Solving Parametric Algebraic Systems

Xiao-Shan Gao
Institute of Systems Science, Academia Sinica

Shang-Ching Chou
Department of Computer Science, The Wichita State University

Abstract. For a parametric polynomial system: $p_1 = 0, \cdots, p_r = 0, d_1 \neq 0, \cdots, d_s \neq 0$ where p_i and d_i are in $K[u_1, \cdots, u_m, x_1, \cdots, x_n]$ and the u are parameters, we present a method for identifying all parametric values for which the system has solutions for the x_i and at the same time giving the solutions (for the x_i) of the system in an explicit way, i.e., the solutions are given by polynomial sets in triangular form. The algorithm has been implemented and several examples reported in this paper show the algorithm is of practical value.

1. Introduction

Consider the following algebraic equation system from [BU1]. We need to solve x_1, x_2, x_3, x_4 in terms of the parameters a_1, a_2, a_3, a_4.

$$\begin{aligned} & x_4 - a_4 + a_2 = 0 \\ & x_4 + x_3 + x_2 + x_1 - a_4 - a_3 - a_1 = 0 \\ & x_3x_4 + x_1x_4 + x_2x_3 + x_1x_3 + (-a_3 - a_1)a_4 - a_1a_3 = 0 \\ & x_1x_3x_4 - a_1a_3a_4 = 0, \end{aligned} \tag{1.1}$$

In the literature of solving polynomial equations, e.g., [BU1,LA1,WU3], parametric systems as (1.1) are solved in $A = B[x_1, x_2, x_3, x_4]$ where $B = \mathbf{Q}(a_1, a_2, a_3, a_4)$ is the field of rational functions of a_i. The solutions of (1.1) in A are given by the equations (1.2) below [BU1].

$$\begin{aligned} & x_1^3 - c_1x_1^2 + c_2x_1 - \frac{a_1^2a_3^2a_4^2}{(a_4-a_2)^3} = 0 \\ & x_2 + c_3x_1^2 + c_4x_1 + a_4 - a_2 = 0 \\ & x_3 + c_5x_1^2 + c_6x_1 - a_4 - a_3 - a_1 = 0 \\ & x_4 - a_4 + a_2 = 0 \end{aligned} \tag{1.2}$$

where the c_i are in $Q(a_1, \cdots, a_4)$. (1.2) only gives the general solutions of (1.1) and some special solutions of (1.1) are missing, e.g. $a_1 = 0$, $x_1 = 0$, $x_2 = a_2$, $x_3 = a_3$, $x_4 = a_4 - a_2$ provide a solution of (1.1), but are not in (1.2).

In this paper, we present a method of solving parametric systems like (1.1). Our method works as follows: for a parametric polynomial system:

$$p_1 = 0, \cdots, p_r = 0, d_1 \neq 0, \cdots, d_s \neq 0$$

where p_i and d_i are in $K[u_1, \cdots, u_m, x_1, \cdots, x_n]$ and the u are parameters, we can construct some unmixed quasi algebraic sets, say S_i, $i = 1, \cdots, s$, in the parametric space. For each S_i there is a polynomial set $ASC_i \subset K[U, X] - K[U]$ in triangular form such that for a parametric value $u' \in S_i$, if x' is a solution of ASC_i corresponding u' which do not make the leading coefficients of the polynomials in ASC_i zero (all such solutions consist of an unmixed quasi algebraic set) then (u', x') is a solution of the parametric system. Furthermore all the solutions of the system can be obtained in this way. Since ASC_i are in triangular form, we can solve the x_i successively in an explicit way.

In [SI1], similar problems for linear parametric systems are studied carefully by W. Sit. In [WE1], Weispfenning studied parametric systems through the concept of comprehensive Gröbner bases. His work, though also deals with parametric systems, is with different emphasis and uses different methods with our algorithm. An advantage of our approach is that it can be extended to deal with algebraic differential equations, details of which will be given in another paper.

We present our method in two forms. The coarse form (Section 3.2) is a direct application of Wu's projection algorithm [WU2]. The difference is that Wu's projection algorithm eliminates the variables one by one while our algorithm here can eliminate all the variables for a triangular polynomial set directly. Another improvement is that by using our extended affine dimension theorem (see Theorem (4.4), [CG1]), we may insure that each non-empty set in the projection is an unmixed quasi algebraic set. The refined form (Section 3.3) uses the concept of regular chain which has been studied by many researchers [CY1, KA1, LA1, ZY1]. For the refined form, we not only know the dimension but also the degree of the unmixed solution sets obtained by our algorithm. We also give a method to reduce solving of certain one dimensional systems to solving of zero dimensional systems.

