Science in China Series A: Mathematics
Oct., 2007, Vol. 50, No. 10, 1441–1450
www.scichina.com
www.springerlink.com

An algorithm for decomposing a polynomial system into normal ascending sets

Ding-kang WANG† & Yan ZHANG

Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100080, China
(email: dwang@mmrc.iss.ac.cn, yzhang@mmrc.iss.ac.cn)

Abstract We present an algorithm to decompose a polynomial system into a finite set of normal ascending sets such that the set of the zeros of the polynomial system is the union of the sets of the regular zeros of the normal ascending sets. If the polynomial system is zero dimensional, the set of the zeros of the polynomials is the union of the sets of the zeros of the normal ascending sets.

Keywords: zero decomposition, normal ascending set, polynomial system

MSC(2000): 68Q40, 13P10

1 Introduction

The characteristic set method was introduced by Ritt[1] and Wu[2]. This method has been used for mechanical geometric theorem proving by Wu. It can also be used for solving a system of polynomial equations. In order to solve a system of polynomial equations, the polynomial system should be decomposed into a triangular form. An algorithm to decompose a polynomial system into ascending sets was proposed in [2]. Many improvements for this algorithm have been proposed by Chou[3], Chou and Gao[4,5], and Wang[6]. Wu's algorithm may produce redundant decompositions of varieties and the components may be empty. One can discover the possible emptiness of a component, which is defined by an ascending set by computing the projection[7]. Wu also gave an algorithm to decompose a variety into irreducible components, with each irreducible component being not empty, and factorization over the algebraic extension field needed for the irreducible decomposition of the variety. An algorithm to factor polynomials over an algebraic extension field was proposed by Trager[8], and factorization has also been investigated by Wang[6] and Yuan[9]. Generally, polynomial factorization over an algebraic extension field is costly. To avoid the emptiness of the varieties and the factorization, Yang and Zhang[10] introduced regular chains and gave an algorithm to compute the regular decomposition of a polynomial system. Kalbrener[11] also presented an algorithm to decompose a system of polynomials into a series of regular chains such that the variety defined by the system of polynomials is the union of the regular zeros of the regular chains. Lazard[12] introduced a normalized triangular set and gave a method to decompose a polynomial system into a series

Received August 4, 2006; accepted April 16, 2007; Published online July 31, 2007
DOI: 10.1007/s11425-007-0118-0

† Corresponding author

This work was partially supported by the National Key Basic Research Project of China (Grant No. 2004CB318000)

of normalized triangular sets uniquely. Maza and others[13,14] gave an efficient algorithm for solving zero-dimensional systems following Lazard's method. Szanto[15] also investigated the representation of algebraic sets by regular chains. Kandri and others[16,17] introduced the concept of invertibility for a polynomial with respect to an ascending set and gave an algorithm to decompose a polynomial system into a finite set of regular chains. In his algorithm, it is required to compute the Gröbner basis for lexical order and the cost of computation is expensive. In this paper, we will present an algorithm, which is different from the above algorithms, to decompose a polynomial system into a series of normal ascending sets which are particular regular chains. As a part of the algorithm, this algorithm can also be used to decompose a polynomial system into a series of regular chains.

After giving some preliminaries in Sec. 2, some properties of regular chains will be investigated in Sec. 3. We will give the main algorithm and prove the correctness and termination of the algorithm in Sec. 4. An example will be given to illustrate the algorithm in Sec. 5. Conclusions will be given in the final section.

2 Preliminaries

Let K be a field of characteristic zero, $K[x_1,\dots,x_n]$ be the polynomial ring with $x_1,\dots,x_n$ as indeterminates and the coefficients in K. Let E be an algebraically closed extension field of K. For a polynomial set $\mathcal{F}$, $\mathrm{Zero}(\mathcal{F})$ denotes the common zeros in E^n of the polynomials in $\mathcal{F}$. Let J be a polynomial, $\mathrm{Zero}(\mathcal{F}/J)$ be the common zeros in E^n of the polynomials in $\mathcal{F}$ which are not zeros of J. Given a variable ordering, for any nonzero polynomial P, the leading variable of P is denoted by $\mathrm{lv}(P)$, and the leading coefficient of P w.r.t. $\mathrm{lv}(P)$ is called the initial of P, denoted by $\mathrm{init}(P)$. The degree of P w.r.t. $\mathrm{lv}(P)$ is called the leading degree denoted by $\mathrm{ldeg}(P)$. We define the reductum of P as $\mathrm{red}(P) = P - \mathrm{init}(P)\mathrm{lv}(P)^{\mathrm{ldeg}(P)}$. For a polynomial P and a varaible x, the degree of P w.r.t. x will be denoted by $\deg(P,x)$, and the leading coefficient of P w.r.t. x will be denoted by $\mathrm{lc}(P,x)$. The psudoremainder of P divided by Q w.r.t. x will be denoted by $\mathrm{Prem}(P,Q,x)$. The Sylvester resultant of two polynomials P and Q w.r.t. x will be denoted by $\mathrm{Res}(P,Q,x)$.

Definition 2.1. *Let P be a polynomial, $\mathcal{A}: A_1,\dots,A_s$ be an ascending set. Let $R_s = P$, $R_{i-1} = \mathrm{Prem}(R_i, A_i, \mathrm{lv}(A_i))$ for $i = s,\dots,1$. $R = R_0$ is called the remainder of P w.r.t. $\mathcal{A}$, denoted by $\mathrm{Prem}(P,\mathcal{A})$. There are polynomials Q_i such that*

$$JP = \sum_{i=1}^{s} Q_i A_i + R, \tag{1}$$

where $J = I_1^{k_1}\cdots I_s^{k_s}$, each k_i is a nonnegative integer and I_i is the initial of A_i for $i = 1,\dots,s$.

