# Counting the Number of Solutions for Algebraic Parametric Equation Systems

Dingkang Wang and Xiao-Shan Gao
Institute of Systems Science, Academia Sinica, Beijing 100080
Email:(dwang,xgao)@mmrc.iss.ac.cn

**Abstract**

Reducing a set of equations in general form to triangular form is a basic idea in equation solving. In this paper, we show how to recover the information about the number of solutions for parametric equation systems by introducing two new forms of triangularization techniques: *the decomposition tree* and *the refined cover*. The decomposition tree can be used to compute the maximal number of solutions for the equation system. The refined cover gives a complete classification of the number of solutions for the equation systems. That is we decompose the value space for the parameters into disjoint components. On each component, the equation system has a fixed number of solutions.
**Keywords:** Parametric equation system, number of solutions, characteristic set method, zero-decomposition theorem.

## 1 Introduction

Parametric algebraic equation systems occur in many application fields such as chemical equilibrium [2], computer vision [4], robotics [1], celestial mechanics [18, 9], etc. Actually, most equation systems raised from applications have parameters. Parametric equations are more complicated than equation systems without parameters in that their solutions vary dramatically for different values of the parameters. For instance, consider the following equation system for the P3P problem from computer vision [4].

$$p_1 = y^2 + z^2 - 2yzp - a^2 = 0$$
$$p_2 = z^2 + x^2 - 2zxq - b^2 = 0$$
$$p_3 = x^2 + y^2 - 2xyr - c^2 = 0$$

where $a, b, c, p, q, r$ are the parameters. Polynomials $p_1, p_2, p_3$ generate a prime ideal and is of zero dimension if the parameters are considered as scalars. But if the parameters satisfy certain algebraic condition, the system will have infinite number of solutions.

In [17], Weispfenning studied parametric equation systems through the concept of comprehensive Gröbner bases. In [14], Sit proposed the concepts of solution function and cover for linear parametric equation systems, which provide an effective method of solving parametric equation systems. Sit's method was extended to general equation systems and differential equation systems in [6, 7, 16]. In [9], Lazard proposed a method to count the number of solutions for parametric systems with parameters less than or equal to two.

The previous work focuses on two problems about the parametric equation systems: (1) for what values of the parameters the equation systems have solutions, and (2) for these parametric values how to solve the equation system. In this paper, we will consider the problem of counting the number of solutions for parametric systems over the field of complex numbers. This problem is raised from applications from computer vision and celestial mechanics [4, 9]. Another motivation of the work is to count the number of solutions for parametric equation systems over the field of real numbers. In [20], a method is proposed to count the number of real and complex roots for a univariate equation with parametric coefficients. A combination of the method in this paper and the method in [20] could give a method to count the number of solutions over the field of real numbers for an equation system.

Reducing a set of equations in general form to triangular form is a basic idea in equation solving, and there exist many methods of triangularization [1, 16, 18]. In this paper, we show how to recover the information about the number of solutions for parametric equation systems by introducing two new forms of triangularization techniques: *the decomposition tree* and *the refined cover*. The decomposition tree can be used to compute the maximal number of solutions for the equation system. The refined cover gives a complete classification of the number of solutions for the equation systems. That is we decompose the value space for the parameters into disjoint components. On each component, the equation system has a fixed number of solutions and these solutions can be represented by equation systems in triangular form. For instance, a complete solution classification for the simple parametric equation $ax^2 + bx + c = 0$ is as follows

1. If $a = b = c = 0$, this equation has infinite solutions.
2. If $a \neq 0$ and $b^2 - 4ac \neq 0$ then the equation has 2 different solutions.
3. If $a \neq 0$ and $b^2 - 4ac = 0$ then the equation has only one solution.
4. If $a = 0$ and $b \neq 0$ then the equation has only one solution.
5. If $a = b = 0$ and $c \neq 0$ then the equation has no solution.

The rest of this paper is organized as follows. In Section 2, we give the method to find the maximal number of solutions. In Section 3, we give the method of complete solution classification.

# 2 Maximal Number of Solutions

## 2.1 Preliminary Results

Let $K$ be a computable field of characteristic zero and $\mathcal{B}[x_1,...,x_n]$ where $\mathcal{B} = \mathbf{K}[\mathbf{u_1},\cdots,\mathbf{u_m}]$. We use $\mathcal{X}$ and $\mathcal{U}$ to denote the variables $x_1,...,x_n$ and $u_1,\cdots,u_m$. A polynomial in $\mathcal{B}$ is called a *u-pol.* Unless explicitly mentioned otherwise, all polynomials in this paper are in $\mathcal{B}[\mathcal{X}]$.

For $P \in B[\mathcal{X}] - B$, 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*, $\frac{\partial P}{x_p} = d c_d x_p^{d-1} + ... + c_1$ the *separant*, $x_p$ the *leading variable*, and $d$ the *leading degree* of $P$ respectively, or $\mathrm{cls}(P) = p$, $\mathrm{init}(P) = c_d$, $\mathrm{sep}(P) = \partial P x_p$, $\mathrm{lvar}(P) = x_p$, $\mathrm{ldeg}(P) = d$. The class of a u-polynomial is zero.

