A Zero Structure Theorem for Differential Parametric Systems*

XIAO-SHAN GAO
Institute of Systems Science, Academia Sinica, Beijing
SHANG-CHING CHOU
Department of Computer Science
Wichita State University,Wichita KS 67260, USA

July 1993

Abstract

We present a zero structure theorem for a differential parametric system:

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

where p_i and d_i are differential polynomials in $K\{u_1, \cdots, u_m, x_1, \cdots, x_n\}$ and the u are parameters. According to this theorem we can identify all parametric values for which the parametric system has solutions for the x_i and at the same time giving the solutions for the x_i in an explicit way, i.e., the solutions are given by differential polynomial sets in triangular form. In the algebraic case, i.e. when p_i and d_i are polynomials, we present a refined algorithm with higher efficiency. As an application of the zero structure theorem presented in this paper, we give a new algorithm of quantifier elimination over differential algebraic closed fields. The algorithm has been implemented and several examples reported in this paper show that the algorithm is of practical value.

1 Introduction

Let K be a differential field and $K\{u_1, \cdots, u_m, x_1, \cdots, x_n\}$ or $K\{U, X\}$ be the differential polynomial ring of parameters $u_1, \cdots, u_m$ and variables $x_1, \cdots, x_n$. By a parametric system, we mean

$$p_1 = 0, \cdots, p_r = 0, d_1 \neq 0, \cdots, d_s \neq 0 \tag{1.1}$$

*The work reported here was supported in part by the NSF grant CCR-917870 and a grant from the Chinese NSF.

where p_i and d_j, $i = 1, \cdots, r, j = 1, \cdots, s$, are differential polynomials in $K\{U, X\}$. In this paper, we present a method for identifying all parametric values for which the system has solutions for the x_i over a differentially closed field E containing K, and at the same time giving the solutions for the x_i in an explicit way, i.e., the solutions are given by differential polynomial sets in triangular form. More precisely, we give a zero structure theorem for (1.1) of the form $(S_1, TS_1), \cdots, (S_t, TS_t)$ where S_i are some unmixed quasi-varieties in E^m and TS_i are triangular sets of the variables x_i such that for each $\eta \in S_i$, when replacing the u by η, the TS_i become

$$A_1(\eta, x_1, \cdots, x_d), A_2(\eta, x_1, \cdots, x_{d+1}), \cdots, A_l(\eta, x_1, \cdots, x_n)$$

and the equation system $A_1 = 0, A_2 = 0, \cdots, A_l = 0$ has solutions which are also solutions of system (1.1). Furthermore, all solutions of (1.1) can be given in this way. This method is a generalization and combination of two well known algorithms: the quantifier elimination algorithm (Seidenberg, 1956) and Ritt-Wu's zero decomposition algorithm (Ritt, 1950, Wu, 1986).

In the algebraic case, i.e. when p_i and d_i are polynomials, we present a refined algorithm of higher efficiency. This refined form uses the concept of the regular ascending chain which has been studied by many researchers (Kalkbrenner, 1990, Lazard, 1991, Zhang, 1992).

Related work in the case of algebraic systems can be found in (Sit, 1991, Weispfenning, 1992, Gao, Chou, 1992, Kapur, 1992, Wang, 1993).

An application of the structure theorem is the solving of polynomial parametric equation systems. Consider the following algebraic equation system from (Buchberger, 1985). 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.

$$\begin{aligned}
&x_4 - a_4 + a_2 = 0\\
&x_4 + x_3 + x_2 + x_1 - a_4 - a_3 - a_1 = 0\\
&x_3x_4 + x_1x_4 + x_2x_3 + x_1x_3 + (-a_3 - a_1)a_4 - a_1a_3 = 0\\
&x_1x_3x_4 - a_1a_3a_4 = 0
\end{aligned} \tag{1.2}$$

