

# On the Parameterization of Algebraic Curves\*

Xiao-Shan Gao  
Institute of Systems Science, Academia Sinica  
Shang-Ching Chou  
Wichita State University

The paper is published on “*Journal of Applicable Algebra in Engineering, Communication and Computing*”, **3**, 27-38 (1992)

**Abstract.** In this paper, by using the concept of resolvents of a prime ideal introduced by Ritt, we give methods for constructing a hypersurface which is birational to a given irreducible variety and birational transformations between the hypersurface and the variety. In the case of algebraic curves, this implies that for an irreducible algebraic curve  $C$ , we can construct a plane curve which is birational to  $C$ . We also present a method to find rational parametric equations for a plane curve if it exists. Hence we have a complete method of parameterization for algebraic curves. The method is used to find a set of parametric equations of the intersection curve of two space surfaces.

**Keywords.** Computer modeling, parameterization, surface intersections, algebraic curves, resolvents, Ritt–Wu’s decomposition algorithm, Gröbner bases.

## 1 Introduction

Rational algebraic curves are widely used in computer modeling and computer graphics and it is recognized that both implicit and parametric representations

---

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

## 1. Introduction

for rational curves have their inherent advantages: the parametric representation 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 [Sederberg & Anderson, 1984]. This motivates the search for a means of converting from one representation to the other. In this paper, we give a complete method of parameterization for algebraic curves in an affine space of any dimension.

In [Abhyankar & Bajaj, 1988], a method for computing the genus of plane curves is given, and if genus = 0, they also gave a method for computing the rational parametric equations of the curve. A natural way for parameterizing a space curve is first to find a plane curve which is birational to the space curve and then a set of parametric equations for the space curve can be found if we can find a set of parametric equations for the plane curve. In [Abhyankar & Bajaj, 1989], this has been done for a special class of space curves, i.e., space curves which can be represented by transversal intersection of two surfaces.

On the other hand, it is a well known result in algebraic geometry that an irreducible variety is birational to a hypersurface [Hartshorne, 1977]. In particular, an irreducible algebraic curve is birational to an irreducible plane curve. However, we need a constructive method for calculating that irreducible plane curve to solve the general parameterization problem for arbitrary algebraic curves. Such a constructive method implicitly exists in a classic book of Ritt [Ritt, 1954]. In this paper, based on Ritt's concept of resolvents, we give algorithms of constructing a hypersurface which is birational to a given irreducible variety. Birational maps between the hypersurface and the variety can also be given. Our algorithms for constructing resolvents are different from Ritt's algorithm in two aspects. First, the input of our algorithms is a set of generators of an ideal, while the input of Ritt's algorithm is an irreducible characteristic set of a prime ideal. Second, our algorithms use Ritt–Wu's decomposition algorithm [Wu, 1984] or the Gröbner basis method [Buchberger, 1985].

In the case of algebraic curves, this implies that for an irreducible algebraic curve  $C$ , we can construct a plane curve which is birational to  $C$ . Thus, to find a set of parametric equations for  $C$  we only need to find a set of parametric equations for the plane curve. Such an algorithm has been given in [Abhyankar & Bajaj, 1988]. In this paper, we present a new algorithm which does not need to compute the genus of the plane curve. Our method is based on the existence of proper parametric equations for a plane curve.

The method is used to surface/surface intersection problem. The calculation of intersection curves between general space surfaces is one of the important problems in computer aided design. Algorithms for intersection problem have been proposed using various elimination theories, e.g [Pratt & Geisow, 1986]. But by randomly eliminating some variables, the plane curve obtained is not necessarily birational to the original space curve. By using the method in this paper, we can find a plane curve which is birational to the intersection of two space surfaces.

## 2. Preliminaries

The implementation of the algorithms in this paper is based on Ritt–Wu’s decomposition algorithm a detailed description of which can be found in [Wu, 1984] or in [Chou & Gao, 1990].

This paper is organized as follows. In section 2, we introduce some basic notations and notions necessary for the rest of this paper. In section 3, we present methods of constructing a resolvent for a prime ideal. In section 4, we present our method of parameterization for a plane curve. In section 5, we consider the applications to space curves.

### 2 Preliminaries

Let  $K$  be a computable field of characteristic zero and  $K[x_1, \dots, x_n]$  or  $K[x]$  be the ring of polynomials in the indeterminates  $x_1, \dots, x_n$ . Unless explicitly mentioned otherwise, all polynomials in this paper are in  $K[x]$ .

