J. Symbolic Computation (1993) **16**, 83–114

An Elimination Method for Polynomial Systems

DONGMING WANG

Research Institute for Symbolic Computation

Johannes Kepler University, A-4040 Linz, Austria

(Received September 28, 1992)

We present an elimination method for polynomial systems, in the form of three main algorithms. For any given system $[\mathbb{P},\mathbb{Q}]$ of two sets of multivariate polynomials, one of the algorithms computes a sequence of triangular forms $\mathbb{T}_1,\ldots,\mathbb{T}_e$ and polynomial sets $\mathbb{U}_1,\ldots,\mathbb{U}_e$ such that $\text{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \text{Zero}(\mathbb{T}_i/\mathbb{U}_i)$, where $\text{Zero}(\mathbb{P}/\mathbb{Q})$ denotes the set of common zeros of the polynomials in $\mathbb{P}$ which are not zeros of any polynomial in $\mathbb{Q}$, and similarly for $\text{Zero}(\mathbb{T}_i/\mathbb{U}_i)$. The two other algorithms compute the same zero decomposition but with nicer properties such as $\text{Zero}(\mathbb{T}_i/\mathbb{U}_i) \neq \emptyset$ for each i. One of them, for which the computed triangular systems $[\mathbb{T}_i,\mathbb{U}_i]$ possess the projection property, provides a quantifier elimination procedure for algebraically closed fields. For the other, the computed triangular forms $\mathbb{T}_i$ are irreducible. The relationship between our method and some existing elimination methods is explained. Experimental data for a set of test examples by a draft implementation of the method are provided, and show that the efficiency of our method is comparable with that of some well-known methods. A few encouraging examples are given in detail for illustration.

1. Introduction

The procedures of triangularizing systems of multivariate (differential) polynomials by successively eliminating the variables are called *elimination methods*. The development of elimination methods and their underlying theory has a long history in mathematics. It may be traced back to the Chinese matrix method for linear systems described in *Chiu Chang Suan Shu* early in the first century (cf. Needham, 1959 and Boyer, 1968). This method was further developed by Chinese algebraists, leading to the method of *Thien Yuan* for general polynomial systems in the medieval centuries. Several elimination methods have appeared in the European literature since the 18th century. They include the early methods of Euler (1840) and Bezout, the well known method of Gauss (1873) and the dialytic method of Sylvester (1904). Among these methods, the last was generalized late on as resultant theory by other British mathematicians including Cayley, Macaulay (1916), Hodge & Pedoe (1947) and is for general polynomial systems, while the others are merely for linear systems. Two remarkable elimination methods, one associated with the concept of characteristic sets (Ritt, 1932, 1950, Wu, 1984a, 1986) and the other with Gröbner bases (Buchberger, 1970, 1985), were developed in this century and have received much attention recently in the area of symbolic computation. A fundamental application of elimination methods is to solve systems of polynomial equations, which is of practical

0747–7171/93/020083+32 $08.00/0

importance and has been extensively investigated by many prominent researchers, see Buchberger (1970, 1985), Canny, Kaltofen & Yagati (1989), Grigor'ev & Chistov (1983, 1984), Kalkbrener (1991), Lazard (1979, 1981, 1991, 1992), Sturmfels (1991) and Wu (1986, 1987) for instance.

The purpose of this paper is to present another elimination method for polynomial systems. This method has root in the elimination theory of A. Seidenberg (1956a, 1956b) that seems to be little known up to the present. The goal of Seidenberg was to decide whether a system of (differential) polynomial equations ($=$) and inequations ($\neq$) has a solution in some extension of the ground field. This was motivated from an observation on the relationship between elimination methods and Hilbert's Nullstellensatz. His method was then developed to give a constructive proof of the Nullstellensatz in various cases and to "throw light on the Nullstellensatz". This motivation and goal made Seidenberg put his emphasis mainly on the theory (together with its completeness) without taking real construction into account. Apparently, his method is neither efficient nor quite appropriate for nowaday applications.

Our elimination method incorporates several notable ideas underlying Seidenberg's theory and some ideas form the method of characteristic sets, and it is presented in the form of three main algorithms. For any given system $[\mathbb{P}, \mathbb{Q}]$ of two sets of multivariate polynomials, one of the algorithms either determines that $\text{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$, or computes a sequence of (fine) triangular forms $\mathbb{T}_1, \ldots, \mathbb{T}_e$ and polynomial sets $\mathbb{U}_1, \ldots, \mathbb{U}_e$ such that $\text{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \text{Zero}(\mathbb{T}_i/\mathbb{U}_i)$, where $\text{Zero}(\mathbb{P}/\mathbb{Q})$ denotes the set of common zeros of the polynomials in $\mathbb{P}$ which are not zeros of any polynomial in $\mathbb{Q}$, and similarly for $\text{Zero}(\mathbb{T}_i/\mathbb{U}_i)$. The two other algorithms compute the same zero decomposition but with nicer properties such as $\text{Zero}(\mathbb{T}_i/\mathbb{U}_i) \neq \emptyset$ for each i. One of them, for which the computed triangular systems $[\mathbb{T}_i, \mathbb{U}_i]$ enjoy the *projection property*, provides a quantifier elimination procedure and thus a decision procedure for algebraically closed fields. For the other, the computed triangular forms $\mathbb{T}_i$ are all (quasi-) irreducible.

As Seidenberg's original method, our method, when applied to the solvability problem of systems of polynomial equations and inequations (and thus the membership problem of radical ideals), does not necessarily require polynomial factorization†, and it works for ordinary polynomials, differential polynomials and partial differential polynomials over fields of any characteristic. In the present paper we restrict ourselves to ordinary polynomials over a ground field of characteristic 0. The method for the other cases will be presented in the sequel.

The following sections of the paper are structured as follows. We first introduce some terminologies and notations, followed by three simple lemmas, in Section 2. In Section 3, two main algorithms are described and their termination and correctness are proved. The first algorithm computes the above-mentioned zero decomposition and is structurally simple. This algorithm is modified by embedding the projection process which guarantees the perfectness of the computed triangular systems and provides the quantifier elimination procedure for the elementary theory of algebraically closed fields. The presentation of this second algorithm is somewhat involved. The perfectness of the triangular systems can also be ensured if we use algebraic factorization instead of projection. This is

† This claim is of significance merely in theory. In practice, polynomial factorization can be employed heuristically to reduce the size of the occurring polynomials and to simplify the output. Moreover, polynomial factorization over algebraic extension fields is required when we are concerned with the irreducible decomposition of polynomial systems (cf. Section 4).

elaborated in Section 4, provided with an algorithm for computing the irreducible zero decomposition. Our method can be applied to all such problems that the characteristic set method can, but it has different style, algorithmic structure and efficiency. The similarities and differences between our method and the characteristic set method as well as several other existing ones are explained in Section 5. In the last section, we point out a few details for the implementation of the algorithms and report some experimental data on a set of test examples by a draft implementation of the method in the Maple system. It is shown that our method is very efficient and the extent of its efficiency is at least comparable with that of the methods of characteristic sets and Gröbner bases. A few encouraging examples are also given in detail for illustration.

2. Terminologies, Notations and Lemmas

Let K be a fixed basic field of characteristic 0 and

$$x_1 \prec \cdots \prec x_n,$$

abbreviated sometimes to x, be a set of n variables with the fixed ordering. If $x_i \prec x_j$ (or equivalently $i < j$) we say that x_i is *lower* than x_j or x_j is *higher* than x_i. By a polynomial we shall mean one in the variables $x_1, \ldots, x_n$ with coefficients in K, i.e., an element of the ring $K[x_1, \ldots, x_n]$. For any polynomial P and a variable x_i we denote the degree of P in x_i by $\deg(P, x_i)$. If $P \notin K$ (i.e., it is not a constant), then the leading variable of P, denoted by $\mathrm{lvar}(P)$, is defined as

$$\mathrm{lvar}(P) = \max_{\prec}\{x_i | \deg(P, x_i) \neq 0, 1 \leq i \leq n\},$$

where $\max_{\prec} \Delta$ is the highest element of Δ (with respect to $\prec$), similarly for $\min_{\prec} \Delta$. We define the leading variable of any constant to be x_0 which is $\prec x_1$. If $P \notin K$, the leading coefficient of P with respect to $\mathrm{lvar}(P)$ will be called the *initial* of P, denoted by $\mathrm{ini}(P)$.

Let P be a non-constant polynomial with $x_p = \mathrm{lvar}(P)$, $I = \mathrm{ini}(P)$ and $m = \deg(P, x_p)$. Then P can always be put in the form

$$P = Ix_p^m + P_1 x_p^{m-1} + \cdots + P_m, \quad I, P_i \in K[x_1, \ldots, x_{p-1}].$$

$P_1 x_p^{m-1} + \cdots + P_m$ will be called the *reductum* of P, denoted by $\mathrm{red}(P)$. If Q is any other polynomial, the pseudo-remainder R of Q with respect to P in x_p will be denoted by $\mathrm{prem}(Q, P)$; then we have a remainder formula of the form

$$I^s Q = AP + R,$$

where s is a non-negative integer and A, R are polynomials with $\deg(R, x_p) < \deg(P, x_p)$.

By a polynomial set we mean a finite non-empty set of non-zero polynomials in $K[x_1, \ldots, x_n]$ unless otherwise specified. For any polynomial set $\mathbb{P}$, the set of those polynomials in $\mathbb{P}$ which involve the variables $x_1, \ldots, x_k$ only is denoted by

$$\mathbb{P}^{(k)} = \mathbb{P} \cap K[x_1, \ldots, x_k].$$

Moreover, $\mathbb{P} \setminus \mathbb{P}^{(k)}$ will be denoted by $\mathbb{P}^{[k]}$, so $\mathbb{P}^{(k)} \cup \mathbb{P}^{[k]} = \mathbb{P}$. A polynomial set $\mathbb{P}$ is said to be of *level* k, denoted as $\mathrm{level}(\mathbb{P}) = k$, if $\mathbb{P} \subset K[x_1, \ldots, x_k]$ and $\mathbb{P}^{[k-1]} \neq \emptyset$ (i.e., k is the smallest integer such that $\mathbb{P} \subset K[x_1, \ldots, x_k]$). If $a_1, \ldots, a_k$ are k elements of some extension field of K, then the set of polynomials obtained form $\mathbb{P}$ by substituting $a_1, \ldots, a_k$ respectively for $x_1, \ldots, x_k$ is denoted by

$$\mathbb{P}^{(a,k)} = \mathbb{P}|_{x_1=a_1,\ldots,x_k=a_k}.$$

Throughout the paper, $\tilde{K}$ denotes an algebraic closure of $K[x_1, \ldots, x_n]$. Let $\mathbb{Q}$ be another polynomial set, possibly empty. Then any common zero of the polynomials in $\mathbb{P}$ which is not a zero of any polynomial in $\mathbb{Q}$ is contained in a field which is isomorphic to a subfield of $\tilde{K}$. We denote, by $\tilde{K}$-Zero$(\mathbb{P}/\mathbb{Q})$, the set of all such common zeros, called the *difference set* of common zeros of $\mathbb{P}$ and $\mathbb{Q}$. In other words,

$$\begin{aligned}\tilde{K}\text{-Zero}(\mathbb{P}/\mathbb{Q}) &= \tilde{K}\text{-Zero}(\mathbb{P}) \setminus \tilde{K}\text{-Zero}(\bar{Q}) \\ &= \{x \in \tilde{K} \mid P(x) = 0 \text{ for all } P \in \mathbb{P}, \bar{Q}(x) \neq 0\},\end{aligned}$$

where $\bar{Q} = \prod_{Q \in \mathbb{Q}} Q$. If the field $\tilde{K}$ is not specified, then $\tilde{K}$-Zero$(\mathbb{P}/\mathbb{Q})$ will be simply written as Zero$(\mathbb{P}/\mathbb{Q})$. From now on, while writing Zero$(\mathbb{P}/\mathbb{Q}) \neq \emptyset$ (or Zero$(\mathbb{P}/\mathbb{Q}) = \emptyset$), unless explained otherwise we shall always mean that $\tilde{K}$-Zero$(\mathbb{P}/\mathbb{Q}) \neq \emptyset$ (or $\tilde{K}$-Zero$(\mathbb{P}/\mathbb{Q}) = \emptyset$), that is, the corresponding system of polynomial equations and inequations has a solution (or has no solution) in K. We shall write Zero$(P/\mathbb{Q})$ for Zero$(\{P\}/\mathbb{Q})$ and Zero$(\mathbb{P}/Q)$ for Zero$(\mathbb{P}/\{Q\})$, and write Zero$(\mathbb{P})$ for Zero$(\mathbb{P}/\mathbb{Q})$ when $\mathbb{Q} = \emptyset$ or all elements of $\mathbb{Q}$ are constants.

REMARK 1. It is easy to see that, for any polynomial sets $\mathbb{H}, \mathbb{P}_i, \mathbb{Q}_i$, if Zero$(\mathbb{P}/\mathbb{Q}) = \bigcup_i$ Zero$(\mathbb{P}_i/\mathbb{Q}_i)$, then Zero$(\mathbb{P} \cup \mathbb{H}/\mathbb{Q}) = \bigcup_i$ Zero$(\mathbb{P}_i \cup \mathbb{H}/\mathbb{Q}_i)$ and Zero$(\mathbb{P}/\mathbb{Q} \cup \mathbb{H}) = \bigcup_i$ Zero$(\mathbb{P}_i/\mathbb{Q}_i \cup \mathbb{H})$. ∎

By a *polynomial system* we mean a pair $[\mathbb{P}, \mathbb{Q}]$ of polynomial sets with which the zero set Zero$(\mathbb{P}/\mathbb{Q})$ is concerned, where $\mathbb{Q}$ may be empty. As a convention, a zero of the polynomial system $[\mathbb{P}, \mathbb{Q}]$ will be meant an element of the set Zero$(\mathbb{P}/\mathbb{Q})$. In other words, we are concerned with the solutions of a system of polynomial equations $\mathbb{P} = 0$ and inequations $\mathbb{Q} \neq 0$. The level of $\mathbb{P}$ will also be called the *level* of the polynomial system $[\mathbb{P}, \mathbb{Q}]$.

In what follows, we shall use a *list* for an ordered set and form it by putting its elements into a pair of square brackets. In particular, ϕ and $\emptyset$ stand respectively for *empty list* and *empty set*. All operations of sets are applied to the considered lists in the usual way except for preserving the order. For example, $[b, a] \cup [c]$ is equal to $[b, a, c]$, but neither to $[a, b, c]$ nor to $[a, c, b]$. For a list L, the number of elements of L is also called the *length* of L, denoted by length(L). In case $L \neq \phi$, the first term of L will be denoted by first(L). For a non-empty set S, we define a function **aef**(S) which takes an arbitrary element from S.

DEFINITION 1. *A finite non-empty list*

$$\mathbb{T}: \quad [T_1, T_2, \ldots, T_r]$$

of non-constant polynomials is called a triangular form *(or* triangular list*) if*

$$\text{lvar}(T_1) \prec \text{lvar}(T_2) \prec \cdots \prec \text{lvar}(T_r).$$

A triangular form $\mathbb{T}$ *with* $I_i = \text{ini}(T_i)$ *is said to be* fine *if either* $r = 1$, *or* $r > 1$ *while* $\text{prem}(\cdots \text{prem}(I_i, T_{i-1}), \ldots, T_1) \neq 0$ *for* $i = 2, \ldots, r$. *It is said to be* perfect *if* Zero$(\mathbb{T}/\{I_1, \ldots, I_r\}) \neq \emptyset$.

For example, the triangular form $\mathbb{T} = [x_1^2 - 2, x_2^2 - 2x_1x_2 + 2, (x_2 - x_1)x_3 + 1]$ is fine but not perfect because any zero of the first two polynomials of $\mathbb{T}$ vanishes the initial $x_2 - x_1$ of the third polynomial (actually, Zero$(\mathbb{T}) = \emptyset$), whereas the triangular form $[x_1^2 - 1, (x_1^3 - 1)x_2 + 1]$ is perfect. It is easy to show that any perfect triangular form is fine.

Let Q be any polynomial and $\mathbb{T} = [T_1, \ldots, T_r]$ be a triangular form. Q is said to be *reduced* with respect to $\mathbb{T}$ if $\deg(Q, \mathrm{lvar}(T_i)) < \deg(T_i, \mathrm{lvar}(T_i))$ for all i. The polynomial $\mathrm{prem}(\cdots \mathrm{prem}(Q, T_r), \ldots, T_1)$, denoted simply by $\mathrm{prem}(G, \mathbb{T})$, will be called the *pseudo-remainder* (or *remainder* for short) of Q with respect to $\mathbb{T}$. If Q is reduced with respect to $\mathbb{T}$, then clearly $\mathrm{prem}(Q, \mathbb{T}) = Q$. For a polynomial set $\mathbb{Q}$, $\mathrm{prem}(\mathbb{Q}, T_i)$ stands for $\{\mathrm{prem}(Q, T_i) | \ Q \in \mathbb{Q}\}$ and $\mathrm{prem}(\mathbb{Q}, \mathbb{T})$ for $\{\mathrm{prem}(Q, \mathbb{T}) | \ Q \in \mathbb{Q}\}$.

DEFINITION 2. *A* triangular system *is a pair* $[\mathbb{T}, \mathbb{U}]$ *in which* $\mathbb{T}$ *is a triangular form and* $\mathbb{U}$ *is a polynomial set, possibly empty, such that* $\mathrm{Zero}(\mathrm{ini}(T)) \cap \mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \emptyset$ *for all* $T \in \mathbb{T}$. *A triangular system* $[\mathbb{T}, \mathbb{U}]$ *is said to be* fine *if* $0 \notin \mathrm{prem}(\mathbb{U}, \mathbb{T})$. *It is said to be* perfect *if* $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) \neq \emptyset$.