Definition 2.2. *Let P be a polynomial, $\mathcal{A}: A_1,\dots,A_s$ be an ascending set. Let $R_s = P$, $R_{i-1} = \mathrm{Res}(R_i, A_i, \mathrm{lv}(A_i))$ for $i = s,\dots,1$. R_0 is called the resultant of P w.r.t. $\mathcal{A}$, denoted by $\mathrm{Res}(P,\mathcal{A})$. There are polynomials F, G_i for $i = 1,\dots,s$ such that*

$$FP + \sum_{i=1}^{s} G_i A_i = \mathrm{Res}(P,\mathcal{A}). \tag{2}$$

Definition 2.3. *Suppose $\mathcal{A}$ is an ascending set, let J be the product of the initials of the polynomials in $\mathcal{A}$, if $\xi \in \mathrm{Zero}(\mathcal{A}/J)$, then ξ is called a regular zero of $\mathcal{A}$.*

Definition 2.4. *Let $\mathcal{A}: A_1, \ldots, A_s$ be an ascending set, $x_{i_1}, \ldots, x_{i_s}$ be the leading variables of $A_1, \ldots, A_s$ and $x_{i_{s+1}}, \ldots, x_{i_n}$ be the other variables where $x_{i_1}, \ldots, x_{i_n}$ is a permutation of $x_1, \ldots, x_n$. A zero $(\xi_1, \ldots, \xi_n)$ of $\mathcal{A}$ is said to be regular generic if $\xi_{i_{s+1}}, \ldots, \xi_{i_n}$ are algebraically independent over K.*

In [6], a regular generic zero is called a regular zero. Here, to avoid confusion over the regular zero defined previously, we use the term regular generic zero. For an ascending set $\mathcal{A}$, the set of regular zeros or zeros of $\mathcal{A}$ may be empty. To avoid this case, Yang and Zhang introduced the concept of a regular ascending set or regular chain in [10].

Definition 2.5. Let $\mathcal{A}: A_1, \ldots, A_s$ *be an ascending set. Let* $\mathcal{A}_i = A_1, \ldots, A_i$ *for* $i = 1, \ldots s$. $\mathcal{A}$ *is a regular chain if s=1 or* $\mathrm{Res}(\mathrm{init}(A_i), \mathcal{A}_{i-1}) \neq 0$ *for* $i = 2, \ldots, s$.

From the above definitions, we know that the set of regular zeros of a regular chain is not empty and an irreducible ascending set is a regular chain.

Now we will give the definition of a normal ascending set.

Definition 2.6. *An ascending set $\mathcal{A}: A_1, \ldots, A_s$ is called a normal ascending set if s=1 or* $\deg(\mathrm{init}(A_i), \mathrm{lv}(A_j)) = 0$ *for* $1 \leqslant i < j \leqslant s$.

A normal ascending set is called a p-chain by Gao and Chou in [7]. Some properties for normal ascending sets have been discussed by Wang in [6].

From the above definition, we know that a normal ascending set is a regular chain.

Definition 2.7. *Let $\mathcal{A}: A_1, \ldots, A_s$ be an ascending set. The ideal generated by $\mathcal{A}$ is denoted by $(\mathcal{A})$. Let J be the product of the initials of the polynomials in $\mathcal{A}$, the saturation ideal of $\mathcal{A}$, denoted by $[\mathcal{A}]$, is defined as $[\mathcal{A}] = \{P | J^k P \in (\mathcal{A})$ for some integer $k \geqslant 0\}$.*

For the resultant of polynomials, in [18] Loos showed that

Lemma 2.8. *Let A, B and Q be polynomials and a_0 is the leading coefficient of A w.r.t. x_i,* $\deg(B, x_i) = m$, $\deg(AQ + B, x_i) = l$. *Then*

$$\mathrm{Res}(A, AQ + B, x_i) = a_0^{l-m} \mathrm{Res}(A, B, x_i),$$

$$\mathrm{Res}(A, BQ, x_i) = \mathrm{Res}(A, B, x_i)\mathrm{Res}(A, Q, x_i).$$

Lemma 2.9. *Let P_1, P_2 be two nonzero polynomials and have positive degrees in x_i. Suppose* $d_1 = \deg(P_1, x_i) \geqslant d_2 = \deg(P_1, x_i) > 0$. *Let* $P_3 = \mathrm{Prem}(P_1, P_2, x_i)$, *then*

$$\mathrm{Res}(P_1, P_2, x_i) | \mathrm{Res}(P_1, P_3, x_i).$$

Proof. Let $d_3 = \deg(P_3, x_i)$. Since P_3 is the pseudo-remainder of P_1 divided by P_2, then we have a polynomial Q such that $I_2^{d_1 - d_2 + 1} P_1 = QP_2 + P_3$. By lemma 2.8, we have

$$\mathrm{Res}(P_1, I_2^{d_1 - d_2 + 1} P_1 - P_3, x_i) = \mathrm{Res}(P_1, -P_3, x_i) = (-1)^{d_1} \mathrm{Res}(P_1, P_3, x_i),$$

and

$$\mathrm{Res}(P_1, QP_2, x_i) = \mathrm{Res}(P_1, Q, x_i)\mathrm{Res}(P_1, P_2, x_i),$$

then

$$(-1)^{d_1} \mathrm{Res}(P_1, P_3, x_i) = \mathrm{Res}(P_1, Q, x_i)\mathrm{Res}(P_1, P_2, x_i).$$

The lemma is proved.