The basis of our algorithm is the coarse form of Ritt-Wu's decomposition algorithm (see Theorem 3.2) which only uses the operations $+, -, *$, and pseudo remainder of polynomials. In essence the decomposition algorithm is to decompose a quasi algebraic set into the union of quasi algebraic sets in triangular form using *generalized polynomial remainder sequences*. In the implementation, we actually use many techniques, e.g., the Collin's reduced prs, reduced prs for several polynomials [LI1], polynomial factorization, affine dimension theorem, techniques from Gröbner bases, etc., to enhance the efficiency [CG2]. For partial analysis of the complexity of the algorithm, see [GM1]. We implemented our algorithm and the examples reported in this paper show that our algorithm is quite efficient.

It is easy to see that Algorithm 3.5 itself provides a new quantifier elimination method over algebraic closed fields. As a direct application, we may give the dimensions of all the components of the parametric systems. Other applications may be seen from the solution of various parametric systems from various fields.

In Section 2, we present our main result. In Section 3, several methods are provided. Section 4 is a collection of several examples.

2. Statement of the Problem

Let K be a computable field of characteristic zero and $A = B[x_1, ..., x_n]$ or $B[X]$ where $B = K[u_1, \cdots, u_m]$. A polynomial (ab. pol) in B is called a ***u*-*pol***. For $P \in B[X] - B$, we can write $P = c_d x_p^d + ... + c_1 x_p + c_0$, where $c_i \in B[x_1, ..., x_{p-1}]$, $p > 0$, and $c_d \neq 0$. We call p the *class*, c_d the *initial*, x_p the *leading variable*, and d the *leading degree* of P respectively, or $class(P) = p$, $init(P) = c_d$, $lv(P) = x_p$, $ld(P) = d$.

A sequence of pols $ASC = A_1, ..., A_p$ in $B[X]$ is said to be a *quasi ascending (*ab. *asc) chain* or in *triangular form*, if either $p = 1$ and $A_1 \neq 0$ or $0 < class(A_i) < class(A_j)$ for $1 \leq i < j$. The variable set $\{x_1, \cdots, x_n\} - \{lv(A_1), \cdots, lv(A_p)\}$ is called the *parameter set* of ASC. We define the dimension of ASC to be $DIM(ASC) = n - p$, i.e. the number of the parameters of ASC.

Let PS be a pol set in $K[U, X]$. For an algebraic closed field E containing K, let

$$Zero(PS) = \{a \in E^{m+n} \mid \forall P \in PS, P(a) = 0\}$$

For two pol sets PS and DS in $K[U, X]$, we define

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

Following [WU2], a *quasi variety* is defined to be $D = \cup_{i=1}^{t} Zero(PS_i/DS_i)$ where PS_i and DS_i are pol sets in $K[U, X]$. D is called *unmixed* if the PS_i are prime ideals with the same dimension.

For pol sets PS and DS in $K[U, X]$, we define the projection with the x_i as follows

$$Proj_{x_1, \cdots, x_n} Zero(PS/DS) =$$

$$\{e \in E^m \ \mid \exists a \in E^n s.t. (e,a) \in Zero(PS/DS)$$

If $m = 0$, we define $Proj_{x_1,\cdots,x_n} Zero(PS/DS)$ = $Truth$ if $Zero(PS/DS) \neq \emptyset$, and $False$ otherwise. It is well known that the projection of a quasi variety is also a quasi variety [JA1].

For two pol sets

$$PS = \{p_1, \cdots, p_t\} \text{ and } DS = \{d_1, \cdots, d_r\}$$

in $K[U,X]$, consider the following parametric equation system

$$p_1 = 0 \wedge \cdots \wedge p_t = 0 \wedge d_1 \neq 0 \wedge \cdots \wedge d_r \neq 0 \tag{2.1}$$

or equivalently $Zero(PS/DS)$. Following [SI1], we have the following definition.

Definition 2.2. A *solution function* of (2.1) is a pair (S, ASC) where S is an unmixed quasi variety in E^m and ASC is a triangular set in $B[X] - B$ such that (a) for each $u' \in S$, let ASC' be obtained by replacing the u by u', then $Zero(ASC'/J')$ (where J' is the production of the initials of the pols in ASC with the u replaced by u') is an unmixed quasi variety of dimension $DIM(ASC) = n - |ASC|$ in E^n; (b) for each $x' \in Zero(ASC'/J')$, $(u', x') \in Zero(PS/DS)$. We call (u', x') a solution of (S, ASC). We call the dimension of $Zero(ASC'/J')$ the dimension of the solution function (S, ASC).

Definition 2.3. A *cover* of (2.1) is a set of solution functions of (2.1) $\{(S_1, ASC_1), \cdots, (S_s, ASC_s)\}$ such that each $(u', x') \in Zero(PS/DS)$ is a solution of some (S_i, ASC_i).

