MM Research Preprints, 77–92
KLMM, AMSS, Academia Sinica
Vol. 26, January 2008

A Characteristic Set Method for Equation Solving in Finite Fields[1]

Xiao-Shan Gao and Zhenyu Huang
Key Laboratory of Mathematics Mechanization
Institute of Systems Science, AMSS, Academia Sinica
Beijing, 100080, China

Abstract. In this paper, we present a characteristic set method to solve polynomial equation systems in finite fields. Due to the special property of finite fields, the given characteristic set methods are much more efficient and have better properties than the general characteristic set method.

Keywords. Characteristic set method, polynomial equation system, finite field.

1. Introduction

The characteristic set (CS) method is a tool for studying systems of polynomial or algebraic differential equations [2, 3]. The idea of the method is reducing equation systems in general form to equation systems in a special "triangular form", also called ascending chains. The zero-set of any finitely generated polynomial or algebraic differential polynomial systems of equations may be decomposed into the union of the zero-sets of ascending chains. With this method, solving an equation system can be reduced to solving univariate equations. We can also use the method to determine the dimension, the degree, and the order for a finitely generated polynomial or differential polynomial systems, to solve the radical ideal membership problem, and to prove theorems from elementary and differential geometries.

CS methods always consider the zeros of polynomial equations in an algebraically closed field which is an infinite field. In [1], the CS method was extended to solving equations in the finite field $\mathbb{F}_2$. In this paper, we will extend the CS method to solve equations in any finite field $\mathbb{F}_q$. More precisely, we consider polynomials in the ring

$$\mathbb{R}_q = \mathbb{F}_q[x_1, \dots, x_n]/(\mathbb{H})$$

where $\mathbb{H} = \{x_1^q - x_1, \dots, x_n^q - x_n\}$.

Due to the special property of $\mathbb{R}_q$, the proposed CS methods are much more efficient and have better properties than the general CS method. We could decompose the zero set of a polynomial equation system in $\mathbb{R}_q$ as the disjoint union of the zero sets of monic proper ascending chains. As a consequence, we could give an explicit formula for the number of solutions of the equation system.

The rest of this paper is organized as follows. In Section 2, we introduce the notations and give some preliminary results. In Section 3, we present the CS methods. In Section 4, we present a direct algorithm to decompose the zero set of a polynomial system into the zero sets of monic proper ascending chains.

[1] Partially supported by a National Key Basic Research Project of China (2004CB318000).

2. Notations and Preliminary Results

Let p be a prime number and $q = p^k$ for a non-negative integer k. $\mathbb{F}_q$ denotes the finite field of q elements. We will consider the problem of solving algebraic equations over $\mathbb{F}_q$. Let $\mathbb{X} = \{x_1, \ldots, x_n\}$ be a set of indeterminants. Since we only consider solutions in $\mathbb{F}_q$, we work in the ring

$$\mathbb{R}_q = \mathbb{F}_q[\mathbb{X}]/(\mathbb{H})$$

where

$$\mathbb{H} = \{x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n\}. \tag{1}$$

It is easy to see that $\mathbb{R}_q$ is not an integral domain. For any $\alpha \in \mathbb{F}_q$, $x_i - \alpha$ is a zero divisor of $\mathbb{R}_q$. An element P in $\mathbb{R}_q$ has the following *canonical representation*:

$$P = \alpha_s M_s + \cdots + \alpha_0 M_0, \quad \alpha_i \in \mathbb{F}_q, \tag{2}$$

where M_i is a monomial and $\deg(M_i, x_j) \leq q - 1$ for any j .

To obtain such a canonical representation for a $P \in \mathbb{F}_q[\mathbb{X}]$, we will replace x_i^q by x_i. For instance, in the field $\mathbb{F}_3 = \{0, 1, 2\}$, $x_1x_2^3 + x_1x_2 + x_3$ can be represented as $2x_1x_2 + x_3$. We still call an element in $\mathbb{R}_q$ a polynomial.

Let $\mathbb{P}$ be a set of polynomials in $\mathbb{R}_q$. We use $\overline{\text{Zero}}(\mathbb{P})$ to denote the common zeros of the polynomials in $\mathbb{P}$ in the affine space $\mathbb{F}_q^n$, that is,

$$\overline{\text{Zero}}(\mathbb{P}) = \{(a_1, \ldots, a_n), a_i \in \mathbb{F}_q, s.t. \forall P \in \mathbb{P}, P(a_1, \ldots, a_n) = 0\}.$$

Let D be a polynomial in $\mathbb{R}_q$. We define a *quasi variety* to be

$$\overline{\text{Zero}}(\mathbb{P}/D) = \overline{\text{Zero}}(\mathbb{P}) \setminus \overline{\text{Zero}}(D).$$

Let $\mathbb{P}$ be a set of polynomials in $\mathbb{F}_q[\mathbb{X}]$. Denote the zeros of $\mathbb{P}$ in an algebraically closed extension of $\mathbb{F}_q$ as $\text{Zero}(\mathbb{P})$. We use $\overline{\mathbb{P}}$ to denote the image of $\mathbb{P}$ under the natural ring homomorphism:

$$\mathbb{F}_q[\mathbb{X}] \Rightarrow \mathbb{R}_q.$$

Lemma 2.1 *Use the notations just introduced. We have* $\text{Zero}(\mathbb{P} \cup \mathbb{H}) = \overline{\text{Zero}}(\overline{\mathbb{P}})$*, where* $\mathbb{H}$ *is defined in (1).*

Proof: Let $P \in \mathbb{P}$. By the definition, we have $P = \overline{P} + \sum_i B_i(x_i^q - x_i)$, where B_i are some polynomials. Note that any zero in $\overline{\text{Zero}}(\overline{\mathbb{P}})$ is also a zero of $x_i^q - x_i$. Then the formula to be proved is a direct consequence of the above relation between P and $\overline{P}$. □

From Lemma 2.1, to solve a set of equations over $\mathbb{F}_q$, we need only consider polynomials in $\mathbb{R}_q$. In the rest of this paper, when we say polynomials , we mean an element of $\mathbb{R}_q$ with the canonical representation (2). We will give some preliminary results about the polynomials in $\mathbb{R}_q$. Most of the them are similar to those in $\mathbb{R}_2$ [1].

Lemma 2.2 *Let P be a polynomial in $\mathbb{R}_q$. We have $P^q = P$.*

Proof: Since $x_i^q = x_i$, for any monomial m in $\mathbb{R}_q$ we have $m^q = m$. Let $P = \sum_i \alpha_i m_i$ where m_i are monomials and $\alpha_i \in \mathbb{F}_q$. Then $P^q = (\sum_i \alpha_i m_i)^q = \sum_i \alpha_i^q m_i^q = \sum_i \alpha_i m_i = P$.
□

Lemma 2.3 *Let* I *be a polynomial ideal in* $\mathbb{R}_q$*. Then* I *is a radical ideal.*

Proof: For any $f^s \in$ I with s an integer, there exists an integer k such that $q + k(q-1) \geq s$. Then $f^s f^{q+k(q-1)-s} = f^{q+k(q-1)} \in I$. $f^{q+k(q-1)} = f^q f^{k(q-1)} = f^{k(q-1)+1} = f^{q+(k-1)(q-1)} = \cdots = f^q = f$. Thus, we have $f \in I$, which implies that I is a radical ideal. □

Lemma 2.4 *Let* I *be a polynomial ideal in* $\mathbb{R}_q$*.*

(1) $\mathrm{I} = (x_0 + a_0, \ldots, x_n + a_n)$ *if and only if* $(a_0, \ldots, a_n)$ *is the only solution of* I.

(2) $\mathrm{I} = (1)$ *if any only* I *has no solutions.*

Proof: If $\mathrm{I} = (x_0 + a_0, \ldots, x_n + a_n)$, it is easy to see that $(a_0, \ldots, a_n)$ is the only solution of I. Conversely, let $(a_0, \ldots, a_n)$ be the only solution of I. By Lemma 2.1, we have $x_i + a_i = 0$ on Zero($\mathrm{I} \cup \mathbb{H}$) in $\mathbb{F}_q[\mathbb{X}]$, where $\mathbb{H}$ is defined in (1). By Hilbert's Nullstellensatz, there is an integer s such that $(x_i + a_i)^s$ is in the ideal generated by $\mathrm{I} \cup \mathbb{H}$ in $\mathbb{F}_q[\mathbb{X}]$. Considering R_q, it means that $(x_i + a_i)^s$ is in I. By Lemma 2.3, I is a radical ideal in $\mathbb{R}_q$. Thus, $x_i + a_i$ is in I. This prove (1). For (2), if I has no solution, we have Zero($\mathrm{I} \cup \mathbb{H}$) = $\emptyset$. By Hilbert's Nullstellensatz, $1 \in (\mathrm{I} \cup \mathbb{H})$. That is, $1 \in$ I. □

Lemma 2.5 *Let* $P \in \mathbb{R}_q$*.* $\overline{\mathrm{Zero}}(P) = \mathbb{F}_q^n$ *iff* $P \equiv 0$*.* $\overline{\mathrm{Zero}}(P) = \emptyset$ *iff* $P^{q-1} - 1 \equiv 0$*.*

Proof: If $P \equiv 0$, $\overline{\mathrm{Zero}}(P) = \mathbb{F}_q^n$ is obvious. Conversely, we prove the result by induction on n. If $n = 1$, we consider the one-variable polynomial $P(x) \in \mathbb{R}_q$. Suppose that $P(x) \neq 0$. Since $\deg(P, x) \leq q - 1$, P has at most $q - 1$ solutions in F_q. Thus, for $n = 1$ we have the result. Now assume the result has been proved for $n = k$. For $n = k + 1$, we have $P(x_1, \ldots, x_n) = f_0 x_n^{q-1} + f_1 x_n^{q-2} + \cdots + f_{q-1}$, where f_i is a k-variable polynomial. By the induction hypothesis, if some f_i is not 0, there exists a element $(a_1, a_2, \ldots, a_k)$ in $\mathbb{F}_q^k$ such that $f_i(a_1, \ldots, a_k) \neq 0$. Then $P(a_1, \ldots, a_k)$ is a nonzero polynomial whose degree of x_{k+1} is less than q. Supposing a_{k+1} is not the solution of $P(a_1, \ldots, a_k)$, we have $(a_1, \ldots, a_{k+1})$ is not the solution of P, a contradiction. Thus, we have $f_i = 0$ for all i. It means that $P \equiv 0$, and the first result is proved.