From [19], we have

Lemma 2.10. *Let P, Q be two polynomials and have positive degree in x_i. Then*
(1) *There exist two polynomials A and B such that $AP + BQ = \mathrm{Res}(P, Q, x_i)$.*
(2) $\mathrm{Res}(P, Q, x_i) = 0$ *if and only if P and Q have a common factor which has positive degree in x_i.*

3 Properties of regular chains

Lemma 3.1. *For any regular chain $\mathcal{A}$ and polynomial P, then*

$$\mathrm{Res}(P, \mathcal{A}) \neq 0 \Leftrightarrow P(\xi) \neq 0 \ for\ any\ regular\ generic\ zero\ \xi\ of \mathcal{A}.$$

See [6] for the proof.

Corollary 3.2. Let $\mathcal{A}$ *be a regular chain, $P \in [\mathcal{A}]$, then for any regular generic zero ξ of $\mathcal{A}$, $P(\xi) = 0$.*

Proof. Suppose $\mathcal{A} : A_1, \ldots, A_s$ and $P \in [\mathcal{A}]$, then there are polynomials Q_i such that

$$J^k P = \sum_{i=1}^{s} Q_i A_i, \tag{3}$$

where k is a nonnegative integer and $J = I_1 \cdots I_s$, I_i is the initial of A_i. Let ξ be a regular generic zero of $\mathcal{A}$, then $A_i(\xi) = 0$ for $i = 1, \ldots, s$. By (3), $J^k(\xi)P(\xi) = 0$. $\mathrm{Res}(I_i, \mathcal{A}) \neq 0$ because $\mathcal{A}$ is a regular ascending set. By Lemma 2.8 and Lemma 3.1, we have $J(\xi) \neq 0$ and $P(\xi) = 0$.

From [14], we have the following lemma.

Lemma 3.3. *Let $\mathcal{A} \subset K[x_1, \ldots, x_n]$ be a regular chain, then $\{P \in K[x_1, \ldots, x_n] | \mathrm{Prem}(P, \mathcal{A}) = 0\}$ is the saturation ideal of $\mathcal{A}$.*

Lemma 3.4. *Let P be a polynomial, $\mathcal{A}$ be a regular chain. Let $R = \mathrm{Prem}(P, \mathcal{A})$, then $\mathrm{Res}(P, \mathcal{A}) = 0$ if and only if $\mathrm{Res}(R, \mathcal{A}) = 0$.*

Proof. It is easy to prove by Lemma 3.1.

Lemma 3.5. *Let $\mathcal{A} = A_1, \ldots, A_s$ be a regular chain. Let P, Q be two polynomials and $\mathrm{Res}(Q, \mathcal{A}) \neq 0$. Then $\mathrm{Prem}(P, \mathcal{A}) = 0$ if and only if $\mathrm{Prem}(QP, \mathcal{A}) = 0$.*

Proof. ($\Rightarrow$) Since $P \in [\mathcal{A}]$, we have $QP \in [\mathcal{A}]$. Then $\mathrm{Prem}(QP, \mathcal{A}) = 0$ by Lemma 3.3.

($\Leftarrow$) Let $R = \mathrm{Prem}(P, \mathcal{A})$, we have $JP = \sum_{i=1}^{s} Q_i A_i + R$, where $J = I_1^{k_1} \cdots I_s^{k_s}$, each k_i is a nonnegative integer and I_i is the initial of A_i.

From $\mathrm{Prem}(QP, \mathcal{A}) = 0$, we have $J'QP = \sum_{i=1}^{s} Q_i' A_i$, where $J' = I_1^{k_1'} \cdots I_s^{k_s'}$, each k_i' is a nonnegative integer and I_i is the initial of A_i. It is easy to check $J'QR \in (\mathcal{A})$. Let $R' = \mathrm{Res}(Q, \mathcal{A}) \neq 0$, we know there exist polynomials H and F_i for $i = 1, \ldots, s$ such that $HQ + \sum_{i=1}^{s} F_i A_i = R'$, $J'HQR \in (\mathcal{A})$, i.e. $J'(R' - \sum_{i=1}^{s} F_i A_i)R \in (\mathcal{A})$, then $J'R'R \in (\mathcal{A})$. By Lemma 3.3, the remainder of RR' w.r.t. $\mathcal{A}$ is 0. Since RR' is already reduced to $\mathcal{A}$, then $R = 0$. The lemma is proved.

Lemma 3.6. *Suppose P is a polynomial which has positive degree in x_i, $\mathcal{A} : A_1, \ldots, A_s$ to be a regular chain and $\deg(A_j, x_i) = 0$ for $j = 1, \ldots, s$. If $\mathrm{Res}(\mathrm{lc}(P, x_i), \mathcal{A}) \neq 0$, then $\mathrm{Prem}(P, \mathcal{A}) \neq 0$.*

Proof. Suppose $P = a_0 x_i^l + a_1 x_i^{l-1} + \cdots + a_l$, $\deg(P, x_i) = l$, $\mathrm{lc}(P, x_i) = a_0$. If $\mathrm{Prem}(P, \mathcal{A}) = 0$, then $a_0 \in [\mathcal{A}]$, then $\mathrm{Res}(a_0, \mathcal{A}) = 0$ by Lemma 3.1. This contradiction shows that $\mathrm{Prem}(P, \mathcal{A}) \neq 0$.

