Computing strong regular characteristic pairs with Gröbner bases

Rina Dong \textsuperscript{1a} and Dongming Wang\textsuperscript{ab}

\textsuperscript{a}BDBC – LMIB – School of Mathematics and Systems Science, Beihang University, Beijing 100191, China
rina.dong@buaa.edu.cn

\textsuperscript{b}Centre National de la Recherche Scientifique, 75794 Paris cedex 16, France
dongming.wang@lip6.fr

Abstract

The W-characteristic set of a polynomial ideal is the minimal triangular set contained in the reduced lexicographical Gröbner basis of the ideal. A pair \((C, G)\) of polynomial sets is a strong regular characteristic pair if \(G\) is a reduced lexicographical Gröbner basis, \(C\) is the W-characteristic set of the ideal \((G)\), the saturated ideal sat\((C)\) of \(C\) is equal to \((G)\), and \(C\) is regular. In this paper, we show that for any regular set \(T\) the W-characteristic set \(C\) and the reduced lexicographical Gröbner basis \(G\) of sat\((T)\) form a strong regular characteristic pair \((C, G)\), and for any polynomial ideal \(I\) with given generators one can either detect that \(I\) is unit, or construct a strong regular characteristic pair \((C, G)\) by computing Gröbner bases such that \(I \subseteq \text{sat}(C)\), so the radical ideal of \(I\) can be split into the saturated ideal sat\((C)\) and the quotient ideal \(I : \text{sat}(C)\). Based on this strategy of splitting by means of quotient and with Gröbner basis and ideal computations, we devise a simple algorithm to decompose an arbitrary polynomial set \(F\) into finitely many strong regular characteristic pairs, from which two representations for the zeros of \(F\) are obtained: one in terms of strong regular Gröbner bases and the other in terms of regular triangular sets. We present some properties about strong regular characteristic pairs and characteristic decompositions and illustrate the proposed algorithm and its performance by examples and experimental results.

Key words: Strong regular, characteristic decomposition, W-characteristic set, Gröbner basis, ideal computation

1 Introduction

Triangular sets \[27, 33, 17, 30\] and Gröbner bases \[5, 6, 4, 10\] are special kinds of well-structured sets of multivariate polynomials that can be used to represent and to study zeros

\footnote{This work was partially supported by the National Natural Science Foundation of China (NSFC 11771034).}

\footnote{Corresponding author: rina.dong@buaa.edu.cn, School of Mathematics and Systems Science, Beihang University, Beijing 100191, China.}
of arbitrary polynomial sets and ideals. A large variety of problems in commutative algebra and algebraic geometry \[10, 11\] may readily be solved by transforming the involved sets of polynomials into triangular sets or Gröbner bases. It is widely known that the theories and methods of triangular sets are different from those of Gröbner bases conceptually and operationally. The questions that have motivated our work here and in \[31, 32\] are what inherent relationship there may exist between triangular sets and Gröbner bases and how to connect or combine the two algorithmic approaches to amplify their applicability and power. These questions have been touched primarily for some special polynomial ideals such as bivariate ideals \[18\] and zero-dimensional ideals \[22, 12, 19\], while the general literature of studies on triangular sets and Gröbner bases is extremely rich (see \[2, 4, 6, 7, 8, 9, 12, 13, 14, 15, 17, 18, 20, 21, 23, 24, 25, 26, 28, 29, 31, 32\] and references therein).

Multivariate polynomials in a triangular set may be ordered strictly according to their leading variables, with respect to a fixed variable ordering, so the number of the polynomials cannot be bigger than that of the variables in any triangular set. On the other hand, Gröbner bases are defined with respect to a fixed term order determined by the variable ordering and the number of elements in a Gröbner basis can be arbitrarily large. For any polynomial ideal with given set \(F\) of generators, one can compute, by using any of the available algorithms, a Gröbner basis that generates the same ideal as \(F\). To represent the zeros of \(F\) using triangular sets, in general one needs more than one triangular set, so decomposition takes place. When a triangular set \(T\) is of concern, the leading coefficients of the polynomials in \(T\) with respect to their leading variables, called the initials of the polynomials in \(T\), play a fundamental role. The saturated ideal of \(T\) by the product of the initials of the polynomials in \(T\), called the saturated ideal of \(T\) and denoted as \(\text{sat}(T)\), is the largest ideal whose zero set contains the set of those zeros of \(T\) which are not zeros of any of the initials.

Triangular sets may be ordered according to the ranks (leading variables and degrees) and then the leading terms of their polynomials. Let the minimal triangular set contained in the reduced lexicographical (lex) Gröbner basis of a polynomial ideal (or trivially \[1\] if the ideal is unit) be called the W-characteristic set of the ideal. By strong regular Gröbner basis, we mean a reduced lex Gröbner basis \(G\) such that the W-characteristic set \(C\) of the ideal \(\langle G \rangle\) is regular and \(\text{sat}(C) = \langle G \rangle\); we call \((C, G)\) a strong regular characteristic pair, or an src pair for short. The pair \((C, G)\) is an interesting object of study because the strong regular Gröbner basis \(G\) and the regular triangular set \(C\) therein not only have remarkable properties but also provide two different yet correlated representations for the zeros of the ideal \(\langle G \rangle\).

What interests us most is algorithmic decomposition of arbitrary polynomial sets into strong regular Gröbner bases, or equivalently into src pairs, for which we have the following general approach. From any polynomial set \(F\), one can compute finitely many regular sets (also called regular chains \[16\]) \(T_1, \ldots, T_e\) such that
\[
\sqrt{\langle F \rangle} = \sqrt{\text{sat}(T_1)} \cap \cdots \cap \sqrt{\text{sat}(T_e)}.
\] (1)

There are two families of algorithms for such regular triangular decomposition. One family of algorithms was proposed initially by Kalkbrener \[17\], and developed further by Moreno Maza and coauthors \[24, \ [1, 8, 9\] with algorithmic techniques from the method of Lazard \[19\]. These algorithms are capable of computing regular triangular representations of the form \[11\]. The other family of algorithms was proposed by the second author \[30, 29\] which can compute regular zero decompositions of the form
\[
Z(F) = Z(T_1/J_1) \cup \cdots \cup Z(T_e/J_e), \quad (2)
\]
where each $J_i$ is the product of the initials of the polynomials in the regular set $T_i$ and $\mathbb{Z}(T_i/J_i)$ denotes the set of all common zeros of the polynomials in $T_i$ which does not make $J_i$ vanish. It is easy to see that the decomposition (2) implies the representation (1). However, the representation (1) does not necessarily lead to the decomposition (2) and generators of the saturated ideals sat$(T_i)$ in (1) are not explicitly provided. Nevertheless, for each sat$(T_i)$ a Gröbner basis can be computed straightforwardly from $T_i$.

Another alternative approach proposed recently by Mou and the authors [32] permits one to decompose an arbitrary polynomial set into normal or regular characteristic pairs directly. This approach is based on a structure theorem about irregular W-characteristic sets [31] for the splitting of ideals and relies strongly upon Gröbner basis computation; it is independent of pseudo-division-based triangular decomposition.

In this paper, we show that from any regular set $T$ an src pair $(C, G)$ with sat$(C) = \text{sat}(T)$ can be easily formed by computing a reduced lex Gröbner basis, and from any polynomial ideal $\mathcal{I}$ with given generators one can either detect that $\mathcal{I}$ is unit, or construct an src pair $(C, G)$ such that $\mathcal{I} \subseteq \text{sat}(C)$ by computing possibly several Gröbner bases. After an src pair $(C^{(1)}, G^{(1)}) = (C, G)$ is constructed, one can divide the saturated ideal sat$(C^{(1)})$ out of $\mathcal{I}$ to obtain an ideal $\mathcal{J}^{(1)}$ by taking ideal quotients: $\mathcal{J}^{(1)} = \mathcal{I} : \text{sat}(C^{(1)})$. If $\mathcal{J}^{(1)}$ is larger than $\mathcal{I}$, then the radical ideal of $\mathcal{I}$ is split as the intersection of the radical ideals of sat$(C^{(1)})$ and $\mathcal{J}^{(1)}$. Otherwise, one can proceed to find another src pair $(C^{(2)}, G^{(2)})$ based on the initials of the polynomials in $C^{(1)}$ and consider the quotient: $\mathcal{J}^{(2)} = \mathcal{I} : \text{sat}(C^{(2)})$. This process may continue until an ideal $\mathcal{J}^{(k)}$ is found to be larger than $\mathcal{I}$; then the radical ideal of $\mathcal{I}$ may be split as the intersection of the radical ideals of sat$(C^{(k)})$ and $\mathcal{J}^{(k)} = \mathcal{J}^{'}$. When $\mathcal{J}^{'}$ is obtained, one can iterate the find-and-divide process with $\mathcal{J}^{'}$ instead of $\mathcal{I}$. Based on this strategy of splitting by means of quotient and with Gröbner basis and ideal computations, we devise a simple algorithm to decompose an arbitrary polynomial set $F$ into finitely many src pairs $(C_1, G_1), \ldots, (C_e, G_e)$ such that

$$\sqrt{\langle F \rangle} = \sqrt{\text{sat}(C_1)} \cap \cdots \cap \sqrt{\text{sat}(C_e)} = \sqrt{\langle G_1 \rangle} \cap \cdots \cap \sqrt{\langle G_e \rangle}. \quad (3)$$

In the above decomposition computed by the find-and-divide algorithm, each $G_i$ is actually the reduced lex Gröbner basis of a saturated ideal sat$(T_i)$, where $T_i$ is the W-characteristic set of a certain ideal that contains $\langle F \rangle$. The regular set $C_i$ is the W-characteristic set of sat$(T_i)$, obtained from $G_i$ as a by-product for free. Moreover, regular sets computed by our algorithm are normal in most cases and they usually have smaller sizes than the corresponding regular sets computed by pseudo-division [1] or subresultant-based algorithms, because the former are minimal triangular sets taken from lex Gröbner bases. In general, the generating sets of the saturated ideals of normal triangular sets are much easier to compute than those of abnormal ones. More importantly, our algorithm generates few redundant components, so the decomposition process usually terminates in a few iterations. The effectiveness of the decomposition algorithm has been demonstrated by our experimental results.

The rest of the paper is organized as follows. After a brief introduction to Gröbner bases, triangular decomposition, and characteristic decomposition in Section 2, we show in Section 3 how to construct from any regular set $T$ an src pair $(C, G)$ such that sat$(C) = \text{sat}(T)$.
sat(\mathcal{T})\), and from an arbitrary ideal \mathcal{J} an src pair \((\mathcal{C}, \mathcal{G})\) such that \mathcal{J} \subseteq \text{sat} (\mathcal{C})\). The find-and-divide algorithm for strong regular characteristic decomposition is described in Section 3. The algorithm and its performance are illustrated by examples and experimental results with a preliminary implementation of the algorithm in Section 5. The paper contains a summary of contributions in Section 6 and some remarks on special cases in Appendix A.

