グレブナー基底の安定条件を求める新たな戦略
New computation method for stability conditions of Gröbner bases

鍋島克輔 *
東京理科大学理学部第一部応用数学科
NABESHIMA, Katsusuke
Department of Applied Mathematics, Tokyo University of Science

Abstract
Stability conditions of Gröbner bases are considered in the context of symbolic computation. New strategies for computing the stabitity conditions are introdcued. Moreover, a new algorithm for computing comprehensive Gröbner systems is given as the application.

1 序

パラメータ付き代数方程式系を解析するための強力な道具の1つとして，包括的グレブナー基底系が知られている．包括的グレブナー基底系は，パラメータ付きグレブナー基底のことであり，1992年にWeispfenning [18] にその概念と計算アルゴリズムが紹介されたあと，Weispfenning 自身 [19, 20]，Montes [7, 8], 鈴木-佐藤 [14, 15, 16]，Kapur-Sun-Wang [5, 6], 鍋島 [10, 12] らにより理論と効率的な計算法が研究されていると共に，多くの応用も紹介されている [9].

本稿では，Kalkbrener [4] によって紹介されたグレブナー基底の安定性を包括的グレブナー基底系計算アルゴリズムに利用した鈴木-佐藤 [16] アルゴリズムの改良を念頭に置き，新たなグレブナー基底の安定条件を求める計算法を紹介し，また，新たな包括的グレブナー基底系計算アルゴリズムも紹介する．

鈴木-佐藤 [16] アルゴリズムの改良として，Kapur-Sun-Wang [5, 6] アルゴリズムと鍋島 [12] アルゴリズムがある．両アルゴリズム共に，より良いグレブナー基底の安定条件を求める方法が包括的グレブナー基底系計算の鍵となっているが，安定条件を求める計算方法は両アルゴリズム共に本質的には同じである．したがって，ある安定条件が計算量の観点から得られなければ，両アルゴリズム共に包括的グレブナー基底系が得られないことが多々ある．そこで，新たなグレブナー基底の安定条件を求める計算方法が望まれており，本稿では，主結果として新たなグレブナー基底の安定条件を求める計算法を与え，また，応用として，主結果を用いた包括的グレブナー基底系計算アルゴリズムについて述べる．

2 準備

ここでは，本稿で用いる記号と定義を紹介する．n 変数 $x_1,\ldots,x_n$ の省略形を x で表わし，m 変数 $t_1,\ldots,t_m$ の省略形を t とし $x \cap t \neq \emptyset$ とする．次節以降では変数 x を主変数をして扱い変数 t をパラメータとして扱う．K を体とし，K を含む代数的閉体を $\bar{K}$ とする．

*nabeshima@rs.tus.ac.jp

係数を $K[t]$ に持つ多項式環を $K[t][x]$ で表す．主変数 x に関する項順序 $\succ_x$ を固定し $f \in K[t][x]$ とする．このとき，f の先頭項，先頭係数，先頭単項をそれぞれ $\mathrm{lpp}_x(f), \mathrm{lc}_x(f), \mathrm{lm}_x(f)$ で表す．ただし，$\mathrm{lm}_x(f) = \mathrm{lc}_x(f)\,\mathrm{lpp}_x(f)$ である．添え字に主変数の x があること注意する．また，集合 $F \subset K[t][x]$ に対して，$\mathrm{lpp}_x(F) = \{\mathrm{lpp}_x(g) | g \in F\}$，$\mathrm{lc}_x(F) = \{\mathrm{lc}_x(g) | g \in F\}$，$\mathrm{lm}_x(F) = \{\mathrm{lm}_x(g) | g \in F\}$ とする．

多項式環 $K[t,x]$ でのブロック項順序を $(\succ_x, \succ_t)$ で表わす．ただし，変数 x における項順序は $\succ_x$ であり，変数 t における項順序は $\succ_t$ であり $x \gg t$ である．

$F \subset K[t]$ とする．アフィン代数多様体を $\mathbb{V}(F) = \{\bar{a} \in \bar{K}^m | f(\bar{a} = 0, f \in F\}$ で定める．また，環 R を $K[t,x]$ もしくは $K[t][x]$ とする．このとき，$f_1, \ldots, f_s \in R$ としたとき，$f_1, \ldots, f_s$ で生成されるイデアルを

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_1 f_i \,\middle|\, h_1, \ldots, h_s \in R \right\}$$

で表わす．

本稿では，係数を $K[t]$ に持つ多項式環 $K[t][x]$ 上でのイデアルの議論を行う．多項式環 $K[t][x]$ でのイデアルのグレブナー基底は次のように定義される．

定義 1 $K[t][x]$ での項順序 $\prec_x$ を固定する．イデアル $I \subset K[t][x]$ の有限部分集合 $G = \{g_1, \ldots, g_r\}$ がもし，

$$\langle \mathrm{lm}_x(g_1), \mathrm{lm}_x(g_2), \ldots, \mathrm{lm}_x(g_r) \rangle = \langle \mathrm{lm}_x(I) \rangle$$

を満たすならば，G は $\succ_x$ に関する I のグレブナー基底である．

多項式環 $K[t][x]$ のイデアル I のグレブナー基底計算は，I を多項式環 $K[t,x]$ のイデアルと見なし，$x \gg t$ となるブロック項順序 $(\succ_x, \succ_t)$ を用いて，I のグレブナー基底 G を $K[t,x]$ で計算すると，G は $K[t][x]$ 上でのイデアル I のグレブナー基底にもなっている．すなわち，グレブナー基底 G は $K[t][x]$ 上で I での $\succ_x$ に関するグレブナー基底となっている．

