グレブナー基底の項順序についての再考

Term order for Groebner basis, revisited

神戸大学大学院・人間発達環境学研究科　　大島谷 遼 [*1]
Ryo OSHIMATANI
Graduate School of Human Development and Environment, Kobe University

神戸大学大学院・人間発達環境学研究科　　長坂 耕作 [*2]
Kosaku NAGASAKA
Graduate School of Human Development and Environment, Kobe University

Abstract

In this preliminary report, we introduce a method to find a term order such that the given set of polynomials F is a Gröbner basis for the ideal $I = \langle F \rangle$. We note that this problem can be solved by the method given by Strumfels and Wiegelmann that is based on the maximum matching problem for bipartite graphs and linear programming, but this time we consider a different approach.

1　はじめに

グレブナー基底を求めるアルゴリズムは，Buchberger アルゴリズム [Buc06] に代表されるように基本的にはイデアルの生成系と項順序を指定して計算するものである．一方で，以下の例のように，イデアル I と一定の項順序において，与えられた多項式集合がそのままグレブナー基底となるようなものが存在する．

例 1
以下の I の $z \succ y \succ x$ での全次数辞書式順序及び全次数逆辞書式順序におけるグレブナー基底は F である．

$$F = \{f_1 = 2xy + yz,\ f_2 = x^2 + y + z\}, \quad I = \langle F \rangle \subset \mathbb{C}[x, y, z]$$

このように，Buchberger アルゴリズムなどでの計算の前に，計算対象である F 自身がグレブナー基底となっているような項順序を求めることができれば，どんな項順序でもいいのでグレブナー基底であるという性質が必要な場合には有効な計算方法であることが考えられる．また，仮に一定の項順序が必要な場合にも，FGLM アルゴリズム [FGLM93] などによって項順序の変換を行うことで，有効な計算方法となることも考えられる．

そこで，本研究では，「イデアル $I = \langle F \rangle$ に対して，F 自身が I の $\prec_M$ に関するグレブナー基底となるような重み行列 M は存在するか．存在するならば一つ求めよ．」という問題を解くことを最終目標とし，今回はその途中経過の発表を行った．

尚，発表後の質疑応答の際に話が挙がった通り，この問題には Groebner basis detection という名前がついており，我々の方法とは異なるが Sturumfels ら [GS93] によって polytope を用いたアルゴリズムが与えられていることに留意されたい．以下で解いている問題と同等なものは structural Groebner basis detection と呼ばれ，二部グラフの最大マッチング問題と線形計画法を用いたアルゴリズムが Sturumfels ら [SW97] によって与えられている．

[*1] E-mail: 208d418d@stu.kobe-u.ac.jp
[*2] E-mail: nagasaka@main.h.kobe-u.ac.jp

1.1 記法と matrix order の定義

K を体とする．多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[x_1, \ldots, x_n] \setminus K$ に対して，$K[x_1, \ldots, x_n]$ のイデアルを $I = \langle F \rangle \subset K[x_1, \ldots, x_n]$ とする．n 変数の項全体の集合を $T_n = \{x_1^{e_1} \times \cdots \times x_n^{e_n} : e_i \in \mathbb{Z}_{\geq 0}\}$ とする．項 $t_1 \in T_n$ の指数ベクトルを，$e(t_1)$ と表す．(例：$t_1 = x^2y^3z^4 \Rightarrow e(t_1) = (2, 3, 4)$) また，重み行列 M で表される matrix order $\prec_M$ を以下のように定義する．

定義 1 (matrix order)
項 $t_1, t_2 \in T_n$ の指数ベクトル $e(t_1), e(t_2)$ に対し，

$$t_1 \succ_M t_2 \Longleftrightarrow Me(t_1) >_{\neq} Me(t_2)$$

ただし，$<_{\neq}$ や $>_{\neq}$ はベクトルの等しくない最初の成分での比較を表す不等号である．

matrix order は任意の項順序を表現可能 [Rob85] であるということがわかっており，column full rank な行列を考えれば十分であるということが分かっているため，本稿では，重み行列 M を $n \times n$ の正方で正則な行列であるとする．

項順序 $\prec$ において，多項式 $f \in F$ に含まれる項で，最も項順序が大きい項に含まれる単項式の，係数を除いた部分を $\mathrm{ht}_\prec(f)$ とし，その単項式の係数を $\mathrm{hc}_\prec(f)$ で表す．

