パラメータを伴った Gröbner 基底の構造的な検出について

— Comprehensive structural Gröbner basis detection —

所属専攻	人間環境学専攻
学籍番号	208D418D
学 生 氏 名	大島谷 遼
指導教員氏名	長坂 耕作 准教授

第 1 章

はじめに

1.1　研究の背景

多項式集合 F が与えられ Gröbner 基底の計算を行う際，Buchberger アルゴリズム [Buc06] などによりイデアルと項順序を固定した上で，Gröbner 基底を得るための計算を行うのが一般的である．しかし，以下の例のように計算を行う前に F がそのまま Gröbner 基底であるような項順序を得ることができる場合もある．

例 1.1.1.
以下の多項式集合 F は，$z \succ y \succ x$ の全次数辞書式順序及び全次数逆辞書式順序においてイデアル $I = \langle F \rangle$ の Gröbner 基底となっている．

$$F = \left\{2xy + yz,\ x^2 + y + z\right\} \subset \mathbb{C}[x, y, z]$$

このような項順序を見つけることができれば，従来の計算を行わずに Gröbner 基底を得ることができる．また，ここで得た項順序を，FGLM アルゴリズム [FGLM93] や Gröbner walk[CKM93] などに代表される change of ordering のアルゴリズムによって変換することで，任意の項順序での Gröbner 基底を得ることも可能であり，有効な計算手段となることが考えられる．

例えば，連立代数方程式の求解のための計算では，多くの場合で辞書式順序（一般的には消去順序）での Gröbner 基底が必要となるが，辞書式順序での計算は遅くなることが知られており，入力の多項式集合の大きさによっては莫大な時間がかかってしまう可能性も否定できない．そこで，多項式集合がそのまま Gröbner 基底となっているような項順序が存在していれば，その項順序を求めたあとに change of ordering により辞書式順序の Gröbner 基底を求めることができる．これらの 2 つの計算の計算量が，元々行おうとしていた Gröbner 基底計算の計算量に比べて少なくなっているのであれば，この計算は有用な計算であったと言える．

このように「そのまま Gröbner 基底である」ような項順序を検出する問題は，Sturmfels らによって解かれた既知の問題であり，*Gröbner basis detection*[GS93] や *Structural Gröbner basis detection*[SW97] という名前が付けられている．

一方で，パラメータを伴った多項式環において，場合分けされたパラメータ空間と，それぞれに対応する Gröbner 基底を組にしたものを**包括的** *Gröbner* **基底系** [Wei92] と呼ぶ．包括的 Gröbner 基底系は，Gröbner 基底計算の中で，S-polynomial の計算が行われる際にパラメータの付いた係数が 0 か否かで場合分けを行い，項を確定させながら Gröbner 基底の計算を行っている．

これら 2 つの議論を踏まえ，本論文では，(Structural) Gröbner basis detection において，問題の設定をパラメータを伴った多項式環へと拡張し，それに付随して発見された定理についても取り上げる．まず第 2 章では，Sturmfels らとは違ったアプローチから，Structural Gröbner basis detection の問題を捉え，そこで新たに発見された定理とアルゴリズムを紹介する．次に，第 3 章では，Gröbner basis detection と Structural

Gröbner basis detection について，既に知られている部分について述べる．第 4 章では，これらの問題をパラメータを伴った多項式環へと拡張するために，パラメータ空間を分割するためのアルゴリズムの直接的な方法を紹介する．最後に，第 5 章では，パラメータ空間の分割を効率化するための議論を行い，最終的なアルゴリズムを完成させる．

1.2 基本的な記法の確認

以下では本論文全体を通して使用される記法を定義しておく．

自然数全体の集合 $\mathbb{N}$ は 0 以上の整数とする．K を体とし，K の代数閉包を L とする．n 変数の項全体の集合を $T_n = \{x_1^{e_1} \cdots x_n^{e_n} : e_i \in \mathbb{N}\}$ とし，項 $t \in T_n$ の指数ベクトルを $e(t) \in \mathbb{N}^{1\times n}$ と表す．項順序を以下のように定義する．

定義 1.2.1 (項順序).
T_n における全順序 $\prec$ が項順序であるとは，

- 任意の $t \in T_n$ に対し $1 \prec t$
- 任意の $t_1, t_2, s \in T_n$ に対し，$t_1 \prec t_2 \Longrightarrow s \cdot t_1 \prec s \cdot t_2$

を満たすことを言う．

項順序 $\prec$ において，多項式 $f \in K[\bar{X}]$ に含まれる項で，最も項順序が大きい単項式を $\mathrm{hm}_\prec(f)$，その係数を除いた部分を $\mathrm{ht}_\prec(f)$，その係数を $\mathrm{hc}_\prec(f)$ と定義し，それぞれ**頭単項式，頭項，頭係数**と呼ぶ．項順序が明らかな場合には，$\mathrm{hm}_\prec(f)$ を単に $\mathrm{hm}(f)$ などと書くこともある．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 1.2.2 (matrix order).
項 $t_1, t_2 \in T_n$ の指数ベクトル $e(t_1), e(t_2) \in \mathbb{N}^{1\times n}$ に対し，行列 $M \in \mathbb{R}^{d\times n}$ が matrix order であるとは，

$$t_1 \prec_M t_2 \Longleftrightarrow Me(t_1) <_{\neq} Me(t_2)$$

を満たすことを言う．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．$d = 1$ のときは，通常の大小関係での比較となる．

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わかっている．

項順序を M とする．多項式 $f, g \in K[x_1, \ldots, x_n]$ に対し，f に含まれる単項式 t が $\mathrm{ht}_M(g)$ で割り切れるとする．このとき，$h = f - \frac{t}{\mathrm{ht}_M(g)} g$ 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，$h = \mathrm{nf}_g(f)$ で表す．また，多項式集合 $G = \{g_i : i \in \{1, 2, \ldots\}\} \subset K[x_1, \ldots, x_n]$ において，$\forall g_i \in G$ で f を単項簡約することを繰り返すことで 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，$h = \mathrm{nf}_G(f)$ で表す．

第 2 章

第 3 章

第 4 章

第 5 章

参考文献

[Buc06] Bruno Buchberger. Bruno buchberger’ s phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of symbolic computation*, 41(3-4):475–511, 2006.

[CKM93] Stephane Collart, Michael Kalkbrener, and Daniel Mall. The gröbner walk. *Dept. of Math., Swiss Federal Inst. of Tech*, 8092, 1993.

[FGLM93] Jean-Charles Faugere, Patrizia Gianni, Daniel Lazard, and Teo Mora. Efficient computation of zero-dimensional gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[GS93] Peter Gritzmann and Bernd Sturmfels. Minkowski addition of polytopes: computational complexity and applications to gröbner bases. *SIAM Journal on Discrete Mathematics*, 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. *Applicable Algebra in Engineering, Communication and Computing*, 8(4):257–263, 1997.

[Wei92] Volker Weispfenning. Comprehensive gröbner bases. *Journal of Symbolic Computation*, 14(1):1–29, 1992.