パラメータ付きイデアルに関する最小多項式の実装と応用

Computing and using minimal polynomials with parameters

東京理科大学大学院理学研究科　　蒋云 [*1]
Yun Jiang
Graduate School of Science, Tokyo University of Science

東京理科大理学部第一部応用数学科　　鍋島克輔 [*2]
Katsusuke Nabeshima
Department of Applied Mathematics, Tokyo University of Science

Abstract

Algorithms for computing parametric minimal polynomial with respect to a parametric ideal are studied in the context of symbolic computation. The key of the algorithms is a comprehensive Gröbner system. Applications of the algoritms are also discussed.

1　はじめに

パラメータを持たないイデアルに関する最小多項式の計算は，グレブナー基底を用いることにより構成可能であり，多くの計算代数システムに実装されている [9]．本研究では，パラメータ付きイデアルに関する最小多項式の計算法について考える．鍵となるのは，パラメータ付きグレブナー基底として有名な包括的グレブナー基底系である．

パラメータを含まないイデアルの最小多項式の計算法としてよく知られている 2 つの計算法がある．この 2 つの方法を包括的グレブナー基底系を用いて拡張し，パラメータ付きイデアルの最小多項式を計算する方法を確立した．

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 $\overline{K}$ とする．

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 $\mathrm{lpp}(f), \mathrm{lc}(f), \mathrm{lm}(f)$ で表す．ただし，$\mathrm{lm}(f) = \mathrm{lc}(f)\,\mathrm{lpp}(f)$ 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，$\mathrm{lpp}(F) = \{\mathrm{lpp}(g) | g \in F\}$，$\mathrm{lc}(F) = \{\mathrm{lc}(g) | g \in F\}$，$\mathrm{lm}(F) = \{\mathrm{lm}(g) | g \in F\}$ とする．

[*1] 〒 162-0825 東京都新宿区神楽坂 1-3　E-mail: 1422520@ed.tus.ac.jp
[*2] 〒 162-0825 東京都新宿区神楽坂 1-3　E-mail: nabeshima@rs.tus.ac.jp

$F \subset K[t]$ とする．アフィン代数多様体を $\mathbb{V}(F) = \{\bar{a} \in \overline{K}^m | f(\bar{a}) = 0, f \in F\}$ で定める．また，$E, N \subset K[t]$ に対して，本稿では，代数的構成可能集合 $\mathbb{V}(E)\backslash\mathbb{V}(N)$ を，$\mathbb{A}$ や $\mathbb{A}', \mathbb{A}_i$ $(1 \leq i \leq \ell)$ または，$\mathbb{B}, \mathbb{B}_j$ $(1 \leq j \leq r)$ などでよく表す．

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

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

で表わす．任意の元 $\bar{a} \in \overline{K}^m$ に対して，特化準同型写像を $\sigma_{\bar{a}} : K[t][x] \longrightarrow \overline{K}[x]$ とする．これは，変数 t への $\bar{a}$ を代入することを意味する．写像 $\sigma_{\bar{a}}$ での集合 $F \subset K[t][x]$ における像は $\sigma_{\bar{a}}(F) = \{\sigma_{\bar{a}}(f)\ F \in I\}$ である．

本稿で重要となる包括的グレブナー基底系の定義として，次を採用する．

定義 1 (包括的グレブナー基底系)
F を $K[t][x]$ の有限部分集合，$\mathbb{A}_1, \mathbb{A}_2, \ldots, \mathbb{A}_\ell$ を $\overline{K}^m$ 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

- $i \neq j$ において，$\mathbb{A}_i \cap \mathbb{A}_j \neq \emptyset$,
- 各 $i \in \{1, \ldots, \ell\}$ において，任意の $\bar{a} \in \mathbb{A}_i$ と $g \in G_i$ で，$\mathrm{lpp}(g) = \mathrm{lpp}(\sigma_{\bar{a}}(g))$ かつ $\sigma_{\bar{a}}(G_i)$ が $\overline{K}[x]$ 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，$\cup_{i=1}^{\ell} \mathbb{A}_i = \overline{K}^m$ 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．