A sequence of polynomials $AS = A_1,...,A_p$ in $\mathcal{B}[\mathcal{X}] - B$ is said to be a *ascending chain* (abbr. chain) or in *triangular form*, if either $p = 1$ and $A_1 \neq 0$ or $0 < \mathrm{cls}(A_i) < \mathrm{cls}(A_j)$ and the degree of $A_j$ in $\mathrm{lvar}(A_i)$ is less than $\mathrm{ldeg}(A_i)$ for $1 \leq i < j$. The variable set $\{x_1,\cdots,x_n\} - \{\mathrm{lvar}(A_1),\cdots,\mathrm{lvar}(A_p)\}$ is called the *parameter set* of $AS$. We define the *dimension* (in $\mathcal{X}$) of $AS$ to be $\dim(AS) = n - p$, i.e. the number of the parameters of $AS$. The *degree* of $AS$ is defined as $\deg(AS) = \prod_{i=1}^{n} \mathrm{ldeg}(A_i)$.

We may define ascending chains in $\mathcal{B}$ and $\mathcal{B}[\mathcal{X}]$ similarly. For a chain $AS$ and a polynomial $P$, we use $\mathrm{Prem}(P, AS)$ to denote the *pseudo-remainder* of $P$ with $AS$ [12, 18].

The *saturation* for a chain $AS$ is defined as

$$\mathrm{Sat}(AS) = \{P | \exists J\ s.t. Jp \in \mathrm{Ideal}(AS)\}$$

where $J$ is a product of the powers of initials of the polynomials in $AS$. It is well-known that $\mathrm{Sat}(AS)$ is either (1) or an un-mixed ideal [1, 5], and if $AS$ is irreducible then $\mathrm{Sat}(AS)$ is a prime ideal [11, 12].

Let $P$ be a polynomial and $AS = A_1,\cdots,A_p$ be a chain in $\mathbf{K}[\mathcal{U},\mathcal{X}] - \mathbf{K}[\mathcal{U}]$. We recursively define $\mathrm{Resultant}(P, AS) = \mathrm{Resultant}(\mathrm{Resultant}(P, A_p, \mathrm{lvar}(A_p)), A_1,\cdots,A_{p-1})$.

**Lemma 2.1** *Let $AS$ be an irreducible chain [12, 18], $P$ a polynomial. If $Prem(P, AS) \neq 0$, then $Resultant(P, AS) \neq 0$.*

*Proof.* See [18].

A chain $AS$ is called a *u-chain* if the initials of the polynomials in $AS$ are u-polynomials.

**Lemma 2.2** *If $AS$ is an irreducible chain whose dimension in the $\mathcal{X}$ is zero, then we can find an irreducible u-chain $AS'$ such that $Sat(AS) = Sat(AS')$.*

*Proof.* Let $AS = B_1, \cdots, B_q, A_1, \cdots, A_n$ such that $B_i$ are u-polynomials and $A_i \in B[X] - B$. Let $I_i = \mathrm{init}(A_i)$. It is clear that $I_1$ is a u-polynomial. For $k > 1$, let $R_k = \mathrm{Resultant}(I_k, A_1, \cdots, A_{k-1})$. Since $AS$ is irreducible, by Lemma 2.1 $R_k$ is a nonzero u-polynomial. By the properties of the resultants, there exist $C_i \in \mathbf{K}[\mathbf{u}, \mathcal{X}], \mathbf{i} = \mathbf{1}, \cdots, \mathbf{k}$ such that $R_k = C_k I_k + \sum_{i=1}^{k-1} C_i A_i$. Let $A'_k = C_k A_k + (\sum_{i=1}^{k-1} C_i A_i) x_k^{\mathrm{ldeg}(A)k)}$. Then the initial of $A'_k$ is $R_k$. Let $AS' = B_1, \cdots, B_q, A_1, A'_2, \cdots, A'_n$. We have $\mathrm{Sat}(AS) = \mathrm{Sat}(AS')$. ∎

Let $PS$ be a polynomial set in $\mathbf{K}[\mathcal{U}, \mathcal{X}]$. For a universal extension field $\mathbf{E}$ of $\mathbf{K}$, let

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

For a polynomial set $PS$ and a polynomial $D$ in $\mathbf{K}[\mathcal{U}, \mathcal{X}]$, we define

$$\mathrm{Zero}(PS/D) = \mathrm{Zero}(PS) - \mathrm{Zero}(D).$$

A *quasi-variety* is defined to be $Q = \cup_{i=1}^{t} \mathrm{Zero}(PS_i/D_i)$ where $PS_i$ are polynomial sets and $D_i$ are polynomials in $\mathbf{K}[\mathcal{U}, \mathcal{X}]$. A *basic quasi-variety* is of the form $\mathrm{Zero}(AS/JD)$ where $AS$ is a chain, $J$ its $I$-product, and $D$ a polynmial. It is known that a basic quasi-variety is either empty of un-mixed with dimension $\dim(AS)$ [5].

