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

神戸大学大学院・人間発達環境学研究科　　大島谷 遼
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 *1
Kosaku Nagasaka
Graduate school of human development and environment, Kobe university

Abstract

In this talk, we introduce a method to find a term order such that the given F, a set of polynomials with parameters is a Gröbner basis for the ideal $\langle F \rangle$. This problem without parameters is called the Gröbner basis detection (GBD) and there is also its simpler problem called the structural Gröbner basis detection (SGBD). GBD can be solved by the equivalent classes of term orders computed by the affine Newton polyhedron of F, and SGBD can be reduced to the maximum matching problem of bipartite graph and linear-inequality feasibility problem. Especially for SGBD with parameters, our method divides the parameter space comprehensively, and then solves each SGBD without parameters. Moreover, we also introduce some improvements using affine Newton polyhedron and comprehensive Gröbner system over modules.

1　研究の背景

多項式集合 F が与えられイデアル $\langle F \rangle$ の Gröbner 基底の計算を行う際，項順序を固定した上で，Buchberger アルゴリズム [Buc06] などにより 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 $\langle F \rangle$ の 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
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 $\langle F \rangle$ 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

*1 E-mail: nagasaka@main.h.kobe-u.ac.jp

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 基底を求めることもできる．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，前者は Gritzmann と Sturmfels，後者は Sturmfels と Wiegelmann によって解かれた既知の問題である．

発表では，(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たものについて述べた．また，パラメータ空間の分割における効率化として，affine Newton polyhedron を用いたものと，加群上の包括的 Gröbner 基底系を用いたものについての概要を紹介する．

1.1 基本的な定義

$\mathbb{N}$ は 0 以上の整数全体の集合とする．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（ただし，$\bar{X} \cap \bar{A} = \phi$）．このような集合 $\bar{X}, \bar{A}$ に対して，主変数 $\bar{X}$ に関する多項式環 $(K[\bar{A}])[\bar{X}]$ を R とする．多項式環上のイデアルを多項式集合 F を用いて $\langle F \rangle$ と表す．イデアル I に対して，その根基イデアルを $\sqrt{I}$ と表す．単項式 $m \in K[\bar{X}]$ に対して，$\mathrm{coeff}_{\bar{X}}(m)$ を m の $\bar{X}$ に関する係数，$\mathrm{term}_{\bar{X}}(m)$ を m の $\bar{X}$ に関する項として定義する．尚，多項式環の主変数が明らかな場合には単に $\mathrm{coeff}(m)$ のように省略して書くこともある．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．項順序を次のように定義する．

定義 1 (項順序)
T_n における全順序 $\prec$ が項順序であるとは，次を満たすことをいう．

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

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 $\mathrm{hm}_\prec(f)$ とし，f の**頭単項式**と呼ぶ．また，$\mathrm{ht}_\prec(f) = \mathrm{term}_{\bar{X}}(\mathrm{hm}_\prec(f))$, $\mathrm{hc}_\prec(f) = \mathrm{coeff}_{\bar{X}}(\mathrm{hm}_\prec(f))$ と定義し，それぞれ**頭項**，**頭係数**と呼ぶ．項順序が明らかな場合には，$\mathrm{hm}_\prec(f)$ を省略して単に $\mathrm{hm}(f)$ 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（$\mathrm{HT}_\prec(F)$ と $\mathrm{HC}_\prec(F)$ についても同様に定義する）．$K[\bar{X}]$ の 0 でないイデアル I に対しては，$\mathrm{HT}_\prec(I)$ を I の元の頭項全体の集合として定義する（$\mathrm{HT}_\prec(I)$ と $\mathrm{HC}_\prec(I)$ 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．ベクトル $\boldsymbol{u}, \boldsymbol{v}$ の内積を $(\boldsymbol{u}, \boldsymbol{v})$ と表す．重みベクトル $\boldsymbol{w}$ を次の定義により項順序と同一視する．

定義 2 (重みベクトルと項順序)
項順序 $\prec$ が重みベクトル $\boldsymbol{w} \in \mathbb{R}^n$ を用いて表されるとは，項 $t_1, t_2 \in T_n$ の指数ベクトル $e(t_1), e(t_2) \in \mathbb{N}^n$ に対して，次を満たすことをいう．

$$t_1 \prec t_2 \Longleftrightarrow (\boldsymbol{w}, e(t_1)) < (\boldsymbol{w}, e(t_2))$$

尚，このままでは項順序の条件を満たさないが，一次独立なベクトルを追加して行列を構成することで，任意の項順序を表現可能であるということがわかっている [Rob85].