包括的グレブナー基底系を計算するアルゴリズムは論文 [3, 4, 5, 6, 7, 10, 11, 13] などで紹介されており，計算機代数システム Risa/Asir [8] に実装されている．

3　パラメトリックイデアルのためのツールの作成

ここでは，パラメータ付きイデアルに関する最小多項式の計算で必要となるツールを構成する．ここで紹介するすべてのアルゴリズムは著者により計算機代数システム Risa/Asir に実装されている．

3.1　パラメトリックイデアルの次元

本稿で紹介する最小多項式の計算法 2 は，ゼロ次元イデアルの時にのみ動作する．そこで，イデアルがゼロ次元である保証が必要となる．ここでは，教科書 [2] に述べられているイデアルの次元を復習すると共に，パラメトリックイデアルの次元判定を行うアルゴリズムを導出する．

定義 2 (イデアルの次元)
I を $K[x]$ のイデアルとし，$u = \{u_1, \ldots, u_r\}$ を x の部分集合とする．もし，$I \cap K[u] = \{0\}$ であれば，u を I の独立集合という．また，I の独立集合 u がどの I の独立集合も含まないとき，u を I の極大独立集合と呼ぶ．また，I の次元 $\dim(I)$ は次のように定義される．

$$\dim(I) = max\{u | u \subset x \text{ が } I \text{ を法として独立である }\}$$

イデアルの次元について次の性質が知られている．

定理 3
I を $K[x]$ のイデアルとし，全次数項順序を固定する．このとき，$\dim(I) = \dim(\langle \mathrm{lpp}(I) \rangle)$ となる．

全次数項順序に関してイデアル I のグレブナー基底 G を計算することによりイデアルの次元は次のように計算可能であることが知られている．

アルゴリズム 1 (イデアルの次元)

Specification: dimension(F)
$\dim(\langle F \rangle)$ の計算.
入力: $F \subset K[x]$,
出力: $\langle F \rangle$ の次元.
BEGIN
$\{g_1, \ldots, g_\ell\} \leftarrow \langle F \rangle$ の全次数項順序でのグレブナー基底を計算;
for $i = 1$ to ℓ **do**
　　$\mathcal{M}_i \leftarrow \mathrm{lpp}(g_i) = x_{i1}^{\alpha_1} x_{i2}^{\alpha_2} \cdots x_{is}^{\alpha_s}$ を構成する変数の集合 $\{x_{i1}, x_{i2}, \ldots, x_{is}\}$, ただし，$\alpha_1, \ldots, \alpha_s \geq 1$;
end-for
$\mathcal{M} \leftarrow \{J \subset x | j \cap \mathcal{M}_j \neq \emptyset, j \in \{1, 2, \ldots, \ell\}$;
$J' \leftarrow |J'| = \min(|J||J \in \mathcal{M})$ となる J' を $\mathcal{M}$ からとる;
return $n - |J'|$;
END

さて，有限部分集合 F がパラメータ t を含む場合，$\langle F \rangle$ の次元は求めるか？パラメータを連続的に変化させるとドラスティックにイデアルの構造は変化するので，イデアルの次元はパラメータの値に依存することがわかる．変化すべてを計算するためには，包括的グレブナー基底系が必要となる．定理 3 と包括的グレブナー基底系の定義にある “$\mathrm{lpp}(g) = \mathrm{lpp}(\sigma_{\bar{a}}(g))$” から，$\langle F \rangle$ の全次数項順序での包括的グレブナー基底系を計算したあと，各セグメント毎にアルゴリズム 1 を実行する．

アルゴリズム 2 (パラメータ付きイデアルの次元)