If $\overline{\mathrm{Zero}}(P) = \emptyset$, then $P \neq 0$ for any element in $\mathbb{F}_q^n$, which implies that $P^{q-1} - 1 = 0$ for any element. Then $P^{q-1} - 1 \equiv 0$. Conversely, if there is a element $(a_1, \ldots, a_n) \in \mathbb{F}_q^n$ such that $P(a_1, \ldots, a_n) = 0$, $P^{q-1} - 1 \neq 0$ for the element, a contradiction. Thus, $\overline{\mathrm{Zero}}(P) = \emptyset$. □

As a consequence of Lemma 2.5, we have

Corollary 2.6 *Let* $q = 2$ *and* $P \in \mathbb{R}_2 \setminus \mathbb{F}_2$*. Then* $\overline{\mathrm{Zero}}(P) \neq \emptyset$*.*

But when $q > 2$, the corollary is not right. For example, considering $\mathbb{F}_3$, it is easy to see that $\overline{\mathrm{Zero}}(x^2 + 1) = \emptyset$.

Lemma 2.7 *Let U, V, and D be polynomials in $\mathbb{R}_q$. We have*

$$(U^{q-1}V^{q-1} - 1) = (U^{q-1} - 1, V^{q-1} - 1). \tag{3}$$

$$(U^{q-1}V^{q-1} - U^{q-1} - V^{q-1}) = (U, V). \tag{4}$$

$$\overline{\mathrm{Zero}}(UV) = \overline{\mathrm{Zero}}(U) \cup \overline{\mathrm{Zero}}(V). \tag{5}$$

$$\overline{\mathrm{Zero}}(\emptyset/D) = \overline{\mathrm{Zero}}(D^{q-1} - 1). \tag{6}$$

$$\overline{\mathrm{Zero}}(\mathbb{P}) = \overline{\mathrm{Zero}}(\mathbb{P} \cup \{U\}) \cup \overline{\mathrm{Zero}}(\mathbb{P} \cup \{U^{q-1} - 1\}). \tag{7}$$

Proof: We have

$$\begin{aligned}(U^{q-1}V^{q-1} - 1) &= (U^{q-1}V^{q-1} - 1, U^{q-1}(U^{q-1}V^{q-1} - 1)) \\ &= (U^{q-1}V^{q-1} - 1, U^{q-1}V^{q-1} - U^{q-1}) \\ &= (U^{q-1}V^{q-1} - 1, U^{q-1} - 1) = (U^{q-1} - 1, V^{q-1} - 1).\end{aligned}$$

This proves (3). Equation (4) can be proved similarly:

$$\begin{aligned}(U^{q-1}V^{q-1} - U^{q-1} - V^{q-1}) &= (U^{q-1}V^{q-1} - U^{q-1} - V^{q-1}, U(U^{q-1}V^{q-1} - U^{q-1} - V^{q-1})) \\ &= (U^{q-1}V^{q-1} - U^{q-1} - V^{q-1}, U) = (U, V).\end{aligned}$$

Since $\mathbb{F}_q$ is a field, (5) is obvious. For any element $\alpha \in \mathbb{F}_q^n$, $D(\alpha) \neq 0$ means that $D^{q-1}(\alpha) - 1 = 0$. Conversely, for any element $\alpha \in \mathbb{F}_q^n$, if $D(\alpha) = 0$, we have $D^{q-1}(\alpha) - 1 \neq 0$, a contradiction. This proves (6). Since $U(U^{q-1} - 1) \equiv 0$, (7) is a consequence of (5). □

3. A Characteristic Set Method in $\mathbb{R}_q$

The general CS methods are for infinite fields and do not take into account of the special property of finite fields. In [1], the CS method was extended to solving equations in the finite field $\mathbb{F}_2$. We will show that most of the properties of the the CS method given in [1] can be extended to CS methods in $\mathbb{R}_q$.

3.1. Triangular Sets

Let $P \in \mathbb{R}_q$. The *class* of P, denoted by class(P), is the largest c such that x_c occurs in P. Then x_c is called the leading variable of P, denoted as lvar(P). If $P \in \mathbb{F}_q$, we set class$(P) = 0$. If class$(P) = c$, let us regard P as a univariate polynomial in x_c. We call $\deg(P, x_c)$ the *degree* of P, denoted as $\deg(P)$. The coefficient of P w.r.t x_c^d is called the *initial* of P, and is denoted by init(P). Then P can be represented uniquely as the following form:

$$P = Ix_c^d + U \tag{8}$$

where $I = \mathrm{init}(P)$, and either $U = 0$ or U is a polynomial with $\deg(U, x_c) < d$. A polynomial P_1 has *higher ordering* than a polynomial P_2, denoted as $P_2 \prec P_1$, if class$(P_1) >$ class(P_2) or class$(P_1) =$ class(P_2) and $\deg(P_1) > \deg(P_2)$. If neither $P_1 \prec P_2$ nor $P_2 \prec P_1$, they are said to have the same ordering, denoted as $P_1 \sim P_2$. It is easy to see that $\prec$ is a partial order on the polynomials in $\mathbb{R}_q$.

A sequence of nonzero polynomials

$$\mathcal{A}: \quad A_1, A_2, \ldots, A_r \tag{9}$$

is a *triangular set* if either $r = 1$ and $A_1 \neq 0$ or $0 < \text{class}(A_1) < \cdots < \text{class}(A_r)$. A *trivial* triangulated set is a polynomial set consisting of a nonzero element in $\mathbb{F}_q$. For a triangular set $\mathcal{A}$, we denote $\mathbf{I}_{\mathcal{A}}$ as the product of the initials of the polynomials in $\mathcal{A}$.

Let $\mathcal{A}'$: $A'_1, A'_2, \ldots, A'_{r'}$ and $\mathcal{A}''$: $A''_1, A''_2, \ldots, A''_{r''}$ be two triangular sets. $\mathcal{A}'$ is said to be of *lower ordering* than $\mathcal{A}''$, denoted as $\mathcal{A}' \prec \mathcal{A}''$, if either there is some k such that $A'_1 \sim A''_1, \ldots, A'_{k-1} \sim A''_{k-1}$, while $A'_k \prec A''_k$; or $r' > r''$ and $A'_1 \sim A''_1, \ldots, A'_{r''} \sim A''_{r''}$. We have the following basic property for triangular sets.

Lemma 3.1 *A sequence of triangular sets steadily lower in ordering is finite. More precisely, let $\mathcal{A}_1 \succ \mathcal{A}_2 \succ \cdots \succ \mathcal{A}_m$ be a strictly decreasing sequence of triangular sets in $\mathbb{R}_q$. Then $m \leq q^n$.*

Proof: Let P be a polynomial in $\mathbb{R}_q$. If $\text{class}(P) = c$ and $\deg(P) = d$, P and x_c^d have the same ordering. Since we only consider the ordering of the triangular sets, we may assume that the triangular sets consist of powers of variables. In this case, two distinct triangular sets can not have the same ordering. To get a triangular set of this kind, we can choose one polynomial from $\{\emptyset, x_i, x_i^2, \ldots, x_i^{q-1}\}$, and set it as the ith polynomial of the triangular set. Thus, there are $q^n - 1$ nontrivial triangular sets consist of powers of variables. Adding the trivial triangular set consist of 1, we have a sequence of triangular sets $\mathcal{C}_1 \succ \mathcal{C}_2 \succ \cdots \succ \mathcal{C}_{q^n}$. Let $\mathcal{A}_1 \succ \mathcal{A}_2 \succ \cdots \succ \mathcal{A}_m$ be a strictly decreasing sequence of triangular sets. If A_i is nontrivial, for $P \in \mathcal{A}_i$, replace it by $\text{lvar}(P)^{\deg(P)}$. If A_i is trivial, replace it by 1. Then we get a strictly decreasing sequence of triangular sets $\mathcal{B}_1 \succ \mathcal{B}_2 \succ \cdots \succ \mathcal{B}_m$. This sequence must be a sub-sequence of $\mathcal{C}_1 \succ \mathcal{C}_2 \succ \cdots \succ \mathcal{C}_{q^n}$. Hence, $m \leq q^n$. □

Let P be given in (8) with $c > 0$. For another polynomial Q, write Q as a polynomial in x_c. First set $R = Q$. Then repeat the following process until $m = deg(R, x_c) < d$: $R := IR - b_m x_c^{m-d} P$, where b_m is the leading coefficient of R in x_c. It is easy to see that m strictly decreases after each iteration. Thus the process terminates. At the end, we have a equation

$$I^s Q = GP + R.$$

where $G, R \in \mathbb{R}_q$, s is a nonnegative integer, and either $R = 0$ or $\deg(R, x_c) < d$. R is called the *pseudo-remainder* of Q wrt P, denoted as $\text{prem}(Q, P)$. If P is a nonzero element in $\mathbb{R}_q$, define $\text{prem}(Q, P) = 0$. For a triangular set $\mathcal{A}$ defined in (9), the *pseudo-remainder* of Q wrt $\mathcal{A}$ is defined recursively as

$$\text{prem}(Q, \mathcal{A}) = \text{prem}(\text{prem}(Q, A_r), A_1, \ldots, A_{r-1}) \text{ and } \text{prem}(Q, \emptyset) = Q.$$

Let $R = \text{prem}(Q, \mathcal{A})$. Then we have

$$I_1^{s_1} I_2^{s_2} \cdots I_r^{s_r} AG = \sum_i Q_i A_i + R \qquad (10)$$

for some polynomials Q_i. The above formula is called the *remainder formula*. Let $\mathbb{P}$ be a set of polynomials and $\mathcal{A}$ a triangular set. We use $\text{prem}(\mathbb{P}, \mathcal{A})$ to denote the set of nonzero $\text{prem}(P, \mathcal{A})$ for $P \in \mathbb{P}$.