定義 2
項順序を $\prec$ とし $f, g \in K[x_1, \ldots, x_n]$ とする．f に含まれる単項式 t が $\mathrm{ht}_\prec(g)$ で割り切れるとする．このとき，$h = f - \dfrac{t}{\mathrm{ht}_\prec(g)} g$ に対し，$f \to_g h$ と書き，f の g での単項簡約と呼ぶ．この操作を 0 回を含む有限回繰り返し，これ以上単項簡約できない h が得られたとき，h を f の g による正規形（*normal form*）と呼び，$h = \mathrm{nf}_g(f)$ と表す．また，多項式集合 $G \subset K[x_1, \ldots, x_n]$ において，$\forall g_i \in G$ で f を単項簡約を繰り返すことで h が得られるとき，同様に h を f の G による正規形と呼び，$h = \mathrm{nf}_G(f)$ と表す．

定義 3
項順序を $\prec$ とし $f, g \in K[x_1, \ldots, x_n]$ とする．このとき，f, g の S 多項式を

$$\mathrm{Spoly}(f, g) = \frac{\mathrm{hc}_\prec(g) \cdot \mathrm{lcm}(\mathrm{ht}_\prec(f), \mathrm{ht}_\prec(g))}{\mathrm{ht}_\prec(f)} \cdot f - \frac{\mathrm{hc}_\prec(f) \cdot \mathrm{lcm}(\mathrm{ht}_\prec(f), \mathrm{ht}_\prec(g))}{\mathrm{ht}_\prec(g)} \cdot g$$

と定義する．

2 アルゴリズム

2.1 アルゴリズムの概要

本稿では簡単のため，F が $I = \langle F \rangle$ のグレブナー基底となるような重み行列 M の必要十分条件を求めるのではなく，以下の定理 4 を十分条件として考えることで，系 5 を満たすような重み行列 M を考える（この問題は structural Groebner basis detection と呼ばれる）．

定理 4 (Buchberger の判定条件)

$$\forall f, g \in K[x_1, \ldots, x_n],\ \gcd(\mathrm{ht}_\prec(f), \mathrm{ht}_\prec(g)) = 1 \Longrightarrow \mathrm{nf}_{\{f,g\}}(\mathrm{Spoly}(f, g)) = 0$$

系 5
イデアル I の生成系を $F = \{f_1, \ldots, f_k\}$ とする．このとき，

$$\forall i, j \ (i \neq j),\ \gcd(\mathrm{ht}_{\prec}(f_i), \mathrm{ht}_{\prec}(f_j)) = 1$$

が成り立つとき， F は I の $\prec_M$ に関するグレブナー基底である．

これにより，以下のようにアルゴリズムの概要を記述することができる．

Algorithm 1 そのままグレブナー基底となるような項順序の導出

Input: 多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[x_1, \ldots, x_n]$
Output: F がイデアル $I = \langle F \rangle$ のグレブナー基底であるような項順序 $\prec_M$

1: 互いに素である単項式の組 $t_1, \ldots, t_k$ をそれぞれの多項式から選出する．
2: $i = 1, \ldots, k$ において $\mathrm{ht}_{\prec_M}(f_i) = t_i$ となる重み行列 M を求める．
3: **return** M

2.2 ステップ 1：互いに素な項の選出

$F = \{f_1, \ldots, f_k\} \subset K[x_1, \ldots, x_n]$ を多項式集合とする．多項式 f_i に含まれる係数が 0 でない項で，定数項を除く項全体の集合を $T(f_i)$ とする．$\mathcal{T}(F) = T(f_1) \times \cdots \times T(f_k)$ とし，

$$\mathcal{T}_{cp} = \{(t_1, \ldots, t_k) \in \mathcal{T} : \forall t_i, t_j \in T_n,\ \gcd(t_i, t_j) = 1 \ (i \neq j)\}$$

とする．また，集合 $V(t)$ を項 t に含まれる変数で，次数 1 以上の変数全体の集合とする．

ステップ 1 はこのままでは全探索によってそれぞれが互いに素かどうかのチェックが行う必要が出てしまう．そこで，系 5 に関連する性質（互いに素となる項や互いに素とならない項）についてのいくつかの補題を与える．

2.2.1 互いに素となり得ない項の性質

補題 6
多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[x_1, \ldots, x_n] \setminus K$ において，

$$f_i \in F,\ t_i \in T(f_i),\ |V(t_i)| > n - k + 1$$

が成り立つとき，$\mathcal{T}_{cp}$ の元で i 番目の要素が t_i であるようなものは存在しない．

証明 $|V(t_i)| > n - k + 1$ が成り立ち，$\mathcal{T}_{cp}$ の元で i 番目の要素が t_i であるようなものが存在すると仮定する．定義より，任意の項 t に対して $|V(t)| \geq 1$ が成り立つ．従って，$j = 1, \ldots, i-1, i+1, \ldots, k$ において，

$$t_j \in T(f_j), \quad \sum_j |V(t_j)| \geq k - 1$$

よって，

$$|V(t_i)| + \sum_j |V(t_j)| > (n - k + 1) + (k - 1)$$

$$> n$$

これより変数の個数の合計が n 個以上であり $t_1, \ldots, t_k$ の中に，ある特定の変数を含む項が 2 つ以上存在する．しかし，$\mathcal{T}_{cp}$ の定義より，$t_1, \ldots, t_k$ は互いに素でなくてはならない．
よって，補題 6 が成り立つ． ∎