Specification: para_dim($F, \succ$)
パラメータ付きイデアル $\langle F \rangle$ の次元の計算.
入力: $F \subset K[t][x]$, $\succ$: 全次数項順序,
出力: $\{(\mathbb{A}_1, G_1, d_1), (\mathbb{A}_2, G_2, d_2), \ldots, (\mathbb{A}_\ell, G_\ell, d_\ell)\}$: $\forall \bar{a} \in \mathbb{A}_i$, $\dim(\langle \sigma_{\bar{a}}(F) \rangle) = d_i$ であり，$\sigma_{\bar{a}}(G_i)$ は $\langle \sigma_{\bar{a}}(F) \rangle$ の $\succ$ に関するグレブナー基底.
BEGIN
$\mathcal{D} \leftarrow \emptyset$;
$\mathcal{G} \leftarrow \langle F \rangle$ の $\succ$ に関する包括的グレブナー基底系を計算;
while $\mathcal{G} \neq \emptyset$ **do**
　　$\mathcal{G}$ から $(\mathbb{A}, G)$ をとる; $\mathcal{G} \leftarrow \mathcal{G} \backslash \{(\mathbb{A}, G)\}$;
　　$\mathcal{D} \leftarrow \mathcal{D} \cup \{(\mathbb{A}, G, \mathrm{dimension}(\mathrm{lpp}(G)))\}$;
return $\mathcal{D}$;
END

アルゴリズム 2 により，パラメトリックイデアルの次元は完璧に計算される．

3.2 パラメトリックイデアル所属問題

ここでは，パラメータ付き多項式がパラメトリックイデアルに所属する条件をどのように求めるかを考える．多項式 $f \in K[x]$ とイデアル $I \subset K[x]$ を考える．このとき，イデアル所属問題は I のグレブナー基底 G を計算し，その G で f を割った余りがゼロであれば，f は I の元であることがわかる．また，G で割った余りは一意であり，その余りを f の G によるノーマルフォームという．割り算アルゴリズムの重要な点は G の先頭項で割り算を行っていることである．すなわち，グレブナー基底の先頭項が消えなければ，通常の割り算アルゴリズムが $K(t)[x]$ 上で使用可能である．

包括的グレブナー基底系の定義に "$\mathrm{lpp}(g) = \mathrm{lpp}(\sigma_{\bar{a}}(g))$" の条件があることより，各セグメント毎に $K(t)[x]$ 上で通常の割り算アルゴリズムを適用することで基本的にはパラメトリックイデアル所属問題は解くことができる．しかし，余りがパラメータだけの式の場合，パラメータの条件との整合性を考える必要がある．この場合は，根基所属問題を $K[x,t]$ で解くことで判定は可能である．

以上の考察から，パラメトリックイデアル所属問題は次のアルゴリズムで解くことができる．$E \subset K[t]$ としたとき，$\sqrt{\langle E \rangle}$ は $\langle E \rangle$ の根基イデアルを表すものとする．

アルゴリズム 3 (パラメトリックイデアル所属問題)

Specification: para_membership(f, F)

パラメトリックイデアル所属問題を解く．

入力: $f \in K[t][x]$, $F \subset K[t][x]$,

出力: $\mathcal{Y} = \{\mathbb{A}_1, \mathbb{A}_2, \ldots, \mathbb{A}_\ell\}$, $\mathcal{N} = \{\mathbb{B}_1, \mathbb{B}_2, \ldots, \mathbb{B}_r\}$: $\forall \bar{a} \in \mathbb{A}_i$, $\sigma_{\bar{a}}(f) \in \langle \sigma_{\bar{a}}(F) \rangle$ $(1 \le i \le \ell)$. $\forall \bar{b} \in \mathbb{B}_i$, $\sigma_{\bar{b}}(f) \notin \langle \sigma_{\bar{b}}(F) \rangle$ $(1 \le i \le r)$.

