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

大島谷 遼*, 長坂 耕作

神戸大学大学院・人間発達環境学研究科

2021年12月21日（火）

去年の発表

Title：グレブナー基底の項順序についての再考

- 多項式集合 F がそのまま Gröbner 基底となる項順序がほしい
- Buchberger の判定条件（頭項が全て互いに素なら，F はそのまま Gröbner 基底）をもとに独自のアルゴリズムを考案（途中）
- 例：

$$F = \{x^2y + z,\ xyz + z^4\} \subset K[x, y, z]$$

去年の発表

Title：グレブナー基底の項順序についての再考

- 多項式集合 F がそのまま Gröbner 基底となる項順序がほしい
- Buchberger の判定条件（頭項が全て互いに素なら，F はそのまま Gröbner 基底）をもとに独自のアルゴリズムを考案（途中）
- 例：

$$F = \{x^2y + z,\ xyz + z^4\} \subset K[x, y, z]$$

- 既知の問題と判明

"Gröbner basis detection[GS93]"

（野呂先生のご指摘）

今日の発表

1. そのまま Gröbner 基底となるような項順序（先行研究の紹介）
   - 項順序選択の重要性
   - Gröbner 基底と Newton polytope
   - Buchberger の判定条件に基づいた Gröbner 基底の構造的な検出
2. パラメータを伴う場合への拡張
   - 直接的方法
   - パラメータ空間の分割の効率化

記法

- K：体
- L：K の代数閉包
- $\bar{X}$：変数全体の集合 $(\{x_1, \ldots, x_n\})$
- $\bar{A}$：パラメータ全体の集合 $(\{a_1, \ldots, a_m\})$
- $\sigma_{\bar{a}}$：$K[\bar{X}, \bar{A}] \to L[\bar{X}]$ を各 a_i への自然な代入（specialization homomorphism）
- $V(f)$：多項式 f の Affine 多様体
- $T_{\bar{X}}(f)$：多項式 f に含まれる $\bar{X}$ に関する項全体の集合
- $\mathrm{HT}_{\boldsymbol{w}}(f)$：項順序 $\boldsymbol{w}$ における多項式 f の頭項
- δ_{ij}：Kronecker delta

Gröbner 基底について

定義 2.1 (Gröbner 基底).

多項式集合 $F \subset K[\bar{X}]$ と F が生成するイデアル I に関して，

$$\langle \mathrm{HT}_{\prec}(I) \rangle = \langle \mathrm{HT}_{\prec}(f_1), \ldots, \mathrm{HT}_{\prec}(f_k) \rangle$$

が満たされるとき，F を項順序 $\prec$ に関する Gröbner 基底であるという．

項順序の例 ($x \succ y \succ z$ のとき)

- 辞書式順序（LexOrder）
  - 例：$x^2yz^2 \succ xy^3z, \quad x \succ y^3z^8$
- 全次数辞書式順序（GrLexOrder）
  - 例：$x^2yz^2 \succ xy^3z, \quad x \prec y^3z^8$
- 全次数逆辞書式順序（GrevLexOrder）
  - 例：$x^2yz^2 \prec xy^3z, \quad x \prec y^3z^8$

matrix order

定義 2.2 (matrix order).

- M：列数 n の column full rank な行列 (or ベクトル)
- t_1, t_2：項 $(\in K[\bar{X}])$
- $e(t)$：項 t の指数ベクトル

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

例

$<_{\neq}$ や $>_{\neq}$ でベクトル同士の，等しくない最初の成分での大小比較を表す.

$$(2, 3, 30) <_{\neq} (2, 5, 3)$$

任意の項順序は matrix order で表現可能 [Rob85].

Gröbner 基底計算では項順序の選択が重要

計算速度 (速さ)

$$\text{LexOrder} <<< \text{GrevLexOrder}$$

連立方程式の求解での例

- LexOrderでの Gröbner 基底を計算 (遅)
- GrevLexOrder での Gröbner 基底を計算 (速)

  → FGLM アルゴリズム [FGLM93] などの基底変換アルゴリズムによりLexOrderでの Gröbner 基底を計算

顕著な例

例

- $F = \{f_1 = xy + yz,\ f_2 = x^2 + y + z\} \subset K[x, y, z]$
- $\langle F \rangle$ での Gröbner 基底を求めたい (項順序は何でもいい).

- $x \succ y \succ z$
- LexOrder, GrLexOrder, GrevLexOrder

$$G = \left\{ \begin{array}{l} g_1 = xy + yz, \\ g_2 = x^2 + y + z, \\ g_3 = y^2 + yz^2 + yz \end{array} \right\}$$

顕著な例

例

- $F = \{f_1 = xy + yz,\ f_2 = x^2 + y + z\} \subset K[x, y, z]$
- $\langle F \rangle$ での Gröbner 基底を求めたい (項順序は何でもいい).

- $x \succ y \succ z$
- LexOrder, GrLexOrder, GrevLexOrder

$$G = \left\{ \begin{array}{l} g_1 = xy + yz, \\ g_2 = x^2 + y + z, \\ g_3 = y^2 + yz^2 + yz \end{array} \right\}$$

- $z \succ y \succ x$
- GrLexOrder, GrevLexOrder

$$G = \left\{ \begin{array}{l} g_1 = xy + yz, \\ g_2 = x^2 + y + z \end{array} \right\}$$

顕著な例

例

- $F = \{f_1 = xy + yz,\ f_2 = x^2 + y + z\} \subset K[x, y, z]$
- $\langle F \rangle$ での Gröbner 基底を求めたい (項順序は何でもいい).

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

$$G = \left\{ \begin{array}{l} g_1 = xy + yz, \\ g_2 = x^2 + y + z, \\ g_3 = y^2 + yz^2 + yz \end{array} \right\}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

$$G = \left\{ \begin{array}{l} g_1 = xy + yz, \\ g_2 = x^2 + y + z \end{array} \right\}$$

顕著な例

例

- $F = \{f_1 = xy + yz,\ f_2 = x^2 + y + z\} \subset K[x, y, z]$
- $\langle F \rangle$ での Gröbner 基底を求めたい (項順序は何でもいい).