A polynomial Q is *reduced* wrt $P \neq 0$ if $\mathrm{class}(P) = c > 0$ and $\deg(Q, x_c) < \deg(P)$. A polynomial Q is *reduced* wrt a triangular set $\mathcal{A}$ if P is reduced wrt to all the polynomials in $\mathcal{A}$. It is clear that the pseudo-remainder of any polynomial wrt $\mathcal{A}$ is reduced wrt $\mathcal{A}$.

The *saturation ideal* of a triangular set $\mathcal{A}$ is defined as follows

$$\mathrm{sat}(\mathcal{A}) = \{P \in \mathbb{R}_q |\ JP \in (\mathcal{A})\}$$

where J is a product of certain powers of the initials of the polynomials in $\mathcal{A}$. We have

Lemma 3.2 *Let* $\mathcal{A} = A_1, \dots, A_r$ *be a triangular set. Then* $\mathrm{sat}(\mathcal{A}) = (A_1, \dots, A_r, \mathbf{I}_{\mathcal{A}}^{q-1} - 1)$.

Proof: Denote $\mathrm{I} = (A_1, \dots, A_r, \mathbf{I}_{\mathcal{A}}^{q-1} - 1)$ and $A_0 = \mathbf{I}_{\mathcal{A}}^{q-1} - 1$. If $P \in \mathrm{sat}(\mathcal{A})$, then $\mathbf{I}_{\mathcal{A}}^{q-1} P \in A$. There exist polynomials B_i such that

$$\mathbf{I}_{\mathcal{A}}^{q-1} P = \sum_{i=1}^{r} B_i A_i$$

Hence, $P = \sum_{i=1}^{r} B_i A_i - P A_0 \in \mathrm{I}$

Conversely, let $P \in \mathrm{I}$. Then there exist polynomials C_i such that

$$P = \sum_{i=1}^{r} A_i + C_0 A_0.$$

Multiply $\mathbf{I}_{\mathcal{A}}$ to both sides of the equation. Since $\mathbf{I}_{\mathcal{A}}(\mathbf{I}_{\mathcal{A}}^{q-1} - 1) = 0$, we have $\mathbf{I}_{\mathcal{A}} P = \sum_{i=1}^{r} \mathbf{I}_{\mathcal{A}} C_i A_i$. Thus, $P \in \mathrm{sat}(\mathcal{A})$. □

Let$\mathbf{I}_{\mathcal{A}}$ be the product of the initials of the polynomials in $\mathcal{A}$. As a consequence of the above lemma, we have

Corollary 3.3 *If* $\mathrm{prem}(\mathbf{I}_{\mathcal{A}}, \mathcal{A}) = 0$, *then* $\mathrm{sat}(\mathcal{A}) = \mathbb{R}_q$ *and* $\overline{\mathrm{Zero}}(\mathrm{sat}(\mathcal{A})) = \emptyset$.

3.2. Proper triangular sets and chains

As we mentioned before, a triangular set could have no zero. For example, $\overline{\mathrm{Zero}}(x^2+1) = \emptyset$ in $\mathbb{F}_3$. To avoid this problem, we introduce the concept of proper triangular sets.

A triangular set $\mathcal{A} = A_1, A_2, \dots, A_r$ is called *proper*, if the following condition holds: if $\mathrm{class}(A_i) = c_i$ and $\deg(A_i) = d_i$, then $\mathrm{prem}(x_{c_i}^{q-d_i} A_i, \mathcal{A}) = 0$.

The following lemmas show that proper triangular sets always have solutions.

Lemma 3.4 *Let* $P(x)$ *be a univariate polynomial in* $\mathbb{R}_q$, *and suppose that* $\deg(P(x)) = d$. *If prem*$(x^{q-d}P(x), P(x)) = 0$, *then* $P(x) = 0$ *has* d *distinct solutions in* $\mathbb{F}_q$.

Proof: Since $P(x)$ is a univariate polynomial, $\mathrm{init}(P) \in \mathbb{F}_q$. If $\mathrm{prem}(x^{q-d}P(x), P(x)) = 0$ in $\mathbb{R}_q$, we have $x^{q-d}P(x) = Q(x)P(x)$, where $Q(x)$ is a polynomial and $\deg(Q(x)) < q - d$. Considering the above equation in $\mathbb{F}_q[x]$, there is a polynomial C such that $x^{q-d}P(x) + C(x^q - x) = Q(x)P(x)$ in $\mathbb{F}_q[x]$, where $x^{q-d}P(x) + C(x^q - x)$ is equal to the canonical representation of $\overline{x^{q-d}P(x)}$ in $\mathbb{R}_q$. Thus, we have $(x^{q-d} - Q(x))P(x) = -C(x^q - x)$. Since all the elements of $\mathbb{F}_q$ are solutions of $x^q - x$, the q distinct elements of $\mathbb{F}_q$ are solutions of $(x^{q-d} - Q(x))P(x)$. Note that $\deg(Q(x)) < q - d$. Then $\deg(x^{q-d} - Q(x)) = q - d$. Thus, $x^{q-d} - Q(x)$ has at most $q-d$ solutions in $\mathbb{F}_q$, which means that $P(x)$ has at least d distinct solutions in $\mathbb{F}_q$. However, $\deg(P(x)) = d$ implies $P(x)$ has at most d solutions in $\mathbb{F}_q$. Hence, we can conclude $P(x)$ has d distinct solutions in $\mathbb{F}_q$. $\square$

A triangular set $\mathcal{A}$ is called *monic* if the initial of each polynomial in $\mathcal{A}$ is 1. For a monic triangular set $\mathcal{A} : A_1, \ldots, A_r$, we call $\deg(A_1)\deg(A_2)\cdots\deg(A_r)$ the degree of $\mathcal{A}$, denoted as $\deg(\mathcal{A})$. Let Y be the set $\{x_i \in \mathbb{X} | \, x_i$ is the leading variable of some $A_j \in \mathcal{A}\}$. Denotes $\mathbb{U}$ as $X \setminus Y$. Then we call $|\mathbb{U}|$ the dimension of $\mathcal{A}$, denoted as $\dim(\mathcal{A})$. For a monic proper triangular set, we have the following lemma.

Theorem 3.5 *Let $\mathcal{A}$ be a monic triangular set. Then $\mathcal{A}$ is proper iff* $|\overline{\mathrm{Zero}}(\mathcal{A})| = \deg(\mathcal{A}) \cdot q^{\dim(\mathcal{A})}$.

Proof: For the variables in $\mathbb{U}$, we can substitute them by any element of $\mathbb{F}_q$. Since $|\mathbb{U}| = \dim(\mathcal{A})$, there are $q^{\dim(\mathcal{A})}$ parametric values for $\mathbb{U}$. For a parametric value U_0 of $\mathbb{U}$ and a polynomial $P \in \mathbb{R}_q$, let P' denote $P(U_0)$. Then we have a monic triangular set $\mathcal{A}' : A'_1, \ldots, A'_r$, where $\mathrm{class}(A'_i) = \mathrm{class}(A_i)$ and $\deg(A'_i) = \deg(A_i)$. Let $c_i = \mathrm{class}(A_i)$ and $d_i = \deg(A_i)$. Since $\mathcal{A}$ is a proper triangular set, we have $x_{c_1}^{q-d_1} A_1 = PA_1$. Then $x_{c_1}^{q-d_1} A'_1 = P'_1 A'_1$. By Lemma 3.4, A'_1 has d_1 distinct solutions. For a solution α of A'_1, consider $A'_2(\alpha)$. Since $x_{c_2}^{q-d_2} A_2 = Q_1 A_1 + Q_2 A_2$, we have $x_{c_2}^{q-d_2} A'_2(\alpha) = Q'_1(\alpha)A'_1(\alpha) + Q'_2(\alpha)A'_2(\alpha)$. Since $A'_1(\alpha) = 0$, it implies that $x_{c_2}^{q-d_2} A'_2(\alpha) = Q'_2(\alpha)A'_2(\alpha)$. By Lemma 3.4, $A'_2(\alpha)$ has d_2 distinct solutions. Then we can recursively prove that $\mathcal{A}'$ has $d_1 d_2 \cdots d_r = \deg(\mathcal{A})$ distinct solutions. Hence, $|\overline{\mathrm{Zero}}(\mathcal{A})| = \deg(\mathcal{A}) \cdot q^{\dim(\mathcal{A})}$. The other direction is proved in Lemma 3.6. $\square$