BEGIN

$\mathcal{Y} \leftarrow \emptyset$; $\mathcal{N} \leftarrow \emptyset$; $\mathcal{G} \leftarrow \langle F \rangle$ の $\succ$ に関する包括的グレブナー基底系を計算;

while $\mathcal{G} \neq \emptyset$ **do**

　$\mathcal{G}$ から $(\mathbb{V}(E) \backslash \mathbb{V}(N), G)$ をとる; $\mathcal{G} \leftarrow \mathcal{G} \backslash \{(\mathbb{V}(E) \backslash \mathbb{V}(N), G)\}$; /*$(E, N \subset K[t])$*/

　$h \leftarrow K(t)[x]$ 上で f を G で割った余り;

　　if $h = 0$ もしくは $h \in \sqrt{\langle E \rangle} \subset K[x,t]$ **then**

　　$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{\mathbb{V}(E) \backslash \mathbb{V}(N)\}$;

　　else

　　$\mathcal{N} \leftarrow \mathcal{N} \cup \{\mathbb{V}(E) \backslash \mathbb{V}(N)\}$;

　　end-if

end-while

return $(\mathcal{Y}, \mathcal{N})$;

END

根基所属問題は新しい変数 y を用いてイデアル $\langle E \cup \{1 - yh\} \rangle$ のグレブナー基底を $K(x)[t,y]$ 上で計算し，$\{1\}$ であれば所属することがわかる．

次節で必要となるのは，ノーマルフォームの計算なので，ノーマルフォームのアルゴリズムとしてアルゴリズム 3 を改良した次を紹介する．

アルゴリズム 4 (パラメトリック・ノーマルフォーム)

Specification: para_nf$(f, \mathcal{G}, \succ)$

パラメトリック・ノーマルフォームの計算.

入力: $f \in K[t][x]$, $\mathcal{G}$:対象となるイデアルの $\succ$ に関する包括的グレブナー基底系.

出力: $\mathcal{Y} = \{(\mathbb{A}_1, G_1, g_1), (\mathbb{A}_2, G_2, g_2), \ldots, (\mathbb{A}_\ell, G_\ell, g_\ell)\}$: $\forall \bar{a} \in \mathbb{A}_i$，対象となるイデアルのグレブナー基底 G_i での f のノーマルフォームが $\sigma_{\bar{a}}(g_i)$ となる．$(1 \leq i \leq \ell)$
BEGIN
$\mathcal{Y} \leftarrow \emptyset$;
while $\mathcal{G} \neq \emptyset$ **do**
　$\mathcal{G}$ から $(\mathbb{V}(E)\backslash\mathbb{V}(N), G)$ をとる; $\mathcal{G} \leftarrow \mathcal{G}\backslash\{(\mathbb{V}(E)\backslash\mathbb{V}(N), G)\}$;　/*$(E, N \subset K[t])$*/
　$g \leftarrow K(t)[x]$ 上で f を G で割った余り;
　$g' \leftarrow \sqrt{\langle E \rangle} \subset K[t]$ のグレブナー基底で $g \subset K[x,t]$ を割った余り;
　$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(\mathbb{V}(E)\backslash\mathbb{V}(N), G, g')\}$;
end-while
return $\mathcal{Y}$;
END

3.3　パラメータ付き連立 1 次方程式

連立 1 次方程式は簡約グレブナー基底を計算することにより解を求めることができる．簡約グレブナー基底は行列の行簡約で最終的にたどり着く “簡約な行列” と対応している．例えば，

$$\begin{cases} x - 2y + z = 0 \\ x + y - z = 1 \\ 2x - y + 3z = 2 \end{cases}$$

の場合，$\langle x - 2y + z, x + y - z - 1, 2x - y + 3z - 2\rangle$ の簡約グレブナー基底系は $\{x - \frac{7}{9}, y - \frac{5}{9}, z - \frac{1}{3}\}$ となり，連立 1 次方程式の解が得られている．

連立 1 次方程式で唯一解をもつ場合，変数の個数と簡約グレブナー基底を構成する式の個数が同じとなる．

連立 1 次方程式にパラメータを含む場合も同様に計算することができるが，その場合，包括的グレブナー基底系が必要となる．唯一解を持つ場合は，上述したように変数の個数とグレブナー基底を構成する式の個数が同じとなるときである．しかしながら，係数環が $K[t]$ がであるので，上記のようなシンプルな形にはならない．