For a quasi variety $Q$, let $\mathbf{M}(\mathbf{Q})$ be the *maximal number of distinct solutions* of $x_i, i = 1, . \cdots, n$ for all possible specific values of the parameters $u_j, j = 1, \cdots, m$.

**Lemma 2.3** *Let $AS$ be a chain in $\mathbf{K}[\mathcal{U}, \mathcal{X}]$ with zero dimension in $\mathcal{X}$ and $J$ the product of initials of the polynomials in $AS$ (abbr. I-product of $AS$). We have* $\mathbf{M}(\mathbf{Zero}(\mathbf{AS}/\mathbf{J})) \leq \mathbf{deg}(\mathbf{AS})$, *and if $AS$ is irreducible then* $\mathbf{M}(\mathbf{Zero}(\mathbf{AS}/\mathbf{J})) = \mathbf{deg}(\mathbf{AS})$.

*Proof.* Let $A_i \in AS$ be the polynomial with leading variable $x_i, i = 1, \cdots, n$. For specific values of the parameters, we may solve $x_1$ with $A_1 = 0$. Substituting each solutions for $x_1$ into $A_2 = 0$, we may solve $x_2$ with $A_2 = 0$, and so on. Therefore, the total number of solutions is less than or equal to $\deg(AS)$. Let $J$ be the product of the initials of $A_i$ and the discriminant of $A_i$ with $\mathcal{X}$ for $i = 1, \cdots, n$. If $AS$ is irreducible, $\mathrm{Prem}(J, AS) \neq 0$. By Lemma 2.1, $R = \mathrm{Resultant}(J, AS) \neq 0$ is a u-polynomial. For a set of parametric values that does not vanish $R$, each $A_i = 0$ has $\mathrm{ldeg}(A_i)$ distinct roots. Hence $\mathbf{M}(\mathbf{Zero}(\mathbf{AS}/\mathbf{J})) = \mathbf{deg}(\mathbf{AS})$. ∎

## 2.2 Zero Decomposition Tree

By a *parametric equation system*, we mean a set of equations and inequations like

$$\begin{cases} P_1(u_1, \cdots, u_m, x_1, \cdots, x_n) = 0 \\ \vdots \\ P_s(u_1, \cdots, u_m, x_1, \cdots, x_n) = 0 \\ D_1(u_1, \cdots, u_m, x_1, \cdots, x_n) \neq 0 \\ \vdots \\ D_t(u_1, \cdots, u_m, x_1, \cdots, x_n) \neq 0 \end{cases} \tag{1}$$

where $u_1, \cdots, u_m$ are the parameters and $x_1, \cdots, x_n$ are the variables to be solved. Let

$$PS = \{P_1, \cdots, P_s\}, D = \prod_{i=1}^{t} D_i. \tag{2}$$

Wu-Ritt's zero decomposition theorem is a general method to solve equations [19, 12]. It is to reduce the zero set for a general equation system to the union of zero sets of equation systems in triangular form.

**Theorem 2.4 (Coarse Form)** *For a polynomial set $PS$ and a polynomial $D$, we can find chains $CS_i$ such that*

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

*where $J_i$ is the I-product of $CS_i$ and $Prem(D, CS_i) \neq 0$. We also have $Zero(CS_i/DJ_i) \cap Zero(CS_j/DJ_j) = \emptyset$ for $i \neq j$.*

In the above theorem, it is easy to estimate the number of solutions for each component in the right hand size with Lemma 2.3. The difficulty is how to estimate the number of solutions for the union of these components. It is obviously false to take the sum of the number of solutions of all the components. For the P3P problem in Section 1, we may obtain more than one thousand components, while the problem has only four solutions at most. We will solve this problem by introducing the zero decomposition tree.

By a careful analysis of the zero decomposition algorithm [12, 18], the following two steps will decompose one zero set into two and hence need to be analyzed.

**Well-Ordering.** A chain $CS$ is called a *characteristic set* of a polynomial set $PS$ if $CS \subset \mathrm{Ideal}(PS)$ and $\mathrm{Prem}(P, CS) = 0$ for each $P \in PS$. If $CS$ is a characteristic set of $PS$, we have

$$\mathrm{Zero}(PS) = \mathrm{Zero}(CS/J) \bigcup \mathrm{Zero}(PS \cup \{J\})$$

where $J$ is the I-product of $CS$.

The well-ordering principle says that for a finite set $PS$ of polynomials, there is an algorithm to find a characteristic set $CS$ of $PS$.

**Splitting.** For a polynomial set $PS$ and two polynomials $P_1$ and $P_2$,

$$\mathrm{Zero}(PS, P_1 * P_2) = \mathrm{Zero}(PS \cup \{P_1\}) \cup \mathrm{Zero}(PS \cup \{P_2\}/P_1)$$

Basically speaking, the zero decomposition algorithm works as follows. We first use the well-ordering algorithm to obtain a characteristic set $CS$ of $PS$. If $CS$ is irreducible [12], then $\mathrm{Zero}(PS)$ is reduced into the union of $\mathrm{Zero}(CS/J)$ and $\mathrm{Zero}(PS \cup J)$. If $CS$ is reducible [12], a polynomial in $CS$ can be factorized into the product of two polynomials. Now, we use the splitting step to reduce $\mathrm{Zero}(PS)$ into two 'simpler' equation systems.