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  $ASC = A_1, \dots, A_p$  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  $ASC = A_1, \dots, A_p$  such that  $class(A_1) > 0$ , we define the pseudo remainder of a polynomial  $G$  wrpt  $ASC$  inductively as

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

Let  $R = prem(G; ASC)$ , then we have the following important *remainder formula*:

$$(2.1) \quad JG - R \in Ideal(A_1, \dots, A_p)$$

where  $J$  is a product of powers of the initials of the polynomials in  $ASC$  and  $ideal(A_1, \dots, A_p)$  is the ideal generated by  $A_1, \dots, A_p$ . For an asc chain  $ASC$ , we define

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

For an asc chain  $ASC = A_1, \dots, A_p$ , we always 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  $u_1, \dots, u_q$ , where  $q = n - p$ . The variables  $u_1, \dots, u_q$  are called the *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 in  $K_{i-1}[y_i]$  where  $K_{i-1} = K(u)[y_1, \dots, y_{i-1}]/D$  where  $D$  is the ideal generated by  $A_1, \dots, A_{i-1}$  in  $K(u)[y_1, \dots, y_{i-1}]$ .

**Definition 2.2.** The dimension of an irreducible ascending chain  $ASC = A_1, \dots, A_p$  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. A *characteristic (ab. char) set* of a polynomial ideal  $D$  is an ascending chain  $ASC$  in  $D$  such that for all  $P \in D$   $prem(P, ASC) = 0$ .

**Lemma 2.3.** (Lemma 3.3, [Wu, 1984]) If  $ASC$  is an irreducible ascending chain then  $PD(ASC)$  is a prime ideal with dimension  $DIM(ASC)$ . Conversely, each char set of a prime ideal is irreducible.

**Lemma 2.4.** (Lemma 3.4, [Wu, 1984]) Let  $ASC$  be an irreducible asc chain with parameters  $u_1, \dots, u_q$ . If  $Q$  is a polynomial not in  $PD(ASC)$ , then we can find a polynomial  $P$  in the  $u$  alone such that  $P \in ideal(ASC \cup \{Q\})$ .

**Lemma 2.5.** Let  $ASC$  be an irreducible asc chain with parameters  $u_1, \dots, u_q$ , 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 parameters  $u$ .

*Proof.* Let  $ASC = \{A_1, \dots, A_p\}$  and  $I_i = int(A_i)$ . By Lemma 2.4, for each  $i$  we can find a polynomial  $P_i$  of  $y_i$  and the  $u$  and polynomials  $Q_k$  ( $k = 1, \dots, i$ ) 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  $ASC' = \{A_1, A'_2, \dots, A'_p\}$  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 char set of  $PD(ASC)$ , i.e.,  $PD(ASC') = PD(ASC)$  and  $ASC'$  is irreducible by Lemma 2.3. .QED.

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

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

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

**Theorem 2.6.** (Theorem 3.2, [Wu, 1984]) For a finite polynomial set  $PS$ , we can either detect the emptiness of  $Zero(PS)$  or furnish an irredundant decomposition of the following form

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

where  $ASC_i$  is an irreducible asc chain for each  $i \leq l$  and there are no  $i \neq j$  such that  $PD(ASC_i) \subset PD(ASC_j)$ .

### 3 Methods of Constructing Resolvents for Prime Ideals

In this section, we shall give a constructive proof for the following theorem [Hartshorne, 1977], i.e., give methods for constructing a hypersurface birational to a given irreducible variety.

**Theorem 3.1.** Any irreducible variety of dimension  $r$  is birational to a hypersurface in  $E^{r+1}$ .

We first introduce the concept of resolvents. A prime ideal distinct from (1) and (0) is called *nontrivial*. In what follows, we assume  $ID$  is a nontrivial prime ideal in  $K[x_1, \dots, x_n]$ . We can divide the  $x$  into two sets,  $u_1, \dots, u_q$  and  $y_1, \dots, y_p$ ,  $p + q = n$ , such that no nonzero polynomial of  $ID$  involves the  $u$  alone, while, for  $j = 1, \dots, p$ , there is a nonzero polynomial in  $ID$  in  $y_j$  and the  $u$  alone. We call the  $u$  a *parameter set* of  $ID$ .

**Lemma 3.2.** Use the notations as above. A char set of  $ID$  under the variable order order  $u_1 < \dots < u_q < y_1 < \dots < y_p$  is of the form

$$(3.2.1) \quad ASC = A_1(u, y_1), A_2(u, y_1, y_2), \dots, A_p(u, y_1, \dots, y_p)$$

where  $A_i$  is a polynomial involving  $y_i$  effectively and we also have  $ID = PD(ASC)$ .