It is easy to see that if $[\mathbb{T}, \mathbb{U}]$ is a perfect triangular system, then $\mathbb{T}$ is a perfect triangular form. Moreover, if $[\mathbb{T}, \mathbb{U}]$ is a fine triangular system, then either $\mathbb{T}$ is a fine triangular form or $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \emptyset$.

In the remaining part of this section we recall a few simple lemmas which are fundamental for the correctness proof of our main algorithms in the following sections. The proofs of these lemmas are given in Appendix A of Wang (1993).

LEMMA 1. *Let* T *be a non-constant polynomial with* $\mathrm{ini}(T) = I$, $[\mathbb{P}, \mathbb{Q}]$ *be a polynomial system and* $\mathbb{R}$ *be the set of all non-zero remainders of the polynomials in* $\mathbb{P}$ *with respect to* T *(i.e.,* $\mathbb{R} = \mathrm{prem}(\mathbb{P}, T) \setminus \{0\}$*). Then*

$$\mathrm{Zero}(\mathbb{P} \cup \{T\}/\mathbb{Q}) = \mathrm{Zero}(\mathbb{R} \cup \{T\}/\mathbb{Q} \cup \{I\}) \cup \mathrm{Zero}(\mathbb{P} \cup \{I, \mathrm{red}(T)\}/\mathbb{Q}). \quad (2.1)$$

LEMMA 2.† *Let* $[\mathbb{P}, \mathbb{Q}]$ *be a polynomial system of level* $\leq i$, *where* $\mathbb{P}$ *is possibly empty. Suppose that* $\mathbb{Q}^{[i]} \neq \emptyset$ *and let* $H_1, \ldots, H_h$ *be all the polynomials in* $\mathbb{Q}^{[i]}$. *Let* $H_{l1}, \ldots, H_{lm_l}$ *be all the non-zero coefficients of the power products in* H_l *with respect to those variables which are* $\succ x_i$. *Then*

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) \neq \emptyset \Longleftrightarrow \bigcup_{1 \leq j_1 \leq m_1, \ldots, 1 \leq j_h \leq m_h} \mathrm{Zero}(\mathbb{P}/\mathbb{Q}_{j_1 \cdots j_h}) \neq \emptyset, \quad (2.2)$$

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{1 \leq j_1 \leq m_1, \ldots, 1 \leq j_h \leq m_h} \mathrm{Zero}(\mathbb{P}/\mathbb{Q}'_{j_1 \cdots j_h}), \quad (2.3)$$

where $\mathbb{Q}_{j_1 \cdots j_h} = \mathbb{Q}^{(i)} \cup \{H_{1j_1}, \ldots, H_{hj_h}\}$ *and* $\mathbb{Q}'_{j_1 \cdots j_h} = \mathbb{Q} \cup \{H_{1j_1}, \ldots, H_{hj_h}\}$.

LEMMA 3. *Let* T *be a non-constant polynomial with* $\mathrm{lvar}(T) = x_i$, $\mathrm{ini}(T) = I$ *and* $\deg(T, x_i) = d$, *and* $[\mathbb{P}, \mathbb{Q}]$ *be a polynomial system of level* $\leq i - 1$ *with* $\mathrm{level}(\mathbb{Q}) \leq i$.

a) If $\mathbb{Q}^{[i-1]} = \emptyset$, *then*

$$\mathrm{Zero}(\mathbb{P} \cup \{T\}/\mathbb{Q} \cup \{I\}) \neq \emptyset \Longleftrightarrow \mathrm{Zero}(\mathbb{P}/\mathbb{Q} \cup \{I\}) \neq \emptyset. \quad (2.4)$$

b) Suppose that $\mathbb{Q}^{[i-1]} \neq \emptyset$ *and let* $H_1, \ldots, H_h$ *be all the polynomials in* $\mathbb{Q}^{[i-1]}$. *Let*

† The zero relations (2.2) and (2.3) in this lemma can be complicated by replacing $\mathbb{P}$ in the right-hand side with $\mathbb{P} \cup \mathbb{H}_{j_1 \cdots j_h}$, where $\mathbb{H}_{j_1 \cdots j_h} = \{H_{lj} | \ 0 \leq j \leq j_l - 1, 1 \leq l \leq h\} \setminus \{0\}$ and $H_{l0} = 0$ for $l = 1, \ldots, h$. This is considered of practical interest because the more polynomials in the system easier the elimination is, in particular, when the system has no zero. This modification of the zero relations would lead the subalgorithm PROJECT_A described in the next section to a complicated version. See Wang (1993) for details.

$R = \text{prem}((H_1 \cdots H_h)^d, T)$ *and* $\mathbb{Q}' = \mathbb{Q}^{(i-1)} \cup \{I, R\}$. *Then*

$$\text{Zero}(\mathbb{P} \cup \{T\}/\mathbb{Q} \cup \{I\}) \neq \emptyset \Longleftrightarrow \text{Zero}(\mathbb{P}/\mathbb{Q}') \neq \emptyset, \tag{2.5}$$

$$\text{Zero}(\mathbb{P} \cup \{T\}/\mathbb{Q} \cup \{I\}) = \text{Zero}(\mathbb{P} \cup \{T\}/\mathbb{Q}'). \tag{2.6}$$

REMARK 2. Referring to (2.2), for any indices $j_1, \ldots, j_h$ and any $(a_1, \ldots, a_i) \in \text{Zero}(\mathbb{P}/\mathbb{Q}_{j_1 \cdots j_h})$, there are in fact some $a_{i+1}, \ldots, a_n \in \tilde{K}$ such that $(a_1, \ldots, a_n) \in \text{Zero}(\mathbb{P}/\mathbb{Q})$. Referring to (2.5), for any $(a_1, \ldots, a_{i-1}) \in \text{Zero}(\mathbb{P}/\mathbb{Q}')$,† there is an $a_i \in \tilde{K}$ such that $(a_1, \ldots, a_i) \in \text{Zero}(\mathbb{P} \cup \{T\}/\mathbb{Q} \cup \{I\})$. See the proofs of (2.2) and (2.5) in Wang (1993). ■

We end this section by defining two simple data structures *triplet* and *quadruplet* which will be throughout used in our presentation of the algorithms.

DATA STRUCTURE. *A* triplet *of level* i $(1 \leq i \leq n)$ *is a list* $[\mathbb{P}, \mathbb{Q}, \mathbb{T}]$ *of three elements, where*

a) $[\mathbb{P}, \mathbb{Q}]$ *is a polynomial system of level* i,

b) $\mathbb{T}$, *if non-empty, is a triangular form with* $\mathbb{T}^{(i)} = \phi$.

A quadruplet *of level* i *is a list* $[\mathbb{P}, \mathbb{Q}, \mathbb{T}, \mathbb{U}]$ *of four elements such that a) and b) above are satisfied and*

c) $\text{level}(\mathbb{Q}) = q \leq p$ *and* $\mathbb{U}$ *is a polynomial set with* $\mathbb{U}^{(q)} = \emptyset$, *where* p *is the index of* $\text{lvar}(\text{first}(\mathbb{T}))$ *if* $\mathbb{T} \neq \phi$, *and* n *otherwise.*

The motivation and reason for introducing these data structures are explained as follows. When introducing the notion of a polynomial system $[\mathbb{P}^*, \mathbb{Q}^*]$, we are concerned with the zero set $\text{Zero}(\mathbb{P}^*/\mathbb{Q}^*)$. We may write $\mathbb{P}^* = \mathbb{P}^{*(i)} \cup \mathbb{P}^{*[i]}$ for every i. Suppose that, for some i, $\mathbb{P}^{*(i)}$, renamed $\mathbb{P}$, is of level i and that $\mathbb{P}^{*[i]}$, put in the form of a list $\mathbb{T}$ with increasing leading variables, is already in triangular form. Then $[\mathbb{P}, \mathbb{Q}^*, \mathbb{T}]$ is a triplet with which the zero set $\text{Zero}(\mathbb{P} \cup \mathbb{T}/\mathbb{Q}^*)$ is concerned.

We may also write $\mathbb{Q}^* = \mathbb{Q}^{*(q)} \cup \mathbb{Q}^{*[q]}$ for some q (say, $= \text{level}(\mathbb{Q}^{*(q)}) \leq p$) and let $\mathbb{Q} = \mathbb{Q}^{*(q)}$ and $\mathbb{U} = \mathbb{Q}^{*[q]}$. Then, $[\mathbb{P}, \mathbb{Q}, \mathbb{T}, \mathbb{U}]$ is a quadruplet with which the zero set $\text{Zero}(\mathbb{P} \cup \mathbb{T}/\mathbb{Q} \cup \mathbb{U})$ is concerned.

Our elimination procedures will start with a triplet $[\mathbb{P}, \mathbb{Q}, \mathbb{T}]$ or a quadruplet $[\mathbb{P}, \mathbb{Q}, \mathbb{T}, \mathbb{U}]$ with $\mathbb{T} = \phi$ and $\mathbb{U} = \emptyset$. The variables x_i are eliminated and the obtained, triangularized polynomials are adjoined to $\mathbb{T}$ (and to $\mathbb{U}$) successively for $i = n, n-1, \ldots, 1$.

3. Elimination Algorithms with and without Projection

In this section we describe two algorithms for decomposing any polynomial system into triangular systems. The second algorithm provides the quantifier elimination procedure for algebraically closed fields. There are three basic ideas which underlie the main algorithms and their subalgorithms: (i) performing the elimination top-down, (ii) splitting the polynomial system whenever pseudo-division is performed, and (iii) preserving the existence of zeros of the given system for the disjunction of the eliminated systems by projection.

† Here, $\mathbb{Q}'$ may be of level i. In that case, for a polynomial $Q = Q(x_1, \ldots, x_i) \in \mathbb{Q}'$, $(a_1, \ldots, a_{i-1}) \notin \text{Zero}(Q)$ means that $Q(a_1, \ldots, a_{i-1}, x_i) \not\equiv 0$.

The main functionality of the subalgorithm ELIMINATE below is to eliminate the variable x_i for a polynomial set of level i, so that after the elimination only one polynomial has leading variable x_i. This is done recursively among the polynomials whose leading variables are x_i by pseudo-dividing those of higher degree with one of minimal degree in x_i. Whenever pseudo-division is performed, the initial of the dividing polynomial is assumed to be non-zero, while the case in which the initial happens to be 0 is considered disjunctively by replacing the corresponding polynomial with its initial and reductum.

SUBALGORITHM ELIMINATE: $[T, \mathbb{P}', \mathbb{Q}', \Delta] \leftarrow$ ELIMINATE$(\mathbb{P}, \mathbb{Q}, i)$. *Given an integer* $i > 0$ *and a polynomial system* $[\mathbb{P}, \mathbb{Q}]$ *of level* i, *this algorithm computes a polynomial* T *with* $\mathrm{lvar}(T) = x_i$, *a polynomial system* $[\mathbb{P}', \mathbb{Q}']$ *of level* $\leq i-1$ *and a set* Δ *of polynomial systems of level* $\leq i$ *such that*

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \mathrm{Zero}(\mathbb{P}' \cup \{T\}/\mathbb{Q}') \cup \bigcup_{[\mathbb{P}^*, \mathbb{Q}^*] \in \Delta} \mathrm{Zero}(\mathbb{P}^*/\mathbb{Q}^*). \tag{3.1}$$

E1. Set $T \leftarrow 0$, $\mathbb{P}' \leftarrow \mathbb{P}$, $\mathbb{Q}' \leftarrow \mathbb{Q}$, $\Delta \leftarrow \emptyset$.
E2. While $\mathbb{P}'^{[i-1]} \neq \{T\}$ do:

E2.1. Let T be an element of $\mathbb{P}'^{[i-1]}$ with minimal degree in x_i.
E2.2. Set $\Delta \leftarrow \Delta \cup \{[(\mathbb{P}' \setminus \{T\}) \cup \{\mathrm{red}(T), \mathrm{ini}(T)\}, \mathbb{Q}']\}$, $\mathbb{Q}' \leftarrow \mathbb{Q}' \cup \{\mathrm{ini}(T)\}$.
E2.3. Compute $\mathbb{P}' \leftarrow \{T\} \cup \mathit{prem}(\mathbb{P}', T) \setminus \{0\}$.

E3. Set $\mathbb{P}' \leftarrow \mathbb{P}' \setminus \{T\}$.

PROOF. Since $\mathbb{P}$ is of level i, initially $\mathbb{P}'^{[i-1]}$ is neither empty nor equal to $\{T\} = \{0\}$. We see clearly that every substep of E2 terminates. As in each iteration of this while-loop $\deg(T, x_i)$ decreases at least by 1, after a finite number of steps all the non-zero remainders of the polynomials in $\mathbb{P}'$ with respect to T will have leading variables $\prec x_i$. Then the set $\mathbb{P}'^{[i-1]}$ becomes $\{T\}$ and the while-loop terminates.

The zero relation (3.1) follows from repeated application of the relation (2.1) in Lemma 1. ∎

Note that step E2.2 can be skipped when $\mathrm{ini}(T)$ is a constant, and the remainders need be computed in step E2.3 actually only for the polynomials in $\mathbb{P}'^{[i-1]} \setminus \{T\}$.

EXAMPLE 1A. We use the following set

$$\mathbb{P} = \{x^{31} - x^6 - x - y, x^8 - z, x^{10} - t\}$$

of 3 polynomials to illustrate our algorithms throughout the paper. The polynomials are taken from a paper by Traverso and Donati (Proc. ISSAC'89, 192-198) on the experimentation of Gröbner bases. We fix the order of the variables as $t \prec z \prec y \prec x$.

To see how ELIMINATE works, we consider the polynomial system $[\mathbb{P}, \emptyset]$ of level 4 as input. Initially, set $T \leftarrow 0, \mathbb{P}' \leftarrow \mathbb{P}, \mathbb{Q}' \leftarrow \emptyset$ and $\Delta \leftarrow \emptyset$ in step E1.

Now we come to the while-loop. First, take $T = x^8 - z$ from $\mathbb{P}'^{[3]} = \mathbb{P}'$ in step E2.1 which has minimal degree 8 in x and initial $I = 1$. Since I is a constant, we can skip step E2.2. Pseudo-dividing the polynomials $x^{31} - x^6 - x - y$ and $x^{10} - t$ in $\mathbb{P}'$ by T, we get two non-zero remainders

$$R_1 = z^3x^7 - x^6 - x - y, \quad R_2 = zx^2 - t,$$

where $\mathrm{lvar}(R_1) = \mathrm{lvar}(R_2) = x$. So in step E2.3, update $\mathbb{P}' \leftarrow \{T, R_1, R_2\}$.

For the second loop, take $T = R_2$ from $\mathbb{P}'^{[3]} = \mathbb{P}'$ in step E2.1 which has minimal degree 2 in x and initial $I = z$. In step E2.2, set $\Delta \leftarrow \{[\{x^8 - z, R_1, z, -t\}, \emptyset]\}$ and $\mathbb{Q} \leftarrow \{z\}$. Similarly, pseudo-dividing the two other polynomials in $\mathbb{P}'$ by $T = R_2$ we get the remainders

$$R_3 = -z^5 + t^4, \quad R_4 = -z^3x - yz^3 + xt^3z^3 - t^3$$

with $\mathrm{lvar}(R_3) = z$ and $\mathrm{lvar}(R_4) = x$. Then set $\mathbb{P}' \leftarrow \{R_2, R_3, R_4\}$ in step E2.3.

For the third loop, set $T \leftarrow R_4$ in step E2.1, where $\deg(R_4, x) = 1 < \deg(R_2, x)$ and the initial $t^3z^3 - z^3$ of R_4 is simplified by $z \in \mathbb{Q}$ to $I = t^3 - 1$. In step E2.2 the polynomial system $[\{R_2, R_3, -z^3y - t^3, t^3 - 1\}, \{z\}]$ is added to Δ and $t^3 - 1$ to $\mathbb{Q}$. Pseudo-dividing R_2 by $T = R_4$, we have

$$R_5 = \mathrm{prem}(R_2, R_4) = -z^5t + 2z^5t^4 - t^7z^5 + y^2z^6 + 2yz^3t^3 + t^6$$

with $\mathrm{lvar}(R_5) = y$. Finally, set $\mathbb{P}' \leftarrow \{R_4, R_3, R_5\}$ and the while-loop terminates.

The algorithm terminates after deleting T from $\mathbb{P}'$ in step E3. The output consists of $T = R_4$, the polynomial system $[\mathbb{P}', \mathbb{Q}'] = [\{R_3, R_5\}, \{z, t^3 - 1\}]$ and the set Δ of 2 other polynomial systems. ■

ALGORITHM TRIANGULARIZE: $\Psi \leftarrow$TRIANGULARIZE$(\mathbb{P}, \mathbb{Q})$. *Given a polynomial system* $[\mathbb{P}, \mathbb{Q}]$, *this algorithm computes a set* Ψ *which is either empty, that means* $\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$, *or of the form* $\{[\mathbb{T}_1, \mathbb{U}_1], \ldots, [\mathbb{T}_e, \mathbb{U}_e]\}$ *such that*

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i), \tag{3.2}$$

where each $[\mathbb{T}_i, \mathbb{U}_i]$ *is a fine triangular system.*

T1. Set $\Psi \leftarrow \emptyset$, $\Phi \leftarrow \{[\mathbb{P}, \mathbb{Q}, \phi]\}$.
T2. While $\Phi \neq \emptyset$ do:

T2.1. Set $[\mathbb{P}', \mathbb{Q}', \mathbb{T}'] \leftarrow \mathrm{aef}(\Phi)$, $\Phi \leftarrow \Phi \setminus \{[\mathbb{P}', \mathbb{Q}', \mathbb{T}']\}$, $m \leftarrow \mathrm{level}(\mathbb{P}')$.
T2.2. For $i = m, \ldots, 1$ do:

T2.2.1. If $\mathbb{P}' \cap K \neq \emptyset$ then go to T2. If $\mathrm{level}(\mathbb{P}') < i$ then go to T2.2 for next i.
T2.2.2. [Elimination for x_i.] Compute $[T, \mathbb{P}', \mathbb{Q}', \Delta] \leftarrow$ELIMINATE$(\mathbb{P}', \mathbb{Q}', i)$ and set $\Phi \leftarrow \Phi \cup \{\delta \cup [\mathbb{T}'] \mid \delta \in \Delta\}$.
T2.2.3. [Reduction.] Compute $\mathbb{Q}' \leftarrow \mathrm{prem}(\mathbb{Q}', T)$.
T2.2.4. If $0 \in \mathbb{Q}'$ then go to T2 else set $\mathbb{T}' \leftarrow [T] \cup \mathbb{T}'$.