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

$$G = \left\{ \begin{array}{l} g_1 = xy + yz, \\ g_2 = x^2 + y + z, \\ g_3 = y^2 + yz^2 + yz \end{array} \right\}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

$$G = \left\{ \begin{array}{l} g_1 = xy + yz, \\ g_2 = x^2 + y + z \end{array} \right\}$$

F がそのまま Gröbner 基底に！

Gröbner basis detection

Gröbner basis detection(GBD)[GS93]

多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ 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.

Gröbner basis detection

Gröbner basis detection(GBD)[GS93]

多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ 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．

- 全ての Spoly のペアがゼロ簡約される
- HT を確定させる必要がある
- $\rightarrow F$ の HT は何種類ある？

f に関して $\boldsymbol{w_1} \equiv \boldsymbol{w_2}$ とは，

$$\mathrm{HT}_{\boldsymbol{w_1}}(f) = \mathrm{HT}_{\boldsymbol{w_2}}(f)$$

Gröbner basis detection

Gröbner basis detection(GBD)[GS93]

多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ 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．

- 全ての Spoly のペアがゼロ簡約される
- HT を確定させる必要がある
- $\rightarrow F$ の HT は何種類ある？

f に関して $\boldsymbol{w_1} \equiv \boldsymbol{w_2}$ とは，

$$\mathrm{HT}_{\boldsymbol{w_1}}(f) = \mathrm{HT}_{\boldsymbol{w_2}}(f)$$

指数ベクトルの convex hull を考えることで，
F の項順序の同値類を分けられる

前提 1

定義 3.1 (前提とする定義).

- 集合 $\mathcal{U}$ が convex

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

- 集合 $\mathcal{V}$ が convex polyhedron

$\iff$ 有限個の半空間の共通部分として得られる凸集合

- 集合 $\mathcal{U}$ の covex hull $\mathcal{V}$

$\iff \mathcal{U}$ を含む全ての凸部分集合の共通部分

- 集合 $\mathcal{V}$ が polytope

$\iff$ 有限個の点の集合の convex hull

前提 2(Minkowski 和と Newton polytope)

定義 3.2 (Minkowski 和).

2 つの polytope $P_1, P_2 \subset \mathbb{R}^n$ に対して，Minkowski 和 $P_1 + P_2$ を

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

※ Minkowski 和は可換かつ結合法則が成り立つため，2 つ以上の polytope にも自然に一般化可能.

定義 3.3 (Newton polytope).

- 多項式 $f = \sum_{i=1}^{t} c_i X^{\alpha_i}$ のNewton polytope $\mathcal{N}(f)$ を，

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

- 多項式集合 $F = \{f_1, \ldots, f_k\}$ の Newton polytope $\mathcal{N}(F)$ を，

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

前提3(affine Newton polyhedron)

定義 3.4 (affine Newton polyhedron).

多項式 f や多項式集合 F のaffine Newton polyhedron $\mathcal{N}_{\mathrm{aff}}(f)$ を

$$\mathcal{N}_{\mathrm{aff}}(f) = \mathcal{N}(f) + \mathbb{R}^n_- \cup \{0\}$$

や

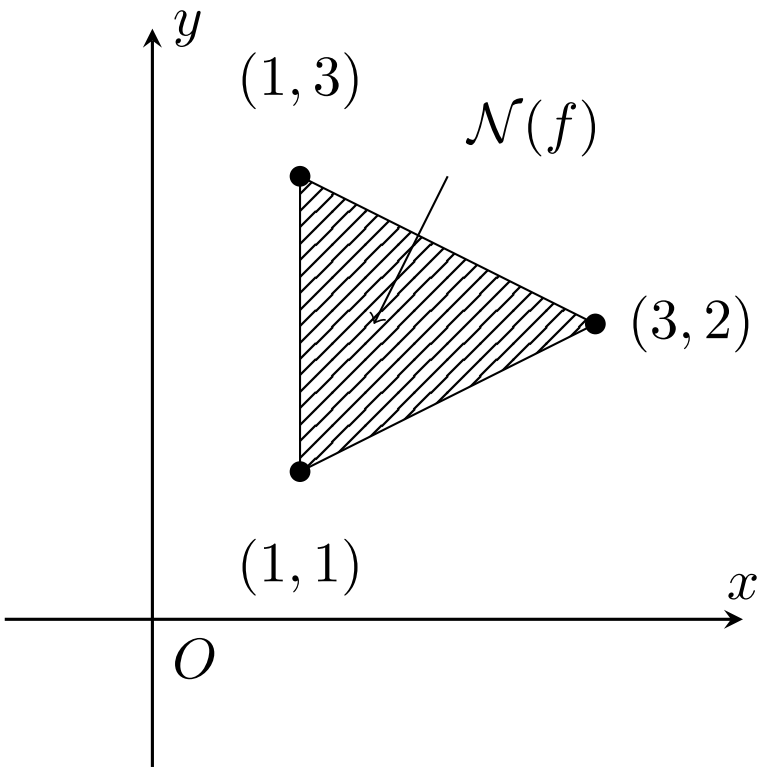
$$\mathcal{N}_{\mathrm{aff}}(F) = \mathcal{N}(F) + \mathbb{R}^n_- \cup \{0\}$$