Theorem 2.4. We have an algorithm to find a cover for the parametric system (2.1).

For a proof of Theorem 2.4, see Section 3. We first state some consequences. Let

$$C = \{(S_1, ASC_1), \cdots, (S_s, ASC_s)\}$$

be a cover of (2.1). Then we have

(1) $DIM(ASC_i) = n - |ASC_i|$, $i = 1, \cdots, s$ are all the possible dimensions of the parametric system (2.1).

(2). Let $M \subset C$ be the set of those (S_i, ASC_i) such that S_i is of dimension m, then in $K(U)[X]$ we have $Zero(PS/DS) = \cup_{(S_j, ASC_j) \in M} Zero(ASC_j/J_j \cup DS)$.

(3) Those (S_i, ASC_i) with dimension zero provide all the isolated solutions of (2.1).

3. Methods of Solving Parametric Systems

3.1. Preliminaries

For pols P and G with $P \notin K$, let $prem(G;P)$ be the *pseudo remainder* of G with P in variable $lv(P)$. For a quasi asc chain $ASC = A_1, ..., A_p$ such that $A_1 \notin K$, we define the pseudo remainder of a pol G with ASC inductively as

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

Lemma 3.1. Let ASC be a quasi asc chain in $K[X]-K$ and $J = \prod_{P\in ASC} init(P)$. If $Zero(ASC/J) \neq \emptyset$ then $Zero(ASC/J)$ is an unmixed quasi variety of dimension $DIM(ASC)$.

See Theorem (4.4) [CG1] or Lemma (4.5) in the TR version of [CG1]. ▮

We have the following coarse form of Ritt-Wu's decomposition algorithm.

Theorem 3.2. For two finite pol sets PS and DS in $K[X]$, we may either prove $Zero(PS/DS) = \emptyset$ or find quasi asc chains ASC_i, $i = 1, ..., l$, such that

$$Zero(PS/DS) = \cup_{i=1}^{l} Zero(ASC_i/\{J_i\} \cup DS) \tag{3.2.1}$$

where J_i is the production of the initials of the pols in ASC_i.

Proof. See [WU1]. For our implementation of the algorithm, see [CG2]. ▮

3.2. A Coarse form

Lemma 3.3. Let $B = \sum_{i=0}^{t} B_i x_1^i \in K[U, x_1]$ where B_i are u-pols, then

$$Proj_{x_1} Zero(\emptyset/B) = \cup_{i=0}^{t} Zero(\emptyset/B_i) \tag{3.3.1}$$

It is easy to check. ▮

Lemma 3.4. Let P, Q be pols in $K[U, x_1]$ such that $d = degree(P, x_1) > 0$ and $degree(Q, x_1) > 0$, then $Proj_{x_1} Zero(P/QI) = Proj_{x_1} Zero(\emptyset/RI)$ where I is the initial of P and $R = prem(Q^d, P)$.

See p. 306 [JA1] or p.44 [WU2]. ▮

The following algorithm provides a proof of Theorem 2.4.

Algorithm 3.5.

INPUT: Two pol sets PS and $DS = \{d_1, \cdots, d_r\}$ in $K[U, X]$.

OUTPUT: A cover of $Zero(PS/DS)$.

S1. Let $D = \prod_{i=1}^{r} d_i$. By Theorem 3.2, in $K[U, X]$ under the variable order $u_1 < \cdots < u_m < x_1 < \cdots < x_n$, we have

$$Zero(PS/D) = \cup_{i=1}^{l} Zero(ASC_i/DJ_i) \tag{3.5.1}$$

For $i = 1, \cdots, l$, do S2 – S8.

S2. Without loss of generality, we write ASC_i as $B_1, \cdots, B_{r_i}, A_1, \cdots, A_{s_i}$ where B_j are u-pols and $lv(A_j) = x_{n+j-s_i}$, $j = 1, \cdots, s_i$.
S3. Let $Z = Zero(ASC_i/J_iD)$. If $degree(D, x_n) = 0$, then $Proj_{x_n} Z = Zero(ASC'/J_iD)$ where $ASC' = \{B_1, \cdots, B_{r_i}, A_1, \cdots, A_{s_i-1}\}$; goto S6. Otherwise, goto S4.
S4. Now $degree(D, x_n) \neq 0$. By Lemma 3.4,

$$Proj_{x_n} Z = Proj_{x_n} Zero(ASC'/J_iR)$$

where $R = prem(D^{ld(A_{s_i})}, A_{s_i})$.
S5. Let $R = \sum_{k=0}^{d} E_k x_n^k$, by (3.3.1),

