# 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

# 目次

# 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，多変数の連立代数方程式の解を求めるためには，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，*Gröbner basis detection*[GS93] や *structural Gröbner basis detection*[SW97] という名前が付けられており，何れも Sturmfels らによって解かれた既知の問題である．

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で 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 基本的な定義

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，$L$ を $K$ の代数閉包とする．$n$ 個の変数全体の集合を $\bar{X} = \{x_1, \ldots, x_n\}$ とし，$m$ 個のパラメータ全体の集合を $\bar{A} = \{a_1, \ldots, a_m\}$ とする．$n$ 変数の項全体の集合を $T_n = \{x_1^{e_1} \cdots x_n^{e_n} : e_i \in \mathbb{N}\}$ とする．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．項 $t \in T_n$ の指数ベクトルを $e(t) \in \mathbb{N}^n$ と表す．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 $e(t_1), e(t_2) \in \mathbb{N}^n$ 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である [Rob85] 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もわかっている．

項順序を $M$ とする．多項式 $f, g \in K[\bar{X}]$ に対し，$f$ に含まれる単項式 $t$ が $\mathrm{ht}_M(g)$ で割り切られるとする．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，有限な多項式集合 $G = \{g_i : i \in \{1, 2, \ldots\}\} \subset K[\bar{X}]$ において，$g_i \in G$ 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．

**定義 1.2.3 (S 多項式).**
項順序を $M$ とし $f, g \in K[\bar{X}]$ とする．このとき，$f, g$ の S 多項式を

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

と定義する．

# 第 2 章

# 項順序についての再考

## 2.1 はじめに

この章では，後に紹介する structural Gröbner basis detection と同じ問題設定において，Sturmfels らによる方法とは違った独自のアプローチによるアルゴリズムを考案する中で発見した新たな定理やアルゴリズムについて述べる．第 1 章にあったとおり，項順序 $M$ は column full rank な行列を考えれば，項順序を十分に定義できることが分かっているため，この章では $M$ を $n \times n$ の正方で正則な行列であると仮定する．ただし，$n$ は多項式環の変数の個数である．

目標とする問題は次の通りであった．

**問題 2.1.1.**
多項式集合 $F$ がイデアル $I = \langle F \rangle$ の Gröbner 基底となるような項順序 $M$ を求めよ．

この問題を解くにあたって，Gröbner 基底となるための必要十分条件ではなく，以下の定理 2.1.2 をもとに十分条件を考えることで，系 2.1.3 を満たすような項順序 $M$ を考える（この問題は，structural Gröbner basis detection と同じ問題設定である）．

**定理 2.1.2 (Buchberger の判定条件).**
項順序を $M$ とする．任意の多項式 $f, g \in K[\bar{X}]$ において，

$$\gcd(\mathrm{ht}_M(f), \mathrm{ht}_M(g)) = 1$$

が成り立つとき，$\mathrm{nf}_{\{f,g\}}(\mathrm{Spoly}(f, g)) = 0$ が成立する．

**系 2.1.3.**
項順序を $M$ とする．多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ に対して，イデアル $I = \langle F \rangle$ とおく．このとき，

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

が成り立つとき， $F$ は項順序 $M$ に関する $I$ の Gröbner 基底である．

つまり，ある項順序において各多項式の頭項同士が全て互いに素であれば，入力の多項式集合はそのまま Gröbner 基底である．これにより，多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ に対して問題 2.1.1 を解くためには次の 2 つのステップが必要となることがわかる．

1. 互いに素な単項式の組 $t_1, \ldots, t_k$ をそれぞれの多項式から選出する．
2. $i \in \{1, \ldots, k\}$ において，$\mathrm{ht}_M(f_i) = t_i$ となるような項順序 $M$ を求める．

## 2.2　互いに素な項の選出（Step1）

多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ に対して，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．また多項式集合 $F$ に対しても $T(F) = \bigotimes_{i=1}^{k} T(f_i)$ と定義する．集合 $V(t)$ を項 $t$ に含まれる次数 1 以上の変数全体の集合とし，集合 $T_{\mathrm{cp}}$ を

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

とする．

Step1 では，互いに素である項を探索し集合 $T_{\mathrm{cp}}$ を構成したいが，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，あらかじめ除外できることが分かっている項は除外しておき，探索のコストをできるだけ小さくしておきたい．項が除外できる理由として，次の 3 つを考える．

- 互いに素となり得ない．
- 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てしまう．
- 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てしまう．

### 2.2.1　互いに素となり得ない項の性質

まず，確実に互いに素とならない場合や，そもそも問題 2.1.1 の解が存在しない場合について考える．

**補題 2.2.1.**
多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}] \setminus K$ 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，$T_{\mathrm{cp}}$ 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，$T_{\mathrm{cp}}$ 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，

$$\begin{aligned} |V(t_i)| + \sum_j |V(t_j)| &> (n - k + 1) + (k - 1) \\ &> n \end{aligned}$$