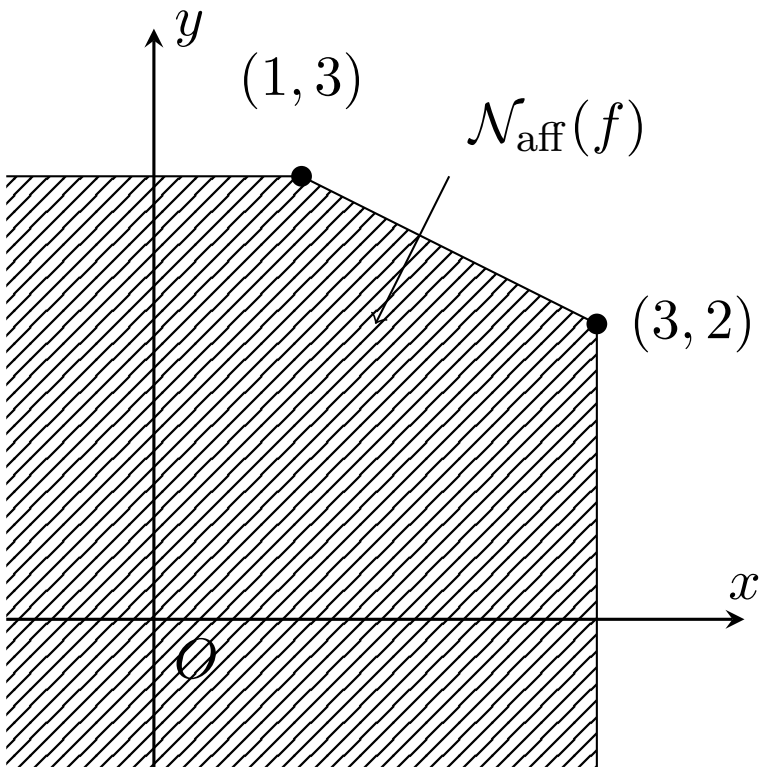
で定義.

affine Newton polyhedron の例

例

- $\mathcal{N}_{\mathrm{aff}}(f) = \mathcal{N}(f) + \mathbb{R}^n_-$
- $f = x^3y^2 + xy^3 + xy \subset K[x, y]$





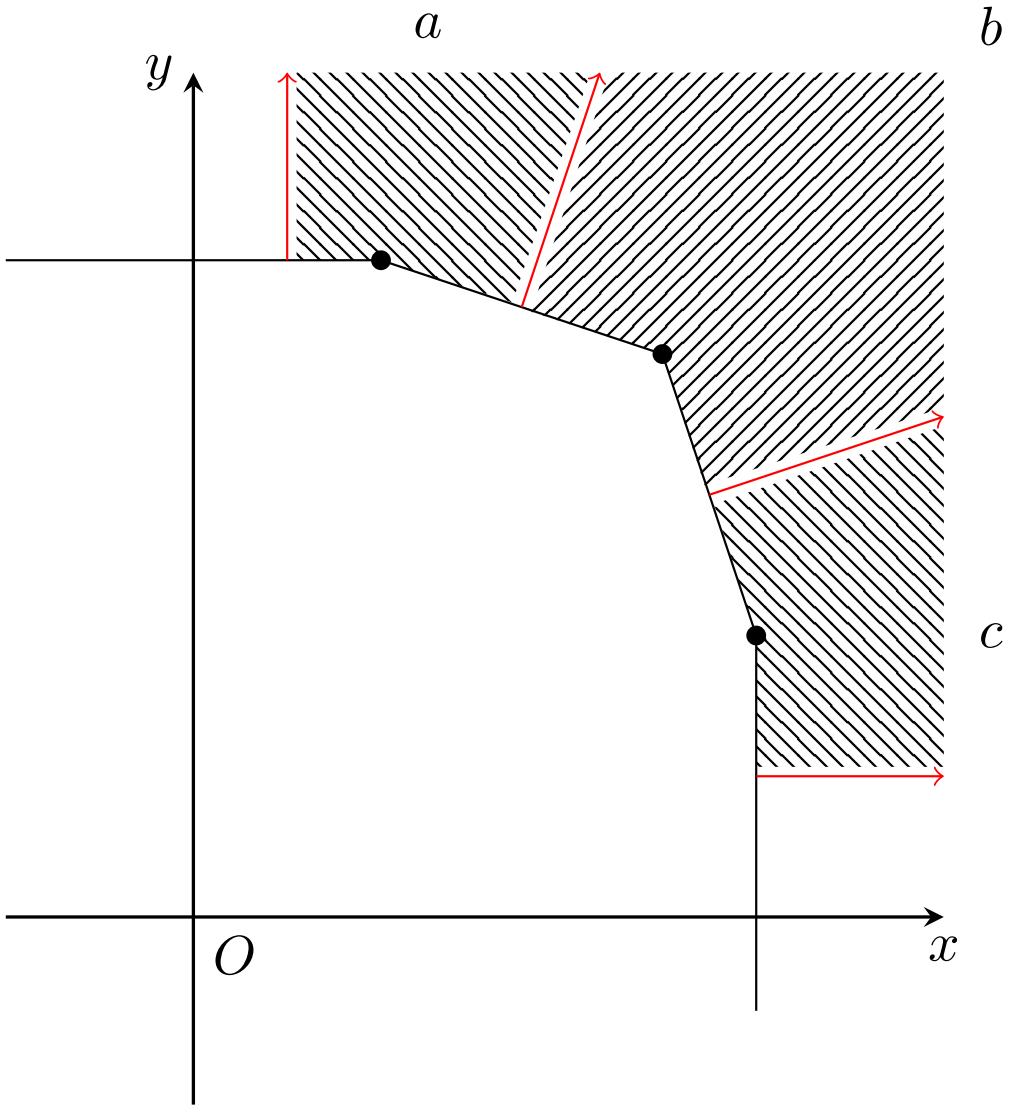
Gröbner 基底と affine Newton polyhedron

定理 3.5 ([GS93, Proposition3.2.1]).

多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ の *affine Newton polyhedron* $\mathcal{N}_{\mathrm{aff}}(F)$ の頂点は，F の項順序の同値類に対応している．

- この定理より，F の項順序の同値類の数がわかる．

Gröbner 基底と affine Newton polyhedron



Gröbner 基底と affine Newton polyhedron

定理 3.5 ([GS93, Proposition3.2.1]).

多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ の *affine Newton polyhedron* $\mathcal{N}_{\mathrm{aff}}(F)$ の頂点は，F の項順序の同値類に対応している.

- この定理より，F の項順序の同値類の数がわかる.
- 同値類の数だけ「そのまま Gröbner 基底となっているか」を確かめる.
- $\rightarrow$ S-polynomial が全てゼロ簡約される項順序の同値類を（全）探索する.