*Proof.* Let  $A_1$  be a polynomial of  $y_1$  and the  $u$  in  $ID$  with lowest degree in  $y_1$  and  $ID_1$  be the polynomials of  $y_1, y_2$ , and the  $u$  in  $ID$  whose degrees in  $y_1$  are less than the degree of  $A_1$  in  $y_1$ .  $ID_1$  is not empty, because by the definition of the  $u$  there is a polynomial  $P$  of the  $u$  and  $y_2$  in  $ID$  and  $P$  is obviously in  $ID_1$ . It is also clear that all the polynomials in  $ID_1$  involve  $y_2$  effectively as  $A_1$  is of lowest degree in  $y_1$ . Let  $A_2$  be a polynomial in  $ID_1$  with lowest degree in  $y_2$ . Let  $ID_2 \subset K[U, y_1, y_2, y_3] \cap ID$  such that the polynomials in  $ID_2$  are with lower degrees in  $y_i$  than  $A_i$ ,  $i = 1, 2$ . Continuing this procedure, at last we obtain an  $ASC$ . For any polynomial  $P \in ID$ ,  $R = \text{prem}(P, ASC)$  is of lower degree in  $y_i$  than the degree of  $y_i$  in  $A_i$  hence must be zero, i.e.  $ASC$  is a char set of  $ID$ . We have proved  $ID \subset PD(ASC)$ . For  $P \in PD(ASC)$ , by (2.1) we have  $JP \in \text{Ideal}(ASC) \subset ID$  where  $J$  is a product of powers of the initials of the polynomials in  $ASC$ . Since the initials are not in  $ID$  and  $ID$  is a prime ideal, we have  $P \in ID$ , i.e.,  $ID = PD(ASC)$ . .QED.

By Lemma 3.2, the parameter set of a prime ideal  $ID$  is also the parameter set of a char set of  $ID$ .

**Lemma 3.3.** Let the notations be the same as above, then for a new variable  $w$ , there exist polynomials  $M_1, \dots, M_p, G$  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  $Q = M_1y_1 + \dots + M_py_p$ ; and

(2) a char set of the prime ideal  $ID_1 = \text{Ideal}(ID, w - Q)$  under the following variable order  $u_1 < \dots < u_q < w < y_1 < \dots < y_p$  is of the form

$$(3.3.1) \quad A(u, w), A_1(u, w, y_1), \dots, A_p(u, w, y_p)$$

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

*Proof.* See p85, [Ritt, 1954]. .QED.

According to Ritt, we call the equation  $A = 0$  a *resolvent* of  $ID$ . Note that  $ID_1$  in Lemma 3.3 is also a prime ideal and the polynomials in  $ID_1$  which are free of  $w$  are precisely the polynomials of  $ID$ .

**Theorem 3.4.** Let  $ID$  be a prime ideal in  $K[u_1, \dots, u_q, y_1, \dots, y_p]$  where the  $u$  are the parameters of  $ID$ , and let  $A(u, w) = 0$  be a resolvent of  $ID$ . Then  $Zero(ID)$  is birational to the hypersurface  $Zero(A)$ .

*Proof.* Use the same notations as Lemma 3.3. We define a morphism

$$MP_1 : Zero(ID) \rightarrow Zero(A)$$

by setting  $MP_1(u_1, \dots, u_q, y_1, \dots, y_p) = (u_1, \dots, u_q, M_1y_1 + \dots + M_py_p)$  where the  $M_i$  are the same as in Lemma 3.3. By (2) of Lemma 3.3, we can assume  $A_i = I_iy_i - U_i, i = 1, \dots, p$  where  $I_i$  and  $U_i$  are polynomials of the  $u$  and  $w$ . By Lemma 2.5, we can further assume that  $I_i$  are free of  $w$ . We define another morphism

$$MP_2 : Zero(A) \rightarrow Zero(ID)$$

by setting  $MP_2(u_1, \dots, u_q, w) = (u_1, \dots, u_q, U_1/I_1, \dots, U_p/I_p)$ . Let  $I = \prod_{i=1}^p I_i$ , then  $MP_2$  is well defined on  $D_1 = Zero(A) - Zero(I)$ . For a zero  $(u', w')$  in  $D_1$ ,  $(u', U_1(u', w')/I_1(u', w'), \dots, U_p(u', w')/I_p(u', w'))$  is a zero of  $w - \sum_i lm_iy_i$ , i.e.,  $MP_1(MP_2)$  is an identity map on  $D_1$ . Since  $I$  and  $M$  are polynomials of the  $u$ ,  $Zero(ID)$  is birational to  $Zero(A)$ . The birational transformations are given by  $MP_1$  and  $MP_2$ . .QED.

The following algorithm provides a constructive proof for Theorem 3.1.

**Algorithm 3.5.** Let  $PS = \{p_1, \dots, p_h\}$  be a polynomial set in  $K[x]$ . The algorithm decides whether  $V = Zero(PS)$  is an irreducible variety, and if it is, finds an irreducible polynomial  $H$  such that  $V$  is birational to the hypersurface  $Zero(H)$ . We also give birational maps between  $V$  and the hypersurface  $Zero(H)$ .

Step 1. By Theorem 2.6, we have an irredundant decomposition

$$Zero(PS) = \cup_{i=1}^m Zero(PD(ASC_i)).$$

$V$  is an irreducible variety iff  $m = 1$ . If  $m = 1$  goto Step 2; otherwise  $Zero(PS)$  is not irreducible and the algorithm terminates.