Lemma 3.7. *Let P_1, P_2 be two nonzero polynomials which have positive degrees in x_i, $\mathcal{A}$ be a regular chain and $\mathcal{A}$ doesn't involve x_i. $R = \mathrm{Prem}(P_2, \mathcal{A})$. If $\mathrm{Prem}(\mathrm{Res}(P_1, P_2, x_i), \mathcal{A}) = 0$ and $\mathrm{Res}(\mathrm{lc}(P_1, x_i), \mathcal{A}) \neq 0$ then $\mathrm{Prem}(\mathrm{Res}(P_1, R, x_i), \mathcal{A}) = 0$.*

Proof. Suppose $\mathcal{A} = A_1, \ldots, A_s$,

$$P_1 = a_0 x_i^l + a_1 x_i^{l-1} + \cdots + a_l, \quad \mathrm{lc}(P_1, x_i) = a_0, \quad P_2 = b_0 x_i^m + b_1 x_i^{m-1} + \cdots + b_m.$$

Let $R = c_0 x_i^m + c_1 x_i^{m-1} + \cdots + c_m$. Since $R = \mathrm{Prem}(P_2, \mathcal{A})$, there exist polynomials Q_i and J such that $JP_2 = \sum_{i-1}^{s} Q_i A_i + R$. c_i can be written as $c_i = Jb_i - d_i, d_i \in (\mathcal{A})$.

$$\mathrm{Res}(P_1\ , P_2, x_i)$$

$$= \begin{vmatrix}
a_0 & & & & b_0 & & & \\
a_1 & a_0 & & & b_1 & b_0 & & \\
 & a_1 & \ddots & & & b_1 & \ddots & \\
\vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\
 & \vdots & & a_1 & & \vdots & & b_1 \\
a_l & & & & b_m & & & \\
 & a_l & & \vdots & & b_m & & \vdots \\
 & & \ddots & & & & \vdots & \\
 & & & a_l & & & & b_m
\end{vmatrix}
= \frac{1}{J^l} \begin{vmatrix}
a_0 & & & & Jb_0 & & & \\
a_1 & a_0 & & & Jb_1 & Jb_0 & & \\
 & a_1 & \ddots & & & Jb_1 & \ddots & \\
\vdots & & \ddots & a_0 & \vdots & & \ddots & Jb_0 \\
 & \vdots & & a_1 & & \vdots & & Jb_1 \\
a_l & & & & Jb_m & & & \\
 & a_l & & \vdots & & Jb_m & & \vdots \\
 & & \ddots & & & & \vdots & \\
 & & & a_l & & & & Jb_m
\end{vmatrix}$$

$$= \frac{1}{J^l} \begin{vmatrix}
a_0 & & & & c_0 + d_0 & & & \\
a_1 & a_0 & & & c_1 + d_1 & c_0 + d_0 & & \\
 & a_1 & \ddots & & & c_1 + d_1 & \ddots & \\
\vdots & & \ddots & a_0 & \vdots & & \ddots & c_0 + d_0 \\
 & \vdots & & a_1 & & \vdots & & c_1 + d_1 \\
a_l & & & & c_m + d_m & & & \\
 & a_l & & \vdots & & c_m + d_m & & \vdots \\
 & & \ddots & & & & \vdots & \\
 & & & a_l & & & & c_m + d_m
\end{vmatrix}$$

Expanding the determinant by row, if $\deg(R, x_i) = k$, we know

$$\mathrm{Res}(P_1, P_2, x_i) = \frac{1}{J^l} a_0^{m-k} \mathrm{Res}(P_1, R, x_i) + d,$$

where $d \in (\mathcal{A})$, i.e. $J^l \mathrm{Res}(P_1, P_2, x_i) = a_0^{m-k} \mathrm{Res}(P_1, R, x_i) + J^l d$. Since $\mathrm{Res}(a_0, \mathcal{A}) \neq 0$, by Lemma 3.3 and Lemma 3.5, we have $\mathrm{Prem}(\mathrm{Res}(P_1, R, x_i), \mathcal{A}) = 0$.

4 Normal decomposition of a polynomial system

Lemma 4.1. *Let $\mathcal{A} = A_1, \ldots, A_s$ be an ascending set, and $\mathcal{A}_{s-1} = A_1, \ldots, A_{s-1}$ be a normal ascending set, I_s be the initial of A_s. If $\mathrm{Res}(I_s, \mathcal{A}_{s-1}) \neq 0$, then we can find a normal ascending set $\mathcal{A}'$ such that*

$$\mathrm{Zero}(\mathcal{A}'/J') \subset \mathrm{Zero}(\mathcal{A}/J) \subset \mathrm{Zero}(\mathcal{A}) \subset \mathrm{Zero}(\mathcal{A}'), \tag{4}$$

where J, J' are the product of the initials of polynomials in $\mathcal{A}$, $\mathcal{A}'$ respectively.

Proof. Let $R = \mathrm{Res}(I_s, \mathcal{A}_{s-1})$, there exist polynomials F,H_i, $i = 1, \dots, s$ such that

$$FI_s + \sum_{i=1}^{s-1} G_i A_i = R. \tag{5}$$

Set $y = lv(A_s)$, $d = \deg(A_s, y)$. Let

$$A'_s = F\ A_s + \left(\sum_{i=1}^{s-1} G_i A_i\right) y^d = F\ (I_s y^d + \mathrm{red}(A_s)) + \left(\sum_{i=1}^{s-1} G_i A_i\right) y^d = Ry^d + F\ \mathrm{red}(A_s). \tag{6}$$

The initial of A'_s is $R = \mathrm{Res}(I_s, \mathcal{A}_{s-1})$, A'_s and A_s have the same leading variable. Let $A''_s = \mathrm{Prem}(A'_s, \mathcal{A}_{s-1})$, from (1), we know that

$$I_1^{n_1} \cdots I_{s-1}^{n_{s-1}} A'_s = \sum_{i=1}^{s-1} P_i A_i + A''_s, \tag{7}$$

where I_i is the initial of A_i and n_i is a nonnegative integer for $i = 1, \dots, s-1$. The leading variable of A''_s is the same as the leading variable of A_s. The initial of A''_s is $I''_s = I_1^{n_1} \cdots I_{s-1}^{n_{s-1}} \mathrm{Res}(I_s, \mathcal{A}_{s-1})$. Now let $\mathcal{A}' = A_1, \dots, A_{s-1}, A''_s$, we will prove that $\mathcal{A}'$ satisfies the following relations:

$$\mathrm{Zero}(\mathcal{A}'/J') \subset \mathrm{Zero}(\mathcal{A}/J) \subset \mathrm{Zero}(\mathcal{A}) \subset \mathrm{Zero}(\mathcal{A}'),$$

where J, J' are the product of the initials of polynomials in $\mathcal{A}$, $\mathcal{A}'$ respectively.