In the literature of solving polynomial equations (Buchberger, 1985, Lazard, 1981, Wu, 1986), parametric systems as (1.2) 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 (1.2) in A are given by the following equations (Buchberger, 1985)

$$\begin{aligned}
&x_1^3 - c_1x_1^2 + c_2x_1 - \tfrac{a_1^2a_3^2a_4^2}{(a_4-a_2)^3} = 0\\
&x_2 + c_3x_1^2 + c_4x_1 + a_4 - a_2 = 0\\
&x_3 + c_5x_1^2 + c_6x_1 - a_4 - a_3 - a_1 = 0\\
&x_4 - a_4 + a_2 = 0
\end{aligned} \tag{1.3}$$

where the c_i are in $Q(a_1, \cdots, a_4)$. However, (1.3) only gives the general solutions of (1.2) and some special solutions of (1.2) are missing, e.g. $\{ a_1 = 0, x_1 = 0, x_2 = a_2, x_3 = a_3, x_4 = a_4 - a_2 \}$ is a set of solutions for (1.2) which is not in

(1.3). Using our zero structure theorem, complete information for the solutions of algebraic or differential parametric systems can be given. The complete solution of (1.2) is given in Example 4.4.

Our zero structure theorem is based on a projection algorithm for triangular sets which is an extension of Wu's projection algorithm (Wu, 1990) to the differential polynomial case. Wu's projection algorithm eliminates the variables one by one, while our algorithm can eliminate all the variables for a triangular polynomial set directly. Another improvement is that we prove that a nonempty algebraic set of a triangular set is unmixed.

In Section 2, we present our main result. In Section 3, we prove the zero structure theorem. In Section 4, we present a refined version of the zero structure theorem for the algebraic case.

2 Statement of the Problem

Before presenting the problem, we first introduce some notions necessary to this paper. Readers who are not familiar with differential algebra may consult (Ritt, 1950, Wu, 1987).

Let K be a differential field of characteristic zero and $K\{x_1,...,x_n\}$ or $K\{X\}$ be the ring of differential polynomials (abbr. d-pols) in the variables $x_1,...,x_n$. Let P be a d-pol in $K\{X\}$. The *class* of P, denoted by $class(P)$, is the largest p such that x_p or some of its derivatives actually occurs in P. If $P \in K$, $class(P) = 0$. The j-th ($j \geq 0$) derivative of a variable x_i is denoted by $x_{i,j}$. The *order* of P in x_i, denoted by $ord(P, x_i)$, is the largest j such that $x_{i,j}$ appears in P. If P does not involve x_i, $ord(P, x_i) = -1$. Let a d-pol P be of class $p > 0$ and $q = ord(P, x_p)$. Then x_p and $x_{p,q}$ are called the *leading variable* (denoted by $lv(P)$) and the *lead* of P respectively.

Let P_1 and P_2 be two d-pols. We say P_2 is of *higher rank* than P_1 in x_i, if either $ord(P_2, x_i) > ord(P_1, x_i)$ or $q = ord(P_2, x_i) = ord(P_1, x_i)$ and P_2 is of higher degree in $x_{i,q}$ than P_1. P_2 is said to be of *higher rank* than P_1, denoted by $P_2 > P_1$, if either $class(P_2) > class(P_1)$ or $p = class(P_2) = class(P_1)$ and P_2 is of higher rank than P_1 in x_p.

If the lead of P is $x_{p,m}$ with $p > 0$, P can be written as

$$P = a_d x_{p,m}^d + a_{d-1} x_{p,m}^{d-1} + \cdots + a_0$$

where the a_i are d-pols of lower rank than $x_{p,m}$ and $a_d \neq 0$. Then d is called the leading degree of P and is denoted by $ld(P)$; a_d is called the *initial* of P and denoted by $init(P)$. The derivation of P is

$$P' = S x_{p,m+1} + a'_d x_{p,m}^d + a'_{d-1} x_{p,m}^{d-1} + \cdots + a'_0$$

where $S = \frac{\partial P}{\partial x_{p,m}} = da_d x_{p,m}^{d-1} + ... + a_1$ is called the *separant* of P and denoted by $sep(P)$. Note that P' is linear in $x_{p,m+1}$ with S as its initial.