**Lemma 2.5** *In the well-ordering step, if $AS$ is a u-chain,*

$$\mathbf{M}(\mathbf{Zero}(\mathbf{PS})) = \max\{\mathbf{M}(\mathbf{Zero}(\mathbf{CS}/\mathbf{J})), \mathbf{M}(\mathbf{Zero}(\mathbf{PS} \cup \{\mathbf{J}\})\}$$

*Proof.* Since $J$ is a u-polynomial, for a set of specific values of the parameters, we have either $J = 0$ or $J \neq 0$. If $J \neq 0$, $\mathrm{Zero}(PS \cup J) = \emptyset$ and $\mathrm{Zero}(PS) = \mathrm{Zero}(CS/J)$. If $J = 0$, $\mathrm{Zero}(CS/J) = \emptyset$ and $\mathrm{Zero}(PS \cup \{J\}) = \mathrm{Zero}(PS)$. The result is clearly true in this case. ∎

The following example shows that the above lemma is not correct if $J$ is not a u-polynomial.

**Example 2.6** *Let $PS = \{x_1^2 - u_1, (x_1 - 1)x_2^2 - x_2 + 1\}$. Note that $PS$ itself is a chain. We have*

$$Zero(PS) = Zero(PS/(x_1 - 1)) \cup Zero(\{u_1 - 1, x_1 - 1, x_2 - 1\}).$$

*In the case $u_1 = 1$, the first component has two solutions and the second component has one solutions, which consist of the three solutions of the equation system. Therefore, in the general case $\mathbf{M}(\mathbf{Zero}(\mathbf{PS})) = \mathbf{M}(\mathbf{Zero}(\mathbf{PS}/(\mathbf{x_1} - \mathbf{1}))) + \mathbf{M}(\mathbf{Zero}(\{\mathbf{u_1} - \mathbf{1}, \mathbf{x_1} - \mathbf{1}, \mathbf{x_2} - \mathbf{1}\})) = \mathbf{5}$. But, the maximal number of solutions of $PS = 0$ is four.*

**Lemma 2.7** *In the splitting step, we have*

1. *If $P_1$ is a u-polynomial*

   $$\mathbf{M}(\mathbf{Zero}(\mathbf{PS} \cup \{\mathbf{P_1} * \mathbf{P_2}\})) = \max\{\mathbf{M}(\mathbf{Zero}(\mathbf{PS} \cup \{\mathbf{P_1}\})), \mathbf{M}(\mathbf{Zero}(\mathbf{PS} \cup \{\mathbf{P_2}\}/\mathbf{P_1}))\}.$$

2. *If both $P_1$ and $P_2$ are not u-polynomial*

   $$\mathbf{M}(\mathbf{Zero}(\mathbf{PS} \cup \{\mathbf{P_1} * \mathbf{P_2}\})) \leq \mathbf{M}(\mathbf{Zero}(\mathbf{PS} \cup \{\mathbf{P_1}\})) + \mathbf{M}(\mathbf{Zero}(\mathbf{PS} \cup \{\mathbf{P_2}\}/\mathbf{P_1})).$$

*Proof.* The proof of the first case is similar to that of Lemma 2.5. The second case is obviously true. ∎

To introduce our new decomposition theorem, we need the concept of *decomposition tree*. The tree has three kinds of notes +-note, $m$-note, and $z$-note. A $z$-note is a basic quasi-variety with zero dimension in $\mathcal{X}$. The leafs of the tree must be $z$-notes and all the other notes are either +-notes or $m$-notes. A +-note or $m$-note $V$ represents the union of all its descendant leafs. Let $V$ be a note and $V_i, i = 1, \cdots, k$ its direct children. If $V$ is a +-note, $\mathbf{M(V)} = \sum_{\mathbf{i=1}}^{\mathbf{k}} \mathbf{M(V_i)}$. If $V$ is an $m$-note, $\mathbf{M(V)} = \max_{\mathbf{i=1}}^{\mathbf{k}} \mathbf{M(V_i)}$.

