On W-Characteristic Sets of Lexicographic Gröbner Bases

Chenqi Mou[a] and Dongming Wang[ab]

[a]LMIB – School of Mathematics and Systems Science, Beihang University, Beijing 100191, China
[ab]Centre National de la Recherche Scientifique, 75794 Paris Cedex 16, France

chenqi.mou@buaa.edu.cn, dongming.wang@lip6.fr

Preliminaries: LEX Gröbner bases

LEX term ordering $\boldsymbol{u} = \boldsymbol{x}^{\boldsymbol{\alpha}} >_{\text{LEX}} \boldsymbol{v} = \boldsymbol{x}^{\boldsymbol{\beta}}$ if the left rightmost nonzero entry in the vector $\boldsymbol{\alpha} - \boldsymbol{\beta}$ is positive

$\rightsquigarrow$ *leading term* $\text{lt}(F)$: the greatest term in a polynomial F

Gröbner basis 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 $\langle \text{lt}(G_1), \ldots, \text{lt}(G_s)\rangle = \langle \text{lt}(\mathfrak{I})\rangle$.

Normal Form $F \in \mathbb{K}[\boldsymbol{x}]$, $\mathcal{G} = \{G_1, \ldots, G_s\}$ a Gröbner basis of $\mathfrak{I}$: there is a unique polynomial $R \in \mathbb{K}[\boldsymbol{x}]$ such that $F - R \in \mathfrak{I}$ and no term of R is divisible by any of $\text{lt}(G_1), \ldots, \text{lt}(G_s)$ $\rightsquigarrow$ R is called the *normal form*, $\text{nform}(F, \mathcal{G})$

$\rightsquigarrow$ $\mathcal{G}$ is *reduced* if any $G \in \mathcal{G}$ is monic and $G = \text{nform}(G, \mathcal{G} \setminus \{G\})$: The reduced Gröbner basis of an ideal is unique.

Ideal $\{G_1, \ldots, G_s\}$ a Gröbner basis $\rightsquigarrow$ $\langle G_1, \ldots, G_s\rangle$

B. Buchberger

ideal		its LEX Gröbner basis
$\mathfrak{I} \subset \mathbb{K}[\boldsymbol{x}]$	$\Longrightarrow$	$\mathcal{G} \subset \mathbb{K}[\boldsymbol{x}]$
$\mathfrak{I} \cap \mathbb{K}[x_1, \ldots, x_k]$	$\Longrightarrow$	$\mathcal{G} \cap \mathbb{K}[x_1, \ldots, x_k]$

Elimination property

⇐Ordering⇒

⇐Definition⇒

⇐Reduction⇒

⇐Ideal⇒

Preliminaries: triangular sets

Variable ordering $x_1 < \ldots < x_n \rightsquigarrow$ *leading variable* $\text{lv}(F)$ of F

$F = I x_i^k + R$, with $I \in \mathbb{K}[\boldsymbol{x}_{i-1}]$, $R \in \mathbb{K}[\boldsymbol{x}_i]$, and $\deg(R, x_i) < k = \deg(F, x_i)$.

$\rightsquigarrow$ I is called the *initial* of F, $\text{ini}(F)$

Triangular set Any finite, nonempty, ordered set $\mathcal{T} = [T_1, \ldots, T_r]$ of polynomials in $\mathbb{K}[\boldsymbol{x}] \setminus \mathbb{K}$ is called a *triangular set* if $\text{lv}(T_1) < \cdots < \text{lv}(T_r)$.

$\rightsquigarrow$ $\mathcal{T}$ is *normal* if each $\text{ini}(T)$ involves only $\{x_1, \ldots, x_n\} \setminus \{\text{lv}(T) : T \in \mathcal{T}\}$

Pseudo-remainder $F, G \in \mathbb{K}[\boldsymbol{x}]$ two polynomials with $\text{lv}(G) = x_k$: there exist Q, R and an integer s such that $\text{ini}(G)^s F = QG + R$ and $\deg(R, x_k) < \deg(G, x_k)$.

$\rightsquigarrow$ R is called the *pseudo-remainder* of F w.r.t. G, $\text{prem}(F, G)$

$\rightsquigarrow$ $\text{prem}(F, \mathcal{T}) := \text{prem}(\cdots(\text{prem}(\text{prem}(F, T_r), T_{r-1}), \ldots), T_1)$

Saturated ideal $\text{sat}(\mathcal{T}) := \langle \mathcal{T} \rangle : J^\infty$, where $J = \text{ini}(T_1) \cdots \text{ini}(T_r)$.