A sequence of d-pols $ASC = A_1, ..., A_p$ is said to be a *quasi ascending (*ab. *q-asc) chain* or a *triangular set*, if either $p = 1$ and $A_1 \neq 0$ or $0 < class(A_i) < class(A_j)$ for $1 \leq i < j$. ASC is called *nontrivial* if $class(A_1) > 0$. A quasi ascending chain $A_1, ..., A_p$ is said to be an ascending chain if A_j is of lower rank than A_i in $lv(A_i)$ for $i < j$.

For a quasi ascending chain $ASC = A_1, ..., A_p$, let A_i be of class m_i. Then we call $\{x_1, ..., x_n\} - \{x_{m_1}, ..., x_{m_p}\}$ the *parameter set* of ASC. The *dimension* of a quasi ascending chain $ASC = A_1, ..., A_p$ is defined to be $DIM(ASC) = n - p$. Thus $DIM(ASC)$ is equal to the number of parameters of ASC.

Let PS and DS be d-pol sets. For a differential algebraic closed extension field E of K, let

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

and $Zero(PS/DS) = Zero(PS) - \cup_{g \in DS} Zero(g)$.
A *quasi variety* is defined to be $D = \cup_{i=1}^{t} Zero(PS_i/DS_i)$ where PS_i and DS_i are d-pol sets in $K\{X\}$. D is called *unmixed* if all PS_i are prime ideals with the same dimension.

Consider a set of parameters: $u_1, \cdots, u_m$ and a set of dependent variables: $x_1, \cdots, x_n$. Let $A = B\{x_1, ..., x_n\}$ or $B\{X\}$ be the d-pol ring over $B = K\{u_1, \cdots, u_m\}$. A d-pol in B is called a *u-pol*.

For d-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 $Proj_{x_1,\cdots,x_n} Zero(PS/DS) = True$ 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. Consider a parametric system

$$p_1 = 0, \cdots, p_r = 0, d_1 \neq 0, \cdots, d_s \neq 0 \tag{2.1}$$

where p_i, d_j are in $K\{U, X\}$. Let $PS = \{p_1, \cdots, p_r\}; DS = \{d_1, \cdots, d_s\}$. Following (Sit, 1991), we have

Definition 1 *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', DS' be obtained from ASC, DS by replacing the u by u'. Then $Zero(ASC'/\{J'\} \cup DS')$ (where J' is the product of the initials and separants of the d-pols in ASC with the u replaced by u') is an unmixed quasi variety of dimension $DIM(ASC)$ in E^n;*

(b) *for each* $x' \in Zero(ASC'/\{J'\} \cup DS')$, $(u', x') \in Zero(PS/DS)$. *We call* (u', x') *a solution of* (S, ASC). *We call the dimension of* $Zero(ASC'/\{J'\} \cup DS')$ *the dimension of the solution function* (S, ASC).

Definition 2 *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 3 *We have an algorithm to find a cover for the parametric system (2.1).*

For the proof of Theorem 3, 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) $DIM(ASC_i)$, $i = 1, \cdots, s$ are all the possible dimensions of the parametric system (2.1).

(2) $Proj_{x_1,\cdots,x_n} Zero(PS/DS) = \cup_{i=1}^{s} S_i$.

(3) Since by (2) an existential quantifier can be eliminated, we have a method of eliminating all quantifiers for differential equation systems.

3 A Zero Structure Theorem for Differential Systems

3.1 A Dimension Theorem

For d-pols P and G with $P \notin K$, let $R = prem(G; P)$ be the *pseudo remainder* of G with P in variable $lv(P)$ (see Ritt, 1950). Then we have the following *remainder formula*:

$$JG = \sum_i B_i P^{(i)} + R \tag{3.1.1}$$

where J is a product of the initial and separant of P; B_i are d-pols; and $P^{(i)}$ is the i-the derivative of P.

For a triangular set ASC, we define

$$QD(ASC) = \{g \mid \exists J, Jg \in Ideal(ASC)\}$$

where J is a product of the initials and separants of the d-pols in ASC.

