DECOMPOSITION OF POLYNOMIAL SETS INTO CHARACTERISTIC PAIRS

DONGMING WANG, RINA DONG, AND CHENQI MOU

ABSTRACT. A characteristic pair is a pair $(\mathcal{G}, \mathcal{C})$ of polynomial sets in which $\mathcal{G}$ is a reduced lexicographic Gröbner basis and $\mathcal{C}$ is the minimal triangular set contained in $\mathcal{G}$. It is said to be normal (or strong normal) if $\mathcal{C}$ is normal (or $\mathcal{C}$ is normal and its saturated ideal equals the ideal generated by $\mathcal{G}$). In this paper, we show that any finite polynomial set $\mathcal{P}$ can be decomposed algorithmically into finitely many (strong) normal characteristic pairs with associated zero relations, which provide representations for the zero set of $\mathcal{P}$ in terms of those of Gröbner bases and those of triangular sets. The algorithm we propose for the decomposition makes use of the inherent connection between Ritt characteristic sets and lexicographic Gröbner bases and is based essentially on the structural properties and the computation of lexicographic Gröbner bases. Several nice properties about the decomposition and the resulting (strong) normal characteristic pairs, in particular relationships between the Gröbner basis and the triangular set in each pair, are established. Examples are given to illustrate the algorithm and some of the properties.

1. INTRODUCTION

Systems of polynomial equations are fundamental objects of study in mathematics which occur in many domains of science and engineering. Such systems may be triangularized by using the well-known method of Gaussian elimination when the equations are linear. There are two approaches, developed on the basis of characteristic sets [37, 49] and Gröbner bases [7, 12], which can be considered as generalizations of Gaussian elimination to the case where the equations are nonlinear. Following these approaches of triangularization, the present paper is concerned with the problem of decomposing an arbitrary set $\mathcal{P}$ of multivariate polynomials into finitely many triangular sets of polynomials that may be used to represent the set of zeros of $\mathcal{P}$ (or equivalently the algebraic variety defined by $\mathcal{P}$, or the radical of the ideal generated by $\mathcal{P}$). This problem of triangular decomposition is conceptually simple, but computationally difficult, and to it satisfactory algorithmic solutions are of both theoretical interest and practical value. The last three decades have witnessed extensive research on polynomial elimination and triangular decomposition, which led to significant developments on the theories, methods, and software tools for polynomial system solving (see, e.g., [3–5, 8–10, 20, 25, 27, 30, 36, 40–42, 48, 50] and

1993

references therein). Along with these developments, triangular decomposition has become a standard approach to studying computational problems in commutative algebra and algebraic geometry, a basic toolkit for building advanced functions in modern computer algebra systems, and a general and powerful technique of breaking complex polynomial systems down into simply structured, easily manageable subsystems for diverse scientific and engineering applications.

To make our statements precise, we fix an order for the variables of the polynomials in question. A *triangular set* $\mathcal{T}$ is meant as an ordered set of polynomials whose greatest variables strictly increase with respect to the fixed variable order. $\mathcal{T}$ is said to be *normal* or called a *normal set* if none of the greatest variables occurs in the leading coefficients of the polynomials in $\mathcal{T}$ with respect to their greatest variables. By a *polynomial system* we mean a pair $[\mathcal{P}, \mathcal{Q}]$ of polynomial sets with which the system of polynomial equations $\mathcal{P} = 0$ and inequations $\mathcal{Q} \neq 0$ is of concern. It is called a *triangular system* or a *normal system*, respectively, if $\mathcal{P}$ is a triangular set or a normal set and $\mathcal{Q}$ satisfies certain subsidiary conditions.

Effective algorithms are now available for decomposing arbitrary polynomial sets or systems of moderate size into triangular sets or systems of various kinds (regular, simple, irreducible, etc.) [27, 33, 43, 45], though it is not yet clear how to measure the quality of triangular decompositions and how to produce triangular sets or systems of high quality in terms of theoretical properties (such as uniqueness, squarefreeness, and normality) and simplicity of expression (with lower degree, smaller size, and fewer components, etc.). One way to obtain "good" triangular decompositions is via computation of lexicographic (lex) Gröbner bases, where the lex term ordering determined by the variable order ensures that the bases have certain triangular structures with nice algebraic properties [6, 12]. For the zero-dimensional case, relationships between Gröbner bases and triangular sets were studied in [31], leading to algorithms for the computation of triangular sets from lex Gröbner bases based on factorization and the D5 principle [14]. More recently, an algorithm for triangular decomposition of zero-dimensional polynomial sets has been proposed in [13], based on an exploration of the structures of lex Gröbner bases. For polynomial ideals of arbitrary dimension, the connection between Ritt characteristic sets and lex Gröbner bases has been investigated in [46]; (pseudo) divisibility relationships established therein will be clarified and used in later sections. The structures of lex Gröbner bases were studied first by Lazard [29] for bivariate ideals and then extended to general zero-dimensional (radical, multivariate) ideals in a number of papers [13, 22, 26, 34] with many deep results.

One kind of presumably good triangular set is the normal set explained above, which appeared for the first time as *normalized* triangular sets in [30] and later as *p-chains* in [20], and were elaborated in [43, Sect. 5.2] and [15]. Normal sets and systems enjoy a number of remarkable properties and are convenient for various applications, in particular dealing with parametric polynomial systems [8, 20, 43] (for which numerical methods based on homotopy continuation [24] and Newton iteration are inapplicable). There are algorithms for normalizing triangular sets, and more generally, for decomposing arbitrary polynomial sets or systems into normal sets or systems [33, 39, 43].

In this paper, we focus our study on what we call a *normal characteristic pair* and a *normal characteristic decomposition*: the former is a pair $(\mathcal{G}, \mathcal{C})$ of polynomial sets in which $\mathcal{G}$ is a reduced lex Gröbner basis, $\mathcal{C}$ is the minimal triangular set contained

in $\mathcal{G}$, and $\mathcal{C}$ is normal; the latter is the decomposition of a finite polynomial set $\mathcal{P}$ into finitely many normal characteristic pairs with associated zero relations, which provide representations for the zero set of $\mathcal{P}$ in terms of those of Gröbner bases and those of triangular sets. Our main contributions include: (1) clarification of the connection between normal sets and lex Gröbner bases via the concept of W-characteristic sets (introduced in [46]), (2) introduction of the concepts of (strong) normal characteristic pairs and normal characteristic decomposition with several properties proved, (3) an algorithm for computing (strong) normal characteristic decompositions of polynomial sets, and (4) experimental results illustrating the performance of our algorithm and its implementation.

The proposed algorithm, which makes use of the inherent connection between characteristic sets and Gröbner bases for splitting, is capable of decomposing any given polynomial set simultaneously into finitely many normal sets $\mathcal{C}_1, \ldots, \mathcal{C}_t$ and lex Gröbner bases $\mathcal{G}_1, \ldots, \mathcal{G}_t$ with every $\mathcal{C}_i$ contained in $\mathcal{G}_i$. It is proved that each $\mathcal{C}_i$ can be reduced to a Ritt characteristic set of the ideal generated by $\mathcal{G}_i$ if it is not reduced (Theorem 3.14 and Corollary 3.15). It is also shown that a strong normal characteristic decomposition can be computed out of any normal characteristic decomposition without need of further splitting (Theorems 3.19 and 3.22).

After a brief review of Gröbner bases, normal sets, and W-characteristic sets in Section 2, we will define (strong) normal characteristic pairs and (strong) normal characteristic decomposition and prove some of their properties in Section 3, describe the decomposition algorithm with proofs of termination and correctness in Section 4, and illustrate how the algorithm works with an example and report our experimental results in Section 5.

2. Gröbner bases, W-characteristic sets, and triangular sets

We recall some basic notions and notation which will be used in later sections and highlight the intrinsic structures of reduced lex Gröbner bases on which the main results of this paper are based. For more details about the theories of Gröbner bases (also called Buchberger–Gröbner bases) and triangular sets, the reader is referred to [3, 12, 43] and the references therein.

2.1. **Lexicographic Gröbner bases.** A Gröbner basis of a polynomial ideal is a special set of generators of the ideal which is well structured and has good properties. The structures and properties of Gröbner bases allow one to solve various computational problems with polynomial ideals, such as basic ideal operation, ideal membership test, and primary ideal decomposition. Introduced by Buchberger [6] in 1965 and having been developed for over half a century [7, 16–19, 23, 28, 38, 47], Gröbner bases have become a truly powerful method that has applications everywhere polynomial ideals are involved.

Let $\mathbb{K}$ be any field, and let $\mathbb{K}[x_1, \ldots, x_n]$ be the ring of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{K}$. In the sequel, we fix the variable order as $x_1 < \cdots < x_n$ unless otherwise specified. For the sake of simplicity, we write $\boldsymbol{x}$ for $(x_1, \ldots, x_n)$, $\boldsymbol{x}_i$ for $(x_1, \ldots, x_i)$, and $\mathbb{K}[\boldsymbol{x}]$ for $\mathbb{K}[x_1, \ldots, x_n]$.

A total ordering $<$ on all the terms in $\mathbb{K}[\boldsymbol{x}]$ is called a *term ordering* if it is a well ordering and for any terms $\boldsymbol{u}, \boldsymbol{v}$, and $\boldsymbol{w}$ in $\mathbb{K}[\boldsymbol{x}]$, $\boldsymbol{u} > \boldsymbol{v}$ implies $\boldsymbol{u}\boldsymbol{w} > \boldsymbol{v}\boldsymbol{w}$. In this paper we are mainly concerned with the lex term ordering, with respect to which Gröbner bases possess rich algebraic structures. For any two terms $\boldsymbol{u} = \boldsymbol{x}^{\boldsymbol{\alpha}}$

and $\boldsymbol{v} = \boldsymbol{x}^{\boldsymbol{\beta}}$ in $\mathbb{K}[\boldsymbol{x}]$, we say that $\boldsymbol{u} >_{\mathrm{lex}} \boldsymbol{v}$ if the left rightmost nonzero entry in the vector $\boldsymbol{\alpha} - \boldsymbol{\beta}$ is positive.

Fix a term ordering $<$. The greatest term in a polynomial $F \in \mathbb{K}[\boldsymbol{x}]$ with respect to $<$ is called the *leading term* of F and denoted by $\mathrm{lt}(F)$. As usual, $\langle \{F_1, \ldots, F_s, \ldots\} \rangle = \langle F_1, \ldots, F_s, \ldots \rangle$ denotes the ideal generated by the polynomials $F_1, \ldots, F_s, \ldots \in \mathbb{K}[\boldsymbol{x}]$.

Definition 2.1. Let $\mathfrak{I} \subseteq \mathbb{K}[\boldsymbol{x}]$ be an ideal, and let $<$ be a term ordering. A finite set $\{G_1, \ldots, G_s\}$ of polynomials in $\mathfrak{I}$ is called a *Gröbner basis* of $\mathfrak{I}$ with respect to $<$ if $\langle \mathrm{lt}(G_1), \ldots, \mathrm{lt}(G_s) \rangle = \langle \mathrm{lt}(\mathfrak{I}) \rangle$, where $\mathrm{lt}(\mathfrak{I})$ denotes the set of leading terms of all the polynomials in $\mathfrak{I}$.

Let $\mathcal{G} = \{G_1, \ldots, G_s\}$ be a Gröbner basis of an ideal $\mathfrak{I} \subseteq \mathbb{K}[\boldsymbol{x}]$ with respect to a fixed term ordering $<$. For any polynomial $F \in \mathbb{K}[\boldsymbol{x}]$, there is a unique polynomial $R \in \mathbb{K}[\boldsymbol{x}]$ corresponding to F such that $F - R \in \mathfrak{I}$ and no term of R is divisible by any of $\mathrm{lt}(G_1), \ldots, \mathrm{lt}(G_s)$. The polynomial R is called the *normal form* of F with respect to $\mathcal{G}$ (denoted by $\mathrm{nform}(F, \mathcal{G})$), and F is said to be *B-reduced* with respect to $\mathcal{G}$ if $F = R$. The Gröbner basis $\mathcal{G}$ itself is said to be *reduced* if the coefficient of each G_i in $\mathrm{lt}(G_i)$ is 1 and no term of G_i lies in $\langle \{\mathrm{lt}(G) \,|\, G \in \mathcal{G}, G \neq G_i\} \rangle$ for all $i = 1, \ldots, s$. The reduced Gröbner basis of $\mathfrak{I}$ with respect to a fixed term ordering is unique.

Example 2.2. Consider $\mathcal{P} = \{x_1 x_2, x_2 x_3 + x_1^2 x_2, x_3^2, x_1 x_4^2, (x_1^2 x_3 + 1) x_4 + x_3 x_2 x_1\} \subseteq \mathbb{K}[x_1, x_2, x_3, x_4]$. The polynomial set $\mathcal{G} = \{x_1 x_2, x_2 x_3, x_3^2, x_4\}$ is a Gröbner basis of the ideal $\langle \mathcal{P} \rangle$ with respect to the lex ordering on $x_1 < x_2 < x_3 < x_4$. One can easily check that $\mathcal{G}$ is also the reduced lex Gröbner basis of $\langle \mathcal{P} \rangle$.

Remark 2.3. The term *B-reduced* is an abbreviation of *Buchberger-reduced* for a polynomial modulo a Gröbner basis. We use the prefix B to distinguish this term from the term *R-reduced* (short for Ritt-reduced, defined below) for a polynomial modulo a triangular set.

2.2. **Normal triangular sets.** Now let F be a polynomial in $\mathbb{K}[\boldsymbol{x}] \setminus \mathbb{K}$. With respect to the variable order, the greatest variable which actually appears in F is called the *leading variable* of F and denoted by $\mathrm{lv}(F)$. Let $\mathrm{lv}(F) = x_i$; then F can be written as $F = I x_i^k + R$, with $I \in \mathbb{K}[\boldsymbol{x}_{i-1}]$, $R \in \mathbb{K}[\boldsymbol{x}_i]$, and $\deg(R, x_i) < k = \deg(F, x_i)$. The polynomial I is called the *initial* of F, denoted by $\mathrm{ini}(F)$. For any polynomial set $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$, $\mathrm{ini}(\mathcal{F})$ denotes $\{\mathrm{ini}(F) \,|\, F \in \mathcal{F}\}$.

Definition 2.4. Any finite, nonempty, ordered set $[T_1, \ldots, T_r]$ of polynomials in $\mathbb{K}[\boldsymbol{x}] \setminus \mathbb{K}$ is called a *triangular set* if $\mathrm{lv}(T_1) < \cdots < \mathrm{lv}(T_r)$ with respect to the variable order.

The *saturated ideal* of a triangular set $\mathcal{T} = [T_1, \ldots, T_r]$ is defined as $\mathrm{sat}(\mathcal{T}) = \langle \mathcal{T} \rangle : J^\infty$, where $J = \mathrm{ini}(T_1) \cdots \mathrm{ini}(T_r)$. We write $\mathrm{sat}_i(\mathcal{T}) = \mathrm{sat}([T_1, \ldots, T_i])$ for $i = 1, \ldots, r$. The variables in $\{x_1, \ldots, x_n\} \setminus \{\mathrm{lv}(T_1), \ldots, \mathrm{lv}(T_r)\}$ are called the *parameters* of $\mathcal{T}$. A triangular set $\mathcal{T}$ is said to be *zero-dimensional* if there is no parameter of $\mathcal{T}$, and *positive-dimensional* otherwise.