(注意) ブロック項順序を用いて得られたグレブナー基底 G は，たとえ $K[t,x]$ 上で簡約グレブナー基底を得たとしても，$K[t][x]$ 上では簡約グレブナー基底になっているとは限らない．多くの場合，G には冗長性があるが，計算速度の観点からブロック項順序を用いた計算法を採用する．他の計算法もしくは $K[t][x]$ 上での簡約グレブナー基底に関しては [1, 11] に詳しく書かれているが，計算量は大きくなる．

定義 2 (極大独立集合) I を空でない $K[x]$ のイデアルとし，$\{u_1, \ldots, u_r\}$ を $\{x_1, \ldots, x_n\}$ の部分集合とする．もし，$I \cap K[u_1, \ldots, u_r] = \{0\}$ であれば，$\{u_1, \ldots, u_r\}$ を I の独立集合という．また，I の独立集合 $\{u_1, \ldots, u_r\}$ がどの I の独立集合も含まないとき，$\{u_1, \ldots, u_r\}$ を I の極大独立集合と呼ぶ．

$u = \{u_1, \ldots, u_r\}$ をイデアル $I \subset K[x]$ の極大独立集合とする．このとき，I は $K(u)[x \backslash u]$ でゼロ次元イデアルとなる．ただし，$K(u)$ は変数 u を持つ有理関数体である．極大独立集合は I のグレブナ—基底を計算することにより，求めることができる [2, 3].

3　グレブナー基底の安定性

本節では，先行研究で紹介されている具体的なグレブナー基底の安定条件とその計算法についてに復習する．ここでは，単項式の集合 $T \subset K[x]$ から生成されるイデアルの極小基底を $\mathrm{MB}(T)$ で表わす．

定理 3 (Kapur-Sun-Wang[5, 6]) $F \subset K[t][x]$ を有限部分集合，$\prec_x$ を x の項順序とする．F を $K[t,x]$ の集合と見做しブロック項順序 $(\prec_x, \prec_t)$ に関して $\langle F \rangle$ の簡約グレブナー基底を G とする．G を $K[t][x]$ の集合と見做し，$E = G \cap K[t]$，$T = \{\mathrm{lpp}_x(g) | g \in G \backslash E\}$, $\mathrm{MB}(T) = \{m_1, \ldots, m_r\} \subset K[x]$ とする．各 $1 \le i \le r$ に対して，$G_{m_i} = \{g | \mathrm{lpp}_x(g) = m_i, g \in G\}$ とする．各 G_{m_i} から *1* 個の多項式 p_i をとり，$h = \sqrt{\prod_{i=1}^r \mathrm{lc}_x(p_i)} \in K[t]$ とする．ただし，$\sqrt{\prod_{i=1}^r \mathrm{lc}_x(p_i)}$ は $\prod_{i=1}^r \mathrm{lc}_x(p_i)$ の無平方多項式とする．

このとき，$\bar{a} \in \mathbb{V}(E) \backslash \mathbb{V}(h) \subset \bar{K}^m$ において，$\sigma_{\bar{a}}(\{p_1, \ldots, p_r\})$ は $\prec$ に関して，$\langle \sigma_{\bar{a}}(F) \rangle$ の極小グレブナー基底となる．

例 4 $F = \{sx^2 - xy + y^2, txy + y, sx^2 - y, (t+1)xy^2 + sx\} \subset \mathbb{C}[s,t][x,y]$ とする．項順序として $\succ_{\{x,y\}}$ は辞書式項順序，$\succ_{\{s,t\}}$ は全次数逆辞書式とし，ブロック項順序 $(\succ_{\{x,y\}}, \succ_{\{s,t\}})$ において，$\langle F \rangle$ の簡約グレブナー基底 G を $\mathbb{C}[s,t,x,y]$ で計算すると次となる．

$$G = \{(s+t^2+t)y, ((-t+2)s-1)y, (s^2+6s-t-3)y, -y^2+(s+2t+1)y, sx+ty, xy+(-s-2t-2)y\}$$

また，$\mathrm{lpp}_{\{x,y\}}(G) = \{y, y^2, x, xy\}$ なので，$\mathrm{MB}(\mathrm{lpp}_{\{x,y\}}(G)) = \{x, y\}$ となり，

$$G_x = \{sx+ty\},\ G_y = \{(s+t^2+t)y, ((-t+2)s-1)y, (s^2+6s-t-3)y\}$$

である．G_x, G_y からそれぞれ *1* つの元をとり $\{sx+ty, (s+t^2+t)y\}$ を考えると，$\forall a \in \mathbb{C}^2 \backslash \mathbb{V}(s(s+t^2+t))$ のとき，$\sigma_a(\{sx+ty, (s+t^2+t)y\})$ は $\succ_{\{x,y\}}$ に関して $\langle \sigma_a(F) \rangle$ の極小グレブナー基底である．

