三角形である準素成分を持つ辞書式順序グレブナー基底について

ダハン　グザビエ [*]

お茶の水女子大学、プロジェクト教育研究院

Xavier Dahan

Ochanomizu University, Graduate School of General Educational Research

Abstract

$\mathcal{G}$ を零次元イデアル I の辞書式順序の極小グレブナー基底とする。I の全ての準素成分の辞書式順序グレブナー基底が三角形だと仮定する。本稿では、I が根基イデアルのときに知られている結果が、この仮定の下でも成立することを説明する。詳しくは : (1) 一般化した中国剰余定理により、準素成分の基底から基底 $\mathcal{G}$ を結合できる。(2) グレブナー基底 $\mathcal{G}$ の多項式に、因数分解のパターンが現れる。(3) stability 性も成り立つ: evaluation 写像により与えた $\mathcal{G}$ の像はまだグレブナー基底である。

Abstract

Let $\mathcal{G}$ be a minimal lexicographic Gröbner basis (lexGb) of a zero-dimensional I. Assume that all the primary components of I have a lexGb that is a triangular set. This note explains that the strong properties known about $\mathcal{G}$ when I is a radical ideal, also hold in this case. These properties are: (1) a reconstruction of the basis $\mathcal{G}$ from that of the primary components by a generalization of the Chinese Reminder Theorem, (2) the factorization pattern of the polynomials in $\mathcal{G}$ and (3) the stability property under specialization maps.

設定　$\mathcal{G}$ を零次元イデアル I の辞書式順序の極小グレブナー基底とする。（ここでは、全てのグレブナー基底が極小かつ辞書式順序によるものだと想定する。）以下のことを仮定する :

$$I \text{ の全ての準素成分のグレブナー基底が三角形である。} \tag{H}$$

その準素成分のグレブナー基底（ここで、三角形集合 $\mathbf{t}^{(i)} = (t_1^{(i)}(x_1), t_2^{(i)}(x_1,x_2), \ldots, t_n^{(i)}(x_1,\ldots,x_n))$ が入力として与えられている。

以下の**記号**を使う : $\ell \leq n$ に対して、$I_{\leq \ell} := I \cap k[x_1,\ldots,x_\ell]$。また $\mathbf{t} = (t_1,\ldots,t_n)$ を三角形集合とし, その時 $\mathbf{t}_{\leq \ell} = (t_1,\ldots,t_\ell)$ と書く。

定理 1

仮定 (H) の下で、 全ての $i \neq j$ に対して、$\mathbf{t}_{\leq \ell}^{(i)} = \mathbf{t}_{\leq \ell}^{(j)}$ かつ $t_{\ell+1}^{(i)} \neq t_{\ell+1}^{(j)}$ を満たす最大整数 $\ell < n$ が存在する。その時、環 $(k[x_1,\ldots,x_\ell]/\langle \mathbf{t}_{\leq \ell}^{(i)} \rangle)[x_{\ell+1},\ldots,x_n]$ の中で、$\langle t_{\ell+1}^{(i)} \rangle + \langle t_{\ell+1}^{(j)} \rangle = \langle 1 \rangle$ が成り立つ。

定理 2 は主な 4 つの結果を記述する。

定理 2

1) 標準単項式の集合 $\text{SM}(I)$ を計算するため、k 上の演算が不要であり、$O(n\,r\,D)$ 程度の k 上における等式テストがかかる。

そこで、整数 r が後に定義され、 $D = |\text{SM}(I)| = \dim_k(k[\mathbf{x}]/I)$ *(I の次数)*

*dahan.xavier@ocha.ac.jp, xdahan@gmail.com

2) (中国剰余定理 – 再結合) I の辞書式順序の極小グレブナー基底を計算するのに、$O(|\mathcal{G}| \cdot D^2)$ 程度の k 上の演算がかかる。

I は根基イデアルのとき、より良い計算量 $O(|\mathcal{G}| \cdot D \cdot \log(D)^3)$ で計算できる。(高速の補間を用いる)

3) 構造: $\mathcal{G}$ の中にある多項式 g を考え、一般性を失わなく $g \notin k[x_1, \ldots, x_{n-1}]$ と仮定できる。次の様式を満たす多項式 $\chi_i \in k[x_1, \ldots, x_i]$ が存在する。

$$\mathrm{LM}(g) = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \quad \Rightarrow \quad g \equiv \prod_{i=1}^{n} \chi_i \bmod I_{\leq n-1}, \quad \mathrm{LM}(\chi_i) = x_i^{\alpha_i}.$$

4) *evaluation* 写像により、グレブナー性が保たれている。(英語で *stability* 性とも言われている)。具体的に：

$\mathcal{G} = \{g_1, \ldots, g_s\}$ と書く。点 $\alpha = (\alpha_1, \ldots, \alpha_\ell) \in \bar{k}^\ell$ とし、ただし $\ell < n$、*evaluation* 写像 $\phi_{\mathbf{a}} : k[x_1, \ldots, x_n] \to \bar{k}[x_{\ell+1}, \ldots, x_n]$、$P(x_1, \ldots, x_n) \mapsto P(\alpha_1, \ldots, \alpha_\ell, x_{\ell+1}, \ldots, x_n)$ を考える。$\phi_{\mathbf{a}}(\mathcal{G})$ はイデアル $\phi_{\mathbf{a}}(I)$ のグレブナー基底である。