(1) It is obvious $\mathrm{Zero}(\mathcal{A}/J) \subset \mathrm{Zero}(\mathcal{A})$.

(2) We will prove $\mathrm{Zero}(\mathcal{A}) \subset \mathrm{Zero}(\mathcal{A}')$.

For any ξ in $\mathrm{Zero}(\mathcal{A})$, then $A_i(\xi) = 0$ for $i = 1, \dots, s$, and from (6), it is easy to see that $A'_s(\xi) = 0$. From (7) we also know that $A''_s(\xi) = 0$. This shows that $\mathrm{Zero}(\mathcal{A}) \subset \mathrm{Zero}(\mathcal{A}')$.

(3) We will prove $\mathrm{Zero}(\mathcal{A}'/J') \subset \mathrm{Zero}(\mathcal{A}/J)$. J', J are the product of the initials of polynomials in $\mathcal{A}'$,$\mathcal{A}$ respectively.

For any ξ in $\mathrm{Zero}(\mathcal{A}'/J')$, i.e. $A_i(\xi) = 0$, $i = 1, \dots, s-1$: $A''_s(\xi) = 0$ and $I_i(\xi) \neq 0$ for $i = 1, \dots, s-1$, $I''_s(\xi) \neq 0$. Since $I''_s = I_1^{n_1} \cdots I_{s-1}^{n_{s-1}} \mathrm{Res}(I_s, \mathcal{A}_{s-1})$, then $\mathrm{Res}(I_s, \mathcal{A}_{s-1})(\xi) \neq 0$. From (5), we know that $I_s(\xi) \neq 0$ and $F(\xi) \neq 0$. From (6) and (7), $A_s(\xi) = 0$. This means $\xi \in \mathrm{Zero}(\mathcal{A}/J)$ so that we have $\mathrm{Zero}(\mathcal{A}'/J') \subset \mathrm{Zero}(\mathcal{A}/J)$.

Definition 4.2. *For an ascending set $\mathcal{A} = A_1, \dots, A_s$, let $\mathcal{A}'_1 = A_1$, $\mathcal{A}'_1$ is a normal ascending set. If for $i = 2, \dots, s$, $\mathrm{Res}(I_i, \mathcal{A}'_{i-1}) \neq 0$, from the above Lemma* 4.1*, we can get a normal ascending set $\mathcal{A}'_i$. Let $\mathcal{A}' = \mathcal{A}'_s$, $\mathcal{A}'$ is called the normalization of $\mathcal{A}$.*

From Lemma 4.1, we have

Corollary 4.3. *If $\mathcal{A}$ is a regular chain, let $\mathcal{A}'$ be the normalization of $\mathcal{A}$, then*

$$\mathrm{Zero}(\mathcal{A}'/J') \subset \mathrm{Zero}(\mathcal{A}/J) \subset \mathrm{Zero}(\mathcal{A}) \subset \mathrm{Zero}(\mathcal{A}'),$$

where J, J' are the product of the initials of polynomials in $\mathcal{A}$, $\mathcal{A}'$ respectively.

Theorem 4.4. *Suppose $\mathcal{A}$ is a regular chain, J is the product of the initials in $\mathcal{A}$ and P is a polynomial reduced to $\mathcal{A}$. If $\mathrm{Res}(P, \mathcal{A}) = 0$, then we can find two nonzero polynomials F and G which are reduced to $\mathcal{A}$ such that $\mathrm{Zero}(\mathcal{A}/J) = \mathrm{Zero}(\{\mathcal{A}, F\}/J) \cup \mathrm{Zero}(\{\mathcal{A}, G\}/J)$*

Proof. Let $\mathcal{A} = A_1, \ldots, A_s$, we will use induction on s, the number of polynomials in $\mathcal{A}$.

For $s = 1$, $\mathcal{A} = A_1$. P is reduced to A_1. From $\mathrm{Res}(P, \mathcal{A}) = 0$, $\mathrm{Res}(P, A_1, \mathrm{lv}(A_1)) = 0$. Hence P has positive degree in $\mathrm{lv}(A_1)$, from Lemma 2.10, P and A_1 have a common factor F, since P is reduced to A_1, then the degree of F w.r.t the variable $\mathrm{lv}(A_1)$ is less than $\mathrm{ldeg}(A_1)$, and A_1 has at least two factors F and G such that $A_1 = FG$ and F, G are reduced to A_1.

$$\mathrm{Zero}(\mathcal{A}/J) = \mathrm{Zero}(\mathcal{A}, F/J) \cup \mathrm{Zero}(\mathcal{A}, G/J).$$

This proves the case s=1.

Now assume that the theorem is true for $s < k$, we will prove the theorem is also true when $s = k$. In this case, $\mathcal{A} = A_1, \ldots, A_{k-1}, A_k$. Let $\mathcal{A}' = A_1, \ldots, A_{k-1}$. Let $y = lv(A_k)$, if $\deg(P, y) = 0$, the theorem is true by induction.