定理 5 (鍋島) $F \subset K[t][x]$ を有限部分集合，$\prec_x$ を x の項順序とする．F を $K[t,x]$ の集合と見做しブロック項順序 $(\prec_x, \prec_t)$ に関しての $\langle F \rangle$ の簡約グレブナー基底を G とする．G を $K[t][x]$ の集合と見做し，$E = G \cap K[t]$，$T = \{\mathrm{lpp}_x(g) | g \in G \backslash E\}$, $\mathrm{MB}(T) = \{m_1, \ldots, m_r\} \subset K[x]$ とする．各 $1 \le i \le r$ に対して，$G_{m_i} = \{g | \mathrm{lpp}_x(g) = m_i, g \in G\}$ とする．

このとき，$\bar{a} \in \mathbb{V}(E) \backslash (\mathbb{V}(G_{m_1}) \cup \mathbb{V}(G_{m_2}) \cup \cdots \cup \mathbb{V}(G_{m_r})) \subset \bar{K}^m$ において，$\sigma_{\bar{a}}(\{p_1, \ldots, p_r\})$ は $\prec_x$ に関して，$\langle \sigma_{\bar{a}}(G_{m_1} \cup \cdots \cup G_{m_r}) \rangle$ のグレブナー基底となる．

例 6 例 *4* と同じパラメータ付きイデアルを考える．

$$G_x = \{sx+ty\},\ G_y = \{(s+t^2+t)y, ((-t+2)s-1)y, (s^2+6s-t-3)y\}$$

であるので，$\forall a \in \mathbb{C}^2 \backslash \left(\mathbb{V}(s) \cup \mathbb{V}(s+t^2+t, (-t+2)s-1, s^2+6s-t-3)\right)$ のとき，$\sigma_a(G_x \cup G_y)$ は $\succ_{\{x,y\}}$ に関して $\langle \sigma_a(F) \rangle$ のグレブナー基底である．

定理 3，定理 5 共に $\langle F \rangle$ を $K[t,x]$ の集合と見做しブロック項順序 $(\prec_x, \prec_t)$ に関しての簡約グレブナー基底を G を計算する必要がある．すなわち，このグレブナー基底 G が計算できなければ『パラメータの条件』と『グレブナー基底』の両方が得ることができない．計算面において，この簡約グレブナー基底 G を計算することがボトルネックである．

4 安定条件の新たな計算法

ここでは，$K(t)$ を変数 t の有理関数体とする．また，$g \in K(t)[x]$ のとき，$\mathrm{dlcm}(g) \subset K[t]$ を g の各係数分母の最小公倍元とする．

定理 7 $F \subset K[t][x]$ を有限部分集合，x の項順序 $\prec_x$ を固定する．F を $K(t)[x]$ の集合と見做し $\langle F \rangle \subset K(t)[x]$ の簡約グレブナー基底を G' とし，$G = \{\mathrm{dlcm}(g)g | g \in G'\} \subset K[t][x]$ とする．また，$h = \prod_{g \in G} \mathrm{lc}_x(g)$ とし，イデアル商 $\langle F \rangle : \langle G \rangle \subset K[t,x]$ のブロック項順序 $(\prec_t, \prec_x)$ での簡約グレブナー基底を S とする．このとき，

(i) $S \cap K[t] \neq \emptyset$,

(ii) 任意の $\bar{a} \in \bar{K}^m \backslash (\mathbb{V}(S \cap K[t]) \cup \mathbb{V}(h))$ において，$\sigma_{\bar{a}}(G)$ は $\prec_x$ に関して $\langle \sigma_{\bar{a}}(F) \rangle$ のグレブナー基底である．

例 8 例 *4* と同じパラメータ付きイデアルを考える．$F = \{sx^2 - xy + y^2, txy + y, sx^2 - y, (t+1)xy^2 + sx\} \subset \mathbb{C}[s,t][x,y]$ であり，$\succ_{\{x,y\}}$ は辞書式項順序，$\succ_{\{s,t\}}$ は全次数逆辞書式であった．

$\mathbb{C}(s,t)[x,y]$ での $\succ_{\{x,y\}}$ に関しての $\langle F \rangle$ の簡約グレブナー基底は

$$G_0 = \{x, y\}$$

であり，G_0 の全ての要素の先頭係数は *1* である．

次に，ブロック項順序 $(\succ_{\{x,y\}}, \succ_{\{s,t\}})$ においてイデアル商 $\langle F \rangle : \langle G_0 \rangle$ の簡約グレブナー基底 S を $\mathbb{C}[s,t,x,y]$ で計算すると

$$S = \{s^2 + (t^2+t)s, (-t+2)s^2 - s, s^3 + 6s^2 + (-t-3)s, y - 2s^2 + (-5t-3)s, sx - s^2 + (-2t-2)s\}$$

となる．

$$S \cap \mathbb{C}[s,t] = \{s^2 + (t^2+t)s, (-t+2)s^2 - s, s^3 + 6s^2 + (-t-3)s\}$$

なので，$\mathbb{C}^2 \backslash \mathbb{V}(s^2 + (t^2+t)s, (-t+2)s^2 - s, s^3 + 6s^2 + (-t-3)s)$ のとき，$\{x, y\}$ が簡約グレブナー基底である．

これは，例 *6* において得たパラメータの条件と同じになっていることに注意する．

定理 7 では，集合 $S \cap K[t]$ を考えたが，$g \in S \cap K[t]$ において，$\mathbb{V}(S \cap K[t]) \subset \mathbb{V}(g)$ であるので次の系が簡単に成り立つ．