T2.3. Set $\Psi \leftarrow \Psi \cup \{[\mathbb{T}', \mathbb{Q}']\}$.

In step T2 of this algorithm, the set Φ of triplets increases and decreases, and meanwhile the triangular systems $[\mathbb{T}', \mathbb{Q}']$ are produced. This procedure terminates when the set Φ becomes empty. Within the while-loop, for each triplet $[\mathbb{P}', \mathbb{Q}', \mathbb{T}']$ of level m taken from Φ the variables are eliminated, successively from x_m to x_1, by the subalgorithm ELIMINATE.

EXAMPLE 1B. Let us recall Example 1a and illustrate the algorithm TRIANGULARIZE with the input system $[\mathbb{P}, \emptyset]$. The sets Ψ and Φ are initially set to $\emptyset$ and $\{[\mathbb{P}, \emptyset, \phi]\}$, respectively.

Now consider the while-loop. First, the only triplet in Φ is taken and deleted from Φ in step T2.1. In step T2.2, first iterate for $i = 4$. Calling the subalgorithm ELIMINATE in step

T2.2.2 yields the polynomial $T = R_4$, the polynomial system $[\mathbb{P}', \mathbb{Q}'] = [\{R_3, R_5\}, \{z, t^3 - 1\}]$ and the set Δ as given in Example 1a. Then, two triplets are formed from the two polynomial systems of Δ and are added to Φ.

Since the two polynomials in $\mathbb{Q}'$ have leading variables $\prec x$, the execution of step T2.2.3 is trivial and does not update the value of any variable. In step T2.2.4, set $\mathbb{T} \leftarrow [R_4]$.

For $i = 3$ and 2, the polynomials R_5 and R_3 in $\mathbb{P}'$ are chosen as T in step T2.2.2, respectively, and no elimination is necessary. Since the remainders of the two polynomials in $\mathbb{Q}'$ with respect to R_5 and R_3 are themselves, $\mathbb{Q}'$ is not updated in step T2.2.3. Therefore, we obtain the first triangular system $[\mathbb{T}_1, \mathbb{U}_1]$ with $\mathbb{T}_1 = [R_3, R_5, R_4]$ and $\mathbb{U}_1 = \{z, t^3 - 1\}$, which is added to Ψ in step T2.3.

Now there are two triplets in Φ which remain to be further considered. For the first $[\{T, R_1, z, -t\}, \emptyset, \phi]$, the two polynomials T, R_1 have leading variable x, of which R_1 has lower degree 7 and initial $z^3 \sim z$. We may split the computation to two cases according as $z = 0$ and $z \neq 0$ by strictly following the described algorithm, which is somewhat complicated. Actually, we may simplify T and R_1 by z and $-t$, as in our implementation, and make the obtained polynomials power-freed. Then we immediately get a triangular form $\mathbb{T}_2 = [-t, z, y, x]$ with $\mathbb{U}_2 = \emptyset$. For the second triplet $[\mathbb{P}', \mathbb{Q}', \mathbb{T}'] = [\{R_3, R_2, -z^3y - t^3, t^3 - 1\}, \{z\}, \phi]$, the polynomials $R_2, -z^3y - t^3, R_3, t^3 - 1$ have leading variables x, y, z, t, respectively, and thus already constitute a triangular form. Hence, we obtain $\mathbb{T}_3 = [t^3 - 1, R_3, -z^3y - t^3, R_2]$ and $\mathbb{U}_3 = \{z\}$. ∎

PROOF OF THE TERMINATION AND CORRECTNESS OF TRIANGULARIZE. For the termination of the algorithm TRIANGULARIZE, we only need to prove that the while-loop terminates. Now, for any triplet ψ taken from Ψ in step T2.1 of TRIANGULARIZE, let $\mathbb{P}'$ be the first component of ψ and $\mathbb{P}^*$ be the first component of some polynomial system in the Δ produced by ELIMINATE from ψ. Then, from the replacement of the polynomial T by its initial and reductum in step E2.2 of ELIMINATE we see clearly that either $\text{level}(\mathbb{P}^*) < \text{level}(\mathbb{P}')$, or $\text{level}(\mathbb{P}^*) = \text{level}(\mathbb{P}') = m$ while the minimal degree in x_m of the polynomials in $\mathbb{P}^{*[m-1]}$ is less than that of the polynomials in $\mathbb{P}'^{[m-1]}$. Since both the level and the minimal degree are positive integers, any steadily decreasing sequence of levels or minimal degrees is finite. Therefore, the while-loop can only have a finite number of iterations. This proves the termination of TRIANGULARIZE.

We view the algorithm TRIANGULARIZE as for computing a multi-branch tree† $\mathfrak{T}$ starting from its root with which the triplet $[\mathbb{P}, \mathbb{Q}, \phi]$ is associated. With each node or leaf i of $\mathfrak{T}$, a triplet $[\mathbb{P}_i, \mathbb{Q}_i, \mathbb{T}_i]$ is associated such that after the execution of every step‡ of TRIANGULARIZE the zero relation

$$\text{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i \text{ over all leaves of } \mathfrak{T}} \text{Zero}(\mathbb{P}_i \cup \mathbb{T}_i/\mathbb{Q}_i) \tag{3.3}$$

is preserved. This is because, according to Remark 1 in Section 2, the relation (3.1) implies that

$$\text{Zero}(\mathbb{P} \cup \mathbb{T}'/\mathbb{Q}) = \text{Zero}(\mathbb{P}' \cup \{T\} \cup \mathbb{T}'/\mathbb{Q}') \cup \bigcup_{[\mathbb{P}^*, \mathbb{Q}^*] \in \Delta} \text{Zero}(\mathbb{P}^* \cup \mathbb{T}'/\mathbb{Q}^*) \tag{3.1'}$$

† The algorithms of computing the decomposition tree in this paper are the depth-first ones. After knowing the basic strategies of our method, one can design the corresponding breadth-first algorithms without essential difficulty.

‡ *For steps T2.2.2 and T2.2.3, the polynomial T is taken into account of the triplet in process.* Namely, $\mathbb{P}_i$ corresponds to $\mathbb{P}' \cup \{T\}$.

for any $\mathbb{T}'$, and because $\text{Zero}(\mathbb{P}' \cup \{T\} \cup \mathbb{T}'/\mathbb{Q}')$ remains unchanged when step T2.2.3 is executed. The branches are generated clearly by the subalgorithm ELIMINATE with the zero relation (3.1) and thus (3.1') above preserved. We can of course cut those leaves i for which $\mathbb{P}_i$ contains a non-zero constant or $\mathbb{Q}_j$ contains 0 at any time. If all the leaves are cut off, then $\text{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$. Otherwise, when the algorithm terminates, $\mathbb{P}_i$ is empty for every leaf i of $\mathfrak{T}$ and we obtain the corresponding pair $[\mathbb{T}_i, \mathbb{U}_i] = [\mathbb{T}_i, \mathbb{Q}_i]$. Then the zero decomposition (3.3) has the form (3.2).

Next we show that each $[\mathbb{T}_i, \mathbb{U}_i]$ is a fine triangular system, i.e., $\text{Zero}(\text{ini}(T)) \cap \text{Zero}(\mathbb{T}_i/\mathbb{U}_i) = \emptyset$ for every $T \in \mathbb{T}_i$ and $0 \notin \text{prem}(\mathbb{U}_i, \mathbb{T}_i)$. Let $\mathbb{T}_i = [T_1, \ldots, T_r]$ with $\text{ini}(T_j) = I_j$ and $\text{lvar}(T_j) = x_{p_j}$. One sees that each I_j is adjoined in step E2.2 of ELIMINATE to the set $\mathbb{Q}'$. Since $\text{lvar}(I_j) \prec x_{p_j}$, I_j remains in $\mathbb{Q}'$ after the execution of T2.2.3 and T2.2.4 for the iteration $i = p_j$. In the next iteration $i = p_{j-1}$, I_j will be replaced by its remainder (which is non-zero, for otherwise this leaf is cut away) with respect to T_{j-1}. This remainder will further be replaced by its non-zero remainder with respect to T_{j-2} in th iteration $i = p_{j-2}$, and so on. Therefore, $\text{prem}(I_j, \mathbb{T}_i) = \text{prem}(I_j, [T_1, \ldots, T_{j-1}])$ is contained in $\mathbb{U}_i$ for all j. From the remainder formula, we know that any zero of I_j which is also a zero of $\mathbb{T}_i$ must be a zero of $\text{prem}(I_j, \mathbb{T}_i) \in \mathbb{U}_i$. Hence, $\text{Zero}(I_j) \cap \text{Zero}(\mathbb{T}_i/\mathbb{U}_i) = \emptyset$ for every j.

Since all the polynomials in $\mathbb{U}_i$ are actually the non-zero remainders of some initials of polynomials with respect to $\mathbb{T}_i$, we see that $0 \notin \text{prem}(\mathbb{U}_i, \mathbb{T}_i)$ for every i. Therefore, each $[\mathbb{T}_i, \mathbb{U}_i]$ is a fine triangular system and the proof is complete. ■

The algorithm TRIANGULARIZE implements the first two ideas mentioned at the beginning of this section. It is structurally simple and practically effective. However, in comparison with other methods (see Section 5) there are two essential issues which should be addressed. First, the fine triangular systems computed by TRIANGULARIZE are not necessarily perfect. That is, a triangular system having no zero is not necessarily detected. This issue is to be treated by embedding the so-called *projection* into TRIANGULARIZE in the remainder of this section and by irreducible decomposition in the next section. Secondly, the second component of a triangular system computed by TRIANGULARIZE may contain many polynomials, which increases the solution size of the problem. Fortunately, this drawback will disappear when an irreducible decomposition is reached.

The main objective of projection is explained as follows. Let a polynomial system $[\mathbb{P}, \mathbb{Q}]$ in the variables $x_1, \ldots, x_n$ be given. We want to eliminate the variables $x_n, \ldots, x_{k+1}$ $(0 \leq k < n)$ and to obtain finitely many other polynomial systems $[\mathbb{P}_1, \mathbb{Q}_1], \ldots, [\mathbb{P}_e, \mathbb{Q}_e]$ in the variables $x_1, \ldots, x_k$ such that $\text{Zero}(\mathbb{P}/\mathbb{Q}) \neq \emptyset$ if and only if $\bigcup_{i=1}^{e} \text{Zero}(\mathbb{P}_i/\mathbb{Q}_i) \neq \emptyset$. We also wish that for any $(a_1, \ldots, a_k) \in \bigcup_{i=1}^{e} \text{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$ there exist $a_{k+1}, \ldots, a_n \in \bar{K}$ such that $(a_1, \ldots, a_n) \in \text{Zero}(\mathbb{P}/\mathbb{Q})$. An elimination procedure only meeting these two requirements is relatively simple. However, the algorithm presented later in this section is somewhat involved mainly because we also want to establish the zero relation between the given system and the eliminated (triangular) systems.

The subalgorithm PROJECT_A below, which is an implementation of Lemma 2, splits the polynomial system $[\mathbb{P}, \mathbb{Q}]$ by projection into a set of subsystems, of which one is separated as $[\mathbb{P}, \mathbb{Q}', \mathbb{T}, \mathbb{U}']$ (in step P2.4) and the others are put in Δ. Those polynomials corresponding to the $H_1, \ldots, H_h$ in Lemma 2 are moved from $\mathbb{Q}$ to $\mathbb{U}$ (and will be finally put together with the polynomials in the corresponding $\mathbb{Q}$), forming the new sets $\mathbb{Q}'$ and $\mathbb{U}'$ (in step P1).

SUBALGORITHM PROJECT_A: $[\mathbb{Q}', \mathbb{U}', \Theta] \leftarrow$PROJECT_A$(\mathbb{P}, \mathbb{Q}, \mathbb{T}, \mathbb{U}, i)$. *Given an integer* $i > 0$ *and a quadruplet* $[\mathbb{P}, \mathbb{Q}, \mathbb{T}, \mathbb{U}]$ *of level* i, *this algorithm computes a polynomial set* $\mathbb{Q}'$ *of level* $\leq i$, *a polynomial set* $\mathbb{U}'$ *with* $\mathbb{U}'^{(i)} = \emptyset$ *and a set* Θ *of quadruplets of level* i *such that*

$$\text{Zero}(\mathbb{P}/\mathbb{Q}) \neq \emptyset \Longleftrightarrow \text{Zero}(\mathbb{P}/\mathbb{Q}') \cup \bigcup_{[\mathbb{P},\mathbb{Q}^*,\mathbb{T},\mathbb{U}^*]\in\Theta} \text{Zero}(\mathbb{P}/\mathbb{Q}^*) \neq \emptyset, \tag{3.4}$$

$$\text{Zero}(\mathbb{P}/\mathbb{Q}) = \text{Zero}(\mathbb{P}/\mathbb{Q}' \cup \mathbb{Q}^{[i]}) \cup \bigcup_{[\mathbb{P},\mathbb{Q}^*,\mathbb{T},\mathbb{U}^*]\in\Theta} \text{Zero}(\mathbb{P}/\mathbb{Q}^* \cup \mathbb{Q}^{[i]}), \tag{3.5}$$

where $\mathbb{U}' = \mathbb{U} \cup \mathbb{Q}^{[i]}$ *and* $\text{level}(\mathbb{Q}^*) \leq i$.

P1. Set $\mathbb{Q}' \leftarrow \mathbb{Q}^{(i)}$, $\mathbb{U}' \leftarrow \mathbb{U} \cup \mathbb{Q}^{[i]}$, $\Theta \leftarrow \emptyset$.
P2. If $\mathbb{Q}^{[i]} \neq \emptyset$ then do:

P2.1. Let $H_1, \ldots, H_h$ be all the polynomials in $\mathbb{Q}^{[i]}$.
P2.2. For $\ell = 1, \ldots, h$ do:

P2.2.1. Compute $V_\ell \leftarrow \{x_j |\ \deg(H_\ell, x_j) > 0, i < j \leq n\}$.
P2.2.2. Let $H_{\ell 1}, \ldots, H_{\ell m_\ell}$ be all the non-zero coefficients of H_ℓ with respect to V_ℓ.

P2.3. Form $\Theta \leftarrow \{[\mathbb{P}, \mathbb{Q}' \cup \{H_{1j_1}, \ldots, H_{hj_h}\}, \mathbb{T}, \mathbb{U}^*] |\ 1 \leq j_1 \leq m_1, \ldots, 1 \leq j_h \leq m_h\}$.
P2.4. Set $\mathbb{Q}' \leftarrow \mathbb{Q}' \cup \{H_{11}, \ldots, H_{h1}\}$, $\Theta \leftarrow \Theta \setminus \{[\mathbb{P}, \mathbb{Q}', \mathbb{T}, \mathbb{U}^*]\}$.

PROOF. *Since there is no loop involved in this algorithm, the termination is obvious.*

To see (3.4) and (3.5), we note that $[\mathbb{P}, \mathbb{Q}']$ here corresponds to the subsystem in Lemma 2 for the indices $j_1 = 1, \ldots, j_h = 1$, while the $[\mathbb{P}^*, \mathbb{Q}^*]$'s put in Θ correspond to the subsystems in Lemma 2 for all other indices. Therefore, (3.4) and (3.5) are actually an alternative form of (2.2) and (2.3) in Lemma 2. ∎

Now, we are ready to present our elimination algorithm with projection. This algorithm is modified from TRIANGULARIZE by (i) replacing the reduction step T2.2.3 with the projection step T2.2.4 below for the case (B) in which there are polynomials with leading variable x_i but no polynomials with leading variables $\succ x_i$ to be "projected" and (ii) by inserting two projection steps T2.2.3 and T2.3 for the case (A) in which there are polynomials with leading variables $\succ x_i$ to be "projected".

ALGORITHM TRIANGULARIZE_P: $\Psi \leftarrow$TRIANGULARIZE_P$(\mathbb{P}, \mathbb{Q}, k)$. *Given a polynomial system* $[\mathbb{P}, \mathbb{Q}]$ *and an integer* k $(0 \leq k < n)$, *this algorithm computes a set* Ψ *which is either empty, that means* $\text{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$, *or of the form* $\{[\mathbb{P}_1, \mathbb{Q}_1, \mathbb{T}_1, \mathbb{U}_1], \ldots, [\mathbb{P}_e, \mathbb{Q}_e, \mathbb{T}_e, \mathbb{U}_e]\}$, *where each* $[\mathbb{P}_i, \mathbb{Q}_i, \mathbb{T}_i, \mathbb{U}_i]$ *is a quadruplet of level* $\leq k$ *with* $\text{level}(\mathbb{Q}_i) \leq k$, *such that*

a)

$$\text{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \text{Zero}(\mathbb{P}_i \cup \mathbb{T}_i/\mathbb{Q}_i \cup \mathbb{U}_i); \tag{3.6}$$

b) for any k *elements* $a_1, \ldots, a_k \in \tilde{K}$,

$$(a_1, \ldots, a_k) \in \bigcup_{i=1}^{e} \text{Zero}(\mathbb{P}_i/\mathbb{Q}_i) \Longleftrightarrow \text{Zero}(\mathbb{P}^{(a,k)}/\mathbb{Q}^{(a,k)}) \neq \emptyset; \tag{3.7}$$

c) for each i and any $(a_1, \ldots, a_k) \in \mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$,

$$[\mathbb{T}_i^{(a,k)}, \mathbb{U}_i^{(a,k)}] \tag{3.8}$$

is a perfect triangular system, and thus so is $[\mathbb{T}_i, \mathbb{U}_i]$.