Definition 2.5. A triangular set $\mathcal{T} = [T_1, \ldots, T_r] \subseteq \mathbb{K}[\boldsymbol{x}]$ is said to be *normal* (or called a *normal set*) if all $\mathrm{ini}(T_1), \ldots, \mathrm{ini}(T_r)$ involve only the parameters of $\mathcal{T}$.

Example 2.6. From the Gröbner basis $\mathcal{G} = \{x_1 x_2, x_2 x_3, x_3^2, x_4\}$ in Example 2.2 one can extract two triangular sets, $\mathcal{T}_1 = [x_1 x_2, x_2 x_3, x_4]$ and $\mathcal{T}_2 = [x_1 x_2, x_3^2, x_4]$.

Both of them are positive-dimensional, with x_1 as their parameter. One can easily see that $\mathcal{T}_1$ is not normal, but $\mathcal{T}_2$ is.

Among the most commonly used triangular sets there are *regular sets* [42] or *regular chains* [3]. A triangular set $\mathcal{T} = [T_1, \ldots, T_r] \subseteq \mathbb{K}[\boldsymbol{x}]$ is called a regular set or said to be regular if for every $i = 2, \ldots, r$, $\mathrm{ini}(T_i)$ is neither zero nor a zero-divisor in $\mathbb{K}[\boldsymbol{x}]/\mathrm{sat}_{i-1}(\mathcal{T})$. By definition any normal set is obviously regular. It is proved in [3,43] that a triangular set $\mathcal{T}$ is regular if and only if $\mathrm{sat}(\mathcal{T}) = \{F \mid \mathrm{prem}(F, \mathcal{T}) = 0\}$.

A nonzero polynomial $P \in \mathbb{K}[\boldsymbol{x}]$ is said to be *R-reduced* with respect to $Q \in \mathbb{K}[\boldsymbol{x}] \backslash \mathbb{K}$ if $\deg(P, \mathrm{lv}(Q)) < \deg(Q, \mathrm{lv}(Q))$; P is *R-reduced* with respect to a triangular set $\mathcal{T} = [T_1, \ldots, T_r] \subseteq \mathbb{K}[\boldsymbol{x}]$ if P is R-reduced with respect to all T_i for $i = 1, \ldots, r$. The triangular set $\mathcal{T}$ itself is said to be *R-reduced* if T_i is R-reduced with respect to $[T_1, \ldots, T_{i-1}]$ for all $i = 2, \ldots, r$.

Denote by $\mathrm{prem}(P, Q)$ the *pseudoremainder* and by $\mathrm{pquo}(P, Q)$ the *pseudoquotient* of $P \in \mathbb{K}[\boldsymbol{x}]$ with respect to $Q \in \mathbb{K}[\boldsymbol{x}] \setminus \mathbb{K}$ in $\mathrm{lv}(Q)$, and for any triangular set $\mathcal{T} = [T_1, \ldots, T_r] \subseteq \mathbb{K}[\boldsymbol{x}]$ define

$$\mathrm{prem}(P, \mathcal{T}) = \mathrm{prem}(\cdots \mathrm{prem}(\mathrm{prem}(P, T_r), T_{r-1}), \ldots, T_1),$$

called the *pseudoremainder* of P with respect to $\mathcal{T}$. Clearly, $\mathrm{prem}(P, Q)$ and $\mathrm{prem}(P, \mathcal{T})$ are, respectively, R-reduced with respect to Q and $\mathcal{T}$. Similarly, we can define the *resultant* of P with respect to $\mathcal{T}$ as

$$\mathrm{res}(P, \mathcal{T}) = \mathrm{res}(\cdots \mathrm{res}(\mathrm{res}(P, T_r), T_{r-1}), \ldots, T_1),$$

where $\mathrm{res}(P, Q)$ denotes the *resultant* of $P \in \mathbb{K}[\boldsymbol{x}]$ and $Q \in \mathbb{K}[\boldsymbol{x}] \setminus \mathbb{K}$ with respect to $\mathrm{lv}(Q)$.

2.3. **W-characteristic sets.** Polynomial ideals discussed from now on are assumed nontrivial unless stated otherwise. From the reduced lex Gröbner basis $\mathcal{G}$ of any polynomial ideal $\langle \mathcal{P} \rangle \subseteq \mathbb{K}[\boldsymbol{x}]$, one can extract the W-characteristic set $\mathcal{C}$ of $\langle \mathcal{P} \rangle$ defined below.

Definition 2.7 ([46, Def. 3.1]). Let $\mathcal{G}$ be the reduced lex Gröbner basis of an ideal $\mathfrak{I} \subseteq \mathbb{K}[\boldsymbol{x}]$, and denote by $\mathcal{G}^{(i)} = \{G \in \mathcal{G} \mid \mathrm{lv}(G) = x_i\}$. Then the set

$$\bigcup_{i=1}^{n} \{G \in \mathcal{G}^{(i)} \mid \forall G' \in \mathcal{G}^{(i)} \setminus \{G\}, G <_{\mathrm{lex}} G'\},$$

ordered according to $<_{\mathrm{lex}}$, is called the *W-characteristic set* of $\mathfrak{I}$.

The ordered set in Definition 2.7 is also called the W-characteristic set of the reduced lex Gröbner basis $\mathcal{G}$ for the sake of simplicity. By definition any W-characteristic set is a triangular set.

Example 2.8. Clearly among the two triangular sets $\mathcal{T}_1$ and $\mathcal{T}_2$ extracted from the reduced lex Gröbner basis $\mathcal{G}$ in Example 2.6, $\mathcal{T}_1$ is the W-characteristic set of $\langle \mathcal{P} \rangle$, for $x_2 x_3 <_{\mathrm{lex}} x_3^2$.

Definition 2.9. Let $\mathcal{P}$ be any finite polynomial set in $\mathbb{K}[\boldsymbol{x}]$. An R-reduced triangular set $\mathcal{C} \subseteq \mathbb{K}[\boldsymbol{x}]$ is called a *Ritt characteristic set* of the ideal $\langle \mathcal{P} \rangle$ if $\mathcal{C} \subseteq \langle \mathcal{P} \rangle$ and for any $P \in \langle \mathcal{P} \rangle$, $\mathrm{prem}(P, \mathcal{C}) = 0$.

The W-characteristic set $\mathcal{C}$ of $\langle \mathcal{P} \rangle$ is a Ritt characteristic set of $\langle \mathcal{P} \rangle$ if $\mathcal{C}$ is R-reduced [46, Thm. 3.3]. Further relationships between Ritt characteristic sets

and lex Gröbner bases are established in [46] with the help of the concept of W-characteristic sets.

For any polynomial $P \in \mathbb{K}[\boldsymbol{x}]$ and polynomial set $\mathcal{P} \subseteq \mathbb{K}[\boldsymbol{x}]$, we denote by $\mathsf{Z}(P)$ the set of zeros of P in $\bar{\mathbb{K}}$, the algebraic closure of $\mathbb{K}$, and by $\mathsf{Z}(\mathcal{P})$ the set of common zeros of all the polynomials in $\mathcal{P}$ in $\bar{\mathbb{K}}^n$. For any nonempty polynomial sets $\mathcal{P}$ and $\mathcal{Q}$ in $\mathbb{K}[\boldsymbol{x}]$, we define $\mathsf{Z}(\mathcal{P}/\mathcal{Q}) = \mathsf{Z}(\mathcal{P}) \setminus \mathsf{Z}(\Pi_{Q \in \mathcal{Q}} Q)$.

Proposition 2.10 ([46, Prop. 3.1]). *Let $\mathcal{C}$ be the W-characteristic set of $\langle \mathcal{P} \rangle \subseteq \mathbb{K}[\boldsymbol{x}]$. Then:*

(a) *for any $P \in \langle \mathcal{P} \rangle$, $\mathrm{prem}(P, \mathcal{C}) = 0$;*
(b) *$\langle \mathcal{C} \rangle \subseteq \langle \mathcal{P} \rangle \subseteq \mathrm{sat}(\mathcal{C})$;*
(c) *$\mathsf{Z}(\mathcal{C}/\mathrm{ini}(\mathcal{C})) \subseteq \mathsf{Z}(\mathcal{P}) \subseteq \mathsf{Z}(\mathcal{C})$.*

The following theorem [46, Thm. 3.9] exploits the pseudodivisibility relationships between polynomials in W-characteristic sets (and thus between those in reduced lex Gröbner bases) for polynomial ideals of arbitrary dimension, while other well-known structural properties of lex Gröbner bases were established only for bivariate or zero-dimensional polynomial ideals. It is these relationships that enable us to adopt an effective splitting strategy for our algorithm of normal characteristic decomposition.

Theorem 2.11 ([46, Thm. 3.9]). *Let $\mathcal{C} = [C_1, \ldots, C_r]$ be the W-characteristic set of $\langle \mathcal{P} \rangle \subseteq \mathbb{K}[\boldsymbol{x}]$. If $\mathcal{C}$ is not normal, then there exists an integer k $(1 \leq k < r)$ such that $[C_1, \ldots, C_k]$ is normal and $[C_1, \ldots, C_{k+1}]$ is not regular.*

Assume that the variables $x_1, \ldots, x_n$ are ordered such that the parameters of $\mathcal{C}$ are all smaller than the other variables, and let $I_{k+1} = \mathrm{ini}(C_{k+1})$ and l be the integer such that $\mathrm{lv}(I_{k+1}) = \mathrm{lv}(C_l)$.

(a) *If I_{k+1} is not R-reduced with respect to C_l, then*
$$\mathrm{prem}(I_{k+1}, [C_1, \ldots, C_l]) = 0,$$
$$\mathrm{prem}(C_{k+1}, [C_1, \ldots, C_k]) = 0.$$

(b) *If I_{k+1} is R-reduced with respect to C_l, then*
$$\mathrm{prem}(C_l, [C_1, \ldots, C_{l-1}, I_{k+1}]) = 0$$
and either $\mathrm{res}(\mathrm{ini}(I_{k+1}), [C_1, \ldots, C_{l-1}]) = 0$ or
$$\mathrm{prem}(C_{k+1}, [C_1, \ldots, C_{l-1}, I_{k+1}, C_{l+1}, \ldots, C_k]) = 0.$$

Example 2.12. The W-characteristic set $\mathcal{T}_1 = [x_1 x_2, x_2 x_3, x_4]$ of $\langle \mathcal{P} \rangle$ in Example 2.8 is not normal, and one can find that $[x_1 x_2]$ is normal, but $[x_1 x_2, x_2 x_3]$ is not (furthermore, it is not regular). The initial x_2 of $x_2 x_3$ is not R-reduced with respect to $x_1 x_2$, and one can check that $\mathrm{prem}(x_2, [x_1 x_2]) = 0$ and $\mathrm{prem}(x_2 x_3, [x_1 x_2]) = 0$, which agree with Theorem 2.11(a).

An obvious consequence of the first part of the above theorem is that the W-characteristic set contained in the reduced lex Gröbner basis of a polynomial ideal, if it is regular, must be normal. This implies that a certain normalization mechanism is integrated into the algorithm of Gröbner bases, so that triangular subsets of lex Gröbner bases are normalized as much as possible.

The condition on the order of $x_1, \ldots, x_n$ for $\mathcal{C}$ in Theorem 2.11 is needed, for otherwise the theorem does not necessarily hold, as shown by [46, Ex. 3.1(b)]. In the latter case, one may change the variable order properly to make the condition satisfied, so as to obtain the pseudodivisibility relations in Theorem 2.11. For

polynomial ideals of dimension 0, their W-characteristic sets do not involve any parameters and thus the condition is naturally satisfied. For the rest of the paper, we assume that the condition is also satisfied for the positive-dimensional case where the structures of lex Gröbner bases are rather complicated.

3. Decomposition into normal characteristic pairs

In this section we discuss the decomposition of an arbitrary polynomial set into (strong) normal characteristic pairs with associated zero relations and prove some properties about the decomposition. A decomposition algorithm will be presented in Section 4.

3.1. Normal and strong normal characteristic pairs.

Definition 3.1. A pair $(\mathcal{G}, \mathcal{C})$ with $\mathcal{G}, \mathcal{C} \subseteq \mathbb{K}[\boldsymbol{x}]$ is called a *characteristic pair* in $\mathbb{K}[\boldsymbol{x}]$ if $\mathcal{G}$ is a reduced lex Gröbner basis and $\mathcal{C}$ is the W-characteristic set of $\langle \mathcal{G} \rangle$. A characteristic pair $(\mathcal{G}, \mathcal{C})$ is said to be *normal* or *regular* if $\mathcal{C}$ is normal or regular, respectively.

This paper focuses on the study of normal and strong normal characteristic pairs and the decomposition of arbitrary polynomial sets into such characteristic pairs. Other kinds of characteristic pairs and the corresponding decompositions will be investigated in forthcoming papers. The following known results (Propositions 3.2–3.4) concerning normal sets are recalled, with references or self-contained proofs, exhibiting some of the nice properties of normal characteristic pairs.

Proposition 3.2. *For any zero-dimensional normal set $\mathcal{N} \subseteq \mathbb{K}[\boldsymbol{x}]$: (a) $\mathrm{sat}(\mathcal{N}) = \langle \mathcal{N} \rangle$; (b) $\mathcal{N}$ is the lex Gröbner basis of $\langle \mathcal{N} \rangle$.*

Proof. As $\mathcal{N}$ is a zero-dimensional normal set, each $\mathrm{ini}(N)$ is a constant in $\mathbb{K}$ for $N \in \mathcal{N}$. Then statement (a) follows directly from the definition of $\mathrm{sat}(\mathcal{N})$, and statement (b) can be derived easily by using [12, Section 2.9, Thm. 3 and Prop. 4]. $\square$

Proposition 3.3 ([35, Prop. 2.2]). *Let $\mathcal{N} \subseteq \mathbb{K}[\boldsymbol{x}]$ be any positive-dimensional normal set with parameters $\tilde{\boldsymbol{x}} \subseteq \boldsymbol{x}$. Then $\mathcal{N}$ is the lex Gröbner basis of $\langle \mathcal{N} \rangle$ over $\mathbb{K}(\tilde{\boldsymbol{x}})$.*

Let $\mathcal{T} = [T_1, \ldots, T_r] \subseteq \mathbb{K}[\boldsymbol{x}]$ be an arbitrary triangular set with parameters $x_1, \ldots, x_d$ ($d + r = n$). For each $i = 0, \ldots, r - 1$, write

$$\mathcal{T}_{\leq i} = \mathcal{T} \cap \mathbb{K}[x_1, \ldots, x_{d+i}] = [T_1, \ldots, T_i], \quad \mathcal{I}_{\leq i} = \mathrm{ini}(\mathcal{T}) \cap \mathbb{K}[x_1, \ldots, x_{d+i}].$$

$\mathcal{T}$ is said to have the *projection property* if for any $i = 0, \ldots, r - 1$ and any $\bar{\boldsymbol{x}}_i \in \mathsf{Z}(\mathcal{T}_{\leq i}/\mathcal{I}_{\leq i})$, there exist $\bar{x}_{i+1}, \ldots, \bar{x}_r \in \bar{\mathbb{K}}$ such that $(\bar{\boldsymbol{x}}_i, \bar{x}_{i+1}, \ldots, \bar{x}_r) \in \mathsf{Z}(\mathcal{T}/\mathrm{ini}(\mathcal{T}))$. Here empty $\mathcal{T}_{\leq i}$ and $\mathcal{I}_{\leq i}$ are understood as $\{0\}$ and $\{1\}$, respectively.