もっと手軽に Gröbner基底を検出したい

Structural Gröbner basis detection

Gröbner basis detection(GBD)[GS93]

多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ 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．

$\Downarrow$

Buchberger の判定条件
（HT が互いに素 $\Rightarrow$Gröbner 基底）
によって，問題を簡単に．

Structural Gröbner basis detection

Gröbner basis detection(GBD)[GS93]

多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ 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．

$\Downarrow$

Buchberger の判定条件
（HT が互いに素 $\Rightarrow$Gröbner 基底）
によって，問題を簡単に．

Structural Gröbner basis detection(SGBD)[SW97]

多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ 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．

(去年の発表と同じ問題設定)

SGBD の例

例

- $F = \{f_1 = xy + yz,\ f_2 = x^2 + y + z\} \subset K[x, y, z]$
- f_1 の yz と f_2 の x^2 は互いに素
- $\Rightarrow \boldsymbol{w} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ などでそれらは互いに素に

SGBD のアルゴリズム（概略）[SW97]

簡単のため，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（違う場合は変数の組合せを網羅することで，この場合に帰着できる）．

Input : 多項式集合 $F = \{f_1, \cdots, f_n\} \subset K[\bar{X}]$

Output: F が $I = \langle F \rangle$ の Gröbner 基底となるような項順序 $\boldsymbol{w} \in \mathrm{R}_+^n$

1. 1 つの変数からなる項で，倍単項式が存在しないような項のみを残す
2. 互いに素な項（先頭項候補）をそれぞれの多項式から選出
3. それらが先頭項となるような項順序を求める

SGBD のアルゴリズム（概略）[SW97]

簡単のため，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（違う場合は変数の組合せを網羅することで，この場合に帰着できる）.

Input : 多項式集合 $F = \{f_1, \cdots, f_n\} \subset K[\bar{X}]$

Output: F が $I = \langle F \rangle$ の Gröbner 基底となるような項順序 $\boldsymbol{w} \in \mathrm{R}_+^n$

1. 1 つの変数からなる項で，倍単項式が存在しないような項のみを残す

   例) $f_i = x^3 + x + xy^3 + y^2 + z^2 \quad \rightarrow \quad \tilde{f}_i = x^3 + z^2$

2. 互いに素な項（先頭項候補）をそれぞれの多項式から選出

3. それらが先頭項となるような項順序を求める

SGBD のアルゴリズム（概略）[SW97]

簡単のため，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（違う場合は変数の組合せを網羅することで，この場合に帰着できる）.

Input : 多項式集合 $F = \{f_1, \cdots, f_n\} \subset K[\bar{X}]$

Output: F が $I = \langle F \rangle$ の Gröbner 基底となるような項順序 $\boldsymbol{w} \in \mathrm{R}_+^n$

1. 1 つの変数からなる項で，倍単項式が存在しないような項のみを残す

   例) $f_i = x^3 + x + xy^3 + y^2 + z^2 \quad \rightarrow \quad \tilde{f}_i = x^3 + z^2$

2. 互いに素な項（先頭項候補）をそれぞれの多項式から選出
   - 二部グラフの最大マッチング問題 (Hungarian method[PL86] など)
3. それらが先頭項となるような項順序を求める

SGBD のアルゴリズム（概略）[SW97]

簡単のため，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（違う場合は変数の組合せを網羅することで，この場合に帰着できる）.

Input : 多項式集合 $F = \{f_1, \cdots, f_n\} \subset K[\bar{X}]$

Output: F が $I = \langle F \rangle$ の Gröbner 基底となるような項順序 $\boldsymbol{w} \in \mathrm{R}_+^n$

1. 1 つの変数からなる項で，倍単項式が存在しないような項のみを残す

   例) $f_i = x^3 + x + xy^3 + y^2 + z^2 \quad \rightarrow \quad \tilde{f}_i = x^3 + z^2$

2. 互いに素な項（先頭項候補）をそれぞれの多項式から選出
   - 二部グラフの最大マッチング問題 (Hungarian method[PL86] など)
3. それらが先頭項となるような項順序を求める
   - 線形計画問題 (Khachian's Ellipsoid method[Sch98] など)

多項式にパラメータが存在する場合はどうか

パラメータを伴ったSGBD

例

多項式集合 $F \subset (K[a])[x, y, z]$

$$F = \left\{ \begin{array}{l} f_1 = x + (a-3)y^2, \\ f_2 = x^3 + z, \\ f_3 = y + z^3 \end{array} \right\}$$

パラメータを伴ったSGBD

例

多項式集合 $F \subset (K[a])[x, y, z]$

$a \neq 3$ のとき,

$$F = \left\{ \begin{array}{l} f_1 = x + (a-3)y^2, \\ f_2 = x^3 + z, \\ f_3 = y + z^3 \end{array} \right\}$$

パラメータを伴ったSGBD

例

多項式集合 $F \subset (K[a])[x, y, z]$

$a = 3$ のとき,

$$F = \left\{ \begin{array}{l} f_1 = x + \cancel{(a-3)y^2}, \\ f_2 = x^3 + z, \\ f_3 = y + z^3 \end{array} \right\}$$

- $a-3 \neq 0 (\Leftrightarrow a \neq 3)$ のとき

$$F = \left\{ \begin{array}{l} f_1 = x + (a-3)y^2 \\ f_2 = x^3 + z, \\ f_3 = y + z^3 \end{array} \right\}$$

項順序 $\boldsymbol{w_1} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ で $\langle F \rangle$ の Gröbner 基底となる.

- $a-3 \neq 0 (\Leftrightarrow a \neq 3)$ のとき

$$F = \left\{ \begin{array}{l} f_1 = x + (a-3)y^2 \\ f_2 = x^3 + z, \\ f_3 = y + z^3 \end{array} \right\}$$

項順序 $\boldsymbol{w_1} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ で $\langle F \rangle$ の Gröbner 基底となる.