T1. Set $\Psi \leftarrow \emptyset$, $\Phi \leftarrow \{[\mathbb{P}, \mathbb{Q}, \phi, \emptyset]\}$.
T2. While $\Phi \neq \emptyset$ do:

T2.1. Set $[\mathbb{P}', \mathbb{Q}', \mathbb{T}', \mathbb{U}'] \leftarrow \mathrm{aef}(\Phi)$, $\Phi \leftarrow \Phi \setminus \{[\mathbb{P}', \mathbb{Q}', \mathbb{T}', \mathbb{U}']\}$, $m \leftarrow \mathrm{level}(\mathbb{P}')$.
T2.2. For $i = m, \ldots, k+1$ do:

T2.2.1. If $\mathbb{P}' \cap K \neq \emptyset$ then go to T2. If $\mathrm{level}(\mathbb{P}') < i$ then go to T2.2 for next i.†
T2.2.2. [Elimination for x_i.] Compute $[T, \mathbb{P}', \mathbb{Q}', \Delta] \leftarrow$ ELIMINATE$(\mathbb{P}', \mathbb{Q}', i)$ and set $\Phi \leftarrow \Phi \cup \{\delta \cup [\mathbb{T}', \mathbb{U}'] \mid \delta \in \Delta\}$.
T2.2.3. [Projection - Case A.] Compute $[\mathbb{Q}', \mathbb{U}', \Theta] \leftarrow$ PROJECT_A $(\mathbb{P}' \cup \{T\}, \mathbb{Q}', \mathbb{T}', \mathbb{U}', i)$ and set $\Phi \leftarrow \Phi \cup \Theta$.
T2.2.4. [Projection - Case B.] If $\mathbb{Q}'^{[i-1]} \neq \emptyset$ then compute $\mathbb{Q}' \leftarrow \mathbb{Q}'^{(i-1)} \cup \{\mathrm{prem}(\prod_{Q \in \mathbb{Q}'^{[i-1]}} Q^{\deg(T, x_i)}, T)\}$.
T2.2.5. If $0 \in \mathbb{Q}'$ then go to T2.1 else set $\mathbb{T} \leftarrow [T] \cup \mathbb{T}$.

T2.3. [Projection - Case A for $i = k$.] Compute $[\mathbb{Q}', \mathbb{U}', \Theta] \leftarrow$ PROJECT_A $(\mathbb{P}', \mathbb{Q}', \mathbb{T}', \mathbb{U}', k)$ and set $\Phi \leftarrow \Phi \cup \Theta$.
T2.4. Set $\Psi \leftarrow \Psi \cup \{[\mathbb{P}', \mathbb{Q}', \mathbb{T}', \mathbb{U}']\}$.

EXAMPLE 1C. See Example 1b. To perform the elimination with projection ($k = 0$), for $z \in \mathbb{U}_1$ we need compute the remainder of z^5, instead of the remainder of z, with respect to R_3 in step T2.2.4. It is $-t^4 \sim t$, so $\mathbb{U}_1$ is replaced by $\{t, t^3 - 1\}$. Similarly, for $z \in \mathbb{U}_3$ we need compute the remainder of z^5 with respect to R_3, which is $-t^4 \sim t$, and then the remainder of t^3 with respect to $t^3 - 1$, which is the constant 1. Hence, $\mathbb{U}_3$ is simplified to $\emptyset$. The projection steps T2.2.3 and T2.3 are trivially executed for this example. ■

PROOF OF THE TERMINATION AND CORRECTNESS OF TRIANGULARIZE_P. For any polynomial system $[\mathbb{P}, \mathbb{Q}]$, we define a triple $\mathrm{index}(\mathbb{P}/\mathbb{Q}) = \langle d, m, p \rangle$, where $m = \mathrm{level}(\mathbb{P})$, $d =$ the minimal degree in x_m of the polynomials in $\mathbb{P}^{[m-1]}$ and $p = \max(m, \mathrm{level}(\mathbb{Q}))$. We order two triples as $\langle d_1, m_1, p_1 \rangle \prec \langle d_2, m_2, p_2 \rangle$ if $p_1 < p_2$, or $p_1 = p_2$ while $m_1 < m_2$, or $p_1 = p_2, m_1 = m_2$ while $d_1 < d_2$. Now, for a quadruplet ψ taken from Ψ in step T2.1 of TRIANGULARIZE_P, let $\mathbb{P}', \mathbb{Q}'$ be the first two components of ψ and $\mathbb{P}^*, \mathbb{Q}^*$ be the two components of some polynomial system in the Δ produced by ELIMINATE or the first two

† We may modify this sentence so that the projection step T2.2.3 is also executed when $\mathrm{level}(\mathbb{P}') < i$. Then PROJECT_A is called for every i and V in step P2.2.1 only contains x_i for each call. This may simplify the presentation a little. In this case, the properties *b)* and *c)* in the specification may be slightly modified: *b')* for any l ($\geq k$) elements $a_1, \ldots, a_l \in \bar{K}$, $(a_1, \ldots, a_l) \in \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{P}_i \cup \mathbb{T}_i^{(l)}/\mathbb{Q}_i \cup \mathbb{U}^{(l)}) \Longleftrightarrow \mathrm{Zero}(\mathbb{P}^{(a,l)}/\mathbb{Q}^{(a,l)}) \neq \emptyset$; *c')* for each i and any $(a_1, \ldots, a_l) \in \mathrm{Zero}(\mathbb{P}_i \cup \mathbb{T}_i^{(l)}/\mathbb{Q}_i \cup \mathbb{U}^{(l)})$ ($l \geq k$), $[\mathbb{T}_i^{[l](a,l)}, \mathbb{U}_i^{[l](a,l)}]$ is a perfect triangular system, and thus so is $[\mathbb{T}_i^{[l]}, \mathbb{U}_i^{[l]}]$. However, if the splitting occurs when $\mathrm{level}(\mathbb{P}') < i \neq k$, then ELIMINATE in step T2.2.2 may be repeatedly called for the same $\mathbb{P}'$.

Even without modifying the sentence, the above *b')* and *c')* hold for $l = k, p_1, \ldots, p_r$, where p_j is the index of the leading variable of the jth term of $\mathbb{T}_i$. See the proof of *c)*.

components of some quadruplet in the Θ produced by PROJECT_A from ψ. Then we always have $\mathrm{index}(\mathbb{P}^*/\mathbb{Q}^*) \prec \mathrm{index}(\mathbb{P}'/\mathbb{Q}')$. Since each component of the triple $\mathrm{index}(\mathbb{P}/\mathbb{Q})$ is a positive integer, any steadily decreasing sequence of index triples is finite. Therefore, the while-loop of TRIANGULARIZE can only have a finite number of iterations and the termination is proved.

It remains to be shown that the computed Ψ satisfies the properties *a*), *b*) and *c*) in the specification of the algorithm.

a) The algorithm TRIANGULARIZE_P can also be viewed as for computing a multi-branch tree $\mathfrak{T}$. Now, with the root of $\mathfrak{T}$, the quadruplet $[\mathbb{P}, \mathbb{Q}, \phi, \emptyset]$ is associated, and with each node or leaf i, a quadruplet $[\mathbb{P}_i, \mathbb{Q}_i, \mathbb{T}_i, \mathbb{U}_i]$ is associated such that after the execution of every step of TRIANGULARIZE_P the zero relation (3.3), when $\mathbb{Q}_i$ on the right-hand side is replaced by $\mathbb{Q}_i \cup \mathbb{U}_i$, is preserved. To see this, we only need note that in the present case, the branches are generated also by the subalgorithm PROJECT_A with the zero relation (3.5) preserved, while (3.5) implies that

$$\mathrm{Zero}(\mathbb{P} \cup \mathbb{T}/\mathbb{Q} \cup \mathbb{U}) = \mathrm{Zero}(\mathbb{P} \cup \mathbb{T}/\mathbb{Q}' \cup \mathbb{U}') \cup \bigcup_{[\mathbb{P}^*, \mathbb{Q}^*, \mathbb{T}, \mathbb{U}] \in \Theta} \mathrm{Zero}(\mathbb{P}^* \cup \mathbb{T}/\mathbb{Q}^* \cup \mathbb{U}'), \quad (3.5')$$

where $\mathbb{U}' = \mathbb{U} \cup \mathbb{Q}^{[i]}$. $\mathrm{Zero}(\mathbb{P}' \cup \{T\} \cup \mathbb{T}'/\mathbb{Q}' \cup \mathbb{U}')$ also remains unchanged when step T2.2.4 is executed.

Cutting those leaves i of $\mathfrak{T}$ for which $\mathbb{P}_i$ contains a non-zero constant or $\mathbb{Q}_i$ contains 0 (supposed that not all of the leaves are cut off), we obtain the zero decomposition (3.6). From the correctness proof of TRIANGULARIZE, we see clearly that $[\mathbb{T}_i, \mathbb{U}_i]$ here is also a triangular system.

b) We first suppose that the left-hand side of (3.7) holds, so there is an i such that $(a_1, \ldots, a_k) \in \mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$. By the property *c*) to be proved, there is some $(a_{k+1}, \ldots, a_n) \in \mathrm{Zero}(\mathbb{T}_i^{\langle a,k \rangle}/\mathbb{U}_i^{\langle a,k \rangle})$. Hence $(a_1, \ldots, a_n) \in \mathrm{Zero}(\mathbb{P}_i \cup \mathbb{T}_i/\mathbb{Q}_i \cup \mathbb{U}_i)$. By (3.6), $(a_1, \ldots, a_n) \in \mathrm{Zero}(\mathbb{P}/\mathbb{Q})$. It follows that $(a_{k+1}, \ldots, a_n) \in \mathrm{Zero}(\mathbb{P}^{\langle a,k \rangle}/\mathbb{Q}^{\langle a,k \rangle})$, so that $\mathrm{Zero}(\mathbb{P}^{\langle a,k \rangle}/\mathbb{Q}^{\langle a,k \rangle}) \neq \emptyset$.

Now suppose that $\mathrm{Zero}(\mathbb{P}^{\langle a,k \rangle}/\mathbb{Q}^{\langle a,k \rangle}) \neq \emptyset$ and let $(a_{k+1}, \ldots, a_n) \in \mathrm{Zero}(\mathbb{P}^{\langle a,k \rangle}/\mathbb{Q}^{\langle a,k \rangle})$. Then $(a_1, \ldots, a_n) \in \mathrm{Zero}(\mathbb{P}/\mathbb{Q})$. By (3.6), there must be an i such that $(a_1, \ldots, a_n) \in \mathrm{Zero}(\mathbb{P}_i \cup \mathbb{T}_i/\mathbb{Q}_i \cup \mathbb{U}_i)$. In particular, we have $(a_1, \ldots, a_k) \in \mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$. Therefore, $(a_1, \ldots, a_k) \in \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$ and (3.6) is proved.

c) Let $\mathbb{P}', \mathbb{Q}', \mathbb{T}', \mathbb{U}'$ and T be as in TRIANGULARIZE_P. We first prove that:

(A). If step T2.2.3 is executed for some i, then after the execution, for any $(a_1, \ldots, a_i) \in \mathrm{Zero}(\mathbb{P}' \cup \{T\}/\mathbb{Q}')$,

$$\mathrm{Zero}(\mathbb{T}'^{\langle a,k \rangle}/\mathbb{U}'^{\langle a,k \rangle}) \neq \emptyset; \quad (3.9)$$

(B). If step T2.2.4 is executed for some i, then after the execution, for any $(a_1, \ldots, a_{i-1}) \in \mathrm{Zero}(\mathbb{P}'/\mathbb{Q}')$,

$$\mathrm{Zero}([T] \cup \mathbb{T}'^{\langle a,k \rangle}/\mathbb{U}'^{\langle a,k \rangle}) \neq \emptyset. \quad (3.10)$$

If $\mathbb{Q}'$ contains 0, then $\mathrm{Zero}(\mathbb{P}'/\mathbb{Q}') = \emptyset$. In this case, the property is trivial and will not be considered.

To avoid the confusion of notations, the quadruplet $[\mathbb{P}', \mathbb{Q}', \mathbb{T}', \mathbb{U}']$ in what follows will always be referred to before the execution of the step under discussion, and the

corresponding components after the execution, if updated, will be referred to by replacing the prime $'$ with the star *. The proof proceeds by induction on the length of $\mathbb{T}'$.

Case (i). $\mathbb{T}' = \phi$.

(A). Let ψ' and ψ^* be the quadruplets corresponding to $[\mathbb{P}', \mathbb{Q}', \mathbb{T}', \mathbb{U}']$ before and after the execution of step T2.2.3 in TRIANGULARIZE_P, respectively. Then $\psi' = [\mathbb{P}', \mathbb{Q}', \phi, \emptyset]$ and $\psi^* = [\mathbb{P}', \mathbb{Q}^*, \phi, \mathbb{U}^*]$, where $\mathbb{U}^* = \mathbb{Q}'^{[i]}$. Let $(a_1, \ldots, a_i) \in \mathrm{Zero}(\mathbb{P}' \cup \{T\}/\mathbb{Q}^*)$. By (3.4), we have $\mathrm{Zero}(\mathbb{P}' \cup \{T\}/\mathbb{Q}') \neq \emptyset$. According to Remark 2, there are in fact some $a_{i+1}, \ldots, a_n$ such that $(a_1, \ldots, a_n) \in \mathrm{Zero}(\mathbb{P}' \cup \{T\}/\mathbb{Q}')$. Since $\mathbb{U}^* \subset \mathbb{Q}'$, $(a_1, \ldots, a_n)$ is not a zero of any polynomial in $\mathbb{U}^*$. Hence, $(a_1, \ldots, a_n) \in \mathrm{Zero}(\phi/\mathbb{U}^*)$ and (3.9) holds.

(B). Now we have $\psi' = [\mathbb{P}', \mathbb{Q}', \phi, \mathbb{U}']$ and $\psi^* = [\mathbb{P}', \mathbb{Q}^*, \phi, \mathbb{U}']$, where $\mathbb{Q}^* = \mathbb{Q}'^{[i-1]} \cup \{\mathrm{prem}(\prod_{Q \in \mathbb{Q}'^{[i-1]}} Q^{\deg(T, x_i)}, T)\}$ if $\mathbb{Q}'^{[i-1]} \neq \emptyset$, and $\mathbb{Q}^* = \mathbb{Q}'$ if $\mathbb{Q}'^{[i-1]} = \emptyset$. In both cases, for any $(a_1, \ldots, a_{i-1}) \in \mathrm{Zero}(\mathbb{P}'/\mathbb{Q}^*)$, by (2.4)-(2.5) and noting that $\mathrm{ini}(T) \in \mathbb{Q}'$ we have $\mathrm{Zero}(\mathbb{P}' \cup \{T\}/\mathbb{Q}') \neq \emptyset$. According to Remark 2 there is an a_i such that $(a_1, \ldots, a_i) \in \mathrm{Zero}(\mathbb{P}' \cup \{T\}/\mathbb{Q}')$. Now for $(a_1, \ldots, a_i) \in \mathrm{Zero}(\mathbb{P}' \cup \{T\}/\mathbb{Q}')$, by (A) above there are $a_{i+1}, \ldots, a_n$ such that $(a_1, \ldots, a_n) \in \mathrm{Zero}(\phi/\mathbb{U}')$. Therefore, $(a_1, \ldots, a_n) \in \mathrm{Zero}([T]/\mathbb{U}')$ and (3.10) holds.

Case (ii). $\mathbb{T}' \neq \phi$.

By induction we suppose that the property in (B) is satisfied after the execution of step T2.2.4 for $i = p$, where p is the index of $\mathrm{lvar}(\mathrm{first}(\mathbb{T}'))$. Note that steps T2.2.5 and T 2.2.1 are trivial, the execution of step T2.2.2 does not update $\mathbb{T}'$ and $\mathbb{U}'$, and for this step any zero of $[\mathbb{P}^* \cup \{T\}, \mathbb{Q}^*]$ is also a zero of $[\mathbb{P}', \mathbb{Q}']$ by (3.1). Hence, the property in (B) is also satisfied after the execution of step T2.2.2.

(A). In this case, we have $\psi' = [\mathbb{P}', \mathbb{Q}', \mathbb{T}', \mathbb{U}']$ and $\psi^* = [\mathbb{P}', \mathbb{Q}^*, \mathbb{T}', \mathbb{U}^*]$, where $\mathbb{U}^* = \mathbb{U}' \cup \mathbb{Q}'^{[i]}$. For any $(a_1, \ldots, a_i) \in \mathrm{Zero}(\mathbb{P}' \cup \{T\}/\mathbb{Q}^*)$, again according to Remark 2 there are $a_{i+1}, \ldots, a_p$ such that $(a_1, \ldots, a_p) \in \mathrm{Zero}(\mathbb{P}' \cup \{T\}/\mathbb{Q}')$. Therefore, by inductive hypothesis there are $a_{p+1}, \ldots, a_n$ such that $(a_1, \ldots, a_n) \in \mathrm{Zero}(\mathbb{T}'/\mathbb{U}')$. Since $\mathbb{U}^{*(p)} = \mathbb{Q}'^{[i]} \subset \mathbb{Q}'$, $(a_1, \ldots, a_n) \in \mathrm{Zero}(\mathbb{T}'/\mathbb{U}^{*(p)} \cup \mathbb{U}') = \mathrm{Zero}(\mathbb{T}'/\mathbb{U}^*)$, so (3.9) holds.