Conversely, we have

Lemma 3.6 *Let $\mathcal{A} = A_1, \ldots, A_r$ be a monic triangular set. If for any parametric value U_0 of $\mathbb{U}$ and any point x in $\overline{\mathrm{Zero}}(A_1(U_0), \ldots, A_{i-1}(U_0))$, $A_i(U_0, x)$ has $\deg(A_i)$ distinct solutions. Then $\mathcal{A}$ is proper.*

Proof: Let $A_i = I_i x_{c_i}^{d_i} + V_i$. For A_1, suppose $\mathrm{prem}(x_{c_1}^{q-d_1} A_1, \mathcal{A}) = R_1 \neq 0$. Then we have $(x_{c_1}^{q-d_1} - P_1)A_1 = R_1$, where P_1 is a polynomial. Choose a parametric value U_0 of $\mathbb{U}$ such that $R_1(U_0) \neq 0$. Then $A_1(U_0)$ has d_1 distinct solutions, this is contradicts to $0 < \deg(R_1(U_0), x_{c_1}) < d_1$. Thus, $R_1 = 0$. Now we consider A_2. Suppose $\mathrm{prem}(x_{c_2}^{q-d_2} A_2, \mathcal{A}) = R_2 \neq 0$. Then we have two polynomials Q_1 and Q_2 such that $x_{c_2}^{q-d_2} A_2 = Q_1 A_1 + Q_2 A_2 + R_2$. Choose a parametric value U_1 of $\mathbb{U}$ such that $R_2(U_1) \neq 0$. Since $\deg(R_2, x_{c_1}) < d_1$, there is a solution x of $A_1(U_1)$ such that $R_2(U_1, x) \neq 0$. Then we have $(x_{c_2}^{q-d_2} - Q_1(U_1, x))A_2(U_1, x) = R_2(U_1, x)$. $A_2(U_1, x)$ has d_2 distinct solutions contradicts to $0 < \deg(R_2(U_1, x_{c_2}) < d_2$. Thus, $R_2 = 0$. Similarly, we have $\mathrm{prem}(x_{c_i}^{q-d_i} A_i, \mathcal{A}) = 0$. Hence, $\mathcal{A}$ is proper. $\square$

A (proper) triangular set $\mathcal{A}$ in (9) is called an *(proper) ascending chain*, or simply a (proper) chain, if A_j is reduced wrt A_i for $i < j$. A chain $\mathcal{A}$ is called conflict if $\mathbf{I}_{\mathcal{A}} = 0$. For a conflict chain, we have $\overline{\mathrm{Zero}}(\mathcal{A}/\mathbf{I}_{\mathcal{A}}) = \emptyset$. In $\mathbb{R}_2$, if $\mathcal{A}$ is non-conflict, $\overline{\mathrm{Zero}}(\mathcal{A}/\mathbf{I}_{\mathcal{A}}) \neq \emptyset$ [1]. This is not valid in $\mathbb{R}_q (q > 2)$.

A proper chain $\mathcal{A} = A_1, \ldots, A_r$ is called a quasi-monic proper chain, if $\mathrm{prem}(\mathrm{init}(A_i)^{q-1} - 1, \mathcal{A}) = 0$. For a quasi-monic proper chain, we have the following lemma.

Lemma 3.7 *Let $\mathcal{A} = A_1, A_2, \ldots, A_r$ be a quasi-monic proper chain. There exists a monic proper chain $\mathcal{B}$ such that* $\mathrm{class}(B_i) = \mathrm{class}(A_i)$*,* $\deg(B_i) = \deg(A_i)$ *and* $\overline{\mathrm{Zero}}(\mathcal{A}) = \overline{\mathrm{Zero}}(\mathcal{B})$*.*

Proof: Let $I_i = \mathrm{init}(A_i)$ and $c_i = \mathrm{class}(A_i)$. Note that $I_1^{q-1} - 1$ is reduced w.r.t $\mathcal{A}$. Then $\mathrm{prem}(I_1^{q-1} - 1, \mathcal{A}) = I_1^{q-1} - 1 = 0$. By Lemma 2.5, we have $\overline{\mathrm{Zero}}(I_1) = \emptyset$. From $\mathrm{prem}(I_2^{q-1} - 1, \mathcal{A}) = 0$ and the remainder formula (10), we have $\overline{\mathrm{Zero}}(A_1) \subseteq \overline{\mathrm{Zero}}(I_2^{q-1} - 1)$. Thus, $\overline{\mathrm{Zero}}(A_1, I_2) = \emptyset$. We can recursively prove that $\overline{\mathrm{Zero}}(A_1, A_2, \ldots, A_i, I_{i+1}^{q-1} - 1) = \overline{\mathrm{Zero}}(A_1, A_2, \ldots, A_i)$ and $\overline{\mathrm{Zero}}(A_1, A_2, \ldots, A_i, I_{i+1}) = \emptyset$, which means that the zero of $\mathcal{A}$ is not the zero of any I_i.

Now we construct a monic proper chain $\mathcal{B}$ from $\mathcal{A}$. Note that $\overline{\mathrm{Zero}}(A_1) = \overline{\mathrm{Zero}}(I_1^{q-2} A_1)$. Let $d_i = \deg(A_i)$ and $c_i = \mathrm{class}(A_i)$. Write $I_1^{q-2} A_1$ as $I_1^{q-2}(I_1 x_{c_1}^{d_i} + U_1) = (I_1^{q-1} - 1) x_{c_1}^{d_1} + x_{c_1}^{d_i} + I_1^{q-2} U_1$. Then $\overline{\mathrm{Zero}}(A_1) = \overline{\mathrm{Zero}}(x_{c_1}^{d_1} + I_1^{q-2} U_1)$. Let $B_1 = x_{c_1}^{d_1} + I_1^{q-2} U_1$. We obtain a monic polynomial B_1 such that $\overline{\mathrm{Zero}}(A_1) = \overline{\mathrm{Zero}}(B_1)$, $\mathrm{class}(A_1) = \mathrm{class}(B_1)$ and $\deg(A_1) = \deg(B_1)$. Then we have $\overline{\mathrm{Zero}}(A_1) = \overline{\mathrm{Zero}}(A_1, I_2^{q-1} - 1) = \overline{\mathrm{Zero}}(B_1, I_2^{q-1} - 1) = \overline{\mathrm{Zero}}(B_1)$. Thus, $\overline{\mathrm{Zero}}(A_1, A_2) = \overline{\mathrm{Zero}}(B_1, I_2^{q-1} - 1, I_2^{q-2} A_2)$. Write $I_2^{q-2} A_2$ as $(I_2^{q-1} - 1) x_{c_2}^{d_2} + x_{c_2}^{d_2} + I_2^{q-2} U_2$. We have $\overline{\mathrm{Zero}}(A_1, A_2) = \overline{\mathrm{Zero}}(B_1, x_{c_2}^{d_2} + I_2^{q-2} U_2)$. Let $R_2 = \mathrm{prem}(I_2^{q-2} U_2, B_1)$. Since B_1 is monic, $\overline{\mathrm{Zero}}(B_1, x_{c_2}^{d_2} + I_2^{q-2} U_2) = \overline{\mathrm{Zero}}(B_1, x_{c_2}^{d_2} + R_2)$. Let $B_2 = x_{c_2}^{d_2} + R_2$. Then we have $\overline{\mathrm{Zero}}(A_1, A_2) = \overline{\mathrm{Zero}}(B_1, B_2)$. Similarly, we can recursively construct B_{r-1} by $\mathcal{A}_{r-1}$. Hence, we obtain a chain $\mathcal{B}$.

Since $\overline{\mathrm{Zero}}(A_1, A_2, \ldots, A_{i-1}, I_i) = \emptyset$ and $\mathcal{A}$ is proper, it is easy to prove that for any parametric value $\mathbb{U}_0$ of $\mathbb{U}$ and any point x in $\overline{\mathrm{Zero}}(A_1(\mathbb{U}_0), \ldots, A_{i-1}(\mathbb{U}_0))$, $A_i(\mathbb{U}_0, x)$ has $\deg(A_i)$ distinct solutions. Since $\overline{\mathrm{Zero}}(A_1, \ldots, A_i) = \overline{\mathrm{Zero}}(B_1, \ldots, B_i)$, by Lemma 3.6, we have $\mathcal{B}$ is a monic proper chain. □

3.3. Well-Ordering Principles

A *characteristic set* (CS) of a polynomial set $\mathbb{P}$ is any chain of lowest ordering contained in $\mathbb{P}$. It is evident that any two characteristic sets of a polynomial set are of the same ordering. We have the following basic property for the basic set[2, 3].