**Theorem 2.8** *Let $PS$ and $D$ be a polynomial set and a polynomial in $\mathbf{K}[\mathcal{U}, \mathcal{X}]$. If $\mathbf{M(Zero(PS/D))}$ is finite, then we have an algorithm to find a decomposition tree whose root equals to $Zero(PS/D)$.*

*Proof.* We may follow the original zero decomposition algorithm [18]. The difference is that in each of the well-ordering step or splitting step, we will use Lemmas 2.5 or 2.7 to generate an $x$-note or an $m$-note. By Lemma 2.2, for each zero dimensional irreducible asc, we may always find an equivalent u-chain. This guarantees that Lemma 2.5 can always be used in the well-ordering step. ∎

**Example 2.9** *Continuing from Example 2.6. With Lemma 2.2, we may change $PS$ into a u-chain $AS = x_1^2 - u_1, (u_1 - 1)x_2^2 - (x_1 + 1)(x_2 - 1)$. Now, we may obtain a zero decomposition as follows.*

$$Zero(PS) = C_1 \cup C_2 \cup C_3$$

*where $C_1 = Zero(AS/(u_1 - 1)), C_2 = Zero(\{u_1 - 1, x_1 - 1, x_2 - 1\}), C_3 = Zero(\{u_1 - 1, x_1 + 1, 2x_2^2 + x_2 - 1\})$ A corresponding decomposition tree is as follows.*

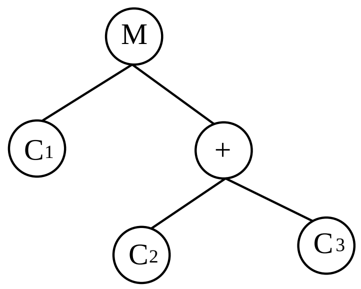


*Fig. The decomposition tree for $Zero(PS)$*

*From this tree, we may conclude that the maximal number of solutions of $PS = 0$ is four. This fact is not trivial, since the Bezout number of the original system is six.*

**Theorem 2.10** *Let $PS$ and $D$ be a polynomial set and a polynomial in $\mathbf{K}[\mathcal{U}, \mathcal{X}]$. We may find chains $CS_i, i = 1, \cdots, r$ with positive dimensions in the $\mathcal{X}$ and a decomposition tree $T$ such that*

$$Zero(PS/D) = \cup_{i=1}^{r} Zero(Sat(CS_i)/D) \bigcup T.$$

*The decomposition tree $T$ represents the isolated zeros of Zero$(PS/D)$.*

*Proof.* In the well-ordering step, if

$$\text{Zero}(PS) = \text{Zero}(CS/J) \bigcup \text{Zero}(PS \cup J)$$

then it is easy to show that

$$\text{Zero}(PS) = \text{Zero}(\text{Sat}(CS)) \bigcup \text{Zero}(PS \cup J).$$

If $CS$ is of positive dimension in the $\mathcal{X}$, then we will use the later form. Otherwise, we will add Zero$(CS/J)$ to the decomposition tree. This will give us a zero decomposition of the desired form. To guarantee that the decomposition tree consists of the isolated zeros, for each leaf Zero$(AS/J)$ in the decomposition tree we will check whether Zero$(AS/J) \subset$ Zero$(\text{Sat}(CS_i))$ for some $i$. If the above relation is valid for some $i$, Zero$(AS/J)$ is contained in a solution component of positive dimension and will be deleted from the decomposition tree. Let $PS_i$ be a basis of Sat$(CS_i)$ which can be computed with Grobner basis ????. The relation Zero$(AS/J) \subset$ Zero$(\text{Sat}(CS_i))$ is valid iff for each $P \in PS_i$, Prem$(P, AS) = 0$. ∎

# 3 Complete Solution Classification

By complete solution classification for a parametric equation system, we mean a division of $\mathbf{E^m}$ into the union of disjoint components such that when the parameters $u_1, \cdots, u_m$ taking values on the same component, the parametric system has the same number of solutions.

## 3.1 U-Zero Decomposition Theorem

For a set of polynomials $PS$ and a polynomial $D$, if Zero$(PS/D)$ consists of a fixed number of solutions for variables $\mathcal{X}$ for all possible values taken from a quasi-variety $D$ of the parameters $u_j$, we say that Zero$(PS/D)$ is *uniform* on $D$, and use the notation $\mathbf{N}(\mathbf{Zero}(\mathbf{PS}/\mathbf{D}))$ to denote the number of solutions.

Let $AS = B_1, \cdots, B_q, A_1, \cdots, A_n$ be an irreducible chain with zero dimension for the $\mathcal{X}$, $I_i$ and $D_i$ the initials and disciminants of $A_i, i = 1, \cdots, n$. By Lemma 2.2, we may assume that $I = \prod_{i=1}^{n} I_i$ is a u-polynomial. Let $R = \text{Resultant}(\prod_{i=1}^{n} D_i, A_1, \cdots, A_n)$. By Lemma 2.1, $R$ is a non-zero u-polynomial. We call $IR$ the *ID-product* of $AS$

**Lemma 3.1** *Using the above notations, Zero$(AS/IR)$ is uniform over $D =$ Zero$(B_1, \cdots, B_q/IR)$ and* $\mathbf{N}(\mathbf{Zero}(\mathbf{AS}/\mathbf{IR})) = \prod_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{ldeg}(\mathbf{A_i})$.