Theorem 4 *Let $ASC = \{A_1, ..., A_p\}$ be a non-trivial triangular set in $K\{x_1, \cdots, x_n\}$, J the set of the initials and separants of all A_i. Then $Zero(ASC/J)$ is either empty or an unmixed quasi variety of dimension $DIM(ASC)$. More precisely*

$$Zero(ASC/J) = \cup_{1\leq i\leq l} Zero(QD(ASC_i)/J)$$

where each ASC_i is irreducible and with the same parameter set as ASC. (For the concept of irreducible ascending chain, see Ritt, 1950).

Proof. First, we show that this theorem is true in the algebraic case. Since the dimension of an irreducible variety is equal to the transcendental degree of its generic zero over K, the dimension of $Zero(ASC/J)$ is equal to the largest transcendental degrees of the elements of $Zero(ASC/J)$ in a universal extension field of K. Thus $Dim(Zero(ASC/J)) \leq n-p$. By the affine dimension theorem, if $Zero(ASC/J) \neq \emptyset$ then its dimension is $\geq n-p$. Thus $Zero(ASC/J)$ is an unmixed variety. Since the initials of the A_i is in J, each ASC_i must have the same parameter set as ASC.

Let $c_i = class(A_i), o_i = ord(A_i, x_{c_i})$. We rename x_{c_i,o_i} as y_i, $i = 1, \cdots, p$, and rename other variables and their derivatives occurring in A_i as $u_1, \cdots, u_m$. Now ASC becomes an ascending chain $ASC' = B_1, \cdots, B_p$ in the ordinary polynomial ring $K[U, y_1, \cdots, y_p]$. By the result we just proved,

$$Zero(ASC'/J) = \cup_{1\leq i\leq l} Zero(QD(ASC_i)/J) \tag{1}$$

where each ASC_i is an irreducible ascending chain with the same parameters as ASC'. Then, in the differential case, each ASC_i is also an irreducible ascending chain and $QD(ASC_i)$ a prime ideal (Ritt,1950). We want to show that (1) is also valid when the zero sets and $QD(ASC_i)$ are considered in the differential case. Let $\eta \in Zero(ASC/J)$ be a zero such that the coordinates of η corresponding to the parameters of ASC are independent indeterminates. Then η is a generic zero of some ASC_i, and hence of $QD(ASC_i)$. Note that every zero of $Zero(ASC/J)$ is a specialization of a zero like η. Therefore $Zero(ASC/J) \subset \cup_{1\leq i\leq l} Zero(QD(ASC_i)/J)$. The other direction is easy. ∎

Our algorithm needs the following coarse form of Ritt-Wu's decomposition algorithm in the differential case which only uses the operations $+, -, *$, differentiation, 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.*

Theorem 5 *For two finite d-pol sets PS and DS in $K\{X\}$, we may either test $Zero(PS/DS) = \emptyset$ or find q-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 a product of the initials and separants of the d-pols in ASC_i.

Proof. See (Wu, 1987). In our implementation, we actually use many techniques to enhance the efficiency (Chou, Gao, 1990 and 1993). ∎

3.2 A Zero Structure Theorem

Lemma 6 *Let P be a d-pol in $K\{U, x_1\}$. Then*

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

where P_i are the coefficients of P as a d-pol in $B\{x_1\}$ where $B = K\{U\}$.

Proof. It is obvious. ∎

Lemma 7 *Let P and Q be d-pols in $K\{U, x_1\}$ such that $o = ord(P, x_1) = ord(Q, x_1) \geq 0$, and $d = degree(P, x_{1,o}) > 0$. Then*

$$Proj_{x_1} Zero(P/QI) = Proj_{x_1} Zero(\emptyset/RI)$$

where I is the initial of P and $R = prem(Q^d, P)$.