2 Preliminaries

In this section we recall some basic notions which will be used in the following sections. For those notions which are not formally introduced in the paper, the reader may consult the references [2, 30, 4, 10].

2.1 Triangular sets, triangular decompositions, and Gröbner bases

Let \( \mathbb{K} \) be a field and \( \mathbb{K}[x_1, \ldots, x_n] \) be the ring of polynomials in \( n \) ordered variables \( x_1 < \cdots < x_n \) with coefficients in \( \mathbb{K} \). Throughout the paper, we write \( x \) for \( (x_1, \ldots, x_n) \).

Let \( F \) be a polynomial in \( \mathbb{K}[x] \setminus \mathbb{K} \). With respect to the variable ordering, the greatest variable appearing in \( F \) is called the \textit{leading variable} of \( F \) and denoted as \( \text{lv}(F) \). Assume that \( \text{lv}(F) = x_i \); then \( F \) can be written as \( F = Ix_i^k + R \), where \( I \in \mathbb{K}[x_1, \ldots, x_{i-1}] \), \( R \in \mathbb{K}[x_1, \ldots, x_i] \), and \( \text{deg}(R, x_i) < k = \text{deg}(F, x_i) \) (the degree of \( F \) in \( x_i \)). The polynomial \( I \) is called the \textit{initial} of \( F \), denoted as \( \text{ini}(F) \). For any polynomial set \( F \subseteq \mathbb{K}[x] \), \( \text{ini}(F) \) stands for \( \{ \text{ini}(F) \mid F \in F \} \).

**Definition 2.1** A finite, nonempty, ordered set \( [T_1, \ldots, T_r] \) of polynomials in \( \mathbb{K}[x] \setminus \mathbb{K} \) is called a \textit{triangular set} if \( \text{lv}(T_1) < \cdots < \text{lv}(T_r) \).

We denote by \( \text{prem}(P, Q) \) the pseudo-reminder of \( P \in \mathbb{K}[x] \) with respect to \( Q \in \mathbb{K}[x] \setminus \mathbb{K} \) in \( \text{lv}(Q) \). Let \( \mathcal{T} = [T_1, \ldots, T_r] \subseteq \mathbb{K}[x] \) be any triangular set; the pseudo-reminder of \( P \) with respect to \( \mathcal{T} \) is defined as

\[
\text{prem}(P, \mathcal{T}) := \text{prem}(\cdots \text{prem}(\text{prem}(P, T_r), T_{r-1}), \ldots, T_1).
\]

The variables in \( \{x_1, \ldots, x_n\} \setminus \{\text{lv}(T_1), \ldots, \text{lv}(T_r)\} \) are called the \textit{parameters} of \( \mathcal{T} \). For any two polynomial sets \( \mathcal{F}, \mathcal{G} \subseteq \mathbb{K}[x] \), define

\[
Z(\mathcal{F}/\mathcal{G}) := \{ \bar{x} \in \mathbb{K}^n \mid F(\bar{x}) = 0, G(\bar{x}) \neq 0 \text{, for all } F \in \mathcal{F}, G \in \mathcal{G} \},
\]

where \( \mathbb{K} \) is the algebraic closure of \( \mathbb{K} \). Sometimes we write \( Z(\mathcal{F}/\prod_{G \in \mathcal{G}} G) \) for \( Z(\mathcal{F}/\mathcal{G}) \) and write \( Z(\mathcal{F}) \) for \( Z(\mathcal{F}/\emptyset) \).

Let \( \mathcal{F} \subseteq \mathbb{K}[x] \) be any polynomial set and denote by \( \langle \mathcal{F} \rangle \) the ideal generated by \( \mathcal{F} \) in \( \mathbb{K}[x] \) and by \( \sqrt{\langle \mathcal{F} \rangle} \) the radical of \( \langle \mathcal{F} \rangle \). For any \( P \subseteq \mathbb{K}[x] \), \( \langle P \rangle : \langle P \rangle \) denotes the ideal quotient of \( \langle P \rangle \) by \( \langle P \rangle \). The \textit{saturated ideal} of a triangular set \( \mathcal{T} = [T_1, \ldots, T_r] \) is defined as \( \text{sat}(\mathcal{T}) := \{ P \in \mathbb{K}[x] \mid \exists i \text{ such that } PJ^i \in \langle \mathcal{T} \rangle \} \), where \( J = \text{ini}(T_1) \cdots \text{ini}(T_r) \).

For any \( c \in \mathbb{K} \setminus \{0\} \), we consider \([c]\) also as a triangular set, which is trivial, and define \( \text{sat}([c]) = (1) \).

**Definition 2.2** Let \( \mathcal{T} = [T_1, \ldots, T_r] \) be any nontrivial triangular set in \( \mathbb{K}[x] \). \( \mathcal{T} \) is said to be \textit{regular}, or called a \textit{regular set} or a \textit{regular chain}, if \( \text{ini}(T_i) \) is neither zero nor a zero-divisor in \( \mathbb{K}[x]/\text{sat}(T_{r-1}) \) for all \( i = 1, \ldots, r \).

Regular sets or chains [29, 2] are special triangular sets with nice properties which have been extensively studied. In particular, it is proved in [30, 29] that a triangular set \( \mathcal{T} \) is
regular if and only if \( \text{sat}(T) = \{ P \in \mathbb{K}[x] \mid \text{prem}(P, T) = 0 \} \). The triangular set \( T \) is called a normal set (or said to be normal) if \( \text{ini}(T) \) does not involve any of the leading variables of the polynomials in \( T \). Obviously, any normal set is regular, while a regular set is not necessarily normal.

For a given term order \(<\), the greatest term in a polynomial \( F \in \mathbb{K}[x] \) with respect to \(<\) is called the leading term of \( F \) and denoted as \( \text{lt}(F) \). In this paper, we are concerned only with \(<\text{lex}, \) the lex term order.

**Definition 2.3** Let \( \mathcal{I} \subseteq \mathbb{K}[x] \) be an ideal, \(<\) be a term order, and \( \langle \text{lt}(\mathcal{I}) \rangle \) stand for the ideal generated by the leading terms of all the polynomials in \( \mathcal{I} \). A finite set \( \{ G_1, \ldots, G_s \} \subseteq \mathcal{I} \) is called a Gröbner basis of \( \mathcal{I} \) with respect to \(<\) if \( \langle \text{lt}(G_1), \ldots, \text{lt}(G_s) \rangle = \langle \text{lt}(\mathcal{I}) \rangle \).

Let \( \mathcal{G} = \{ G_1, \ldots, G_s \} \) be a Gröbner basis of an ideal \( \mathcal{I} \subseteq \mathbb{K}[x] \) with respect to a fixed term order \(<\). For an arbitrary polynomial \( F \in \mathbb{K}[x] \), there exists a unique polynomial \( R \in \mathbb{K}[x] \), called the normal form of \( F \) with respect to \( \mathcal{G} \) and denoted as \( \text{nform}(F, \mathcal{G}) \), such that \( F - R \in \mathcal{I} \) and no term of \( R \) is divisible by any of \( \text{lt}(G_1), \ldots, \text{lt}(G_s) \). If \( F = R \), then \( F \) is said to be B-reduced with respect to \( \mathcal{G} \).

**Definition 2.4** A Gröbner basis \( \{ G_1, \ldots, G_s \} \) is said to be reduced if every \( G_i \) is monic and no term of \( G_i \) is divisible by any \( \text{lt}(G_j) \) for all \( j \neq i \) and \( i, j = 1, \ldots, s \).

In the rest of this paper, the variable ordering will be fixed and all Gröbner bases mentioned are meant reduced lex Gröbner bases.

### 2.2 W-characteristic sets, characteristic pairs, and characteristic decompositions

For any polynomial ideal, one can compute its unique reduced lex Gröbner basis and from the Gröbner basis, one can extract a minimal triangular set. This special triangular set, defined formally as the W-characteristic set of the ideal, possesses remarkable properties and plays a key role in our work on src pairs.

**Definition 2.5** ([31, Def. 3.1]) Let \( \mathcal{F} \) be a polynomial set in \( \mathbb{K}[x] \), \( \mathcal{G} \) be the Gröbner basis of \( \langle \mathcal{F} \rangle \), \( \mathcal{G}^{(i)} = \{ G \in \mathcal{G} \mid \text{lv}(G) = x_i \} \), \( \Theta_i \) be the set consisting of the smallest polynomial in \( \mathcal{G}^{(i)} \) if \( \mathcal{G}^{(i)} \neq \emptyset \), or \( \emptyset \) otherwise (1 \( \leq i \leq n \)). The set \( \Theta_1 \cup \cdots \cup \Theta_n \) of polynomials ordered with increasing leading variables is called the W-characteristic set of \( \langle \mathcal{F} \rangle \).

**Proposition 2.6** ([31, Prop. 3.1]) Let \( \mathcal{F} \) be a polynomial set in \( \mathbb{K}[x] \) and \( \mathcal{C} \) be the W-characteristic set of \( \langle \mathcal{F} \rangle \subseteq \mathbb{K}[x] \). Then:

(a) for any \( F \in \langle \mathcal{F} \rangle \), \( \text{prem}(F, \mathcal{C}) = 0 \);

(b) \( \langle \mathcal{C} \rangle \subseteq \langle \mathcal{F} \rangle \subseteq \text{sat}(\mathcal{C}) \);

(c) \( \mathbb{Z}(\mathcal{C}/\text{ini}(\mathcal{C})) \subseteq \mathbb{Z}(\mathcal{F}) \subseteq \mathbb{Z}(\mathcal{C}) \).

We say that the variable ordering condition is satisfied for a triangular set \( T \) if all the parameters of \( T \) are ordered smaller than the leading variables of the polynomials in \( T \).

**Theorem 2.7** ([31, Thm. 3.9]) Let \( \mathcal{C} = [C_1, \ldots, C_r] \) be the W-characteristic set of \( \langle \mathcal{F} \rangle \subseteq \mathbb{K}[x] \). If the variable ordering condition is satisfied for \( \mathcal{C} \) and \( \mathcal{C} \) 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.
Some structural properties about pseudo-divisibility among polynomials in the Gröbner bases can be found in [31]. Based on those properties, an effective algorithm for normal triangular decomposition of polynomial sets has been proposed in [32].

**Definition 2.8** A pair \((C, G)\) of polynomial sets in \(\mathbb{K}[x]\) is called a characteristic pair if \(G\) is a Gröbner basis and \(C\) is the W-characteristic set of \(<G>\). We say that the pair \((C, G)\) is strong if \(\text{sat}(C) = <G>\).

A characteristic pair \((C, G)\) is said to be regular or normal if \(C\) is regular or normal, respectively. If the characteristic pair is strong and regular, then the Gröbner basis \(G\) in the pair is said to be strong regular. By regular or normal characteristic decomposition of a polynomial set \(F \subseteq \mathbb{K}[x]\), we mean a finite set of regular or normal characteristic pairs \((C_1, G_1), \ldots, (C_e, G_e)\) satisfying the ideal relations in (3).