*Proof.* From the definition of $R$ it is clear that $R \neq 0$ implies $D_i \neq 0, i = 1, \cdots, n$. Take a set of value from $D$ for the parameters and substitute it into $A_i$ to obtain $A_i'$. Then $A_1' = 0$ is a univariate equation of degree $\mathrm{ldeg}(A_1)$ whose discriminant is not zero. Then $A_1' = 0$ has $\mathrm{ldeg}(A_1)$ distinct solutions. Substituting each solution of $A_1' = 0$ into $A_2' = 0$, we obtain a univariate equation $A_2'' = 0$ of degree $\mathrm{ldeg}(A_2)$ whose discriminant is not zero. Hence $A_2'' = 0$ has $\mathrm{ldeg}(A_2)$ distinct equations. Continuing, we may prove the result. ∎

The well-ordering principle and the zero decomposition theorem can also be modified as follows without difficulty.

**Well-ordering Principle**. Let $CS$ be a characteristic set of $PS$. If $CS$ is irreducible and of zero dimension, we have

$$\mathrm{Zero}(PS) = \mathrm{Zero}(CS/J) \bigcup \mathrm{Zero}(PS \cup \{J\})$$

where $J$ is the ID-product of $CS$.

**Theorem 3.2 (D-Zero Decomposition Theorem)** *For a polynomial set $PS$ and a polynomial $D$, we can find irreducible ascending chains $CS_i$ such that*

$$Zero(PS/D) = \cup_{i=1}^{l} \mathrm{Zero}(CS_i/DJ_i)$$

*where $J_i$ is the I-product or ID-product of $CS_i$ if $CS_i$ is of positive or zero dimension in the $\mathcal{X}$.*

**Lemma 3.3** *Let $AS$ be an irreducible u-chain with zero dimension in $\mathcal{X}$, $D$ a polynomial. Then there exists an algorithm to obtain irreducible u-chains $AS_i, \imath = 1, \cdots, r$ of zero dimension in $\mathcal{X}$ and u-polynomials $D_i$ such that*

$$Zero(AS/J * D) = \bigcup Zero(AS_i/J_iD_i)$$

*where $J$ and $J_i$ are the I-products for $AS$ and $AS_i$.*

*Proof.* If $D$ doesn't involve any variables in $\mathcal{X}$, the theorem is obvious. We assume that $\mathrm{Prem}(D, AS) \neq 0$. Otherwise, $\mathrm{Zero}(AS/JD) = \emptyset$. Since $AS$ is irreducible, by Lemma 2.1, $R = \mathrm{Resultant}(D\prime\prime, AS) \neq 0$. Then

$$\begin{aligned} \mathrm{Zero}(AS/J * D) &= \mathrm{Zero}(\{AS, R\}/J * D) \bigcup \mathrm{Zero}(AS/J * D * R) \\ &= \mathrm{Zero}(\{AS, R\}/J * D) \bigcup \mathrm{Zero}(AS/J * R) \end{aligned}$$

For the system $\{AS, R\}$, we have

$$\mathrm{Zero}(\{AS, R\}/J) = \bigcup_j \mathrm{Zero}(AS_j'/J * J' * D').$$

Since $R = 0$, $AS$ must be reducible by Lemma 2.1. Therefore, $AS_j'$ is of lower rank than $AS$. Repeat the above process for $(AS_j', J' * D')$, the process will terminate after a finite number of steps. ∎

The zero decomposition theorem can be further modified as follows.

**Theorem 3.4 (U-Zero Decomposition Theorem)** *For a polynomial set $PS$ and a polynomial $D$, we can find irreducible ascending chains $CS_i$ and u-polynomials $D_i$ such that*

$$Zero(PS/D) = \cup_{i=1}^{l} Zero(CS_i/D_iJ_i) \bigcup \cup_{i=l+1}^{r} Zero(Sat(CS_i/D)).$$

*For $i = 1, \cdots, l$, $CS_i$ are u-chains and of zero dimension in $\mathcal{X}$ and $J_i$ is the ID-product of $CS_i$. For $i = l+1 \cdots, r$, $CS_i$ are of positive dimensions in $\mathcal{X}$ and $J_i$ is the I-product of $CS_i$. Also, the components on the right hand size are disjoint.*

*Proof.* This is a direct consequence of Theorem 3.2 and Lemma 3.3. ∎

## 3.2 Solution Classification

For a polynomial set $PS$ and a polynomial $D$ in $K[\mathcal{U}, \mathcal{X}]$, we define the projection with the $\mathcal{X}$ as follows

$$\mathrm{Proj}_{x_1,\cdots,x_n}\mathrm{Zero}(PS/D) = \{e \in E^m | \exists a \in E^n s.t. (e, a) \in \mathrm{Zero}(PS/D)\}$$

If $m = 0$, we define $\mathrm{Proj}_{x_1,\cdots,x_n}\mathrm{Zero}(PS/D) = Truth$ if $\mathrm{Zero}(PS/D) \neq \emptyset$, and $False$ otherwise. It is known that the projection of a quasi variety is also a quasi variety [19, 8]. In particular, the projection for a chain is easy to compute as shown by the following lemma.