Lemma 3.8 *Let $\mathcal{A}$ be a characteristic set of a polynomial set $\mathbb{P}$. If P is reduced wrt $\mathcal{A}$, then the characteristic set of $\mathbb{P} \cup \{P\}$ is of lower ordering than that of $\mathbb{P}$.*

Let $\mathbb{P}$ be a polynomial set. We set $\mathbb{P}_0 = \mathbb{P}$ and choose a CS $\mathcal{B}_0$ of $\mathbb{P}_0$. Let $\mathbb{R}_0$ be the nonzero remainders of polynomials in $\mathbb{P}_0 \setminus \mathcal{B}_0$ wrt $\mathcal{B}_0$. Suppose that $\mathbb{R}_0 \neq \emptyset$. Then we form a new polynomial set $\mathbb{P}_1 = \mathbb{P} \cup \mathcal{B}_0 \cup \mathbb{R}_0$. Choose now an arbitrary CS $\mathcal{B}_1$ of $\mathbb{P}_1$. By Lemma 3.2, $\mathcal{B}_1$ is of lower ordering than $\mathcal{B}_0$. Continuing in this way, we will obtain successively $\mathbb{P}_i, \mathcal{B}_i, \mathbb{R}_i, i = 1, 2, \ldots$, for which

$$\mathcal{B}_0 \succ \mathcal{B}_1 \succ \mathcal{B}_2 \succ \cdots .$$

By Lemma 3.1, the sequence can only be a finite one so that up to a certain stage m we should have $\mathbb{R}_m = \emptyset$. The above procedure can be exhibited in the form of the scheme (11) below:

$$\begin{array}{ccccccccc} \mathbb{P} & = & \mathbb{P}_0 & \mathbb{P}_1 & \cdots & \mathbb{P}_i & \cdots & \mathbb{P}_m & \\ & & \mathcal{B}_0 & \mathcal{B}_1 & \cdots & \mathcal{B}_i & \cdots & \mathcal{B}_m = \mathcal{C} & \\ & & \mathbb{R}_0 & \mathbb{R}_1 & \cdots & \mathbb{R}_i & \cdots & \mathbb{R}_m = \emptyset & \end{array} \tag{11}$$

where

$$\mathbb{P}_i = \mathbb{P}_{i-1} \cup \mathbb{R}_{i-1} \tag{12}$$

$\mathcal{B}_i$ is a CS of $\mathbb{P}_i$, and $\mathbb{R}_i$ is the set of nonzero remainders of the polynomials in $\mathbb{P}_i$ wrt $\mathcal{B}_i$.

In scheme (11), the corresponding CS $\mathcal{B}_m = \mathcal{C}$ verifies

$$\text{prem}(\mathbb{P}, \mathcal{C}) = \{0\} \text{ and } \text{Zero}(\mathbb{P}) \subset \text{Zero}(\mathcal{C}). \tag{13}$$

Any chain $\mathcal{C}$ verifying the property (13) is called a Wu-CS of the $\mathbb{P}$.

In $\mathbb{R}_2$, using characteristic set, we can decompose the zero set of a polynomial equation system as the disjoint union of the zero sets of monic chain [1]. But when $q > 2$, a monic chain may not have zero. For example, in $\mathbb{R}_3$, $\overline{\text{Zero}}(x_1^2 + 2x_1, x_2^2 + 1) = \emptyset$. From Lemma 3.5, if a monic chain $\mathcal{A}$ is proper, it has $\text{deg}\mathcal{A} \cdot q^{\dim(\mathcal{A})}$ solutions. Thus, we can compute the proper CS, and decompose the zero set of a polynomial equation system as the union of zero set of monic proper chain.

In scheme (11), if $\mathcal{C} = C_1, C_2, \ldots, C_r$ is not proper, let $\mathbb{R}_0^1$ be the nonzero remainders of $x_{c_i}^{q-d_i} C_i$ wrt $\mathcal{C}$, where $c_i = \text{class}(C_i)$ and $d_i = \deg(C_i)$. Then we form $\mathbb{P}_0^1 = \mathbb{P}_m \cup \mathbb{R}_0^1$. For $\mathbb{P}_0^1$, repeat the process of scheme (11). Then we obtain a characteristic set $\mathcal{C}_1$ whose ordering is lower than $\mathcal{C}_0$. If $\mathcal{C}_1$ is not proper, we do the above process again. From Lemma 3.1, we know that the whole process will terminate in l steps, where $l \le q^n$. Then we obtain a sequence of chain

$$\mathcal{B}_0 \succ \cdots \succ \mathcal{B}_{m_1} = \mathcal{C} \succ B_0^1 \succ \cdots \succ B_{m_1}^1 = \mathcal{C}_1 \succ \cdots \succ C_{t-1} \succ B_0^t \succ \cdots \succ B_{m_t}^t = \mathcal{C}_{pro},$$

where $\mathcal{C}_{pro}$ is a proper chain. Similarly, we have

$$\text{prem}(\mathbb{P}, \mathcal{C}_{pro}) = \{0\} \text{ and } \text{Zero}(\mathbb{P}) \subset \text{Zero}(\mathcal{C}_{pro}). \tag{14}$$

Then $\mathcal{C}_{pro}$ is called a *proper characteristic set* (PCS) of $\mathbb{P}$. We have the following key properties of the CS.

Theorem 3.9 (Well-ordering principle) *Let $\mathcal{C}$ be a Wu-CS of a polynomial set $\mathbb{P}$, $H_i = \text{prem}(I_i^{q-1} - 1, \mathcal{C})$. Then we have*

$$\begin{aligned}
&\overline{\text{Zero}}(\mathbb{P}) \\
&= \overline{\text{Zero}}(\mathcal{C}/\mathbf{I}_{\mathcal{C}}) \bigcup \cup_{i=1}^{r} \overline{\text{Zero}}(\mathbb{P} \cup \mathcal{C} \cup \{I_i\}) && (15)\\
&= \overline{\text{Zero}}(\mathcal{C} \cup \{I_1^{q-1} - 1, \ldots, I_r^{q-1} - 1\}) \bigcup \cup_{i=1}^{r} \overline{\text{Zero}}(\mathbb{P} \cup \mathcal{C} \cup \{I_i\}) && (16)\\
&= \overline{\text{Zero}}(\mathcal{C} \cup \{H_1, \ldots, H_r\}) \bigcup \cup_{i=1}^{r} \overline{\text{Zero}}(\mathbb{P} \cup \mathcal{C} \cup \{I_i\}) && (17)\\
&= \overline{\text{Zero}}(\mathcal{C} \cup \{H_1, \ldots, H_r\}) \bigcup \cup_{i=1}^{r} \overline{\text{Zero}}(\mathbb{P} \cup \mathcal{C} \cup \{H_1, \ldots, H_{i-1}, I_i\}) && (18)
\end{aligned}$$

where $I_i, i = 1, \ldots, r$ are the initials of the polynomials in $\mathcal{C}$. When $i < 0$, I_i is assumed not occurring in the formula.

Proof: Equation (15) is a direct consequence of the remainder formula (10) and is the same as the characteristic zero case [3, 4]. By (3), (6) and (15), we have equation (16).

To prove equation (17), it is sufficient to show $\overline{\mathrm{Zero}}(\mathcal{C}\cup\{H_1,\ldots,H_r\}) = \overline{\mathrm{Zero}}(\mathcal{C}\cup\{I_1^{q-1}-1,\ldots,I_r^{q-1}-1\})$. Let x be a element in $\overline{\mathrm{Zero}}(\mathcal{C}\cup\{I_1^{q-1}-1,\ldots,I_r^{q-1}-1\})$. By the remainder formula (10), we have $H_i(x)=0$. Thus, $\overline{\mathrm{Zero}}(\mathcal{C}\cup\{I_1^{q-1}-1,\ldots,I_r^{q-1}-1\}) \subset \overline{\mathrm{Zero}}(\mathcal{C}\cup\{H_1,\ldots,H_r\})$. Conversely, let x be a element in $\overline{\mathrm{Zero}}(\mathcal{C}\cup\{H_1,\ldots,H_r\})$. Since $I_1^{q-1}-1$ is reduced w.r.t $\mathcal{C}$, $I_1^{q-1}-1=H_1$. Then $H_1(x)=0$ implies $I_1^{q-1}(x)-1=0$. Thus, $I_1(x)\neq 0$. By the remainder formula (10), $I_2^{q-1}(x)-1=0$, which means $I_2(x)\neq 0$. We can recursively obtain $I_i^{q-1}(x)-1=0$. Hence, $\overline{\mathrm{Zero}}(\mathcal{C}\cup\{H_1,\ldots,H_r\}) \subset \overline{\mathrm{Zero}}(\mathcal{C}\cup\{I_1^{q-1}-1,\ldots,I_r^{q-1}-1\})$.

Note that $\overline{\mathrm{Zero}}(P)\cup\overline{\mathrm{Zero}}(Q) = \overline{\mathrm{Zero}}(P)\cup\overline{\mathrm{Zero}}(Q/P) = \overline{\mathrm{Zero}}(P)\cup\overline{\mathrm{Zero}}(\{Q,P^{q-1}-1\})$. Then we can obtain (18) from (17) □

This result is significant because it represents the zero set for a general polynomial set as the zero set of an ascending chain.

In procedure (11), the size of $\mathbb{P}_i$ could increase very fast. We may adopt the following way to compute $\mathbb{P}_i$ and Theorem 3.9 is still valid.

$$\mathbb{P}_i = \mathbb{P}\cup\mathcal{B}_{i-1}\cup\mathbb{R}_{i-1} \tag{19}$$

A more drastic way to reduce the size of $\mathbb{P}_i$ is give below. In [5], Wu proposed that instead of (19), we use the the following way to compute $\mathbb{P}_i$

$$\mathbb{P}_i = \mathcal{B}_{i-1}\cup\mathbb{R}_{i-1}. \tag{20}$$

Then $|\mathbb{P}_i|$ is always less than or equal to $|\mathbb{P}|$. In the case of characteristic zero, Wu proved the following theorem.