項順序を $\prec$ で固定する．多項式 $f, g \in K[\bar{X}]$ に対し，f に含まれる単項式 m が $\mathrm{ht}(g)$ で割り切られるとする．このとき，$h = f - \frac{m}{\mathrm{hm}(g)} g$ 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 $G = \{g_i : i \in \{1, 2, \dots\}\} \subset K[\bar{X}]$ において，G に含まれる多項式 g_i で f を単項簡約することで h が得られるとき，同様に $f \to_G h$ と書く．また，g_i による単項簡約を 0 回を含む有限回繰り返すことで，これ以上 g_i による単項簡約ができない h が得られるとき，h を f の G による正規形と呼び，$h = \mathrm{nf}_G(f)$ で表す．

定義 3 (S 多項式)
項順序を $\prec$ で固定し $f, g \in K[\bar{X}]$ とする．このとき，f, g の ***S* 多項式**を次のように定義する．

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

これらを用いて，Gröbner 基底は次のように定義される．

定義 4 (Gröbner 基底)
多項式集合 $F \subset K[\bar{X}]$ と F が生成するイデアル $I = \langle F \rangle$ に対して，

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

が満たされるとき，F を項順序 $\prec$ に対する ***Gröbner* 基底**であるという．

$a \in L^m$ に対して，特化準同型 (specialization homomorphism) $\sigma_a : K[\bar{X}, \bar{A}] \to L[\bar{X}]$ を各 $a_i \in \bar{A}$ への a の自然な代入として定義する．本報告では，代数構成的集合 S を，集合 $E, N \subset K[\bar{A}]$ を用いて $S = V(E) \backslash V(N)$ と表される集合として扱う．多項式環 R における包括的 Gröbner 基底系及び包括的 Gröbner 基底は次のように定義される．

定義 5 (包括的 Gröbner 基底系（Comprehensive Gröbner system; CGS）)
主変数 $\bar{X}$ に関する項順序を $\prec$ で固定する．多項式集合 $F \subset R$ と L^m の代数構成的集合 S に対して，

$$\mathcal{G} = \{(S_1, G_1), \dots, (S_1, G_\ell)\}$$

が F の S 上の**包括的 *Gröbner* 基底系（*CGS*）**であるとは，

- $S_1, \dots, S_\ell$ は L^m の構成的部分集合
- $G_1, \dots, G_\ell$ は R の有限な部分集合
- $\bigcup_{i=1}^{\ell} S_i \supseteq S,\ S_i \cap S_j = \phi \quad (\forall i, j \in \{1, \dots, \ell\},\ i \neq j)$
- 任意の $\bar{a} \in S_i$ に対して，$\sigma_{\bar{a}}(G_i)$ が $\sigma_{\bar{a}}(F)$ の $L[\bar{X}]$ における *Gröbner* 基底である

を満たすときにいう．特に $S = L^m$ のとき，$\mathcal{G}$ を単に F の包括的 *Gröbner* 基底系であるという．

定義 6
集合 $E, N \subset K[\bar{A}]$ に対して，組 (E, N) を**パラメータ制約 *(parametric constraint)*** と呼ぶ．
$V(E) \setminus V(N) \neq \phi$ のとき，(E, N) は ***consistent*** であるといい，$V(E) \setminus V(N) = \phi$ のとき，(E, N) は ***inconsistent*** であるという．L^m の代数構成的集合 S が $S = V(E) \setminus V(N)$ と表されるとき，単に S をパラメータ制約と呼ぶ場合もある．

定義 7 (包括的 Gröbner 基底（CGB）)
多項式集合 $F,\ G \subset R$ に対して，$\{(L^m, G)\}$ が F の包括的 *Gröbner* 基底系であるとき，G を F の**包括的 *Gröbner* 基底（*comprehensive Gröbner basis; CGB*）**という．

2　GBD と SGBD について

この章では，パラメータを伴わない通常の GBD 及び SGBD の概要について述べる．まず，GBD の問題は，次のようになっている．

問題 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 の判定条件により簡単にしたものが，次の SGBD である．

問題 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．

2.1　Gröbner basis detection[GS93]

Gröbner basis detection の問題を解くあたって，重みベクトルに次の同値関係を導入する．

定義 8
重みベクトル $\boldsymbol{w_1}, \boldsymbol{w_2}$ が F に関して同値であるとは，対応する項順序 $\prec_A, \prec_B$ が $\mathrm{HT}_{\prec_A}(F) = \mathrm{HT}_{\prec_B}(F)$ を満たすことをいう．

まずは前提とする定義を与える．

定義 9 ([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，次を満たすときをいう．

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

- 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である．
- $\mathcal{U}$ 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，次のように定義される．

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

定義 10 (Minkowski 和, [GS93, p247])
2 つの *polytope* $P_1, P_2 \subset \mathbb{R}^n$ に対して，***Minkowski*** 和 $P_1 + P_2$ を次で定義する．

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

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* にも自然に一般化できる．

変数全体の集合 $\bar{X} = \{x_1, \ldots, x_n\}$ に対し，ベクトル $\alpha = (\alpha_i)$ で項が $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ と表されるとき，その項を単に X^α と表す．集合 $\mathbb{R}_-$ で 0 以下の実数全体の集合を表す．

