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　3

1.1　研究の背景　3

1.2　基本的な定義　4

第 2 章　項順序についての再考　5

2.1　はじめに　5

2.2　互いに素な項の選出（Step1）　6

2.3　項順序 M の導出（Step2）　9

第 3 章　Gröbner 基底の検出（先行研究の紹介）　10

3.1　はじめに　10

3.2　Gröbner basis detection[GS93]　10

3.3　structural Gröbner basis detection[SW97]　14

第 4 章　パラメータを伴った場合への拡張　18

第 5 章　パラメータ空間の分割の効率化　19

参考文献　20

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．また，多項式集合 F に関して，$\mathrm{HM}_\prec(F) = \{\mathrm{HM}_\prec(f_i) \ : \ f_i \in F\}$ と定義する（$\mathrm{HT}_\prec(F), \mathrm{HC}_\prec(F)$ についても同様に定義する）．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 多項式を次のように定義する．

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

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，後に説明する 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_{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_{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_{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_{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_{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_{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，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．

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．仮に $\boldsymbol{w}$ に有理数の要素が 2 つ以上存在してしまうと，$\boldsymbol{w}$ が $\mathbb{Z}$ 上一次従属となってしまい，項順序の定義である「相異なる項 $t_1, t_2 \in T_n$ に対して $t_1 \neq_{\boldsymbol{w}} t_2$」を満たすことができなくなってしまうためである．

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．

問題 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．

また, GBD の問題を Buchberger の判定条件（定理 2.1.2）により簡単にしたものが, 次の *structural Gröbner basis detection* である．

問題 3.1.2 (structural Gröbner basis detection(SGBD)[SW97]).
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，$\mathrm{HT}_{\boldsymbol{w}}(F)$ に含まれる全ての項が互いに素であるような項順序 $\boldsymbol{w} \in \mathbb{R}_+^n$ は存在するか．存在するならば 1 つ求めよ．

3.2 Gröbner basis detection[GS93]

Gröbner basis detection の問題を解くあたって，多項式集合の項順序に幾何的な解釈を与えることで，項順序の同値類に分けて考えることができるようになる．ここで，多項式集合 F に対して，項順序 $\boldsymbol{w_1}, \boldsymbol{w_2}$ は，

$\mathrm{HT}_{\boldsymbol{w_1}}(F) = \mathrm{HT}_{\boldsymbol{w_2}}(F)$ を満たすときに同値であるという．まずは前提とする定義を与える．

3.2.1 前提とする定義

定義 3.2.1 ([Fre09, p8,9, Definition3.1]).
集合 $\mathcal{U}, \mathcal{V} \subseteq \mathbb{R}^d$ に対して，

- $\mathcal{U}$ が**凸** *(convex)* であるとは，

$$\forall \boldsymbol{u}, \boldsymbol{v} \in \mathcal{U},\ \lambda \in \mathbb{R},\ 0 \leq \lambda \leq 1,\ \lambda \boldsymbol{u} + (1-\lambda)\boldsymbol{v} \in \mathcal{U}$$

  を満たすときをいう．
- **凸多面体** *(convex polyhedron)* とは，有限個の半空間の共通部分として得られる凸型の集合である．
- 集合 $\mathcal{V}$ の**凸包** *(convex hull)* とは，その集合を含む $\mathbb{R}^d$ のすべての凸部分集合の共通部分と定義される．
- $\mathcal{U}$ は有界な多面体である場合，**超多面体** *(polytope)* と呼ばれる．すべての polytope は，有限の点の集合の convex hull である．
- $\mathbb{R}^d$ の凸多面体 (convex polyhedron) の**円錐** *(cone)*C は，

$$\forall \boldsymbol{u}, \boldsymbol{v} \in C,\ \lambda \in \mathbb{R}_{\geq 0},\ \boldsymbol{u} + \boldsymbol{v}, \lambda \boldsymbol{u} \in c$$

  のように定義される．

2 つ以上の polytope の和を次のように定義する．

定義 3.2.2 (Minkowski 和, [GS93, p247]).
2 つの polytope $P_1, P_2 \subset \mathbb{R}^n$ に対して，*Minkowski* **和** $P_1 + P_2$ を

$$P_1 + P_2 = \{x \in \mathbb{R}^n \ :\ \exists x_1 \in P_1, \exists x_2 \in P_2, x = x_1 + x_2\}$$