Theorem 3.10 ([5]) *Let $\mathcal{C}$ be a CS of a polynomials et $\mathbb{P}$ using scheme (11) and (20). Then*

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathcal{C}/K_m)\bigcup\cup_{k=0}^{m}\mathrm{Zero}(\mathbb{P}\cup\{J_k\}/K_{k-1}).$$

where J_i is the product of initials of polynomials in $\mathcal{B}_i$, and $K_i=\prod_{j=0}^{i}J_i$.

In $\mathbb{R}_q$, we can modify the formula as the following form..

Theorem 3.11 (Modified well-ordering principle) *Let $\mathcal{C}$ be a chain computed from a polynomial set $\mathbb{P}$ with procedures (11) and (20), $I_j, j=1,\ldots,s$ the initials of the polynomials in $\mathcal{C}=\mathcal{B}_m,\ldots,\mathcal{B}_0$ (note that the initials of polynomials in $\mathcal{C}$ appear first in the sequence), $H_j=\mathrm{prem}(I_j^{q-1}-1,\mathcal{C})$, $T_j=\mathrm{prem}(I_j,\mathcal{C}), j=1,\ldots,s$ and K_m the product for all the I_j. Then, we have*

$$\begin{aligned}
&\overline{\mathrm{Zero}}(\mathbb{P})\\
&=\overline{\mathrm{Zero}}(\mathcal{C}/K_m)\bigcup\cup_{i=1}^{s}\overline{\mathrm{Zero}}(\mathbb{P}\cup\mathcal{C}\cup\{I_1^{q-1}-1,\ldots,I_{i-1}^{q-1}-1,I_i\}) &(21)\\
&=\overline{\mathrm{Zero}}(\mathcal{C}\cup\{H_1,\ldots,H_s\})\bigcup\cup_{i=1}^{s}\overline{\mathrm{Zero}}(\mathbb{P}\cup\mathcal{C}\cup\{H_1,\ldots,H_{i-1},T_i\}) &(22)
\end{aligned}$$

When $i<0$, I_i will not appear in the formula.

Proof: Let $U_l = \prod_{i=1}^{l} I_i$. From [5], we have the following equation

$$\overline{\text{Zero}}(\mathbb{P}) = \overline{\text{Zero}}(\mathcal{C}/K_m) \bigcup \cup_{i=1}^{s} \overline{\text{Zero}}(\mathbb{P} \cup \mathcal{C} \cup \{I_i\}/U_{i-1}). \qquad (23)$$

Equation (21) is a consequence of (23), (3) and (6). Similar to Theorem 3.9, we can prove

$$\overline{\text{Zero}}(\mathcal{C}/K_m) = \overline{\text{Zero}}(\mathcal{C} \cup \{I_1^{q-1} - 1, \ldots, I_s^{q-1} - 1\}) = \overline{\text{Zero}}(\mathcal{C} \cup \{H_1, \ldots, H_s\}).$$

Since the initial of the polynomials of $\mathcal{C}$ are reduced w.r.t $\mathcal{C}$, for the initial $I_i, i = 1, \ldots, t$ of $\mathcal{C}$, we have $T_i = I_i$. Thus, for $i \le t$,

$$\overline{\text{Zero}}(\mathbb{P} \cup \mathcal{C} \cup \{I_1^{q-1} - 1, \ldots, I_{i-1}^{q-1} - 1, I_i\}) = \overline{\text{Zero}}(\mathbb{P} \cup \mathcal{C} \cup \{H_1, \ldots, H_{i-1}, T_i\}).$$

For $i > t$, by the remainder formula (10), we also have the above equation. This proves equation (22). □

3.4. Zero Decomposition Theorems in $\mathbb{R}_q$

Now we give the zero decomposition theorems. The following traditional form [3, 4] is still valid and the proof is also the same. Note that for a conflict chain $\mathcal{A}$, $\overline{\text{Zero}}(\mathcal{A}/\mathbf{I}_{\mathcal{A}}) = \emptyset$.

Theorem 3.12 (Zero Decomposition Theorem) *There is an algorithm which permits to determine for a given polynomial set $\mathbb{P}$ in a finite number of steps non-conflict chains $\mathcal{A}_j, j = 1, \ldots, s$ such that*

$$\overline{\text{Zero}}(\mathbb{P}) = \cup_{j=1}^{s} \overline{\text{Zero}}(\mathcal{A}_j/\mathbf{I}_{\mathcal{A}_j}).$$

In $\mathbb{R}_2$, we have a monic zero decomposition theorem [1]. As mentioned before, in $\mathbb{R}_q(q > 2)$, a monic chain may have no solution. Thus, we need to use the monic proper chain. Then, we can give the following theorem.

Theorem 3.13 (Monic Zero Decomposition Theorem) *There is an algorithm which permits to determine for a given polynomial set $\mathbb{P}$ in a finite number of steps monic proper chains $\mathcal{A}_j, j = 1, \ldots, t$ such that*

$$\overline{\text{Zero}}(\mathbb{P}) = \cup_{j=1}^{t} \overline{\text{Zero}}(\mathcal{A}_j).$$

Proof: First we get a PCS of $\mathbb{P}$ by process (14). By Theorem 3.9, we have (17). One may repeat the procedure (14) for each $\mathcal{C} \cup \{H_1, \ldots, H_r\}$ and $\mathbb{P} \cup \mathcal{C} \cup \{H_i\}$. Since H_i is reduced wrt $\mathcal{C}$, according to Lemma 3.2, the new chains obtained in this way will be of lower ordering than that of $\mathcal{C}$. By Lemma 3.1, the procedure will end in a finite number of steps. Note that we could also use (22) to obtain the decomposition. In (22), since H_i and T_i are reduced wrt $\mathcal{C}$. By Lemma 3.2, the process will terminate in a finite number of steps.

At the end of the above process we obtain some quasi-monic proper chains $\mathcal{B}_j, j = 1, \ldots, t$ such that $\overline{\text{Zero}}(\mathbb{P}) = \cup_{j=1}^{t} \overline{\text{Zero}}(B_j)$. By Lemma 3.7, for any $j = 1, \ldots, t$, we can obtain a monic proper chain A_j such that $\overline{\text{Zero}}(\mathcal{A}_j) = \overline{\text{Zero}}(\mathcal{B}_j)$ in a finite number of steps. Then we have $\overline{\text{Zero}}(\mathbb{P}) = \cup_{j=1}^{t} \overline{\text{Zero}}(\mathcal{A}_j)$. □

Example 3.14 *In $\mathbb{R}_3$, Let $\mathbb{P} = \{x_1x_2x_3^2-1\}$. First we obtain a PCS $\{x_1^2-1, x_1x_2-1, x_1x_3^2-x_1\}$ of $\mathbb{P}$. By Theorem 3.12, we have $\overline{\text{Zero}}(\mathbb{P}) = \overline{\text{Zero}}(\{x_1^2-1, x_1x_2-1, x_1x_3^2-x_1\}/x_1^2)$. By Theorem 3.13, or (17), $\overline{\text{Zero}}(\mathbb{P}) = \overline{\text{Zero}}(x_1^2-1, x_1x_2-1, x_1x_3^2-x_1) \cup \overline{\text{Zero}}(x_1, x_1^2-1, x_1x_2-1, x_1x_3^2-x_1) = \overline{\text{Zero}}(x_1^2-1, x_2-x_1, x_3^2-1)$.*

The following theorem gives a refined zero decomposition theorem which allows to compute the number of solutions for a finite set of polynomials.

Theorem 3.15 (Disjoint Zero Decomposition Theorem) *For a finite polynomial set $\mathbb{P}$, we can find monic proper chains $\mathcal{A}_j, j = 1, \ldots, s$ such that*

$$\overline{\text{Zero}}(\mathbb{P}) = \cup_{i=1}^{s} \overline{\text{Zero}}(\mathcal{A}_i)$$

and $\overline{\text{Zero}}(\mathcal{A}_i) \cap \overline{\text{Zero}}(\mathcal{A}_j) = \emptyset$ for $i \neq j$. As a consequence, we have

$$|\overline{\text{Zero}}(\mathbb{P})| = \sum_{i=1}^{s} \deg(\mathcal{A}_i) \cdot q^{\dim(\mathcal{A}_i)}.$$

Proof: The proof is similar to that of Theorem 3.13. We just need to use (18) instead of (17). Since the components are disjoint, by Lemma 3.5, the number of solutions are $\sum_{i=1}^{s} \deg(\mathcal{A}_i) \cdot q^{\dim(\mathcal{A}_i)}$. Similar to Theorem 3.12, we could also use (22) to obtain the decomposition. □

Example 3.16 *In $\mathbb{R}_3$, let $\mathbb{P} = \{x_1x_2^2+x_2+1\}$. First we obtain a PCS $\{x_1^2-x_1, x_1x_2+x_2+1\}$. By Theorem 3.15, we have $\overline{\text{Zero}}(\mathbb{P}) = \overline{\text{Zero}}(x_1-1, x_2-1) \cup \overline{\text{Zero}}(x_1, x_2+1)$. Thus, $|\overline{\text{Zero}}(\mathbb{P})| = 3^0 + 3^0 = 2$.*

Now we could give the algorithm **DisMPZD** from Theorem 3.15.

4. A Top-Down Algorithm for Monic Proper Zero Decomposition

The TopDownZD algorithm for obtaining a monic zero decomposition of $\mathbb{P}$ in $\mathbb{R}_2$ is presented in [1]. The main idea is working from the polynomials with the highest rank to that with the lowest rank.

In this section, we will give a algorithm **TopDownPZD** to get a monic proper zero decomposition of $\mathbb{P}$ in $\mathbb{R}_q$. By the special properties of $\mathbb{R}_q$, our algorithm has stronger properties.