(B). Similar to (B) in Case (i), for any $(a_1, \ldots, a_{i-1}) \in \mathrm{Zero}(\mathbb{P}'/\mathbb{Q}^*)$, by (2.4)-(2.5), Remark 2 and noting that $\mathrm{ini}(T) \in \mathbb{Q}'$, there is an a_i such that $(a_1, \ldots, a_i) \in \mathrm{Zero}(\mathbb{P}' \cup \{T\}/\mathbb{Q}')$. By (A) in Case (ii) above, there are $a_{i+1}, \ldots, a_n$ such that $(a_1, \ldots, a_n) \in \mathrm{Zero}(\mathbb{T}'/\mathbb{U}')$. Hence, $(a_1, \ldots, a_n) \in \mathrm{Zero}([T] \cup \mathbb{T}'/\mathbb{U}')$ and (3.10) holds as well.

Finally, we prove that after the execution of step T2.3, for any $(a_1, \ldots, a_i) \in \mathrm{Zero}(\mathbb{P}'/\mathbb{Q}')$, (3.9) holds.

If $\mathbb{T}' = \phi$, then step T2.2 is trivially executed and the execution of step T2.3 is the same as the execution of step T2.2.3 for $i = k$ in (A) of Case (i), noting that the polynomial T does not play any role in PROJECT_A. Therefore, for any $(a_1, \ldots, a_k) \in \mathrm{Zero}(\mathbb{P}'/\mathbb{Q}^*)$, there are $a_{k+1}, \ldots, a_n$ such that $(a_1, \ldots, a_n)$ is not a zero of any polynomial in $\mathbb{U}^* \subset \mathbb{Q}'$. Hence, $(a_1, \ldots, a_n) \in \mathrm{Zero}(\phi/\mathbb{U}^*)$ and (3.9) holds.

If $\mathbb{T}' \neq \phi$, then step T2.2.4 must have been executed before, say for $i = p > k$, where p is the index of $\mathrm{lvar}(\mathrm{first}(\mathbb{T}'))$. Now the execution of step T2.3 is the same as the execution of step T2.2.3 for $i = k$ in (A) of Case (ii). Therefore, for any $(a_1, \ldots, a_k) \in \mathrm{Zero}(\mathbb{P}'/\mathbb{Q}^*)$, there are $a_{k+1}, \ldots, a_n$ such that $(a_1, \ldots, a_n) \in \mathrm{Zero}(\mathbb{T}'/\mathbb{U}^*)$, so (3.9) holds as well.

Clearly, the final $[\mathbb{P}', \mathbb{Q}', \mathbb{T}', \mathbb{U}']$ is some $[\mathbb{P}_i, \mathbb{Q}_i, \mathbb{T}_i, \mathbb{U}_i]$ in the specification of the algorithm. Hence, $[\mathbb{T}_i^{\{a,k\}}, \mathbb{U}_i^{\{a,k\}}]$ is perfect. Since $\mathrm{Zero}(\mathbb{T}_i^{\{a,k\}}/\mathbb{U}_i^{\{a,k\}}) \neq \emptyset$ implies that $\mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i) \neq \emptyset$, by definition the triangular system $[\mathbb{T}_i, \mathbb{U}_i]$ is also perfect.

This completes the correctness proof of TRIANGULARIZE_P. ∎

REMARK 3. The projection step T2.2.4 can be modified by using a more complicated pro-

cedure as follows. Instead of forming $\text{prem}(\prod_{Q\in\mathbb{Q}'[t-1]} Q^{\deg(T,x_i)}, T)$, after squarefreeing T we compute the GCD (greatest common divisor) of T and each polynomial $Q \in \mathbb{Q}'[t-1]$ with respect to x_i, say by pseudo-division, and delete it as a factor from T and Q. After the deletion of all such common divisors, the GCD of T and every polynomial in $\mathbb{Q}'[t-1]$ should be 1. Then, $\text{Zero}(T/\mathbb{Q}'[t-1]) \neq \emptyset$ if and only if T is of positive degree in x_i (cf. Seidenberg, 1956a). Along with computing the GCD's, we split the system into finitely many other systems so that the necessary zero relations are preserved. ■

The algorithm TRIANGULARIZE_P provides a quantifier elimination procedure and thus a decision procedure for the existential theory of algebraically closed fields. As a corollary of this algorithm, we have the following projection theorem.

THEOREM 1 (*The Projection Theorem of Elimination Theory - Affine Case*). *Let* $\mathbb{F}_i(x,y)$, $i = 1,\ldots,s$, *be a finite conjunction of polynomial equations and inequations over* K *in the variables* $(x,y) = (x_1,\ldots,x_n,y_1,\ldots,y_m)$. *Then there is a finite set of* $\mathbb{G}_j(x)$ *of which each one is a finite conjunction of polynomial equations and inequations over* K *having the following property: for every point* $a = (a_1,\ldots,a_n)$ *of the affine space* V^n *over some extension field* $\bar{K}$ *of* K *there is a point* $b = (b_1,\ldots,b_m)$ *of the affine space* W^m *over some algebraic extension field of* $\bar{K}$ *such that* (a,b) *satisfies at least one of the* $\mathbb{F}_i(x,y)$ *if and only if* a *satisfies one of the* $\mathbb{G}_j(x)$.

One proof of this theorem was contained in the classical decision method of Tarski (1951) and clarified by N. Jacobson (1974, Chapter 5). Another proof appeared in Seidenberg (1956a), see also Seidenberg (1956b, 1969). A recent proof was given by W. T. Wu (1990).

For every polynomial system $[\mathbb{P}_i,\mathbb{Q}_i]$ in (3.6), we can further compute a decomposition for $\text{Zero}(\mathbb{P}_i/\mathbb{Q}_i)$ having the form (3.2) by the algorithm TRIANGULARIZE. Such zero decompositions may be merged with (3.6). As a consequence, there is an algorithm which computes, for any polynomial system $[\mathbb{P},\mathbb{Q}]$ and an integer k $(0 \leq k < n)$, a set Ψ which is either empty, that means $\text{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$, or of the form $\{[\mathbb{P}_1,\mathbb{Q}_1,\mathbb{T}_1,\mathbb{U}_1],\ldots,[\mathbb{P}_e,\mathbb{Q}_e,\mathbb{T}_e,\mathbb{U}_e]\}$ such that *a*), *b*) and *c*) in the specification of TRIANGULARIZE_P are all satisfied and moreover each $[\mathbb{P}_i \cup \mathbb{T}_i, \mathbb{Q}_i \cup \mathbb{U}_i]$ is a (fine) triangular system, where $\mathbb{P}_i$ is put in the form of a list with increasing leading variables. See Wang (1993) for the details of such an algorithm. In this case, we call $n-k$ the *dimension* of projection and say that the elimination is performed with *full* projection if the dimension is n, and *without* projection if the dimension is 0.

4. Irreducible Triangular Forms and Zero Decompositions

Instead of projection, in this section we are concerned with the irreducibility of triangular forms. A triangular form $\mathbb{T}$ is said to be *quasi-irreducible* if every polynomial in $\mathbb{T}$ is irreducible over the ground field K. A triangular system $[\mathbb{T},\mathbb{U}]$ is said to be *quasi-irreducible* if $\mathbb{T}$ is quasi-irreducible. Let us modify the algorithm TRIANGULARIZE to TRIANGULARIZE_Q with the following specification:

ALGORITHM TRIANGULARIZE_Q: $\Psi \leftarrow$ TRIANGULARIZE_Q$(\mathbb{P},\mathbb{Q},\mathbb{T})$. *Given a triplet* $[\mathbb{P},\mathbb{Q},\mathbb{T}]$ *with* $[\mathbb{T},\mathbb{Q}]$ *constituting a quasi-irreducible triangular system and all polynomials in* $\mathbb{Q}$ *reduced with respect to* $\mathbb{T}$, *this algorithm computes a set* Ψ *which is either empty, that*

means $\mathrm{Zero}(\mathbb{P} \cup \mathbb{T}/\mathbb{Q}) = \emptyset$, *or of the form* $\{[\mathbb{T}_1, \mathbb{U}_1], \ldots, [\mathbb{T}_e, \mathbb{U}_e]\}$ *such that*

$$\mathrm{Zero}(\mathbb{P} \cup \mathbb{T}/\mathbb{Q}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i), \tag{4.1}$$

where each $[\mathbb{T}_i, \mathbb{U}_i]$ *is a fine quasi-irreducible triangular system.*

This algorithm is obtained from TRIANGULARIZE by replacing **T1** with

T1′. [Initialize.] Set $\Psi \leftarrow \emptyset$, $\Phi \leftarrow \{[\mathbb{P}, \mathbb{Q}, \mathbb{T}]\}$.

and **T2.2.3** with

T2.2.3′. [Factorization.] Compute all the irreducible factors $F_1, \ldots, F_t$ of T over K and set $\bar{\mathbb{Q}} \leftarrow \mathbb{Q}'$.

T2.2.3″. [Splitting.] For $j = 1, \ldots, t$ do:

T2.2.3.1. [Reduction.] Compute $\bar{\mathbb{Q}}' \leftarrow \mathrm{prem}(\bar{\mathbb{Q}}, F_j)$.

T2.2.3.2. If $j = 1$ then set $\mathbb{Q}' \leftarrow \bar{\mathbb{Q}}'$, $T \leftarrow F_j$. Otherwise, if $0 \notin \bar{\mathbb{Q}}'$ then set $\Phi \leftarrow \Phi \cup \{[\mathbb{P}', \bar{\mathbb{Q}}', [F_j] \cup \mathbb{T}']\}$.

PROOF. For the modification of step T1 to T1′, we note that $\mathbb{P} \cup \mathbb{T}$ here corresponds to the set $\mathbb{P}$ in the input of TRIANGULARIZE, while the cases in which the initials of the polynomials in $\mathbb{T}$ happen to be zero need not be considered because $[\mathbb{T}, \mathbb{Q}]$ is a triangular system. Actually, any triplet from Φ in TRIANGULARIZE is of the same form as the input triplet to TRIANGULARIZE_Q. For the modification of step T2.2.3 to T2.2.3′, the polynomial T produced by ELIMINATE is factorized over the ground field K and the polynomial system is then split into subsystems by replacing T with its factors. We see that for any triplet, say $[\mathbb{P}^*, \mathbb{Q}^*, \mathbb{T}^*]$, produced in step T2.2.3.2, the level of $\mathbb{P}^*$ is less than the level of $\mathbb{P}'$, the first component of the corresponding triplet taken form Φ in step T2.1 (see the termination proof of TRIANGULARIZE). Hence, the algorithm TRIANGULARIZE_Q terminates as well.

To see the correctness of this algorithm, we only need note that the splitting of systems via factorization preserves the zero relation. That is, for any polynomial system $[\mathbb{P}^*, \mathbb{Q}^*]$, if $F_1, \ldots, F_t$ are all the irreducible factors of a polynomial F in $\mathbb{P}^*$, we have

$$\mathrm{Zero}(\mathbb{P}^*/\mathbb{Q}^*) = \bigcup_{j=1}^{t} \mathrm{Zero}(\mathbb{P}_j^*/\mathbb{Q}^*),$$

where $\mathbb{P}_j^* = (\mathbb{P}^* \setminus \{F\}) \cup \{F_j\}$ for each j. Therefore, (4.1) is proved by the same argument as for the proof of (3.1). Since the corresponding T is replaced by its irreducible factors, by definition $\mathbb{T}_i$ is quasi-irreducible and thus so is $[\mathbb{T}_i, \mathbb{U}_i]$ for each i. $[\mathbb{T}_i, \mathbb{U}_i]$ is fine because all polynomials in $\mathbb{U}_i$ are actually the remainders of some polynomials (and thus are reduced) with respect to $\mathbb{T}_i$. ∎

Note in passing that those F_j whose leading variables are $\prec x_i$ are factors of the initial of F and thus need not be considered in fact. Consequently, the corresponding triplets can be deleted from the set Φ.

EXAMPLE 1D. Let us recall Examples 1a-1b given before and apply the algorithm TRIANGULARIZE_Q to the triplet $[\mathbb{P}, \emptyset, \phi]$ of level 4. It is easy to verify that all polynomials in the triangular forms $\mathbb{T}_1$ and $\mathbb{T}_2$ produced by the algorithm TRIANGULARIZE are irreducible.

However, the first polynomial t^3+1 in $\mathbb{T}_3$ is reducible and can be factorized as the product of two polynomials $t-1$ and t^2+t+1. Hence, in TRIANGULARIZE_Q $[\mathbb{T}_3, \mathbb{U}_3]$ is split into two triangular systems $[\mathbb{T}_3', \mathbb{U}_3']$ and $[\mathbb{T}_3'', \mathbb{U}_3'']$ with $\mathbb{T}_3' = [t^2+t+1, R_3, -z^3y-t^3, R_2]$, $\mathbb{T}_3'' = [t-1, R_3, -z^3y-t^3, R_2]$ and $\mathbb{U}_3' = \mathbb{U}_3'' = \{z\}$. ■

Let the leading variables of a triangular form $\mathbb{T}$ be $y_1 = x_{p_1}, \ldots, y_r = x_{p_r}$ and all the other x's be denoted by $u_1, \ldots, u_d$ $(d+r=n)$, abbreviated sometimes to u. Then $\mathbb{T}$ can be written in the form

$$\mathbb{T}: \quad [T_1(u, y_1), T_2(u, y_1, y_2), \ldots, T_r(u, y_1, y_2, \ldots, y_r)].$$

Let K_0 be the transcendental extension field $K(u) = K(u_1, \ldots, u_d)$ of K gotten by adjoining $u_1, \ldots, u_d$. We define inductively the *irreducibility* and *generic points* of a fine triangular form as follows.

DEFINITION 3. *A fine triangular form $\mathbb{T}$ containing only one polynomial $T_1(u, y_1)$ is said to be* irreducible *if T_1 is irreducible as a polynomial in $K_0[y_1]$. In that case, let η_1 be a zero of T_1 in some extension field of K_0; then (u, η_1) is called a* generic point *of $\mathbb{T}$.*

Suppose that the irreducibility and generic points of any fine triangular form of length $< r$ has already been defined.

A fine triangular form $\mathbb{T}$ as above of length $r > 1$ is said to be irreducible *if the fine triangular form $[T_1, \ldots, T_{r-1}]$ formed by the first $r-1$ terms of $\mathbb{T}$ is irreducible with a generic point $(u, \eta_1, \ldots, \eta_{r-1})$, and if the polynomial $\bar{T}_r = T_r|_{y_1=\eta_1, \ldots, y_{r-1}=\eta_{r-1}} \in K_{r-1}[y_r]$ is irreducible, where $K_{r-1} = K_0(\eta_1, \ldots, \eta_{r-1})$ is the algebraic extension field gotten from K_0 by adjoining $\eta_1, \ldots, \eta_{r-1}$. In that case, let η_r be a zero of $\bar{T}_r$ in some extension field of K_{r-1}; then $(u, \eta_1, \ldots, \eta_r)$ is called a* generic point *of $\mathbb{T}$.*

A fine triangular system $[\mathbb{T}, \mathbb{U}]$ is said to be irreducible *if $\mathbb{T}$ is irreducible.*

Let $\mathbb{T}$ as above be an irreducible triangular form. For convenience, we call $T_1, \ldots, T_r$ *adjoining polynomials* and $\mathbb{T}$ an *adjoining triangular form* of the algebraic extension field $K_r = K_0(\eta_1, \ldots, \eta_r)$. Evidently, any generic point $(u, \eta_1, \ldots, \eta_r)$ of $\mathbb{T}$ can be considered as a point of the linear space $\bar{K}^n$. The above d is called the dimension of $\mathbb{T}$, denoted by $\dim(\mathbb{T})$. It is not difficult to prove that any irreducible triangular form is perfect.

LEMMA 4. *If a fine triangular form $\mathbb{T}$ is irreducible with a generic point $\bar{\eta} = (u, \eta_1, \ldots, \eta_r)$, then for a polynomial $P \in K[u, y_1, \ldots, y_r]$ to have remainder 0 with respect to $\mathbb{T}$, it is necessary and sufficient that $\bar{\eta}$ is a zero of P.*

LEMMA 5. *Let $\mathbb{T}$ be an irreducible triangular form and P be a polynomial whose remainder with respect to $\mathbb{T}$ is non-zero. If $\dim(\mathbb{T}) = 0$, then*

$$\mathrm{Zero}(\{P\} \cup \mathbb{T}) = \emptyset$$

and, in particular,

$$\mathrm{Zero}(\mathbb{T}/\mathbb{I}) = \mathrm{Zero}(\mathbb{T}),$$

where $\mathbb{I} = \{\mathrm{ini}(T) | \ T \in \mathbb{T}\}$.

The proof of Lemma 4 is a simple copy of the proof of Lemma 3 in Section 3 of Wu (1984a). The first half of Lemma 5 follows directly from Lemma 4 in Section 3 of Wu

(1984a) or the dimension theorem in Wu (1984b), and the second half is obvious by noting that

$$\text{Zero}(\mathbb{T}) = \text{Zero}(\mathbb{T}/\mathbb{I}) \cup \bigcup_{I \in \mathbb{I}} \text{Zero}(\{I\} \cup \mathbb{T}).$$

If a fine triangular form $\mathbb{T}$ as above is reducible, then there is a k such that

$$\mathbb{T}_{k-1}: \quad [T_1, T_2, \ldots, T_{k-1}]$$

is irreducible with a generic point

$$\bar{\eta}_{k-1} = (u, \eta_1, \ldots, \eta_{k-1})$$

and the polynomial $\bar{T}_k = T_k|_{y_1=\eta_1,\ldots,y_k=\eta_{k-1}}$ is reducible in $\boldsymbol{K}_{k-1}[y_k]$, where $\boldsymbol{K}_{k-1} = \boldsymbol{K}_0(\eta_1, \ldots, \eta_{k-1})$.