$$Proj_{x_n} Zero(ASC'/J_iR) = \cup_{k=0}^{d} Zero(ASC'/J_iE_k).$$

S6. By now, we have obtained $Proj_{x_n} Z$. Repeating S3-S5, we may eliminate x_{n-1}, x_{n-2}, $\cdots$, x_{n+1-s_i} similarly (note that now J_i may involve x_{n-1}, etc). At last, we have

$$Proj_{x_{n+1-s_i}, \cdots, x_n} Z = \cup_{k=1}^{s} Zero(\{B_1, \cdots, B_{r_i}\}/G_k)$$

where G_k is the product of the initials of the B_j and a pol $H_k \in K[U, x_1, \cdots, x_{n-s_i}]$.
S7. If H_k involves $x_1, \cdots, x_{n-s_i}$, we use (3.3.1) repeatedly to eliminate them. We have

$$S_i = Proj_{x_1, \cdots, x_n} Z = \cup_{k=1}^{r} Zero(\{B_1, \cdots, B_{r_i}\}/F_k) \quad (3.5.2)$$

where F_k is the product of the initials of the B_j and a u-pol. We may write (3.5.2) as

$$S_i = Zero(\{B_1, \cdots, B_{r_i}\}/I_i) - Zero(\{\frac{F_1}{I_i}, \cdots, \frac{F_r}{I_i}\}) \quad (3.5.3)$$

where $I_i = \prod_{j=1}^{r_i} init(B_j)$.
S8. Note that in (3.5.2), $\{B_1, \cdots, B_{r_i}\}$ is in triangular form and F_k is the product of the initials of the B_j and a u-pol. Then we may compute $D_i = Proj_{u_1, \cdots, u_m} S_i$ by repeating S3-S7. If $D_i = Truth$ ($S_i \neq \emptyset$), by Lemma 3.1 (S_i, ASC_i) is a solution function of $Zero(PS/DS)$. If $D_i = False$, $Zero(ASC_i/J_iD) = \emptyset$. We discard it. From (3.5.1), all solution functions thus obtained furnish a cover for $Zero(PS/DS)$.

Example 3.6. Consider an example from [WU3]. Let $PS = \{y^2 - zxy + x^2 + z - 1, xy + z^2 - 1, y^2 + x^2 + z^2 - r^2\}$ where r is the parameter. Under the variable order $r < z < x < y$, we have: $Zero(PS) = Zero(ASC_1/x) \cup Zero(ASC_2)$ where

$ASC_1 = \{z^3 - z^2 + r^2 - 1,$
$x^4 + (z^2 - r^2)x^2 + z^4 - 2z^2 + 1,$
$xy + z^2 - 1\};$
$ASC_2 = \{r^4 - 4r^2 + 3, z + r^2 - 2, x, y^2 - r^2 + 1\}.$

For ASC_1, following S2-S7 in Algorithm 3.5, we have $Proj_{x,z,y}Zero(ASC_1/x) = E$. For ASC_2, it is clear that $Proj_{x,z,y}Zero(ASC_2) = Zero(r^4-4r^2+3)$. Therefore a cover of $Zero(PS)$ is $\{(E, ASC_1), (Zero(r^4 - 4r^2 + 3), ASC_2')\}$ where $ASC_2' = \{z+r^2-2, x, y^2-r^2+1\}$. Since $r^4-4r^2+3 = (r^2-1)(r^2-3)$, we obtain another cover: $\{(E, ASC_1), (\{\pm 1\}, \{z-1, x, y^2\}), (\{\pm\sqrt{3}\}, \{z+1, x, y^2-2\})\}$.

3.3. A Refined Form

For two pols $P, Q \in B[X]$ such that $P \notin B$, we define the resultant of Q and P in the following way: if $degree(Q, lv(P)) = 0$ define $resl(Q; P) = Q$; otherwise $resl(Q; P)$ is the resultant of P and Q in the variable $lv(P)$. For a quasi asc chain $ASC = A_1, ..., A_p$ such that $A_1 \notin B$, we define the resultant of a pol G and ASC inductively as

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

Then $R \in B[X]$ and there exist pols C and C_i such that $R = CG + C_1A_1 + \cdots + C_pA_p$.

A quasi asc chain $ASC = A_1, ..., A_p$ is called *regular* if $resl(init(A_i); A_1, \cdots, A_{i-1}) \neq 0$, $i = 2, \cdots, p$. We need the following properties of regular asc chains.

Lemma 3.7. Let $ASC = A_1, \cdots, A_p$ be a regular asc chain in $K[x_1, \cdots, x_n]$, then $Zero(ASC/J)$ is an unmixed quasi-variety of dimension $DIM(ASC)$ and degree $D = \prod_{i=1}^{p} ld(A_i)$.