The expression (3) can be rewritten in terms of the zero sets or varieties as

\[
Z(F) = \bigcup_{i=1}^{e} Z(G_i) = \bigcup_{i=1}^{e} Z(\text{sat}(C_i)).
\]  

(4)

When the regular or normal characteristic pairs \((C_i, G_i)\) are computed by the algorithms described in [29, 32], the zero relation

\[
Z(F) = \bigcup_{i=1}^{e} Z(C_i/\text{ini}(C_i))
\]  

(5)

is also satisfied.

To compute a desired characteristic decomposition of a polynomial set \(F\), we first proceed to decompose \(F\) into finitely many Gröbner bases \(G_i\) of certain kinds and then form the characteristic pairs \((C_i, G_i)\) by simply extracting the W-characteristic sets \(C_i\) from \(G_i\).

### 3 Computing strong regular characteristic pairs

The main objective of this section is to show how to construct from any regular set \(T\) an src (strong regular characteristic) pair \((C, G)\) such that \(\text{sat}(C) = \text{sat}(T)\), and from an arbitrary ideal \(I\) an src pair \((C, G)\) such that \(I \subseteq \text{sat}(C)\) by computing Gröbner bases. The construction enables us to devise a novel algorithm for decomposing any polynomial set into finitely many src pairs.

**Definition 3.1** A Gröbner basis \(G\) is said to be characterizable if \(<G> = \text{sat}(C)\), where \(C\) is the W-characteristic set of \(<G>\).

Obviously, the W-characteristic set \(C\) extracted from the Gröbner basis \(G\) is unique. The following proposition shows that if \(\text{sat}(C) = <G>\), then \(C\) must be regular and thus \((C, G)\) is an src pair. In other words, the Gröbner basis \(G\) in any src pair \((C, G)\) is characterizable. Otherwise, \(\text{sat}(C) \neq <G>\); in this case, \(G\) may not necessarily be determined by \(C\) (i.e., there may be two Gröbner bases \(G_1\) and \(G_2\) such that \(<G_1>\) and \(<G_2>\) have the same W-characteristic set \(C\)).

**Proposition 3.2** The W-characteristic set of the ideal generated by any characterizable Gröbner basis is regular.
Proof Let \( G \) be any characterizable Gröbner basis and \( C = [C_1, \ldots, C_r] \) be the W-characteristic set of \( \langle G \rangle \). For any \( P \in \text{sat}(C) \), we have \( P \in \langle G \rangle \) since \( \langle G \rangle = \text{sat}(C) \). From Proposition 2.4, (a) one can see that \( \text{prem}(P, C) = 0 \), which means that \( \text{sat}(C) \subseteq \{ P \in \mathbb{K}[x] \mid \text{prem}(P, C) = 0 \} \subseteq \text{sat}(C) \). Therefore, by [2] Thm. 6.1, \( C \) is regular.

**Lemma 3.3 (30, Lem. 6.2.6)** Let \( T \) be a regular set in \( \mathbb{K}[x] \). For any \( F \in \mathbb{K}[x] \), if \( \text{res}(F, T) \neq 0 \), then \( \text{sat}(T) : F^\infty = \text{sat}(T) \). 

**Lemma 3.4 (31, Lem. 2.4)** Let \( T = [T_1, \ldots, T_r] \subset \mathbb{K}[x] \) be a regular set with \( \text{lv}(T_i) < x_n \). Then \( T, P, G \) are polynomial with \( \text{lv}(P) = x_m > \text{lv}(T_i) \) and \( \text{deg}(P, x_m) = d \). Then \( \text{prem}(P, T) = 0 \) if and only if \( \text{prem}(P, T) = 0 \) for all \( i = 0, 1, \ldots, d \), \( k \in \mathbb{K}[x_1, \ldots, x_{k-1}] \). As \( x_k \notin \text{lv}(T) \), from Lemma 3.4 we know that \( \text{prem}(T_i, T) = 0 \) and thus \( G_i \in \text{sat}(T) \cap \mathbb{K}[x_1, \ldots, x_{k-1}] = \langle G \rangle \cap \mathbb{K}[x_1, \ldots, x_{k-1}] = \langle G^{(k-1)} \rangle \) for \( i = 0, 1, \ldots, d \). It follows that \( \text{ufnorm}(G_i, G^{(k-1)}) = 0 \), so that \( \text{ufnorm}(G, G^{(k-1)}) = 0 \), which contradicts with the fact that \( G \) is reduced with respect to \( G^{(k-1)} \). Therefore, \( \text{lv}(C) \subseteq \text{lv}(T) \). 

On the other hand, suppose that there exists an \( x_l \) \( (1 \leq l \leq n) \) such that \( x_l \notin \text{lv}(T) \), but \( x_l \notin \text{lv}(C) \). Let \( T \) be the polynomial in \( T \) such that \( \text{lv}(T) = x_l \); then \( T \) can be written as \( T = \text{ini}(T)x_l^p + R \) with \( \text{deg}(R, x_l) < p \). Since \( T \in \text{sat}(T) = \langle G \rangle \), \( \text{ufnorm}(T, G) = 0 \). Noting that \( x_l \notin \text{lv}(C) = \text{lv}(G) \), one can see that \( \text{ufnorm}(\text{ini}(T), G) = 0 \), so that \( \text{ini}(T) \in \langle G \rangle = \text{sat}(T) \). This contradicts with the fact that \( T \) is regular. Hence \( \text{lv}(T) = \text{lv}(C) \). 

Now we show that \( \text{deg}(T_i, x_p_i) = \text{deg}(C_i, x_p_i) \) for \( i = 1, \ldots, r \), where \( x_p_i = \text{lv}(T_i) = \text{lv}(C_i) \). Since \( C_i \in \langle G \rangle = \text{sat}(T) \) and \( T \) is regular, we have \( \text{prem}(C_i, T) = 0 \). Suppose that \( \text{deg}(C_i, x_p_i) \neq \text{deg}(T_i, x_p_i) \). Then \( \text{prem}(C_i, T_i) = C_i \) and thus \( \text{prem}(C_i, T) = \text{prem}(C_i, T_{i-1}) = 0 \). Write \( C_i = C_{id}x_p_i^d + \cdots + C_{0i} \) with \( d_i = \text{deg}(C_i, x_p_i) \) and \( C_{ij} \in \mathbb{K}[x_1, \ldots, x_{p_i-1}] \) for \( j = 0, \ldots, d_i \). From Lemma 3.4, we know that \( \text{prem}(C_{ij}, T) = 0 \), so that \( \text{ufnorm}(C_{ij}, G^{(p_i-1)}) = 0 \), which contradicts with the fact that \( G \) is a reduced Gröbner basis. Suppose that \( \text{deg}(C_i, x_p_i) > \text{deg}(T_i, x_p_i) \). One can easily see that \( T_i \in \langle G \rangle \) and \( T_i <_{\text{lex}} C_i \). This leads to contradiction with the minimality of \( C_i \). Therefore, \( \text{deg}(T_i, x_p_i) = \text{deg}(C_i, x_p_i) \) for \( i = 1, \ldots, r \). 

(b) Let \( D_i = \text{gcd}(C_i, T_i) \) for \( i = 1, \ldots, r \). Then there exist \( A_i, B_i \in \mathbb{K}[x] \) such that \( D_i = A_iC_i + B_iT_i \in \text{sat}(T_i) \subseteq \langle G \rangle \) since \( C_i, T_i \in \text{sat}(T_i) \). From \( D_i \mid C_i \), we know that \( D_i <_{\text{lex}} C_i \). If \( \text{deg}(D_i) \neq \text{deg}(C_i) \), then \( \text{ini}(C_i) \neq \text{ini}(C_i) \) and thus \( \text{ini}(C_i) \notin \text{sat}(T_i) \subseteq \langle G \rangle \), which is a contradiction. Otherwise, \( \text{lv}(D_i) = \text{lv}(C_i) \) and \( D_i \neq C_i \). This leads to contradiction with the minimality of \( C_i \). Therefore, we have \( D_i = C_i \) and thus \( C_i \mid T_i \). \( \square \)
Theorem 3.6 (Strengthening) Let $\mathcal{T} = [T_1, \ldots, T_r] \subseteq \mathbb{K}[\mathbf{x}]$ be a regular set, $\mathcal{G}$ be the Gröbner basis of $\text{sat}(\mathcal{T})$, and $\mathcal{C}$ be the W-characteristic set of $\langle \mathcal{G} \rangle$. Then $\mathcal{C}$ is regular and $\text{sat}(\mathcal{C}) = \text{sat}(\mathcal{T})$.

Proof We prove the theorem by induction on the number $r$ of polynomials in $\mathcal{T}$. The case $r = 1$ is trivial. Now we assume that the theorem is true for $r \leq k - 1$ and proceed to prove that $\mathcal{C}^{(k)}$ is regular and $\text{sat}(\mathcal{C}^{(k)}) = \text{sat}(\mathcal{T}^{(k)})$.

Suppose otherwise that $\mathcal{C}^{(k)}$ is not regular. We want to derive a contradiction. Let $I_i = \text{ini}(C_i)$ for $i = 1, \ldots, k$ and $J = I_1 \cdots I_k$. Since $\mathcal{C}^{(k-1)}$ is regular by induction, either $I_k \subseteq \text{sat}(\mathcal{C}^{(k-1)})$ or $Q I_k \subseteq \text{sat}(\mathcal{C}^{(k-1)})$ for some $Q \notin \text{sat}(\mathcal{C}^{(k-1)})$. Also by induction hypothesis, $\text{sat}(\mathcal{C}^{(k-1)}) = \text{sat}(\mathcal{T}^{(k-1)})$, and thus either $I_k \subseteq \text{sat}(\mathcal{T}^{(k-1)})$ or $Q I_k \subseteq \text{sat}(\mathcal{T}^{(k-1)})$. From Proposition 3.5 (b) we know that $C_k \mid T_k$, which implies $I_k \mid \text{ini}(T_k)$. It follows that either $\text{ini}(T_k) \subseteq \text{sat}(\mathcal{T}^{(k-1)})$ or $Q \text{ini}(T_k) \subseteq \text{sat}(\mathcal{T}^{(k-1)})$ for some $Q \notin \text{sat}(\mathcal{T}^{(k-1)})$, which contradicts with the fact that $\mathcal{T}$ is regular.