In the following, we will discuss the case that P has positive degree in y. Let $R = \mathrm{Res}(P, A_k)$. There are three cases: (1) $R = 0$. (2) $\mathrm{Prem}(R, \mathcal{A}') = 0$. (3) $\mathrm{Prem}(R, \mathcal{A}') \neq 0$. For case (1) and (3), the theorem is true by induction.

Now we will consider the case $\mathrm{Prem}(R, \mathcal{A}') = 0$. Let $P_1 = A_k$, $P_2 = P$, $I_1 = \mathrm{lc}(P_1, y)$, $I_2 = \mathrm{lc}(P_2, y)$;

Let $R_i = \mathrm{Prem}(P_1, P_{i-1}, y)$, $P_i = \mathrm{Prem}(R_i, \mathcal{A}')$, $I_i = \mathrm{lc}(P_i, y)$, $i = 3, 4, \ldots$. $\deg(P_1, y) > \deg(P_2, y) > \deg(P_3, y) > \cdots$.

By Lemma 2.9, we have $\mathrm{Prem}(\mathrm{Res}(P_1, R_i, y), \mathcal{A}') = 0$. Since $\mathcal{A}$ is a regular chain, $\mathrm{Res}(I_1, \mathcal{A}') \neq 0$, by Lemma 3.7, we have

$$\mathrm{Prem}(\mathrm{Res}(P_1, P_i, y), \mathcal{A}') = 0. \tag{8}$$

Let j be the smallest i such that $P_i = 0$ or $P_i \neq 0$, $\deg(P_i, y) = 0$.

$$I_{j-1} P_1 = Q_{j-1} P_{j-1} + R_j. \tag{9}$$

Let $F = P_{j-1} \neq 0$, $G = \mathrm{Prem}(Q_{j-1}, \mathcal{A}')$. F and G are reduced to $\mathcal{A}'$, so they are reduced to $\mathcal{A}$. If $\mathrm{Res}(I_{j-1}, \mathcal{A}') = 0$, the theorem is true by induction.

Now assuming $\mathrm{Res}(I_{j-1}, \mathcal{A}') \neq 0$, we will prove $G \neq 0$ for the cases (i) $P_i = 0$ (ii) $P_i \neq 0$, $\deg(P_i, y) = 0$.

(i) $P_j = 0$, i.e. $\mathrm{Prem}(R_j, \mathcal{A}') = 0$. By the assumption, $\mathrm{Res}(I_{j-1}, \mathcal{A}') \neq 0$, by Lemma 3.3 and Lemma 3.6, from (9) we know that $G \neq 0$.

(ii) $P_j \neq 0$ and $\deg(P_j, y) = 0$. If $G = 0$, then $\mathrm{Prem}(Q_{j-1}, \mathcal{A}') = 0$. From (8), by Lemma 3.3, for a positive integer m, we have $\mathrm{Prem}(R_j^m, \mathcal{A}') = 0$. i.e. $\mathrm{Prem}((I_{j-1}P_1 - Q_{j-1}P_{j-1})^m, \mathcal{A}') = 0$. By Lemma 3.3, $\mathrm{Prem}((I_{j-1}P_1)^m, \mathcal{A}') = 0$. Since $\mathrm{Res}(I_{j-1}, \mathcal{A}') \neq 0$ and $\mathrm{Res}(I_1, \mathcal{A}') \neq 0$, then $\mathrm{Res}(\mathrm{lc}((I_{j-1}P_1)^m), \mathcal{A}') = \mathrm{Res}((I_{j-1}I_1)^m, \mathcal{A}') \neq 0$. By Lemma 3.6, $\mathrm{Prem}((I_{j-1}P_1)^m, \mathcal{A}') \neq 0$. This contradiction shows that $G \neq 0$.

For both (i) and (ii), it is easy to check $\mathrm{Zero}(\mathcal{A}/J) = \mathrm{Zero}(\{\mathcal{A}, F\}/J) \cup \mathrm{Zero}(\{\mathcal{A}, G\}/J)$. The theorem is proved.

Based on the above theorem, we have the following algorithm.

```
Algorithm: Dec
  Input  : $P$ is a nonzero polynomial
           $\mathcal{A} = A_1, \ldots, A_s$ is a normal ascending set.
           $P$ is reduced to $\mathcal{A}$ and $\mathrm{Res}(P, \mathcal{A}) = 0$
  Output: $F, G$ are nonzero polynomials and reduced to $\mathcal{A}$ such that
           $\mathrm{Zero}(\mathcal{A}/J) = \mathrm{Zero}(\{\mathcal{A}, F\}/J) \cup \mathrm{Zero}(\{\mathcal{A}, G\}/J)$.
 if $s = 1$ then  $F \leftarrow$ the greatest common divisor of $P$ and $A_1$; $G \leftarrow A_1/F$
 return $\{F, G\}$
  $y \leftarrow \mathrm{lv}(A_s)$
  $\mathcal{A}' \leftarrow A_1, \ldots, A_{s-1}$
  if $\deg(P, y) = 0$ then  return $\mathrm{Dec}(P, \mathcal{A}')$
  $P_1 \leftarrow A_s$
  $P_2 \leftarrow P$
     repeat
   $P_3 \leftarrow \mathrm{Prem}(P_1, P_2, y)$
     if  $\deg(P_3, y) = 0$ or $\mathrm{Prem}(P_3, \mathcal{A}') = 0$ then
      $F \leftarrow P_2$
        $Q \leftarrow$ the psudo-quotient of $P_1$ divided by $F$
        $G \leftarrow \mathrm{Prem}(Q, \mathcal{A}')$
      return $\{F, G\}$
   end
     $P_2 \leftarrow \mathrm{Prem}(P_3, \mathcal{A}')$
     $I \leftarrow \mathrm{lc}(P_2, y)$
until $\mathrm{Res}(I, \mathcal{A}') = 0$ ;
  return $\mathrm{Dec}(I, \mathcal{A}')$
```

Theorem 4.5. *For a polynomial system $\mathcal{F}$, there is an algorithm which permits the computation of a series of normal ascending sets $\mathcal{A}_i$ in finite steps such that $\mathrm{Zero}(\mathcal{F}) = \bigcup_i \mathrm{Zero}(\mathcal{A}_i/J_i)$, where J_i is the product of the initials of the polynomials in $\mathcal{A}_i$.*

Proof. Now we will prove the correctness of algorithm ND.