**Lemma 3.5** *Let $AS = B_1, \cdots, B_q, A_1, \cdots, A_n$ be a u-chain, $J$ its I-product, and $D$ a u-polynomial. Then*

$$Proj_{x_1,\cdots,x_n} Zero(AS/JD) = Zero(B_1, \cdots, B_q/JD).$$

*Proof.* It is obvious. ∎

We extending the concept cover introduced by Sit [14] as follows. A *refined cover* for parametric equation system (1) is a set of *solution functions*

$$(S_i, AS_{i,j}, j = 1, \cdots, k_i), i = 1, \cdots, k$$

such that

- $S_i, i = 1, \cdots, k$ are disjoint quasi-varieties in $E^m$ and $AS_{i,j}$ are chains in $\mathbf{K}[\mathcal{U}, \mathcal{X}] - \mathbf{K}[\mathcal{U}]$ for all $i$ and $j$.
- $\mathrm{Proj}_{x_1,\ldots,x_n}\mathrm{Zero}(PS/D) = \cup_j S_i$.
- For each $u' \in S_i$,
$$\mathrm{Zero}(PS/D) = \cup_j \mathrm{Zero}(AS_{i,j}/J_{i,j})$$
where $J_{i,j}$ is the I-product of $AS_{i,j}$.

- If Zero$(PS/D)$ is of zero dimension in $\mathcal{X}$, then Zero$(PS/D)$ is uniform over $S_i$ and for each $i$,

$$\mathbf{NZero(PS/D)} = \mathbf{Max}_{\mathbf{i=1}}^{\mathbf{k}} \sum_{\mathbf{j=1}}^{\mathbf{k_i}} \mathbf{deg(AS_{i,j})}$$

We will give an algorithm to find a refined cover for a parametric equation system (1).

**Theorem 3.6** *There exists an algorithm to find a refined cover for parametric equation system (1).*

*Proof.* By Theorem 3.4, we have a decomposition of the following form

$$\text{Zero}(PS/D) = \cup_{i=1}^{l}\text{Zero}(CS_i/E_iJ_i) \bigcup \cup_{i=l+1}^{r}\text{Zero}(CS_i/DJ_i).$$

Let $T_i = \text{Proj}_{x_1,\cdots,x_n}\text{Zero}(CS_i/E_iJ_i), i = 1,\cdots,l,\ T_i = \text{Proj}_{x_1,\cdots,x_n}\text{Zero}(CS_i/DJ_i), i = l+1,\cdots,r$. $T_i$ is easy to compute [6]. Let $AS_i = CS_i \cap (K[\mathcal{U},\mathcal{X}] - K[\mathcal{U}])$. We will obtain the refined cover from $T_i$ and $AS_i$ by repeating the following step. At the beginning, let $S_1 = T_1,\ AS_{1,1} = AS_1$. Let

$$(S_i, AS_{i,j}, j = 1,\cdots,k_i), i = 1,\cdots,d$$

be a set of solution functions obtained from $T_i$ and $AS_i, i = 1,\cdots,k$. We will show how to obtain a set of new solution functions by adding $T_{k+1}$ and $AS_{k+1}$. For each $(S_i, AS_{i,j})$, let $S_i' = S_i \cap T_{k+1}$, $S_i'' = S_i - S_i'$, $S_i''' = T_{k+1} - S_i'$. Then on $S_i'$, the solutions of the equation system may be obtained from $AS_{k+1}$ and $AS_{i,j}, j = 1,\cdots,k_i$. On $S_i''$, the solutions of the equation system may be obtained from $AS_{i,j}, j = 1,\cdots,k_i$. On $S_i'''$, the solutions of the equation system may be obtained from $AS_{k+1}$. We replace $(S_i, AS_{i,j}, j = 1,\cdots,k_i)$ by the three new solution functions: $(S_i', AS_{k+1}, AS_{i,j}, j = 1,\cdots,k_i)$, $(S_i'', AS_{i,j}, j = 1,\cdots,k_i)$, $(S_i''', AS_{k+1})$ to obtain a set of new solution functions. Of course, we need only add those solution functions whose first part is not empty.

We will prove that the set of solution functions thus obtained are a refined cover for the equation system. The first and second conditions are clearly true. The third condition is also true, because the $S_i$ are disjoint. For the fourth condition, we need only consider those solution functions with chains of zero dimension in $\mathcal{X}$. From Theorem 3.4 and Lemma 3.1, $AS_i$ is uniform over $T_i$ and $\mathbf{N(Zero(AS_i/J_i))}$ equals to the product of the leading degrees of the polynomials in $AS_i$. Also note that the components in (2) are disjoint. Then, the number of solutions of (1) is equal to the sum of the number of solutions for individual chains. ∎

In the above theorem, we need to compute the intersection and the difference of two quasi-varieties. Such methods can be found in [15].