系 9 $F \subset K[t][x]$ を有限部分集合，x の項順序 $\prec_x$ を固定する．F を $K(t)[x]$ の集合と見做し $\langle F \rangle \subset K(t)[x]$ の簡約グレブナー基底を G' とし，$G = \{\mathrm{dlcm}(g)g | g \in G'\} \subset K[t][x]$ とする．また，$h = \prod_{g \in G} \mathrm{lc}_x(g)$ とし，イデアル商 $\langle F \rangle : \langle G \rangle \subset K[t,x]$ のブロック項順序 $(\prec_t, \prec_x)$ での簡約グレブナー基底を S とし，$g \in S \cap K[t]$ とする．

このとき，任意の $\bar{a} \in \bar{K}^m \backslash (\mathbb{V}(g) \cup \mathbb{V}(h))$ において，$\sigma_{\bar{a}}(G)$ は $\prec_x$ に関して $\langle \sigma_{\bar{a}}(F) \rangle$ のグレブナー基底である．

例 10 例 *8* を再び考える．

$$S \cap \mathbb{C}[s,t] = \{s^2 + (t^2+t)s, (-t+2)s^2 - s, s^3 + 6s^2 + (-t-3)s\}$$

であるので，$s^2 + (t^2+t)s \in S \cap \mathbb{C}[s,t]$ を選択する．系 *9* より，$\mathbb{C}^2 \backslash \mathbb{V}(s^2 + (t^2+t)s)$ のとき，$\{x, y\}$ が簡約グレブナー基底である．

これは，例 *4* において得たパラメータの条件と同じになっていることに注意する．

定理 3 と 5 では，$\langle F \rangle$ を $K[t][x]$ のグレブナー基底計算を 1 度するだけで必要な情報を得ているのに対し，定理 7 は以下の 2 つのステップを踏んでいる．

(1) $\langle F \rangle \subset K(t)[x]$ の簡約グレブナー基底を計算.

(2) $K[t,x]$ 上でイデアル商 $\langle F \rangle : \langle G \rangle$ のグレブナー基底を $x \gg t$ となるブロック項順序で計算.

図 1: Method 1 vs Method 2

Method 1		**Method 2**
大きなグレブナー基底を $K[t,x]$ で 1 度だけ計算.	VS	(1) $K(t)[x]$ でグレブナー基底を計算. (2) イデアル商を計算.

(1) ではグレブナー基底の形を求め，(2) ではグレブナー基底となるパラメータの条件を計算している．すなわち，グレブナー基底計算とパラメータの条件の計算を個別に行っていることになる．

定理 3 や 5 のように $K[t,x]$ 上で大きなグレブナー基底を 1 度だけ計算する方法を Method 1 とし，定理 7 のようにそれぞれ個別に計算する方法を Method 2 とする．

現在まで Method 1 のみが計算法として知られていたが，今回，新たに Method 2 を紹介した．これにより，計算できなかったものが計算できるようになると思われる．(図 1 は Method 1 と Method 2 の比較をイメージ的にまとめたものである.)

次の 9 個の問題において Method 1 と Method 2 の計算速度比較を行う．ここでは，x, y, z を変数とし，a, b をパラメータする．

```
F1=[x^4+y^2*x+y^3,y^3+x^3+b*x^3*y,x^3*y^3+y^4+a*x*y];
F2=[x^4+y^2*x+y^3,y^3+x^3+b*x^3*y,x^3*y^3+y^4+a*x^2*y];
F3=[a*y^2*x^5+y^2*x+a*y,y^2*x^4+x^3+y^2,b*y*x^6+x^2];
F4=[x^5+a*y^3+b*x^2*y+5*y,x^2*y^2+x^3*y^2+y,4*x^5*y+x^2*y^6+y^2+b*x^5,x^3+x*y^3];
F5=[x^3+a*x^4+b*x*y+5*y,x^2*y+a*x^3*y^2+y^4,4*x^5*y+x*y^6+y^2+b*x^5*y^2,x^3+y^3+x*y^3];
F6=[x^5+a*y^2+x*z^3,y^5*z^2+x^3*y,x^3*y+x^2*y^4*z,x^2*y*z+x^3+b];
F7=[x^5+y^2*x+a*y^3,y^3*x^3+x^2+b*x^3*y,x^3*y+y^4+x*y];
F8=[x^6+y^2*x+a*y^3,x^3+y^2,y^3*x^3+x^2+b*x^3*y,x^3*y+y^4+x^2*y];
F9=[x^6+y^2*x+a*y^3,x^6+y^5,y^3*x^3+x^2+b*x^3*y,x^4*y+x^3+a*x^2*y];
```

用いた計算機は [Win11, CPU:i5-8265U 1.6GHz, Mem:16Gb] であり，計算機代数システム Risa/Asir を用いた．Method 1 の計算には

```
nd_gr(F,[x,y,z,a,b],0,[[0,3],[0,2]])
```

を用い，Method 2 の計算には

```
nd_gr(noro_pd.ideal_colon(F,nd_gr(F,[x,y,z],0,0),[x,y,z,a,b]),[x,y,z,a,b],[[0,3],[0,2]])
```

を用いた．`nd_gr` がグレブナー基底計算コマンドを表し，`noro_pd.ideal_colon` はイデアル商計算コマンドを表す．表 1 の単位は CPU 秒であり，>10m は，出力を得るには 10 分以上かかることを意味する．