We rename $lv(A_i)$ as y_i and the parameters of ASC as $v_1, \cdots, v_q$ where $q = n-p$. Let $R_i = resl(init(A_i); A_1, \cdots, A_{i-1}), i = 2, \cdots, p$. Then $R = init(A_1)\prod_{i=2}^{p} R_i \neq 0$ involves the v alone. For each $v' \in E^q$ such that $R(v') \neq 0$, we replace the v by v' in A_1 and get a pol $A_1' \in E[x_1]$ such that $degree(A_1', x_1)$ = $ld(A_1)$ since $R(v') \neq 0$. Thus A_1' has $ld(A_1)$ solutions: $x_{1,1}, \cdots, x_{1,ld(A_1)}$. For each solution of A_1', say $x_{1,1}$, replacing v, x_1 by v', x_{11} in A_2 we get a pol $A_2' \in E[x_2]$. Since $R(v') \neq 0$, we have $init(A_2)(u', x_{11}) \neq 0$ or $degree(A_2', x_2) = ld(A_2)$. Thus A_2' has $ld(A_2)$ solutions. Continuing in this way, at last we obtain D zeros of $Zero(ASC/J)$ and it is clear that they are all the zeros of $Zero(ASC/J)$ corresponding to the parameter value v'. The unmixity comes from Lemma 3.1. ∎

A quasi asc chain ASC is called a *p-chain* if the initial of every pol in ASC

involves the parameters of ASC alone. It is clear that a p-chain is a regular asc chain.

Lemma 3.8. Let $ASC = A_1, \cdots, A_p$ be a regular asc chain in $K[X]$, then we can find a p-chain ASC' such that

$$Zero(ASC/J) = Zero(ASC'/J') \cup Zero(ASC \cup \{J'\}/J)$$

where J and J' are the product of the initials of the pols in ASC and ASC' respectively.

As in the proof of Lemma 3.7, we rename $lv(A_i)$ as y_i. Let $A_i = I_i y_i^{d_i} - U_i$ where I_i is the initial of A_i. We put $A_1' = A_1$. For $i = 2, \cdots, p$, let $R_i(u) = resl(I_i; A_1, \cdots, A_{i-1}) \neq 0$, then there exist $Q_i, B_{i,j} \in A$ such that

(3.8.1) $\quad R_i(u) = Q_i I_i + \sum_{j=1}^{i-1} B_{i,j} A_j$

Let

(3.8.2) $A_i' = A_i Q_i + (\sum_{j=1}^{i-1} B_{i,j} A_j) y_i^{d_i} = R_i y_i^{d_i} + Q_i U_i$.

Let $Q = \prod_{i=2}^{p} Q_i$ and $R = \prod_{i=2}^{p} R_i$. It is clear that $Zero(ASC/J) = Zero(ASC/JQ) \cup Zero(ASC, \{Q\}/J)$. From (3.8.1), $Zero(ASC \cup \{Q\}/J) = Zero(ASC \cup \{I_1 \prod_{i=2}^{p} Q_i I_i\}/J)$ = $Zero(ASC \cup \{R\}/J)$. By (3.8.1) and (3.8.2),

$$\begin{aligned} Zero(ASC/JQ) &= Zero(\{A_1, A_2Q_2, \cdots, A_pQ_p\}/JQ) \\ &= Zero(ASC'/J') \end{aligned}$$

(consider inductively from p to 1). We have completed the proof. ∎

Remark. The usefulness of regular chains lays to the facts that we may obtain a decomposition of the form (3.2.1) such that each ASC_i is a regular chain without using pol factorization [ZY1, KA1]. Now we have the refined form of solving parametric algebraic systems.

Algorithm 3.9.

INPUT: PS is a pol set in $K[U, X]$.

OUTPUT: A cover of $Zero(PS)$. Furthermore, for each solution function (S_i, ASC_i) in the cover, ASC_i is a p-chain.

S1. By Theorem 3.2, in $K[U, X]$ we have $Zero(PS) = \cup_{i=1}^{l} Zero(ASC_i/\{J_i\})$. By the Remark after Lemma 3.8, we may assume ASC_i are regular asc chains. By Lemma 3.8, we may further assume ASC_i are p-chains. For $i = 1, \cdots, l$, do S2 -S4.

S2. Without loss of generality, ASC_i can be written as $B_1, \cdots, B_{r_i}, A_1, \cdots, A_{s_i}$ where B_j are u-pols and $lv(A_j) = x_{n+j-s_i}$, $j = 1, \cdots, s_i$.