例えば，a, b をパラメータ，x, y, z を変数としたとき次のパラメータ付き連立 1 次方程式を考える．

$$\begin{cases} ax - 2y + z = 0 \\ x + y - z = b \\ 2x - y + 3z = 2 \end{cases}$$

このとき，$\langle ax - 2y + z, x + y - z - b, 2x - y + 3z - 2\rangle$ の（極小）包括的グレブナー基底系 $\mathcal{G}$ は次となる．

$$\begin{aligned} \mathcal{G} = \{&(\mathbb{V}(2a-1, -b+3), \{-7y + 3z + 3, -7x - 2z + 12\}), \\ &(\mathbb{V}(2a-1), \backslash\mathbb{V}(b-3), \{1\}), \\ &(\mathbb{C}^2\backslash\mathbb{V}(2a-1), \{(2a-1)z + (-b-9)a + 4b - 6, 7y - 3z - 2b + 3, 7x + 2z - b - 9\})\}. \end{aligned}$$

このとき，$\mathbb{V}(2a-1, -b+3)$ の場合，複数個（無限）の解が存在し，$\mathbb{V}(2a-1)$ のとき，解が存在しないことがわかる．また，$\mathbb{C}^2\backslash\mathbb{V}(2a-1)$ のとき，各パラメータの値に対して，解が 1 個存在することがわかる．しかしながら，$\mathbb{C}^2\backslash\mathbb{V}(2a-1)$ のとき，解の形は複雑でありすぐにはわかりずらい．そこで，包括的グレブナー基底系の定義に “$\mathrm{lpp}(g) = \mathrm{lpp}(\sigma_{\bar{a}}(g))$” の条件があることを思い出そう．先頭係数はゼロにならないことなので，$\mathbb{C}(a,b)[x,y,z]$ 上で $\{(2a-1)z + (-b-9)a + 4b - 6, 7y - 3z - 2b + 3, 7x + 2z - b - 9\}$ の簡約化を同じ項順序に関して計算することにより，より簡単な式となる．この時のグレブナー基底は次である．

$$\{(2a-1)z+(-b-9)a+4b-6, (2a-1)y+(-b-3)a+2b-3, (2a-1)x-b+3\}$$

ここから，

$$x=\frac{b-3}{2a-1}, y=\frac{(b+3)a-2b+3}{2a-1}, z=\frac{(b+9)a-4b+6}{2a-1}$$

を得ることができる．

パラメータ付き最小多項式を計算するときには唯一解が欲しいので唯一解と，そうでない条件を計算するアルゴリズムを次にまとめる．

アルゴリズム 5 (パラメータ付き連立 1 次方程式)

Specification: para_solve($\mathbb{A}, F$)
$\mathbb{A}$ 上での連立一次方程式系 F の解法.
入力: $F \subset K[t][x]$: 1 次式の集合, $\mathbb{A} \subset \overline{K}^m$.
出力: $\mathcal{Y} = \{(\mathbb{A}_1, S_1), \ldots, (\mathbb{A}_\ell, S_\ell)\}$, $\mathcal{N} = \{\mathbb{B}_1, \mathbb{B}_2, \ldots, \mathbb{B}_r\}$: $\forall \bar{a} \in \mathbb{A}_i$, $\sigma_{\bar{a}}(S_1)$ は $\sigma_{\bar{a}}(F)$ の唯一解となる．$(1 \leq i \leq \ell)$. $\forall \bar{b} \in \mathbb{B}_i$, $\sigma_{\bar{b}}(F)$ は唯一解が存在しない．$(1 \leq i \leq r)$.
BEGIN
$\mathcal{Y} \leftarrow \emptyset$; $\mathcal{N} \leftarrow \emptyset$;
$\mathcal{G} \leftarrow \langle F \rangle$ の $\mathbb{A}$ 上の (極小) 包括的グレブナー基底系を計算;
while $\mathcal{G} \neq \emptyset$ **do**
　$\mathcal{G}$ から $(\mathbb{A}, G)$ をとる; $\mathcal{G} \leftarrow \mathcal{G} \backslash \{(A, G)\}$;
　　if $|G| = n$ **then**
　　$G' \leftarrow G$ を $K(t)[x]$ で簡約して解を出す;
　　$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(\mathbb{A}, G')\}$;
　　else
　　$\mathcal{N} \leftarrow \mathcal{N} \cup \{\mathbb{A}\}$;
　　end-if
end-while
return $(\mathcal{Y}, \mathcal{N})$;
END