Wen-tsun Wu

$$
\begin{array}{l}
T_1(x_1, \ldots, x_{s_1}) \\
T_2(x_1, \ldots, x_{s_1}, \ldots, x_{s_2}) \\
T_3(x_1, \ldots, x_{s_1}, \ldots, x_{s_2}, \ldots, x_{s_3}) \\
\quad \vdots \\
T_r(x_1, \ldots, x_{s_1}, \ldots, x_{s_2}, \ldots, x_{s_3}, \ldots, \ldots, x_{s_r})
\end{array}
$$

Triangular set

W-characteristic sets of LEX Gröbner bases

Background: structures of LEX Gröbner bases They were studied first by Lazard [4] for bivariate ideals and then extended to general zero-dimensional multivariate (radical) ideals [3, 6, 2]. Based on the structures of LEX Gröbner bases, algorithms have been proposed to compute triangular decompositions out of LEX Gröbner bases for zero-dimensional ideals [5, 2]. The relationships between LEX Gröbner bases and Ritt characteristic sets were explored in [1] and then made clearer in [8] with the concept of W-characteristic sets.

W-characteristic set Let $\mathcal{P} \subset \mathbb{K}[\boldsymbol{x}]$ be a polynomial set and $\mathcal{G}$ be the reduced LEX Gröbner basis of $\langle \mathcal{P} \rangle$. Then the set

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

ordered according to $<_{\text{LEX}}$, where $\mathcal{G}^{(i)} := \{G \in \mathcal{G} : \text{lv}(G) = x_i\}$, is called the *W-characteristic set* of $\langle \mathcal{P} \rangle$.

Basic properties Let $\mathcal{C}$ be the W-characteristic set of $\langle \mathcal{P} \rangle \subseteq \mathbb{K}[\boldsymbol{x}]$. Then (a) for any $P \in \langle \mathcal{P} \rangle$, $\text{prem}(P, \mathcal{C}) = 0$; (b) $\langle \mathcal{C} \rangle \subseteq \langle \mathcal{P} \rangle \subseteq \text{sat}(\mathcal{C})$; (c) $\mathsf{Z}(\mathcal{C}/\text{ini}(\mathcal{C})) \subseteq \mathsf{Z}(\mathcal{P}) \subseteq \mathsf{Z}(\mathcal{C})$.

An example in $\mathbb{K}[a, x, y, z]$ with $a < x < y < z$

$$
\left\{
\begin{array}{l}
x^3 + 2x^2 + (1 - a^2)x - a^2, \\
x^2 y + xy - ax - x,\ ay - x - 1,\ xy^2 - x - 1, \\
(x^2 + x - a^2)z,\ (xy - a)z,\ z^2 - yz + y^3 - y
\end{array}
\right\}
\Longrightarrow
\begin{array}{l}
x^3 + 2x^2 + (1 - a^2)x - a^2 \\
ay - x - 1 \\
(x^2 + x - a^2)z
\end{array}
$$

LEX Gröbner basis — W-characteristic set

Minimal triangular set contained in Gröbner basis

Normality and Psuedo-divisibility in W-characteristic sets (and thus in LEX Gröbner bases)

Either normality or pseudo-divisibility: a theorem

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 $(1 \leq k \leq r)$ 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 $I_{k+1} = \text{ini}(C_{k+1})$ and l be the integer such that $\text{lv}(I_{k+1}) = \text{lv}(C_l)$.

(a) If I_{k+1} is not R-reduced with respect to C_l, then

$$\text{prem}(I_{k+1}, [C_1, \ldots, C_l]) = 0, \quad \text{prem}(C_{k+1}, [C_1, \ldots, C_k]) = 0.$$

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

Pseudo-divisibility

Example (continued)

The W-characteristic set above

$$
\begin{bmatrix}
x^3 + 2x^2 + (1 - a^2)x - a^2 \\
ay - x - 1 \\
(x^2 + x - a^2)z
\end{bmatrix}
$$

is not normal (the initial $x^2 + x - a^2$ involves x), and thus it is not regular:

$$x^3 + 2x^2 + (1 - a^2)x - a^2 = (x^2 + x - a^2)(x + 1),$$

which corresponds to (b) left.