定義 11 (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．

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

また，多項式集合 $F = \{f_1, \ldots, f_k\} \subset K[\bar{X}]$ の *Newton polytope* を，次の *Minkowski* 和で定義する．

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

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

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

多項式集合 F についても同様に次で定義する．

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

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 1 と図 2 に図示する．
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，

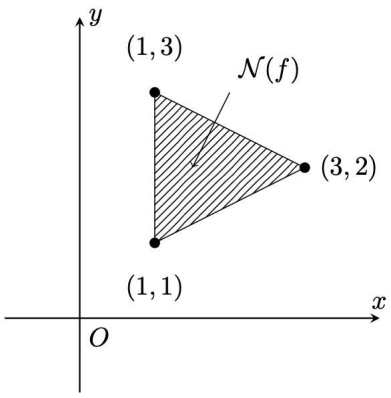

図 1: Newton polytope $\mathcal{N}(f)$

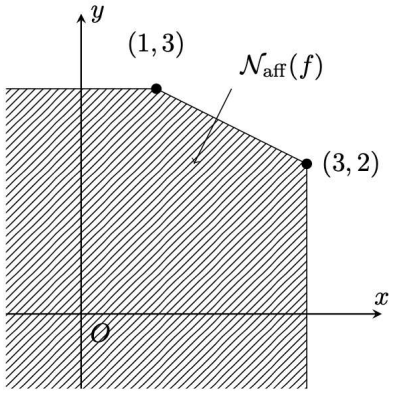

図 2: Newton polytope $\mathcal{N}(f)$

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している．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除去することができることを意味している．

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 12 ([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．

この定理により，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，

1. affine Newton polyhedron $\mathcal{N}_{\mathrm{aff}}(F)$ の頂点を求める．
2. その頂点の数だけ項順序の同値類を得る．
3. 各同値類の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る．
4. 3 の条件を満たす項順序が GBD の解である．

具体的には，図 3 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．

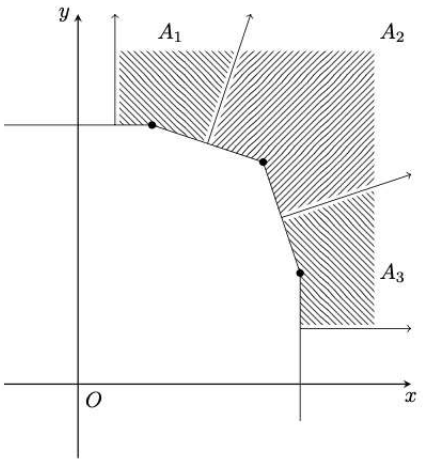

図 3: 項順序の同値類に対応している領域

2.2 structural Gröbner basis detection[SW97]

GBD の問題は，結局は項順序の同値類の数だけ S 多項式の正規形を計算する必要があり，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 SGBD である．

2.2.1 $n = k$ 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．その上で，多項式集合 $F = \{f_1, \ldots, f_n\}$ の各多項式 f_i が

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

と表されるもののみを考える．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，

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

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．しかしながら，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 13 ([SW97, Lemma5])
式 *(1)* の条件を満たす多項式集合 F に対して，次を満たすような ρ は存在しない．

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

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 $X^{a_{1\varphi(1)}}_{\varphi(1)}, \ldots, X^{a_{n\varphi(n)}}_{\varphi(n)}$ 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 2 を参照）．

次に，実際にそのような項の組 $X^{a_{1\varphi(1)}}_{\varphi(1)}, \ldots, X^{a_{n\varphi(n)}}_{\varphi(n)}$ 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 14 ([SW97, Lemma6])
多項式集合 F を式 *(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 $i \in \{1, \ldots, n\}$ 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．

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 1 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 $\boldsymbol{w} \in \mathbb{R}_+^n$ or ゼロベクトル $\mathbf{0} \in \mathbb{R}^n$

1: **for each** $i, j \in \{1, 2, \ldots, n\}$ **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

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

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: $M = \{(u_i, v_{\varphi(i)}) \ : \ i \in \{1, 2, \ldots, n\}\}$
16: **end if**
17: 行列 Γ を補題 14 と同じように構成し，次の線形の制約充足問題を解く.

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

18: **return** $\boldsymbol{w}$

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]．

2.3 $n \neq k$ のとき

次に，$n \neq k$ のときを考える．$n < k$ を満たすときには，明らかに SGBD で求めるべき互いに素な項が存在しない．そのため，$n > k$ のときを考える．

補題 15 ([SW97, Lemma9])
$\bar{X} \cap \bar{Y} = \phi$ を満たすような新たな変数の集合として $\bar{Y} = \{y_1, \ldots, y_p\}$ を定義する．$S_1 \cup \cdots \cup S_p$ を変数 $\{x_1, \ldots, x_n\}$ の分割とし，写像 π を $x_i \mapsto y_i$ で定義される $K[\bar{X}]$ から $K[\bar{Y}]$ への写像とする．写像 $\varphi : \{1, \ldots, p\} \to \{1, \ldots, p\}$ を今までと同様のものとする．$\mathrm{HT}_{\boldsymbol{w}_y}(\pi(f_i))$ が $y_{\varphi(i)}$ のべき乗であるような $K[\bar{Y}]$ 上の項順序 $\boldsymbol{w}_y$ がある場合に限り，$\mathrm{HT}_{\boldsymbol{w}_x}(f_i)$ が $S_{\varphi(i)}$ に含まれているような $K[\bar{X}]$ 上の項順序 $\boldsymbol{w}_x$ が存在する．