表 1: 計算速度比較

問題	Method 1	Method 2
F1	>10m	2.391
F2	1.781	47.3
F3	0.8281	12.89
F4	>10m	4.859
F5	>10m	33.47
F6	8.172	14.33
F7	>10m	0.9688
F8	>10m	0.01563
F9	>10m	53.77

Method 1, Method 2 のどちらかが絶対的に速いということはないが，Method 2 に適した問題がそれなりに存在し，Method 1 では現実的な時間では結果が得られなかったものが，Method 2 では結果が得られている．

定理 7 を更に一般化させたものが次の定理である．

定理 11 $K[t]$ の有限部分集合を E とし，$\langle E\rangle$ の極大独立集合を $u \subset t$ とする．$K[t][x]$ の有限部分集合を F とし，E と F を $K(u)[t\backslash u, x]$ の集合と見做し，$K(u)[t\backslash u, x]$ において $\langle F \cup E\rangle$ の $(\succ_x, \succ_{t\backslash u})$ に関する簡約グレブナー基底を G' とする．また，$G'' = \{\mathrm{dlcm}(g)g | g \in G'\} \subset K[t][x]$，$G = G''\backslash(G'' \cap E)$, $h = \prod_{g\in G} \mathrm{lc}_x(g)$, イデアル商 $\langle F \cup E\rangle : \langle G\rangle \subset K[t, x]$ の $(\succ_x, \succ_t)$ に関する簡約グレブナー基底を S とする．このとき，次が成り立つ．

(i) $S \cap K[t] \neq \emptyset$.

(ii) 任意の $\bar{a} \in \mathbb{V}(E)\backslash(\mathbb{V}(h) \cup \mathbb{V}(S \cap K[t])) \subset \bar{K}^m$ において，$\sigma_{\bar{a}}(G)$ は $\prec_x$ に関して，$\langle\sigma_{\bar{a}}(F)\rangle$ の簡約グレブナー基底となる．

例 12 $E = \{s^2 + t\} \subset \mathbb{C}[s, t]$ と $F = \{x^2y - sxy, xy^2 + x^2y + xy, sy^2 - tx^2\} \subset \mathbb{C}[s, t][x, y]$ を考える．ここでは，$x \succ_{\{x,y\}} y$ となる辞書式項順序 $\succ_{\{x,y\}}$ を用いる．$\langle E\rangle$ における極大独立集合の一つは $\{t\}$ である．($\{s\}$ としても定理 *11* は成り立つがここでは $\{t\}$ の場合を考える.)

- $\mathbb{C}(t)[s, x, y]$ での $\langle F \cup E\rangle$ のブロック項順序 $(\succ_{\{x,y\}}, \succ_{\{s\}})$ 簡約グレブナー基底で分母を払ったものは

$$G'' = \{s^2 + t, y^3, xy, tx^2 - sy^2\}$$

である．

- $G = G''\backslash(G'' \cap \langle E\rangle) = \{y^3, xy, tx^2 - sy^2\}$,
- $h = t$,
- イデアル商 $\langle F \cup E\rangle : \langle G\rangle \subset K[t, x]$ の $(\succ_x, \succ_t)$ に関する簡約グレブナー基底は

$$S = \{st-s-t^2+2t, -s^2-t, s-t^3+2t^2-t, ty+s+t^2-t, sy+s-t, -tx+s+t^2-2t, sx+t, xy+x-t, x^2+t\}$$

となる．よって，

$$S \cap \mathbb{C}[s,t] = \{st - s - t^2 + 2t, -s^2 - t, s - t^3 + 2t^2 - t\}$$

である．

したがって，パラメータ (s,t) が

$$\mathbb{V}(s^2+t)\backslash\left(\mathbb{V}(t) \cup \mathbb{V}(st - s - t^2 + 2t, -s^2 - t, s - t^3 + 2t^2 - t)\right)$$

に属するならば,

$$\{y^3, xy, tx^2 - sy^2\}$$

が $\langle F \rangle$ の $\succ_{\{x,y\}}$ に関する簡約グレブナー基底となる．

次に，定理 7 と定理 11 を利用した包括的グレブナー基底系計算アルゴリズムについてみる．

定義 13 (包括的グレブナー基底系) F を $K[t][x]$ の有限部分集合，$\mathbb{A}_1, \mathbb{A}_2, \ldots, A_\ell$ を $\bar{K}^m$ の代数構造的集合, $G_1, G_2, \ldots, G_\ell$ を $K[t][x]$ の有限部分集合とする．このとき，ペアの有限部分集合 $\mathcal{G} = \{(\mathbb{A}_1, G_1), (\mathbb{A}_2, G_2), \ldots, (G_\ell, G_\ell)\}$ が $\cup_{i=1}^{\ell} \mathbb{A}_i$ 上で $\langle F \rangle$ の包括的グレブナー基底系（*Comprehensive Gröbner system (CGS)*）であるとは，任意の $\bar{a} \in \mathbb{A}_i$ において，$\sigma_{\bar{a}}(G_i)$ が $\bar{K}[x]$ 上のイデアル $\langle \sigma_{\bar{a}}(F) \rangle$ のグレブナー基底であることである．また，各 $(\mathbb{A}_i, G_i)$ を $\mathcal{G}$ の断片といい，もし，$\cup_{i=1}^{\ell} \mathbb{A}_i = \bar{K}^m$ であれば，$\mathcal{G}$ を単に $\langle F \rangle$ の包括的グレブナー基底系という．