のように定義する．Minkowski 和は，可換であり結合法則が成り立つため，2 つ以上の polytope にも自然に一般化することができる．

変数の集合 $\bar{X}$ に対し，$\bar{X}$ の任意の指数ベクトル $\alpha \in \mathbb{N}^n$ とし，$K[\bar{X}]$ の任意の単項式を X^α と表現する．また，ベクトル $\boldsymbol{u}, \boldsymbol{v}$ の内積を $(\boldsymbol{u}, \boldsymbol{v})$ と表す．集合 $\mathbb{R}_-$ は 0 以下の実数全体の集合である．

定義 3.2.3 (Newton polytope).
多項式 $f = \sum_{i=1}^{t} c_i X^{\alpha_i}$ の *Newton polytope* $\mathcal{N}(f)$ を，$\mathbb{R}^n$ における単項式の convex hull で定義する．つまり，

$$\mathcal{N}(f) = \mathrm{conv}\{\alpha_1, \ldots, \alpha_t\}$$

である．また，多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ の Newton polytope を，それぞれの多項式の Newton polytope の Minkowski 和

$$\mathcal{N}(F) = \mathcal{N}(f_1) + \cdots + \mathcal{N}(F)$$

で定義する．また，多項式 f の *affine Newton polyhedron* $\mathcal{N}_{\mathrm{aff}}(f)$ を Minkowski 和

$$\mathcal{N}_{\mathrm{aff}}(f) = \mathcal{N}(f) + \mathbb{R}_-^n$$

で定義する．多項式集合 F についても同様に，

$$\mathcal{N}_{\mathrm{aff}}(F) = \mathcal{N}(F) + \mathbb{R}_-^n$$

で定義する．

remark 3.2.4.
多項式の Newton polytope の Minkowski 和は，多項式の積の Minkowski 和と対応している．つまり，多項式 $f_1, \ldots, f_k \subset K[\bar{X}]$ に対して，

$$\mathcal{N}(f_1) + \mathcal{N}(f_2) + \cdots + \mathcal{N}(f_k) = \mathcal{N}(f_1 \cdots f_k)$$

である．

ここで，例として多項式 $f = x^3y^2 + xy^3 + xy \subset K[x, y]$ の Newton polytope と affine Newton polyhedron を図示する．

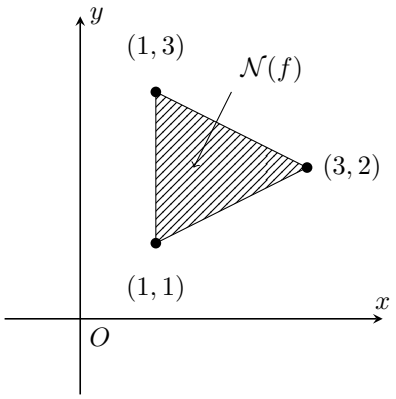

図 3.1　Newton polytope $\mathcal{N}(f)$

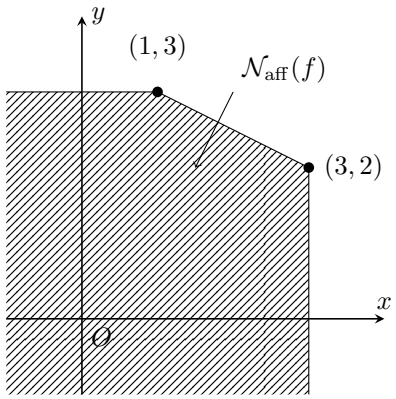

図 3.2　affine Newton polyhedron $\mathcal{N}_{\mathrm{aff}}(f)$

図 3.2.1 のように，Newton polytope は単に多項式 f に含まれる項の指数ベクトルを頂点とした集合となっている．対して，図 3.2.1 のように，affine Newton polyhedron では，$\mathcal{N}(f)$ と $\mathbb{R}^2_-$ との Minkowski 和を取ることで，”左下”全体を含んだ領域を取る無限集合となっているが，頂点に着目すると，それに伴って”左下”にあった頂点 $(1, 1)$ がなくなっている．これは，多項式の中で「先頭項になりそうにない次数の低い項」を取り除く操作に対応できる．この例では，項 xy は項順序の定義から先頭項にはならず，affine Newton polyhedron を取ることでそのような項を検出することができることを意味している．