Theorem 4.1 *Algorithm* **TopDownPZD** *is correct and to obtain each monic proper chain of $\mathbb{P}$, we need $O(n(q-1)l)$ polynomial arithmetic operations where $l = |\mathbb{P}|$.*

Proof. We consider the set $\mathbb{Q}$ of polynomials in the algorithm. $\mathbb{Q}_1 \subset \mathbb{Q}$ is the set of polynomials with the highest class and $Q \in \mathbb{Q}_1$ a polynomial whose degree is lowest and initial is of the lowest ordering. Let $c = \text{class}(Q)$, $d = \deg(Q)$ and $I = \text{init}(Q)$. If $I = 1$, then for $P \in \mathbb{Q}_1$, as a consequence of remainder formula (10), $\overline{\text{Zero}}(\{Q, P\}) = \overline{\text{Zero}}(\{Q, P_1\})$. Therefore, we have

$$\overline{\text{Zero}}(\mathbb{Q}) = \overline{\text{Zero}}((\mathbb{Q} \setminus \mathbb{Q}_1) \cup \{Q\} \cup \{\text{prem}(P, Q) \neq 0 \,|\, P \in \mathbb{Q}_1\}).$$

If $I \neq 1$, by (6), we can split $\overline{\text{Zero}}(\mathbb{Q})$ as the following two parts:

$$\begin{aligned}\overline{\text{Zero}}(\mathbb{Q}) &= \overline{\text{Zero}}(\mathbb{Q} \cup \{I^{q-1} - 1\}) \cup \overline{\text{Zero}}(\mathbb{Q} \cup \{I\}) \\ &= \overline{\text{Zero}}((\mathbb{Q} \setminus \{Q\}) \cup \{Q_1\} \cup \{I^{q-1} - 1\}) \cup \overline{\text{Zero}}((\mathbb{Q} \setminus \{Q\}) \cup \{I, U\}).\end{aligned}$$

The first part can be treated similarly to the case of $I = 1$ and the second case will be treated recursively with algorithm **TopDownPZD**. This proves that after the step 2 of the algorithm, we get $\mathcal{A}_1, \dots, \mathcal{A}_q$ such that $\text{Zero}(\mathbb{P}) = \cup_i \text{Zero}(A_i)$. Then we determine whether $\mathcal{A}_i$ is a proper triangular set in step 4. If it is proper, we turn it into a chain form $\mathcal{A}'_i$. Since $\mathcal{A}_i$ is monic, by the remainder formula (10), $\overline{\text{Zero}}(\mathcal{A}'_i) = \overline{\text{Zero}}(\mathcal{A}_i)$. If $\mathcal{A}_i$ is not proper, suppose $\mathcal{A}_i = A_{i1}, \dots, A_{ip_i}$. we add $\text{prem}(x_{c_{ij}}^{q-d_{ij}} A_{ij}, \mathcal{A}_i) \neq 0$ to $\mathcal{A}_i$, and get a polynomials set $\mathcal{B}_i$. We have $\overline{\text{Zero}}(\mathcal{A}_i) = \overline{\text{Zero}}(\mathcal{A}_i, x_{c_{ij}}^{q-d_{ij}} A_{ij}) = \overline{\text{Zero}}(\mathcal{A}_i, \text{prem}(x_{c_{ij}}^{q-d_{ij}} A_{ij}, \mathcal{A}_i))$. Thus, $\overline{\text{Zero}}(\mathcal{A}_i) = \overline{\text{Zero}}(\mathcal{B}_i)$. Then we treated $\mathcal{B}_i$ recursively with algorithm **TopDown-PZD**. Hence, if $\mathcal{A}'_1, \dots, \mathcal{A}'_s$ is the output of the algorithm, we have $\overline{\text{Zero}}(\mathbb{P}) = \cup_i \overline{\text{Zero}}(A'_i)$.

The termination of step 2 of the algorithm can be proved in two steps. First, we will show the termination for the inner loop of step 2, that is, for each finite polynomial set $\mathbb{Q}$, the algorithm will terminate. After each iteration of the loop, the lowest degree of the polynomials of highest class in $\mathbb{Q}$ will decrease. Then the highest class of the polynomials in $\mathbb{Q}$ will be reduced and the polynomial Q will be added to $\mathcal{A}$. Hence, this loop will end and give a triangular set $\mathcal{A}$. Second, we need to show the termination for the outer loop. For a polynomial set $\mathbb{P}$, we assign an index $(c_{n,q-1}, c_{n,q-2}, \dots, c_{n,1}, \dots, c_{1,q-1}, \dots, c_{1,1})$ where $c_{i,j}$ is the number of polynomials in $\mathbb{P}$ and with class i and degree j. In the step 2, there are essentially two cases where new polynomial sets are generated. In the first case, we replace $\mathbb{Q}$ with $\mathbb{Q}' = (\mathbb{Q} \setminus \mathbb{Q}_1) \cup \{Q\} \cup \{I^{q-1} - 1\} \cup \{\text{prem}(P, Q) \neq 0 \,|\, P \in \mathbb{Q}_1\}$. In the second case, we add $\mathbb{Q}' = (\mathbb{Q} \setminus \{Q\}) \cup \{I, U\}$ to $\mathbb{P}^*$, where $Q = Ix_c + U$. It is clear that the index of $\mathbb{Q}'$ is less than the index of $\mathbb{Q}$ in the lexicographical ordering in both cases. It is easy to show that a strictly decreasing sequence of indexes must be finite. This proves the termination of the step 2.

Suppose we get $\mathcal{A}^* = \mathcal{A}_1, \dots, \mathcal{A}_q$ after step 2. If it is proper, the process of turning it into the chain form is terminational. If $\mathcal{A}_i = A_{i1}, \dots, A_{ip_i}$ is not proper, as mentioned above, we get a polynomial set $\mathcal{B}_i$ such that there are polynomials reduced wrt $\mathcal{A}_i$ in $\mathcal{B}_i$.

To prove the termination of the whole algorithm, it is sufficient to show that the new monic triangular sets we get from $\mathcal{B}_i$ by step 2 is of lower ordering than that of $\mathcal{A}_i$. Note that the inner loop of step 2 generates monic triangular sets while the outer loop generates new polynomial sets. There is a polynomial $Q \in \mathcal{B}_i$ with the highest class and lowest degree such that Q is reduced wrt $\mathcal{A}_i$. Let $Q = Ix_c^d + U$. Then step 2 splits $\overline{\text{Zero}}(\mathcal{B}_i)$ into two parts:

$$\overline{\text{Zero}}(\mathcal{B}_i) = \overline{\text{Zero}}(\{\mathcal{B}_i \setminus \{Q\}\} \cup \{x_c^d + U\} \cup \{I^{q-1} - 1\}) \cup \overline{\text{Zero}}(\{\mathcal{B}_i \setminus \{Q\}\} \cup \{I, U\}).$$

It is easy to prove the following property of step 2: Let $\mathcal{B}$ be a input of step 2. Assume there is a monic polynomial B_s in $\mathcal{B}$ such that $\text{class}(B_s) = c$. Let $\mathcal{B}'_1, \dots, \mathcal{B}'_r$ be the monic triangular sets getting from step 2. Then, for any i, there is a polynomial $B'_{ij} \in \mathcal{B}'_i$ such that $\text{class}(B'_{ij}) = c$ and $\deg(B'_{ij}) \leq \deg(B_s)$.

Since $x_c^d + U$ is reduced wrt $\mathcal{A}_i$ and $\mathcal{A}_i \subseteq \mathcal{B}_i$, the monic triangular sets we obtain from $\{\mathcal{B}_i \setminus \{Q\}\} \cup \{x_c^d + U\} \cup \{I^{q-1} - 1\}$ is of lower ordering than $\mathcal{A}_i$. For $\{\mathcal{B}_i \setminus \{Q\}\} \cup \{I, U\}$, since I and U is reduced wrt $\mathcal{A}_i$, it can be treated recursively as $\mathcal{B}_i$. Hence, we prove the termination of the algorithm.

Finally, we will analyze the complexity of the inner loop of step 2 of the algorithm, that is, the complexity to obtain a monic triangular set from $\mathbb{Q}$. Let $l = |\mathbb{Q}|$. After each iteration, the lowest degree of the highest class of the polynomials in $\mathbb{Q}$ will be reduced at least by one. Then, this loop will execute at most $n(q-1)$ times. In each iteration, we need to select the polynomials with the highest class and the polynomials with lowest degree and initials. These operations need $O(l)$ comparison of integers. If $I = 1$, then the new $\mathbb{Q}$ contains at most $l-1$ polynomials. If $I \neq 1$, the new $\mathbb{Q}$ contains at most l polynomials. Then, after each iteration, the new $\mathbb{Q}$ contains at most l polynomials. In each iteration, we also need to compute at most $l-1$ pseudo-remainders. Suppose we want to get $\mathrm{prem}(P, Q)$. It takes at most 2 polynomial multiplications when we decrease the degree of P by one. When we reduce a class of polynomials in $\mathbb{Q}$, the lowest degree decreases to 0, and the highest degree at most decreases to 1. Thus, we need at most $2(q-1+q-2)(l-1)$ multiplications to reduce a class of polynomials in $\mathbb{Q}$. In all, the algorithm needs $O(n(q-1)l)$ polynomial arithmetic operations and $O(n(q-1)l)$ comparison of integers. ▮

References

[1] Gao, X.S., Chai, F., Yuan, C. A Characteristic Set Method for Equation Solving in F2 and Applications in Cryptanalysis of Stream Ciphers, *MM-Preprints*, 42-56, 2006.