Let $\mathcal{A}$ be the characteristic set of $\mathcal{F}$, $\mathcal{A} = A_1, \ldots, A_s$, then $\mathrm{Zero}(\mathcal{A}/J) \subset \mathrm{Zero}(\mathcal{F}) \subset \mathrm{Zero}(\mathcal{A})$ where J is the product of the initials of the polynomials in $\mathcal{A}$.

First, for $s = 1$, the proof is obvious. Second, there is a positive integer i such that $\mathrm{Res}(I_i, \mathcal{A}') = 0$, from theorem 4.4, there are nonzero polynomials F, G such that $\mathrm{Zero}(\mathcal{A}'/J') = \mathrm{Zero}(\{\mathcal{A}', F\}/J') \cup \mathrm{Zero}(\{\mathcal{A}', G\}/J')$. Since $\mathrm{Zero}(\mathcal{F}) \subset \mathrm{Zero}(\mathcal{A}) \subset \mathrm{Zero}(\mathcal{A}')$,

$$\begin{aligned}\mathrm{Zero}(\mathcal{F}) &= \mathrm{Zero}(\{\mathcal{F}, \mathcal{A}'\}/J') \cup \mathrm{Zero}(\{\mathcal{F}, \mathcal{A}', J'\}) \\ &= \mathrm{Zero}(\{\mathcal{F}, \mathcal{A}', F\}/J') \cup \mathrm{Zero}(\{\mathcal{F}, \mathcal{A}', G\}/J') \cup \bigcup_{j=1}^{i-1} \mathrm{Zero}(\{\mathcal{F}, \mathcal{A}', I_i'\})\end{aligned}$$

where I_i' is the initial of A_i' in $\mathcal{A}'$. Third, $\mathcal{A}'$ is the normalization of $\mathcal{A}$, from Corollary 4.3, we know that $\mathrm{Zero}(\mathcal{A}'/J') \subset \mathrm{Zero}(\mathcal{A}/J)$, then $\mathrm{Zero}(\mathcal{F}) = \mathrm{Zero}(\mathcal{A}'/J') \cup \bigcup_{j=1}^{s} \mathrm{Zero}(\{\mathcal{F}, \mathcal{A}', I_i'\})$ where I_i' is the initial of A_i' in $\mathcal{A}'$.

In the following, we will prove the termination of algorithm ND.

Each I_i', which is the initial of A_i', is reduced to $\mathcal{A}'$, and nonzero polynomials F, G are also reduced to $\mathcal{A}'$. This shows that the algorithm will terminate.

Algorithm: ND

```
Input   : $\mathcal{F}$ is a polynomial set
Output: $\mathcal{A}_i$ is a series of normal ascending sets such that
            $\mathrm{Zero}(\mathcal{F}) = \bigcup_i \mathrm{Zero}(\mathcal{A}_i/J_i)$
            $J_i$ is the product of the initials of the polynomials in $\mathcal{A}_i$
$\mathcal{A} \leftarrow$ the characteristic set of $\mathcal{F}$ # Suppose $\mathcal{A} = A_1, \ldots, A_s$;
$\mathcal{A}' \leftarrow A_1$
$i \leftarrow 2$
if $s = 1$ then
    $I_1 \leftarrow \mathrm{init}(A_1)$
    return $\mathcal{A}' \cup ND(\{\mathcal{F}, \mathcal{A}, I_1\})$
end
while $i < s$ do
    if $\mathrm{Res}(I_i, \mathcal{A}') = 0$ then
        $\{F, G\} \leftarrow Dec(I_i, \mathcal{A}')$
        for $j$=1 to $i$-1 do $I_j \leftarrow \mathrm{init}(A'_j)$
        return ( $\bigcup_{j=1}^{i-1} ND(\{\mathcal{F}, \mathcal{A}, \mathcal{A}', I_i\})) \cup ND(\{\mathcal{F}, \mathcal{A}, \mathcal{A}', F\}) \cup ND(\{\mathcal{F}, \mathcal{A}, \mathcal{A}', G\})$
    else
        $\mathcal{A}' \leftarrow \mathcal{A}', A_i$
        $\mathcal{A}' \leftarrow$  the normalization of $\mathcal{A}'$ # For regular decomposition, omit this line.
    end
end
# Suppose $A' = A'_1, \ldots, A'_s$;
for $j$=1 to $s$ do $I_j \leftarrow \mathrm{init}(A'_j)$
return $\mathcal{A}' \cup \bigcup_{j=1}^{s} ND(\{\mathcal{F}, \mathcal{A}, \mathcal{A}', I_j\}$
```

This algorithm can also be used to decompose a polynomial system into a finite set of regular ascending sets.

5 Example

Example 5.1. *Compute the normal decomposition of the polynomial system* $\mathcal{F} = \{x^2 + x + 1, y^2 + y + 1, (xy + x + 1)z^2 + z - 1\}$.