S3. Since ASC_i is a p-chain,

$$\begin{aligned} &Proj_{x_{n+1-s_i}, \cdots, x_n} Zero(ASC_i/J_i) \\ &= Zero(\{B_1, \cdots, B_{r_i}\}/J_i). \end{aligned}$$

S4. Since B_j are free of x_i, we may use (3.3.1) repeatedly to obtain the

$$\begin{aligned} S_i &= Proj_{x_1,\cdots,x_n} Zero(ASC_i/J_i) \\ &= \cup_{k=1}^{r} Zero(\{B_1,\cdots,B_{r_i}\}/F_k) \end{aligned}$$

where each F_i is the product of the initials of the B_i and a u-pol. Since ASC_i is a p-chain, F_k are pols of the parameters of ASC_i alone. Therefore $S_i \neq \emptyset$ and (S_i, ASC_i) is a solution function for $Zero(PS)$.

Example 3.10. Let PS be the same as in Example 3.6. The decomposition in S1 of Algorithm 3.9 is $Zero(PS) = \cup_{i=1}^{5} Zero(ASC_i/J_i)$ where

$ASC_1 = \{z^3 - z^2 + r^2 - 1,$
$x^4 + (z^2 - r^2)x^2 + z^4 - 2z^2 + 1,$
$(r^4 - 4r^2 + 3)y + (-z^2 + (r^2 - 1)z - r^2 + 1)x^3$
$+((r^2 - 1)z^2 + (-r^4 + 2r^2 - 1)z + 2r^2 - 2)x, \};$
$ASC_2 = \{r^4 - 4r^2 + 3, z + r^2 - 2, x, y^2 - r^2 + 1\};$
$ASC_3 = \{r^2 - 1, z, x^4 - x^2 + 1, y + x^3 - x\};$
$ASC_4 = \{r^2 - 3, z + 1, x^2 - 2, y\};$
$ASC_5 = \{r^2 - 3, \quad z^2 - 2z + 2, \quad x^4 + (2z - 5)x^2 - 4z + 1,$
$5y + (2z - 1)x^3 + (-4z - 3)x\}.$

$ASC_i, i = 1, \cdots, 5$ are p-chains. The other steps are trivial.

3.4. A Fast Method for Special Systems

For a polynomial set $PS = \{p_1, \cdots, p_n\}$ where $p_i \in K[u_1, \cdots, u_m, x_1, \cdots, x_n]$, consider the following system

$$p_1 = 0 \wedge \cdots \wedge p_n = 0 \tag{3.11}$$

We further assume that for each special value u' of the u, (3.11) only has finite number of solutions for the x_i. It is clear that for such a system $Zero(PS)$ is of zero dimension in $K(u)[X]$. Therefore, in $K(u)[X]$ we have

$$Zero(PS) = \cup_{i=1}^{t} Zero(ASC_i/J_i) \tag{3.12}$$

where $DIM(ASC_i) = 0, i = 1, \cdots, t$. By Lemma 3.9, we may assume that each ASC_i is a p-chain. Furthermore, we assume $ASC_i \subset K[u, X]$.

Theorem 3.13. Assume the conditions in the above paragraph. Then in $K[u, X]$ we have

$$Zero(PS) = \cup_{i=1}^{t} Zero(ASC_i/J_i) \cup Zero(PS \cup \{J\}) \tag{3.13.1}$$

where $J = \prod_{i=1}^{t} J_i \in K[u]$.
Since for any u', (3.11) only has finite number of solutions, the dimension of $Zero(PS)$ must be $\leq m$. On the other hand, by the affine dimension theorem (ref. e.g., Theorem (4.4) [CG1]), each irredundant component of $Zero(PS)$ is of dimension $\geq m$. Therefore $Zero(PS)$ is an unmixed variety of dimension m. Thus, in $K[u,x]$, $Zero(PS) = \cup_{i=1}^{t} Zero(PD(ASC_i))$ Since $Zero(PD(ASC_i)) = Zero(ASC_i/J_i) \cup Zero(PD(ASC_i) \cup \{J_i\})$, (3.13.1) is true. ∎

If $m = 1$, the above results have the following simple form. When decomposing (3.11) in $K[u_1, x]$, Let $Z' = Zero(ASC'/J')$ be a zero dimensional component of $Zero(PS)$ where $ASC' = A_0(u_1), A_1, \cdots, A_n$. If A_0 is not a factor of J (in Theorem 3.13) then Z' must be redundant and can be removed. Furthermore, to solve (3.11), we may first solve the zero dimensional system $Zero(PS)$ in $K(u_1)[X]$ and the remaining zeros are $Zero(PS \cup \{J\})$ which is of zero dimension in $K[u_1, X]$. Therefore we need solving two zero dimensional systems. Solving of zero dimensional systems is relatively easy. Once the decomposition of $Zero(PS)$ is given, we may obtain a cover of $Zero(PS)$ easily.