To prove that $\text{sat}(\mathcal{C}^{(k)}) = \text{sat}(\mathcal{T}^{(k)})$, we first prove that $\text{res}(J, \mathcal{T}^{(k)}) \neq 0$ by refutation. Suppose that $\text{res}(J, \mathcal{T}^{(k)}) = 0$. Then $I_k \subseteq \text{sat}(\mathcal{T}^{(k-1)})$ or $Q I_k \subseteq \text{sat}(\mathcal{T}^{(k-1)})$ for some $Q \notin \text{sat}(\mathcal{T}^{(k-1)})$. Recall the induction hypothesis $\text{sat}(\mathcal{C}^{(k-1)}) = \text{sat}(\mathcal{T}^{(k-1)})$. If $I_k \subseteq \text{sat}(\mathcal{T}^{(k-1)})$, then $I_k \subseteq \text{sat}(\mathcal{C}^{(k-1)});$ otherwise, $Q I_k \subseteq \text{sat}(\mathcal{C}^{(k-1)})$. Both cases contradict the above-proved conclusion that $\mathcal{C}^{(k)}$ is regular. It is thus proved that $\text{res}(J, \mathcal{T}^{(k)}) \neq 0$. Finally, by Lemma 3.3 we have

$$\text{sat}(\mathcal{C}^{(k)}) = \langle \mathcal{C}^{(k)} \rangle : J^\infty \subseteq \langle \mathcal{G}^{(k)} \rangle : J^\infty = \text{sat}(\mathcal{T}^{(k)}) : J^\infty = \text{sat}(\mathcal{T}^{(k)})$$

Obviously $\text{sat}(\mathcal{C}^{(k)})$ contains $\text{sat}(\mathcal{T}^{(k)})$, and the theorem is therefore proved. \qed

Remark 3.7 The proof of Theorem 3.6 above has used some of the techniques from the proof of [24, Thm. 4.4] which asserts that the W-characteristic set of the saturated ideal of a normal set is normal when the parameters are ordered smaller than the other variables.

Theorem 3.8 (Strong Regularization) Let $\mathcal{C}_i$ be the W-characteristic set of an arbitrary ideal $\mathfrak{I} \subseteq \mathbb{K}[\mathbf{x}]$, $\mathcal{G}_i$ be the Gröbner basis of $\text{sat}(\mathcal{C}_i-1)$, and $\mathcal{C}_i$ be the W-characteristic set of $\langle \mathcal{G}_i \rangle$ for $i \geq 2$. Then there exists an integer $m \geq 2$ such that $\mathfrak{I} \subseteq \text{sat}(\mathcal{C}_1) \subseteq \text{sat}(\mathcal{C}_m)$ and either $\mathcal{C}_m$ is a regular set, or $\text{sat}(\mathcal{C}_m) = \langle 1 \rangle$.

Proof From Proposition 2.6 (a) and $\text{sat}(\mathcal{C}_{i-1}) = \langle \mathcal{G}_i \rangle \subseteq \text{sat}(\mathcal{C}_i)$ we know that $\text{sat}(\mathcal{C}_i) \subseteq \text{sat}(\mathcal{C}_2) \subseteq \cdots \subseteq \text{sat}(\mathcal{C}_m) \subseteq \cdots$ for $i \geq 2$. Then by the Ascending Chain Condition there exists an $m \geq 2$ such that $\text{sat}(\mathcal{C}_{m-1}) = \text{sat}(\mathcal{C}_m) = \cdots$. It follows that the Gröbner basis $\mathcal{G}_m$ is characterizable unless $\text{sat}(\mathcal{C}_m) = \langle 1 \rangle$. Therefore, one sees from Proposition 3.2 that $\mathcal{C}_m$ is regular. \qed

The process of constructing the chain of W-characteristic sets $\mathcal{C}_i$ of $\mathfrak{I}_i = \langle \mathcal{G}_i \rangle$ for $i = 1, \ldots, m$ such that $\mathcal{C}_m$ is regular and $\text{sat}(\mathcal{C}_m) = \text{sat}(\mathcal{C}_{m-1})$ (called strong regularization) shown in Theorem 3.8 is depicted by the diagram in Figure II.
\[ \mathcal{J} = \mathcal{J}_1 = \langle \mathcal{G}_1 \rangle \rightarrow \mathcal{C}_1 \rightarrow \text{sat}(\mathcal{C}_1) \ (\neq \langle 1 \rangle) \]
\[ = \mathcal{J}_2 = \langle \mathcal{G}_2 \rangle \rightarrow \mathcal{C}_2 \rightarrow \text{sat}(\mathcal{C}_2) \ (\neq \langle 1 \rangle) \]
\[ \vdots \]
\[ = \mathcal{J}_{m-1} = \langle \mathcal{G}_{m-1} \rangle \rightarrow \mathcal{C}_{m-1} \rightarrow \text{sat}(\mathcal{C}_{m-1}) \ (\neq \langle 1 \rangle) \]
\[ = \mathcal{J}_m = \langle \mathcal{G}_m \rangle \rightarrow \mathcal{C}_m \rightarrow \text{sat}(\mathcal{C}_m) = \text{sat}(\mathcal{C}_{m+1}) = \ldots \]

Figure 1: Strong regularization of W-characteristic sets by means of saturation

From Theorem 3.6 we know that for any triangular set \( \mathcal{T} \), if \( \mathcal{T} \) is regular, then the W-characteristic set \( \mathcal{C} \) of \( \text{sat}(\mathcal{T}) \) is also regular and \( \text{sat}(\mathcal{T}) = \text{sat}(\mathcal{C}) \); thus \( (\mathcal{C}, \mathcal{G}) \) is an src pair. Theorem 3.6 corresponds in some way to the case of Theorem 3.8 when \( \mathcal{C}_1 \) is assumed to be regular; in this case \( \mathcal{C}_2 \) is always regular and thus \( m = 2 \). However, \( \mathcal{C}_2 \) is not necessarily regular (i.e., \( m \) may be greater than 2) when \( \mathcal{C}_1 \) is not regular, as shown by Example 3.10 (where \( m = 3 \)). The example also illustrates that Theorem 3.6 does not hold if \( \mathcal{T} \) is not assumed regular.

For any triangular set \( \mathcal{T} \), \( \text{sat}(\mathcal{T}) \) is said to be equiprojectable if there exists a regular set \( \mathcal{T} \) such that \( \text{sat}(\mathcal{T}) = \text{sat}(\mathcal{T}) \) [3]. The following corollary follows directly from Theorem 3.8.

**Corollary 3.9** For any triangular set \( \mathcal{T} \), \( \text{sat}(\mathcal{T}) \) is equiprojectable if and only if the W-characteristic set \( \mathcal{C} \) of \( \text{sat}(\mathcal{T}) \) is regular and \( \text{sat}(\mathcal{T}) = \text{sat}(\mathcal{C}) \).

Corollary 3.9 points out explicitly how to construct \( \mathcal{T} \) from \( \mathcal{T} \) and thus how to check whether \( \text{sat}(\mathcal{T}) \) is equiprojectable.

**Example 3.10** Let \( \mathcal{C}_1 = [x^2 - x, (y^2 - x)(y - 1), (y - 1)z] \subseteq \mathbb{K}[x, y, z] \) with \( x < y < z \). It is easy to verify that \( \mathcal{C}_1 \) is a Gröbner basis, it is a triangular set, and it is also the W-characteristic set of \( \mathcal{J} = \langle \mathcal{C}_1 \rangle \), but \( \mathcal{C}_1 \) is not regular. The Gröbner basis of the saturated ideal of \( \mathcal{C}_1 \) may be easily computed as \( \mathcal{G}_2 = \{ z, x(x-1), y^2 - x, x(y+1) \} \). The W-characteristic set of \( \langle \mathcal{G}_2 \rangle = \text{sat}(\mathcal{C}_1) \) is \( \mathcal{C}_2 = [x(x-1), x(y+1), z] \). Obviously \( \mathcal{C}_2 \) is not regular and thus \( \text{sat}(\mathcal{C}_1) \) is not equiprojectable, while the W-characteristic set \( \mathcal{C}_3 = [x - 1, y + 1, z] \) of \( \text{sat}(\mathcal{C}_2) \) is regular. Therefore, for this example the integer \( m \) in Theorem 3.8 is equal to 3.

Algorithm [1] can be used to compute an src pair from any polynomial ideal. The termination and correctness of this algorithm follow directly from Theorem 3.8.

**4 Strong regular characteristic decomposition**

In this section, we present an algorithm to compute strong regular characteristic decompositions of polynomial sets using Gröbner basis and ideal computations.

**4.1 Computing src pairs with ideal operations**

**Definition 4.1** Let \( \mathcal{J} \) be an ideal in \( \mathbb{K}[x] \) and \( \mathcal{C} \) be the W-characteristic set of \( \mathcal{J} \). \( \mathcal{C} \) is said to be **strong** if \( \text{sat}(\mathcal{C}) = \mathcal{J} \), or **morbid** if \( \mathcal{J} : \text{sat}(\mathcal{C}) = \mathcal{J} \).
Let \( \mathcal{C} \) be the W-characteristic set of an ideal \( \mathfrak{J} \subseteq \mathbb{K}[x] \). If \( \mathcal{C} \) is strong, then \( \mathcal{C} \) carries all the information of \( \mathfrak{J} \). If \( \mathcal{C} \) is morbid, then the associated primes of \( \mathfrak{J} \) are all properly contained in those of \( \text{sat}(\mathcal{C}) \); in this case the structure of \( \mathfrak{J} \) is so complicated that \( \mathcal{C} \) carries almost no information of \( \mathfrak{J} \).

**Proposition 4.2** Let \( \mathfrak{J} \) and \( \bar{\mathfrak{J}} \) be two ideals in \( \mathbb{K}[x] \) such that \( \mathfrak{J} \subseteq \bar{\mathfrak{J}} \). Then \( \sqrt{\mathfrak{J}} = \sqrt{\bar{\mathfrak{J}}} \cap \sqrt{\bar{\mathfrak{J}} : \mathfrak{J}} \).