Proposition 3.4. *Any normal set $\mathcal{N} \subset \mathbb{K}[\boldsymbol{x}]$ has the projection property.*

Proof. Let $\mathcal{N} = [N_1, \ldots, N_r]$, and let $I_i = \mathrm{ini}(N_i)$ for $i = 1, \ldots, r$. Since $\mathcal{N}$ is a normal set, $\mathcal{I}_{\leq i} = \{I_1, \ldots, I_r\}$ for $i = 0, \ldots, r$. Thus for any $i = 0, \ldots, r-1$ and any $\bar{\boldsymbol{x}}_i \in \mathsf{Z}(\mathcal{N}_{\leq i}/\mathcal{I}_{\leq i})$, $I_j(\bar{\boldsymbol{x}}_i) \neq 0$ for all $j = i+1, \ldots, r$, so there exist $\bar{x}_{i+1}, \ldots, \bar{x}_r \in \bar{\mathbb{K}}$ such that $(\bar{\boldsymbol{x}}_i, \bar{x}_{i+1}, \ldots, \bar{x}_r) \in \mathsf{Z}(\mathcal{N}/\mathrm{ini}(\mathcal{N}))$. $\square$

Remark 3.5. In general regular sets do not have the projection property. Consider, for example, $\mathcal{T} = [x^2 - u, xy + 1] \subseteq \mathbb{Q}[u, x, y]$, where $\mathbb{Q}$ is the field of rational numbers and $u < x < y$. Then u is the parameter of $\mathcal{T}$. Now $\mathcal{T}_{\leq 0} = \mathcal{I}_{\leq 0} = \emptyset$ and the parametric value $\bar{u} = 0 \in \bar{\mathbb{Q}} = \mathsf{Z}(\mathcal{T}_{\leq 0}/\mathcal{I}_{\leq 0})$, but $\mathsf{Z}(\mathcal{T}/\operatorname{ini}(\mathcal{T})) = \emptyset$ when $u = \bar{u}$.

Proposition 3.6. *Let $\mathcal{C}$ be the W-characteristic set of a polynomial ideal $\langle \mathcal{P} \rangle \subseteq \mathbb{K}[\boldsymbol{x}]$. If $\operatorname{sat}(\mathcal{C}) = \langle \mathcal{C} \rangle$, then $\operatorname{sat}(\mathcal{C}) = \langle \mathcal{P} \rangle$.*

Proof. The proposition follows immediately from $\langle \mathcal{C} \rangle \subseteq \langle \mathcal{P} \rangle \subseteq \operatorname{sat}(\mathcal{C})$ (Proposition 2.10(b)). $\qquad \square$

The reverse direction of Proposition 3.6, namely $\operatorname{sat}(\mathcal{C}) = \langle \mathcal{P} \rangle$ implies $\operatorname{sat}(\mathcal{C}) = \langle \mathcal{C} \rangle$, is not correct in general. For example, $\mathcal{G} = \{y^2, xz + y, yz, z^2\} \subseteq \mathbb{K}[x, y, z]$ is a reduced lex Gröbner basis with $x < y < z$: the W-characteristic set of $\langle \mathcal{G} \rangle$ is $\mathcal{C} = [y^2, xz + y]$, and one can check that $\langle \mathcal{G} \rangle = \operatorname{sat}(\mathcal{C})$, but $\langle \mathcal{C} \rangle \neq \operatorname{sat}(\mathcal{C})$.

What is of special interest between $\mathcal{G}$ and $\mathcal{C}$ in a characteristic pair $(\mathcal{G}, \mathcal{C})$ is whether the equality $\langle \mathcal{G} \rangle = \operatorname{sat}(\mathcal{C})$ holds. This equality does hold when $\operatorname{sat}(\mathcal{C}) = \langle \mathcal{C} \rangle$ (according to Proposition 3.6), but the condition $\operatorname{sat}(\mathcal{C}) = \langle \mathcal{C} \rangle$ does not necessarily hold as the above example shows. Moreover, it is computationally difficult to verify whether $\operatorname{sat}(\mathcal{T}) = \langle \mathcal{T} \rangle$ holds for a triangular set $\mathcal{T}$ [1, 32].

Definition 3.7. A normal characteristic pair $(\mathcal{G}, \mathcal{C})$ is said to be *strong normal* if $\operatorname{sat}(\mathcal{C}) = \langle \mathcal{G} \rangle$.

Definition 3.8. A reduced lex Gröbner basis $\mathcal{G}$ is said to be *characterizable* if $\langle \mathcal{G} \rangle = \operatorname{sat}(\mathcal{C})$, where $\mathcal{C}$ is the W-characteristic set of $\mathcal{G}$.

Note that the variety defined by any characterizable Gröbner basis is unmixed and equidimensional (i.e., its irreducible components are all of the same dimension with the same parameters [21]). It is easy to see that every W-characteristic set is determined by a reduced lex Gröbner basis, while a characterizable Gröbner basis is also determined by its W-characteristic set. A strong normal characteristic pair thus furnishes a characterizable Gröbner basis with a normal W-characteristic set. In what follows we show that the W-characteristic set of any characterizable Gröbner basis is normal, so that the characterizable Gröbner basis and its W-characteristic set form a strong normal characteristic pair.

Proposition 3.9. *The W-characteristic set of any characterizable Gröbner basis is normal.*

Proof. We prove the proposition by contradiction. Suppose that the W-characteristic $\mathcal{C} = [C_1, \ldots, C_r]$ of the characterizable Gröbner basis $\mathcal{G}$ is abnormal. Then by Theorem 2.11 there exist two polynomials C_{k+1} and C_l $(l \leq k)$ in $\mathcal{C}$ with $\operatorname{lv}(C_l) = \operatorname{lv}(I_{k+1})$ such that either (a) $\operatorname{prem}(\operatorname{ini}(C_{k+1}), [C_1, \ldots, C_l]) = 0$, when $\operatorname{ini}(C_{k+1})$ is not R-reduced with respect to C_l; or (b) $\operatorname{prem}(C_l, [C_1, \ldots, C_{l-1}, \operatorname{ini}(C_{k+1})]) = 0$, when $\operatorname{ini}(C_{k+1})$ is R-reduced.

Let $I_i = \operatorname{ini}(C_i)$ for $i = 1, \ldots, l$ and $I_{k+1} = \operatorname{ini}(C_{k+1})$.

For case (a), from the pseudoremainder formula we know that $I_{k+1} \in \operatorname{sat}(\mathcal{C})$. Write $C_{k+1} = I_{k+1} \operatorname{lv}(C_{k+1})^d + R$, where $\deg(R, \operatorname{lv}(C_{k+1})) < d$. If $R = 0$, then $\operatorname{lv}(C_{k+1})^d \in \operatorname{sat}(\mathcal{C})$, but $\operatorname{lv}(C_{k+1})^d <_{\text{lex}} C_{k+1}$, which contradicts with the minimality of $\mathcal{G}$ as the reduced lex Gröbner basis of $\operatorname{sat}(\mathcal{C})$; if $R \neq 0$, clearly $R \in \operatorname{sat}(\mathcal{C})$, but $R \notin \langle \mathcal{G} \rangle$ for R is B-reduced with respect to $\mathcal{G}$, which contradicts the equality $\langle \mathcal{G} \rangle = \operatorname{sat}(\mathcal{C})$.

For case (b), it follows from the pseudoremainder formula that there exist $i_1, \ldots, i_l \in \mathbb{Z}_{\geq 0}$ (the set of nonnegative integers) and $Q_1, \ldots, Q_l \in \mathbb{K}[\boldsymbol{x}]$ such that

$$I_1^{i_1} \cdots I_{l-1}^{i_{l-1}} \operatorname{ini}(I_{k+1})^{i_l} C_l = Q_1 C_1 + \cdots + Q_{I-1} C_{I-1} + Q_l I_{k+1};$$

clearly $Q_l \in \operatorname{sat}(\mathcal{C})$. Since $\deg(I_{k+1}, \operatorname{lv}(C_l)) < \deg(C_l, \operatorname{lv}(C_l))$ in this case and all $I_1, \ldots, I_{l-1}$ involve only the parameters, we have $\operatorname{lv}(Q_l) = \operatorname{lv}(C_l)$ but $\deg(Q_l, \operatorname{lv}(C_l)) < \deg(C_l, \operatorname{lv}(C_l))$, and thus $Q_l <_{\operatorname{lex}} C_l$. This contradicts with the minimality of $\mathcal{G}$. $\qquad \square$

Remark 3.10. Gröbner bases are good representations of polynomial ideals. Here it is shown that the W-characteristic set $\mathcal{C}$ of a characterizable Gröbner basis $\mathcal{G}$ provides another representation of the same ideal $\langle \mathcal{G} \rangle$. The representation $\mathcal{C}$ is simpler than $\mathcal{G}$ because $\mathcal{C}$ is a subset of $\mathcal{G}$, whereas $\mathcal{G}$ can be computed from $\mathcal{C}$ if needed. In other words, characterizable Gröbner bases are those special Gröbner bases whose W-characteristic sets can characterize or represent the ideals they generate.

3.2. **Normal characteristic decomposition and its properties.** Let $\mathcal{F}$ be a finite, nonempty set of polynomials in $\mathbb{K}[\boldsymbol{x}]$. We call a finite set $\{(\mathcal{G}_1, \mathcal{C}_1), \ldots, (\mathcal{G}_t, \mathcal{C}_t)\}$ of characteristic pairs in $\mathbb{K}[\boldsymbol{x}]$ a *characteristic decomposition* of $\mathcal{F}$ if the following zero relations hold:

$$(3.1) \qquad \mathsf{Z}(\mathcal{F}) = \bigcup_{i=1}^{t} \mathsf{Z}(\mathcal{G}_i) = \bigcup_{i=1}^{t} \mathsf{Z}(\mathcal{C}_i / \operatorname{ini}(\mathcal{C}_i)) = \bigcup_{i=1}^{t} \mathsf{Z}(\operatorname{sat}(\mathcal{C}_i)).$$

A characteristic decomposition is said to be *normal* or *regular* if every characteristic pair in the decomposition is normal or regular, respectively.

Theorem 3.11. *From any finite, nonempty polynomial set $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$, one can compute in a finite number of steps a normal characteristic decomposition of $\mathcal{F}$.*

The above theorem will be proved by giving a concrete algorithm (Algorithm 1 in Section 4.1) with correctness and termination proof (in Section 4.2). In what follows, we focus our attention on the properties of normal characteristic decomposition.

Remark 3.12. From any normal characteristic decomposition of a polynomial set $\mathcal{F}$, one can extract a normal decomposition $\{\mathcal{C}_1, \ldots, \mathcal{C}_t\}$ of $\mathcal{F}$, with each $\mathcal{C}_i$ a normal set for $i = 1, \ldots, t$ and $\mathsf{Z}(\mathcal{F}) = \bigcup_{i=1}^{t} \mathsf{Z}(\mathcal{C}_i / \operatorname{ini}(\mathcal{C}_i))$. The projection property of normal sets (see Proposition 3.4) allows us to write the conditions on the parameters for a normal set to have zeros for the variables, which makes normal decomposition an appropriate approach for parametric polynomial system solving [8, 20, 30]. The obtained parametric conditions are not necessarily disjoint and thus do not necessarily lead to a partition of the parameter space. However, since the conditions derived from normal sets are expressed by means of initials which involve only the parameters, it is easier to compute comprehensive triangular decomposition [8] via normal decomposition than via regular decomposition.

A proper ideal in $\mathbb{K}[\boldsymbol{x}]$ is said to be *purely equidimensional* if its associated prime ideals are all of the same height. According to [2, Prop. 4.1.3], $\operatorname{sat}(\mathcal{T})$ is purely equidimensional for any regular set $\mathcal{T} \subseteq \mathbb{K}[\boldsymbol{x}]$. Thus it follows from Proposition 3.6

that for any normal characteristic pair $(\mathcal{G}, \mathcal{C})$ in the normal characteristic decomposition of $\mathcal{F}$, $\langle \mathcal{G} \rangle$ is purely equidimensional if $\mathrm{sat}(\mathcal{C}) = \langle \mathcal{C} \rangle$ is verified. More precisely, we have the following.

Proposition 3.13. *Let Ψ be a normal characteristic decomposition of $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$ and assume that $\mathrm{sat}(\mathcal{C}) = \langle \mathcal{C} \rangle$ for every normal characteristic pair $(\mathcal{G}, \mathcal{C}) \in \Psi$. Then $\sqrt{\langle \mathcal{F} \rangle} = \bigcap_{(\mathcal{G}, \mathcal{C}) \in \Psi} \sqrt{\langle \mathcal{G} \rangle}$ and each $\langle \mathcal{G} \rangle$ is purely equidimensional.*

In fact, the ideal $\langle \mathcal{G} \rangle$ in Proposition 3.13 is also *unmixed* and *strongly* equidimensional according to [21] and [2, Thm. 4.1.4]. The following theorem shows how a Ritt characteristic set of a polynomial ideal can be constructed from the W-characteristic set (when it is normal) of the ideal.

Theorem 3.14. *Let $\mathcal{C} = [C_1, \ldots, C_r]$ be the W-characteristic set of $\langle \mathcal{P} \rangle \subseteq \mathbb{K}[\boldsymbol{x}]$, and let*

$$(3.2) \qquad \mathcal{C}^* = [C_1, \mathrm{prem}(C_2, [C_1]), \ldots, \mathrm{prem}(C_r, [C_1, \ldots, C_{r-1}])].$$

If $\mathcal{C}$ is normal, then the following statements hold:

(a) *$\mathcal{C}^*$ is a normal set;*
(b) *$\mathcal{C}^*$ is a Ritt characteristic set of $\langle \mathcal{P} \rangle$;*
(c) *$\mathsf{Z}(\mathcal{C}^* / \mathrm{ini}(\mathcal{C}^*)) = \mathsf{Z}(\mathcal{C} / \mathrm{ini}(\mathcal{C}))$.*

Proof. Let $\mathcal{C}^* = [C_1^*, \ldots, C_r^*]$, let $I_i = \mathrm{ini}(C_i)$, and let $I_i^* = \mathrm{ini}(C_i^*)$ for $i = 1, \ldots, r$.