Step 2. Let  $ASC_1 = A_1, \dots, A_p$ . 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  $u_1, \dots, u_q$ , where  $q = n - p$ .

Step 3. Let  $lm_1, \dots, lm_p, w$  be new indeterminates and let  $ID = Ideal(PD(ASC_1), w - Q)$  where  $Q = lm_1y_1 + \dots + lm_py_p$ .  $ID$  is a prime ideal in  $K[u, lm, w, y]$  with parameters  $u$  and  $lm$ . Let

$$(3.5.1) \quad R(u, lm, w), R_1(u, lm, w, y_1), \dots, R_p(u, lm, w, y_p)$$

be a char set of  $ID$ . As the  $lm$  are indeterminates, by (1) of Lemma 3.3,  $R_i$  are linear in  $y_i$ .

Step 4. To construct (3.5.1), we first make a simplification. We replace  $lm_i$  by 0 in  $Q$  if  $A_i$  is linear in  $y_i$ . we denote the new  $Q$  by  $Q'$  and  $ID' =$

$Ideal(PD(ASC_1), w - Q')$ . This is possible, because if  $A_i$  is linear in  $y_i$  then all other polynomials in  $ASC$  are free of  $y_i$  and hence  $y_i$  does no effect the linearization of the other variables. If all  $A_i$  are linear in  $y_i$  then  $V$  is birational to the affine space  $E^q$ . Otherwise goto Step 5.

Step 5. By Theorem 2.6, under the variable order  $u < lm < w < y_1 < \dots < y_p$  we have

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

We shall show below that there only exists one component in the above decomposition, say  $Zero(PD(ASC'_1))$ , with the  $u$  and the  $lm$  as parameter set and  $ASC'_1$  is a char set of  $ID'$ . For convenience, we assume  $ASC'_1$  is (3.5.1).

Step 6. By Lemma 2.5, we can assume that for each  $1 \leq i \leq p$ , the initial  $I_i$  of  $R_i$  involves the  $u$  alone. Let  $D = I \prod_{i=1}^p I_i$  where  $I$  is the initial of  $R$ , then  $D$  is a polynomial of the  $u$  and the  $lm$ .

Step 7. Let  $a_1, \dots, a_p$  be integers for which  $D$  becomes a nonzero polynomial in the  $u$  when each  $lm_i$  is replaced by  $a_i$ , then for  $lm_i = a_i, i = 1, \dots, p$ , (3.5.1) becomes

$$(3.5.2) \quad R', R'_1, \dots, R'_p$$

where  $R$  and  $R'$  have the same degree in  $w$ , and  $y_i$  occurs in  $R'_i$  effectively.

Step 8. We shall prove below that  $R'$  is an irreducible polynomial in  $w$  and (3.5.2) is a char set of  $ID'' = Ideal(PD(ASC_1), w - a_1y_1 - \dots - a_p y_p)$ . Hence  $R'$  is a resolvent of  $PD(ASC_1)$  and  $Zero(R')$  is birational to  $Zero(PS)$ . The birational transformations can be obtained as Theorem 3.4. .QED.

**Proof of the Correctness for Algorithm 3.5.** Only Step 5 and Step 8 need proofs. In Step 5, let  $ASC_1 = A_1, \dots, A_p$ , by (2.1) we have

$$Zero(ASC_1) = Zero(PD(ASC_1)) \cup \bigcup_{i=1}^p Zero(ASC_1 \cup \{int(A_i)\})$$

where  $int(A_i)$  is the initial of  $A_i$ . By Lemma 2.4, there is a polynomial  $U_i$  in the  $u$  and the  $lm$  such that  $U_i$  is in  $Ideal(ASC_1 \cup \{int(A_i)\})$ . Thus, in  $Zero(ASC_1, w - Q')$  there is only one irreducible component, i.e.  $Zero(PD(ASC_1), w - Q')$ , on which the  $u$  and the  $lm$  are algebraic independent. Therefore  $ASC'_1$  is a char set of  $ID'$ . For Step 8, we only need to prove that  $R'$  is irreducible in  $w$ . Other results are obvious. If  $R'$  is reducible in  $w$ ,  $ID''$  will have a char set  $T, T_1, \dots, T_p$  with  $T$  of lower degree  $g$  in  $w$  than  $R'$  and  $T_i$  are linear in  $y_i$ . We can assume the initials of the  $T_i$  are free of  $w$ . If  $D$  is the product of those initials, we have, for a generic zero of  $ID''$ ,

$$(3.5.3) \quad y_i = \frac{C_{i,g-1}w^{g-1} + \dots + C_{i,0}}{D}$$

where the  $C$  are polynomials in the  $u$ . Let us consider the prime ideal  $ID''' = Ideal(ID, v - lm_1y_1 - \dots - lm_p y_p)$  in  $K[u, lm, v, y]$  for a new indeterminate  $v$ . We will show that  $ID'''$  contains a nonzero polynomial  $P$ , free of the  $y$ , which is