- $a-3 = 0 (\Leftrightarrow a = 3)$ のとき

$$F = \left\{ \begin{array}{l} f_1 = x + \cancel{0 \cdot y^2} \\ f_2 = x^3 + z, \\ f_3 = y + z^3 \end{array} \right\}$$

項順序 $\boldsymbol{w_2} = \begin{pmatrix} 1 & 16 & 4 \end{pmatrix}$ で $\langle F \rangle$ の Gröbner 基底となる.

- $a-3 \neq 0 (\Leftrightarrow a \neq 3)$ のとき

$$F = \left\{ \begin{array}{l} f_1 = x + (a-3)y^2 \\ f_2 = x^3 + z, \\ f_3 = y + z^3 \end{array} \right\}$$

項順序 $\boldsymbol{w_1} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ で $\langle F \rangle$ の Gröbner 基底となる.

- $a-3 = 0 (\Leftrightarrow a = 3)$ のとき

$$F = \left\{ \begin{array}{l} f_1 = x + \cancel{0 \cdot y^2} \\ f_2 = x^3 + z, \\ f_3 = y + z^3 \end{array} \right\}$$

項順序 $\boldsymbol{w_2} = \begin{pmatrix} 1 & 16 & 4 \end{pmatrix}$ で $\langle F \rangle$ の Gröbner 基底となる.

- 求めたいもの：$\{(\{a-3 \neq 0\}, \boldsymbol{w_1}), (\{a-3 = 0\}, \boldsymbol{w_2})\}$

パラメータを伴ったSGBD

Comprehensive structural Gröbner basis detection(CSGBD)

$S \subseteq L^m$ を代数構成的集合とする．多項式集合 $F \subset K[\bar{X}, \bar{A}]$ に対して，

$$\tilde{\mathcal{G}} = \{(S_1, \boldsymbol{w_1}), \ldots, (S_\ell, \boldsymbol{w_\ell})\}$$

- S_i：パラメータの条件 (和集合が S を包含する L^m の構成的部分集合)
- $\boldsymbol{w_i}$：項順序 (matrix order の weight vector)

パラメータの条件 S_i と weight vector $\boldsymbol{w_i} \in \mathbb{R}_+^n$ は次を満たす．

- $\bar{a} \in S_i$ に対し，
  $\sigma_{\bar{a}}(F)$ がイデアル $\langle \sigma_{\bar{a}}(F) \rangle$ の項順序 $\boldsymbol{w_i}$ での Gröbner 基底．

そのような項順序が見つからないとき，$\boldsymbol{w_i} = \boldsymbol{0}$ とする．

（CGS[Wei92] を踏襲した定義）

CSGBD のアルゴリズム (直接的方法)

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

Output: $\tilde{\mathcal{G}} = \{(S_1, \boldsymbol{w_1}), \ldots, (S_\ell, \boldsymbol{w_\ell})\}$(先程の条件を満たすもの)

1. パラメータ空間 S を，項が確定するように分割する.

2. 変数の組み合わせを網羅する形で SGBD のアルゴリズムを行う.

パラメータ空間の分割

例

$K[x,y,a]$ を x,y についての多項式環 $(K[a])[x,y]$ とみなす．次の多項式集合 $F \subset K[x,y,a]$ を考える．

$$F = \left\{ \begin{array}{l} f_1 = (a-1)x^2 + y^2, \\ f_2 = x + (a-2)y^3 \end{array} \right\}$$

場合分けは $4(= 2^2)$ つ必要 (？)

1. $a-1=0, a-2=0$ のとき
2. $a-1=0, a-2\neq 0$ のとき
3. $a-1\neq 0, a-2=0$ のとき
4. $a-1\neq 0, a-2\neq 0$ のとき

パラメータ空間の分割

例

$K[x,y,a]$ を x,y についての多項式環 $(K[a])[x,y]$ とみなす．次の多項式集合 $F \subset K[x,y,a]$ を考える．

$$F = \left\{ \begin{array}{l} f_1 = (a-1)x^2 + y^2, \\ f_2 = x + (a-2)y^3 \end{array} \right\}$$

場合分けは $4(= 2^2)$ つ必要 (？)

1. $a-1=0, a-2=0$ のとき $\rightarrow (E,N) = (\{a-1, a-2\}, \{\})$
2. $a-1=0, a-2\neq 0$ のとき $\rightarrow (E,N) = (\{a-1\}, \{a-2\})$
3. $a-1\neq 0, a-2=0$ のとき $\rightarrow (E,N) = (\{a-2\}, \{a-1\})$
4. $a-1\neq 0, a-2\neq 0$ のとき $\rightarrow (E,N) = (\{\}, \{a-1, a-2\})$

パラメータ空間の分割についての詳細 (CPSS)

定義 5.1 (包括的多項式項集合系 (Comprehensive polynomial support system)).

多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}, \bar{A}]$ とし，$S \subseteq L^m$ を代数構成的集合 (algebraically constructible subsets) とする．$S_1, \ldots, S_\ell$ を

$$\bigcup_{i=1}^{\ell} S_i \supseteq S,\ S_i \cap S_j = \phi \quad (\forall i, j \in \{1, \ldots, \ell\},\ i \neq j)$$

を満たす L^m の構成的部分集合とするとき，集合 $E_i, N_i \subseteq K[\bar{A}]$ に対して $S_i = V(E_i) \setminus V(N_i)$ が成立するものとする．
集合 $\mathcal{P} = \{(E_1, N_1, \mathscr{T}_1), \ldots, (E_\ell, N_\ell, \mathscr{T}_\ell)\}$ や $\mathcal{P}' = \{(S_1, \mathscr{T}_1), \ldots, (S_\ell, \mathscr{T}_\ell)\}$ を F に関する S 上の包括的多項式項集合系（**comprehensive polynomial support system**）と呼ぶ．
特に，$S = L^m$ を満たす場合，上記 $\mathcal{P}$ を単に F の包括的多項式項集合系と呼ぶ．ただし，$i = 1, \ldots, \ell$ に対して

$$\mathscr{T}_i = \{T_{i1}, \ldots, T_{ik} \ :\ T_{ij} \subset K[\bar{X}],\ j = 1, \ldots, k\}$$

とし，任意の $a_i \in S_i \subset L^m$ に対して $\mathscr{T}_i = T_{\bar{X}}(\sigma_{a_i}(F))$ を満たす集合族とする．

（CGS を踏襲した定義）

パラメータ空間の分割についての詳細 (CPSS)

定義 5.1 (包括的多項式項集合系 (Comprehensive polynomial support system)).