(a)–(b) According to [46, Thm. 3.4], $\mathcal{C}^*$ is a regular set and $\mathcal{C}^*$ is a Ritt characteristic set of $\langle \mathcal{P} \rangle$; hence it suffices to prove that $\mathcal{C}^*$ is normal. Since $C_i^* = \mathrm{prem}(C_i, [C_1, \ldots, C_{i-1}])$ for any $i = 2, \ldots, r$, there exist $q_1, \ldots, q_{i-1} \in \mathbb{Z}_{\geq 0}$ and $Q_1, \ldots, Q_{i-1} \in \mathbb{K}[\boldsymbol{x}]$ such that

$$(3.3) \qquad I_1^{q_1} \cdots I_{i-1}^{q_{i-1}} C_i = Q_1 C_1 + \cdots + Q_{i-1} C_{i-1} + C_i^*.$$

Since $\mathrm{ini}(C_i)$ does not involve any of $\mathrm{lv}(C_1), \ldots, \mathrm{lv}(C_{i-1})$, we have $\mathrm{ini}(C_i^*) = I_1^{q_1} \cdots I_{i-1}^{q_{i-1}} I_i$ for $i = 1, \ldots, r$; thus $\mathcal{C}^*$ is normal.

(c) On one hand, for any $\bar{\boldsymbol{x}} \in \mathsf{Z}(\mathcal{C} / \mathrm{ini}(\mathcal{C}))$, $C_i(\bar{\boldsymbol{x}}) = 0$ and $I_i(\bar{\boldsymbol{x}}) \neq 0$ for $i = 1, \ldots, r$. From (3.3) we know that $C_i^*(\bar{\boldsymbol{x}}) = 0$ and $I_i^*(\bar{\boldsymbol{x}}) \neq 0$ for $i = 1, \ldots, r$; or equivalently $\bar{\boldsymbol{x}} \in \mathsf{Z}(\mathcal{C}^* / \mathrm{ini}(\mathcal{C}^*))$. On the other hand, for any $\hat{\boldsymbol{x}} \in \mathsf{Z}(\mathcal{C}^* / \mathrm{ini}(\mathcal{C}^*))$, $C_i^*(\hat{\boldsymbol{x}}) = 0$ and $I_i^*(\hat{\boldsymbol{x}}) \neq 0$ for $i = 1, \ldots, r$. Clearly $C_1 = C_1^*$, $C_1(\hat{\boldsymbol{x}}) = 0$, and $I_1(\hat{\boldsymbol{x}}) \neq 0$. Suppose now that $C_i(\hat{\boldsymbol{x}}) = 0$ and $I_i(\hat{\boldsymbol{x}}) \neq 0$ hold for $i = 2, \ldots, k-1$. Then by (3.3) and $I_k^* = I_1^{q_1} \cdots I_{k-1}^{q_{k-1}} I_k$ we have $C_k(\hat{\boldsymbol{x}}) = 0$ and $I_k(\hat{\boldsymbol{x}}) \neq 0$. By induction, $\hat{\boldsymbol{x}} \in \mathsf{Z}(\mathcal{C} / \mathrm{ini}(\mathcal{C}))$. $\square$

Corollary 3.15. *Let Ψ be a normal characteristic decomposition of $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$, and let $\mathcal{C}^*$ be computed from $\mathcal{C}$ according to (3.2) for each normal characteristic pair $(\mathcal{G}, \mathcal{C}) \in \Psi$. Then*

$$\mathsf{Z}(\mathcal{F}) = \bigcup_{(\mathcal{G}, \mathcal{C}) \in \Psi} \mathsf{Z}(\mathcal{C}^* / \mathrm{ini}(\mathcal{C}^*)) = \bigcup_{(\mathcal{G}, \mathcal{C}) \in \Psi} \mathsf{Z}(\mathrm{sat}(\mathcal{C}^*)),$$

and $\mathcal{C}^*$ is a Ritt characteristic set of $\langle \mathcal{G} \rangle$ for each $(\mathcal{G}, \mathcal{C}) \in \Psi$.

Corollary 3.16. *Let $\mathcal{C} = [C_1, \ldots, C_r]$ be the W-characteristic set of $\langle \mathcal{P} \rangle \subseteq \mathbb{K}[\boldsymbol{x}]$ such that $\mathcal{C}$ is normal, let $\mathcal{C}^*$ be as defined in (3.2), and let $\tilde{\boldsymbol{x}} \subseteq \boldsymbol{x}$ be the parameters of $\mathcal{C}$. Then both $\mathcal{C}$ and $\mathcal{C}^*$ are lex Gröbner bases of $\langle \mathcal{P} \rangle$ over $\mathbb{K}(\tilde{\boldsymbol{x}})$. Furthermore, let $\mathcal{C}^* = [C_1^*, \ldots, C_r^*]$. Then $\{C_1^* \mathrm{ini}(C_1^*)^{-1}, \ldots, C_r^* \mathrm{ini}(C_r^*)^{-1}\}$ is the reduced lex Gröbner basis of $\langle \mathcal{P} \rangle$ over $\mathbb{K}(\tilde{\boldsymbol{x}})$.*

Proof. By Proposition 3.3, $\mathcal{C}$ is the lex Gröbner basis of $\langle \mathcal{C} \rangle$ over $\mathbb{K}(\tilde{\boldsymbol{x}})$. As $\mathrm{sat}(\mathcal{C}) = \langle \mathcal{C} \rangle$ over $\mathbb{K}(\tilde{\boldsymbol{x}})$, from Proposition 3.6 we know that $\mathcal{C}$ is the lex Gröbner basis of $\langle \mathcal{P} \rangle$ over $\mathbb{K}(\tilde{\boldsymbol{x}})$. Moreover, since each $\mathrm{ini}(C_i^*)$ is a constant in $\mathbb{K}(\tilde{\boldsymbol{x}})$ for $i = 1, \ldots, r$ and $\deg(C_j^*, \mathrm{lv}(C_i^*)) < \deg(C_i^*, \mathrm{lv}(C_i^*))$ $(1 \leq i, j \leq r,\ j \neq i)$, $\{C_1^* \mathrm{ini}(C_1^*)^{-1}, \ldots, C_r^* \mathrm{ini}(C_r^*)^{-1}\}$ is the reduced lex Gröbner basis of $\langle \mathcal{P} \rangle$ over $\mathbb{K}(\tilde{\boldsymbol{x}})$. □

Note that the R-reduced normal set $\mathcal{C}^*$ computed in (3.2) is not necessarily a subset of $\mathcal{G}$ (while the W-characteristic set $\mathcal{C}$ is). Corollary 3.16 does not hold when the W-characteristic set $\mathcal{C}$ is abnormal. In fact, the problem of constructing a Ritt characteristic set of an ideal $\mathfrak{I}$ from the reduced lex Gröbner basis of $\mathfrak{I}$ was already studied by Aubry, Moreno Maza, and Lazard in their influential paper [3] of 1999. It is the first author of this paper who pointed out with an example in [46] that the relevant results including Theorem 3.1, Proposition 3.4, and Theorem 3.2 in Section 3 of [3] are flawed. He showed that the construction is simple and straightforward in the normal case and made the problem of effective construction open again for the abnormal case. The incorrectness of the construction process in [3] is caused essentially by the noncloseness of addition on polynomials having pseudoremainder 0 with respect to an irregular triangular set $\mathcal{T}$, that is, $\mathrm{prem}(P, \mathcal{T}) = \mathrm{prem}(Q, \mathcal{T}) = 0$ does not necessarily imply $\mathrm{prem}(P + Q, \mathcal{T}) = 0$ for arbitrary polynomials P and Q. The noncloseness seems to be a major obstacle for constructing abnormal Ritt characteristic sets of polynomial ideals.

3.3. Strong normal characteristic decomposition.
Now we show that for any normal characteristic decomposition $\Psi = \{(\mathcal{G}_1, \mathcal{C}_1), \ldots, (\mathcal{G}_t, \mathcal{C}_t)\}$ of $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$, one can explicitly transform Ψ into a strong normal characteristic decomposition $\bar{\Psi} = \{(\bar{\mathcal{G}}_1, \bar{\mathcal{C}}_1), \ldots, (\bar{\mathcal{G}}_t, \bar{\mathcal{C}}_t)\}$, where each $(\bar{\mathcal{G}}_i, \bar{\mathcal{C}}_i)$ is a strong normal characteristic pair for $i = 1, \ldots, t$.

Lemma 3.17 ([46, Lem. 2.4]). *Let $\mathcal{T} = [T_1, \ldots, T_r] \subseteq \mathbb{K}[\boldsymbol{x}]$ be a regular set with $\mathrm{lv}(T_r) < x_n$, and let $P = P_d x_m^d + \cdots + P_1 x_m + P_0 \in \mathbb{K}[\boldsymbol{x}]$ be a polynomial with $\mathrm{lv}(P) = x_m > \mathrm{lv}(T_r)$ and $\deg(P, x_m) = d$. Then $\mathrm{prem}(P, \mathcal{T}) = 0$ if and only if $\mathrm{prem}(P_i, \mathcal{T}) = 0$ for all $i = 0, 1, \ldots, d$.*

Lemma 3.18 ([43, Lem. 6.2.6]). *Let $\mathcal{T}$ be a regular set in $\mathbb{K}[\boldsymbol{x}]$. Then for any $F \in \mathbb{K}[\boldsymbol{x}]$, if $\mathrm{res}(F, \mathcal{T}) \neq 0$, then $\mathrm{sat}(\mathcal{T}) : F^\infty = \mathrm{sat}(\mathcal{T})$.*

Theorem 3.19. *Let $(\mathcal{G}, \mathcal{C})$ be a normal characteristic pair, let $\bar{\mathcal{G}}$ be the reduced lex Gröbner basis of $\mathrm{sat}(\mathcal{C})$, and let $\bar{\mathcal{C}}$ be the W-characteristic set of $\langle \bar{\mathcal{G}} \rangle$. Then the following statements hold:*

    (a) *the parameters of $\bar{\mathcal{C}}$ coincide with those of $\mathcal{C}$;*

    (b) *$\bar{\mathcal{C}}$ is a normal set, $\mathrm{sat}(\bar{\mathcal{C}}) = \mathrm{sat}(\mathcal{C})$, and thus $(\bar{\mathcal{G}}, \bar{\mathcal{C}})$ is a strong normal characteristic pair.*

Proof. (a) Let $\mathrm{lv}(\mathcal{G}) = \{\mathrm{lv}(G) \mid G \in \mathcal{G}\}$, and let $\mathrm{lv}(\bar{\mathcal{G}}) = \{\mathrm{lv}(\bar{G}) \mid \bar{G} \in \bar{\mathcal{G}}\}$. It suffices to prove that $\mathrm{lv}(\mathcal{G}) = \mathrm{lv}(\bar{\mathcal{G}})$.

$(\mathrm{lv}(\mathcal{G}) \supseteq \mathrm{lv}(\bar{\mathcal{G}}))$ Suppose that $x_k \in \mathrm{lv}(\bar{\mathcal{G}})$, but $x_k \notin \mathrm{lv}(\mathcal{G})$. Then there exists a $\bar{G} \in \bar{\mathcal{G}}$ with $\mathrm{lv}(\bar{G}) = x_k$. Since $\bar{G} \in \langle \bar{\mathcal{G}} \rangle = \mathrm{sat}(\mathcal{C})$, $\mathrm{prem}(\bar{G}, \mathcal{C}) = 0$. Write $\bar{G} = \bar{H}_p x_k^p + \cdots + \bar{H}_0$, where $p = \deg(\bar{G})$ and $\bar{H}_i \in \mathbb{K}[x_1, \ldots, x_{k-1}]$ for $i = 0, \ldots, p$. Since $x_k \notin \mathrm{lv}(\mathcal{G})$ and $\mathrm{prem}(\bar{G}, \mathcal{C}) = 0$, from Lemma 3.17 we know that for $i = 0, \ldots, p$, $\mathrm{prem}(\bar{H}_i, \mathcal{C}) = 0$, and thus $\bar{H}_i \in \mathrm{sat}(\mathcal{C}) = \langle \bar{\mathcal{G}} \rangle$. This implies that $\mathrm{nform}(\bar{H}_i, \bar{\mathcal{G}} \setminus \{\bar{G}\}) = 0$ for $i = 0, \ldots, p$, and thus $\mathrm{nform}(\bar{G}, \bar{\mathcal{G}} \setminus \{\bar{G}\}) = 0$, which contradicts with $\bar{\mathcal{G}}$ being the reduced lex Gröbner basis.

$(\mathrm{lv}(\mathcal{G}) \subseteq \mathrm{lv}(\bar{\mathcal{G}}))$ Suppose that $x_l \in \mathrm{lv}(\mathcal{G})$, but $x_l \notin \mathrm{lv}(\bar{\mathcal{G}})$. Then there exists a $C \in \mathcal{C} \subseteq \mathcal{G}$ with $\mathrm{lv}(C) = x_l$, and thus $C \in \mathrm{sat}(\mathcal{C}) = \langle \bar{\mathcal{G}} \rangle$; it follows that $\mathrm{nform}(C, \bar{\mathcal{G}}) = 0$. Write $C = \mathrm{ini}(C) x_l^d + R$, where $d = \deg(C, x_l)$ and $R \in \mathbb{K}[x_1, \ldots, x_l]$. Then from $\mathrm{nform}(C, \bar{\mathcal{G}}) = 0$ and $x_l \notin \mathrm{lv}(\bar{\mathcal{G}})$, we know that $\mathrm{nform}(\mathrm{ini}(C), \bar{\mathcal{G}}) = 0$, and thus $\mathrm{ini}(C) \in \langle \bar{\mathcal{G}} \rangle = \mathrm{sat}(\mathcal{C})$. It follows that $\mathrm{prem}(\mathrm{ini}(C), \mathcal{C}) = 0$; this contradicts with the fact that $C \in \mathcal{C}$ and $\mathcal{C}$ is a normal set.

(b) Let $\mathcal{C} = [C_1, \ldots, C_r]$. By (a) we can assume that $\bar{\mathcal{C}} = [\bar{C}_1, \ldots, \bar{C}_r]$ with $\mathrm{lv}(\bar{C}_i) = \mathrm{lv}(C_i)$ for $i = 1, \ldots, r$. Since $\bar{C}_i \in \langle \bar{\mathcal{G}} \rangle = \mathrm{sat}(\mathcal{C})$ and $\mathcal{C}$ is regular, $\mathrm{prem}(\bar{C}_i, \mathcal{C}) = 0$. We claim that $\deg(C_i, \mathrm{lv}(C_i)) \le \deg(\bar{C}_i, \mathrm{lv}(\bar{C}_i))$. Otherwise, if $\deg(C_i, \mathrm{lv}(C_i)) > \deg(\bar{C}_i, \mathrm{lv}(\bar{C}_i))$, then $\mathrm{prem}(\bar{C}_i, \mathcal{C}) = \mathrm{prem}(\bar{C}_i, [C_1, \ldots, C_{i-1}]) = 0$. Write $\bar{C}_i = \sum_{j=0}^d \bar{C}_{i,j} \mathrm{lv}(\bar{C}_i)^j$, where $d = \deg(\bar{C}_i, \mathrm{lv}(\bar{C}_i))$ and $\mathrm{lv}(\bar{C}_{i,j}) < \mathrm{lv}(\bar{C}_i)$. Then by Lemma 3.17 we have $\mathrm{prem}(\bar{C}_{i,j}, [C_1, \ldots, C_{i-1}]) = 0$ for $j = 0, \ldots, d$, and thus $\bar{C}_{i,j} \in \mathrm{sat}(\mathcal{C}) = \langle \bar{\mathcal{G}} \rangle$. Since $\mathrm{lv}(\bar{C}_{i,j}) < \mathrm{lv}(\bar{C}_i)$, we know that $\mathrm{nform}(\bar{C}_{i,j}, \bar{\mathcal{G}} \setminus \{\bar{C}_i\}) = 0$ for $j = 0, \ldots, d$, and thus $\mathrm{nform}(\bar{C}_i, \bar{\mathcal{G}} \setminus \{\bar{C}_i\}) = 0$; this contradicts with the fact that $\bar{\mathcal{G}}$ is a reduced Gröbner basis.