of degree no more than  $g$  in  $v$ . This contradicts to the fact that (3.5.1) is a char set of  $ID$  as both  $w$  and  $v$  are new indeterminates. We consider the relations

$$v^i = (lm_1y_1 + \dots + lm_py_p)^i, \quad i = 1, \dots, g.$$

We replace the  $y$  by their expression in (3.5.3) and depress the degrees in  $w$  of the second members to less than  $g$ , using the relation  $T = 0$ . We have such get a set  $PS$  of  $g$  polynomials of the  $u$ , the  $lm$ ,  $v$ , and  $w$  such that the polynomials in  $PS$  are of degree less than  $g$  in  $w$  and of degree no more than  $g$  in  $v$ . Treating  $w, w^2, \dots, w^{g-1}$  as independent variables in the polynomials in  $PS$ , we eliminate them and get a nonzero polynomial  $Q$  in  $v$  and the  $u$  and the  $lm$ . Note the special position of the  $v^i$  in the polynomials of  $PS$ ,  $Q$  is of degree no more than  $g$  in  $v$ . This polynomial is in  $ID'''$  as  $ID'' \cap K[x] = ID''' \cap K[x]$ . We have completed the proof. .QED.

There are Modifications of Algorithm 3.5. They are different in Step 5.

**Modification 3.6.** In Step 5 of Algorithm 3.5, we can use the Gröbner basis method instead of Theorem 2.6 to compute a char set of  $ID'$  as follows. Let  $GB$  be a Gröbner basis of  $Ideal(PS')$  ( $PS' = ASC_1 \cup \{w - Q'\}$ ) in  $K(u, lm)[w, y]$  in the purely lexicographic ordering  $w < y_1 < \dots < y_p$  (for the Gröbner basis method, see [Buchberger, 1985]). As in  $K(u, lm)[w, y]$ ,  $ID = Ideal(PS')$  defines a zero dimensional prime ideal in  $K(u, lm)[w, y]$ , then  $GB$  is also a char set of  $Ideal(PS')$  by [Chou & Schelter, 1989]. Alternatively, we can also calculate a Gröbner basis  $GB$  of  $Ideal(PS')$  in the pure lexicographic order  $u < lm < w < y_1 < \dots < y_p$  and obtain a char set of  $ID'$  from  $GB$  (see [Chou & Schelter, 1989]).

**Remark.** In practice, Algorithm 3.5 may be very slow, because by introducing new variables  $lm_i$  large dense polynomials could be produced in the procedure. An idea to improve the efficiency is that we can randomly select  $p$  integers  $a_1, \dots, a_p$  and use  $Q' = w - a_1y_1 - \dots - a_py_p$  instead of  $Q = w - alm_1y_1 - \dots - lm_py_p$  to compute the resolvent. We have the following modifications based on this idea.

**Modification 3.7.** In Step 5 of Algorithm 3.5, we randomly select  $p$  integers  $a_1, \dots, a_p$  and find a char set  $ASC$  of  $Ideal(PS \cup \{w - a_1y_1 - \dots - a_py_p\})$  using Theorem 2.6 under the variable order  $u < w < \dots < y_p$ . If  $ASC = \{A(u, w), A_1(u, w, y_1), \dots, A_p(u, w, y_1, \dots, y_p)\}$  where  $A_i$  are linear in  $y_i$ , then the  $A = 0$  is a resolvent of  $PD(ASC_1)$ . The success probability of the selection of the integers should be one, because by Step 7 of Algorithm 3.5, the integer sets which do not suit for the above purpose consist of an algebraic set of lower dimension than  $p$ .

## 4 The Parameterization of Algebraic Curves

An irreducible *algebraic curve* is an irreducible variety of dimension one.

**Definition 4.1.** An irreducible algebraic curve  $C = Zero(PS)$  (where  $PS \subset$



#### 4. The Parameterization of Algebraic Curves

$K[x]$  is called *rational* if there exist polynomials  $u_1, \dots, u_n, w$  of an indeterminate  $t$  such that not all of  $u_i/w$ ,  $i = 1, \dots, n$ , are constants in  $K$  and for  $\forall P \in PS$ ,  $P(u_1/w, \dots, u_n/w) \equiv 0$ . If such polynomials  $u_i$  and  $w$  exist, we call

$$x_1 = u_1/w, \dots, x_n = u_n/w$$

a set of *parametric equations* for the curve. The maximum of the degrees of  $u_i$  and  $w$  is called the degree of the parametric equations.

**Theorem 4.2.** For an irreducible algebraic curve  $C$  in  $A^n$ , we can find a plane curve  $f(x, y) = 0$  which is birational to  $C$ . The birational maps between  $C$  and  $f = 0$  can also be obtained.