3.2.2　Gröbner 基底と Newton polytope

多項式集合が Gröbner 基底となるためには，Buchberger アルゴリズムの計算過程にもある通り，全ての S ペアが 0 へ簡約される必要がある．その際に S 多項式の計算を行うためには，多項式の先頭項を確定させる必要がある．もし，多項式集合における項順序の同値類の数が分かれば，それぞれの適当な代表元において，全ての S ペアの簡約が 0 となるかどうかを調べることで，与えられた多項式集合がそのまま Gröbner 基底となるような項順序が存在するのかどうかを確かめることができる．次の定理では，項順序の同値類を，先程定義した多項式集合の affine Newton polyhedron で記述するものとなっている．

定理 3.2.5 ([GS93, p263, Proposition3.2.1]).
多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ に対して，affine Newton polyhedron $\mathcal{N}_{\mathrm{aff}}(F)$ の各頂点は，F に関する項順序の同値類と一対一に対応している．

証明. 多項式 $f_i \in F$ は $f_i = \sum_{j=1}^{t_i} c_{ij} X^{\alpha_{ij}}$ で表されるとする．2 つの異なる項順序 $\boldsymbol{w_1}, \boldsymbol{w_2} \in \mathbb{R}^n$ は多項式集合

F が任意の $i \in \{1, \ldots, k\}$ に対して

$$\max\{(\alpha_{ij}, \boldsymbol{w_1}) \ : \ 1 \leq j \leq t_i\} = \max\{(\alpha_{ij}, \boldsymbol{w_2}) \ : \ 1 \leq j \leq t_i\}$$

を満たすときに限り等しくなる．以下のような項のインデックスに関する集合 $\mathcal{J}$ を考える．

$$\mathcal{J} = \{\boldsymbol{j} = (j_1, \ldots, j_k) \in \mathbb{N}^k \ : \ \forall i \in \{1, \ldots, k\},\ 1 \leq j_i \leq t_i\}$$

$\mathcal{J}$ の各要素 $\boldsymbol{j}$ に polyhedral cone $C_{\boldsymbol{j}}$ を

$$C_{\boldsymbol{j}} = \{\boldsymbol{w} \in \mathbb{R}^n \ : \ \forall i \in \{1, \ldots, k\},\ \forall j \in \{1, \ldots, t_i\} \setminus \{j_i\},\ (\alpha_{ij_i}, \boldsymbol{w}) > (\alpha_{ij}, \boldsymbol{w})\}$$

のように定義する．重みベクトル $\boldsymbol{w}$ が $C_{\boldsymbol{j}}$ に含まれるのは，$\boldsymbol{j}$ でインデックス付けされた単項式が $\boldsymbol{w}$ に関する F の先頭項である場合に限られる．したがって，F に関する項順序の同値類は、空ではない $C_{\boldsymbol{j}}$ と一対一に対応している．

Newton polytope $\mathcal{N}(F)$ は、点 $\alpha_{\boldsymbol{j}} = \sum_{i=1}^{k} \alpha_{ij_i}$ の convex hull である (ただし $\boldsymbol{j} = (j_1, \ldots, j_k) \in \mathcal{J}$)．また，affine Newton polyhedron $\mathcal{N}_{\mathrm{aff}}(F)$ の頂点の集合は，$\mathcal{N}(F)$ の頂点の部分集合である．頂点 $\alpha_{\boldsymbol{j}}$ は $\mathbb{R}^n$ への線型汎関数 ($\mathbb{R}_+^d \to \mathbb{R}_+$) が最大値である場合に先頭項となるため，その場合に限って $\mathcal{N}_{\mathrm{aff}}(F)(= \mathcal{N}(F) + \mathbb{R}_-^n)$ の頂点となる．これは、$(\alpha_{\boldsymbol{j}}, \boldsymbol{w}) = \sum_{i=1}^{k} \alpha_{j_i} \boldsymbol{w}$ が他のすべての $\boldsymbol{j'} \in \mathcal{J}$ に対して $(\alpha_{\boldsymbol{j'}}, \boldsymbol{w})$ より大きいような重みベクトル $\boldsymbol{w}$ が存在することを意味している．しかし，このとき $\boldsymbol{w} \in C_{\boldsymbol{j}}$ となる．よって，空でない $C_{\boldsymbol{j}}$ は polyhedron $\mathcal{N}_{\mathrm{aff}}(F)$ の頂点への法線円錐 (the normal cones to the vertices) であることを示した。 □