Proof. It is clear that $Proj_{x_1} Zero(P/QI) \subset Proj_{x_1} Zero(\emptyset/RI)$. If $R = 0$, then

$$Proj_{x_1} Zero(\emptyset/RI) \subset Proj_{x_1} Zero(P/QI);$$

if $R \neq 0$,

$$Proj_{x_1} Zero(\emptyset/RI) \subset Proj_{x_1} Zero(P/QI)$$

is still true. Otherwise, for $e \in Proj_{x_1} Zero(\emptyset/RI)$, each zero of P not vanishing I vanishes Q. When P and Q are considered as polynomials in $K(U, x_1, x_{1,1}, \cdots, x_{1,o-1})[x_{1,o}]$, P must have a factor occurring in Q and hence $R = 0$. This contradiction proves the Lemma. For more details see (Seidenberg, 1956). ∎

Lemma 8 *Let P and Q be d-pols in $K\{U, x_1\}$ such that $o = ord(P, x_1) > ord(Q, x_1)$. Then $Proj_{x_1} Zero(P/QSI) = Proj_{x_1} Zero(\emptyset/QSI)$ where I and S are the initial and separant of P respectively.*

Proof. It is clear that $Proj_{x_1} Zero(P/QSI) \subset Proj_{x_1} Zero(\emptyset/QSI)$. Let G be an irreducible factor of P which involves $x_{1,o}$ effectively. Then a generic zero of the prime ideal determined by G is not a zero of Q. Thus $Proj_{x_1} Zero(\emptyset/QSI) \subset Proj_{x_1} Zero(P/QSI)$. For more details see (Seidenberg, 1956). ∎

We first give a projection algorithm for a triangular set.

Algorithm 9

INPUT: $ASC = A_1, \cdots, A_p$ is a triangular set in $K\{U, x_1, \cdots, x_n\}$ where $lv(A_j) = x_{n+j-p}$, $j = 1, \cdots, p$. D is a d-pol in $K\{U, X\}$.

OUTPUT: $Proj_{x_1,\cdots,x_n} Zero(ASC/J_n D)$ where J_n is the product of the initials and separants of the d-pols $A_1, \cdots, A_n$.

S1. Let $Z = Zero(ASC/J_nD)$. We distinguish three cases:

(a) If $order(J_nD, x_n) < order(A_p)$, then by Lemma 8 and Lemma 6

$$Proj_{x_n}Z = Proj_{x_n}Zero(ASC'/J_{n-1}I_nD) = \cup_k Zero(ASC'/J_{n-1}D_k)$$

where $ASC' = \{A_1, \cdots, A_{p-1}\}$; $I_n = J_n/J_{n-1}$; D_k are d-pols in $K\{U, x_1, \cdots, x_{n-1}\}$.

(b) If $order(J_nD, x_n) = order(A_p)$, by Lemma 7 and Lemma 6

$$Proj_{x_n}Z = Proj_{x_n}Zero(ASC'/J_{n-1}I_nR) = \cup_k Zero(ASC'/J_{n-1}R_k)$$

where $R = prem(D^{ld(A_p)}, A_p)$; and R_k are d-pols in $K\{U, x_1, \cdots, x_{n-1}\}$.

(c) If $order(D, x_n) > order(A_p)$, let $R = prem(D, A_p)$. By the remainder formula (3.1.1), we have $Z = Zero(ASC/J_nR)$ and the projection of Z can be reduced to case (a) or (b).

S2. By now, we have obtained $Proj_{x_n}Z$. Note that the components in $Proj_{x_n}Z$ are still in triangular form. Then we can repeat S1 to eliminate x_{n-1}, x_{n-2}, $\cdots$, x_{n+1-p} similarly. At last, we have

$$Z_1 = Proj_{x_{n+1-p},\cdots,x_n}Z = \cup_{k=1}^{s} Zero(\emptyset/G_k)$$

where each G_k is a d-pol $K\{U, x_1, \cdots, x_{n-p}\}$.

S3 By repeated use of Lemma 6, we may assume that the G_k are free of x_i, i.e., each G_k is a u-pol and $Proj_{x_1,\cdots,x_n}Zero(ASC/JD) = \cup_{k=1}^{s} Zero(\emptyset/G_k)$. ▮

The following algorithm provides a constructive proof for Theorem 3.