*Proof.* By Lemma 3.2, the dimension of a prime ideal is equal to the number of its parameters. Then an irreducible algebraic curve  $C$  has one parameter  $u_1$ . By Algorithm 3.5, the resolvent  $A(u_1, w) = 0$  of the prime ideal which defines  $C$  is a plane curve. The birational maps between  $C$  and  $A = 0$  can be obtained similar as Theorem 3.4. .QED.

It is obvious that  $C$  is rational iff  $f(x, y) = 0$  is rational. Furthermore, using the birational maps between  $C$  and  $f = 0$ , we can find a set of parametric equations for  $C$  (or  $f = 0$ ) if a set of parametric equations for  $f = 0$  (or  $C$ ) is given. Hence, we only need to find a set of rational parametric equations for  $f(x, y) = 0$ .

**Definition 4.3.** A set of parametric equations  $x = u_i/w$  for a curve  $C$  is called *proper* if, except a finite number of points, for each point  $(x'_1, \dots, x'_n)$  on  $C$  there only exists one value  $t_0$  for  $t$  such that  $x'_i = u_i(t_0)/w(t_0)$ ,  $i = 1, \dots, n$ .

By Lüroth's theorem, a rational curve always has a set of proper parametric equations [Walker, 1950].

**Theorem 4.4.** 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.

*Proof.* Let  $f$  be of degree  $d$  and the parametric equations be of degree  $d'$ . Let  $ax + by - 1 = 0$  be the equation of a generic line where  $a$  and  $b$  are indeterminates. The parametric values corresponding to the intersection points between the curve and the line are the roots of the equation  $P(t) = au(t) + bv(t) - w(t) = 0$ . Since  $\gcd(u, v, w) = 1$ ,  $P(t) = 0$  has no repeated roots for general values of  $a$  and  $b$ . Thus  $P(t) = 0$  has  $d'$  distinct roots. By Bezout's theorem [Walker, 1950], the degree of  $f = 0$  is equal to the number of the intersection points between  $f = 0$  and a generic straight line. Hence  $d \leq d'$ . Since the parametric equations are proper,  $d \geq d'$ , i.e.  $d = d'$ . .QED.

**Algorithm 4.5.** Let  $PS$  be a finite set of polynomials in  $K[x]$ . The algorithm decides whether  $C = \text{Zero}(PS)$  is a rational irreducible algebraic curve, and if it is, finds a set of parametric equations for  $C$ .

Step 1. By Theorem 2.6, we have an irredundant decomposition

$$\text{Zero}(PS) = \cup_{i=1}^m \text{Zero}(PD(ASC_i))$$

$C$  is an irreducible algebraic curve iff  $m = 1$  and  $ASC_1$  contains  $n - 1$  polynomials. If  $C$  is an irreducible curve goto Step 2. Otherwise, the algorithm terminates.

Step 2. By Theorem 4.2, we can find a resolvent  $f(x, y) = 0$  of degree  $d$  for  $C$  and birational transformations between  $f = 0$  and  $C$ .

Step 3. Let

$$(4.5.1) \quad x = u(t)/w(t), y = v(t)/w(t)$$

where  $u(t) = u_d t^d + \dots + u_0$ ,  $v(t) = v_d t^d + \dots + v_0$ , and  $w(t) = w_d t^d + \dots + w_0$  for indeterminates  $u_i$ ,  $v_i$ , and  $w_i$ .

Step 4. Replacing  $x$  and  $y$  by  $u(t)/w(t)$  and  $v(t)/w(t)$  in  $f(x, y) = 0$  and clearing denominators, we obtain a polynomial  $Q$  of  $t$  whose coefficients are polynomials of  $u_i$ ,  $v_i$  and  $w_i$ . Let the set of coefficients of  $Q$  as a polynomial of  $t$  is  $HS = \{P_1, \dots, P_h\}$ .

Step 5. By Definition 4.1,  $f = 0$  has a set of parametric equations iff  $HS$  has a set of zeros such that the  $u/w$  and  $v/w$ , when the coefficients of  $u(t)$ ,  $v(t)$ , and  $w(t)$  are replaced by the zeros, are not constants in  $K$ . By step 6, we can decide whether there exist such zeros of  $HS$ .

Step 6. Let  $DS_1 = \{u_i w_j - u_j w_i \mid i, j = 1, \dots, d\}$ ,  $DS_2 = \{v_i w_j - v_j w_i \mid i, j = 1, \dots, d\}$ . Then  $f = 0$  is rational iff  $HD = Zero(HS) - (Zero(DS_1) \cup Zero(DS_2))$  is not empty, and if it is not empty, each zero of  $HD$  provides a set of parametric equations for  $f = 0$ . .QED.

In step 6 of the above algorithm, we have to solve a system of algebraic equations. There are many methods for doing this. We can use the method based on Ritt-Wu's decomposition algorithm [Wu, 1987] or the method based on Gröbner bases method [Buchberger, 1985]. These methods are complete in the field of complex numbers. If one wants to find real coefficients parametric equations, we have to find the real zeros of a system of polynomials which can be done by Collins' CAD method [Collins, 1975].