By the same arguments as in Wu (1984a) (see also Wang, 1989), we know that T_k has an irreducible factorization of the form

$$DT_k \doteq F_1 \cdots F_t \tag{4.2}$$

over $\boldsymbol{K}_{k-1}$, where the polynomials $D \in \boldsymbol{K}[u, y_1, \ldots, y_{k-1}]$, $F_j \in \boldsymbol{K}[u, y_1, \ldots, y_k]$ are all reduced with respect to $\mathbb{T}_{k-1}$ and the dot equality means that $\text{prem}(DT_k - F_1 \cdots F_t, \mathbb{T}_{k-1}) = 0$.

LEMMA 6. *Let $[\mathbb{T}, \mathbb{U}]$ be a fine triangular system with $\mathbb{T}$ as before. Suppose that $\mathbb{T}$ is reducible, so that there is a k for which the kth term T_k of $\mathbb{T}$ has an irreducible factorization into polynomials $F_1, \ldots, F_t$ as of the form* (4.2). *Then there is a zero decomposition of the form*

$$\text{Zero}(\mathbb{T}/\mathbb{U}) = \text{Zero}(\{D\} \cup \mathbb{T}/\mathbb{U}) \cup \bigcup_{j=1}^{t} \text{Zero}(\mathbb{T}_j/\mathbb{U} \cup \{D\}), \tag{4.3}$$

where each $\mathbb{T}_j$ is a polynomial list obtained from $\mathbb{T}$ by replacing T_k with F_j.

PROOF. For any $\bar{x} \in \text{Zero}(\mathbb{T}/\mathbb{U})$, we have $T_k(\bar{x}) = 0$, so there must be an i such that $F_j(\bar{x}) = 0$. If $D(\bar{x}) \neq 0$, then $\bar{x} \in \text{Zero}(\mathbb{T}_j/\mathbb{U} \cup \{D\})$. Otherwise, $\bar{x} \in \text{Zero}(\{D\} \cup \mathbb{T}/\mathbb{U})$. Hence, in any case $\bar{x}$ belongs to the right-hand side of (4.3).

On the other hand, let $\bar{x}$ be contained in the right-hand side of (4.3). If $\bar{x} \in \text{Zero}(\{D\} \cup \mathbb{T}/\mathbb{U})$, then $\bar{x} \in \text{Zero}(\mathbb{T}/\mathbb{U})$ obviously. Otherwise, there is a j such that $\bar{x} \in \text{Zero}(\mathbb{T}_j/\mathbb{U} \cup \{D\})$, so $F_j(\bar{x}) = 0$ and $D(\bar{x}) \neq 0$. It follows from (4.2) that $T_k(\bar{x}) = 0$. Therefore $\bar{x} \in \text{Zero}(\mathbb{T}/\mathbb{U})$. ∎

REMARK 4. If, in particular, $D \in \boldsymbol{K}$ or $\dim(\mathbb{T}_{k-1}) = 0$, then (4.3) can be simplified to

$$\text{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{j=1}^{t} \text{Zero}(\mathbb{T}_j/\mathbb{U}).$$

This is trivial for $D \in \boldsymbol{K}$. If $\dim(\mathbb{T}_{k-1}) = 0$, then $\text{Zero}(\{D\} \cup \mathbb{T}/\mathbb{U}) = \emptyset$ and $\text{Zero}(\mathbb{T}_j/\mathbb{U} \cup \{D\}) = \text{Zero}(\mathbb{T}_j/\mathbb{U})$ by Lemma 5. ∎

Let $\mathbb{U}_j = \text{prem}(\mathbb{U} \cup \{D\}, \mathbb{T}_j)$ (where the division need be performed actually only with respect to $[T_1, \ldots, T_{k-1}, F_j]$). If $\mathbb{U}_j$ contains 0 for some j, then the corresponding component in (4.3) can be simply removed. For those components in which $\mathbb{U}_j$ does not

contain 0, it is easy to see that $[\mathbb{T}_j, \mathbb{U}_j]$ is still a fine triangular system (and, in particular, the triangular form constituted by the first k terms of $\mathbb{T}_j$ is irreducible) for each j.

However, the polynomial set $\{D\} \cup \mathbb{T}$ may no longer be in triangular form. To further triangularize this polynomial set, we may apply the algorithm TRIANGULARIZE_Q to $[\{T_1, \ldots, T_q, D\}, \mathbb{U}, [T_{q+1}, \ldots, T_r]]$, where q is the biggest index such that $\mathrm{lvar}(T_q) \preceq \mathrm{lvar}(D)$.

SUBALGORITHM DECOMPOSE: $[\Psi, \Phi] \leftarrow$DECOMPOSE$(\mathbb{T}, \mathbb{U})$. *Given a fine quasi-irreducible triangular system* $[\mathbb{T}, \mathbb{U}]$, *this algorithm computes two sets* Ψ *and* Φ *which are either both empty, that means* $\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \emptyset$, *or of the forms* $\{[\mathbb{T}_1, \mathbb{U}_1], \ldots, [\mathbb{T}_e, \mathbb{U}_e]\}$ *and* $\{[\mathbb{P}_1, \mathbb{Q}_1, \mathbb{T}'_1], \ldots, [\mathbb{P}_h, \mathbb{Q}_h, \mathbb{T}'_h]\}$, *respectively, such that*

$$\mathrm{Zero}(\mathbb{T}/\mathbb{U}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i) \cup \bigcup_{j=1}^{h} \mathrm{Zero}(\mathbb{P}_j \cup \mathbb{T}'_j/\mathbb{Q}_j), \tag{4.4}$$

where each $[\mathbb{T}_i, \mathbb{U}_i]$ *is an irreducible triangular system and each* $[\mathbb{P}_j, \mathbb{Q}_j, \mathbb{T}'_j]$ *is a triplet with* $[\mathbb{T}'_j, \mathbb{Q}_j]$ *constituting a fine quasi-irreducible triangular system.*

D1. Set $\Phi \leftarrow \emptyset$, $r \leftarrow$length$(\mathbb{T})$. If $r = 1$ then set $\Psi \leftarrow \{[\mathbb{T}, \mathbb{U}]\}$ and the algorithm terminates else set $\Omega \leftarrow \{[[\mathrm{first}(\mathbb{T})], \mathbb{T} \setminus [\mathrm{first}(\mathbb{T})], \mathbb{U}]\}$.

D2. For $i = 2, \ldots, r$ do:

D2.1. Set $\Psi \leftarrow \emptyset$.

D2.2. [Decomposition.] For each $[\bar{\mathbb{T}}, \bar{\mathbb{T}}', \bar{\mathbb{U}}] \in \Omega$ do:

D2.2.1. Set $T \leftarrow \mathrm{first}(\bar{\mathbb{T}}')$, $\bar{\mathbb{T}}' \leftarrow \bar{\mathbb{T}}' \setminus [T]$.

D2.2.2. [Algebraic factorization.] Compute an irreducible factorization of T as $DT_k \doteq F_1 \cdots F_t$ over the algebraic extension field of K with $\bar{\mathbb{T}}$ as an adjoining triangular form.

D2.2.3. Set $\bar{\mathbb{T}}^- \leftarrow [\bar{T} \in \bar{\mathbb{T}} | \ \mathrm{lvar}(\bar{T}) \preceq \mathrm{lvar}(D)]$, $\bar{\mathbb{T}}^+ \leftarrow [\bar{T} \in \bar{\mathbb{T}} | \ \mathrm{lvar}(\bar{T}) \succ \mathrm{lvar}(D)]$. If $D \notin K$ and $\dim(\bar{\mathbb{T}}^-) > 0$ then set $\Phi \leftarrow \Phi \cup \{[\bar{\mathbb{T}}^- \cup \{D\}, \bar{\mathbb{U}}, \bar{\mathbb{T}}^+ \cup [T] \cup \bar{\mathbb{T}}']\}$, $\bar{\mathbb{U}} \leftarrow \bar{\mathbb{U}} \cup \{D\}$.

D2.2.4. [Splitting.] For $j = 1, \ldots, t$ do:

D2.2.4.1. [Reduction.] Set $\bar{\mathbb{U}}' \leftarrow \mathrm{prem}(\bar{\mathbb{U}}, \bar{\mathbb{T}} \cup [F_j])$.

D2.2.4.2. If $0 \notin \bar{\mathbb{U}}'$ then set $\Psi \leftarrow \Psi \cup \{[\bar{\mathbb{T}} \cup [F_j], \bar{\mathbb{T}}', \bar{\mathbb{U}}']\}$.

D2.3. Set $\Omega \leftarrow \Psi$.

D3. Set $\Psi \leftarrow \{[\bar{\mathbb{T}}, \bar{\mathbb{U}}] | \ [\bar{\mathbb{T}}, \phi, \bar{\mathbb{U}}] \in \Psi\}$.

PROOF. There is no loop involved in this algorithm, so the termination is trivial. The correctness of the algorithm follows form Lemma 6 and Remark 4. ∎

EXAMPLE 1E. Let us consider the triangular system $[\mathbb{T}'_3, \mathbb{U}'_3]$ produced in the preceding example. By algebraic factorization one finds that the second polynomial of $\mathbb{T}'_3$ can be factorized as

$$-z^5 + t \doteq (t + 1 + z)(t - z^2 t + z^3 t + 1 - z + z^3 - z^4) \tag{4.5}$$

over the algebraic extension field obtained from Q with the first of $\mathbb{T}'_3$ as adjoining

polynomial. Then by replacing the polynomial $-z^5+t$ with its two factors, respectively, we obtain two triangular systems $[\mathbb{T}_3^*, \mathbb{U}_3^*]$ and $[\mathbb{T}_3^{**}, \mathbb{U}_3^{**}]$ with

$$\mathbb{T}_3^* = [t^2+t+1, z+t+1, -z^3y-t^3, zx^2-t],$$
$$\mathbb{T}_3^{**} = [t^2+t+1, t-z^2t+z^3t+1-z+z^3-z^4, -z^3y-t^3, zx^2-t],$$
$$\mathbb{U}_3^* = \{-t-1\}, \quad \mathbb{U}_3^{**} = \{z\}.$$

Since the third polynomial of $\mathbb{T}_3^*$ and of $\mathbb{T}_3^{**}$ is linear in y (and thus irreducible), we need only to test whether the last polynomial $-t+x^2z$ is irreducible over the successive algebraic extension field $Q(t,z)$ obtained from Q with $[t^2+t+1, z+t+1]$ and with $[t^2+t+1, t-z^2t+z^3t+1-z+z^3-z^4]$ as adjoining triangular forms, respectively. Again, by using algebraic factorization one determines that it is reducible and can be factorized as

$$-t+x^2z \doteq -(t+1)(x+t)(x-t), \tag{4.6}$$

$$\begin{aligned} -t+x^2z \doteq & \frac{z}{3t+2z^3+zt+z^2t+4z^3t+2z^2-2z} \cdot \\ & (xt+2t+z^3t+x+1-z+z^3x+z^3+xz^2+z^2) \cdot \\ & (txz+2z^3x-zt-z^3+xt-t-xtz^2+xtz^3-z^3t+x), \end{aligned} \tag{4.7}$$

respectively, where the factors $t+1$, z and the denominator are viewed as elements of the field $Q(t,z)$. Replacing the last polynomial of $\mathbb{T}_3^*$ and of $\mathbb{T}_3^{**}$ respectively by the two factors whose leading variables are x, we obtain four irreducible triangular systems $[\mathbb{T}_{31}, \mathbb{U}_{31}], \ldots, [\mathbb{T}_{34}, \mathbb{U}_{34}]$ with

$$\mathbb{T}_{31} = [t^2+t+1, z+t+1, -z^3y-t^3, x+t],$$
$$\mathbb{T}_{32} = [t^2+t+1, z+t+1, -z^3y-t^3, x-t],$$
$$\mathbb{T}_{33} = [t^2+t+1, t-z^2t+z^3t+1-z+z^3-z^4, -z^3y-t^3,$$
$$\quad xt+2t+z^3t+x+1-z+z^3x+z^3+xz^2+z^2],$$
$$\mathbb{T}_{34} = [t^2+t+1, t-z^2t+z^3t+1-z+z^3-z^4, -z^3y-t^3,$$
$$\quad txz+2z^3x-zt-z^3+xt-t-xtz^2+xtz^3-z^3t+x],$$
$$\mathbb{U}_{31} = \mathbb{U}_{32} = \{-t-1\}, \quad \mathbb{U}_{33} = \mathbb{U}_{34} = \{z\}.$$

Hence the triangular system $[\mathbb{T}_3', \mathbb{U}_3']$ is decomposed into a set $\Psi = \{[\mathbb{T}_{31}, \mathbb{U}_{31}], \ldots, [\mathbb{T}_{34}, \mathbb{U}_{34}]\}$ of 4 irreducible triangular systems.

As for the corresponding polynomial D in the algebraic factorizations (4.5)-(4.7), it is the constant 1 for the first two cases and is the denominator

$$D = 3t+2z^3+zt+z^2t+4z^3t+2z^2-2z$$

for the last case. Since the irreducible triangular form

$$[t^2+t+1, t-z^2t+z^3t+1-z+z^3-z^4]$$

corresponding to $\bar{\mathbb{T}}^-$ is of dimension 0, by Lemma 5 the adjunction of D into the triangular form does not need to be considered. Therefore, $\Phi = \emptyset$. ∎

ALGORITHM TRIANGULARIZE_I: $\Psi \leftarrow$TRIANGULARIZE_I$(\mathbb{P}, \mathbb{Q})$. *Given a polynomial system* $[\mathbb{P}, \mathbb{Q}]$, *this algorithm computes a set* Ψ *which is either empty, that means* $\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \emptyset$,

or of the form $\{[\mathbb{T}_1, \mathbb{U}_1], \ldots, [\mathbb{T}_e, \mathbb{U}_e]\}$ *such that*

$$\text{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \text{Zero}(\mathbb{T}_i/\mathbb{U}_i), \tag{4.8}$$

where each $[\mathbb{T}_i, \mathbb{U}_i]$ *is an irreducible triangular system.*

T1. Set $\Psi \leftarrow \emptyset$, $\Phi \leftarrow \{[\mathbb{P}, \mathbb{Q}, \phi]\}$.
T2. While $\Phi \neq \emptyset$ do:

T2.1. Set $[\mathbb{P}', \mathbb{Q}', \mathbb{T}'] \leftarrow \text{aef}(\Phi)$, $\Phi \leftarrow \Phi \setminus \{[\mathbb{P}', \mathbb{Q}', \mathbb{T}']\}$.
T2.2. [Quasi-irreducible decomposition.] Compute $\Psi' \leftarrow$ TRIANGULARIZE_Q$(\mathbb{P}', \mathbb{Q}', \mathbb{T}')$.
T2.3. [Decomposition via algebraic factorization.] For each $[\mathbb{T}, \mathbb{U}] \in \Psi'$ do:

T2.3.1. Compute $[\bar{\Psi}, \bar{\Phi}] \leftarrow$ DECOMPOSE$(\mathbb{T}, \mathbb{U})$.
T2.3.2. Set $\Psi \leftarrow \Psi \cup \bar{\Psi}$, $\Phi \leftarrow \Phi \cup \bar{\Phi}$.

The correctness of this algorithm follows from the zero relations (4.1) and (4.4). The termination is guaranteed if the while-loop terminates. We guess that it indeed terminates. However, we are now unable to prove the termination without modifying the algorithm. The troubles are caused by the triplets produced in DECOMPOSE with the polynomial D arising from the algebraic factorization. Our previous arguments based on levels for the termination proof are not applicable in this situation. To ensure the termination, we may modify the algorithm by forming the triplet $[\mathbb{P}' \cup \bar{\mathbb{T}} \cup \{D, T\} \cup \bar{\mathbb{T}}', \bar{\mathbb{U}}, \phi]$ instead of $[\bar{\mathbb{T}}^- \cup \{D\}, \bar{\mathbb{U}}, \bar{\mathbb{T}}^+ \cup [T] \cup \bar{\mathbb{T}}']$ in step D2.2.3 of DECOMPOSE, where $\mathbb{P}'$ is the first component of the corresponding triplet taken from Φ in step T2.1. Then the termination may be proved by considering the ranks of the (quasi-) basic sets of the first polynomial sets of the triplets in the language of characteristic sets. The reason for returning to characteristic sets is that the decomposition of a quasi-irreducible triangular system into irreducible triangular systems is performed bottom-up (see step D2) rather than our top-down strategy. The above modification, in particular, the transit of the $\mathbb{P}'$ from TRIANGULARIZE_I to DECOMPOSE, would increase much complication and destroy the natural form we have presented. The termination problem in the present case is merely of theoretical interest because the set $\bar{\Phi}$ in step T2.3.1 seldom happens to be non-empty (i.e., the corresponding D from the algebraic factorization has to be considered). In fact, for all the 40 complete test examples given in Section 6 we have even never met such a case. In view of this, we are not going to pursue the termination of this algorithm at the cost of its simplicity and natural form in this paper. The termination problem will be clarified later on. In case the termination is much concerned, we can deal with the triplets in $\bar{\Phi}$ produced in step T2.3.1 simply by other methods like the characteristic set method of Ritt-Wu.