Algorithm 10

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

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

S1. Let $D = \prod_{i=1}^{r} d_i$. By Theorem 5, in $K\{U, X\}$ under the variable order $u_1 < \cdots < u_m < x_1 < \cdots < x_n$, we have

$$Zero(PS/D) = \cup_{i=1}^{l} Zero(ASC_i/DJ_i) \tag{3.7.1}$$

For $i = 1, \cdots, l$, do S2 – S5.

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. By Algorithm 9,

$$S_i = Proj_{x_1,\cdots,x_n}Zero(ASC_i/DJ_i) = \cup_{k=1}^{s} Zero(\{B_1, \cdots, B_{r_i}\}/G_k) \tag{3.7.2}$$

where each G_k is the product of the initials and separants of the B_j and a u-pol.

S4. Note that in (3.7.2), each $\{B_1, \cdots, B_{r_i}\}$ is in triangular form and G_k is the product of the initials and separants of the B_j and a u-pol. Then we may compute $D_i = Proj_{u_1,\cdots,u_m} S_i$ using Algorithm 9.

S5. If $D_i = Truth$ ($S_i \neq \emptyset$), by Theorem 4 (S_i, ASC_i) is a solution function of $Zero(PS/DS)$. If $D_i = False$, then $Zero(ASC_i/J_iD) = \emptyset$. We discard it. From (3.7.1), all solution functions thus obtained furnish a cover for $Zero(PS/DS)$. ∎

In (Diop, 1991), elimination theories are used to obtain the input-output equations for nonlinear control systems. Using our structure theorem, we can give not only the input-output equations but also the dependent equations between the "state" variables and the input, output variables. The following is an illustrative example from (Diop, 1991).

Example 11 *Consider the following control system with control or input variable u, state variable x and output variable y*

$$x' = ux^2 + u^2x; \qquad y = x^2. \tag{3.8.1}$$

We need to eliminate x. Using Theorem 5, $Zero(3.8.1) = Zero(\{y'^2 - 4u^2yy' - 4u^2y^3 + 4u^4y^2, 2uyx - y' + 2u^2y\}/u(y' - 2u^2y)) \cup Zero(\{u, y', x^2 - y\}/x) \cup Zero(\{y, x\})$. *A cover of 3.8.1 is*

$(Zero(\{y'^2 - 4u^2yy' - 4u^2y^3 + 4u^4y^2\}/u(y' - 2u^2y)); 2uyx - y' + 2u^2y)$,
$(Zero(\{u, y'\}/y); x^2 - y)$,
$(Zero(\{y\}); x)$.

Then we have three input-output relations. Furthermore, we give the value of the state variable x at each input-output relation set.

4 A Refined Form for the Algebraic Case

In the algebraic case, we may obtain stronger results. First due to the work of Gallo and Mishra, 1992, we may obtain an upper bound for the degrees of the polynomials in the triangular sets. Another improvement is the use of ascending chains of more restricted form.

For two polynomials $P, Q \in B[X]$ 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 q-asc chain $ASC = A_1, ..., A_p$ such that $A_1 \notin B$, we define the resultant of a polynomial 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 polynomials C and C_i such that $R = CG + C_1A_1 + \cdots + C_pA_p$.

A q-asc chain $A_1, ..., A_p$ is called *regular* if $resl(init(A_i); A_1, \cdots, A_{i-1}) \neq 0$, $i = 2, \cdots, p$. Note that this definition of the regular q-asc chain is equivalent to the definition of regular chain in (Kalkbrenner, 1990). We need the following properties of regular asc chains.

Lemma 12 *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 of degree $\prod_{i=1}^{p} ld(A_i)$.*

Proof. 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 polynomial $A_1' \in E[x_1]$ 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 $x_{1,1}$, by replacing v, x_1 by v', x_{11} in A_2 we get a polynomial $A_2' \in E[x_2]$. 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 $D = \prod_{i=1}^{p} ld(A_i)$ 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'. Since $Zero(ASC/J)$ is not empty, it is an unmixed quasi variety by Theorem 4. ∎

A q-asc chain ASC is called a *p-chain* if the initial of every polynomial in ASC involves the parameters of ASC alone. A p-chain is a regular asc chain.