**Proof** On one hand, for any polynomial \( P \in \mathfrak{J} \), we have \( P \in \mathfrak{J} \) and \( P \neq \bar{\mathfrak{J}} \) since \( \mathfrak{J} \subseteq \bar{\mathfrak{J}} \) and \( \mathfrak{J} \subseteq \mathfrak{J} : \bar{\mathfrak{J}} \). It follows that \( P \in \mathfrak{J} \cap \bar{\mathfrak{J}} : \mathfrak{J} \), which implies that \( \sqrt{\mathfrak{J}} \subseteq \sqrt{\mathfrak{J} : \bar{\mathfrak{J}}} \). On the other hand, for any polynomial \( P \in \sqrt{\bar{\mathfrak{J}}} \cap \sqrt{\mathfrak{J} : \bar{\mathfrak{J}}} \), we have \( P \in \sqrt{\mathfrak{J}} \) and \( P \in \sqrt{\mathfrak{J} : \bar{\mathfrak{J}}} \). As \( P \in \sqrt{\mathfrak{J}} \), there exists an \( m \) such that \( P^m \in \mathfrak{J} \); as \( P \) also belongs to \( \sqrt{\mathfrak{J} : \bar{\mathfrak{J}}} \), one can find an \( s \) such that \( P^s H \subseteq \mathfrak{J} \) for any polynomial \( H \in \mathfrak{J} \). Therefore, \( P^s P^m \in \mathfrak{J} \) and thus \( P \in \sqrt{\mathfrak{J}} \). Hence \( \sqrt{\mathfrak{J}} \cap \sqrt{\mathfrak{J} : \bar{\mathfrak{J}}} \subseteq \sqrt{\mathfrak{J}} \). \( \Box \)

Let \( \mathfrak{J} \) and \( \bar{\mathfrak{J}} \) be two ideals in \( \mathbb{K}[x] \) with \( \mathfrak{J} \subseteq \bar{\mathfrak{J}} \). Then by Proposition 4.2, \( \sqrt{\mathfrak{J}} = \sqrt{\bar{\mathfrak{J}}} \cap \sqrt{\bar{\mathfrak{J}} : \mathfrak{J}} \). If \( \sqrt{\mathfrak{J}} : \mathfrak{J} \neq \sqrt{\mathfrak{J}} \), then one can split \( \sqrt{\mathfrak{J}} \) as the intersection of \( \sqrt{\mathfrak{J}} \) and \( \sqrt{\mathfrak{J} : \mathfrak{J}} \) for further decomposition. In fact, one can always find a prime ideal \( \mathfrak{J} \) such that \( \sqrt{\mathfrak{J}} : \mathfrak{J} \neq \sqrt{\mathfrak{J}} \). As \( \sqrt{\mathfrak{J}} \) can be decomposed into finitely many prime ideals \( \mathfrak{J}_1, \ldots, \mathfrak{J}_s \) such that \( \sqrt{\mathfrak{J}} = \mathfrak{J}_1 \cap \cdots \cap \mathfrak{J}_s \), \( \mathfrak{J}_i \not\subseteq \mathfrak{J}_j \) for any \( i \neq j \). The decomposition is irredundant as no \( \mathfrak{J}_i \) can be removed from the intersection. Then any prime ideal \( \mathfrak{J} \) from the irredundant decomposition of \( \mathfrak{J} \) can be taken as \( \bar{\mathfrak{J}} \). The technique of splitting ideals by taking quotient according to Proposition 4.2 originates from the idea of dividing a known subvariety out of any given variety explained in [30, pp. 196–197].

### 4.2 A find-and-divide algorithm for src decomposition

In this subsection, we describe an algorithm to decompose any polynomial set (or the ideal it generates) into finitely many src pairs. Based on the strategy of splitting ideals by means of quotient, the algorithm works by finding an src pair and then dividing the saturated ideal of the W-characteristic set in the pair out of the original ideal iteratively.

Consider an ideal \( \mathfrak{J} \), initially with input \( \mathcal{F} \subseteq \mathbb{K}[x] \) as its generating set of polynomials. Let \( \Psi \) be the set of src pairs already computed; it is \( \emptyset \). Initially. First compute the Gröbner basis \( \mathcal{G} \) of \( \mathfrak{J} \) and extract the W-characteristic set \( \mathcal{C} \) of \( \mathfrak{J} \) from \( \mathcal{G} \). Then compute \( (\mathcal{C}, \mathcal{G}) := \text{srcPair}(\text{sat}(\mathcal{C})) \) with \( \mathcal{C} = [\mathcal{C}_1, \ldots, \mathcal{C}_r] \), \( I_i = \text{ini}(\mathcal{C}_i) \) for \( i = 1, \ldots, r \), and \( \mathfrak{J} = I_1 \cdots I_r \).

---

**Algorithm 1:** \( \Psi := \text{srcPair}(\mathfrak{J}) \) (for computing an src pair from a polynomial ideal)

**Input:** \( \mathfrak{J} \), an ideal in \( \mathbb{K}[x] \).

**Output:** \( (\mathcal{C}, \mathcal{G}) \), an src pair such that \( \mathfrak{J} \subseteq \text{sat}(\mathcal{C}) = \langle \mathcal{G} \rangle \), or \( ([1], [1]) \) otherwise.

\[
\begin{align*}
1 & \quad \mathcal{G} := \text{Gröbner basis of } \mathfrak{J}; \\
2 & \quad \text{if } \mathcal{G} \neq \{1\} \text{ then} \\
3 & \quad \quad \mathcal{C} := \text{W-characteristic set of } \langle \mathcal{G} \rangle; \\
4 & \quad \quad \text{while } \text{sat}(\mathcal{C}) \neq \langle \mathcal{G} \rangle \text{ do} \\
5 & \quad \quad \quad \quad \mathcal{G} := \text{Gröbner basis of } \text{sat}(\mathcal{C}); \\
6 & \quad \quad \quad \quad \text{if } \mathcal{G} = \{1\} \text{ then} \\
7 & \quad \quad \quad \quad \quad \quad \text{return } ([1], [1]); \\
8 & \quad \quad \quad \quad \text{else} \\
9 & \quad \quad \quad \quad \quad \quad \mathcal{C} := \text{W-characteristic set of } \langle \mathcal{G} \rangle; \\
10 & \quad \quad \text{return } ([1], [1]); \\
11 & \quad \text{return } (\mathcal{C}, \mathcal{G});
\end{align*}
\]
1. If $\mathcal{J} : \text{sat}(\mathcal{C}) \neq \mathcal{J}$, then $\mathcal{J}$ is decomposed into $\text{sat}(\mathcal{C})$ and $\mathcal{J} : \text{sat}(\mathcal{C})$; in this case, $(\mathcal{C}, \mathcal{G}) \neq ([1], \{1\})$ and an src pair is obtained and adjoined to $\Psi$. From Proposition 4.2 we know that
\[ \sqrt{\mathcal{J}} = \sqrt{\text{sat}(\mathcal{C})} \cap \sqrt{\mathcal{J} : \text{sat}(\mathcal{C})}, \] so the procedure can continue to decompose $\mathcal{J} : \text{sat}(\mathcal{C})$ instead of $\mathcal{J}$.

2. Otherwise, $\mathcal{J} : \text{sat}(\mathcal{C}) = \mathcal{J}$ and $\text{sat}(\mathcal{C}) \neq \mathcal{J}$ (because $\mathcal{J} \neq (1)$); in this case, one can find a polynomial $F \in \text{sat}(\mathcal{C})$ such that $F \notin \mathcal{J}$. Let $\mathcal{H}$ be the set of all the squarefree factors of $JF$ which are not in $\mathcal{J}$.

2.1. If $\mathcal{J} : \text{sat}(\mathcal{C}) \neq \mathcal{J}$, where $(\mathcal{C}, \mathcal{G}) \neq ([1], \{1\})$ is an src pair computed by Algorithm srcPair from $(\text{sat}(\mathcal{C}'))$ and $\mathcal{C}'$ is the W-characteristic set of $\langle G \cup \{H\} \rangle$ for some $H \in \mathcal{H}$, then $(\mathcal{C}, \mathcal{G})$ is adjoined to $\Psi$. Now (6) holds by Proposition 4.2 and the decomposition procedure continues with $\mathcal{J} : \text{sat}(\mathcal{C})$ instead of $\mathcal{J}$.

2.2. If there exists no such $H \in \mathcal{H}$, then let $\mathcal{J}$ be any prime ideal in the irredundant prime decomposition of $\sqrt{\mathcal{J}}$. Compute the Gröbner basis $\bar{\mathcal{G}}$ of $\mathcal{J}$ and extract the W-characteristic set $\bar{\mathcal{C}}$ of $\mathcal{J}$ from $\bar{\mathcal{G}}$. Then $\sqrt{\mathcal{J}} : \text{sat}(\mathcal{C}) \neq \mathcal{J}$ and $(\bar{\mathcal{C}}, \bar{\mathcal{G}}) \neq ([1], \{1\})$ is an src pair, so it is adjoined to $\Psi$. Again by Proposition 4.2
\[ \sqrt{\mathcal{J}} = \sqrt{\text{sat}(\mathcal{C})} \cap \sqrt{\mathcal{J} : \text{sat}(\mathcal{C})}. \] Then the decomposition continues with $\sqrt{\mathcal{J} : \mathcal{J}}$ instead of $\mathcal{J}$.

The above process of decomposition will terminate in finitely many iterations. We formulate the process as Algorithm [2]. The algorithm is practically effective because the case $\mathcal{J} : \text{sat}(\mathcal{C}) = \mathcal{J}$ does not occur often. In fact, we have never encountered an example for which step 2.2 is executed. This step is used undesirably as an alternative to make the algorithm complete as we are unable to ensure that step 2.1 always succeeds in producing an src pair.

**Proof (Proof of Termination and Correctness of Algorithm [2])**

(Termination) Every time after the ideal $\mathcal{J}$ is decomposed, a new ideal $\mathcal{J}'$ is obtained and then further decomposed in the same way, so decomposition in Algorithm [2] is an iterative process. Obviously every new ideal generated in Lines 9, 17, and 20 is strictly enlarged. Thus by the Ascending Chain Condition, Algorithm [2] terminates.

(Correctness) When $\langle F \rangle = (1)$ in Line 4 $\Psi = \emptyset$ is returned. Hence we only need to show that when $\langle F \rangle \neq (1)$, $\Psi$ is an src decomposition of $F$, namely all the pairs in $\Psi$ are src pairs and the relation (3) holds. It is clear that only in Lines 8, 16, or 25 is an src pair ($\bar{\mathcal{C}}, \bar{\mathcal{G}}$) is generated and adjoined to $\Psi$, namely all the pairs in $\Psi$ are src pairs and the relation (3) holds. It is also easy to see that the pairs ($\bar{\mathcal{C}}, \bar{\mathcal{G}}$) generated in Lines 8 and 16 are src pairs as well since $(\bar{\mathcal{C}}, \bar{\mathcal{G}}) \neq ([1], \{1\})$. For those pairs generated in Line 25 since $\mathcal{J}$ is a prime ideal, there exists an irreducible triangular set $\mathcal{T}$ such that $\mathcal{J} = \text{sat}(\mathcal{T})$ and thus $\bar{\mathcal{C}}$ is the W-characteristic set of $\mathcal{T}$. As $\mathcal{T}$ is also regular, we know from Theorem 3.6 that $\bar{\mathcal{C}}$ is regular and sat($\mathcal{C}$) = sat($\mathcal{T}$) = $\mathcal{J}$ = ($\bar{\mathcal{G}}$). Therefore, each element in $\Psi$ is an src pair.