多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}, \bar{A}]$ とし，$S \subseteq L^m$ を代数構成的集合 (algebraically constructible subsets) とする．$S_1, \ldots, S_\ell$ を

$$\bigcup_{i=1}^{\ell} S_i \supseteq S,\ S_i \cap S_j = \phi \quad (\forall i, j \in \{1, \ldots, \ell\},\ i \neq j)$$

を満たす L^m の構成的部分集合とするとき，集合 $E_i, N_i \subseteq K[\bar{A}]$ に対して $S_i = V(E_i) \setminus V(N_i)$ が成立するものとする．
集合 $\mathcal{P} = \{(E_1, N_1, \mathscr{T}_1), \ldots, (E_\ell, N_\ell, \mathscr{T}_\ell)\}$ や $\mathcal{P}' = \{(S_1, \mathscr{T}_1), \ldots, (S_\ell, \mathscr{T}_\ell)\}$ を F に関する S 上の包括的多項式項集合系（**comprehensive polynomial support system**）と呼ぶ．
特に，$S = L^m$ を満たす場合，上記 $\mathcal{P}$ を単に F の包括的多項式項集合系と呼ぶ．ただし，$i = 1, \ldots, \ell$ に対して

$$\mathscr{T}_i = \{T_{i1}, \ldots, T_{ik} \ :\ T_{ij} \subset K[\bar{X}],\ j = 1, \ldots, k\}$$

とし，任意の $a_i \in S_i \subset L^m$ に対して $\mathscr{T}_i = T_{\bar{X}}(\sigma_{a_i}(F))$ を満たす集合族とする．

（CGS を踏襲した定義）

パラメータ空間の分割

例

$K[x,y,a]$ を x,y についての多項式環 $(K[a])[x,y]$ とみなす．次の多項式集合 $F \subset K[x,y,a]$ を考える．

$$F = \left\{ \begin{array}{l} f_1 = (a-1)x^2 + y^2, \\ f_2 = x + (a-2)y^3 \end{array} \right\}$$

場合分けは $4(= 2^2)$ つ必要 (？)

1. $a-1=0, a-2=0$ のとき $\rightarrow (E,N) = (\{a-1, a-2\}, \{\})$
2. $a-1=0, a-2\neq 0$ のとき $\rightarrow (E,N) = (\{a-1\}, \{a-2\})$
3. $a-1\neq 0, a-2=0$ のとき $\rightarrow (E,N) = (\{a-2\}, \{a-1\})$
4. $a-1\neq 0, a-2\neq 0$ のとき $\rightarrow (E,N) = (\{\}, \{a-1, a-2\})$

パラメータ空間の分割

例

$K[x,y,a]$ を x,y についての多項式環 $(K[a])[x,y]$ とみなす．次の多項式集合 $F \subset K[x,y,a]$ を考える．

$$F = \left\{ \begin{array}{l} f_1 = (a-1)x^2 + y^2, \\ f_2 = x + (a-2)y^3 \end{array} \right\}$$

場合分けは $4(= 2^2)$ つ必要 (？)

1. $a-1=0, a-2=0$ のとき $\rightarrow (E,N) = (\{a-1, a-2\}, \{\})$
2. $a-1=0, a-2\neq 0$ のとき $\rightarrow (E,N) = (\{a-1\}, \{a-2\})$
3. $a-1\neq 0, a-2=0$ のとき $\rightarrow (E,N) = (\{a-2\}, \{a-1\})$
4. $a-1\neq 0, a-2\neq 0$ のとき $\rightarrow (E,N) = (\{\}, \{a-1, a-2\})$

パラメータ空間に矛盾が生じる場合とその対処法

1. 等号制約 E に矛盾のある場合 $(V(E) = \phi)$

例

$$(E, N) = (\{a - 1,\ a - 2\},\ \{b^2 + 3\})$$

$\Rightarrow$ E が生成するイデアル $\langle E \rangle$ の,
任意の項順序での簡約 Gröbner 基底が $\{1\}$ に等しい.

パラメータ空間に矛盾が生じる場合とその対処法

1. 等号制約 E に矛盾のある場合 $(V(E) = \phi)$

例

$$(E, N) = (\{a - 1,\ a - 2\},\ \{b^2 + 3\})$$

$\Rightarrow$ E が生成するイデアル $\langle E \rangle$ の,
任意の項順序での簡約 Gröbner 基底が $\{1\}$ に等しい.

2. 等号制約 E と不等号制約 N の間の矛盾 $(V(E) \setminus V(N) = \phi)$

例

$$(E, N) = (\{(a - 3)^2,\ b - 1\},\ \{a - 3,\ b + 3\})$$

$\Rightarrow$ N の要素それぞれがラディカル $\sqrt{E}$ に含まれているか
を確かめる.

Algorithm 1 ParameterDivisionMain

Require: $\{(E, N, \mathscr{T})\}$（ただし $\mathscr{T} = \{T_1, \ldots, T_k\},\ N = \{a_N\},\ a_N \in K[\bar{A}]$ とする.）
Ensure: $\mathrm{PolySet}(\mathscr{T})$ の $V(E) \setminus V(N)$ 上の CPSS$\{(E_1, N_1, \mathscr{T}_1), \ldots, (E_{\ell'}, N_{\ell'}, \mathscr{T}_{\ell'})\}$