この補題のように $n = k$ となるように変数の組み合わせを構成することで，$n > k$ の場合も $n = k$ のときのアルゴリズム (アルゴリズム 2) に帰着できる．

3 パラメータを伴った SGBD

この章では，特に structural Gröbner basis detection の問題において，対象の多項式環が，パラメータを伴った多項式環へと拡張された場合について述べる．

例 2
$K[x, y, z, a]$ を主変数 x, y, z に関する多項式環とする．次のような多項式集合 $F \subset K[x, y, z, a]$ を考える．

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

- $a - 3 \neq 0$ のとき
  f_1 の y^2 の項は 0 にならず，$\boldsymbol{w_1} = (1, 2, 3)$ などが *SGBD* の解となるベクトルである．

$$\mathrm{ht}_{\boldsymbol{w_1}}(f_1) = y^2, \quad \mathrm{ht}_{\boldsymbol{w_1}}(f_2) = x^3, \quad \mathrm{ht}_{\boldsymbol{w_1}}(f_3) = z^3$$

- $a - 3 = 0$ のとき
  f_1 の y^2 の項が 0 となるため，$\boldsymbol{w_2} = (1, 16, 4)$ などが *SGBD* の解となるベクトルである．

$$\mathrm{ht}_{\boldsymbol{w_2}}(f_1) = x, \quad \mathrm{ht}_{\boldsymbol{w_2}}(f_2) = z, \quad \mathrm{ht}_{\boldsymbol{w_3}}(f_3) = y$$

例のパラメータを伴った多項式環においては，パラメータの付いた係数が 0 となるか否かによって多項式に含まれる項が変わるため，項を確定させるためにパラメータ空間を包括的に分割する必要がある．逆に，最初にパラメータ空間の分割を行い項を確定させる事ができれば，SGBD においてはその後に項同士の計算が発生しないため，パラメータを伴わない通常の SGBD に帰着することができる．このように，パラメータを伴った多項式環における SGBD の問題を，次のように定義する．

問題 3 (comprehensive structural Gröbner basis detection; comprehensive SGBD)
$S \subseteq L^m$ を代数構成的集合とする．多項式集合 $F \subset R$ に対し，集合 $\tilde{\mathcal{G}}$ を次の条件を満たすように構成せよ．

- $S_1, \ldots, S_\ell$ は L^m の構成的部分集合，$\boldsymbol{w_1}, \ldots, \boldsymbol{w_\ell}$ は $\mathbb{R}^n_{\geq 0}$ のベクトル
- $\bigcup_{i=1}^{\ell} S_i \supseteq S,\ S_i \cap S_j = \phi \quad (\forall i, j \in \{1, \ldots, \ell\},\ i \neq j)$
- $\tilde{\mathcal{G}} = \{(S_1, \boldsymbol{w_1}), \ldots, (S_\ell, \boldsymbol{w_\ell}))\}$
- $\bar{a} \in S_i$ に対し，$\sigma_{\bar{a}}(F)$ が $\boldsymbol{w_i}$ を重みベクトルに持つ項順序におけるイデアル $\langle \sigma_{\bar{a}}(F) \rangle$ の *Gröbner* 基底
- そのような項順序がない場合，$\boldsymbol{w_i} = \boldsymbol{0}$

3.1 包括的多項式項集合系の構成

パラメータ空間が包括的に分割されているかに注意しながら，多項式集合の項の確定を行うためのものが次の定義である．

定義 16 (包括的多項式項集合系（comprehensive polynomial support system; CPSS）)
代数構成的集合 $S \subseteq L^m$ と多項式集合 $F \subset K[\bar{X}, \bar{A}]$ に対して，$\mathcal{P} = \{(S_1, \mathscr{T}_1), \ldots, (S_\ell, \mathscr{T}_\ell)\}$ が以下の条件を満たすとき，$\mathcal{P}$ を F に関する S 上の**包括的多項式項集合系（*comprehensive polynomial support system; CPSS*）**と呼ぶ．

- $S_1, \ldots, S_\ell$ は L^m の構成的部分集合，$\mathscr{T}_1, \ldots, \mathscr{T}_\ell$ は項 $t \in T_n$ の集合族
- $\bigcup_{i=1}^{\ell} S_i \supseteq S,\ S_i \cap S_j = \phi \quad (\forall i, j \in \{1, \ldots, \ell\},\ i \neq j)$
- $\forall i \in \{1, \ldots, \ell\},\ \forall a_i \in S_i \subset L^m,\ \mathscr{T}_i = T_{\bar{X}}(\sigma_{a_i}(F))$