Now we prove that $\sqrt{\langle F \rangle} = \sqrt{\mathcal{C} \in \Psi \sqrt{\text{sat}(\mathcal{C})}}$ by considering all the src pairs generated in Lines 8, 16, and 25. For those src pairs generated in Line 8, one can easily see that $\mathcal{J} \subseteq \text{sat}(\mathcal{C})$, and in Line 16 we have $\mathcal{J} \subseteq \langle G \cup \{H\} \rangle \subseteq \text{sat}(\mathcal{C'}) \subseteq \text{sat}(\mathcal{C})$ for any $H \in \mathcal{H}$ since $\mathcal{C}'$ is the W-characteristic set of $\langle G \cup \{H\} \rangle$; thus from Proposition 4.2 we know that the relation (6) holds. For those src pairs in Line 25, as $\mathcal{J}$ is an irredundant associated prime ideal of $\mathcal{J}$, again by Proposition 4.2 the relation (7) holds.
Algorithm 2: \( \Psi := \text{srcDec}(\mathcal{F}) \) (for an src decomposition of a polynomial set)

\[ \text{Input: } \mathcal{F}, \text{ a finite, nonempty set of polynomials in } \mathbb{K}[x]. \]
\[ \text{Output: } \Psi, \text{ an src decomposition of } \mathcal{F} \text{ such that } \sqrt{\langle \mathcal{F} \rangle} = \bigcap_{\mathcal{C} \subseteq \Psi} \sqrt{\text{sat}(\mathcal{C})} = \bigcap_{\mathcal{G} \subseteq \Psi} \sqrt{\langle \mathcal{G} \rangle}. \]

1. \( \Psi := \emptyset; \)
2. \( \mathcal{J} := \langle \mathcal{F} \rangle; \)
3. \( \mathcal{G} := \text{Gröbner basis of } \mathcal{J}; \)
4. \( \text{while } \mathcal{G} \neq [1] \text{ do} \)
5. \( \mathcal{C} := \text{W-characteristic set of } \langle \mathcal{G} \rangle; \)
6. \( (\bar{\mathcal{C}}, \bar{\mathcal{G}}) := \text{srcPair}(\text{sat}(\mathcal{C})); \)
7. \( \text{if } \mathcal{J} : \text{sat}(\bar{\mathcal{C}}) \neq \mathcal{J} \text{ then} \)
8. \( \Psi := \Psi \cup \{(\bar{\mathcal{C}}, \bar{\mathcal{G}})\}; \)
9. \( \mathcal{J} := \mathcal{J} : \text{sat}(\bar{\mathcal{C}}); \)
10. \( \text{else} \)
11. \( \mathcal{H} := \{ H \in \mathbb{K}[x] | H \notin \mathcal{J}, H \not\in \mathcal{J} : QJ \text{ and } Q \in \mathcal{Q} \}; \)
12. \( \text{for } H \in \mathcal{H} \text{ do} \)
13. \( (\bar{\mathcal{C}}', \bar{\mathcal{G}}) := \text{srcPair}(\text{sat}(\bar{\mathcal{C}}')); \)
14. \( \text{if } \mathcal{J} : \text{sat}(\bar{\mathcal{C}}') \neq \mathcal{J} \text{ then} \)
15. \( \Psi := \Psi \cup \{(\bar{\mathcal{C}}, \bar{\mathcal{G}})\}; \)
16. \( \mathcal{J} := \mathcal{J} : \text{sat}(\bar{\mathcal{C}}'); \)
17. \( \text{break; } \)
18. \( \text{else} \)
19. \( \mathcal{H} := \mathcal{H} \setminus \{H\}; \)
20. \( \text{if } \mathcal{H} = \emptyset \text{ then} \)
21. \( \text{Take a prime ideal } \mathcal{J} \text{ from the irredundant prime decomposition of } \sqrt{\mathcal{J}}; \)
22. \( \mathcal{G} := \text{Gröbner basis of } \mathcal{J}; \)
23. \( \mathcal{C} := \text{W-characteristic set of } \langle \mathcal{G} \rangle; \)
24. \( \Psi := \Psi \cup \{(\bar{\mathcal{C}}, \bar{\mathcal{G}})\}; \)
25. \( \mathcal{J} := \sqrt{\mathcal{J}} : \mathcal{J}; \)
26. \( \mathcal{G} := \text{Gröbner basis of } \mathcal{J}; \)
27. \( \text{return } \Psi \)

The relations (6) and (7) imply that every polynomial \( F \in \sqrt{\mathcal{J}} \) is in the intersection of \( \sqrt{\text{sat}(\bar{\mathcal{C}})} \) and \( \sqrt{\mathcal{J}'} \), where \( \mathcal{J}' \) is a new ideal obtained which remains for further processing. This proves that the relation \( \sqrt{\mathcal{F}} = \bigcap_{\mathcal{C} \subseteq \Psi} \sqrt{\text{sat}(\mathcal{C})} \) holds when Algorithm 2 terminates with \( \mathcal{J}' = \langle 1 \rangle \). Since for every src pair \( (\mathcal{C}, \mathcal{G}) \in \Psi \), we have \( \langle \mathcal{G} \rangle = \text{sat}(\mathcal{C}) \); therefore \( \sqrt{\mathcal{F}} = \bigcap_{\mathcal{G} \subseteq \Psi} \sqrt{\langle \mathcal{G} \rangle} \). This completes the proof of the relation (3). \( \square \)

5 Examples and experiments

5.1 Examples for src decomposition

Example 5.1 Let \( \mathcal{F} = \{uxy, vy^2 + y, vx^2 + y^2 \} \subseteq \mathbb{K}[u, v, x, y] \) with \( u < v < x < y \). The Gröbner basis of \( \mathcal{J}_1 = \langle \mathcal{F} \rangle \) can be easily computed as
\[ \mathcal{G}_1 = \{ux^2, v^2x^4 + vx^2, y - y^2x^2 \} \]
and the W-characteristic set of \( \langle \mathcal{G}_1 \rangle \) is \( \mathcal{C}_1 = \{ux^2, y - y^2x^2 \} \). The saturated ideal of \( \mathcal{C}_1 \) is \( \text{sat}(\mathcal{C}_1) = \langle x^2, y \rangle \). One sees that \( \mathcal{C}_1 \) is regular, so that \( (\bar{\mathcal{C}}_1, \bar{\mathcal{G}}_1) \) is an src pair, where
\[ G_1 = \{x^2, y\} \] is the Gröbner basis and \( \tilde{C}_1 = [x^2, y] \) is the W-characteristic set of \( \text{sat}(C_1) \). It is easy to verify that

\[ \mathcal{I}_1 : \text{sat}(\tilde{C}_1) = \langle uw, vy, v^2 + y, v^2 y + v, y^4 - vy^2, y^2 + vy^2 \rangle \]

is strictly larger than \( \mathcal{I}_1 \); hence \( (\tilde{C}_1, \tilde{G}_1) \) is adjoined to \( \Psi \) and the procedure continues to decompose \( \mathcal{I}_2 = \mathcal{I}_1 : \text{sat}(\tilde{C}_1) \) instead of \( \mathcal{I}_1 \). The Gröbner basis of \( \mathcal{I}_2 \) and the W-characteristic set of \( \langle G_2 \rangle \) consist of the same polynomials:

\[ G_2 = \{uw, vP, Q\}, \quad C_2 = [uw, vP, Q], \]

where \( P = v^3 x^2 + 1 \) and \( Q = y - x v^2 \). Since \( \text{sat}(C_2) = \langle 1 \rangle \), the pair \( \{[1], \{1\}\} \) is obtained and \( \mathcal{I}_2 : \{1\} = \mathcal{J}_2 \). Now we need to consider the set \( \mathcal{H} \), which can be easily determined as \( \mathcal{H} = \{u, v\} \). Choose \( v \in \mathcal{H} \), compute the Gröbner basis \( G_3 = [v, y] \) of \( \langle G_2 \cup \{v\} \rangle \), and extract the W-characteristic set \( C_3 = [v, y] \) of \( \langle G_3 \rangle \); one finds that \( C_3 \) is regular and \( \text{sat}(C_3) = \langle v, y \rangle = \langle G_3 \rangle \) and \( \mathcal{J}_2 : \text{sat}(C_3) = \langle u, P, Q \rangle \) is strictly larger than \( \mathcal{I}_2 \). Then the src pair \( (C_3, G_3) \) is obtained and adjoined to \( \Psi \). The procedure continues with \( \mathcal{I}_3 = \langle u, P, Q \rangle \).

Simple computation shows that the Gröbner basis and the W-characteristic set of \( \mathcal{I}_3 \) contain the same polynomials:

\[ G_4 = \{u, P, Q\}, \quad C_4 = [u, P, Q]. \]

One can check that \( (C_4, G_4) \) is an src pair and \( \mathcal{J}_3 : \text{sat}(C_4) = \langle 1 \rangle \). Therefore, \( (C_4, G_4) \) is added to \( \Psi \) and the procedure terminates. Finally, an src decomposition

\[ \Psi = \{(\tilde{C}_1, \tilde{G}_1), (C_3, G_3), (C_4, G_4)\} \]

of \( F \) is obtained.

**Example 5.2** Consider the polynomial set

\[ F = \{-ct^2u + t^3 - uv^2 - wu^2, -ct^2v + t^3 - u^2v - vu^2, -ct^2w + t^3 - u^2w - v^2w\} \]

(which is Ex 9 in Table 1) with variable ordering \( w < v < u < t < c \). The ideal generated by \( F \), which is of dimension 2 and not radical, consists of 8 primary components (none of them is embedded). The polynomial set \( F \) can be decomposed by Algorithm 2 into 6 src pairs

\[ (C_1, G_1) = ([v, u, t], \{v, u, t\}), \quad (C_2, G_2) = ([w, u, t^2], \{w, u, t^2\}), \quad (C_3, G_3) = ([w, v, t^2], \{w, v, t^2\}), \]  
\[ (C_4, G_4) = ([v - w, u - w, wt^2c - t^3 + 2w^3], \{v - w, u - w, wt^2c - t^3 + 2w^3\}), \]  
\[ (C_5, G_5) = ([v - w, P, Q], \{v - w, P, Q, t^2c - wu + w^2\}), \]  
\[ (C_6, G_6) = ([G_1, G_2, G_3], \{G_1, \ldots, G_5\}) \]

where the polynomials \( G_1, \ldots, G_5 \) consist of 6, 3, 4, 10, 3 terms respectively and

\[ P = t^3 - wu^2 - w^2u, \quad Q = u^2c + wuc - ut - wt. \]

It may be observed that \( (1) \) \( C_i \) is normal for all \( i \), \( (2) \) \( \sqrt{\langle G_i \rangle} \) is prime for \( i = 1, \ldots, 5 \), and \( (3) \) \( \sqrt{\langle G_6 \rangle} \) is composed of 3 prime ideals.

The cyclic-\( n \) systems are well-known examples for which triangular decompositions based on pseudo-division are more difficult to compute than Gröbner bases. Our algorithm can compute src pairs for cyclic-6 in a few minutes, while other triangular decomposition algorithms cannot (see Ex 21 in Table 1).
5.2 Implementation and experimental results

We have implemented Algorithm 2 as a Maple function srcDec and carried out experiments with the implementation on an Intel(R) Core(TM) i5-4210U CPU at 1.70 GHz × 4 with 7.7 GB RAM under Ubuntu 16.04 LTS. The implementation is based on the functions for Gröbner basis computation available in the FGb library and Maple’s built-in packages. Selected results of experiments on some test examples are presented in Table 1. Ex 1–4 are taken from the Epsilon library, Ex 5–9 from [26], Ex 10 from [8], Ex 11 from the FGb library, Ex 12–16 can be found at http://www.lifl.fr/~lemaire/BCLM09/BCLM09-systems.txt, and Ex 17–21 can be found at http://homepages.math.uic.edu/~jan/Demo/TITLES.html.