[2] Ritt, J.F. *Differential Algebra*, Amer. Math. Soc. Colloquium, 1950.

[3] Wu, W.T. *Basic Principle of Mechanical Theorem Proving in Geometries*, (in Chinese) Science Press, Beijing, 1984; English translation, Springer, Wien, 1994.

[4] Wu, W.T. On Zeros of Algebraic Equations - An Application of Ritt Principle, *Chinese Science Bulletin*, **31**, 1-5, 1986.

[5] Wu, W.T. Some Remarks on Characeteristic-Set Formation, *MM-Preprints*, Vol. 3, 27-29, 1989.

Algorithm 1 — DisMPZD($\mathbb{P}$)

```
Input:   A finite set of polynomials $\mathbb{P}$.
Output:  A sequence of monic proper chains $\mathcal{A}_i$ such that $\overline{\mathrm{Zero}}(\mathbb{P}) = \cup_i \overline{\mathrm{Zero}}(\mathcal{A}_i)$.
1 Set $\mathbb{P}^* = \{\mathbb{P}\}$, $\mathcal{A}^* = \emptyset$.
2 While $\mathbb{P}^* \neq \emptyset$ do
  2.1 Choose a $\mathbb{P}$ from $\mathbb{P}^*$.
  2.2 Set $\mathbb{Q} = \mathbb{P}$
  2.3 Do
      2.3.1 Do
              C=The characteristic set of $\mathbb{Q}$.
              $\mathbb{R} = \mathrm{prem}(\mathbb{Q} \setminus \mathcal{C}, \mathcal{C})$.
              $\mathbb{Q} = \mathbb{Q} \cup \mathbb{R}$ (or $\mathbb{P} \cup \mathcal{C} \cup \mathbb{R}$).
            Until $\mathbb{R} = \emptyset$.
      2.3.2 Let $\mathcal{C} = \{C_1, C_2, \ldots, C_r\}$, class$(C_i) = c_i$ and deg$(C_i) = d_i$.
      2.3.3 Set $\mathbb{R}_1 = \emptyset$.
      2.3.4 For $i$ from 1 to $k$ do
              $\mathbb{R}_1 = \mathbb{R}_1 \cup \mathrm{prem}(x_{c_i}^{q-d_i} C_i, \mathcal{C}) \neq 0$.
      2.3.5 $\mathbb{Q} = \mathbb{Q} \cup \mathbb{R}_1$ (or $\mathbb{P} \cup \mathcal{C} \cup \mathbb{R}_1$).
    Until $\mathbb{R}_1 = \emptyset$.
  2.4 Set $\mathbb{I} = \{\mathrm{init}(P) | P \in \mathcal{C}\} = \{I_1, \ldots, I_s\}$.
  2.5 Set $J = \prod_{i=1}^{s} I_i$.
  2.6 Set $\mathbb{H} = \{H_i \neq 0 | H_i = \mathrm{prem}(I_i^{q-1} - 1, \mathcal{C})\}$.
  2.7 If $\mathbb{H} = \emptyset$, do $\mathcal{A}^* = \mathcal{A}^* \cup \{C\}$.
  2.8 Else, do
    2.8.1 If $J \neq 0$, do $\mathbb{P}^* = \mathbb{P}^* \cup \{\mathcal{C} \cup \mathbb{H}\}$.
    2.8.2 For i from 1 to s, do
            $\mathbb{P}_1 = \mathbb{P} \cup \mathcal{C} \cup \{H_1, \ldots, H_{i-1}, I_i\}$.
            $\mathbb{P}^* = \mathbb{P}^* \cup \{\mathbb{P}_1\}$.
3 Let $\mathcal{A}^* = \{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_q\}$ and $\mathcal{A}_i = \{A_{i1}, \ldots, A_{ip_i}\}$.
4 For $i$ from 1 to $q$ do
  4.1 Set $\mathcal{B} = \emptyset$.
  4.2 For $j$ from 1 to $p_i$ do
        4.2.1 Let $A_{ij} = I_{ij} x_{c_{ij}}^{d_{ij}} + R_{ij}$
        4.2.2 $A_{ij} = \mathrm{prem}(x_{c_{ij}}^{d_{ij}} + I_{ij}^{q-2} R_{ij}, \mathcal{B})$.
        4.2.3 $\mathcal{B} = \mathcal{B} \cup \{A_{ij}\}$.
Return $\mathcal{A}^*$
```

Algorithm 2 — TopDownPZD($\mathbb{P}$)

Input: A finite set of polynomials $\mathbb{P}$.

Output: A sequence of monic proper chains $\mathcal{A}_i$ such that $\overline{\text{Zero}}(\mathbb{P}) = \cup_i \overline{\text{Zero}}(\mathcal{A}_i)$.

```
1 Set $\mathbb{P}^* = \{\mathbb{P}\}$, $\mathcal{A}^* = \emptyset$ and $\mathcal{C}^* = \emptyset$.
2 While $\mathbb{P}^* \neq \emptyset$ do
    2.1 Choose a $\mathbb{Q}$ from $\mathbb{P}^*$.
    2.2 Set $\mathcal{A} = \emptyset$.
    2.3 While $\mathbb{Q} \neq \emptyset$ do
        2.3.1 If some element $\alpha$ of $\mathbb{F}_q$ is in $\mathbb{Q}$, $\overline{\text{Zero}}(\mathbb{Q}) = \emptyset$. Set $\mathbb{Q} = \mathcal{A} = \emptyset$ and goto 2.4.
        2.3.2 Let $\mathbb{Q}_1 \subset \mathbb{Q}$ be the polynomials with the highest class.
        2.3.3 Let $Q \in \mathbb{Q}_1$ be a polynomial whose degree is lowest and initial is of the lowest
              ordering.
        2.3.4 Let $Q = Ix_c^d + U$ such that class$(Q) = c$, deg$(Q) = d$ and init$(Q) = I$.
        2.3.5 If $I = 1$ do
                  Set $\mathbb{R} = \text{prem}(\mathbb{Q}_1, Q)$.
                  If the classes of polynomials in $\mathbb{R}$ are lower than $c$, do
                      $\mathcal{A} = \mathcal{A} \cup \{Q\}$.
                      $\mathbb{Q} = \text{prem}(\mathbb{Q}_1, Q) \cup \{\mathbb{Q} \setminus \mathbb{Q}_1\}$.
                  Else, do
                      $\mathbb{Q} = \text{prem}(\mathbb{Q}_1, Q) \cup \{Q\} \cup \{\mathbb{Q} \setminus \mathbb{Q}_1\}$ and goto 2.3.2.
        2.3.6 Else do
                  Set $Q_1 = x_c^d + I^{q-2}U$ and $\mathbb{Q}_2 = \mathbb{Q}_1 \setminus \{Q\}$.
                  $\mathbb{Q} = \text{prem}(\mathbb{Q}_2, Q_1) \cup \{I^{q-1} - 1\} \cup \{\mathbb{Q} \setminus \mathbb{Q}_1\}$.
                  $\mathbb{P}_1 = \{\mathbb{Q} \setminus \{Q\}\} \cup \mathcal{A} \cup \{I, U\}$.
                  $\mathbb{P}^* = \mathbb{P}^* \cup \{\mathbb{P}_1\}$.
                  Set $\mathbb{R} = \text{prem}(\mathbb{Q}_2, Q_1)$.
                  If the classes of polynomials in $\mathbb{R}$ are lower than $c$, do
                      $\mathcal{A} = \mathcal{A} \cup \{Q_1\}$.
                  Else, do
                      $\mathbb{Q} = \mathbb{Q} \cup \{Q_1\}$. and goto 2.3.2.
    2.4 If $\mathcal{A} \neq \emptyset$, do
        2.4.1 $\mathcal{A}^* := \mathcal{A}^* \cup \{\mathcal{A}\}$.
3 Let $\mathcal{A}^* = \{\mathcal{A}_1, \ldots, \mathcal{A}_q\}$ and $\mathcal{A}_i = \{A_{i1}, \ldots, A_{ip_i}\}$.
4 For $i$ from 1 to $q$ do
    4.1 Set $\mathcal{B} = \emptyset$.
    4.2 For $j$ from 1 to $p_i$ do
        4.2.1 Let class$(A_{ij}) = c_{ij}$ and deg$(A_{ij}) = d_{ij}$.
        4.2.2 $\mathcal{B} = \mathcal{B} \cup \{\text{prem}(x_{c_{ij}}^{q-d_{ij}} A_{ij}, A)\} \neq 0$.
    4.3 If $\mathcal{B} \neq \emptyset$, do
        4.3.1 $\mathbb{P}^* = \mathbb{P}^* \cup \{\mathcal{A}_i \cup \mathcal{B}\}$.
    4.4 Else, do
        4.4.1 Set $\mathcal{C} = \emptyset$.
        4.4.2 For $j$ from 1 to $p_i$ do
                  $\mathcal{C} = \mathcal{C} \cup \{\text{prem}(A_{ij}, \mathcal{C})\}$.
        4.4.3 $\mathcal{C}^* = \mathcal{C}^* \cup \{\mathcal{C}\}$ and $\mathcal{A}^* = \mathcal{A}^* \setminus \{\mathcal{A}_i\}$
5 If $\mathcal{A}^* \neq \emptyset$, do
    5.1 $\mathcal{A}^* := \emptyset$, goto 2. Return $\mathcal{C}^*$
```