Lemma 13 *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 polynomials in ASC and ASC' respectively.

Proof. We rename the variables as in the proof of Lemma 12. 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

$$R_i(u) = Q_i I_i + \textstyle\sum_{j=1}^{i-1} B_{i,j} A_j \qquad (4.2.1)$$

Let

$$A_i' = A_i Q_i + (\textstyle\sum_{j=1}^{i-1} B_{i,j} A_j) y_i^{d_i} = R_i y_i^{d_i} + Q_i U_i. \qquad (4.2.2)$$

Let $ASC' = A_1', \cdots, A_p'$ and $Q = \prod_{i=2}^{p} Q_i$. The $J' = I_1 \prod_{i=2}^{p} R_i$. It is clear that $Zero(ASC/J) = Zero(ASC/JQ) \cup Zero(ASC, \{Q\}/J)$. From (4.2.1), $Zero(ASC \cup \{Q\}/J) = Zero(ASC \cup \{I_1 \prod_{i=2}^{p} Q_i I_i\}/J) = Zero(ASC \cup \{J'\}/J)$. By (4.2.1) and (4.2.2), $Zero(ASC/JQ) = Zero(\{A_1, A_2Q_2, \cdots, A_pQ_p\}/JQ) =$

$Zero(ASC'/J')$ (consider inductively from p to 1). We have completed the proof. ∎

Remark. The usefulness of regular chains is due 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 polynomial factorization (Zhang, et al, 1992, Kalkbrenner, 1990). Now we have the refined form of solving parametric algebraic systems.

Algorithm 14

INPUT: PS is a polynomial 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 5, in $K[U,X]$ we have $Zero(PS) = \cup_{i=1}^{l} Zero(ASC_i/\{J_i\})$. By Lemma 13 and the remark after Lemma 13, we may assume that 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, $J_i \in K[U, x_1, \cdots, x_{n-s_i}]$. We have

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

S4. Since B_j are free of x_i, we use Lemma 6 repeatedly to eliminate other variables

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

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, by Lemma 12 $S_i \neq \emptyset$. Therefore (S_i, ASC_i) is a solution function for $Zero(PS)$. ∎

We have implemented the algorithm in a SUN-3/50 using Common Lisp. The following are some examples solved by our program based on Algorithm 14.

Example 15 *System (1.2) is to find the Equilibrium Points of a Chemical System (Boege, et al, 1986, Buchberger, 1985, Weispfenning, 1992). In $Q[a_1, \cdots, x_4]$,*

$$Zero((1.2)) = \cup_{i=1}^{9} Zero(ASC_i/J_i)$$

where

$$\begin{aligned} ASC_1 = \{&(a_4 - a_2)x_1 - a_1a_3, (a_4 - a_2)x_2 + a_4^2 + (-a_3 - 2a_2 - a_1)a_4 \\ &+(a_2 + a_1)a_3 + a_2^2 + a_1a_2, x_3 - a_4, x_4 - a_4 + a_2\}; \\ ASC_2 = \{&(a_4 - a_2)x_1 - a_1a_4, (a_4 - a_2)x_2 - a_2a_4 + a_2^2 + a_1a_2, \\ &x_3 - a_3, x_4 - a_4 + a_2\}; \end{aligned}$$

$ASC_3 = \{(a_4 - a_2)x_1 - a_3 a_4, (a_4 - a_2)x_2 - a_2 a_4 + a_2 a_3 + a_2^2,$
$\quad x_3 - a_1, x_4 - a_4 + a_2\};$
$ASC_4 = \{a_3, a_4 - a_2, x_2 + x_1 - a_2, x_3 - a_1, x_4\};$
$ASC_5 = \{a_3, a_4 - a_2, x_2 + x_1 - a_1, x_3 - a_2, x_4\};$
$ASC_6 = \{a_1, a_4 - a_2, x_2 + x_1 - a_2, x_3 - a_3, x_4\};$
$ASC_7 = \{a_1, a_4 - a_2, x_2 + x_1 - a_3, x_3 - a_2, x_4\};$
$ASC_8 = \{a_2, a_4, x_2 + x_1 - a_1, x_3 - a_3, x_4\};$
$ASC_9 = \{a_2, a_4, x_2 + x_1 - a_3, x_3 - a_1, x_4\}.$

Since the ASC_i are p-chains, we may obtain a cover of (1.2) trivially. The following is a more difficult problem.