The function srcDec is implemented for direct decomposition of polynomial sets into src pairs. To observe the performance of our algorithm, we made comparative experiments on srcDec in Maple 18 with two other relevant functions for unmixed decomposition of polynomial sets into Gröbner bases of saturated ideals of triangular sets: one is the Epsilon function uvd which is implemented for decomposing an arbitrary algebraic variety into unmixed subvarieties. The other function computes first the decomposition of a polynomial set into regular sets using the RegularChains function Triangularize and then the Gröbner bases of the saturated ideals of the computed regular sets.

In Table 1, Label indicates the label used in the above-cited references and Var, Pol, and Dim denote the number of variables, the number of polynomials in the example, and the dimension of the ideal generated by the polynomials, respectively. Total, GB, SAT, and QUO under Algorithm 2 record respectively the total time (followed by the number of src pairs in parenthesis) for src decomposition using Algorithm 2 the time for computing all the Gröbner bases, saturated ideals, and ideal quotients; Total under uvd records the total time for unmixed decomposition. Total and Regular under Triangularize record the total time for unmixed decomposition (followed by the number of components in parenthesis) and the time for regular decomposition respectively.

Table 1: Timings for src decomposition (in second)

| Ex | Label | Var | Pol | Dim | Total (GB SAT QUO) | Algorithm 2 Total (GB SAT QUO) | uvd Total | Triangularize Total (Regular) |
|----|-------|-----|-----|-----|-------------------|--------------------------------|-----------|-------------------------------|
| 1  | E1    | 10  | 10  | 1   | 3.901(2) 0.480 0.221 3.189 | 0.867(3) 0.241(13) | 1.709     |
| 2  | E5    | 15  | 17  | 4   | 74.554(1) 0.039 0.466 74.035 | 3.374(1) | 7.684(7) 5.225 |
| 3  | E11   | 4   | 3   | 1   | 0.037(1) 0.008 0.008 0.015 | 0.122(1) | 0.079(3) 0.035 |
| 4  | E34   | 14  | 16  | 0   | 0.574(0) 0.556 0. 0. | > 1000 | 50.650(0) 50.649 |
| 5  | S1    | 4   | 3   | 2   | 0.055(2) 0.017 0.007 0.022 | 0.011(3) | 0.054(3) 0.034 |
| 6  | S6    | 4   | 3   | 2   | 0.175(3) 0.035 0.018 0.111 | 0.032(3) | 0.080(3) 0.052 |
| 7  | S7    | 4   | 3   | 1   | 0.089(1) 0.008 0.052 0.031 | 0.052(1) | 0.127(1) 0.084 |
| 8  | S8    | 4   | 3   | 2   | 0.058(2) 0.018 0.004 0.030 | 0.112(2) | 0.099(2) 0.081 |
| 9  | S14   | 5   | 3   | 2   | 1.024(6) 0.372 0.299 0.235 | 3.767(6) | 0.184(8) 0.109 |
| 10 | nueral | 4   | 3   | 1   | 1.225(2) 0.445 0.187 0.574 | > 1000 | 0.222(5) 0.115 |
| 11 | F663  | 10  | 9   | 2   | 21.976(1) 1.208 1.539 19.198 | > 1000 | 4.312(4) 0.935 |
| 12 | Katsura-4 | 5  | 5   | 0   | 0.333(1) 0.254 0.086 0.001 | 0.006(1) | 6.583(4) 5.343 |
| 13 | nld-3-4 | 4   | 4   | 0   | 2.037(8) 0.175 0.624 1.121 | 1.066(8) | 0.754(29) 0.520 |
| 14 | nld-8-3 | 3   | 3   | 0   | 2.464(2) 2.254 0.207 0.70 | 3.334(2) | 17.360(8) 0.268 |
| 15 | nql-5-4 | 5   | 5   | 0   | 2.908(1) 2.088 0.0.06 0.086 | 25.422(1) | 35.508(1) 30.335 |
| 16 | caprasse-li | 4  | 4   | 0   | 104.055(2) 0.066 101.836 2.145 | 2.883(3) | 0.967(7) 0.634 |
| 17 | Cyclic-5 | 5   | 5   | 0   | 6.139(4) 0.052 0.046 0.015 | > 1000 | 1.079(15) 0.798 |
| 18 | geneig | 6   | 6   | 0   | 0.566(1) 0.135 0.003 0.417 | > 1000 | – 0.00 |
| 19 | reimer5 | 5   | 5   | 0   | 32.850(1) 30.983 0.005 1.820 | > 1000 | – > 1000 |
| 20 | redcyc6 | 6   | 6   | 0   | 36.920(6) 2.039 0.556 35.079 | > 1000 | – > 4000 |
| 21 | Cyclic-6 | 6   | 6   | 0   | 368.988(6) 2.455 332.158 33.780 | > 1000 | – > 1000 |

The most time-consuming steps in algorithm srcDec are for the computation of lex Gröbner bases of the input ideals and the Gröbner bases of ideal quotients, while the computation of the Gröbner bases of saturated ideals is not very expensive for most examples, as one can see from Table 1. The reason behind is that regular sets computed
by our algorithm are normal in most cases and they usually have smaller sizes than the corresponding regular sets computed by pseudo-division or subresultant-based algorithms, so that the Gröbner bases of the saturated ideals of the regular sets produced by our algorithm tend to be easier to compute than those produced by uvd or Triangularize. More importantly, the number of src pairs in an src decomposition computed by srcDec is usually smaller than the number of components in the corresponding unmixed decomposition computed by uvd or regular decomposition by Triangularize, as shown by the experimental data in Table 1. This is because our find-and-divide algorithm using ideal quotient generates few redundant components. For example, the computation of the src decomposition using srcDec takes much less time than that of the regular decomposition using Triangularize for Ex 14, as the src decomposition contains only two src pairs.

6 Conclusion

In this paper, it is shown that a strong regular characteristic (src) pair \((C, G)\) can be constructed from any polynomial ideal \(I\) with given generating set \(F\) such that \(I \subseteq \text{sat}(C)\). The constructed src pair may be used to split the radical ideal of \(I\) into the radicals of the saturated ideal \(\text{sat}(C)\) and the quotient ideal \(I : \text{sat}(C)\). The process of construction and splitting can be repeated for \(I : \text{sat}(C)\) instead of \(I\) and recursively, yielding an algorithm capable of decomposing the polynomial set \(F\) into finitely many src pairs \((C_1, G_1)\), \ldots, \((C_e, G_e)\) such that

\[
Z(F) = \bigcup_{i=1}^{e} Z(G_i) = \bigcup_{i=1}^{e} Z(\text{sat}(C_i))
\]

or equivalently (3) holds. The relation (8) provides two representations for the zero set of \(F\): one in terms of the Gröbner bases \(G_1, \ldots, G_e\) and the other in terms of the regular sets \(C_1, \ldots, C_e\). Several nice properties about strong regular characteristic pairs and characteristic decompositions have been presented, and the implementation and performance of our proposed algorithm have been illustrated by examples and experimental results.

The main contributions of this paper include: (1) two main theorems (Theorems 3.6 and 3.8) showing how to form an src pair \((C, G)\) such that \(\text{sat}(T) = \text{sat}(C)\) for any regular set \(T\) and how to construct an src pair \((C, G)\) such that \(I \subseteq \text{sat}(C)\) from an arbitrary ideal \(I\); (2) an algorithm for decomposing any polynomial set \(F\) into src pairs \((C_i, G_i)\) such that (3) and (8) hold; (3) some experiments with a preliminary implementation of the decomposition algorithm.

The triangular sets in an src decomposition are normal in most cases (cf. [32, 31]). It turns out that comprehensive triangular decompositions [8] and/or Gröbner systems [23] can be reproduced rather easily from src sets computed by our algorithm, and we are working on the details. The W-characteristic set of an ideal may be morbid. How to establish equivalent conditions for a W-characteristic set to be morbid and how to retrieve information of an ideal from its morbid W-characteristic set are among the questions that remain for further investigation.

References

[1] P. Alvandi, C. Chen, S. Marcus, M. Moreno Maza, É. Schost, and P. Vrbik. Doing algebraic geometry with the RegularChains library. In H. Hong and C. K. Yap, editors, Proceedings of ICMS 2014, pages 472–479. Springer-Verlag, Berlin Heidelberg, 2014.
[2] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, 28(1–2):105–124, 1999.

[3] P. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *Journal of Symbolic Computation*, 30(6):635–651, 2000.

[4] T. Becker, V. Weispfenning, and H. Kredel. *Gröbner Bases: A Computational Approach to Commutative Algebra*. Graduate Texts in Mathematics. Springer, New York, 1993.

[5] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenring nach einem nulldimensionalen Polynomideal*. PhD thesis, Universität Innsbruck, Austria, 1965.

[6] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N. Bose, editor, *Multidimensional Systems Theory*, pages 184–232. Springer, Dordrecht, 1985.

[7] T. Becker, V. Gerdt, M. Lange-Hegermann, and D. Robertz. Algorithmic Thomas decomposition of algebraic and differential systems. *Journal of Symbolic Computation*, 47(10):1233–1266, 2012.

[8] C. Chen, O. Golubitsky, F. Lemaire, M. Moreno Maza, and W. Pan. Comprehensive triangular decomposition. In V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov, editors, *Proceedings of CASC 2007*, pages 73–101. Springer-Verlag, Berlin Heidelberg, 2007.

[9] C. Chen and M. Moreno Maza. Algorithms for computing triangular decompositions of polynomial systems. *Journal of Symbolic Computation*, 47(6):610–642, 2012.

[10] D. Cox, J. Little, and D. O’Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer, New York, 1997.

[11] D. Cox, J. Little, and D. O’Shea. *Using Algebraic Geometry*. Graduate Texts in Mathematics. Springer, New York, 1998.

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

[13] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[14] S. Gao, F. Volny, and M. Wang. A new framework for computing Gröbner bases. *Mathematics of Computation*, 85(297):449–465, 2016.

[15] X.-S. Gao and S.-C. Chou. On the dimension of an arbitrary ascending chain. *Chinese Science Bulletin*, 38(10):799–799, 1993.

[16] M. Kalkbrener. *Three Contributions to Elimination Theory*. PhD thesis, Johannes Kepler University, Austria, 1991.

[17] M. Kalkbrener. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *Journal of Symbolic Computation*, 15(2):143–167, 1993.
[18] D. Lazard. Ideal bases and primary decomposition: Case of two variables. *Journal of Symbolic Computation*, 1(3):261–270, 1985.

[19] D. Lazard. Solving zero-dimensional algebraic systems. *Journal of Symbolic Computation*, 13(2):117–131, 1992.