系 7
多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[x_1, \ldots, x_n] \setminus K$ において次が成り立つ．

$$n < k \Longrightarrow \mathcal{T}_{cp} = \phi$$

系 7 をより，系 5 を満たすような項順序は存在しないことがわかり，補題 6 より，F の多項式に含まれる項から互いに素になり得ないものを除外することが可能となる．

2.2.2 互いに素にはなるが，同じ多項式内で頭項としたときに矛盾が生じる項の性質

補題 8
多項式 f において，$t \mid t'$ を満たすような項 $t, t' \in T(f)$ が存在するとき，t は f の頭項となり得ない．ただし，$t \neq t'$．

証明 $t \mid t'$ より，$t' = rt$ と置ける．ただし，$r \in T_n$．t が f の頭項であると仮定する．すなわち，$t' \prec t$ であるため，$rt' \prec rt = t'$ となり，項順序の定義に矛盾する．よって，t は f の頭項となり得ない． ∎

2.2.3 互いに素にはなるが，それぞれが頭項となるような項順序に矛盾が生じる項の性質

補題 9
多項式 $f_1, f_2 \in K[x_1, \ldots, x_n]$ と単項式 $t_1, t_1' \in T(f_1)$, $t_2, t_2' \in T(f_2)$ に対して，

$$t_2 \mid t_1',\ t_1 \mid t_2'$$

が満たされるとき，t_1, t_2 はそれぞれの多項式で同時に頭項となり得ない．ただし，$t_1 \neq t_1', t_2 \neq t_2'$．

証明 t_1, t_2 はそれぞれ f_1, f_2 の頭項であると仮定する．仮定より，$t_2 \mid t_1',\ t_1 \mid t_2'$．つまり，

$$t_1' = r_2 t_2,$$
$$t_2' = r_1 t_1$$

ただし，$r_1, r_2 \in T_n$．いま，$t_2 \succ t_2'$ より，

$$\begin{aligned} r_2 t_2 &\succ r_2 t_2' \\ t_1' &\succ r_2 t_2' && (\because t_1' = r_2 t_2) \\ t_1 &\succ r_2 \cdot r_1 t_1 && (\because t_2' = r_1 t_1) \end{aligned}$$

これは，t_1 が f_1 の頭項であることに矛盾する． ∎

補題 10
多項式 $f_1, f_2 \in K[x_1, \ldots, x_n]$ と項 $t_1' \in T(f_1), t_2 \in T(f_2)$ に対して，

$$t_2 \mid t_1'$$

が成り立ち，項 $t_1 \in T(f_1), t_2' \in T(\frac{t_1'}{t_2} f_2)$ に対して，

$$t_1 \mid t_2'$$

が成り立つとき，t_1, t_2 はそれぞれの多項式で同時に頭項になり得ない．ただし，$t_1 \neq t_1', t_2 \neq t_2'$．

証明 補題 9 とほぼ同じ手順で証明できる．∎

以上より，まず補題 6 と系 7 によって，互いに素となり得ない項を除外でき，補題 8 によって，同じ多項式内にて頭項としたときに矛盾する項を除外できる．更に，補題 9 と補題 10 によって，複数の多項式間で矛盾が発生する項を除外することにより，探索対象の単項を減らすことができる．これらの性質を用いても，総当たりであることには変わらないが，本稿ではひとまずこの性質のみで話を進めることにする．

2.2.4 アルゴリズムの詳細と具体例

以上の系や補題より，アルゴリズムは以下のように記述できる．

Algorithm 2 そのままグレブナー基底となっているような項順序の導出

Input: 多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[x_1, \ldots, x_n]$

Output: F がイデアル $I = \langle F \rangle$ のグレブナー基底であるような項順序 $\prec_M$ 又は None

1: **if** $n < k$ **then**:
2: **return** None
3: **end if**
4: 補題 6，系 7，補題 8 の条件を満たす $f_1, \ldots, f_k$ の項を除外し，新たに $\tilde{F} = \{\tilde{f}_1, \ldots, \tilde{f}_k\}$ とする．
5: $T_{\tilde{F}} \leftarrow \mathcal{T}(\tilde{F})$
6: 補題 9，補題 10 の条件を満たす項の組を含むものを $T_{\tilde{F}}$ の中から除外し，$\tilde{T}_{\tilde{F}}$ とする．
7: $\mathcal{T}_{cp}$ と $\tilde{T}_{\tilde{F}}$ の共通部分を取り，それらを $t_1, \ldots, t_k$ とする．
8: $i = 1, \ldots, k$ において，$\mathrm{ht}_{\prec_M}(f_i) = t_i$ となる重み行列 M を求める．
9: **return** M