Now we prove that $\bar{\mathcal{C}}$ is a normal set, namely, no element of $\mathrm{ini}(\bar{\mathcal{C}})$ involves the variables in $\mathrm{lv}(\bar{\mathcal{C}})$. If, otherwise, some $\mathrm{ini}(\bar{C}_i)$ involves variables in $\mathrm{lv}(\bar{\mathcal{C}})$, then, under the assumption that all the parameters of $\bar{\mathcal{C}}$ are ordered smaller than the variables in $\mathrm{lv}(\bar{\mathcal{C}})$, we have $\mathrm{lt}(C_i) <_{\mathrm{lex}} \mathrm{lt}(\bar{C}_i)$ and thus $C_i <_{\mathrm{lex}} \bar{C}_i$, for $\deg(C_i, \mathrm{lv}(C_i)) \le \deg(\bar{C}_i, \mathrm{lv}(\bar{C}_i))$. From $C_i \in \mathrm{sat}(\mathcal{C}) = \langle \bar{\mathcal{G}} \rangle$, we know that there exists a polynomial $\bar{G} \in \bar{\mathcal{G}}$ such that $\mathrm{lt}(\bar{G}) \mid \mathrm{lt}(C_i)$. (1) If $\mathrm{lt}(\bar{G})$ does not involve $\mathrm{lv}(C_i)$, then the fact that $\mathrm{ini}(C_i)$ does not involve any variable in $\mathrm{lv}(\mathcal{C})$ implies that $\mathrm{lt}(\bar{G})$ involves no variable in $\mathrm{lv}(\mathcal{C})$, which contradicts with the fact that $\mathrm{lt}(\bar{G})$ has to involve $\mathrm{lv}(\bar{G}) \in \mathrm{lv}(\bar{\mathcal{G}}) = \mathrm{lv}(\mathcal{C})$. (2) Otherwise, $\mathrm{lt}(\bar{G})$ involves $\mathrm{lv}(C_i) = \mathrm{lv}(\bar{C}_i)$. Then in view of $\bar{G} <_{\mathrm{lex}} C_i <_{\mathrm{lex}} \bar{C}_i$ and by the definition of $\bar{C}_i$ as a polynomial in the W-characteristic set, we see that $\bar{C}_i = G$ and thus $\mathrm{lt}(\bar{C}_i) \mid \mathrm{lt}(C_i)$, which is impossible because $\mathrm{ini}(\bar{C}_i)$ contains some variable in $\mathrm{lv}(\bar{\mathcal{C}})$ but $\mathrm{ini}(C_i)$ does not. This proves that $\bar{\mathcal{C}}$ is a normal set.

Next we show the equality $\mathrm{sat}(\bar{\mathcal{C}}) = \mathrm{sat}(\mathcal{C})$. Since $\langle \bar{\mathcal{G}} \rangle = \mathrm{sat}(\mathcal{C})$, it suffices to show that $\langle \bar{\mathcal{G}} \rangle = \mathrm{sat}(\bar{\mathcal{C}})$. On one hand, from Proposition 2.10(b) we know that $\langle \bar{\mathcal{G}} \rangle \subseteq \mathrm{sat}(\bar{\mathcal{C}})$. On the other hand, let $\bar{I} = \prod_{\bar{C} \in \bar{\mathcal{C}}} \mathrm{ini}(\bar{C})$. Since $\bar{I}$ only involves the parameters of $\mathcal{C}$, $\mathrm{res}(\bar{I}, \mathcal{C}) = \bar{I} \neq 0$. By Lemma 3.18 we have $\mathrm{sat}(\mathcal{C}) : \bar{I}^\infty = \langle \bar{\mathcal{G}} \rangle$. With the inclusion $\bar{\mathcal{C}} \subseteq \bar{\mathcal{G}}$, the relation

$$\mathrm{sat}(\bar{\mathcal{C}}) = \langle \bar{\mathcal{C}} \rangle : \bar{I}^\infty \subseteq \langle \bar{\mathcal{G}} \rangle : \bar{I}^\infty = \mathrm{sat}(\mathcal{C}) : \bar{I}^\infty = \langle \bar{\mathcal{G}} \rangle$$

holds. $\qquad \square$

Example 3.20. The pair

$$(\mathcal{G}, \mathcal{C}) = (\{y^2, x^2 z + xy, yz + xz + y\}, [y^2, x^2 z + xy])$$

is a normal characteristic pair in $\mathbb{Q}[x, y, z]$ with $x < y < z$. The reduced lex Gröbner basis $\bar{\mathcal{G}}$ of $\mathrm{sat}(\mathcal{C})$ is $\{y^2, xz + y, yz, z^2\}$, so the W-characteristic set $\bar{\mathcal{C}}$ of $\bar{\mathcal{G}}$ is $[y^2, xz + y]$. One can check that the parameter of both $\mathcal{C}$ and $\bar{\mathcal{C}}$ is x, $\bar{\mathcal{C}}$ is normal, and $\mathrm{sat}(\mathcal{C}) = \mathrm{sat}(\bar{\mathcal{C}})$.

Lemma 3.21. *Let both $\mathcal{C} = [C_1, \ldots, C_r]$ and $\bar{\mathcal{C}} = [\bar{C}_1, \ldots, \bar{C}_r]$ be as in Theorem 3.19. Then $\mathrm{ini}(\bar{C}_i) \mid \mathrm{ini}(C_i)$ for $i = 1, \ldots, r$.*

Proof. From the proof of Theorem 3.19 we know that $\operatorname{prem}(\bar{C}_i, \mathcal{C}) = 0$, $\operatorname{prem}(C_i, \bar{\mathcal{C}}) = 0$, and $\deg(\bar{C}_i, \operatorname{lv}(\bar{C}_i)) = \deg(C_i, \operatorname{lv}(C_i))$ for $i = 1, \ldots, r$. Then

$$\operatorname{ini}(C_i)\bar{C}_i = \operatorname{ini}(\bar{C}_i)C_i \mod \operatorname{sat}(\mathcal{C}_{\leq i-1}),$$

where $\mathcal{C}_{\leq i-1} = [C_1, \ldots, C_{i-1}]$. Therefore, $\operatorname{ini}(\bar{C}_i) \mid \operatorname{ini}(C_i)\bar{C}_i$ modulo $\operatorname{sat}(\mathcal{C}_{\leq i-1})$.

If $\operatorname{ini}(\bar{C}_i) \mid \operatorname{ini}(C_i)$ modulo $\operatorname{sat}(\mathcal{C}_{\leq i-1})$, then clearly $\operatorname{ini}(\bar{C}_i) \mid \operatorname{ini}(C_i)$, for both $\operatorname{ini}(\bar{C}_i)$ and $\operatorname{ini}(C_i)$ involve only the parameters. Otherwise, there exists an $\bar{I} \notin \mathbb{K}$ such that $\bar{I} \mid \operatorname{ini}(\bar{C}_i)$ and $\bar{I} \mid \bar{C}_i$ modulo $\operatorname{sat}(\mathcal{C}_{\leq i-1})$. Then by $(\bar{C}_i/\bar{I})\bar{I} = \bar{C}_i \in \langle \bar{\mathcal{C}} \rangle$, we have $\bar{C}_i/\bar{I} \in \operatorname{sat}(\bar{\mathcal{C}}) = \langle \bar{\mathcal{G}} \rangle$, but $\bar{C}_i/\bar{I} <_{\text{lex}} \bar{C}_i$, which contradicts with the minimality of $\bar{C}_i$ as a polynomial in the W-characteristic set. $\square$

Theorem 3.22. *Let $\Psi = \{(\mathcal{G}_1, \mathcal{C}_1), \ldots, (\mathcal{G}_t, \mathcal{C}_t)\}$ be a normal characteristic decomposition of $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$. For each $(\mathcal{G}_i, \mathcal{C}_i) \in \Psi$, let $(\bar{\mathcal{G}}_i, \bar{\mathcal{C}}_i)$ be the corresponding strong normal characteristic pair as constructed in Theorem 3.19, with $i = 1, \ldots, t$. Then*

$$\mathsf{Z}(\mathcal{F}) = \bigcup_{i=1}^{t} \mathsf{Z}(\bar{\mathcal{G}}_i) = \bigcup_{i=1}^{t} \mathsf{Z}(\bar{\mathcal{C}}_i / \operatorname{ini}(\bar{\mathcal{C}}_i)) = \bigcup_{i=1}^{t} \mathsf{Z}(\operatorname{sat}(\bar{\mathcal{C}}_i)).$$

Proof. Note that the zero relation (3.1) holds for the normal characteristic decomposition Ψ, which may be computed according to Theorem 3.11. The first and the third equalities above can be proved by using the equalities $\operatorname{sat}(\mathcal{C}_i) = \operatorname{sat}(\bar{\mathcal{C}}_i)$ in Theorem 3.19(b) and $\langle \bar{\mathcal{G}}_i \rangle = \operatorname{sat}(\mathcal{C}_i)$:

$$\mathsf{Z}(\mathcal{F}) = \bigcup_{i=1}^{t} \mathsf{Z}(\operatorname{sat}(\mathcal{C}_i)) = \bigcup_{i=1}^{t} \mathsf{Z}(\operatorname{sat}(\bar{\mathcal{C}}_i)) = \bigcup_{i=1}^{t} \mathsf{Z}(\bar{\mathcal{G}}_i).$$

Now we prove that $\mathsf{Z}(\mathcal{F}) = \bigcup_{i=1}^{t} \mathsf{Z}(\bar{\mathcal{C}}_i / \operatorname{ini}(\bar{\mathcal{C}}_i))$. Since $\mathsf{Z}(\bar{\mathcal{C}}_i / \operatorname{ini}(\bar{\mathcal{C}}_i)) \subseteq \mathsf{Z}(\operatorname{sat}(\bar{\mathcal{C}}_i))$, we have

$$\bigcup_{i=1}^{t} \mathsf{Z}(\bar{\mathcal{C}}_i / \operatorname{ini}(\bar{\mathcal{C}}_i)) \subseteq \bigcup_{i=1}^{t} \mathsf{Z}(\operatorname{sat}(\bar{\mathcal{C}}_i)) = \mathsf{Z}(\mathcal{F}).$$

To show the other inclusion, observe first that

$$(3.4) \qquad \mathsf{Z}(\mathcal{C}_i / \operatorname{ini}(\mathcal{C}_i)) \subseteq \mathsf{Z}(\operatorname{sat}(\mathcal{C}_i)) = \mathsf{Z}(\bar{\mathcal{G}}_i) \subseteq \mathsf{Z}(\bar{\mathcal{C}}_i)$$

for $i = 1, \ldots, t$. Write $\mathcal{C}_i = [C_{i1}, \ldots, C_{ir_i}]$ and $\bar{\mathcal{C}}_i = [\bar{C}_{i1}, \ldots, \bar{C}_{ir_i}]$. Then for any $\bar{\boldsymbol{x}} \in \mathsf{Z}(\mathcal{C}_i / \operatorname{ini}(\mathcal{C}_i))$, $\prod_{j=1}^{r_i} \operatorname{ini}(C_{ij})(\bar{\boldsymbol{x}}) \neq 0$. By Lemma 3.21 we have $\operatorname{ini}(\bar{C}_{ij}) \mid \operatorname{ini}(C_{ij})$ for $j = 1, \ldots, r_i$, and thus $\prod_{j=1}^{r_i} \operatorname{ini}(\bar{C}_{ij})(\bar{\boldsymbol{x}}) \neq 0$. Combining this inequality with (3.4), we have $\mathsf{Z}(\mathcal{C}_i / \operatorname{ini}(\mathcal{C}_i)) \subseteq \mathsf{Z}(\bar{\mathcal{C}}_i / \operatorname{ini}(\bar{\mathcal{C}}_i))$, and thus $\mathsf{Z}(\mathcal{F}) = \bigcup_{i=1}^{t} \mathsf{Z}(\mathcal{C}_i / \operatorname{ini}(\mathcal{C}_i)) \subseteq \bigcup_{i=1}^{t} \mathsf{Z}(\bar{\mathcal{C}}_i / \operatorname{ini}(\bar{\mathcal{C}}_i))$. This completes the proof. $\square$

Remark 3.23. As shown by Theorems 3.19 and 3.22, any normal characteristic decomposition Ψ of a polynomial set can be transformed into a strong normal characteristic decomposition of the polynomial set by computing the reduced lex Gröbner basis of the saturated ideal of the W-characteristic set in each normal characteristic pair in Ψ. No splitting occurs in this transformation; the number of strong normal characteristic pairs produced by the transformation is the same as that of the normal characteristic pairs in Ψ.

4. ALGORITHM FOR NORMAL CHARACTERISTIC DECOMPOSITION

In this section we present an algorithm that computes a normal characteristic decomposition of any finite, nonempty set of nonzero polynomials.

4.1. **Algorithm description.** An overall strategy based on Theorem 2.11 for normal characteristic decomposition is sketched in [46, Sect. 4]. Following this strategy, we detail the decomposition method below.

Let Φ be a set of polynomial sets, initialized as $\{\mathcal{F}\}$ with $\mathcal{F} \subseteq \mathbb{K}[\boldsymbol{x}]$ being the input set, and let Ψ be a set of normal characteristic pairs already computed. Now we pick a polynomial set $\mathcal{P} \in \Phi$ and remove it from Φ, compute the reduced lex Gröbner basis $\mathcal{G}$ of the ideal $\langle \mathcal{P} \rangle$, and extract the W-characteristic set $\mathcal{C} = [C_1, \ldots, C_r]$ of $\langle \mathcal{P} \rangle$ from $\mathcal{G}$. Let $I_i = \mathrm{ini}(C_i)$ for $i = 1, \ldots, r$.

(1) If $\mathcal{C}$ is normal, then from Proposition 2.10(c) we know that

(4.1) $$\mathsf{Z}(\mathcal{C}/\mathrm{ini}(\mathcal{C})) \subseteq \mathsf{Z}(\mathcal{P}) \subseteq \mathsf{Z}(\mathcal{C}).$$

In view of this zero relation, we put the normal characteristic pair $(\mathcal{G}, \mathcal{C})$ into Ψ and adjoin the polynomial sets $\mathcal{G} \cup \{I_1\}, \ldots, \mathcal{G} \cup \{I_r\}$ to Φ for further processing.