Example 3.14. Let PS be the same as in Example 3.6. From the decomposition in Example 3.6, we know that this system satisfies the conditions of this section. In $Q(r)[z,x,y]$, we have $Zero(PS) = Zero(ASC_1)$ where ASC_1 is the same as in Example 3.10. Then by Theorem 3.14, in $Q[r,z,x,y]$ we have

$$Zero(PS) = Zero(ASC_1/J_1) \cup Zero(PS \cup \{J_1\})$$

where $J_1 = r^4 - 4r^2 + 3$.

4. Examples

We have implemented the algorithm in a SUN-3/50 using Common Lisp. The following are some examples sovled by our program based on Algorithm 3.9.

Example 4.1. System (1.1) is to find the *Equilibrium Points of Chemical Systems* [BG1,BU1,WE1]. In $Q[a_1, \cdots, x_4]$, $Zero((1.1)) = \cup_{i=1}^{9} Zero(ASC_i/J_i)$ where

$$\begin{aligned} ASC_1 = \{&(a_4 - a_2)x_1 - a_1a_3, \\ &(a_4 - a_2)x_2 + a_4^2 + (-a_3 - 2a_2 - a_1)a_4 \\ &\quad +(a_2 + a_1)a_3 + a_2^2 + a_1a_2; \\ &x_3 - a_4, \\ &x_4 - a_4 + a_2\}; \end{aligned}$$

$$\begin{aligned} ASC_2 = \{&(a_4 - a_2)x_1 - a_1a_4, \\ &(a_4 - a_2)x_2 - a_2a_4 + a_2^2 + a_1a_2, \\ &x_3 - a_3, \\ &x_4 - a_4 + a_2\}; \end{aligned}$$

$$
\begin{aligned}
ASC_3 = \{&(a_4 - a_2)x_1 - a_3a_4,\\
&(a_4 - a_2)x_2 - a_2a_4 + a_2a_3 + a_2^2,\\
&x_3 - a_1,\\
&x_4 - a_4 + a_2\};
\end{aligned}
$$
$ASC_4 = \{a_3, a_4 - a_2, x_2 + x_1 - a_2, x_3 - a_1, x_4\};$
$ASC_5 = \{a_3, a_4 - a_2, x_2 + x_1 - a_1, x_3 - a_2, x_4\};$
$ASC_6 = \{a_1, a_4 - a_2, x_2 + x_1 - a_2, x_3 - a_3, x_4\};$
$ASC_7 = \{a_1, a_4 - a_2, x_2 + x_1 - a_3, x_3 - a_2, x_4\};$
$ASC_8 = \{a_2, a_4, x_2 + x_1 - a_1, x_3 - a_3, x_4\};$
$ASC_9 = \{a_2, a_4, x_2 + x_1 - a_3, x_3 - a_1, x_4\}.$

Since the ASC_i are p-chains, we may obtain a cover of (1.1) trivially.

Example 4.2. In [GC1], we gave a method of finding *Inversion Maps of Rational Parametric Equations*. But some special solutions with lower dimensions are not considered in the method. Using the method in this paper, we may find a complete inversion map. Considering the following parametric equations:

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

The problem of finding inversion maps is actually to solve t in terms of x and y. Using Algorithm 3.5, a cover is: $\{(Zero(x^2 + y^2 - 1/x - 1), \sqrt{2}(x-1)t^2 - 2yt + \sqrt{2}(-x+1)); (Zero(x-1, y), t)\}$.

Example 4.3. To find the equilibrium points of the following Lorentz system [LU1].

$$
\begin{aligned}
x_1' &= x_2(x_3 - x_4) - x_1 + c\\
x_2' &= x_3(x_4 - x_1) - x_2 + c\\
x_3' &= x_4(x_1 - x_2) - x_3 + c\\
x_4' &= x_1(x_2 - x_3) - x_4 + c
\end{aligned}
$$

Let $PS = \{x_2(x_3-x_4)-x_1+c, x_3(x_4-x_1)-x_2+c, x_4(x_1-x_2)-x_3+c, x_1(x_2-x_3) - x_4 + c\}$. We have $Zero(PS) = \cup_{i=1}^{10} Zero(ASC_i/J_i)$ where all ASC_i are p-chains. The asc chains are too long (two pages) to print here. They can be found in [GC2]. It is easy to find a cover of the system from the decomposition. Four of the ten asc chains are already given in [LU1]. This example need the special techniques of Section 3.4.