if $E \neq \phi \wedge \mathrm{ReducedGröbnerBasis}(E, \prec_{\bar{A}}) = \{1\}$ **then**
▷ 等号制約 E の矛盾を検出する if 文
  return ϕ
end if
if $a_N \neq 1 \wedge E \neq \phi \wedge \mathrm{ReducedGröbnerBasis}(E \cup \{1 - y \cdot a_N\}, \prec_{\bar{A},y}) = \{1\}$ **then**
▷ 不等号制約 N の矛盾を検出する if 文
  return ϕ
end if
if $\forall i \in \{1, \ldots, k\},\ \forall t_i \in T_i,\ t_i \in K[\bar{X}]$ **then** ▷ 再帰の終了条件
  return $\{(E, N, \mathscr{T})\}$
end if
if $\forall j \in \{1, \ldots, \ell\},\ \exists t_j \in T_j,\ t_j \notin K[\bar{X}]$ **then** ▷ 項 t を E, N に追加し，再帰的に繰り返す
  $m \leftarrow t_j$
  $c,\ t \leftarrow \mathrm{coeff}_{\bar{X}}(m),\ \mathrm{term}_{\bar{X}}(m)$
end if
$\mathscr{T}_E \leftarrow \{T_1, \ldots, T_{j-1}, T_j \setminus \{m\}, T_{j+1}, \ldots, T_k\})$ ▷ $c = 0$ のとき（項が消える）
$\mathscr{T}_N \leftarrow \{T_1, \ldots, T_{j-1}, (T_j \cup \{t\}) \setminus \{m\}, T_{j+1}, \ldots, T_k\})$ ▷ $c \neq 0$ のとき（項が残る）
return $\mathrm{ParameterDivisionMain}(E \cup \{c\}, N, \mathscr{T}_E)$
  $\cup \mathrm{ParameterDivisionMain}(E, N \wedge \{c\}, \mathscr{T}_N)$

多項式集合 F が与えられたとき，

SGBD

- 変数の数と $\mathrm{card}(F)$ が違う場合は，変数の組み合わせを構成.
- 倍単項式が存在しない，且つ単一変数のみからなる項をピックアップ.
- 変数と指数部分からなる二部グラフを構成し，最大マッチング問題を解く.
- 線形計画問題を解き，求めたい weight vector を計算.

多項式集合 F が与えられたとき，

SGBD

- パラメータ空間を分割し，項を確定させる（後で新たな場合分けが発生しない）.
- 変数の数と $\mathrm{card}(F)$ が違う場合は，変数の組み合わせを構成.
- 倍単項式が存在しない，且つ単一変数のみからなる項をピックアップ.
- 変数と指数部分からなる二部グラフを構成し，最大マッチング問題を解く.
- 線形計画問題を解き，求めたい weight vector を計算.

多項式集合 F が与えられたとき，

SGBD

- パラメータ空間を分割し，項を確定させる（後で新たな場合分けが発生しない）.
- 変数の数と $\mathrm{card}(F)$ が違う場合は，変数の組み合わせを構成.
- 倍単項式が存在しない，且つ単一変数のみからなる項をピックアップ.
- 変数と指数部分からなる二部グラフを構成し，最大マッチング問題を解く.
- 線形計画問題を解き，求めたい weight vector を計算.

GBD

- affine Newton polyhedron $\mathcal{N}_{\mathrm{aff}}(F)$ を得る.
- $\mathcal{N}_{\mathrm{aff}}(F)$ の頂点が項順序の同値類に対応している.
- 各同値類の代表元で，全ての Spoly がゼロ簡約されるか調べる.

多項式集合 F が与えられたとき，

SGBD

- パラメータ空間を分割し，項を確定させる（後で新たな場合分けが発生しない）.
- 変数の数と $\mathrm{card}(F)$ が違う場合は，変数の組み合わせを構成.
- 倍単項式が存在しない，且つ単一変数のみからなる項をピックアップ.
- 変数と指数部分からなる二部グラフを構成し，最大マッチング問題を解く.
- 線形計画問題を解き，求めたい weight vector を計算.

GBD

- パラメータ空間を分割する
- affine Newton polyhedron $\mathcal{N}_{\mathrm{aff}}(F)$ を得る.
- $\mathcal{N}_{\mathrm{aff}}(F)$ の頂点が項順序の同値類に対応している.
- 各同値類の代表元で，全ての Spoly がゼロ簡約されるか調べる.

多項式集合 F が与えられたとき，

SGBD

- パラメータ空間を分割し，項を確定させる（後で新たな場合分けが発生しない）.
- 変数の数と $\mathrm{card}(F)$ が違う場合は，変数の組み合わせを構成.
- 倍単項式が存在しない，且つ単一変数のみからなる項をピックアップ.
- 変数と指数部分からなる二部グラフを構成し，最大マッチング問題を解く.
- 線形計画問題を解き，求めたい weight vector を計算.

GBD

- パラメータ空間を分割する
- affine Newton polyhedron $\mathcal{N}_{\mathrm{aff}}(F)$ を得る.
- $\mathcal{N}_{\mathrm{aff}}(F)$ の頂点が項順序の同値類に対応している.
- 各同値類の代表元で，全ての Spoly がゼロ簡約されるか調べる.
  - Spoly の計算時に新たな場合分けが発生する可能性がある.

ここまでのまとめ

1. 多項式集合がそのまま Gröbner 基底であるような項順序を求めたい.
2. "(Structural) Gröbner basis detection"という問題 (Sturmfels ら).
3. GBD は affine Newton polyhedron の計算,
   SGBD は二部グラフの最大マッチング問題と線形計画問題に帰着可能.
4. パラメータを伴っている場合でも，適切に場合分けすれば計算可能.

ここまでのまとめ

1. 多項式集合がそのまま Gröbner 基底であるような項順序を求めたい.
2. "(Structural) Gröbner basis detection"という問題 (Sturmfels ら).
3. GBD は affine Newton polyhedron の計算,
   SGBD は二部グラフの最大マッチング問題と線形計画問題に帰着可能.
4. パラメータを伴っている場合でも，適切に場合分けすれば計算可能.