(2) If $\mathcal{C}$ is not normal, then by Theorem 2.11 we have certain pseudodivisibility relations between polynomials in $\mathcal{C}$ and can use them to split $\mathcal{G}$ as follows, where the integers k and l are as in Theorem 2.11.

(2.1) If I_{k+1} is not R-reduced with respect to C_l, then the polynomial sets $\mathcal{G} \cup \{I_1\}, \ldots, \mathcal{G} \cup \{I_l\}, \mathcal{G} \cup \{I_{k+1}\}$ are adjoined to Φ.

(2.2) If I_{k+1} is R-reduced with respect to C_l, then let $Q = \mathrm{pquo}(C_l, I_{k+1})$ be the pseudoquotient of C_l with respect to I_{k+1}, and let $\mathcal{C}_{l-1} = [C_1, \ldots, C_{l-1}]$.

(2.2.1) If $\mathrm{prem}(\mathrm{ini}(Q), \mathcal{C}_{l-1}) = 0$, then the polynomial sets $\mathcal{G} \cup \{I_1\}, \ldots, \mathcal{G} \cup \{I_{l-1}\}, \mathcal{G} \cup \{\mathrm{ini}(I_{k+1})\}$ are adjoined to Φ.

(2.2.2) If $\mathrm{prem}(\mathrm{ini}(Q), \mathcal{C}_{l-1}) \neq 0$, then the polynomial sets $\mathcal{G} \cup \{I_1\}, \ldots, \mathcal{G} \cup \{I_{l-1}\}, \mathcal{G} \cup \{\mathrm{prem}(Q, \mathcal{C}_{l-1})\}, \mathcal{G} \cup \{I_{k+1}\}$ are adjoined to Φ.

After the splitting of $\mathcal{G}$, we continue picking another polynomial set $\mathcal{P}'$ (and meanwhile remove it) from Φ, compute the reduced lex Gröbner basis $\mathcal{G}'$ of $\langle \mathcal{P}' \rangle$, extract the W-characteristic set of $\langle \mathcal{P}' \rangle$ from $\mathcal{G}'$, and split $\mathcal{G}'$ when necessary. This process is repeated until Φ becomes empty.

The method for normal characteristic decomposition, whose main steps are outlined above, is described formally as Algorithm 1.

Algorithm 1 $\Psi = \mathsf{CharDec}(\mathcal{F})$. Given a finite, nonempty set $\mathcal{F}$ of nonzero polynomials in $\mathbb{K}[\boldsymbol{x}]$, this algorithm computes a normal characteristic decomposition Ψ of $\mathcal{F}$, or the empty set meaning that $\mathsf{Z}(\mathcal{F}) = \emptyset$.

C1. Set $\Psi = \emptyset$ and $\Phi = \{\mathcal{F}\}$.

C2. Repeat the following steps until $\Phi = \emptyset$:

C2.1. Pick $\mathcal{P} \in \Phi$ and remove it from Φ.

C2.2. Compute the reduced lex Gröbner basis $\mathcal{G}$ of $\langle \mathcal{P} \rangle$.

C2.3. If $\mathcal{G} = \{1\}$, then go to C2; otherwise:

C2.3.1. Extract the W-characteristic set $\mathcal{C}$ from $\mathcal{G}$.

C2.3.2. If $\mathcal{C}$ is normal (case 1), then reset Ψ with $\Psi \cup \{(\mathcal{G}, \mathcal{C})\}$, and Φ with

(4.2) $$\Phi \cup \{\mathcal{G} \cup \{\mathrm{ini}(C)\} \mid \mathrm{ini}(C) \notin \mathbb{K}, C \in \mathcal{C}\},$$

and go to C2.

C2.3.3. Pick the smallest polynomial C in $\mathcal{C}$ such that $[T \in \mathcal{C} \mid \mathrm{lv}(T) \leq \mathrm{lv}(C)]$ as a triangular set is abnormal.

C2.3.4. Let $I = \text{ini}(C)$ and $y = \text{lv}(I)$.

C2.3.5. Pick the polynomial C^* in $\mathcal{C}$ such that $\text{lv}(C^*) = y$.

C2.3.6. If I is not R-reduced with respect to C^* (case (2.1)), then reset Φ with

$$(4.3) \qquad \Phi \cup \{\mathcal{G} \cup \{\text{ini}(T)\} \mid \text{lv}(T) \leq y, T \in \mathcal{C}\} \cup \{\mathcal{G} \cup \{I\}\},$$

and go to C2.

C2.3.7. If $\text{prem}(\text{ini}(Q), [T \in \mathcal{C} \mid \text{lv}(T) < y]) = 0$ (case (2.2.1)), then reset Φ with

$$(4.4) \qquad \Phi \cup \{\mathcal{G} \cup \{\text{ini}(T)\} \mid \text{lv}(T) < y, T \in \mathcal{C}\} \cup \{\mathcal{G} \cup \{\text{ini}(I)\}\},$$

and go to C2.

C2.3.8. Reset Φ with

$$(4.5) \qquad \begin{aligned} &\Phi \cup \{\mathcal{G} \cup \{\text{ini}(T)\} \mid \text{lv}(T) < y, T \in \mathcal{C}\} \cup \\ &\{\mathcal{G} \cup \{\text{prem}(Q, [T \in \mathcal{C} \mid \text{lv}(T) < y])\}, \mathcal{G} \cup \{I\}\} \end{aligned}$$

(case (2.2.2)) and go to C2.

C3. Output Ψ.

4.2. Correctness and termination.

Theorem 4.1. *Algorithm* 1 *terminates in a finite number of steps with correct output.*

Proof. (*Termination*) The process of splitting in Algorithm 1 can be viewed as building up a tree from its root as the input set $\mathcal{F}$. Every time a polynomial set $\mathcal{P}$ is picked from Φ, splitting occurs according to one of the four cases, treated in steps C2.3.2, C2.3.6, C2.3.7, and C2.3.8 of Algorithm 1, as long as the reduced lex Gröbner basis of $\langle \mathcal{P} \rangle$ is not $\{1\}$ (for otherwise $\mathcal{P}$ has no zero). Suppose that the split polynomial sets $\mathcal{G}_1, \ldots, \mathcal{G}_s$ are adjoined to Φ. In the sense of building up the tree, this means that the child nodes of $\mathcal{P}$ are $\mathcal{G}_1, \ldots, \mathcal{G}_s$.

To prove the termination of Algorithm 1, we need to show that each path in the tree is of finite length. Thus by the Ascending Chain Condition (see, e.g., [12, Chap. 2, Thm. 7]), it suffices to show that for all the four cases of splitting, each polynomial set $\mathcal{G}' = \mathcal{G} \cup \{H\}$ adjoined to Φ for some H generates an ideal $\langle \mathcal{G}' \rangle$ that is strictly greater than $\langle \mathcal{G} \rangle$, or equivalently $H \notin \langle \mathcal{G} \rangle$.

Let the W-characteristic set $\mathcal{C}$ in step C2.3.1 be written as $[C_1, \ldots, C_r]$ with $I_i = \text{ini}(C_i)$, and let $\mathcal{C}_i = [C_1, \ldots, C_i]$ for $1 \leq i \leq r$. Then C, I, and C^* in steps C2.3.3–C2.3.5 correspond to C_{k+1}, I_{k+1}, and C_l, respectively, for some integers $l \leq k$ as stated in Theorem 2.11.

Let $H \notin \mathbb{K}$ be the initial of some $C \in \mathcal{C}$ as in (4.2) in step C2.3.2. We claim that H is B-reduced with respect to $\mathcal{G}$; for otherwise C will be reducible by some polynomial in $\mathcal{G} \setminus \{C\}$, which conflicts with the fact that $\mathcal{G}$ is the reduced lex Gröbner basis of $\langle \mathcal{P} \rangle$. Therefore, $H \notin \langle \mathcal{G} \rangle$ for all $C \in \mathcal{C}$ in (4.2). With similar arguments, one can show that $H \notin \langle \mathcal{G} \rangle$ as well if $H \notin \mathbb{K}$ is the initial of some polynomial $T \in \mathcal{C}$ as in (4.3), (4.4), and (4.5).

To complete the proof of termination, it remains to show that $H = \text{prem}(Q, \mathcal{C}_{l-1}) \notin \langle \mathcal{G} \rangle$, where $Q = \text{pquo}(C_l, I_{k+1})$. In step C2.3.8, the conditions $\text{lv}(Q) > \text{lv}(C_{l-1})$ and $\text{prem}(\text{ini}(Q), \mathcal{C}_{l-1}) \neq 0$ hold. By Theorem 2.11, $\mathcal{C}_{l-1}$ is normal and thus regular; then by Lemma 3.17, $\text{prem}(Q, \mathcal{C}_{l-1}) \neq 0$ and

$$(4.6) \qquad \deg(\text{prem}(Q, \mathcal{C}_{l-1}), \text{lv}(C_i)) < \deg(C_i, \text{lv}(C_i))$$

for $i = 1, \ldots, l - 1$. Furthermore, as $Q = \operatorname{pquo}(C_l, I_{k+1})$ and $\operatorname{lv}(C_l)$ also appear in I_{k+1} (by Theorem 2.11), we have $\deg(Q, \operatorname{lv}(C_l)) < \deg(C_l, \operatorname{lv}(C_l))$, and thus

$$(4.7) \qquad \deg(\operatorname{prem}(Q, \mathcal{C}_{l-1}), \operatorname{lv}(C_l)) < \deg(C_l, \operatorname{lv}(C_l)).$$

Since $\mathcal{C}$ is the W-characteristic set of $\mathcal{G}$, the relations (4.6) and (4.7) imply that $\operatorname{prem}(Q, \mathcal{C}_{l-1})$ is B-reduced with respect to $\mathcal{G}$, and thus $\operatorname{prem}(Q, \mathcal{C}_{l-1}) \notin \langle \mathcal{G} \rangle$.

(*Correctness*) When $\mathsf{Z}(\mathcal{F}) = \emptyset$, $\mathcal{G} = \{1\}$ in step C2.3 and $\Psi = \emptyset$ is returned. Therefore, to prove the correctness of Algorithm 1, we need to show that when $\mathsf{Z}(\mathcal{F}) \neq \emptyset$, Ψ is a normal characteristic decomposition of $\mathcal{F}$, namely all the pairs $(\mathcal{G}, \mathcal{C}) \in \Psi$ are normal characteristic pairs and the zero relation (3.1) holds.

It is clear that each $(\mathcal{G}, \mathcal{C}) \in \Psi$ is a normal characteristic pair, for only in step C2.3.2 is the output set Ψ adjoined with a new pair $(\mathcal{G}, \mathcal{C})$, where $\mathcal{G}$ is a reduced lex Gröbner basis and $\mathcal{C}$ is its normal W-characteristic set. We first prove that $\mathsf{Z}(\mathcal{F}) = \bigcup_{(\mathcal{G}, \mathcal{C}) \in \Psi} \mathsf{Z}(\mathcal{C}/\operatorname{ini}(\mathcal{C}))$ by considering all the four cases of splitting. For this purpose, let $\mathcal{C} = [C_1, \ldots, C_r]$ be the W-characteristic set, let $I_i = \operatorname{ini}(C_i)$ $(1 \leq i \leq r)$, and let $L = \operatorname{ini}(I_{k+1})$.

Case 1 (step C2.3.2). The W-characteristic set $\mathcal{C}$ is normal. In this case, let $J = I_1 \cdots I_r$. Then $\mathsf{Z}(\mathcal{P}) = (\mathsf{Z}(\mathcal{P}) \setminus \mathsf{Z}(J)) \cup \mathsf{Z}(\mathcal{P} \cup \{J\})$. It follows from the zero relation (4.1) that $\mathsf{Z}(\mathcal{P}) \setminus \mathsf{Z}(J) = \mathsf{Z}(\mathcal{C}/\operatorname{ini}(\mathcal{C}))$. Moreover, as $J = 0$ implies that $I_1 = 0$, or $I_2 = 0, \ldots$, or $I_r = 0$,

$$\mathsf{Z}(\mathcal{P} \cup \{J\}) = \bigcup_{i=1}^{r} \mathsf{Z}(\mathcal{P} \cup \{I_i\}) = \bigcup_{i=1}^{r} \mathsf{Z}(\mathcal{G} \cup \{I_i\}).$$

Therefore,

$$(4.8) \qquad \mathsf{Z}(\mathcal{P}) = \mathsf{Z}(\mathcal{C}/\operatorname{ini}(\mathcal{C})) \cup \bigcup_{i=1}^{r} \mathsf{Z}(\mathcal{G} \cup \{I_i\}).$$

Case 2.1 (step C2.3.6). $\mathcal{C}$ is abnormal and $\deg(I_{k+1}, \operatorname{lv}(I_{k+1})) \geq \deg(C_l, \operatorname{lv}(I_{k+1}))$. By Theorem 2.11(a) we have $\operatorname{prem}(I_{k+1}, \mathcal{C}_l) = 0$, and thus there exist $Q_1, \ldots, Q_l \in \mathbb{K}[\boldsymbol{x}]$ and $q_1, \ldots, q_l \in \mathbb{Z}_{\geq 0}$ such that $I_1^{q_1} \cdots I_l^{q_l} I_{k+1} = Q_1 C_1 + \cdots + Q_l C_l$. This means that $I_1^{q_1} \cdots I_l^{q_l} I_{k+1} \in \langle C_1, \ldots, C_l \rangle \subseteq \langle \mathcal{P} \rangle = \langle \mathcal{G} \rangle$, so

$$(4.9) \quad \mathsf{Z}(\mathcal{P}) = \mathsf{Z}(\mathcal{G}) = \mathsf{Z}(\mathcal{G} \cup \{I_1^{q_1} \cdots I_l^{q_l} I_{k+1}\}) = \bigcup_{i=1}^{l} \mathsf{Z}(\mathcal{G} \cup \{I_i\}) \cup \mathsf{Z}(\mathcal{G} \cup \{I_{k+1}\}).$$

Case 2.2.1 (step C2.3.7). $\mathcal{C}$ is abnormal, $\deg(I_{k+1}, \operatorname{lv}(I_{k+1})) < \deg(C_l, \operatorname{lv}(I_{k+1}))$, and $\operatorname{prem}(\operatorname{ini}(Q), \mathcal{C}_{l-1}) = 0$. By the formula $L^q C_l = Q I_{k+1} + R$ of the pseudo-division of C_l with respect to I_{k+1}, where $q \in \mathbb{Z}_{\geq 0}$ and $Q, R \in \mathbb{K}[\boldsymbol{x}]$, we have $\operatorname{ini}(Q) = L^{q-1} I_l$. Since

$$\operatorname{prem}(\operatorname{ini}(Q), \mathcal{C}_{l-1}) = \operatorname{prem}(L^{q-1} I_l, \mathcal{C}_{l-1}) = I_l \operatorname{prem}(L^{q-1}, \mathcal{C}_{l-1}) = 0,$$

$\operatorname{prem}(L^{q-1}, \mathcal{C}_{l-1}) = 0$, and thus

$$(4.10) \qquad \mathsf{Z}(\mathcal{P}) = \bigcup_{i=1}^{l-1} \mathsf{Z}(\mathcal{G} \cup \{I_i\}) \cup \mathsf{Z}(\mathcal{G} \cup \{L\})$$

follows from arguments similar to those in case (2.1).