## 5 The Case of Space Curves

Since *space curves* have applications in computer modeling, we pay special attention to it.

### 5.1. A Refined Algorithm for Space Curve

**Algorithm 5.1.** Let  $PS$  be a polynomial set of indeterminates  $x, y$ , and  $z$ . The algorithm decides whether  $C = Zero(PS)$  is an irreducible space curve, and if it is, finds a plane curve which is birational to  $C$ .

Step 1. Using Theorem 2.6, we find an irredundant decomposition

$$Zero(PS) = \cup_{i=1}^m Zero(PD(ASC_i))$$

## 5. The Case of Space Curves

where  $ASC_i$  are irreducible asc chains.  $C$  is an irreducible space curve iff  $m = 1$  and  $ASC_1$  contains two polynomials. If  $C$  is an irreducible space curve, then goto Step 2, otherwise the algorithm stops.

Step 2. Without loss of generality, we assume  $x$  is the parameter of  $ASC_1$ , then  $ASC_1 = A_1(x, y), A_2(x, y, z)$  ( $x < y < z$ ).

Step 3. If  $A_2$  is linear in  $z$ , i.e.  $A_2 = I_2z - U_2$ ,  $C$  is birational to the plane curve  $A_1 = 0$ . Otherwise goto Step 4.

Step 4. If  $A_1$  is linear in  $y$ , according to the definition of asc chain,  $A_2$  is free of  $y$ . Thus  $C$  is birational to  $Zero(A_2)$ . Otherwise goto Step 5.

Step 5. If there is no polynomial in  $PS \cup \{A_1, A_2\}$  which is linear in some variables, goto Step 6. Otherwise, let  $P$  be a polynomial in  $PS \cup \{A_1, A_2\}$  which is linear in, say  $x$ . Let  $Q$  be another polynomial in  $PS \cup \{A_1, A_2\}$ . We eliminate  $x$  from  $Q$  to obtain a non zero polynomial  $Q'$  of  $y$  and  $z$ . By Step 1, such  $Q$  exists. Let  $Q_1, \dots, Q_l$  be the irreducible factors of  $Q'$ , then one of them, say  $Q_1$ , must be in  $PD(ASC_1)$  (i.e.,  $prem(Q_1, ASC_1) = 0$ ). Then  $C$  is birational to  $Zero(Q_1)$ .

Step 6. This is the general case. For  $(i, j) = (1, 1), (1, -1), (-1, 1), (-1, -1), \dots, (\infty, \infty)$ , by Theorem 2.6, under the variable order  $x < w < y < z$  we have

$$Zero(PS, w - iy - jz) = Zero(PD(ASC))$$

where  $ASC = R(x, w), R_1(x, w, y), R_2(x, w, y, z)$ ; if  $R_1$  is linear in  $y$  and  $R_2$  is linear in  $z$ , goto Step 7. Since such pair of integers actually exists by Algorithm 3.5, this step will terminate after a finite number of steps.

Step 7.  $C$  is birational to  $Zero(R)$ . The birational transformations can be obtained similarly as Theorem 3.4. .QED.

**Example 5.2.** Let  $C$  be the curve defined by  $f = z^2 + y^3 - y^2 - 1 = 0$  and  $g = z^2 - y^2 - x^2 = 0$ . Find a plane curve which is birational to  $C$ .

By Theorem 2.6, under the variable order  $x < y < z$ , we have

$$Zero(f, g) = Zero(PD(ASC_1))$$

where  $ASC_1 = \{A_1 = y^3 + x^2 - 1, A_2 = z^2 - y^2 - x^2\}$ . Thus  $C$  is an irreducible space curve. According to Step 6 of Algorithm 5.1, we chose two integers  $(1, 1)$  and let  $h = w - y - z$ . By Theorem 2.6, under the variable order  $x < w < y < z$ , we have

$$\begin{aligned} Zero(h, f, g) &= Zero(PD(ASC_2)) \quad \text{where} \\ ASC_2 &= \{B_1, B_2, B_3\} \quad \text{and} \\ B_1 &= w^6 - 3x^2w^4 + (8x^2 - 8)w^3 + 3x^4w^2 - x^6 \\ B_2 &= 2wy - w^2 + x^2 \\ B_3 &= 2wz - w^2 - x^2 \end{aligned}$$

$C$  is birational to  $H = Zero(B_1)$ . A birational map from  $C$  to  $H$  is  $(x, y, z) \rightarrow (x, y + z)$ . A birational map from  $H$  to  $C$  is  $(x, w) \rightarrow (x, \frac{w^2 - x^2}{2w}, \frac{w^2 + x^2}{2w})$ . The

curve  $C$  is not rational, because if  $C$  is rational then as the projection of  $C$  to the  $xy$ -plane,  $A_1 = y^3 + x^2 - 1$  must also be rational. But  $A_1 = 0$  is a nonsingular cubic curve which is known to be not rational.