[20] B. Li and D.-K. Wang. An algorithm for transforming regular chain into normal chain. In D. Kapur, editor, *Proceedings of ASCM 2007*, pages 236–245. Springer-Verlag, Berlin Heidelberg, 2008.

[21] X. Li, C. Mou, and D. Wang. Decomposing polynomial sets into simple sets over finite fields: The zero-dimensional case. *Computers and Mathematics with Applications*, 60(11):2983–2997, 2010.

[22] M. G. Marinari and T. Mora. A remark on a remark by Macaulay or enhancing Lazard structural theorem. *Bulletin of the Iranian Mathematical Society*, 29(1):1–45, 2003.

[23] A. Montes. A new algorithm for discussing Gröbner bases with parameters. *Journal of Symbolic Computation*, 33(2):183–208, 2002.

[24] M. Moreno Maza. On triangular decompositions of algebraic varieties. Technical Report 4/99, NAG, UK, 2000. Presented at the MEGA-2000 Conference, Bath, UK.

[25] C. Mou and D. Wang. Characteristic decomposition: From regular sets to normal sets. *Journal of Systems Science and Complexity*, 32(1):37–46, 2019.

[26] C. Mou, D. Wang, and X. Li. Decomposing polynomial sets into simple sets over finite fields: The positive-dimensional case. *Theoretical Computer Science*, 468:102–113, 2013.

[27] J. F. Ritt. *Differential Algebra*. American Mathematical Society, New York, 1950.

[28] T. Shimoyama and K. Yokoyama. Localization and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 22(3):247–277, 1996.

[29] D. Wang. Computing triangular systems and regular systems. *Journal of Symbolic Computation*, 30(2):221–236, 2000.

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

[31] D. Wang. On the connection between Ritt characteristic sets and Buchberger-Gröbner bases. *Mathematics in Computer Science*, 10:479–492, 2016.

[32] D. Wang, R. Dong, and C. Mou. Decomposition of polynomial sets into characteristic pairs. Preprint at arXiv:1702.08664, 2017.

[33] W.-T. Wu. Basic principles of mechanical theorem proving in elementary geometries. *Journal of Automated Reasoning*, 2(3):221–252, 1986.
A Appendix

A.1 Strong regular characteristic decomposition of radical ideals

Recall that an ideal $\mathfrak{J} \subset \mathbb{K}[x]$ is prime if for any $F, G \in \mathbb{K}[x]$, $FG \in \mathfrak{J}$ implies that either $F \in \mathfrak{J}$, or $G \in \mathfrak{J}$ [10, Def. 6.2]. Two ideals $a$ and $b$ are said to be coprime if $a + b = \langle 1 \rangle$. Clearly, $a$ and $b$ are coprime if and only if there exist $x \in a$ and $y \in b$ such that $x + y = 1$.

**Lemma A.1** Let $\mathfrak{J}$ and $\mathfrak{J}'$ be two ideals in $\mathbb{K}[x]$. Then $\sqrt{\mathfrak{J}} : \sqrt{\mathfrak{J}}$ and $\sqrt{\mathfrak{J}}$ are coprime.

**Proof** Since $\sqrt{\mathfrak{J}}$ is radical, there exists a squarefree polynomial $P \in \sqrt{\mathfrak{J}} \subseteq \sqrt{\mathfrak{J}} : \sqrt{\mathfrak{J}}$. Suppose that $\sqrt{\mathfrak{J}} = \langle J_1, \ldots, J_t \rangle$ and let $H = \gcd(J_1, \ldots, J_t)$ and $H' = \gcd(P, H)$. Then there exist polynomials $Q_1, \ldots, Q_t, F, G \in \mathbb{K}[x]$ such that $Q_1J_1 + \cdots + Q_tJ_t = H \in \sqrt{\mathfrak{J}}$, and $H' = FP + GH$. Therefore, $FP + GQ_1J_1 + \cdots + GQ_tJ_t = H'$. Let $J \in \sqrt{\mathfrak{J}}$; then $H' | J$. Obviously, $\frac{P}{H' J} = PJ \in \sqrt{\mathfrak{J}}$. It follows that $(\frac{P}{H'})^2 \in \sqrt{\mathfrak{J}}$, so that $\frac{P}{H'} J \in \sqrt{\mathfrak{J}}$, which means $\frac{P}{H'} \in \sqrt{\mathfrak{J}} : \sqrt{\mathfrak{J}}$. Since $P$ is squarefree and $H' = \gcd(P, H)$, we have $\gcd(\frac{P}{H'}, H) = 1$. Hence $\sqrt{\mathfrak{J}} : \sqrt{\mathfrak{J}}$ and $\sqrt{\mathfrak{J}}$ are coprime. □

**Proposition A.2** Let $\mathfrak{J}$ and $\mathfrak{J}'$ be two radical ideals in $\mathbb{K}[x]$. Then:

(a) the saturated ideal of the W-characteristic of $\mathfrak{J}$ is radical;

(b) the ideal quotient $\mathfrak{J} : \mathfrak{J}'$ is also radical.

**Proof** (a) Let $\mathcal{T}$ be the W-characteristic set of $\mathfrak{J}$. To show that sat($\mathcal{T}$) is radical, it suffices to show that sat($\mathcal{T}$) is radical. The inclusion sat($\mathcal{T}$) $\subseteq$ sat($\mathcal{T}$) is obvious. For any $P \in \sqrt{\text{sat}(\mathcal{T})}$, we have $P^n I^n \in \langle \mathcal{T} \rangle \subseteq \mathfrak{J}$ for some nonnegative integers $m$ and $n$, where $I = \prod_{T \in \mathcal{T}} \text{ini}(T)$. Thus $(IP)^{\text{max}(m, n)} \in \mathfrak{J}$; it follows that $IP \in \sqrt{\mathfrak{J}} = \mathfrak{J}$, so that prem($IP, \mathcal{T}$) = 0, which means that $P \in \text{sat}(\mathcal{T})$. Therefore, sat($\mathcal{T}$) $\subseteq$ sat($\mathcal{T}$).

(b) To prove that $\mathfrak{J} : \mathfrak{J}'$ is radical, we only need to prove that $\sqrt{\mathfrak{J} : \mathfrak{J}'} \subseteq \mathfrak{J} : \mathfrak{J}'$. For any $F \in \sqrt{\mathfrak{J} : \mathfrak{J}'}$ and $J \in \mathfrak{J}'$, there exists a nonnegative integer $n$ such that $F^n J \in \mathfrak{J}'$; it follows that $(FJ)^n \in \mathfrak{J}'$, so that $FJ \in \sqrt{\mathfrak{J} : \mathfrak{J}'}$. Hence $FJ \in \sqrt{\mathfrak{J}} = \mathfrak{J}$. □

By Proposition [A.2], for any radical ideal $\mathfrak{J}$, the saturated ideal sat($\mathcal{C}$) of every regular set $\mathcal{C}$ appearing in the src decomposition $\Psi$ of $\mathfrak{J}$ is radical. According to Lemma [A.1] for any two src pairs $(\mathcal{C}_i, \mathcal{G}_i)$ and $(\mathcal{C}_j, \mathcal{G}_j)$ ($i \neq j$) in $\Psi$, sat($\mathcal{C}_i$) and sat($\mathcal{C}_j$) are coprime and none of them is redundant. This means that the two varieties $Z(\text{sat}(\mathcal{C}_i))$ and $Z(\text{sat}(\mathcal{C}_j))$ are disjoint in the sense that they do not have any irredundant common subvariety. Therefore, the number of src pairs in $\Psi$ must be smaller than the number of irredundant irreducible components of the variety $Z(F)$. We are unable to establish this bounding property for non-radical ideals because when $\mathfrak{J}$ and $\mathfrak{J}'$ in Lemma [A.1] are not radical, $\mathfrak{J} : \mathfrak{J}'$ and $\mathfrak{J}$ are not necessarily coprime. Taking $\mathfrak{J} = \langle x^3 y \rangle$ and $\mathfrak{J}' = \langle x \rangle$ as an example, we have $\mathfrak{J} : \mathfrak{J}' = \langle x^2 y \rangle$, which has the same zero set as $\mathfrak{J}'$.

A.2 Triangular decomposition and characteristic decomposition

Let $\mathfrak{J} \subset \mathbb{K}[x]$ be a polynomial ideal with generating set $\mathcal{F}$ and $\Psi = \{(\mathcal{C}_1, \mathcal{G}_1), \ldots, (\mathcal{C}_e, \mathcal{G}_e)\}$ be an src decomposition of $\mathcal{F}$ computed by Algorithm [2]. Then $\{\mathcal{C}_1, \ldots, \mathcal{C}_e\}$ is a regular triangular decomposition of $\mathcal{F}$ obtained from $\Psi$ with no further computation. Therefore, the decomposition $\Psi$ provides two representations for $Z(\mathcal{F})$: one in terms of the strong regular Gröbner bases $\mathcal{G}_1, \ldots, \mathcal{G}_e$, and the other in terms of the regular triangular sets $\mathcal{C}_1, \ldots, \mathcal{C}_e$.  

18
**Theorem A.3** Let \( \{T_1, \ldots, T_e\} \) be a regular triangular decomposition of \( F \subseteq \mathbb{K}[x] \) and each \((C_i, G_i)\) be constructed from \( T_i \) according to Theorem 3.6. Then \( \{(C_1, G_1), \ldots, (C_e, G_e)\} \) is a strong regular characteristic decomposition of \( F \).

**Proof** As \( \{T_1, \ldots, T_e\} \) is a triangular decomposition of \( F \), we have \( \sqrt{\langle F \rangle} = \bigcap_{i=1}^e \sqrt{\text{sat}(T_i)} \).

By Theorem 3.6 the W-characteristic set \( C_i \) of \( \text{sat}(T_i) \) is regular and \( \text{sat}(C_i) = \langle G_i \rangle \), so each \((C_i, G_i)\) is an src pair for \( i = 1, \ldots, e \). Using the equalities \( \text{sat}(T_i) = \text{sat}(C_i) \) and \( \langle G_i \rangle = \text{sat}(T_i) \) one can easily prove that

\[
\sqrt{\langle F \rangle} = \bigcap_{i=1}^e \sqrt{\text{sat}(T_i)} = \bigcap_{i=1}^e \sqrt{\text{sat}(C_i)} = \bigcap_{i=1}^e \sqrt{\langle G_i \rangle}.
\]

Therefore, \((C_1, G_1), \ldots, (C_e, G_e)\) is an src decomposition of \( F \).

More generally, for any decomposition of an ideal \( I = \langle F \rangle \subseteq \mathbb{K}[x] \) into \( e \) ideals \( I_1, \ldots, I_e \) such that \( \sqrt{I} = \bigcap_{i=1}^e \sqrt{I_i} \), one can apply Algorithm 2 to each generating set of \( I_i \) for \( i = 1, \ldots, e \) and then combine the results for all \( i \) to yield a strong regular characteristic decomposition of \( F \), from which a regular triangular decomposition of \( F \) is obtained as by-product.