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．また，$S = \phi$ であるとき，任意の多項式集合 F の S 上の包括的多項式項集合系を ϕ とする．$\mathcal{P}$ の要素である組 $(S_i, \mathscr{T}_i)$ を**セグメント**と呼ぶ．

注意 1
包括的多項式項集合系を求める実際のアルゴリズムでは，扱いやすさの観点から L^m の構成的部分集合 S_i をパラメータ制約 (E_i, N_i) を用いて記述する．尚，元の集合 S_i は，パラメータ制約の *Affine* 多様体の差 $V(E_i) \setminus V(N_i)$ として表現する．

次に，包括的多項式項集合系を構成するためのアルゴリズムに関する補題を記す．

補題 17
パラメータ制約 (E, N) と多項式集合 $F \subset K[\bar{X}, \bar{A}]$ に対して，$\forall m \in M_{\bar{X}}(F),\ m \in K[\bar{X}]$ を満たすとき，F の $V(E) \setminus V(N)$ 上の包括的多項式項集合系は $\{(E, N, T_{\bar{X}}(F))\}$ となる．

証明　仮定より，$\forall a \in V(E) \setminus V(N)$, $\sigma_a(F) = F$ が成立する．よって，$T_{\bar{X}}(\sigma_a(F)) = T_{\bar{X}}(F)$. ∎

補題 18
パラメータ制約 (E, N) に対し $S = V(E) \setminus V(N)$ とする．多項式集合 $F \subset K[\bar{X}, \bar{A}]$ に対し，F に含まれる多項式の中で $m \notin K[\bar{X}]$ を満たす単項式 m を含むものが存在すると仮定する．ただし，$c \in K$, $t \in T_n$, $m = c{\cdot}t$ とする．このとき，集合 $S_E = V(E \cup \{c\}) \setminus V(N)$, $S_N = V(E) \setminus V(N \wedge \{c\})$ は $S_E \cup S_N \supseteq S$, $S_E \cap S_N = \phi$ を満たす L^m の構成的部分集合である．

証明　まず

$$\begin{aligned} S_E &= V(E \cup \{c\}) \setminus V(N) = (V(E) \cap V(\{c\})) \setminus V(N) \\ &= (V(E) \setminus V(N)) \cap (V(\{c\}) \setminus V(N)) = S \cap \tilde{N} \end{aligned}$$

ただし，$\tilde{N} := V(\{c\}) \setminus V(N)$．次に，

$$\begin{aligned} S_N &= V(E) \setminus V(N \wedge \{c\}) = V(E) \setminus (V(N) \cup V(\{c\})) \\ &= (V(E) \setminus V(N)) \cap (V(E) \setminus V(\{c\})) = S \cap \tilde{E} \end{aligned}$$

となる．ただし，$\tilde{E} := V(E) \setminus V(\{c\})$．よって，

$$\begin{aligned} S_E \cup S_N &= (S \cap \tilde{N}) \cup (S \cap \tilde{E}) = ((S \cap \tilde{N}) \cup S) \cap ((S \cap \tilde{N}) \cup \tilde{E}) \\ &= S \cap ((S \cap \tilde{N}) \cup \tilde{E}) = S \cap ((S \cup \tilde{E}) \cap (\tilde{N} \cup \tilde{E})) = S \cap (S \cup \tilde{E}) \cap (\tilde{N} \cup \tilde{E}) \end{aligned} \tag{2}$$

ここで，この式 (2) に出てきた $\tilde{N} \cup \tilde{E}$ は

$$\begin{aligned} \tilde{N} \cup \tilde{E} &= (V(\{c\}) \setminus V(N)) \cup (V(E) \setminus V(\{c\})) \\ &= (V(N)^c \cap V(\{c\})) \cup (V(\{c\})^c \cap V(E)) \\ &= \{(V(N)^c \cap V(\{c\}) \cup V(\{c\})^c)\} \cap \{(V(N)^c \cap V(\{c\}) \cup V(E))\} \\ &= \{(V(N)^c \cup V(\{c\})^c) \cap L^m\} \cap \{(V(N)^c \cup V(E)) \cap (V(\{c\}) \cup V(E))\} \\ &= (V(N)^c \cup V(\{c\})^c) \cap (V(N)^c \cup V(E)) \cap (V(\{c\}) \cup V(E)) \end{aligned} \tag{3}$$

と式変形できる．今，$S = V(E) \setminus V(N) = V(N)^c \cap V(E)$ より，$V(N)^c \supseteq S$, $V(E) \supseteq S$ が成り立つ．よって，

$$V(N)^c \cup V(\{c\})^c \supseteq S, \quad V(N)^c \cup V(E) \supseteq S, \quad V(\{c\}) \cup V(E) \supseteq S$$