**Example 3.7** *Continuing from Example 2.9. With Theorem 3.4, a u-zero decomposition for Zero$(PS)$ is*

$$Zero(PS) = C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6$$

*where*

$C_1 = Zero(AS/u_1(u_1-1)(16u_1-25))$ *in which* $AS = x_1^2-u_1, (u_1-1)x_2^2-(x_1+1)(x_2-1)$
$C_2 = Zero(\{u_1-1, x_1-1, x_2-1\})$
$C_3 = Zero(\{u_1-1, x_1+1, 2x_2^2+x_2-1\})$
$C_4 = Zero(\{u_1, x_1, x_2^2+x_2-1\},$
$C_5 = Zero(\{16u_1-25, 4x_1-5, x_2-2\}.$
$C_6 = Zero(\{16u_1-25, 4x_1+5, 9x_2^2-4x_2+4\}$

*From this decomposition, we may obtain the following refined cover for* $PS = 0$.
$S_1 = Zero(/u_1(u_1-1)(16u_1-25))$
$TS_{1,1} = \{x_1^2-u_1, (u_1-1)x_2^2-(x_1+1)(x_2-1)\}$

$S_2 = Zero(\{u_1-1\})$
$TS_{2,1} = \{x_1-1, x_2-1\})$
$TS_{2,1} = \{x_1+1, 2x_2^2+x_2-1\})$

$S_3 = Zero(u_1)$
$TS_{3,1} = \{x_1, x_2^2+x_2-1\}$

$S_3 = Zero(16u_1-25)$
$TS_{4,1} = \{4x_1-5, x_2-2\}$
$TS_{4,1} = \{4x_1+5, 9x_2^2-4x_2+4\}$

*From this refined cover it is easy to see that the equation system may have 2,3,4 solutions respectively.*

# 4 Conclusion

In this paper, we give two algorithms. The first algorithm is a modification of Wu-Ritt's zero decomposition theorem. In the algorithm, we may construct a zero decomposition tree which gives the maximal number of solutions. The second algorithm gives a complete solution classification for a parametric equation system.

The work in this paper may be further extended in several directions. For convenience, we use irreducible ascending chain in our methods. Actually, regular ascending chains [1] are enough for most of the results in this paper. We only count the number of solutions over algebraically closed field. It is interesting to go further by counting the number of real solutions. It is known that the number of solutions for algebraic varieties can be obtained with the Hilbert function [3]. It is interesting to see whether this technique can be extended to parametric equations.

# References

[1] P. Aubry, D. Lazard, and M. M. Maza, On the Theory of Triangular Sets, *J. of Symbolic Computation*, **25**, 105-124, 1999.

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

[3] G. Björck and R. Fröberg, A Faster Way to Count the Solutions of Inhomogeneous Systems of Algebraic Equations, *J. of Symbolic Computation*, **12**, 329-336, 1991.

[4] M. A. Fishler, and R. C. Bolles, Random Sample Consensus: A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartomated Cartography, *Communications of the ACM*, **24**,381-395, 1981.

[5] X.-S. Gao and S.-C. Chou, On the Dimension for Arbitrary Ascending Chains, *Chinese Bull. of Scis.*, **38**, 396-399, 1993.

[6] X.-S. Gao and S.-C. Chou, Solving Parametric Algebraic Systems, *Proc. of ISSAC-92,* 335-341, 1992, ACM Press, New York.

[7] X.-S. Gao and S.-C. Chou, A Zero Structure Theorem for Differential Parametric Systems, *J. of Symbolic Computation*, **16**, 585-595, 1994.

[8] J. Heintz, Definability and Fast Quantifier Elimination in Algebraically Closed Fields, *Theoretic Computing Science*, **24**, 239-278, 1983.

[9] D. Lazard, Resolution of Polynomial Systems, *Computer Mathematics*, (eds. X.S. Gao and D. Wang), World Scientific, 1-8, 2000, Singapore.

[10] D. Lazard, A New method for Solving Algebraic Systems of Positive Dimension, *Discrete Appl. Math.*, **33**, 147-160, 1991.

[11] E. R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, 1973, London.

[12] J. F. Ritt, *Differential algebra*, Amer. Math. Sco. Colloquium, (1950), New York.

[13] A. Seidenberg, An Elimination Theory for Differential Algebra, *Univ. California Publication in Math.*, 3, 31-65, 1956.

[14] W.Y. Sit, A Theory for Parametric Linear Systems, *In Proc. of ISSAC-91.* 112-121, 1991, ACM Press, New York.

[15] W.Y. Sit, Computations of Quasi-Varieties, Preprints, 2000.

[16] D. Wang, *Elimination Methods*, 2000, Springer, Berlin.

[17] V. Weispfenning, Comprehensive Groebner Bases. *J. of Symbolic Computation.* **14**, 1-29, 1992.

[18] W.-T. Wu, *Basic Principles of Mechanical Theorem Proving in Geometries*, Volume I: Part of Elementary Geometries, Science Press, Beijing (in Chinese), 1984. English Version, 1994, Springer-Verlag, Berlin.

[19] W.-T. Wu, *Mathematics Mechanization*, Science Press/Kluwer, Beijing, 2000.

[20] L. Yang, J.Z. Zhang, and X.R. Hou, *Non-linear Algebraic Equations and Automated Theorem Proving*, ShangHai Science and Education Pub., ShangHai, 1996.