EXAMPLE 1F. Let us look at the previous examples. The triangular system $[\mathbb{T}_2, \mathbb{U}_2]$ is trivially irreducible. By using algebraic factorization, it can be determined that the triangular system $[\mathbb{T}_1, \mathbb{U}_1]$ is also irreducible. For the triangular system $[\mathbb{T}_3', \mathbb{U}_3']$, we have seen in the preceding example that it can be decomposed into 4 irreducible triangular systems. It is easy to see that $[\mathbb{T}_3'', \mathbb{U}_3'']$ is reducible, because substitution of $t = 1$ into the second polynomial of $\mathbb{T}_3''$ yields $z^5 - 1$ which is of course reducible. In fact, this triangular system can also be decomposed by the algorithm DECOMPOSE into four irreducible triangular systems $[\mathbb{T}_{35}, \mathbb{U}_{35}], \ldots, [\mathbb{T}_{38}, \mathbb{U}_{38}]$ with $\mathbb{T}_{35} = [t - 1, z - 1, y + 1, x - 1]$, $\mathbb{T}_{36} =$

$[t-1, z-1, y+1, x+1], \mathbb{T}_{37} = [t-1, z^4+z^3+z^2+z+1, z^3y+1, x-z^2], \mathbb{T}_{38} = [t-1, z^4+z^3+z^2+z+1, z^3y+1, x+z^2]$ and $\mathbb{U}_{35} = \mathbb{U}_{36} = \emptyset, \mathbb{U}_{37} = \mathbb{U}_{38} = \{z\}$. We omit the details for this decomposition.

In summary, the original polynomial set $\mathbb{P}$ is decomposed into a sequence of 10 irreducible triangular systems $[\mathbb{T}_1, , \mathbb{U}_1], [\mathbb{T}_2, \mathbb{U}_2], [\mathbb{T}_{31}, \mathbb{U}_{31}], \ldots, [\mathbb{T}_{38}, \mathbb{U}_{38}]$ such that

$$\text{Zero}(\mathbb{P}) = \text{Zero}(\mathbb{T}_1/\mathbb{U}_1) \cup \text{Zero}(\mathbb{T}_2/\mathbb{U}_2) \cup \bigcup_{j=1}^{8} \text{Zero}(\mathbb{T}_{3j}/\mathbb{U}_{3j}).$$

■

Finally, we prove the following remarkable property for the irreducible zero decomposition (4.8).

THEOREM 2. *Let $[\mathbb{P}, \mathbb{Q}]$ be a polynomial system having a zero decomposition of the form (4.8), where every $[\mathbb{T}_i, \mathbb{U}_i]$ is an irreducible triangular system.*

a)† *Then* $\text{prem}(P, \mathbb{T}_i) = 0$ *for all* $P \in \mathbb{P}$ *and* $\text{prem}(Q, \mathbb{T}_i) \neq 0$ *for any* $Q \in \mathbb{Q}$.

b) *Let* $\mathbb{I}_i = \{\text{ini}(T) | \ T \in \mathbb{T}_i\}$ *for each* i. *Then the irreducible zero decomposition* (4.8) *can be replaced by*

$$\text{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \text{Zero}(\mathbb{T}_i/\mathbb{I}_i \cup \mathbb{Q}). \tag{4.9}$$

Moreover, for any i, *if* $\dim(\mathbb{T}_i) = 0$, *then* $\text{Zero}(\mathbb{T}_i/\mathbb{I}_i \cup \mathbb{Q})$ *in* (4.9) *can be simplified to* $\text{Zero}(\mathbb{T}_i/\mathbb{Q})$.

PROOF. *a*) Let η be any generic point of $\mathbb{T}_i$. Since $0 \notin \text{prem}(\mathbb{U}_i, \mathbb{T}_i)$, by Lemma 4 η is not a zero of any polynomial in $\mathbb{U}_i$. It follows that $\eta \in \text{Zero}(\mathbb{T}_i/\mathbb{U}_i)$, so that $\eta \in \text{Zero}(\mathbb{P}/\mathbb{Q})$. Hence, η is a zero of all polynomials in $\mathbb{P}$ but not a zero of any polynomial in $\mathbb{Q}$. By Lemma 4 again, all polynomials in $\mathbb{P}$ have remainder 0 with respect to $\mathbb{T}_i$ and every polynomial in $\mathbb{Q}$ has remainder non-zero with respect to $\mathbb{T}_i$.

b) By *a*) just proved and the remainder formula, any element of the zero set on the right-hand side of (4.9) is contained in the zero set on the left-hand side. On the contrary, let $\bar{x} \in \text{Zero}(\mathbb{P}/\mathbb{Q})$. Then by (4.8) there is an i such that $\bar{x} \in \text{Zero}(\mathbb{T}_i/\mathbb{U}_i)$. Since $[\mathbb{T}_i, \mathbb{U}_i]$ is a triangular system, $\bar{x}$ is not a zero of any polynomial in $\mathbb{I}$. Hence $\bar{x} \in \text{Zero}(\mathbb{T}_i/\mathbb{I}_i \cup \mathbb{Q})$, i.e., $\bar{x}$ is contained in the zero set on the right-hand side of (4.9). For any i, if $\dim(\mathbb{T}_i) = 0$, by Lemma 5 $\text{Zero}(\mathbb{T}_i/\mathbb{I}_i \cup \mathbb{Q})$ can be simplified to $\text{Zero}(\mathbb{T}_i/\mathbb{Q})$. ■

If we consider the special case $\mathbb{Q} = \emptyset$, then the decomposition (4.9) becomes

$$\text{Zero}(\mathbb{P}) = \bigcup_{i=1}^{e} \text{Zero}(\mathbb{T}_i/\mathbb{I}_i).$$

Now the zero set $\text{Zero}(\mathbb{P})$ defines an algebraic variety, say V, yet each $\text{Zero}(\mathbb{T}_i/\mathbb{I}_i)$ does not necessarily define an algebraic variety (it defines a *quasi-variety*). In order to decompose V into irreducible components, we have to determine, from each $\mathbb{T}_i$, a finite set of

† This property is satisfied for each irreducible triangular system $[\mathbb{T}_i, \mathbb{U}_i]$, no matter whether or not the other triangular systems are irreducible. It can be used to avoid some verifications of the 0 remainder in Ritt-Wu's zero decompositions.

polynomials that defines an irreducible subvariety of V. This can be done as usual by using methods such as those based on Chow bases (Wu, 1989) and Gröbner bases (Wang, 1989).

5. Relationship and Comparisons with Other Elimination Methods

The discovery of our elimination method was inspired by the elimination theory of Seidenberg and our through study of the method of characteristic sets. However, it can be seen clearly that the method presented in the previous sections has a big difference from the original method of Seidenberg at least in the following aspects. First, the method of Seidenberg only concerns with the solvability of polynomial systems and no concept of triangular forms or so was introduced, while our method not only deals with the solvability problem but also establishes the zero relations between the given polynomial system and the produced triangular systems. We are interested not only in the existence of zeros of a polynomial system (or in other words solutions of the polynomial equations and inequations) but also in finding possible zeros and establishing the structural relations of zeros between the given system and eliminated triangular systems. Second, the elimination performed without projection was not considered by Seidenberg, and neither was the concept of irreducible triangular forms, nor the irreducible zero decomposition. Even for determining the solvability of polynomial systems, we have made several improvements to the original method of Seidenberg which premise the method to be of practical value.

The principal reduction in our elimination method is pseudo-division. It is apparently different from the reduction in the Gröbner basis method (Buchberger, 1970, 1985). Our method differs from the Gröbner basis method also by its style. The latter provides many nice properties with ideals, while in our method the use of ideals is essentially avoided. Instead we are concerned with properties about the difference sets of zeros of polynomial sets. Of course, there are many problems to which both methods can be applied. As in practice, preliminary experiments show that the efficiency of our method is comparable with that of the Gröbner basis method. We expect to have a more systematic comparison of our method with the Gröbner basis method (as well as other existing methods not comprehensively discussed in this paper) in the future.

Our method does not seem to be much related to the resultant-based methods. But we are interested in investigating their relationship. It is easy to see that our method has similarities to all the pseudo-division-based methods including Ritt-Wu's characteristic sets (Ritt, 1932, 1950, Wu, 1984a, 1986), Lazard's triangular sets (Lazard, 1991, 1992) and Kalkbrener's regular chains (Kalkbrener, 1991), yet it is different from each of them. Our method differs from the method of characteristic sets by its style and structure, whereas the goal and applicability of both are quite similar. We have also used some concepts and results from the theory and method of characteristic sets. The design of a method in the present form has been our intention to overcome the difficulties inherent in the method of characteristic sets by borrowing the ideas of Seidenberg. Let us first discuss the relationship, similarities and differences between our method and Ritt-Wu's characteristic sets as follows (which explain why our method appears to be more efficient than Ritt-Wu's for the test examples as shown in the table of the next section).

a) In the characteristic set method, the elimination is performed simultaneously for all the variables. It is a common feeling that the top-down elimination is more efficient, and researchers have tried to use it to triangularize polynomial sets in the characteristic sets computation (see Chou, 1989, Ko & Chou, 1985 and Wang, 1989). However, the

top-down procedures proposed so far are incomplete and/or only as heuristics because the triangularized sets are not guaranteed to be characteristic sets. As one of the different features our method successfully employs the top-down elimination by splitting the polynomial system when pseudo-division is performed, which relaxes the requirement for the produced triangular forms to be characteristic sets while preserves the necessary zero relations still.

b) For a computed ascending set $\mathbb{C}$ to be the characteristic set of an input polynomial set $\mathbb{P}$ one has to ensure that $\text{prem}(P, \mathbb{C}) = 0$ for all $P \in \mathbb{P}$. This leads to extensive verifications of the 0 remainder which are very time-consuming. The author has proposed some heuristics (Wang, 1992b) which can avoid some verifications of the 0 remainder but do not enable the problem be entirely settled. In our new elimination method, there are no verifications of the 0 remainder. For this method not a triangular form of a given polynomial set is defined.

c) An ascending set in Ritt's sense is a triangular form $\mathbb{T} = [T_1, \ldots, T_r]$ with the requirement that $\deg(T_j, \text{lvar}(T_i)) < \deg(T_i, \text{lvar}(T_i))$ for each pair $j > i$. Having this requirement satisfied in the characteristic sets computation often increases the size of polynomials. This leads to the usage of different senses like the quasi-sense and weak sense of Wu. Since an ascending set in the quasi-sense (that is a triangular form, not necessarily fine) may not be well defined, it is not possible to set up the whole theory for characteristic sets in this sense. An alternative as proposed in Chou (1989) is to verify whether the remainders of the initials with respect to the ascending set are 0. In this approach, it is hard to avoid the repetition of verifications. In our method, the remainders of the initials with respect to the triangular form are collected (maybe with other polynomials) as the second component of the triangular system, which both solves the problem of polynomial size and avoids the possible repetition of remainder computations.

d) Without using polynomial factorization over algebraic extension fields the original method of characteristic sets is not complete for determining the solvability of a polynomial system. In a coarse zero decomposition, some empty components are not necessarily detected. It is now possible to determine the solvability of a polynomial system by computing characteristic sets with no algebraic factorization but the projection theorem of Wu (1990). For Wu's projection method, a complete zero decomposition has to be computed before each projection of dimension 1 is performed. In our method the projection process is embedded in the elimination procedure.

e) In the various decompositions for $\text{Zero}(\mathbb{P}/\mathbb{Q})$ based on characteristic sets, $\text{Zero}(\mathbb{C}_i/\mathbb{Q} \cup \mathbb{I}_i)$ or the like is placed instead of the corresponding $\text{Zero}(\mathbb{T}_i/\mathbb{U}_i)$ in our zero decompositions, where each $\mathbb{C}_i$ is an ascending set and $\mathbb{I}_i = \{\text{ini}(C) | \, C \in \mathbb{C}_i\}$ having the properties that $\text{prem}(\mathbb{P}, \mathbb{C}_i) = \{0\}$ and $0 \notin \text{prem}(\mathbb{Q}, \mathbb{C}_i)$. The first property may be lost in our zero decompositions: there is in general no guarantee that $\text{prem}(\mathbb{P}, \mathbb{T}_i) = \{0\}$. Moreover, each $\mathbb{U}_i$ may contain many more polynomials than $\mathbb{Q} \cup \mathbb{I}_i$ does. It is remarkable that the lost property is recovered in our method (Theorem 2) when we arrive at an irreducible zero decomposition. Therefore, the construction of irreducible algebraic varieties from the irreducible zero decomposition in our case is straightforward, as it is done from the irreducible zero decomposition based on characteristic sets.

f) The characteristic sets computation for the enlarged polynomial sets obtained by successive adjunction of initials in general has to perform pseudo-divisions which have been done previously. This leads to a lot of unnecessary repeated computations. In our method, the already triangularized systems are retained along with the triplets or quadru-

plets. This helps keep the amount of information useful for the subsequent computation so that the repeated computations are avoided.

g) It appears that our algorithms may produce a large number of branches. Nevertheless, the branch problem here is actually not more serious than that in the characteristic sets computation. This is partially because many of the branches produced in our algorithms are empty (i.e., the corresponding polynomial systems have no zeros) and more polynomials in the second component of a polynomial system, which has no zero, more chances they create to discard the system. Some analysis shows that the number of involved pseudo-divisions for the triangularization in our algorithms is similar to that in the corresponding algorithms based on characteristic sets (for the input polynomials to which the algorithms are applicable within the current hardware facilities). Due to the advantages explained above the computation for every individual branch in our algorithms is less expensive. In any case, it is profitable and necessary to detect the empty components via heuristics.

In what follows we try to point out some differences and similarities between our method and the elimination methods of Lazard (1991, 1992) and Kalkbrener (1991), which the author has been already aware of. Due to our limited understanding of these two methods and the lake of necessary practical experiments with them, we are certainly not in the position of comparing the efficiency of these methods. A systematic analysis and comparison among them both theoretically and practically remain interesting for future work.

h) Lazard's method has an objective at improving the characteristic set method in the direction of having more canonical representations for zeros of polynomial systems. To this end, some conditions such as normality and squarefreeness are imposed on the so-called *triangular sets* in Lazard's terminology. The canonical representation property is not preserved in our method, nor in the method of Kalkbrener. The so-called *regular chains* which are stronger than (fine, perfect) triangular forms were introduced in Kalkbrener's method to represent the generic points of the irreducible components of an unmixed-dimensional algebraic variety with an aim at computing an unmixed-dimensional decomposition for any given algebraic variety. In both the methods of Lazard and Kalkbrener, the irreducibility requirement is dropped by performing the GCD and resultant computation of univariate polynomials over extension fields, rather than projection as in our method.

i) The structure of the algorithms of Lazard and Kalkbrener is different from that of ours. Their algorithms use an incremental elimination which in some sense is between the bottom-up and top-down procedures, whereas our algorithms have a tree structure (which allows easy parallelization) with top-down elimination as pointed out previously.

j) Since the irreducibility requirement is dropped for the triangular sets and regular chains, the irreducible zero decomposition was not considered in Lazard's and Kalkbrener's methods. Therefore, their methods cannot be well applied to such problems as the irreducible decomposition of algebraic varieties where the irreducibility issue is essential. As the irreducible decomposition requires polynomial factorization over successive algebraic extension fields, it has been considered as a bottle-neck and as an obstacle to bypass. However, our experiments (see the next section) show that algebraic factorization is not necessarily the most time-consuming process within the elimination methods, and the irreducible zero decomposition is not much more expensive than the other decompositions. See also our previous experiments on the characteristic set method (Wang, 1991, 1992b).

k) The technique of splitting polynomial systems into subsystems when the problem of "zero-divisors" occurs during the computation of GCD's and pseudo-divisions are also employed in the methods of Lazard and Kalkbrener. However, the use of this technique in their methods is different in some way from that in ours. It appears that the splitting in our subalgorithm ELIMINATE is somewhat close to that used in Kalkbrener's algorithm $\mathbf{ggcd}_n$.

l) As already repeated, in our method the drop of irreducibility is accomplished by performing the projection. The projection process is incorporated partially in Lazard's and Kalkbrener's methods via (normalization and GCD) computations over extension fields represented by triangular sets and regular chains. The similarity among the methods in this aspect increases when we perform the projection in Case B according to Remark 3. Also see the concepts of normal ascending sets in Wang (1990), regular chains and *p*-chains in Gao & Chou (1992).

m) The verifications of the 0 remainder, which are necessary in the characteristic sets computation, are also avoided, at least partially, in the methods of Lazard and Kalkbrener. We are not clear whether there are some verifications behind in these two methods.

6. Implementation and Experiments

For an implementation of the algorithms described in the previous sections several details should be carefully taken into account for the sake of efficiency and tidy output. Such details include (i) quitting the while-loop whenever $\mathbb{P}'$ occurs to contain a constant, (ii) removing the factors of the polynomials in $\mathbb{P}'$ which are the divisors of some polynomials in $\mathbb{Q}'$, (iii) squarefreeing the produced polynomials or freeing their power products, (iv) compressing $\mathbb{Q}'$ by examining the common divisors of its polynomials, (v) splitting the systems via factorization of the initials, (vi) discarding the empty components via GCD computation and other heuristics, and (vii) deleting some polynomials from $\mathbb{Q}'$ by verifying their GCD's with the polynomials in $\mathbb{T}'$. Most of these techniques are related to polynomial division, squarefree decomposition, GCD computation and polynomial factorization which are all time-consuming. The efficiency of the algorithms can be enhanced if, and only if, the techniques are appropriately implemented. It should be noted that the removal of redundant factors is of particular importance. This is why we even included the simple subalgorithm SIMPLIFY in our early presentation of the method (see Wang, 1993). This subalgorithm as well as other details is omitted in this paper for simplicity.