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，$T_{\mathrm{cp}}$ 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 2.2.1 が成り立つ． □

**系 2.2.2.**
多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}] \setminus K$ において次が成り立つ．

$$n < k \Longrightarrow T_{\mathrm{cp}} = \phi$$

系 2.2.2 より，$n < k$ のときに系 2.1.3 を満たすような項順序は存在せず，問題 2.1.1 の解が存在しないことがわかり，補題 2.2.1 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できる．

### 2.2.2 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 2.2.3.**
多項式 $f$ において，$t \mid t'$ $(t \neq t')$ 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．

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．このとき，$t' \prec t$ 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． □

**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 2.2.4.**
多項式 $f_1, f_2 \in K[\bar{X}]$ 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，

$$\begin{aligned} t_1' &= r_2 t_2, \\ t_2' &= r_1 t_1 \end{aligned}$$

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 2.2.5.**
多項式 $f_1, f_2 \in K[\bar{X}]$ 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 2.2.4 とほぼ同じ手順で証明できる． □

### 2.2.3 アルゴリズムの詳細と具体例

以上より，まず補題 2.2.1 と系 2.2.2 によって，互いに素となり得ない項を除外でき，補題 2.2.3 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 2.2.4 と補題 2.2.5 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，ひとまずこの性質のみで話を進めることにする．

アルゴリズムは以下のように記述できる．

**Algorithm 1** 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 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$

**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 $M$ 又は None

1: **if** $n < k$ **then**:
2: **return** None
3: **end if**
4: 補題 2.2.1，系 2.2.2，補題 2.2.3 の条件を満たす $f_i$ の項を除外し，新たに $\tilde{F} = \{\tilde{f}_1, \ldots, \tilde{f}_k\}$ とする．
5: $T_{\tilde{F}} \leftarrow T(\tilde{F})$
6: 補題 2.2.4，補題 2.2.5 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: $T_{\mathrm{cp}}$ 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，$\mathrm{ht}_M(f_i) = t_i$ となる項順序 $M$ 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 2.2.6.**
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 2.2.3 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 2.2.4 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 2.2.7.**
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，

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

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 2.2.5 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 項順序 $M$ の導出（Step2）

求めたい項順序 $M$ を，

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

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．

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

ここで，$\ell$ は，$M$ の第 $(\ell - 1)$ 行ベクトルまでとの積が等しく，第 $\ell$ 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．

# 第 3 章

# Gröbner 基底の検出（先行研究の紹介）

## 3.1 はじめに

第 2 章では，項順序を matrix order の重み行列 $M$ で表現し，$M$ は多項式環の変数の個数 $n$ に対して $n$ 次の正方且つ正則な行列として扱っていた．本章以降は，項順序を重みベクトル $\boldsymbol{w} \in \mathbb{R}_+^n$ にて表現する．ただし，$\mathbb{R}_+$ は正の実数全体の集合とする．

**remark (ベクトルで表現された項順序について).**
項順序は column full rank な行列 $M$ だけでなくベクトル $\boldsymbol{w} \in \mathbb{R}_+^n$ でも表現可能である．ただし，$\boldsymbol{w} = (w_i : i \in \{1, 2, \ldots, n\})$ において，少なくとも $(n-1)$ 個の要素が無理数である必要がある．これは項順序の定義より，相異なる項 $t_1, t_2 \in T_n$ に対して $t_1 \neq_{\boldsymbol{w}} t_2$ を満たす必要があるためである．

ベクトル $\boldsymbol{w}$ に有理数である要素が $w_1, w_2$ の 2 つ存在していると仮定すると，

この章では，問題 2.1.1 についての Sturmfels らによる先行研究について述べる．第 2 章では同じ問題設定の中で，互いに素な項の選出を，探索数を減らせるとはいえ全探索により行ったり，求めたい項順序の計算についての効率的な計算方法については与えなかったが，先行研究では，何れにおいても効率的なアルゴリズムが与えられている．

先行研究では，この問題を *Gröbner basis detection* と名付けており，次のように定義されている．

**定義 3.1.1 (Gröbner basis detection(GBD)[GS93]).**
多項式集合 $F \subset K[\bar{X}]$ とイデアル $I = \langle F \rangle$ が与えられたとき，$F$ が $I$ の Gröbner 基底となるような項順序 $\boldsymbol{w} \in \mathbb{R}_+^n$ は存在するか．存在するならば 1 つ求めよ．

# 第 4 章

# パラメータを伴った場合への拡張

第 5 章

# パラメータ空間の分割の効率化

# 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.