ここでは，包括的グレブナー基底系を用いたパラメータ付き連立 1 次方程式の解法を紹介した．パラメータ付き掃き出し法を実装することも可能であるが，問題によって計算速度と，分割の個数に違いが出る．計算は可能であるが，より良いパラメータ付き連立 1 次方程式の解法はまだ知られていないようである．アルゴリズム 5 が速いかどうかは，ここでは問題としないが，計算可能であることは確かである．

4　パラメータ付き最小多項式

本節では，パラメトリックイデアルに対して 2 通りの最小多項式を計算する方法について述べる．パラメータを含まない最小多項式の定義は次である．

定義 4
I を $K[x]$ のイデアルとし，$f \in K[x]$ とする．$J_f = \{g(z) \in K[z] | g(f) \in I\}$ とおくと，J_f は $K[z]$ のイデアルとなる．$K[z]$ は単項イデアル整域であるので，J_f が 0 イデアルでないとき，あるモニックな多項式 $\mu_f(z)$ がただ 1 つ存在し，$J_f = \langle \mu_f \rangle$ となる．このとき，$\mu_f(z)$ を f の I に関する最小多項式という．

4.1 計算法 1

I を $K[x]$ のイデアルとし，$f \in K[x]$ とする．このとき，新しい変数 z を用いて，$I \cup \langle f - z \rangle$ の簡約グレブナー基底 G を消去項順序 $x \gg z$ に関して計算することにより f の I に関する最小多項式を計算することができる．すなわち，$G \cap K[z]$ が空でなければ，そこに z のみの多項式が 1 個存在し，それが最小多項式となる．また，$G \cap K[z]$ が空であれば 0 が最小多項式となる．

擬似コードをとして以下にまとめる．

アルゴリズム 6 最小多項式の計算法 1

Specification: minipoly1(f, F)
f の $\langle F \rangle$ に関する最小多項式の計算
入力: $f \in K[x]$, $F \subset K[x]$.
出力: $g \subset K[z]$ or 0: f の $\langle F \rangle$ に関する最小多項式.
BEGIN
$G \leftarrow x \gg z$ となる消去項順序で $\langle F \cup \{f - z\} \rangle \subset K[x, z]$ の簡約グレブナー基底を計算する;
if $G \cap K[z] \neq \emptyset$ **then**
　$g \leftarrow G \cap K[z]$ から元 g をとる;
　return g;
end-if
return 0;
END