We will give the normal decomposition for the variable ordering $x < y < z$. Let $\mathcal{A} = A_1, A_2, A_3$. $A_1 = x^2 + x + 1, A_2 = y^2 + y + 1, A_3 = (xy + x + 1)z^2 + z - 1$. It is already an ascending set, and is itself the characteristic set. $\mathcal{A}' = A_1, A_2$ is a normal ascending set. The initial of A_3 is $I_3 = xy + x + 1$. $\mathrm{Res}(I_3, \mathcal{A}') = \mathrm{Res}(\mathrm{Res}(I_3, A_2, y), A_1, x) = \mathrm{Res}(x^2 + x + 1, x^2 + x + 1, x) = 0$. In fact, $\mathrm{Prem}(\mathrm{Res}(I_3, A_2, y), A_1) = 0$. Let $P_1 = A_2$, $P_2 = I_3$, $\mathcal{A}'' = A_1$. Let $P_3 = \mathrm{Prem}(P_1, P_2, y) = x^2 + x + 1$. We have $\mathrm{Prem}(P_3, \mathcal{A}'') = 0$

$$x^2(y^2 + y + 1) = (xy - 1)I_3 + r, r = x^2 + x + 1.$$

Let $F = I_3 = xy + x + 1$, $G = xy - 1$. We have

$$\mathrm{Zero}(\mathcal{A}') = \mathrm{Zero}(\mathcal{A}', F) \cup \mathrm{Zero}(\mathcal{A}', G), \quad \mathrm{Zero}(\mathcal{F}) = \mathrm{Zero}(\mathcal{A}) = \mathrm{Zero}(\mathcal{A}, F) \cup \mathrm{Zero}(\mathcal{A}, G).$$

The characteristic set of $\{\mathcal{A}, F\}$ is $\mathcal{A}_1 = x^2+x+1, x+1+y, -3z^2+(x-1)z-x+1$. The characteristic set of $\{\mathcal{A}, G\}$ is $\mathcal{A}_2 = x^2+x+1, y-x, z-1$. Since the initials of $\mathcal{A}_1$ and $\mathcal{A}_2$ are integers, we have $\text{Zero}(\mathcal{F}) = \text{Zero}(\mathcal{A}_1) \cup \text{Zero}(\mathcal{A}_2)$ where $\mathcal{A}_1$ and $\mathcal{A}_2$ are normal ascending sets.

6 Conclusions

In this paper, we present an algorithm to decompose a polynomial system into a series of normal ascending sets such that the zeros of the polynomial system are the union of the regular zeros of the normal ascending set. In fact, this algorithm can also be used to decompose the polynomial system into a series of regular chains. If the system is zero dimensional, then the zeros of the polynomial system are the union of the zeros of the normal ascending sets where the initials are constants.

Acknowledgements We thank L. H. Zhi and Z. M. Li for helpful discussions. We also cordially thank two anonymous referees for their valuable comments which led to the improvement of this paper.

References

[1] Ritt J F. Differential Algebra. New York: American Mathematical Society, 1950

[2] Wu W T. Basic principles of mechanical theorem proving in elementary geometries. *J Sys Sci & Math Sci*, **4**: 20–235 (1984)

[3] Chou S C, Mechanical Geometry Theorem-proving, Dordrecht: D. Reidel Pub. Company, 1988

[4] Gao X S, Chou S C. The dimension of ascending chains. *Chin Sci Bull*, **38**(5): 396–399 (1993)

[5] Gao X S, Chou S C. Ritt-Wu's decomposition algorithm and geometry theorem proving. In: Proceedings of CADE-10, Lecture Notes in Artificial Intelligence. **449**: 207–220 (1990)

[6] Wang D M. Elimination Method. Wien-New York: Springer-Verlag, 2001

[7] Gao X S, Chou S C. Solving parametric algebraic systems. In: Proceedings of ISSAC'92, 1992, 335–341

[8] Trager B M. Algebraic factoring and rational function integration. In: Proceedings of ACM SYMSAC, 1976, 219–226

[9] Yuan C M. Trager's factorization algorithm over successive extension field. *J Sys Sci & Math Scis*, **26**(5): 53–40 (2006)

[10] Yang L, Zhang J Z. Searching dependency between algebraic equations: An algorithm applied to automated reasoning. In: Johnson J, McKee S,Vella A, eds. Artificial Intelligence in Mathematics. Oxford: Oxford University Press, 1994, 147–156

[11] Kalbrener M. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *J Sym Comput*, **15**: 143–167 (1993)

[12] Lazard D. A new method for solving algebraic systems of positive dimension. *Discrete Appl Math*, **33**: 147–160 (1991)

[13] Maza M M. On triangular decompositions of algebraic varieties. Technical Report TR 4/99, NAG Ltd, Oxford, UK, 1999

[14] Aubry P, Lazard D, Maza M M. On the theories of triangular sets. *J Sym Comput*, **28**: 105–124 (1999)

[15] Szanto A. Computation with polynomial systems. Dissertation for the Doctoral Degree. Cornell: Cornell University, 1999

[16] Kandri R A, Maarouf H, Ssafini M. Triviality and dimension of a system of algebraic differential equations. *J Aut Rea*, **20**: 365–385 (1998)

[17] Bouziane D, Kandri R A, Maarouf H. Unmixed-dimensional decomposition of a finitely generated perfect differential ideal. *J Sym Comput*, **31**: 631–649 (2001)

[18] Loos R. Computing in algebraic extensions. In: Buchberger B, Collins G E, Loos R, eds. Computer Algebra: Symbolic and Algebraic Computation. 2nd ed. Wien-New York: Springer-Verlag, 1983, 173–188

[19] Cox D, Little J, Shea D O'. Ideals, Varieties, and Algorithms. 2nd ed. New York: Springer-Verlag, 1997, 149–159