が成立し，これと (3) の結果より，

$$\tilde{N} \cup \tilde{E} \supseteq S \cap S \cap S \supseteq S \tag{4}$$

が成立する．よって，$S \cup \tilde{E} \supseteq S$ であることと，(2), (4) より，

$$S_E \cup S_N \supseteq S \cap S \cap S \supseteq S \tag{5}$$

また，

$$S_E \cap S_N = (S \cap \tilde{E}) \cap (S \cap \tilde{N}) = S \cap (\tilde{E} \cap \tilde{N}) = \phi \tag{6}$$

以上 (5), (6) より，S_E, S_N は $S_E \cup S_N \supseteq S$, $S_E \cap S_N = \phi$ を満たす L^m の構成的部分集合である． ∎

これらの補題を基に，多項式集合 F から，その包括的多項式集合系 $\mathcal{P}$ を求めるアルゴリズムを記す．ただし，集合 A, B に対して，$A \wedge B := \{ab : a \in A, b \in B\}$ と定義する．

Algorithm 2 CPSS の構成（呼び出し）

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

output: F の包括的多項式項集合系 $\mathcal{P} = \{(E_1, N_1, \mathscr{T}_1), \ldots, (E_\ell, N_\ell, \mathscr{T}_\ell)\}$

1: **function** ParameterDivision(F)
2: **return** ParameterDivisionMain($\{(\phi, \{1\}, M_{\bar{X}}(F))\}$)
3: **end function**

単項式集合族または項集合族である $\mathscr{T}$ に対し，PolySet($\mathscr{T}$) を

$$\mathrm{PolySet}(\mathscr{T}) = \left\{ \sum_{t \in T} t \ : \ T \in \mathscr{T} \right\}$$

と定義する．

Algorithm 3 CPSS の構成（本体）

input: $\{(E, N, \mathcal{M})\}$（ただし $\mathcal{M} = \{M_1, \ldots, M_k\},\ N = \{a_N\},\ a_N \in K[\bar{A}]$ とする．）

output: PolySet($\mathcal{M}$) の $V(E) \setminus V(N)$ 上の包括的多項式項集合系 $\{(E_1, N_1, \mathscr{T}_1), \ldots, (E_{\ell'}, N_{\ell'}, \mathscr{T}_{\ell'})\}$

1: **function** ParameterDivisionMain($\{(E, N, \mathcal{M})\}$)
2: **if** $E \neq \phi \wedge \mathrm{ReducedGröbnerBasis}(E, \prec_{\bar{A}}) = \{1\}$ **then**
3: **return** ϕ
4: **end if**
5: **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**
6: **return** ϕ
7: **end if**
8: **if** $\forall i \in \{1, \ldots, k\},\ \forall m_i \in M_i,\ m_i \in K[\bar{X}]$ **then**
9: **return** $\{(E, N, \mathcal{M})\}$
10: **end if**
11: **if** $\forall j \in \{1, \ldots, \ell\},\ \exists m_j \in M_j,\ m_j \notin K[\bar{X}]$ **then**
12: $m \leftarrow m_j$
13: $c,\ t \leftarrow \mathrm{coeff}_{\bar{X}}(m),\ \mathrm{term}_{\bar{X}}(m)$
14: **end if**
15: $\mathcal{M}_E \leftarrow \{M_1, \ldots, M_{j-1}, M_j \setminus \{m\}, M_{j+1}, \ldots, M_k\})$
16: $\mathcal{M}_N \leftarrow \{M_1, \ldots, M_{j-1}, (M_j \cup \{t\}) \setminus \{m\}, M_{j+1}, \ldots, M_k\})$
17: **return** ParameterDivisionMain($E \cup \{c\}, N, \mathcal{M}_E$) $\cup$ ParameterDivisionMain($E, N \wedge \{c\}, \mathcal{M}_N$)
18: **end function**

補題 19

$E \neq \phi,\ N = \{a_N\} \neq \phi$ ($a_N \in K[\bar{A}]$) を仮定する．アルゴリズム *3* において，パラメータ制約 (E, N) が *inconsistent* であるとき，必ず *2*，*5* 行目の *if* 文の条件のうちのどちらか一方を満たす．

証明 パラメータ制約 (E, N) が inconsistent であるとき，$V(E) \setminus V(N) = \phi$ が成り立つ．$V(E) = \phi$ のとき，E の固定された項順序における $\langle E \rangle$ の簡約 Gröbner 基底は $\{1\}$ となる．つまり，2 行目の if 文に必ず入る．$V(E) \neq \phi$ のとき，$V(E) \subseteq V(N)$ が成り立つ．このとき，$a_N \in \sqrt{\langle E \rangle}$ を満たす．従って，新たな変数 $y \notin \bar{X} \cup \bar{A}$ に対して，集合 $\{E \cup \{1 - y \cdot a_N\}\}$ の簡約 Gröbner 基底が $\{1\}$ となる．つまり，5 行目の if 文に必ず入る．