## 5.2 The Surface/Surface Intersection Problem

Using Algorithm 5.1, we can find a plane curve which is birational to the intersection of two space surfaces. Furthermore, we can find parametric equations for the intersection curves if possible. We consider three cases for the intersection problem.

(i) implicit/implicit.

Let curve  $C$  be the intersection of two surfaces whose equations are

$$f(x, y, z) = 0 \text{ and } g(x, y, z) = 0.$$

Using Algorithm 5.1, we can decide whether  $f = 0$  and  $g = 0$  define exactly one irreducible curve, and if it is, find a plane curve which is birational to  $C$ . Example 5.2 belongs to this case.

(ii) implicit/parametric.

Let curve  $C$  be the intersection of two surfaces whose equations are

$$f(x, y, z) = 0 \text{ and } r(u, v) = (x(u, v), y(u, v), z(u, v)).$$

Let  $F(u, v) = f(x(u, v), y(u, v), z(u, v))$ , then there is a surjective rational map from the plane curve  $F = 0$  to  $C$

$$(u, v) \rightarrow (x(u, v), y(u, v), z(u, v)).$$

If we find a set of parametric equations for  $F = 0$ , we can also find a set of parametric equations for  $C$ . But one point on  $C$  may correspond to many points on  $F = 0$ . To find a plane curve which is birational to  $C$ , we can use an idea in [Sederberg & Anderson, 1984]: we first use the elimination theory (e.g., the method in [Sederberg & Anderson, 1984]) to find the implicit equation  $g(x, y, z) = 0$  for the surface represented by  $r(u, v)$  and then use Algorithm 5.1 to find a plane curve which is birational to  $C = \text{Zero}(f, g)$ .

(iii) parametric/parametric.

Let curve  $C$  be the intersection of two surfaces whose equations are

$$r_1 = (x_1(u, v), y_1(u, v), z_1(u, v)) \text{ and } r_2 = (x_2(t, w), y_2(t, w), z_2(t, w)).$$

Similar to case (ii), we can first find the implicit equations  $f(x, y, z) = 0$  and  $g(x, y, z) = 0$  for the surfaces represented by  $r_1(u, v)$  and  $r_2(t, w)$  and then use Algorithm 5.1 to find a plane curve which is birational to  $C = \text{Zero}(f, g)$ .

The following example shows that in case (iii),  $C$  is not necessarily a rational curve, though  $C$  is the intersection of two rational surfaces. Let  $f = y^2 - x^3 + z$ ,  $g = z - 1$ , then  $C$  is obvious birational to  $F = y^2 - x^3 + 1 = 0$  which is not a rational curve. But both  $f = 0$  and  $g = 0$  are obviously rational surfaces.

## References

- [1] bhyankar, S.S. and Bajaj, C. (1988), Automatic Parameterization of Rational Curves and Surfaces, III: Algebraic Plane Curves, *Comp. Aided Geo. Design*, 5(1988), 309-321.
- [2] bhyankar, S.S. and Bajaj, C. (1989), Automatic Parameterization of Rational Curves and Surfaces, IV: Algebraic Space Curves, *ACM Tran. in Graphics*, 8(4), 1989, 325-333.
- [3] uchberger, B. (1985), Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory, in *Recent Trends in Multidimensional Systems theory* (ed. N.K. Bose), D.Reidel Publ. Comp., 1985.
- [4] 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, 1990.
- [5] hou, S.C., Schelter, W. and Yang, G.J. (1989) “Characteristic Sets and Gröbner Bases in Geometry Theorem Proving”, *Resolution of Equations in Algebraic Structure*, Vol. I, pp33–92, Academic Press, Boston.
- [6] ollins, G.E. (1975), Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition, *Lect. Notes Comp. Sci.* 33, 134–183, Springer-Verlag.
- [7] artshorne, R. (1977), *Algebraic Geometry*, Springer-verlag.
- [8] ratt, M.J. and Geisow, A.D. (1986), Surface/Surface Intersection Problems, in *The Mathematics of Surfaces* (ed. by J.A. Gregory), Clarendon Press, Oxford, pp. 19–46.
- [9] itt, J.F. (1954), *Differential Algebra*, Amer. Math. Soc..
- [10] ederberg, T.W., Anderson, D.C. and Goldman, R.N. (1984) Implicit Representation of Parametric Curves and Surfaces, *Comp. Vision, Graph, Image*, vol28 pp 72–84.
- [11] alker, R. (1950), *Algebraic Curves*, Princeton Univ. Press.
- [12] 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.
- [13] u, W.T. (1987), A Zero Structure Theorem for Polynomial Equation - Solving, MM Research Preprints, No1, Ins. of Systems Science.