Example 4.4. Consider a system comes from the analysis of *Neural Network* [KA1]. Let $PS = \{zx^2+zy^2-cz+1, yx^2+(z^2-c)y+1, (y^2+z^2-c)x+1\}$ where c is the parameter. We have $Zero(PS) = \cup_{i=1}^{5} Zero(ASC_i/J_i)$ in $Q[c,z,y,x]$ where

$ASC_1 = \{$
$2cz^4 - 2z^3 - c^2z^2 - 2cz - 1,$
$2y - 2c^2z^3 + 4cz^2 + (c^3 - 2)z + c^2,$ $2x - 2c^2z^3 + 4cz^2 + (c^3 - 2)z + c^2\};$

$ASC_2 = \{2z^4 - 3cz^2 + z + c^2,$ $cy - 2z^3 + 2cz - 1,$ $x - z\};$

$ASC_3 = \{2z^4 - 3cz^2 + z + c^2,$ $y - z,$ $cx - 2z^3 + 2cz - 1\}.$

$ASC_4 = \{2z^3 - cz + 1, y - z, x - z\};$

$ASC_5 = \{z^3 - cz - 1, y^2 + zy + z^2 - c, x + y + z\};$

Since the ASC_i are p-chains, it is easy to find a cover of the system. Compare with the solutions of the system in $Q(c)[z, y, x]$ given in [KA1]. This example uses the special techniques of section 3.4.

Acknowledgement. The authors want to thank a refree for valuable comments on results of section 3.4 of the paper.

Reference.

[BG1] W. Boege, R. Gebauer & H. Kredel, Some Examples for Solving Systems of Algebraic Equations by Calculating Gröbner Bases, *J. Symbolic Computation*, (1986)1, 83-98.

[BU1] B. Buchberger,Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory, *Recent Trends in Multidimensional Systems theory* (ed. N.K. Bose), D.Reidel Publ. Comp., 1985.

[CG1] S.C. Chou & X.S. Gao, 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. Also see TR-89-09, Comp. Sci. Dep., The Univ. of Texas at Austin.

[CG2] S.C. Chou & X.S.Gao, Techniques for Ritt-Wu's Decomposition Algorithm, TR-90-02, Computer Sciences Department, The University of Texas at Austin, February, 1990.

[CY1] S.C. Chou and J.G. Yang, Two Properties of Regular Ascending Chains, preprints, 1986.

[GC1] X.S. Gao & S.C. Chou, Computations with Parametric Equations, *Proc. of ISSAC'91*, ACM, New York, pp.122-127.

[GC2] X.S. Gao & S.C. Chou, Solving Parametric Algebraic Systems, MM-preprints, No. 7, March 1992, Institute of Sys. Science, Academia Sinica.

[GM1] C. Gallo and B. Mishra, Efficient Algorithms and Bounds for Wu-Ritt Characteristic Sets, TR, Courant Institute of Math. Sciences, 1989.

[JA1] N. Jacobson, *Basic Algebra* vol. 1, W.H. Freeman and Company, 1974.

[KA1] M. Kalkbrenner, *Three Contributions to Elimination Theory*, Phd Theses, RISC - Linz, 1990.

[LA1] D. Lazard, A New Method for Solving Algebraic Systems of Positive Algebraic Systems of Positive Dimension, to appear in Discr. Applied Math., 1991.

[LA2] D. Lazard, Resolution des Systemes d'Equationes Algebriques, Theor. Comp. Sci., 15:77-110, 1981.

[LI1] Li Ziming, On The Triangulation for any Finite Polynomial Set (I), MM Research Preprints, No2, 1987, Ins. of Systems Science, Academia Sinica.

[LU1] Liu Zhuojun, An Algorithm on Finding All Isolated zeros of polynomial equations, MM Research Preprints, No4, 1987, Ins. of Systems Science, Academia Sinica. Also see *Proc. of ISSAC'90*, p.300.

[SI1] W. Y. Sit, A Theory for Parametric Linear Systems, *Proc. of ISSAC-91*, p.112–121, ACM Press, 1991.

[WE1] V. Weispfenning, Comprehensive Gröbner Bases, Tech. Berichte der Fakultät für Math. und Informatik, Univ. Passau, MIP-9003.

[WU1] Wu Wen-tsün, Basic Principles of Mechanical Theorem Proving in Elementary Geometries, *J. Sys. Sci. & Math. Scis.*, 4(1984), 207 –235.

[WU2] Wu Wen-tsün, On a Projection Theorem of Quasi-Varieties in Elimination Theory *MM Research Preprints*, No. 4, Ins. of Sys. Sci., Academia Sinica.

[WU3] Wu Wen-tsün, A Zero Structure Theorem for pol Equation -Solving, MM Research Preprints, No1, 1987, Ins. of Sys. Sci.

[ZY1] J.Z. Zhang and L. Yang, A Method to Overcome the Reducibility Difficulty in Mechanical Theorem Proving, IC/89/263, International Centre for Theoretical Physics, Trieste, 1989.