Case 2.2.2 (step C2.3.8). $\mathcal{C}$ is abnormal, $\deg(I_{k+1}, \mathrm{lv}(I_{k+1})) < \deg(C_l, \mathrm{lv}(I_{k+1}))$, and $\mathrm{prem}(\mathrm{ini}(Q), \mathcal{C}_{l-1}) \neq 0$. By Theorem 2.11(b), we have

$$\mathrm{prem}(C_l, [C_1, \ldots, C_{l-1}, I_{k+1}]) = \mathrm{prem}(\mathrm{prem}(C_l, I_{k+1}), \mathcal{C}_{l-1})$$
$$= \mathrm{prem}(L^q C_l - Q I_{k+1}, \mathcal{C}_{l-1}) = 0,$$

where Q and q are as in case 2.2.1. Then there exist $q_1, \ldots, q_{l-1} \in \mathbb{Z}_{\geq 0}$ and $Q_1, \ldots, Q_{l-1}$
$\in \mathbb{K}[\boldsymbol{x}]$ such that $I_1^{q_1} \cdots I_{l-1}^{q_{l-1}}(L^q C_l - Q I_{k+1}) = \sum_{i=1}^{l-1} Q_i C_i$. It follows that

$$(4.11) \qquad\qquad -I_1^{q_1} \cdots I_{l-1}^{q_{l-1}} I_{k+1} Q = \sum_{i=1}^{l} Q_i C_i$$

for $Q_l = -I_1^{q_1} \cdots I_{l-1}^{q_{l-1}} L^q$. Let the formula of the pseudodivision of Q with respect to $\mathcal{C}_{l-1}$ be

$$(4.12) \qquad\qquad I_1^{\bar{q}_1} \cdots I_{l-1}^{\bar{q}_{l-1}} Q = \sum_{i=1}^{l-1} \bar{Q}_i C_i + \mathrm{prem}(Q, \mathcal{C}_{l-1})$$

for some $\bar{q}_1, \ldots, \bar{q}_{l-1} \in \mathbb{Z}_{\geq 0}$ and $\bar{Q}_1, \ldots, \bar{Q}_{l-1} \in \mathbb{K}[\boldsymbol{x}]$. Then one can find $\hat{q}_1, \ldots, \hat{q}_{l-1}$
$\in \mathbb{Z}_{\geq 0}$ and $\hat{Q}_1, \ldots, \hat{Q}_l \in \mathbb{K}[\boldsymbol{x}]$ such that

$$I_1^{\hat{q}_1} \cdots I_{l-1}^{\hat{q}_{l-1}} I_{k+1} \mathrm{prem}(Q, \mathcal{C}_{l-1}) = \sum_{i=1}^{l} \hat{Q}_i C_i$$

holds (in view of the formulas (4.11) and (4.12)). Therefore,

$$(4.13) \qquad \mathsf{Z}(\mathcal{P}) = \bigcup_{i=1}^{l-1} \mathsf{Z}(\mathcal{G} \cup \{I_i\}) \cup \mathsf{Z}(\mathcal{G} \cup \{I_{k+1}\}) \cup \mathsf{Z}(\mathcal{G} \cup \{\mathrm{prem}(Q, \mathcal{C}_{l-1})\}).$$

The zero relations in (4.8), (4.9), (4.10), and (4.13) show that for each polynomial set $\mathcal{P} \in \Phi$, any zero of $\mathcal{P}$ is either in $\mathsf{Z}(\mathcal{C}/\mathrm{ini}(\mathcal{C}))$ if the W-characteristic set $\mathcal{C}$ of $\langle \mathcal{P} \rangle$ is normal in case (1) or in $\mathsf{Z}(\mathcal{P}')$ for another polynomial set $\mathcal{P}'$ adjoined to Φ for later computation in the other cases. This proves the zero relation $\mathsf{Z}(\mathcal{F}) = \bigcup_{(\mathcal{G}, \mathcal{C}) \in \Psi} \mathsf{Z}(\mathcal{C}/\mathrm{ini}(\mathcal{C}))$; for Algorithm 1 terminates when Φ becomes empty.

On one hand, by the zero relation (4.1), we have

$$\mathsf{Z}(\mathcal{F}) = \bigcup_{(\mathcal{G}, \mathcal{C}) \in \Psi} \mathsf{Z}(\mathcal{C}/\mathrm{ini}(\mathcal{C})) \subseteq \bigcup_{(\mathcal{G}, \mathcal{C}) \in \Psi} \mathsf{Z}(\mathcal{G}).$$

On the other hand, $\mathsf{Z}(\mathcal{G}) \subseteq \mathsf{Z}(\mathcal{F})$ holds for all $(\mathcal{G}, \mathcal{C}) \in \Psi$ according to the zero relations (4.8), (4.9), (4.10), and (4.13) for the four cases of splitting. This proves the equality $\mathsf{Z}(\mathcal{F}) = \bigcup_{(\mathcal{G}, \mathcal{C}) \in \Psi} \mathsf{Z}(\mathcal{G})$. For each $(\mathcal{G}, \mathcal{C}) \in \Psi$, we have $\mathsf{Z}(\mathcal{C}/\mathrm{ini}(\mathcal{C})) \subseteq \mathsf{Z}(\mathrm{sat}(C)) \subseteq \mathsf{Z}(G)$, and thus

$$\mathsf{Z}(\mathcal{F}) = \bigcup_{(\mathcal{G}, \mathcal{C}) \in \Psi} \mathsf{Z}(\mathcal{C}/\mathrm{ini}(\mathcal{C})) \subseteq \bigcup_{(\mathcal{G}, \mathcal{C}) \in \Psi} \mathsf{Z}(\mathrm{sat}(\mathcal{C})) \subseteq \bigcup_{(\mathcal{G}, \mathcal{C}) \in \Psi} \mathsf{Z}(\mathcal{G}) = \mathsf{Z}(\mathcal{F}).$$

This completes the proof of the zero relation (3.1). $\qquad\qquad\qquad\qquad\qquad \square$

5. Example and experiments

5.1. Example for normal characteristic decomposition.

Let $\mathcal{F} = \{ay - x - 1, -xyz + az, xz^2 - az + y\} \subseteq \mathbb{K}[a, x, y, z]$ with $a < x < y < z$. The procedure to compute a normal characteristic decomposition of $\mathcal{F}$ using Algorithm 1 is shown in Table 1, where $\mathcal{G}_i$ is the computed reduced lex Gröbner basis and $\mathcal{C}_i$ is its W-characteristic set in the ith loop.

TABLE 1. Illustration for Algorithm 1

i	Φ	$\mathcal{P}$	$\mathcal{G}_i$	$\mathcal{C}_i$	Normal	Case	Ψ
1	$\{\mathcal{F}\}$	$\mathcal{F}$	$\{G_1, G_2, G_3, G_4,$ $zG_5, zG_6, G_7\}$	$[G_1, G_2, zG_5]$	No	2.2.2	$\emptyset$
2	$\{\mathcal{F}_1, \mathcal{F}_2\}$	$\mathcal{F}_1$	$\{x+1, y, az, z^2\}$	$[x+1, y, az]$	Yes	1	$\{(\mathcal{G}_2, \mathcal{C}_2)\}$
3	$\{\mathcal{F}_2, \mathcal{F}_3\}$	$\mathcal{F}_2$	$\{G_2, G_4, G_5,$ $zG_6, G_7\}$	$[G_2, G_5, zG_6]$	No	2.1	$\{(\mathcal{G}_2, \mathcal{C}_2)\}$
4	$\{\mathcal{F}_3, \mathcal{F}_4, \mathcal{F}_5\}$	$\mathcal{F}_3$	$\{a, x+1, y, z\}$	$[a, x+1, y, z]$	Yes	1	$\{(\mathcal{G}_2, \mathcal{C}_2), (\mathcal{G}_4, \mathcal{C}_4)\}$
5	$\{\mathcal{F}_4, \mathcal{F}_5\}$	$\mathcal{F}_4$	$\{G_5, G_2, G_6, G_7\}$	$[G_5, G_2, G_7]$	Yes	1	$\{(\mathcal{G}_2, \mathcal{C}_2), (\mathcal{G}_4, \mathcal{C}_4)$ $(\mathcal{G}_5, \mathcal{C}_5)\}$
6	$\{\mathcal{F}_5, \mathcal{F}_6\}$	$\mathcal{F}_5$	$\{a, x+1, y^2,$ $yz, z^2 - y\}$	$[a, x+1, y^2, yz]$	No	2.2.2	$\{(\mathcal{G}_2, \mathcal{C}_2), (\mathcal{G}_4, \mathcal{C}_4)$ $(\mathcal{G}_5, \mathcal{C}_5)\}$
7	$\{\mathcal{F}_6\}$	$\mathcal{F}_6$	$\{a, x+1, y, z^2\}$	$[a, x+1, y, z^2]$	Yes	1	$\{(\mathcal{G}_2, \mathcal{C}_2), (\mathcal{G}_4, \mathcal{C}_4)$ $(\mathcal{G}_5, \mathcal{C}_5), (\mathcal{G}_7, \mathcal{C}_7)\}$

The polynomial sets $\mathcal{F}_i$ and polynomials G_j in Table 1 are listed below:

$$\mathcal{F}_1 = \{x+1, y, ay, az, (y+a)z, G_7\}, \quad \mathcal{F}_2 = \{G_4, aG_2, zG_6, G_2, G_7, G_5\},$$
$$\mathcal{F}_3 = \{a, x+1, y, z\}, \quad\quad\quad\quad\quad \mathcal{F}_4 = \{G_5, G_2, G_6, G_7\},$$
$$\mathcal{F}_5 = \{a, x+1, x^2+x, G_4, xyz, G_7\}, \quad \mathcal{F}_6 = \{a, x+1, x^2+x, xy, G_7\};$$
$$G_1 = x^3 + 2x^2 + (1-a^2)x - a^2, \quad G_2 = ay - x - 1,$$
$$G_3 = x^2y + xy - ax - a, \quad\quad\quad\quad G_4 = xy^2 - x - 1,$$
$$G_5 = x^2 + x - a^2, \quad\quad\quad\quad\quad\quad G_6 = xy - a,$$
$$G_7 = z^2 - yz + y^3 - y.$$

The output normal characteristic decomposition of $\mathcal{P}$, as shown in Table 1, is $\{(\mathcal{G}_2, \mathcal{C}_2), (\mathcal{G}_4, \mathcal{C}_4), (\mathcal{G}_5, \mathcal{C}_5), (\mathcal{G}_7, \mathcal{C}_7)\}$.

5.2. Experimental results.

Algorithm 1 has been implemented in Maple 17 based on functions available in the FGb and Maple's built-in packages for Gröbner basis computation. The implementation will be included in the upcoming new version of the Epsilon package for triangular decomposition [44].

In Theorem 2.11 there is an assumption on the variable order (i.e., all the parameters of a W-characteristic set are ordered before the other variables). This assumption always holds in the zero-dimensional case. Our experiments show that in the positive-dimensional case there are about one-fourth of the test examples for which the assumption does not hold. The assumption is made to ensure that the (pseudo) divisibility relationships in Theorem 2.11 occur. In the case where the assumption does not hold, we can make such relationships occur by heuristically changing the variable order. In fact, using the heuristics we were able to obtain

necessary (pseudo) divisibility relationships to complete the characteristic decomposition for all the test examples. More experimental investigations on the effect of heuristical change of variable orders will be reported elsewhere.

Let us emphasize that Algorithm 1 decomposes any polynomial set into normal characteristic pairs of reduced lex Gröbner bases and their W-characteristic sets at one stroke. The two kinds of objects that resulted from the combined decomposition, each having its own structures and properties, are interconnected. This makes our algorithm distinct from other existing ones for triangular decomposition. To observe the computational performance of the algorithm, in comparison with algorithms for indirect normal decomposition (that is, first computing a regular decomposition and then normalizing the regular sets in the decomposition), we made some experiments on an Intel(R) Core(TM) Quad CPU at 2.83 GHz with 4.00 GB RAM under Windows 7 Home Basic. Selected results of the experiments are presented in Table 2, of which the first 9 are taken from [8] and the others are from benchmarks for the FGb library. We implemented Algorithm 1 as CharDec in MAPLE for normal characteristic decomposition and used the functions Triangularize (from the RegularChains package in MAPLE) and RegSer (from the Epsilon package for MAPLE) for regular decomposition and the function normat (from the miscel module of Epsilon) for normalization.

In Table 2, "Source" indicates the label in the above-cited references and "Dim" denotes the dimension of the ideal in the example. "Total" under CharDec records the total time (followed by the number of pairs in parenthesis) for normal characteristic decomposition using Algorithm 1; "GB" under CharDec records the time for computing all the reduced lex Gröbner bases; "Total" and "Regular" under RegSer and Triangularize record the total time for normal decomposition and the time for regular decomposition (followed by the numbers of components in parenthesis), respectively, where normal decompositions are computed from regular decompositions by means of normalization using normat. The marks "lost" and "> 4000" in the columns mean that MAPLE reports "lost kernel connections" and that the computation does not terminate within 4000 seconds, respectively.

The most time-consuming step in CharDec is for the computation of lex Gröbner bases, as one can see from Table 2. In our implementation, the FGb library is first invoked to compute Gröbner bases with respect to graded reverse lexicographic term ordering, and the computed Gröbner bases are then converted to lex Gröbner bases by changing the term ordering using either the FGLM algorithm for the zero-dimensional case [18] or the Gröbner walk otherwise [11]. Unfortunately, the built-in implementation of the Gröbner walk algorithm in MAPLE is very inefficient and it is the current bottleneck of our implementation.