アルゴリズム 6 をパラメータ版に一般化するには，包括的グレブナー基底系を用いることにより簡単に次のように構成できる．

アルゴリズム 7 パラメータ付き最小多項式の計算法 1

Specification: para_minipoly1(f, F)
f の $\langle F \rangle$ に関するパラメータ付き最小多項式の計算
入力: $f \in K[t][x]$, $F \subset K[t][x]$.
出力: $\{(\mathbb{A}_1, g_1), (\mathbb{A}_2, g_2), \ldots, (\mathbb{A}_\ell, g_\ell)\}$: $\forall \bar{a} \in \mathbb{A}_i$ $(1 \leq i \leq \ell)$, $\sigma_{\bar{a}}(f)$ の $\langle \sigma_{\bar{a}}(F) \rangle$ に関する最小多項式は $\sigma_{\bar{a}}(g_i)$ となる．
BEGIN
$\mathcal{Y} \leftarrow \emptyset$;
$\mathcal{G} \leftarrow x \gg z$ となる消去項順序で $\langle F \cup \{f - z\} \rangle \subset K[t][x, z]$ の（極小）包括的グレブナー基底を計算する;
while $\mathcal{G} \neq \emptyset$ **do**
　$\mathcal{G}$ から $(\mathbb{A}, G)$ をとる; $\mathcal{G} \leftarrow \mathcal{G} \backslash \{(A, G)\}$;
　　if $G \cap K[t][z] \neq \emptyset$ **then**
　　$g \leftarrow G \cap K[t][z]$ から元 g をとる; $\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(\mathbb{A}, g)\}$;
　　else
　　$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(\mathbb{A}, 0)\}$;
end-if
end-while
return $\mathcal{Y}$;
END

例 1
$F = \{ax^2 + 2by^2, 2x^2 + 2y^2, 2abx - 2y + 1\}$ とし，$f = x + y$ とする，a, b をパラメータとし，x, y は変数とする．$x \succ y$ の辞書式順序で f の $\langle F \rangle$ に関するの最小多項式を計算する．まず，包括的グレブナー基底系計算する．$\langle F \cup \{z - (x + y)\} \rangle$ の包括的グレブナー基底系 $\mathcal{G}$ を $\{x, y\} \gg z$ のブロック項順序で計算する，ここでは $\{x, y\}$ に $x \succ y$ となる辞書式項順序を用いる．

$$\begin{aligned}\mathcal{G} = \{&(\mathbb{V}(2b^2 + 1, a - 2b) \setminus \mathbb{V}(4b^4 + 1), \{2z - 1, -2x - 2y + 1, 8y^2 - 4y + 1\}),\\ &(\mathbb{V}(2b^2 - 2b + 1, a - 2b), \{2z - b, 4y - 1, -4x + 2b - 1\}),\\ &(\mathbb{V}(a - 2b) \setminus \mathbb{V}(8b^6 + 4b^4 + 2b^2 + 1), \{(4b^2 + 2)y - 4b^2 z - 1, -x - y + z, (8b^4 + 2)z^2 + (4b^2 - 2)z + 1\}),\\ &(\mathbb{V}(2b^2 + 2b + 1, a - 2b), \{2z + b, 4y - 1, -4x - 2b - 1\}), (\mathbb{C}^2 \setminus \mathbb{V}(a - 2b), \{1\})\}.\end{aligned}$$

以上より，次となる．

1. パラメータが $\mathbb{V}(2b^2 + 1, a - 2b) \setminus \mathbb{V}(4b^4 + 1)$ に属するとき，最小多項式は $z - \frac{1}{2}$ である．
2. パラメータが $\mathbb{V}(2b^2 - 2b + 1, a - 2b)$ に属するとき，最小多項式は $z - \frac{b}{2}$ である．
3. パラメータが $\mathbb{V}(a - 2b) \setminus \mathbb{V}(8b^6 + 4b^4 + 2b^2 + 1)$ に属するとき，最小多項式は $z^2 + \frac{2b^2 - 1}{4b^4 + 1} z + \frac{1}{8b^4 + 2}$ である．
4. パラメータが $\mathbb{V}(2b^2 + 2b + 1, a - 2b)$ に属するとき，最小多項式は $z + \frac{b}{2}$ である．
5. パラメータが $\mathbb{C}^2 \setminus \mathbb{V}(a - 2b)$ に属するとき，最小多項式は 1 である．

4.2 計算法 2

ここでは，ゼロ次元イデアルに特化した計算法について考える．ゼロ次元イデアルの場合，最小多項式は線形代数の手法を用いて計算可能であることが知られている．この手法を紹介すると共に，パラメータ版に拡張する．

定理 5
$I \subset K[x]$ をゼロ次元イデアルとし，任意の多項式式を $f \in K[x]$ とする．このとおき，I に関する 0 でない最小多項式 $\mu_f(z)$ が存在する．