∎

定理 20
アルゴリズム *3* は正当性と有限停止性を有する．

証明 まず，正当性を示す．
2，5 行目の if 文では，パラメータ制約が inconsistent な場合を検出している．逆にこのとき，補題 19 より，パラメータ制約が inconsistent な場合を全て検出することができている．
補題 17 より，8 行目の if 文の条件を満たす場合の包括的多項式項集合系は $\{(E, N, \mathcal{M})\}$ である．
11 行目の if 文では，8 行目の if 文の条件を満たしていないため，$M \in \mathcal{M}$ において係数にパラメータを含む単項式 m が必ず存在する．ここで，$S = V(E)\setminus V(N)$, $S_E = V(E \cup \{c\})\setminus V(N)$, $S_N = V(E)\setminus V(N \wedge \{c\})$ とする．補題 18 より，S_E, S_N は $S_E \cup S_N \supseteq S$, $S_E \cap S_N = \phi$ を満たす L^m の構成的部分集合である．これに加え，これまでの証明の中で，それぞれの if 文での出力の正当性が示されているため，最終的に関数を再帰的に呼び出す 11 行目の if 文の出力も正しいことが導かれ，アルゴリズム 3 の正当性が示された．
次に，アルゴリズム 3 の有限停止性を示す．4 つに分岐する if 文の中で，2, 5, 8 行目の if 文に入った場合は明らかに有限停止性を有する．11 行目の if 文に入った場合，$m \notin K[\bar{X}]$ を満たす単項式 m が存在するが，15, 16 行目にて，もともと m が属していた単項式集合 M_j から m が取り除かれるため，集合族 $\mathcal{M}_E$ 及び $\mathcal{M}_N$ 全体では，$m \notin K[\bar{X}]$ を満たす単項式は必ず 1 つ減っている．そのため，再帰呼び出しの中で必ず 8 行目の if 文の条件を満たすときが訪れるため，アルゴリズム 3 は有限停止性を有する． ∎

系 21
アルゴリズム *2* は正当性と有限停止性を有する．

3.2 パラメータ空間の分割の効率化

アルゴリズム 2, 3 で包括的多項式項集合系を直接的に構成し，各セグメントにおける SGBD の計算を行うことで comprehensive SGBD の問題を解くことが可能である．しかし，あくまでも直接的な方法であるため，効率的な方法であるとは言えない．例えば，次の例のように，SGBD の計算を踏まえたときに無駄なセグメントが発生してしまう可能性がある．

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

$$F = \left\{ f_1 = ax^3 + bx^2 + y,\ f_2 = y^3 + x \right\}$$

この例において，*CPSS* は次のようになる．

$$\mathcal{P} = \left\{ \begin{array}{l} P_1 = \left(\{a, b\}, \{\}, \{\{y\}, \{y^3, x\}\}\right), \\ P_2 = \left(\{a\}, \{b\}, \{\{x^2, y\}, \{y^3, x\}\}\right), \\ P_3 = \left(\{b\}, \{a\}, \{\{x^3, y\}, \{y^3, x\}\}\right), \\ P_4 = \left(\{\}, \{a, b\}, \{\{x^3, x^2, y\}, \{y^3, x\}\}\right) \end{array} \right\}$$

この $\mathcal{P}$ 自体は，パラメータ制約が *consistent* な *CPSS* の条件を満たしているが，セグメント P_4 では $f_1 = x^3 + x^2 + y$ となっているため，*SGBD* の計算を行うアルゴリズム *2.2.1* の *1*〜*9* 行目の *for* 文において x^2 が取り除かれてしまう．すなわち，$P_4 = (E_4, N_4, \{T_{4,1}, T_{4,2}\})$ から $b \in N_4$ と $x^2 \in T_{4,1}$ が必要なくなり，実質的に P_3 と等しいセグメントとなってしまっている．

このように，特にアルゴリズム 2.2.1 の 1〜9 行目の for 文を主な原因として，無駄なセグメントが発生してしまう可能性がある．

注意 2
次に 2 つの改善方法を述べるが，あくまでも *comprehensive SGBD* のためのパラメータ空間の分割の改善であり，何れにおいても *CPSS* を求めるものではないことに留意されたい．

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

affine Newton polyhedron は，項 $t \in T_n$ に関して取ると，各変数において t より次数の低い全ての項を得ることができる．つまり，$\mathcal{N}_{\mathrm{aff}}(t)$ は t を倍単項式として持つような項全体の集合と言い換えることができる（ただし，t 自身も含まれている）．よって，CPSS を構成するアルゴリズム 2, 3 の段階で項の affine Newton polyhedron を項集合から取り除くことで，アルゴリズム 2.2.1 の 1〜9 行目の一部に相当する手続きを予め行うことができる．つまり，アルゴリズム 3 の 16 行目において，

$$\mathcal{M}_N \leftarrow \{M_1, \ldots, M_{j-1}, (M_j \cup \{t\}) \setminus \{m\}, M_{j+1}, \ldots, M_k\})$$