定理 7 と定理 11 を用いることにより，次のように包括的グレブナー基底系計算アルゴリズムを構成することができる．

アルゴリズム (CGS)

Specification: CGS$(E, N, F, \succ)$
$\mathbb{V}(E)\backslash\mathbb{V}(N)$ 上での $\langle F \rangle$ の包括的グレブナー基底系の計算.
入力: $E, N \subset K[t]$, $F \subset K[t][x]$, $\succ$: x における項順序,
出力: $\mathcal{G}$: $\mathbb{V}(E)\backslash\mathbb{V}(N)$ 上で $\succ$ に関しての $\langle F \rangle$ の包括的グレブナー基底系.
BEGIN
$\mathcal{G} \leftarrow \emptyset$;
if $\mathbb{V}(E)\backslash\mathbb{V}(N) = \emptyset$ **then**
  return $\mathcal{G}$;
end-if
$u \leftarrow \langle E \rangle \subset K[t]$ の極大独立集合;
$G \leftarrow \langle F \cup E \rangle \subset K(u)[t\backslash u, x]$ の $(\succ, \succ_{t\backslash u})$ に関する簡約グレブナー基底;
if $1 \in G$ **then**
  $\mathcal{G} \leftarrow \mathcal{G} \cup \{(\mathbb{V}(E)\backslash\mathbb{V}(N), \{1\})\}$;
  return $\mathcal{G}$;
end-if
$G' \leftarrow G\backslash G \cap \langle E \rangle$;
$h \leftarrow \sqrt{\prod_{g \in G'} \mathrm{lc}_x(g)}$;
$S \leftarrow$ イデアル商 $\langle F \cup E \rangle : \langle G' \rangle$ の $(\succ, \succ_t)$ に関する簡約グレブナー基底;
$E_1 \leftarrow S \cap K[t]$;
if $(\mathbb{V}(E)\backslash\mathbb{V}(\{h\} \wedge E_1))\backslash\mathbb{V}(N) \neq \emptyset$ **then**

$\mathcal{G} \leftarrow \mathcal{G} \cup \{(\mathbb{V}(E) \backslash \mathbb{V}((\{h\} \wedge E_1) \wedge N), G')\}$;
end-if
$h_1 h_2 h_3 \cdots h_\ell \leftarrow h$ の素因子分解;
$\{P_1, \ldots, P_r\} \leftarrow$ 根基イデアル $\sqrt{E_1}$ の素イデアル分解; /*P_i は素イデアルの基底*/
$\mathcal{G} \leftarrow \mathcal{G} \cup \mathrm{CGS}(E \cup \{h_1\}, N, F, \succ) \cup \mathrm{CGS}(E \cup \{h_2\}, N \wedge \{h_1\}, F, \succ) \cup \mathrm{CGS}(E \cup \{h_3\}, N \wedge \{h_1 h_2\}, F, \succ) \cup$
$\cdots \cup \mathrm{CGS}(E \cup \{h_\ell\}, N \wedge \{h_1 \cdots h_{\ell-1}\}, F, \succ) \cup$
$\cup \mathrm{CGS}(P_1, N \wedge \{h\}, F, \succ) \cup \mathrm{CGS}(P_2, N \wedge \{h\} \wedge P_1, F, \succ) \cup \mathrm{CGS}(P_3, N \wedge \{h\} \wedge P_1 \wedge P_2, F, \succ) \cup$
$\cdots \cup \mathrm{CGS}(P_r, N \wedge \{h\} \wedge P_1 \wedge \cdots \wedge P_{r-1}, F, \succ)$;
return $\mathcal{G}$;
END
(注意：$A, B \subset K[U]$, $A \wedge B = \{pq \mid p \in A, q \in B\}$)

(注意 1) 任意の $f \in K[t, x]$，$p \in \langle E \rangle$ において，$fp \in \langle E \rangle \subset \langle F \cup E \rangle$ であるので，$\langle E \rangle \subset \langle F \cup E \rangle : \langle G' \rangle$ となる．したがって，$E \subset \langle E_1 \rangle \subset \langle P_i \rangle \subset K[t]$ となる．
(注意 2) 実際は，$N \wedge \{h\} \wedge P_1 \wedge \cdots \wedge P_{r-1}$ は計算する必要はなく，$((((\langle P_r \rangle : h^\infty) : \langle P_1 \rangle^\infty) : \cdots) : \langle P_{r-1} \rangle^\infty$ が $\langle 1 \rangle$ になるかどうかで空集合のチェックはできるので，そのままの形で保存することができるが，アルゴリズムの "分かりやすさ" と "シンプルさ" を重視し上のように書いた．また，最適化も含めた多くの計算テクニック [6, 9, 13, 15] も省いている．

例 14 $F = \{sx^2 - xy + y^2, txy + y, sx^2 - y, (t+1)xy^2 + sx\} \subset \mathbb{C}[s, t][x, y]$ とする．項順序として $\succ_{\{x,y\}}$ は辞書式項順序，$\succ_{\{s,t\}}$ は全次数逆辞書式とし，ブロック項順序 $(\succ_{\{x,y\}}, \succ_{\{s,t\}})$ とする．例 *8* より，