ここからのはなし

1. パラメータ空間の分割の効率化

SGBD のアルゴリズム（概略）[SW97]

簡単のため，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（違う場合は変数の組合せを網羅することで，この場合に帰着できる）．

Input : 多項式集合 $F = \{f_1, \cdots, f_n\} \subset K[\bar{X}]$

Output: F が $I = \langle F \rangle$ の Gröbner 基底となるような項順序 $\boldsymbol{w} \in \mathrm{R}_+^n$

1. 1 つの変数からなる項で，倍単項式が存在しないような項のみを残す

   例) $f_i = x^3 + x + xy^3 + y^2 + z^2 \quad \rightarrow \quad \tilde{f}_i = x^3 + z^2$

2. 互いに素な項（先頭項候補）をそれぞれの多項式から選出
   - 二部グラフの最大マッチング問題 (Hungarian method[PL86] など)
3. それらが先頭項となるような項順序を求める
   - 線形計画問題 (Khachian's Ellipsoid method[Sch98] など)

例

$$F = \begin{Bmatrix} f_1 = (a-3)x^3 + (b-2)x^2 + \cdots, \\ f_2 = \cdots \end{Bmatrix}$$

(E, N) は

- $(\{a-3, b-2\}, \{\})$
- $(\{a-3\}, \{b-2\})$
- $(\{\}, \{a-3, b-2\})$
- $(\{b-2\}, \{a-3\})$

例

$$F = \left\{ \begin{array}{l} f_1 = (a-3)x^3 + (b-2)x^2 + \cdots, \\ f_2 = \cdots \end{array} \right\}$$

(E, N) は

- $(\{a-3, b-2\}, \{\})$
- $(\{a-3\}, \{b-2\})$
- $(\{\}, \{a-3, \cancel{b-2}\})$
- $(\{\cancel{b-2}\}, \{a-3\})$

} 同じ

f_1 の項 x^2 は HT 候補から外れる.

$\mathcal{N}_{\mathrm{aff}}(t)$ を用いた改善

1: **if** $\forall j \in \{1,\dots,\ell\},\ \exists t_j \in T_j,\ t_j \notin K[\bar{X}]$ **then** ▷ 項 t を E, N に追加し，再帰的に繰り返す
2: $m \leftarrow t_j$
3: $c,\ t \leftarrow \mathrm{coeff}_{\bar{X}}(m),\ \mathrm{term}_{\bar{X}}(m)$
4: **end if**
5: $\mathscr{T}_E \leftarrow \{T_1,\dots,T_{j-1}, T_j \setminus \{m\}, T_{j+1},\dots,T_k\})$ ▷ $c=0$ のとき（項が消える）
6: $\mathscr{T}_N \leftarrow \{T_1,\dots,T_{j-1}, (T_j \cup \{t\}) \setminus \{m\}, T_{j+1},\dots,T_k\})$ ▷ $c\neq 0$ のとき（項が残る）
7: **return** $\mathrm{ParameterDivisionMain}(E\cup\{c\}, N, \mathscr{T}_E) \cup \mathrm{ParameterDivisionMain}(E, N\wedge\{c\}, \mathscr{T}_N)$

⇓

1: **if** $\forall j \in \{1,\dots,\ell\},\ \exists t_j \in T_j,\ t_j \notin K[\bar{X}]$ **then** ▷ 項 t を E, N に追加し，再帰的に繰り返す
2: $m \leftarrow t_j$
3: $c,\ t \leftarrow \mathrm{coeff}_{\bar{X}}(m),\ \mathrm{term}_{\bar{X}}(m)$
4: **end if**
5: $\mathscr{T}_E \leftarrow \{T_1,\dots,T_{j-1}, T_j \setminus \{m\}, T_{j+1},\dots,T_k\})$ ▷ $c=0$ のとき（項が消える）
6: $\mathscr{T}_N \leftarrow \{T_1,\dots,T_{j-1}, (T_j \setminus \mathcal{N}_{\mathrm{aff}}(t)) \cup \{t\}, T_{j+1},\dots,T_k\})$ ▷ $c\neq 0$ のとき（項が残る）
7: **return** $\mathrm{ParameterDivisionMain}(E\cup\{c\}, N, \mathscr{T}_E) \cup \mathrm{ParameterDivisionMain}(E, N\wedge\{c\}, \mathscr{T}_N)$

$F = \{f_1, \ldots, f_k\}$ の項の確定をしたい

- $R = K[\bar{X}, \bar{A}]$
- $f_i = t_{i1} + t_{i2} + \cdots + t_{ir_i}$, $\boldsymbol{e_i} = (\delta_{ij}) \in \mathbb{R}^k$

- 加群 R^k の部分加群 $I = \langle M \rangle$ で，M はそのまま CGS

$$M = \bigcup_{i=1}^{k} \{t_{i1}\boldsymbol{e_i}, \ldots, t_{ir_i}\boldsymbol{e_i}\} \subset R^k$$

- minimal CGS にすると，項の確定ができる（？）

$$t_\beta \mid t_\alpha \Longrightarrow t_\alpha \text{が取り除かれる}$$

消したいのは t_β のほう！
しかし，t_α が消えてしまう

$F = \{f_1, \ldots, f_k\}$ の項の確定をしたい

- $R = K[\bar{X}, \bar{A}]$
- $f_i = t_{i1} + t_{i2} + \cdots + t_{ir_i}$, $\boldsymbol{e_i} = (\delta_{ij}) \in \mathbb{R}^k$
- $\hat{t}_{ij}$: t_{ij} の f_i での reversal（次数反転）
- 加群 R^k の部分加群 $\hat{I} = \hat{M}$ で，$\hat{M}$ はそのまま CGS

$$\hat{M} = \bigcup_{i=1}^{k} \{\hat{t}_{i1}\boldsymbol{e_i}, \ldots, \hat{t}_{ir_i}\boldsymbol{e_i}\} \subset R^k$$

- minimal CGS にすると，項の確定ができる（！）

$$\hat{t}_\alpha \mid \hat{t}_\beta \Longrightarrow \hat{t}_\beta \text{が取り除かれる}$$

反転していた次数を元に戻すと

$$t_\beta \mid t_\alpha \Longrightarrow \text{消したい } t_\beta \text{が消える！}$$

Reference I

[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 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 European Conference on Computer Algebra, pages 513–517. Springer, 1985.

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

Reference II

[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.