としていたものを，

$$\mathcal{M}_N \leftarrow \{M_1, \ldots, M_{j-1}, (M_j \setminus \mathcal{N}_{\mathrm{aff}}(t)) \cup \{t\}, M_{j+1}, \ldots, M_k\})$$

と置き換えることで，これが実現可能となる．

3.2.2 加群 R^k の極小な包括的 Gröbner 基底系を用いた改善

3.2.1 節で述べたような改善は，加群の極小な包括的 Gröbner 基底系（CGS）を考えることでも可能となる．多項式集合 $F = \{f_1, \ldots, f_k\} \subset R$ において，多項式 $f_i \in F$ は単項式 $m_{ij} \in R$ を用いて

$$f_i = m_{i1} + m_{i2} + \cdots + m_{ir_i} \in F$$

と表されるものとする．ベクトル $\boldsymbol{e_i} \in \mathbb{R}^k$ は Kronecker delta δ_{ij} を用いて $\boldsymbol{e_i} = (\delta_{ij})$ と表されるものとする．このとき，加群 R^k の部分加群 $M = \langle H \rangle$ の生成系である H を次のように定める．

$$H = \bigcup_{i=1}^{k} \{m_{i1}\boldsymbol{e_i}, m_{i2}\boldsymbol{e_i}, \ldots, m_{ir_i}\boldsymbol{e_i}\} \subset R^k$$

部分加群 M の生成系は全て単項から成るため，H はそのまま包括的 Gröbner 基底（CGB）となっている．しかし，極小な CGS とはなっていない．極小な Gröbner 基底では，基底に存在する単項式 m_α, m_β が $m_\beta \mid m_\alpha$ を満たすとき，基底から m_α が取り除かれる．今，SGBD では倍単項式の存在する単項式を取り除きたいので，m_β が取り除きたい単項式である．そこで，多項式の次数を反転させるために，次を定義する．

定義 22 (反転多項式（reversal polynomial）)
多項式 $f(x_1, \ldots, x_n) \in K[\bar{X}]$ とベクトル $\boldsymbol{d} = (d_i) \in \mathbb{N}^n$ に対し，f の**反転多項式（*reversal polynoimal*）**を次式で定義し，$\mathrm{rev}_{\boldsymbol{d}}(f)$ で表す．

$$\mathrm{rev}_{\boldsymbol{d}}(f) = f(x_1^{-1}, \ldots, x_n^{-1}) \cdot \prod_{i=1}^{n} x_i^{d_i}$$

定理 23
$\mathrm{rev}_{\boldsymbol{d}}(\mathrm{rev}_{\boldsymbol{d}}(f)) = f$

証明

$$\begin{aligned}\mathrm{rev}_{\boldsymbol{d}}(\mathrm{rev}_{\boldsymbol{d}}(f)) &= f\left((x_1^{-1})^{-1}, \ldots, (x_n^{-1})^{-1}\right) \cdot \left(\prod_{i=1}^{n} x_i^{d_i}\right)^{-1} \cdot \prod_{i=1}^{n} x_i^{d_i} \\ &= f((x_1^{-1})^{-1}, \ldots, (x_n^{-1})^{-1}) \\ &= f(x_1, \ldots, x_n) \\ &= f\end{aligned}$$

∎

これらを踏まえて，部分加群の構成の段階から見直す．ベクトル $\boldsymbol{d}$ の要素 d_i を，多項式 $f = m_{i1} + m_{i2} + \cdots + m_{ir_i}$ における変数 $x_i \in \bar{X}$ の最大のべきとする．多項式 f のベクトル $\boldsymbol{d}$ における反転多項式を $\mathrm{rev}_{\boldsymbol{d}}(f) = m^\star_{i1} + m^\star_{i2} + \cdots + m^\star_{ir_i} =: f^\star$ とする．加群 R^k の部分加群 $M^\star = \langle H^\star \rangle$ を

$$H^\star = \bigcup_{i=1}^{k} \{m^\star_{i1}\boldsymbol{e_i}, m^\star_{i2}\boldsymbol{e_i}, \ldots, m^\star_{ir_i}\boldsymbol{e_i}\} \subset R^k$$

このとき，部分加群 $M^\star$ の極小な CGS を考える．今，単項式 $m^\star_\alpha, m^\star_\beta$ において，

$$m^\star_\alpha \mid m^\star_\beta \tag{7}$$

が成り立っているものとする．このとき，極小な CGS を考えると，$m^\star_\beta$ が基底から取り除かれる．ここで，再度 $f^\star$ のベクトル $\boldsymbol{d}$ における反転多項式を取ると，式 (7) より，各項において $\mathrm{rev}_{\boldsymbol{d}}(m^\star_\beta) \mid \mathrm{rev}_{\boldsymbol{d}}(m^\star_\alpha)$ が成り立つため，定理 23 より $m_\beta \mid m_\alpha$ が成り立ち，結果的に取り除きたい項である m_β を取り除くことができている．

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.