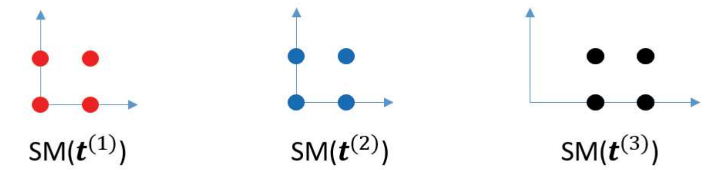
コメント　上記の 4 つの結果が相互接続されている。特に、結果 1)-2) と 3)-4) の証明は密に関連する。結果 1)-2) は一般化した中国剰余定理 (CRT) に従う。その戦略は I が根基イデアルのとき、論文 [6] で記述されている。CRT による再結合を行うために、木を用いるデータ表現を使う。結果 3) は、葉から根まで (ボトムアップ) 木の深さ n による帰納法で証明される。そこから、結果 4) が出される。

整数 r について　定理 2 1) においてはある整数 r を含む。[5, § 2.2] で呼ばれた「準素分解の木」の子の最大数である。この木は結合アルゴリズムを導く。例を用いて大まかに説明する。

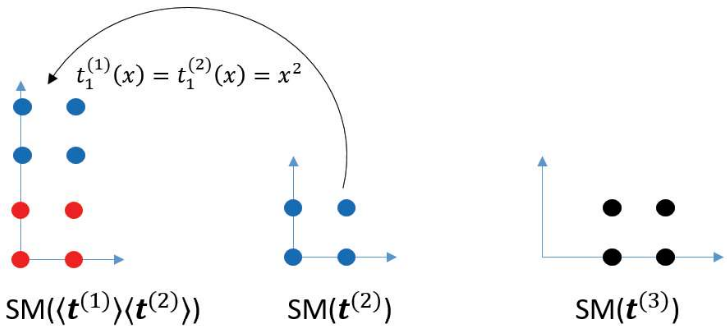
例. 入力：三つの互いに素な三角形集合（準素成分の辞書式順序グレブナー基底)

$$\begin{cases} t_1^{(1)}(x) = x^2 \\ t_2^{(1)}(x,y) = y^2 + xy + 2x \end{cases} \quad \begin{cases} t_1^{(2)}(x) = x^2 \\ t_2^{(2)}(x,y) = (y+1)^2 + x(y+1) - x \end{cases} \quad \begin{cases} t_1^{(3)}(x) = (x-1)^2 \\ t_2^{(3)}(x,y) = y^2 + 2(x-1)y + 3(x-1) \end{cases}$$

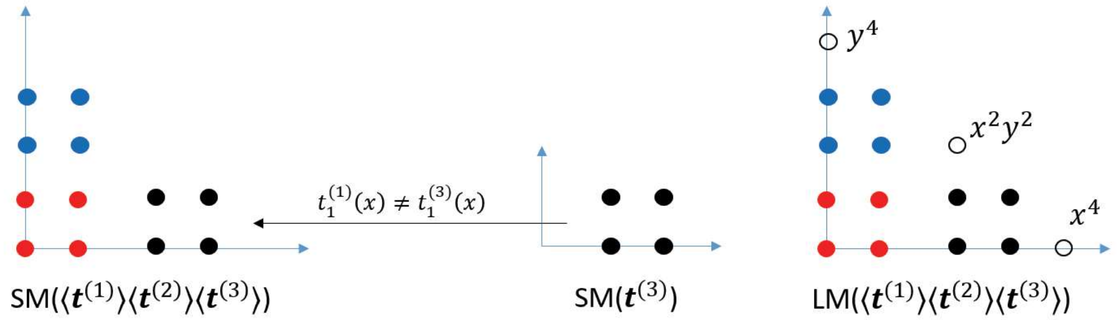
下の図は標準単項式を表す。



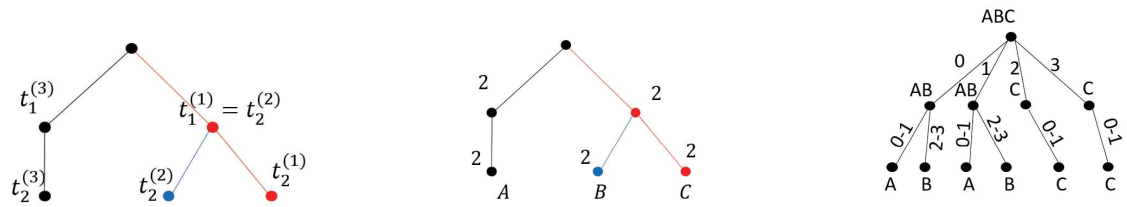
多項式 $t_1^{(1)}(x_1)$ と $t_1^{(2)}(x_1)$ が等しいから、三角形集合 $\mathbf{t}^{(1)}$ と $\mathbf{t}^{(2)}$ が y-軸に沿って結合されている。イデアル $\langle \mathbf{t}^{(1)} \rangle \langle \mathbf{t}^{(2)} \rangle$ の標準単項式を得られる。