- パラメータが $\mathbb{C}^2 \backslash \mathbb{V}(s^2 + (t^2 + t)s, (-t+2)s^2 - s, s^3 + 6s^2 + (-t-3)s)$ に属するとき，$\{x, y\}$ が $\succ_{\{x,y\}}$ に関して簡約グレブナー基底である．

次に，根基イデアル $\sqrt{\langle s^2 + (t^2 + t)s, (-t+2)s^2 - s, s^3 + 6s^2 + (-t-3)s \rangle}$ の素イデアル分解を計算すると

$$\sqrt{\langle s^2 + (t^2 + t)s, (-t+2)s^2 - s, s^3 + 6s^2 + (-t-3)s \rangle} = \langle s \rangle \cap \langle t^3 - t^2 - 2t - 1, s + t^2 + t \rangle$$

となる．

(1) $E = \{s\}$ とし，定理 *11* を適用する．$\langle E \rangle \subset \mathbb{C}[s, t]$ の極大独立集合は $\{t\}$ である．$\mathbb{C}(t)[s, x, y]$ において $\langle F \cup E \rangle$ の $(\succ_{\{x,y\}}, \succ_{\{s\}})$ に関する簡約グレブナー基底 G_1 は

$$G_1 = \{s, y\}$$

である．$G'_1 = G_1 \backslash G_1 \cap \langle E \rangle = \{y\}$ とする．イデアル商 $\langle F \cup E \rangle : \langle G'_1 \rangle$ の $(\succ_{\{x,y\}}, \succ_{\{s,t\}})$ に関する簡約グレブナー基底は $\{1\}$ である．したがって，

- パラメータが $\mathbb{V}(s)$ に属するとき，$\{y\}$ が $\succ_{\{x,y\}}$ に関しての簡約グレブナー基底となる．

(2) $E = \{t^3 - t^2 - 2t - 1, s + t^2 + t\}$ とし，定理 *11* を適用する．$\langle E \rangle \subset \mathbb{C}[s, t]$ はゼロ次元イデアルなので極大独立集合は空集合である．$\mathbb{C}[s, t, x, y]$ において $\langle F \cup E \rangle$ の $(\succ_{\{x,y\}}, \succ_{\{s,t\}})$ に関する簡約グレブナー基底 G_2 は

$$G_2 = \{[s + t^2 + t, (-t+2)s - 1, s^2 + 6s - t - 3, y^2 - (s + 2t + 1)y, x + (s + 3t)y]\}$$

であり，$s+t^2+t, (-t+2)s-1, s^2+6s-t-3 \in \langle E\rangle$ であるので

$$G'_2 = G_2 \backslash G_2 \cap \langle E\rangle = \{y^2-(s+2t+1)y, x+(s+3t)y\}$$

とする．イデアル商 $\langle F\cup E\rangle : \langle G'_2\rangle$ の $(\succ_{\{x,y\}}, \succ_{\{s,t\}})$ に関する簡約グレブナー基底は $\{1\}$ である．したがって，

- パラメータが $\mathbb{V}(t^3-t^2-2t-1, s+t^2+t)$ に属するとき，$\{y^2-(s+2t+1)y, x+(s+3t)y\}$ が $\succ_{\{x,y\}}$ に関して簡約グレブナー基底である．

以上より，$\langle F\rangle$ の包括的グレブナー基底系 $\mathcal{G}$ は

$$\begin{aligned}\mathcal{G} \;=\; & \big\{(\mathbb{C}^2\backslash\mathbb{V}(s^2+(t^2+t)s, (-t+2)s^2-s, s^3+6s^2+(-t-3)s), \{x,y\}),\\ & (\mathbb{V}(s), \{y\}),\\ & (\mathbb{V}(t^3-t^2-2t-1, s+t^2+t), \{y^2-(s+2t+1)y, x+(s+3t)y\}\big\}\end{aligned}$$

となる．

例 15 $F = \{y^4-sx^3y^2, sy^3+tx^3y^2+x^4+x, txy^3+x^3y^2\} \subset \mathbb{C}[s,t][x,y]$ とする．項順序として $\succ_{\{x,y\}}$ は辞書式項順序, $\succ_{\{s,t\}}$ は全次数逆辞書式とし，ブロック項順序 $(\succ_{\{x,y\}}, \succ_{\{s,t\}})$ とする．

(1) $\mathbb{C}(s,t)[x,y]$ において，$\langle F\rangle$ の $\succ_{\{x,y\}}$ に関する簡約グレブナー基底は

$$G_1 = \{y^4, xy^2, x^4+x+sy^3\}$$

であり，イデアル商 $\langle F\rangle : \langle G_1\rangle$ の $(\succ_{\{x,y\}}, \succ_{\{s,t\}})$ に関する簡約グレブナー基底は

$$\{s^6t^{11}-s^6t^7+s^3t^6+1, y+s^2t^3, x-st^2\}$$

である．

したがって，断片

$$(\mathbb{C}^2\backslash\mathbb{V}(s^6t^{11}-s^6t^7+s^3t^6+1), \{y^4, xy^2, x^4+x+sy^3\})$$