特に，多項式集合が斉次のとき，次のような系を得られる．

系 3.2.6 ([GS93, p264, Corollary3.2.2]).
斉次な多項式集合 $F = \{f_1, \ldots, f_k\}$ に対して，Newton polytope $\mathcal{N}(F)$ の各頂点は，F に対する項順序の同値類と一対一対応している．

証明. f_i が R_i-斉次であるとし，$R = R_1 + \cdots + R_k$ とする．このとき，Newton polytope $\mathcal{N}(F)$ は affine 超平面 (affine hyperplane)

$$\left\{ \boldsymbol{y} \in \mathbb{R}^n \ : \ \sum_{j=1}^{n} y_j = R \right\}$$

に含まれる．$\mathcal{N}(F)$ のある頂点 $\alpha_{\boldsymbol{j}}$ があるベクトル $\boldsymbol{w}$ に対して極大 (extremal) であるならば，それは任意の $c \in \mathbb{R}_+$ に対して $\boldsymbol{w} + (c, c, \ldots, c)$ の方向でも極大 (extremal) である．

$$(\because \forall \alpha \in \mathcal{N}(F),\ (\alpha, \boldsymbol{c}) = cR = (const)\ )$$

c を適切にとったときに，$\alpha_{\boldsymbol{j}}$ は $\mathcal{N}_{\mathrm{aff}}(F)$ の頂点でもあることを示す．

$$\beta \in \mathcal{N}_{\mathrm{aff}}(F),\ \gamma \in \mathbb{R}_-^n,\ \beta = \alpha + \gamma$$

とする．$\mathcal{N}_{\mathrm{aff}}(F) \subseteq \mathcal{N}(F)$ より，$\beta \in \mathcal{N}(F)$．故に，$(\alpha_{\boldsymbol{j}}, \boldsymbol{c}) = (\beta, \boldsymbol{c}) = cR$．よって，

$$(\boldsymbol{w} + \boldsymbol{c}, \beta) = (\boldsymbol{w}, \beta) + cR$$
$$(\boldsymbol{w} + \boldsymbol{c}, \alpha_{\boldsymbol{j}} + \gamma) = (\boldsymbol{w}, \alpha_{\boldsymbol{j}}) + cR + (\boldsymbol{w}, \gamma) + (\boldsymbol{c}, \gamma)$$

式 (3.2.2) と式 (3.2.2) は等しくなるため，

$$(\boldsymbol{w}, \gamma) + (\boldsymbol{c}, \gamma) = \boldsymbol{0}$$

よって，

$$\gamma = \mathbf{0}$$
$$\Longleftrightarrow \alpha_{\boldsymbol{j}} = \beta \in \mathcal{N}_{\mathrm{aff}}(F)$$

$\alpha_{\boldsymbol{j}} \in \mathcal{N}_{\mathrm{aff}}(F)$ がわかったため，定理 3.2.5 と同様に導ける． □

これらの定理により，Gröbner basis detection は次のように解くことができる．多項式集合 F に対して，

- affine Newton polyhedron $\mathcal{N}_{\mathrm{aff}}(F)$ を求める．F が斉次の場合は Newton polytope $\mathcal{N}(F)$ を考える．
- その頂点の数をして項順序の同値類の数がわかる．
- 適当な代表元において，S 多項式のペアが全て 0 に簡約化されるかどうかを調べ，そのような項順序が GBD で求めたいものである．

具体的には，定理 3.2.5 の証明より，次の図のように各頂点を結ぶ辺の法線ベクトルで区切られた領域が，一つの同値類に対応している．

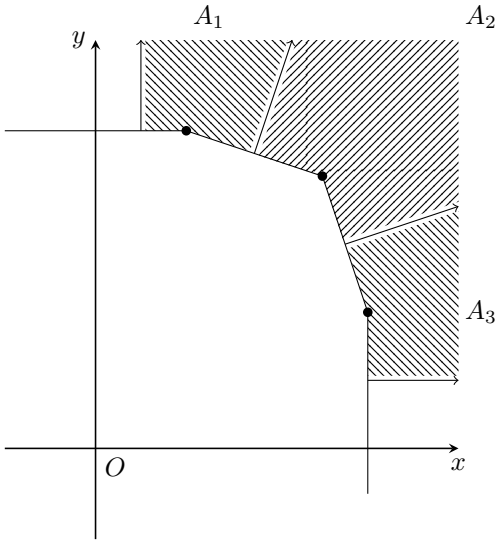

図 3.3　項順序の同値類に対応している領域

3.3　structural Gröbner basis detection[SW97]