A draft implementation of our algorithms with some of the above-mentioned techniques has been made in the Maple system. Preliminary experiments show that the method is very efficient (though its theoretical complexity has not yet been analyzed). The extent of its efficiency is at least comparable with that of the methods of characteristic sets and Gröbner bases. In the table below, we give timings for the algorithms with our current implementation. The experimental data are for the same set of 50 test examples as experimented in Wang (1991, 1992b) for the zero decompositions based on Ritt-Wu's characteristic sets. In the case without using factorization, our algorithm TRIANGULARIZE is faster than all 3 variants of Ritt-Wu's algorithm for 37 of the 40 successful examples, and in the case of using algebraic factorization, our algorithm TRIANGULARIZE_I is faster than Ritt-Wu's algorithm for 36 of the 40 successful examples. The interested reader may compare the following table with the known timings for Gröbner bases computation and the tables given in Wang (1991, 1992b, 1993). The speed-ups here with respect to our

experiments reported in Wang (1993) are achieved mainly by some heuristic detection of the empty components.

Example	TRIANGULARIZE	TRIANGULARIZE_P	TRIANGULARIZE_Q	TRIANGULARIZE_I
1	1.817	3.617	5.967	♣19.000
2	67.383	75.733	77.150	77.783
3	—	—	—	—
5	5.966	6.050	7.133	♣9.484
6	1.133	>2000	4.600	4.667
8	.450	.533	.550	.834
9	3.100	3.833	3.533	♣4.533
10	.167	.217	.233	.267
11	.383	.399	.717	1.684
12	31.633	47.034	72.500	♣82.000
13	.117	.100	.150	.167
14	>2000	>2000	>2000	>2000
15	2.100	97.550	4.133	4.133
16	>2000	>2000	>2000	>2000
17	130.217	>2000	185.617	190.000
18	.634	1.217	1.300	1.333
19	6.950	—	11.033	11.150
20	1.000	1.166	1.800	2.217
21	>2000	>2000	>2000	>2000
22	24.016	>2000	34.567	34.734
23	1.717	1.916	2.750	♣18.500
24	11.316	234.717	20.400	♣27.050
25	2.067	—	4.866	4.916
26	1.783	2.133	1.717	1.767
27	1.866	3.400	2.600	3.133
28	1.817	26.283	3.034	3.150
29	.783	.850	1.767	♣23.317
30	6.217	6.466	6.333	6.400
32	3.033	2.733	3.700	4.584
33	51.917	366.517	63.967	68.166
34	>2000	>2000	>2000	>2000
35	10.533	23.333	13.450	14.367
36	.200	.183	.183	.233
37	.467	.500	.383	.550
38	2.117	17.367	3.617	3.850
39	40.233	>2000	44.883	45.650
41	22.083	22.184	27.050	30.351
42	.517	.566	.650	.683
43	22.233	>2000	39.517	♣256.300
44	20.167	35.034	21.533	25.083
45	2.250	13.350	3.767	4.017
46	1.033	1.650	.983	1.017
47	6.617	>2000	15.717	♣196.050
48	.617	.667	1.000	1.467
49	28.633	30.517	120.117	122.433

The experiments were made on an Apollo DN10000 under a UNIX operating system. The elimination by TRIANGULARIZE_P is performed with full projection. The timings are given in CPU seconds and include the time for garbage collection. The cases in which

the computation was rejected by the Maple system for the reason "object too large" are indicated by —, and in which polynomial factorization over algebraic extension fields† is required are indicated by ♣.

From the table above, one sees that the elimination with full projection is sometimes rather expensive and is even more expensive than the irreducible zero decomposition. The computational costs increase dramatically when the polynomials are powered in the projection case B. We feel that the amount of computing time for our algorithms can be considerably reduced by some practical improvements on the implementation issue. We shall report further timing statistics and make a systematic comparison on the practical efficiency and applicability of our method with other existing ones in the near future.

Below we give some remarks on a few examples which appear to be quite encouraging. The timings concerning characteristic sets and Gröbner bases were obtained by using the author's charsets package (Wang, 1992a) and the built-in grobner package in Maple 4.3 on the same machine.

Let us first report on the timings about Examples 1a-1f (which are actually the test example 29) used for illustration throughout the paper. The elimination without projection by TRIANGULARIZE was carried out in 0.783 seconds. When the elimination is performed with full projection, it took 0.85 seconds. The decomposition took 1.767 seconds by TRIANGULARIZE_Q and 23.317 seconds by TRIANGULARIZE_I.

However, with respect to the pure lexicographic ordering the computation of the Gröbner basis of $\mathbb{P}$ by using the built-in grobner package of Maple 4.3 requires 898.266 seconds. With respect to the same variable ordering, the computation of the coarse zero decomposition took 158.150 seconds by using Ritt's original algorithm of characteristic sets and 67.467, 67.650, 81.467 seconds respectively by using three different variants of Wu's improved algorithm. By a strategy proposed in Wang (1992b) the times for Wu's algorithm can be reduced to 3.35, 3.06, 20.334 seconds, respectively. The irreducible zero decomposition using Ritt-Wu's algorithm in two variants took 203.349 and 832.9 seconds, respectively.

EXAMPLE 2 (Test example 47). Determine the implicit form (in the variables x and y) of the curve given by the following system of equations

$$\begin{aligned}
&(x-u)^2+(y-v)^2-1=0,\\
&v^2-u^3=0,\\
&2v(x-u)+3u^2(y-v)=0,\\
&(3wu^2-1)(2wv-1)=0.
\end{aligned}$$

This is a formulation of an offset to the curve $y^2-x^3=0$. The example was communicated by P. Vermeer from the Department of Computer Science, Purdue University. The author was told that it ran out of swap space (280 MB) before completing the computation by using the Gröbner basis implementation available in Macsyma on a Symbolic machine for getting the solution. We have tried to compute the Gröbner basis of the corresponding polynomial set (with respect to the pure lexicographic ordering determined by $x \prec y \prec u \prec v \prec w$) in Maple 4.3 on our Apollo DN10000 without success within 2000 seconds. We

† From the timing difference between TRIANGULARIZE_I and TRIANGULARIZE_Q, one may see the costs of algebraic factorization, where the routines for algebraic factorization are implemented on the basis of two algorithms, one proposed by the author jointly with S. Hu and the other by the author alone.

have also tried to determine the implicit equations by using the characteristic set method with Wu's projection theorem. First, we do not decompose the polynomial set according to the given factorization of the last polynomial. The computation of the characteristic set (with respect to the same variable ordering) is very easy (in 10.1 seconds), but the zero decomposition is rather difficult. We tried to compute it with six variants, of which four did not succeed within 2000 CPU seconds. For the two successful variants, 11 quasi-irreducible ascending sets were produced in 937.3 and 1003.883 seconds, respectively (Wang, 1991). The biggest integer coefficient of the occurring polynomials has more than 800 digits (while the biggest coefficient of the input polynomials is 6). The projection of these ascending sets using the author's implementation of Wu's algorithm took more than 2000 seconds. The irreducibility test of the 11 ascending sets all requires polynomial factorization over algebraic extension fields, and we did not succeed in completing the factorization of all the polynomials within 2000 seconds of time limit.

If we decompose the input set into two sets of polynomials, then the quasi-irreducible zero decomposition can be computed in about 740 seconds, yielding 18 ascending sets, where the occurring polynomials have big integer coefficients too. Among these ascending sets, the irreducibility of 4 is trivial (as in each of them there is only one polynomial having high degree in its leading variable) and the irreducibility test of the remaining 14 ascending sets all needs polynomial factorization over algebraic extension fields, too. We did not succeed in factorizing these polynomials within 2000 seconds either.

By using our algorithms, the elimination without projection took 6.617 seconds, yielding 5 triangular systems. If the elimination is performed with projection of dimension 3, then 5 triangular systems can be computed in 18.534 seconds. From them and with some simplification we were able to determine the implicit equations (see Wang, 1993). However, we failed in computing the triangular systems with full projection within 2000 seconds. The (quasi-) irreducible decomposition can be computed in (15.717) 196.05 seconds, yielding 14 irreducible triangular systems. If the input polynomial set is decomposed into two sets, then the elimination without projection took 5.316 and 5.383 seconds, respectively, yielding 12 (= 6 + 6) triangular systems. When the elimination is performed with projection of dimension 3, it took 17.5 and 16.95 seconds, respectively, yielding 11 (= 5 + 6) triangular systems. The (quasi-) irreducible decomposition for the two polynomial sets took (9.267) 164.7 and (9.217) 153.067 seconds, respectively, yielding 14 (= 7 + 7) irreducible triangular systems.

Note that some of the produced triangular systems counted above are redundant. We shall discuss elsewhere how to remove such redundant triangular systems. ■

EXAMPLE 3 (Test example 17). As another example, let us consider the following set $\mathbb{P}$ of four polynomials

$$
\begin{aligned}
F_1 &= 2(b-1)^2 + 2(q - pq + p^2) + c^2(q-1)^2 - 2bq + 2cd(1-q)(q-p) \\
&\quad + 2bpqd(d-c) + b^2d^2(1-2p) + 2bd^2(p-q) + 2bdc(p-1) + 2bpq(c+1) \\
&\quad + (b^2 - 2b)p^2d^2 + 2b^2p^2 + 4b(1-b)p + d^2(p-q)^2, \\
F_2 &= d(2p+1)(q-p) + c(p+2)(1-q) + b(b-2)d + b(1-2b)pd \\
&\quad + bc(q + p - pq - 1) + b(b+1)p^2d, \\
F_3 &= -b^2(p-1)^2 + 2p(p-q) - 2(q-1), \\
F_4 &= b^2 + 4(p-q^2) + 3c^2(q-1)^2 - 3d^2(p-q)^2 + 3b^2d^2(p-1)^2 + b^2p(p-2) \\
&\quad + 6bdc(p + q + pq - 1)
\end{aligned}
$$

taken from a paper by Czapor & Geddes (Proc. SYMSAC'86, 233-237). We consider b as a free parameter and fix the ordering of the other variables as $p \prec d \prec c \prec q$.

It is not very difficult to compute a characteristic set of $\mathbb{P}$. For different variants and in different senses the CPU time for computing the characteristic set ranges from some tens to hundreds of seconds. To compute a zero decomposition of $\mathbb{P}$, we tried six variants of Ritt-Wu's algorithm, but did not succeed in any variant within 2000 CPU seconds.

By using our algorithms, the coarse zero decomposition (without projection), quasi-irreducible and irreducible zero decompositions can all be computed within 200 seconds as shown in the table. We note in passing that the Gröbner bases of $\mathbb{P}$ with respect to the total degree ordering and the pure lexicographic ordering determined by $p \prec d \prec c \prec q$ both cannot be computed within 2000 seconds by using the Maple built-in package. ■

Finally, we remark that there are several other test examples for which the zero decompositions by using our algorithms took much less time than those by using Ritt-Wu's. However, there is also a couple of examples, notably numbers 12 and 49, for which our method took more time. We have not completely made clear the reason for this, since the computational behaviour in both of the methods is quite complex. It seems to be due to the branch expansion and the reducibility of many polynomials occurring in the computation. It is also observed that for these examples some of the characteristic sets are much simpler than the corresponding triangular forms in terms of polynomial size.

ACKNOWLEDGMENTS. This work has been supported in part by the Austrian Ministry of Science and the Commission of the European Communities under ESPRIT Basic Research Action 3125 (MEDLAR I) and Project 6471 (MEDLAR II). The author wishes to thank two referees for their valuable comments on improving the presentation.

References

Boyer, C. B. (1968). *A History of Mathematics.* New York: John Wiley & Sons.

Buchberger, B. (1970). An algorithmical criterion for the solvability of algebraic systems of equations (in German). *Aequantiones Math.* 4, 374-383.

Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. In: *Multidimensional Systems Theory* (N. K. Bose, ed.). Dordrecht-Boston: D. Reidel Publishing Company, pp. 184-232.

Canny, J. F., Kaltofen, E. and Yagati, L. (1989). Solving systems of non-linear polynomial equations faster. *Proc. ISSAC'89* (G. H. Gonnet, ed.), pp. 121-128.

Chou, S. C. (1989). *Mechanical Geometry Theorem Proving.* Dordrecht-Boston-Lancaster-Tokyo: D. Reidel Publishing Company.

Euler, L. (1840). *Elements of Algebra.* Translated by Rev. John Hewlett. London: Longman, Orme, and Co. Reprinted by Springer-Verlag.

Gao, X. S. and Chou, S. C. (1992). Solving parametric algebraic systems. *MM Research Preprints* No. 7, 14-30.

Gauss, C. F. (1873). *Werke.* Band IV, Herausgegeben von der Königlichen Gesellschaft der Wissenshaft zu Göttingen.

Gianni, P., Trager, B. and Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comput.* 6, 149-167.

Gröbner, W. (1949). *Moderne Algebraische Geometrie.* Wien-Innsbruck: Springer-Verlag.

Grigor'ev, D. Yu. and Chistov, A. L. (1983). Subexponential-time solving systems of algebraic equations. *Preprints* LOMI E-9-83 and E-10-83, Leningrad.

Grigor'ev, D. Yu. and Chistov, A. L. (1984). Fast decomposition of polynomials into irreducible

ones and the solution of systems of algebraic equations. *Soviet Math. Dokl.* (AMS Translation) **29**, 380-383.

Hodge, W. V. D. and Pedoe, D. (1947). *Methods of Algebraic Geometry*, Vol. I. Cambridge: Cambridge Univ. Press.

Jacobson, N. (1974). *Basic Algebra I.* San Francisco: W. H. Freeman and Company.

Kalkbrener, M. (1991). *Three Contributions to Elimination Theory.* Ph.D thesis. RISC-LINZ, Johannes Kepler Univ., Austria.

Ko, H. P. and Chou, S. C. (1985). Polynomial triangulation for pseudo common divisors. *Technical Report 85CRD242.* General Electric Company, USA.

Lazard, D. (1979). Systems of algebraic equations. *Proc. EUROSAM'79* (E. W. Ng, ed.), pp. 88-94.

Lazard, D. (1981). Resolution des systemes d'equation algebriques. *Theoretical Comput. Sci.* **15**, 77-110.

Lazard, D. (1991). A new method for solving algebraic systems of positive dimension. *Discrete Applied Math.* **33**, 147-160.

Lazard, D. (1992). Solving zero-dimensional algebraic systems. *J. Symb. Comput.* **13**, 117-131.

Macaulay, F. S. (1916). *The Algebraic Theory of Modular Systems.* Cambridge: Cambridge Univ. Press. Reprinted by Stechert-Hafner Service Agency (1964).

Needham, J. (1959). *Science and Civilisation in China*, Vol. 3. Cambridge: Cambridge Univ. Press.

Ritt, J. F. (1932). *Differential Equations from the Algebraic Standpoint.* New York: Amer. Math. Soc.

Ritt, J. F. (1950). *Differential Algebra.* New York: Amer. Math. Soc.

Seidenberg, A. (1956a). Some remarks on Hilbert's Nullstellensatz. *Arch. Math.* **7**, 235-240.

Seidenberg, A. (1956b). An elimination theory for differential algebra. *Univ. California Publ. Math.* (N.S.) **3**(2), 31-66.

Seidenberg, A. (1969). On k-constructable sets, k-elementary formulae, and elimination theory. *J. reine angew. Math.* **239/240**, 256-267.

Sturmfels, B. (1991). Sparse elimination theory. *Comput. Algebraic Geometry and Commutative Algebra* (D. Eisenbud and L. Robbiano, eds.), to appear.

Sylvester, J. J. (1904). *The Collected Mathematical Papers*, Vol. I. Cambridge: Cambridge Univ. Press.

Tarski, A. (1951). *A Decision Method for Elementary Algebra and Geometry.* Berkeley-Los Angeles: Univ. of California Press.

Wang, D. M. (1989). Characteristic sets and zero structure of polynomial sets. *Lecture Notes.* RISC-LINZ, Johannes Kepler Univ., Austria.

Wang, D. M. (1990). Some notes on algebraic methods for geometry theorem proving. *Preprint.* Presented at MEDLAR 12-Month Workshop (Schloß Weinberg, Austria, November 1990).

Wang, D. M. (1991). On Wu's method for solving systems of algebraic equations. *RISC-Linz Series* no. 91-52.0. Johannes Kepler Univ., Austria.

Wang, D. M. (1992a). An implementation of the characteristic set method in Maple. *Proc. DISCO'92* (Bath, England, April 13-15, 1992), to appear.

Wang, D. M. (1992b). Some improvements on Wu's method for solving systems of algebraic equations. *Proc. Int. Workshop Math. Mechanization* (Beijing, July 16-18, 1992), pp. 89-100.

Wang, D. M. (1993). An elimination method based on Seidenberg's theory and its applications. *Comput. Algebraic Geometry* (F. Eyssette and A. Galligo, eds.), Progress in Math. **109**, Birkhäuser, Boston, pp. 301-328.

Wu, W. T. (1984a). Basic principles of mechanical theorem proving in elementary geometries. *J. Sys. Sci. & Math. Scis.* **4**, 207-235; *J. Automated Reasoning* **2**, 221-252 (1986).

Wu, W. T. (1984b). *Basic Principles of Mechanical Theorem Proving in Geometries (Part on elementary geometries).* Beijing: Science Press.

Wu, W. T. (1986). On zeros of algebraic equations — An application of Ritt principle. *Kexue Tongbao* **31**, 1-5.

Wu, W. T. (1987). A zero structure theorem for polynomial equations-solving. *MM Research Preprints* No. 1, 2-12.

Wu, W. T. (1989). On the generic zero and Chow basis of an irreducible ascending set. *MM Research Preprints* No. 4, 1-21.

Wu, W. T. (1990). On a projection theorem of quasi-varieties in elimination theory. *Chinese Ann. Math. Ser. B* **11**(2), 220-226.

Author's present address:

LIFIA - IMAG - CNRS, 46, avenue Félix Viallet, 38031 Grenoble Cédex, France