao, X. S. and Chou S.C. (1991a): Computations with parametric equations, *Proc. of ISSAC-91*, ACM Press, New York, pp.122-127.

Gao, X. S. and Chou S.C. (1991b): On the normal parameterization of curves and surfaces, *The International Journal of Computational Geometry and Applications*, **1**, 125–136, World Scientific Press.

Gao, X. S. and Chou S.C. (1992a): Implicitization of rational parametric equations, *Journal of Symbolic Computation*, **14**, 459–470.

Gao, X. S. and Chou, S. C. (1992b): On the parameterization of algebraic curves, *Applicable Algebra in Elementary Communication and Computing*, **3**, 27–38.

Gao, X. S. and Chou, S. C. (1992c): Solving parametric algebraic systems, *Proc. ISSAC-92*, P.S. Wang (eds), pp. 335–341, ACM Press.

Garrity, T. and Warren, J. (1989): On computing the intersection of a pair of algebraic surfaces, *Computer Aided Geometric Design*, **6**, 137–153.

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

Heintz, J. (1983): Definability and fast quantifier elimination in algebraically closed fields, *Theoretic Computing Science*, **24**, 239–278.

Hoffmann, C. M. (1989): *Geometric and solid modeling: an introduction*, Morgan Kaufmann Publishers Inc, 1989.

Hoffmann, C. M. (1990): Algebraic and numeric techniques for offsets and blends, in *Computations of Curves and Surfaces*, (eds. W. Dahman), pp.499–529, Kluwer Academic Publishers.

Kalkbrener, M.(1990a): Implicitization of rational parametric curves and surfaces, *Proc. of AAECC-8,*, ACM press, New York.

Kalkbrener, M.(1990b): Implicitization by using Gröbner bases, Technical Report RISC Series 90–27, Unin. of Linz.

Kalkbrener, M. (1990c): Birational projections of irreducible varieties, Tech. Report, RISC-Linz no. 90-59.0.

Li, L. (1996): Approximate parametrization of prime ideals in neighborhood of a given point, *Proc. od ASCM'96*, pp. 19–30, Kobe, Scientists Incorporated.

Li, Z. M. (1987): On the triangulation for any polynomial set, *MM Research Preprints*, No. 2, pp.48–54, Institute of systems science, Academia Sinica.

Li, Z. M. (1989): Automatic implicitization of parametric objects, *MM Research Preprints*, No. 4, pp. 54-62, Inst. of Sys. Sci., Academia Sinica.

Manocha, D. and Canny J. F. (1991): Efficient techniques for multipolynomial resultant algorithms, *proc. of ISSAC'90*, ACM Press, Bonn.

Ollivier, F. (1989): Inversibility of rational mappings and structural identifiability in automatics, *Proc. of ISSAC-89*, pp.43–54, ACM Press.

Pratt, M. J. (1986): Parametric curves and surfaces used in computer aided design, in *The Mathematics of Surfaces* (ed. by J.A. Gregory), pp.19–46, Clarendon Press, Oxford.

Sederberg, T. W. (1986): Improperly parameterized rational curves, *Computer Aided Geometric Design*, **3**, 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.*, **28**, 72–84.

Sederberg, T.W., Anderson, D. C. and Goldman, R. N. (1985): Implicitization, inversion, and intersection of planar rational cubic curves, *Vision, Graph, Image Proc.*, **31**, 89–102.

Sederberg, T.W. and Kakimoto, M. (1990): Approximation rational curves using polynomial curves, ECGL 90-03, June 1990.

Sendra, J. R. and Winkler, F. (1991): Symbolic parameterization curves, *J. of Symbolic Computation*, **12**, 607–632, 1991.

Seidenberg, A. (1956): An elimination theory for differential algebra. Univ. California Publ. Math. (N.S.) **3**/2: 31–66.

Shannon, S. and Sweedler, M. (1988): Using Gröbner bases to determine algebraic membership, *J. Symbolic Computation*, **6**, 267–273, Academic Press.

Schicho, J. (1995): *Rational Parameterization of Algebraic Surfaces*, PhD Thesis, Johannes Kepler University, Linz.

Shoenfield, J. R. (1967): *Mathematical logic*, Addison-Wesley.

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.

Wang, D. (1992): Irreducible decomposition of algebraic varieties via characteristic set method and Gröbner basis method, *CAGD*. **9**, 471–484.

Wang, D. (1995a): An implementation of the characteristic set method in Maple. In: Pfalzgraf, J., Wang, D. (eds.): *Automated practical reasoning: Algebraic approaches.* Springer, Wien New York, pp. 187–201.

Wang, D. (1995b): Reasoning about geometric problems using an elimination method. In: Pfalzgraf, J., Wang, D. (eds.): *Automated practical reasoning: Algebraic approaches.* Springer, Wien New York, pp. 147–185.

Wu, W. T. (1984): Basic principles of mechanical theorem proving in elementary geometries, *J. Sys. Sci.* and *Math. Scis.*, **4**(1984), 207–235, Re-published in *J. Automated Reasoning*, 1986.

Wu, W.T. (1986): On zeros of algebraic equations — an application of Ritt principle, *Kexue Tongbao*, **31**, 1–5.

Wu, W.T. (1989): On a projection theorem of quasi-varieties in elimination theory, *MM Research Preprints*, No. 4, Inst. of Sys. Sci., Academia Sinica, pp.40–48.