このアルゴリズムをもとに，以下のような例を考えてステップ 1 の項の除去を実際に行ってみる．

例 2
次のような多項式集合 $F \subset K[x, y]$ を考える．

$$F = \left\{ \begin{array}{l} f_1 = x^2 + xy + y, \\ f_2 = x + y^2 \end{array} \right\}$$

まず，f_1 において $y \mid xy$ が満たされることから，補題 8 より xy が除外される．次に，$y \in T(f_1)$ と $y^2 \in T(f_2)$ において，$y \mid y^2$ を満たし，$x \in T(f_2)$ と $x^2 \in T(f_1)$ において，$x \mid x^2$ を満たすことから，補題 9 より f_1 の y と f_2 の x が除外される．よって，最終的に

$$\tilde{T}(\tilde{F}) = \{(x^2, y^2)\}$$

から互いに素となる項の組を選べば良いことになり，

$$t_1 = x^2,\ t_2 = y^2$$

となる．

例 3
次のような多項式集合 $F \subset K[x, y, z]$ を考える．

$$F = \left\{ \begin{array}{l} f_1 = xy + yz, \\ f_2 = x^2 + y + z \end{array} \right\}$$

まず，$z \in T(f_2)$ と $yz \in T(f_1)$ において，$z \mid yz$ を満たす．一方で，f_2 の項を割り切るような f_1 の項は存在しない．しかし，$yz \div z$ の商である y を f_2 に掛け，

$$\begin{aligned} f_1 &= xy + yz, \\ y \cdot f_2 &= x^2y + y^2 + yz \end{aligned}$$

を考えると，$xy \in T(f_1)$ と $x^2y \in T(y \cdot f_2)$ が $xy \mid x^2y$ を満たすので，補題 *10* より，f_1 の xy と f_2 の z は除外され，最終的に

$$\tilde{T}(\tilde{F}) = \{(yz, x^2), (yz, y)\}$$

から互いに素となる項の組を選べば良いことになり，

$$t_1 = yz,\ t_2 = x^2$$

となる．

2.3　ステップ 2：項順序の導出

求めたい重み行列 M を，

$$M = \begin{pmatrix} \overrightarrow{m_1} \\ \vdots \\ \overrightarrow{m_n} \end{pmatrix} = \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{pmatrix}$$

とする．matrix order の定義より，項 t_1, t_2 が $t_1 \succ_M t_2$ を満たすとき，$Me(t_1) >_{\neq} Me(t_2)$ が満たされる．これを一般の等号と不等号を用いて表すと以下のようになる．

$$\begin{cases} \overrightarrow{m_1} \cdot e(t_1) = \overrightarrow{m_1} \cdot e(t_2) \\ \qquad\qquad \vdots \qquad\qquad\qquad , \quad \overrightarrow{m_\ell} \cdot e(t_1) > \overrightarrow{m_\ell} \cdot e(t_2) \\ \overrightarrow{m_{\ell-1}} \cdot e(t_1) = \overrightarrow{m_{\ell-1}} \cdot e(t_2) \end{cases}$$

ここで，ℓ は，M の第 $(\ell - 1)$ 行ベクトルまでとの積が等しく，第 ℓ ベクトルで初めて差がつくときことを表している．この連立不等式を解くことによって，重み行列 M を求めることができるが，その効率的な方法については検討中である．

謝　　辞

この発表の質疑応答の時間において，立教大学の野呂先生には先行研究の論文を教えて頂くなど，大変貴重なご助言を頂きました．この場を借りて深く御礼申し上げます．

参 考 文 献

[Buc06] Bruno Buchberger. An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *J. Symbolic Comput.*, 41(3-4):475–511, 2006. Translated from the 1965 German original by Michael P. Abramson.

[FGLM93] 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(4):329–344, 1993.

[GS93] Peter Gritzmann and Bernd Sturmfels. Minkowski addition of polytopes: computational complexity and applications to Gröbner bases. *SIAM J. Discrete Math.*, 6(2):246–269, 1993.

[Rob85] Lorenzo Robbiano. Term orderings on the polynomial ring. In *EUROCAL '85, Vol. 2 (Linz, 1985)*, volume 204 of *Lecture Notes in Comput. Sci.*, pages 513–517. Springer, Berlin, 1985.

[SW97] Bernd Sturmfels and Markus Wiegelmann. Structural Gröbner basis detection. *Appl. Algebra Engrg. Comm. Comput.*, 8(4):257–263, 1997.