Structures of LEX Gröbner bases

Characteristic pairs

Characteristic pair A pair $(\mathcal{G}, \mathcal{C})$ with $\mathcal{G}, \mathcal{C} \subseteq \mathbb{K}[\boldsymbol{x}]$ is called a *characteristic pair* if $\mathcal{G}$ is a reduced LEX Gröbner basis, $\mathcal{C}$ is the W-characteristic set of $\mathcal{G}$, and $\mathcal{C}$ is normal.

Connecting two ideals Let $\mathcal{C}$ be the W-characteristic set of $\langle \mathcal{P} \rangle$. If $\text{sat}(\mathcal{C}) = \langle \mathcal{C} \rangle$, then $\text{sat}(\mathcal{C}) = \langle \mathcal{P} \rangle$.

$\rightsquigarrow$ The reverse of the above property does not hold in general.

Strong characteristic pair A characteristic pair $(\mathcal{G}, \mathcal{C})$ is *strong* if $\langle \mathcal{G} \rangle = \text{sat}(\mathcal{C})$.

$\rightsquigarrow$ A reduced LEX Gröbner basis $\mathcal{G}$ is *characterizable* if $\langle \mathcal{G} \rangle = \text{sat}(\mathcal{C})$, where $\mathcal{C}$ is the W-characteristic set of $\mathcal{G}$.

Normality The W-characteristic set of any characterizable Gröbner basis is normal.

$\rightsquigarrow$ Every characteristic pair has a characterizable LEX Gröbner basis, and a characterizable Gröbner basis furnishes a characteristic pair with its W-characteristic set.

Characteristic decomposition

Characteristic decomposition A set $\{(\mathcal{G}_1, \mathcal{C}_1), \ldots, (\mathcal{G}_t, \mathcal{C}_t)\}$ of characteristic pairs in $\mathbb{K}[\boldsymbol{x}]$ is called a *characteristic decomposition* of $\mathcal{F}$ if

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

$\rightsquigarrow$ A characteristic decomposition is *strong* if its characteristic pairs are all strong.

Algorithm proposed

Transform to Ritt characteristic set $\mathcal{C} = [C_1, \ldots, C_r]$ W-characteristic set of $\langle \mathcal{P} \rangle$,

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

If $\mathcal{C}$ is normal, then $\mathcal{C}^*$ is normal and is a Ritt characteristic set of $\langle \mathcal{P} \rangle$.

Transform to strong characteristic pair $(\mathcal{G}, \mathcal{C})$ a characteristic pair, let $\bar{\mathcal{G}}$ and $\bar{\mathcal{C}}$ be the reduced LEX Gröbner basis and W-characteristic set of $\text{sat}(\mathcal{C})$ respectively. Then $\bar{\mathcal{C}}$ is normal, $\text{sat}(\bar{\mathcal{C}}) = \langle \bar{\mathcal{G}} \rangle$, and thus $(\bar{\mathcal{G}}, \bar{\mathcal{C}})$ is a strong characteristic pair.

LEX Gröbner bases and W-characteristic sets with rich interconnections

References

[1] Philippe Aubry, Daniel Lazard, and Marc Moreno Maza, *On the theories of triangular sets*, J. Symbolic Comput. **28** (1999), no. 1–2, 105–124.

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

[3] Michael Kalkbrener, *Solving systems of algebraic equations by using Gröbner bases*, Proceedings of Eurocal '87, Springer-Verlag, Berlin Heidelberg, 1989, pp. 282–292.

[4] Daniel Lazard, *Ideal bases and primary decomposition: Case of two variables*, J. Symbolic Comput. **1** (1985), no. 3, 261–270.

[5] Daniel Lazard, *Solving zero-dimensional algebraic systems*, J. Symbolic Comput. **13** (1992), no. 2, 117–131.

[6] Maria Grazia Marinari and Teo Mora, *A remark on a remark by Macaulay or enhancing Lazard structural theorem*, Bull. Iranian Math. Soc. **29** (2003), no. 1, 1–45.

[7] Chenqi Mou, Dongming Wang, and Xiaoliang Li, *Decomposing polynomial sets into simple sets over finite fields: The positive-dimensional case*, Theoret. Comput. Sci. **468** (2013), 102–113.

[8] Dongming Wang, *On the connection between Ritt characteristic sets and Buchberger-Gröbner bases*, Math. Comput. Sci. **10** (2016), 479–492.

[9] Dongming Wang, Rina Dong, and Chenqi Mou, *Decomposition of polynomial sets into characteristic pairs*, arXiv:1702.08664 (2017).