Finally, we add a few remarks to conclude the paper: we have studied normal characteristic pairs (that is, pairs of reduced lex Gröbner bases and normal triangular sets) and the problem of normal characteristic decomposition (that is, decomposition of arbitrary polynomial sets into normal characteristic pairs). We have proved a number of properties about normal characteristic pairs and normal characteristic decomposition, and proposed an algorithm with implementation for the decomposition. The algorithm explores the inherent connection between Ritt characteristic sets and lex Gröbner bases and mainly involves the computation of lex Gröbner bases; normal triangular sets are obtained as a by-product almost for free. Associated to a normal characteristic decomposition $\{(\mathcal{G}_1, \mathcal{C}_1), \ldots, (\mathcal{G}_t, \mathcal{C}_t)\}$ of

TABLE 2. Timings for characteristic/normal decomposition

		CharDec		RegSer		Triangularize	
Source	Dim	Total	GB	Total	Regular	Total	Regular
S5	4	0.14(8)	0.047	4.182(31)	0.484(19)	1.513(9)	0.124(1)
S7	1	0.156(5)	0.078	0.251(7)	0.11(4)	0.249(5)	0.109(1)
S8	2	0.062(2)	0.32	0.062(3)	0.062(3)	0.156(2)	0.141(2)
S9	2	0.125(5)	0.078	0.483(21)	0.14(8)	0.188(6)	0.094(1)
S10	3	0.594(16)	0.313	0.438(7)	0.172(5)	0.36(3)	0.235(1)
S13	3	0.312(13)	0.14	0.171(8)	0.109(8)	0.125(2)	0.094(1)
S14	2	0.531(9)	0.327	0.14(6)	0.109(6)	0.157(8)	0.125(8)
S16	3	0.640(6)	0.344	0.703(7)	0.609(7)	4.609(8)	4.609(8)
S17	6	lost	lost	lost	lost	lost	lost
nueral	1	1.826(15)	1.514	> 4000	> 4000	0.233(6)	0.14(5)
F663	2	2.949(6)	2.326	1.935(16)	1.202(15)	1.607(6)	1.045(4)
Dessin2	0	27.222(1)	27.207	> 4000	> 4000	> 4000	> 4000
Wang16	0	0.203(1)	0.171	14.555(1)	0.437(1)	14.086(1)	0.156(1)
filter9	0	0.640(1)	0.593	> 4000	> 4000	lost	lost
fabrice24	0	436.7(1)	436.7	lost	lost	lost	lost
uteshev bikker	0	3.806(1)	3.766	lost	lost	> 4000	> 4000
Cyclic6	0	2.153(25)	1.244	lost	lost	> 4000	> 4000

a polynomial set $\mathcal{P}$ are zero decompositions

$$\mathsf{Z}(\mathcal{P}) = \mathsf{Z}(\mathcal{G}_1) \cup \cdots \cup \mathsf{Z}(\mathcal{G}_t) = \mathsf{Z}(\mathcal{C}_1/\operatorname{ini}(\mathcal{C}_t)) \cup \cdots \cup \mathsf{Z}(\mathcal{C}_t/\operatorname{ini}(\mathcal{C}_t))$$

and the corresponding radical ideal decompositions

$$\sqrt{\langle\mathcal{P}\rangle} = \sqrt{\langle\mathcal{G}_1\rangle} \cup \cdots \cup \sqrt{\langle\mathcal{G}_t\rangle} = \sqrt{\operatorname{sat}(\mathcal{C}_1)} \cup \cdots \cup \sqrt{\operatorname{sat}(\mathcal{C}_t)}.$$

In these decompositions, the reduced lex Gröbner bases $\mathcal{G}_1, \ldots, \mathcal{G}_t$ and normal triangular sets $\mathcal{C}_1, \ldots, \mathcal{C}_t$ are closely linked and well-structured polynomial sets whose usefulness has been widely recognized.

REFERENCES

[1] G. Angermüller, *Triangular systems and a generalization of primitive polynomials*. part 1, J. Symbolic Comput. **68** (2015), 316–325, DOI 10.1016/j.jsc.2014.09.022. MR3283849

[2] P. Aubry, *Ensembles triangulaires de polynômes et résolution de systemes algébriques. implantation en axiom*, Ph.D. thesis, Université Pierre et Marie Curie, France, 1999.

[3] P. Aubry, D. Lazard, and M. Moreno Maza, *On the theories of triangular sets*: *Polynomial elimination—algorithms and applications*, J. Symbolic Comput. **28** (1999), no. 1-2, 105–124, DOI 10.1006/jsco.1999.0269. MR1709419

[4] P. Aubry and M. Moreno Maza, *Triangular sets for solving polynomial systems: a comparative implementation of four methods*: *Polynomial elimination—algorithms and applications*, J. Symbolic Comput. **28** (1999), no. 1-2, 125–154, DOI 10.1006/jsco.1999.0270. MR1709420

[5] T. Bächler, V. Gerdt, M. Lange-Hegermann, and D. Robertz, *Algorithmic Thomas decomposition of algebraic and differential systems*, J. Symbolic Comput. **47** (2012), no. 10, 1233–1266, DOI 10.1016/j.jsc.2011.12.043. MR2926124

[6] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal*, Ph.D. thesis, Universität Innsbruck, Austria, 1965.

[7] B. Buchberger, *Gröbner bases: An algorithmic method in polynomial ideal theory*, Multidimensional Systems Theory (Nirmal Bose, ed.), Springer, Netherlands, 1985, pp. 184–232.

[8] C. Chen, O. Golubitsky, F. Lemaire, M. Moreno Maza, and W. Pan, *Comprehensive Triangular Decomposition*, Proceedings of CASC 2007 (Victor Ganzha, Ernst Mayr, and Evgenii Vorozhtsov, eds.), Springer-Verlag, Berlin Heidelberg, 2007, pp. 73–101.

[9] C. Chen and M. Moreno Maza, *Algorithms for computing triangular decomposition of polynomial systems*, J. Symbolic Comput. **47** (2012), no. 6, 610–642, DOI 10.1016/j.jsc.2011.12.023. MR2908585

[10] S.-C. Chou and X. S. Gao, *Ritt-Wu's Decomposition Algorithm and Geometry Theorem Proving*, 10th International Conference on Automated Deduction (Kaiserslautern, 1990), Lecture Notes in Comput. Sci., vol. 449, Springer, Berlin, 1990, pp. 207–220, DOI 10.1007/3-540-52885-7_89. MR1077003

[11] S. Collart, M. Kalkbrener, and D. Mall, *Converting bases with the Gröbner walk: Computational algebra and number theory (London, 1993)*, J. Symbolic Comput. **24** (1997), no. 3-4, 465–469, DOI 10.1006/jsco.1996.0145. MR1484492

[12] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, 3rd ed., Undergraduate Texts in Mathematics, Springer, New York, 2007. An Introduction to Computational Algebraic Geometry and Commutative Algebra. MR2290010

[13] X. Dahan, *On lexicographic Gröbner bases of radical ideals in dimension zero: Interpolation and structure*, Preprint at arXiv:1207.3887, 2012.

[14] J. D. Dora, C. Dicrescenzo, and D. Duval, *About a new method for computing in algebraic number fields*, Proceedings of EUROCAL '85 (Bruno Buchberger, ed.), Springer-Verlag, Berlin Heidelberg, 1985, pp. 289–290.

[15] S. Dellière, *On the links between triangular sets and dynamic constructible closure*, J. Pure Appl. Algebra **163** (2001), no. 1, 49–68, DOI 10.1016/S0022-4049(00)00136-5. MR1847375

[16] J.-C. Faugére, *A new efficient algorithm for computing Gröbner bases (F_4): Effective methods in algebraic geometry (Saint-Malo, 1998)*, J. Pure Appl. Algebra **139** (1999), no. 1-3, 61–88, DOI 10.1016/S0022-4049(99)00005-5. MR1700538

[17] J. C. Faugére, *A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F_5)*, Proceedings of ISSAC 2002 (Teo Mora, ed.), ACM Press, 2002, pp. 75–83.

[18] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J. Symbolic Comput. **16** (1993), no. 4, 329–344, DOI 10.1006/jsco.1993.1051. MR1263871

[19] S. Gao, F. Volny IV, and M. Wang, *A new framework for computing Gröbner bases*, Math. Comp. **85** (2016), no. 297, 449–465, DOI 10.1090/mcom/2969. MR3404457

[20] X.-S. Gao and S.-C. Chou, *Solving Parametric Algebraic Systems*, Proceedings of ISSAC 1992 (Paul Wang, ed.), ACM Press, 1992, pp. 335–341.

[21] X.-S. Gao and S.-C. Chou, *On the dimension of an arbitrary ascending chain*, Chinese Science Bulletin - English Edition **38** (1993), 799–799.

[22] P. Gianni, *Properties of Gröbner Bases Under Specializations*, Proceedings of EUROCAL '87 (Leipzig, 1987), Lecture Notes in Comput. Sci., vol. 378, Springer, Berlin, 1989, pp. 293–297, DOI 10.1007/3-540-51517-8_128. MR1033305

[23] P. Gianni, B. Trager, and G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symbolic Comput. **6** (1988), no. 2-3, 149–167, DOI 10.1016/S0747-7171(88)80040-3. Computational aspects of commutative algebra. MR988410

[24] J. D. Hauenstein, A. J. Sommese, and C. W. Wampler, *Regeneration homotopies for solving systems of polynomials*, Math. Comp. **80** (2011), no. 273, 345–377, DOI 10.1090/S0025-5718-2010-02399-3. MR2728983

[25] E. Hubert, *Notes on Triangular Sets and Triangulation-decomposition Algorithms. I. Polynomial systems*, Symbolic and numerical scientific computation (Hagenberg, 2001), Lecture Notes in Comput. Sci., vol. 2630, Springer, Berlin, 2003, pp. 1–39, DOI 10.1007/3-540-45084-X_1. MR2043699

[26] M. Kalkbrener, *Solving Systems of Algebraic Equations by Using Gröbner Bases*, Proceedings of EUROCAL '87 (Leipzig, 1987), Lecture Notes in Comput. Sci., vol. 378, Springer, Berlin, 1989, pp. 282–292, DOI 10.1007/3-540-51517-8_127. MR1033304

[27] M. Kalkbrener, *A generalized Euclidean algorithm for computing triangular representations of algebraic varieties*, J. Symbolic Comput. **15** (1993), no. 2, 143–167, DOI 10.1006/jsco.1993.1011. MR1218756

[28] D. Kapur, Y. Sun, and D. Wang, *A New Algorithm for Computing Comprehensive Gröbner Systems*, ISSAC 2010—Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2010, pp. 29–36, DOI 10.1145/1837934.1837946. MR2920533

[29] D. Lazard, *Ideal bases and primary decomposition: case of two variables*, J. Symbolic Comput. **1** (1985), no. 3, 261–270, DOI 10.1016/S0747-7171(85)80035-3. MR849035

[30] D. Lazard, *A new method for solving algebraic systems of positive dimension: Applied algebra, algebraic algorithms, and error-correcting codes (Toulouse, 1989)*, Discrete Appl. Math. **33** (1991), no. 1-3, 147–160, DOI 10.1016/0166-218X(91)90113-B. MR1137743

[31] D. Lazard, *Solving zero-dimensional algebraic systems*, J. Symbolic Comput. **13** (1992), no. 2, 117–131, DOI 10.1016/S0747-7171(08)80086-7. MR1153638

[32] F. Lemaire, M. Moreno Maza, W. Pan, and Y. Xie, *When does ⟨T⟩ equal sat(T)?*, J. Symbolic Comput. **46** (2011), no. 12, 1291–1305, DOI 10.1016/j.jsc.2011.08.010. MR2860999

[33] B. Li and D. Wang, *An Algorithm for Transforming Regular Chain into Normal Chain*, Computer Mathematics (Deepak Kapur, ed.), Springer-Verlag, Berlin Heidelberg, 2008, pp. 236–245.

[34] M. G. Marinari and T. Mora, *A remark on a remark by Macaulay or enhancing Lazard structural theorem* (English, with Persian summary), Bull. Iranian Math. Soc. **29** (2003), no. 1, 1–45, 85. MR2046304

[35] C. Mou, D. Wang, and X. Li, *Decomposing polynomial sets into simple sets over finite fields: the positive-dimensional case*, Theoret. Comput. Sci. **468** (2013), 102–113, DOI 10.1016/j.tcs.2012.11.009. MR3003772

[36] A. Poteaux and É. Schost, *On the complexity of computing with zero-dimensional triangular sets*, J. Symbolic Comput. **50** (2013), 110–138, DOI 10.1016/j.jsc.2012.05.008. MR2996871

[37] J. F. Ritt, *Differential Algebra*, American Mathematical Society Colloquium Publications, Vol. 33, American Mathematical Society, New York, N. Y., 1950. MR0035763

[38] T. Shimoyama and K. Yokoyama, *Localization and primary decomposition of polynomial ideals*, J. Symbolic Comput. **22** (1996), no. 3, 247–277, DOI 10.1006/jsco.1996.0052. MR1427183

[39] D.-k. Wang and Y. Zhang, *An algorithm for decomposing a polynomial system into normal ascending sets*, Sci. China Ser. A **50** (2007), no. 10, 1441–1450, DOI 10.1007/s11425-007-0118-0. MR2390461

[40] D. M. Wang, *An elimination method for polynomial systems*, J. Symbolic Comput. **16** (1993), no. 2, 83–114, DOI 10.1006/jsco.1993.1035. MR1253907

[41] D. Wang, *Decomposing polynomial systems into simple systems*, J. Symbolic Comput. **25** (1998), no. 3, 295–314, DOI 10.1006/jsco.1997.0177. MR1615318

[42] D. Wang, *Computing triangular systems and regular systems*, J. Symbolic Comput. **30** (2000), no. 2, 221–236, DOI 10.1006/jsco.1999.0355. MR1777174

[43] D. Wang, *Elimination Methods*, Springer-Verlag, Wien, 2001.

[44] D. Wang, *Epsilon: A Library of Software Tools for Polynomial Elimination*, Mathematical software (Beijing, 2002), World Sci. Publ., River Edge, NJ, 2002, pp. 379–389. MR1932623

[45] D. Wang, *Elimination Practice: Software tools and applications; With 1 CD-ROM (UNIX/LINUX, Windows)*, Imperial College Press, London, 2004. MR2050441

[46] D. Wang, *On the connection between Ritt characteristic sets and Buchberger-Gröbner bases*, Math. Comput. Sci. **10** (2016), no. 4, 479–492, DOI 10.1007/s11786-016-0279-8. MR3569681

[47] V. Weispfenning, *Comprehensive Gröbner bases*, J. Symbolic Comput. **14** (1992), no. 1, 1–29, DOI 10.1016/0747-7171(92)90023-W. MR1177987

[48] W. J. Wu, *On zeros of algebraic equations—an application of Ritt principle*, Kexue Tongbao (English Ed.) **31** (1986), no. 1, 1–5. MR850170

[49] W. T. Wu, *Mechanical Theorem Proving in Geometries*: *Basic Principles*, Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 1994. Translated from the 1984 Chinese original by Xiao Fan Jin and Dong Ming Wang. MR1284925

[50] W.-T. Wu, *Mathematics Mechanization*: *Mechanical Geometry Theorem-proving, Mechanical Geometry Problem-solving and Polynomial Equations-solving*, Mathematics and its Applications, vol. 489, Kluwer Academic Publishers Group, Dordrecht; Science Press Beijing, Beijing, 2000. MR1834540

BDBC – LMIB – School of Mathematical Sciences, Beihang University, Beijing 100191, China; Centre National de la Recherche Scientifique, 75794 Paris cedex 16, France

Email address: dongming.wang@lip6.fr

LMIB – School of Mathematical Sciences, Beihang University, Beijing 100191, China
Email address: rina.dong@buaa.edu.cn

BDBC – LMIB – School of Mathematical Sciences, Beihang University, Beijing 100191, China
Email address: chenqi.mou@buaa.edu.cn