一方、$t_1^{(1)}(x_1) \neq t_1^{(3)}(x_1)$ から三角形集合 $\mathbf{t}^{(3)}$ を結合する際に、x-軸に沿って行う（左下の図）。イデアル $I = \langle \mathbf{t}^{(1)} \rangle \langle \mathbf{t}^{(2)} \rangle \langle \mathbf{t}^{(3)} \rangle$ の標準単項式を得られる。そこから、先頭単項式を読める：$\mathrm{LM}(I) = \langle x^4\ ,\ x^2y^2\ ,\ y^4 \rangle$。（右下の図）



結果 1) は標準単項式についてだけ対処するが、上記の結合式を導くように根本的な予備結果である。実際、木というデータ構造だけを取り扱い、k 上の演算が不要である。左下の図は「準素分解の木」[5, § 2.2] である。真ん中の木は三角形集合の実数を示す。最後に、右下の木は、[6] で導入された「単項式のトライ木」の一般化である。この定義はやや複雑で、本稿で省く。ここで、整数 r は 2 であり、準素分解の木における子の最大数である。



先行研究　二種類ある：第一、本稿の仕方と同様に、辞書式順序グレブナー基底に専念されるアルゴリズム [3, 4, 6, 9, 10, 7, 8]。第二は Buchberger-Möller 氏らによるアルゴリズムに従う手法 [2, 1]、単項式順序を問わず任意の順序に関するグレブナー基底を計算できる。前者は何とか CRT に基づいており、後者は線形代数に基づいている。次の表（Table 1）では本研究と先行研究の比較をまとめる。

References

[1] John Abbott, Martin Kreuzer, and Lorenzo Robbiano. Computing zero-dimensional schemes. *Journal of Symbolic Computation*, 39(1):31–49, 2005.

[2] B. Buchberger and H. Möller. The construction of multivariate polynomials with preassigned zeros. In *Lecture Notes in Computer Science (EUROCAM'82)*, volume 144, pages 24–31, London, UK, 1982.

[3] L. Cerlienco and M. Mureddu. From algebraic sets to monomial linear bases by means of combinatorial algorithms. *Discrete Mathematics*, 139(1—3):73 – 87, 1995.

[4] Luigi Cerlienco and Marina Mureddu. Multivariate interpolation and standard bases for macaulay modules. *Journal of Algebra*, 251(2):686 – 726, 2002.

研究	年	扱う場合	結　果 1)-4)	正しさ	1) / 2) に対する計算量	被約？
This	2018	(H)	1) - 4)	おそらく	$O(r\,n\,D)$ / $O(\|\mathcal{G}\|.D^2)$	no
[2]	1982	IdPoint	2)	○	$O(nD^3)$	yes
[1]	2005	General	2)	○	$\cdot$ / $> O(nD^3)$	yes
[3]	1995	IdPoint	1) - 2)	○	$O(n^2D^2)$ / $\cdot$	no
[4]	2002	ShiftMonId	1)	○	$O(n^2D^2)/\cdot$	no
[6]	2006	IdPoint	1) - 2)	○	$O(r\,n\,D)/\cdot$	no
[9]	2003	IdPoint	3) - 4)	複雑	$\cdot$ / $\cdot$ (NG)	no
[10]	2006	ShiftMonId	3) - 4)	複雑	$\cdot$ / $\cdot$ (NG)	no
[7]	2008	IdPoint	1) - 2)	○	$\cdot$ / $\cdot$ (NG)	yes
[8]	2014	ShiftMonId	1) - 2)	複雑	$\cdot$ / $\cdot$ (NG)	?

Table 1: IdPoint = 点のイデアル. ShiftMonId = Shifted 単項式イデアル. (H) = 仮定 (H). (NG) = Not Good. ○ = 正しい

[5] Xavier Dahan. Gcd modulo a primary triangular set of dimension zero. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 109–116, New York, NY, USA, 2017. ACM.

[6] B. Felszeghy, B. Ráth, and L. Rónyai. The lex game and some applications. *J. of Symbolic Comput.*, 41(6):663 – 681, 2006.

[7] M. Lederer. The vanishing ideal of a finite set of closed points in affine space. *J. of Pure and Applied Algebra*, 212:1116–1133, 2008.

[8] Na Lei, Yuan Teng, and Yu-xue Ren. A fast algorithm for multivariate hermite interpolation. *Applied Mathematics-A Journal of Chinese Universities*, 4(29):438–454, 2014.

[9] M. G. Marinari and T. Mora. A remark on a remark by Macaulay or enhancing Lazard structural theorem. *Bull. Iranian Math. Soc.*, 29(1):1–45, 85, 2003.

[10] M. G. Marinari and T. Mora. Cerlienco-Mureddu correspondence and Lazard structural theorem. *Investigaciones Mathematicas*, 27:155–178, 2006.