Gröbner basis detection の問題は，結局は項順序の同値類の数だけ S 多項式の計算をする必要があり，Buchberger アルゴリズム等の前処理としての役割には適していない．そこで，Buchberger の判定条件を用いて問題を簡略化したものが問題 3.1.2 の structural Gröbner basis detection である．

3.3.1　$n = k$ のとき

まず，変数の個数 n と多項式集合の濃度 k が等しいときを考える．後になってわかることだが，$n \neq k$ のときも，この場合のアルゴリズムに帰着して考えることができる．

次のような多項式を例に考える．

例 3.3.1.
多項式集合 $F = \{f_1, \ldots, f_n\}$ を n 変数の多項式環 $K[\bar{X}]$ の部分集合とし，

$$f_i = X_1^{a_{i1}} + \cdots + X_n^{a_{in}} - 1$$

と表されるとものとする．

このような多項式集合 F に対して，項順序 $\boldsymbol{w} \in \mathbb{R}_+^n$ における各多項式の先頭項の集合は，

$$\mathrm{HT}_{\boldsymbol{w}}(F) = \{X_{\varphi(1)}^{a_{1\varphi(1)}}, \ldots, X_{\varphi(i)}^{a_{i\varphi(i)}}\}$$

のように各多項式の先頭項のインデックスを表す写像 $\varphi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ によって表すことができる．SGBD の問題を解くためには，この $\mathrm{HT}_{\boldsymbol{w}}(F)$ を適切に定める必要があるが，写像 φ で表現可能な $n!$ 通りの中から探さなくてはならない．

次の補題により，$\mathrm{HT}_{\boldsymbol{w}}(F)$ は $n!$ 通りのうち 1 通りに絞られることがわかる．

補題 3.3.2 ([SW97, Lemma5]).
例 3.3.1 の条件を満たす多項式集合 F に対して，

$$\prod_{i=1}^{n} a_{i\rho(i)} \geq \prod_{i=1}^{n} a_{i\varphi(i)}$$

を満たすような ρ は存在しない．

証明．f_i の項 $X_{\varphi(i)}^{a_{i\varphi(i)}}$ を先頭項とするような項順序を $\boldsymbol{w} = (w_i)_{i \in \{1,\ldots,n\}} \in \mathbb{R}_+^n$ とし，それ以外の任意の像を $\rho \neq \varphi$ とする．項順序 $\boldsymbol{w}$ の下で各多項式の先頭項は $X_{\varphi(i)}^{a_{i\varphi(i)}}$ となるので，任意の $i \in \{1, 2, \ldots, n\}$ に対して

$$w_{\varphi(i)} a_{i\varphi(i)} > w_{\rho(i)} a_{i\rho(i)}$$

となる．つまり，$\varphi(i) \neq \rho(i)$ を満たす i が少なくとも 1 つ存在する．従って，n 個の不等式の総積によって，以下の式が得られる．

$$\begin{aligned} &\prod_{i=1}^{n} w_{\varphi(i)} a_{i\varphi(i)} > \prod_{i=1}^{n} w_{\rho(i)} a_{i\rho(i)} \\ \Longleftrightarrow &\prod_{i=1}^{n} w_i a_{i\varphi(i)} > \prod_{i=1}^{n} w_i a_{i\rho(i)} \end{aligned}$$

両辺を $\prod_{i=1}^{n} w_i > 0$ で割ると，

$$\prod_{i=1}^{n} a_{i\rho(i)} < \prod_{i=1}^{n} a_{i\varphi(i)}$$

□

この補題により，SGBD を解くために先頭項候補は，総積 $\prod_{i=1}^{n} a_{i\varphi(i)}$ を最大化するような項の組

$$X_{\varphi(1)}^{a_{1\varphi(1)}}, \ldots, X_{\varphi(n)}^{a_{n\varphi(n)}}$$

であることがわかる．このような項の組は二部グラフの最大マッチング問題を解くことによって求めることができる（詳細は後述のアルゴリズム 3.3.1 を参照）．

次に，実際にそのような項の組 $X_{\varphi(1)}^{a_{1\varphi(1)}}, \ldots, X_{\varphi(n)}^{a_{n\varphi(n)}}$ がそれぞれの先頭項となるような項順序 $\boldsymbol{w} \in \mathbb{R}_+^n$ を求める方法を考える．以下の補題により，これは線形計画問題を解くことで求めることができることがわかる．