Example 16 *To find the equilibrium points of the following Lorentz system (Liu, 1990).*

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

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 to print here. (They can be found on p.28-29 of the technical report version of (Gao, Chou, 1992).) It is easy to find a cover of the system from the decomposition. Only four of the ten asc chains were found in (Liu, 1990).

Acknowledgment. The authors wish to thank the referees for valuable suggestions.

References

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

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

[3] Chou, S.C., Gao, X.S. (1990). Ritt-Wu's Decomposition Algorithm and Geometry Theorem Proving. *Prof. of CADE'10*, M.E. Stickel (Ed.), pp 207–220, Lect. Notes in Comp. Sci., No. 449, Springer-Verlag.

[4] Chou, S.C., Gao, X.S. (1993). Automated Reasoning in Differential Geometry and Mechanics: Part I. An Improved Version of Ritt–Wu's Decomposition Algorithm. *Journal of Automated Reasoning*, 10:161–172.

[5] Diop, S. (1991). Elimination in Control Theory. *Mathematics of Control, Signal and Systems*, No.4, p.17-33.

[6] Gao X.S., Chou, S.C. (1992). Solving Parametric Algebraic Systems. *Proc. ISSAC'92*, P.S. Wang (eds), p. 335–341, ACM Press. The full paper is in MM-preprints, No. 7, pp.20-29, Institute of Systems Science, Academia Sinica, Beijing, 100080.

[7] Gallo C., Mishra, B. (1992). Efficient Algorithms and Bounds for Wu-Ritt Characteristic Sets. *Effective Methods in Algebraic Geometry*, p.119-142, Birkhauser.

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

[9] Kapur, D. (1992). Solving Parametric Equations (abstract). *Procs. of IWMM'92*, Beijing.

[10] Lazard, D. (1981). Resolution des Systemes d'Equationes Algebriques. *Theoretic Computer Science,* 15:77-110.

[11] Lazard, D. (1991). A New Method for Solving Algebraic Systems of Positive Dimension. *Discr. Applied Math.,* 33, p.147-160.

[12] Lazard, D. Solving Zero-Dimensional Algebraic Systems, to appear in *J. of Symbolic Computation*.

[13] Liu, Z.J. (1990). An Algorithm on Finding All Isolated zeros of Polynomial equations. *Proc. of ISSAC'90*, p.300, ACM Press.

[14] Ritt, J.F. (1950). *Differential Algebra*. Amer. Math. Sco. Colloquium.

[15] Seidenberg, A. (1956). An Elimination Theory for Differential Algebra. *Univ. of California Pub. of Math*, vol. 3, No. 2, p.31-65.

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

[17] Wang, D.M. (1993) An Elimination Method for Polynomial Systems, *J. of Symbolic Computation*, **16**, 83-114.

[18] Weispfenning, V. (1992). Comprehensive Gröbner Bases. *J. of Symbolic Computation*, 14, p.1-29.

[19] Wu Wen-tsün, (1986). On Zeros of Algebraic Equations — an Applications of Ritt Principle, Kexue Tongbao, 31(1986), 1–5.

[20] Wu Wen-tsün, (1987). A Constructive Theory of Differential Algebraic Geometry. *Lect. Notes in Math.*, No. 1255, pp 173–189, Springer-verlag.

[21] Wu Wen-tsün, (1990). On a Projection Theorem of Quasi-Varieties in Elimination Theory *Chinese Ann. of Math.*, 11B(1990), p.220-226.

[22] Zhang J.Z., Yang, L., Hou, X.R. (1992). A Criterion of Dependency Between Algebraic Equations and Its Applications. *Proc. of the 1992 international Workshop on Mechanization of Mathematics*, p.110-134, Inter. Academic Publishers.