を得る．根基イデアル $\sqrt{\langle s^6t^{11}-s^6t^7+s^3t^6+1\rangle}$ の素イデアル分解は

$$\sqrt{\langle s^6t^{11}-s^6t^7+s^3t^6+1\rangle} = \langle s^6t^{11}-s^6t^7+s^3t^6+1\rangle$$

である．

(2) $E = \{s^6t^{11}-s^6t^7+s^3t^6+1\}$ とし，定理 *11* を適用する．$\langle E\rangle \subset \mathbb{C}[s,t]$ の極大独立集合は $\{s\}$ である．$\mathbb{C}(s)[t,x,y]$ において $\langle F\cup E\rangle$ の $(\succ_{\{x,y\}}, \succ_{\{t\}})$ に関する簡約グレブナー基底 G_2 は

$$G_2 = \{s^6t^{11}-s^6t^7+s^3t^6+1, y+s^2t^3, x-st^2\}$$

である．$G'_2 = G'_2\backslash G'_2 \cap \langle E\rangle = \{y+s^2t^3, x-st^2\}$ である．イデアル商 $\langle F\cup E\rangle : \langle G'_2\rangle$ の簡約グレブナー基底は $\{1\}$ である．

したがって，断片

$$(\mathbb{V}(s^6t^{11}-s^6t^7+s^3t^6+1), \{y+s^2t^3, x-st^2\})$$

を得る．

以上より，$\langle F \rangle$ の包括的グレブナー基底系 $\mathcal{G}$ は

$$\begin{aligned}\mathcal{G} \;\; = \;\; &\big\{(\mathbb{C}^2 \backslash \mathbb{V}(s^6t^{11} - s^6t^7 + s^3t^6 + 1), \{y^4, xy^2, x^4 + x + sy^3\}), \\ &\quad (\mathbb{V}(s^6t^{11} - s^6t^7 + s^3t^6 + 1), \{y + s^2t^3, x - st^2\})\big\}\end{aligned}$$

となる．

実装したプログラムの速度比較はまだ成されておらず，今後，別の場所で発表する予定である．

謝辞

この研究は日本学術振興会科学研究補助金 基盤研究 (C) 課題番号 18K032140，19K034841 の助成を受けております．

参 考 文 献

[1] Adams, W. and Loustaunau, P.: An introduction to Gröbner bases. Amerian Mathematical Society, (1994)

[2] Becker, T. and Weispfenning, V.: Gröbner Bases - A computational approach to commutative algebra -. Springer, (1993)

[3] Cox, D., Little, J. and O'Shea, D.: Ideals, varieties, and algorithms (2nd edition). Springer, (1997)

[4] Kalkbrener, M.: On the stability of Gröbner bases under specializations. J. Symb. Comp., **24**, pp. 51–58, (1997)

[5] Kapur, D., Sun, D. and Wang, D.: A new algorithm for computing comprehensive Göbner systems. Proc. ISSAC 2010, pp. 29-36, ACM, (2010)

[6] Kapur, D., Sun, D. and Wang, D.: An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system. J. Symb. Comp., **49**, pp. 27–44, (2013)

[7] Montserrat, M. and Montes, A.: Improving DISPGB algorithm using the discriminant ideal. J. Symb. Comp., **41**, pp. 1245–1263, (2006).

[8] Montes, A.: A new algorithm for discussing Gröbner basis with parameters. J. Symb. Comp., **33**, pp. 183–208, (2002).

[9] Montes, A.: The Groebner Cover. (Algorithms and Computation in Mathematics, 27). Springer, (2019)

[10] Nabeshima, K.: A speed-up of the algorithm for computing comprehensive Gröbner systems. In: Proc. ISSAC 2007, pp. 299–306. ACM (2007)

[11] Nabeshima, K.: Reduced Gröbner Bases in Polynomial Rings over a Polynomial Ring. Mathematics in Computer Science, **4**, 587–599, (2009)

[12] Nabeshima, K.: Stability conditions of monomial bases and comprehensive Gröbner systems. In: Proc. CASC 2012, LNCS, Vol. **7442**, pp. 248–259, Springer (2012).

[13] Sato, Y., Fukasakua, R. and Nabeshima, K. On simple representation of locally closed sets. Proc. Asian Technology Conference in Mathematics 2016, pp. 190–199, Published by Mathematics and Technology, LLC, (2016)

[14] Suzuki, A. and Sato, Y.: An alternative approach to Comprehensive Gröbner bases. In: Proc. ISSAC 2002, pp. 255–261. ACM (2002)

[15] Suzuki, A. and Sato, Y.: An alternative approach to comprehensive Gröbner bases. J. Symb. Comp., **36**, pp. 649–667, (2003).

[16] Suzuki, A. and Sato, Y.: A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In: Proc. ISSAC 2006, pp. 326–331. ACM (2006)

[17] Noro, M., Takeshima, T.: Risa/Asir - A computer algebra system. In: Proc. ISSAC 1992, pp. 387–396. ACM (1992) `http://www.math.kobe-u.ac.jp/Asir/asir.html`

[18] Weispfenning, V.: Comprehensive Gröbner bases. J. Symb. Comp., **14**, pp. 1–29, (1992)

[19] Weispfenning, V.: Canonical comprehensive Gröbner bases. J. Symb. Comp., **36**, pp. 669–683, (2003)

[20] Weispfenning, V.: Comprehensive Gröbner bases and regular rings. J. Symb. Comp., **41**, pp. 285–296, (2006)