補題 3.3.3 ([SW97, Lemma6]).
多項式集合 F を例 3.3.1 の条件を満たすような集合とし，X^{α_i} を多項式 $f_i \in F$ の項とする．任意の $i \in \{1,\dots,n\}$ と $X^{\beta_i} \neq X^{\alpha_i}$ を満たす f_i の任意の項 X^{β_i} に対して，指数ベクトルの差のベクトル $\alpha_i - \beta_i$ を列として持つ行列を Γ とする．このとき，$\mathrm{HT}_{\boldsymbol{w}}(f_i) = X^{\alpha_i}$ を満たすような項順序 $\boldsymbol{w} \in \mathbb{R}^n_+$ が唯一存在し，連立不等式 $\Gamma\boldsymbol{w} > 0, \boldsymbol{w} > 0$ を解くことによって求めることができる．

証明. $\mathrm{HT}_{\boldsymbol{w}}(f_i) = X^{\alpha_i}$ という仮定から，行列 Γ と $\boldsymbol{w}$ との積は正となる必要がある． □

これらの補題をもとに，$n = k$ のときに SGBD を解くアルゴリズムは以下のように記述することができる．尚，SGBD の条件を満たすような項順序が存在しなかった場合には，ゼロベクトルを返すようにしている．

Algorithm 2 solving structural Gröbner basis detection for $n = k$ [SW97, Algorighm7]

input: 多項式集合 $F \subset K[\bar{X}]$

output: F が $\langle F\rangle$ の Gröbner 基底となるような項順序 $w \in \mathbb{R}^n_+$ or ゼロベクトル $\mathbf{0} \in \mathbb{R}^n$

1: **for** $1 \le i, j \le n$ **do**
2: **if** $X_j^{\alpha} \notin T(f_i) \quad (\alpha \neq 0)$ **then**
3: $a_{ij} \leftarrow 0$
4: **end if**
5: $a_{ij} \leftarrow (f_i$の単項式 X_jの最大指数$)$
6: **if** $X_j^{a_{ij}} X^{\alpha} \in T(f_i) \quad (\alpha \neq 0)$ **then**
7: $a_{ij} \leftarrow 0$
8: **end if**
9: **end for**
10: 頂点が $2n$ 個ある二部グラフ $B = \{\bar{V}, \bar{E}\}$ を次のように構成

$$\bar{V} = \{u_1,\dots,u_n,v_1,\dots,v_n\}, \quad (u_i, v_i) \in \bar{E} \quad (a_{ij} > 0 \text{ のときのみ})$$

11: B の最大マッチング M を求める．
12: **if** $|M| < n$ **then**
13: **return** $\mathbf{0} \in \mathbb{R}^n$
14: **else**
15: $M = \{(u_i, v_{\varphi(i)}) \ : \ i \in \{1,2,\dots,n\}\}$
16: **end if**
17: 行列 Γ を補題 3.3.3 と同じように構成し，

$$\begin{cases} \Gamma\boldsymbol{w} > 0 \\ \boldsymbol{w} > 0 \end{cases}$$

を解く．
18: **return** $\boldsymbol{w}$

定理 3.3.4.
アルゴリズム 3.3.1 は正当性と有限停止性を有する．

証明. まず，1 行目の for 文において，入力の多項式を例 3.3.1 の条件を満たすような項のみを残すように変換している．10 行目〜16 行目は補題 3.3.2 に基づいて二部グラフを構成し，17 行目では補題 3.3.3 に基づいて行列を構成し，線形計画問題を解いている． □

このアルゴリズムでは，大きく分けて

1. 単項のみから成り，且つ倍単項式が同じ多項式に存在しないような項のみを残す
2. 二部グラフの最大マッチング問題を解く
3. 線形計画問題を解く

という 3 つのステップがある．2 つ目のステップでは，Hungarian method[PL86] にて，3 つ目のステップでは Khachian's Ellipsoid method[Sch98] などの方法を採用することで，アルゴリズム全体は多項式時間で解くことができる [SW97].

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.

[Fre09] Jacqueline Freeke. Linking groebner bases and toric varieties, 2009.

[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.

[PL86] Michael D Plummer and László Lovász. *Matching theory*. Elsevier, 1986.

[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.

[Sch98] Alexander Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1998.

[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.