補題 6
ゼロ次元イデアル $I \subset K[x]$ のグレブナー基底を G とし，未定係数 $c_k, \ldots, c_0 \in K$ に対し，$g(z) = z^k + c_{k-1} z^{k-1} + \cdots + c_1 z + c_0$ とする．このとき，$g(t) = m_f(z)$ となる $c_{k-1}, \ldots, c_0 \in K$ は，$g(f)$ を G で割った余りが 0 となる最小の k となる $c_k, \ldots, c_0$ である．

補題 6 から，最小多項式は未定係数を用いた連立 1 次方程式を解くことで求められることが分かる．

アルゴリズム 8 最小多項式の計算法 2

Specification: minipoly2(f, F)
f の $\langle F \rangle$ に関する最小多項式の計算
入力: $f \in K[x]$，$F \subset K[x]$: $\langle F \rangle$ はゼロ次元イデアル．

出力: $g \subset K[z]$: f の $\langle F \rangle$ に関する最小多項式.
BEGIN
$G \leftarrow \langle F \rangle \subset K[x]$ のグレブナー基底に関して計算する; $k \leftarrow 1$;
while 1 **do**
$h \leftarrow f^k + c_{k-1}f^{k-1} + \cdots + c_1 f + c_0$ を G で割った余り; ($c_{k-1}, \ldots, c_0$ は未定変数)
$C \leftarrow h$ の各項のすべての係数;
  if $c_{k-1}, \ldots, c_0$ の連立 1 次方程式 $\{g = 0 | g \in C\}$ が解を持つ **then**
    $p \leftarrow c_{k-1}, \ldots, c_0$ の解を $z^k + c_{k-1}z^{k-1} + \cdots + c_1 z + c_0$ に代入;
    return p;
  end-if
end-while
END

アルゴリズム 8 をパラメータ版に拡張するには次が必要である.

1. パラメトリックイデアルの次元判定.
2. 包括的グレブナー基底系での割り算の余りの計算. (パラメトリックノーマルフォームの計算)
3. $c_{k-1}, \ldots, c_0$ を求めるためにパラメータ付き連立 1 次方程式の解法.

上記の計算法については 3 節ですべて紹介されており, アルゴリズム 2, アルゴリズム 4 とアルゴリズム 5 を用いることで次のようにパラメータ版に拡張するすることができる.

アルゴリズム 9 パラメータ付き最小多項式の計算法 2

Specification: para_minipoly2(f, F)
f の $\langle F \rangle$ に関するパラメータ付き最小多項式の計算
入力: $f \in K[t][x]$, $F \subset K[t][x]$.
出力: $(\mathcal{S}, \mathcal{B})$: $\forall(\mathbb{A}, g) \in \mathcal{S}$, $\forall \bar{a} \in \mathbb{A}$, $\sigma_{\bar{a}}(g)$ は $\sigma_{\bar{a}}(f)$ の $\langle \sigma_{\bar{a}}(F) \rangle$ に関する最小多項式. $\forall \mathbb{B} \in \mathcal{B}$, $\forall \bar{b} \in \mathbb{B}$, $\langle \sigma_{\bar{b}}(F) \rangle$ は正次元イデアル.
BEGIN
$\mathcal{G} \leftarrow$ **para_dim**$(F, \succ)$(アルゴリズム 2) ただし, $\succ$ は全次数項順序;
$\mathcal{Z} \leftarrow \{(\mathbb{A}, G) | (\mathbb{A}, G, 0) \in \mathcal{G}\}$; $\mathcal{B} \leftarrow \{\mathbb{B} | (\mathbb{B}, G_d, d) \in \mathcal{G}, d \neq 0\}$; $\mathcal{S} \leftarrow \emptyset$; $k \leftarrow 1$;
while $\mathcal{Z} \neq \emptyset$ **do**
  $h \leftarrow f^k + c_{k-1}f^{k-1} + \cdots + c_1 f + c_0$; ($c_{k-1}, \ldots, c_0$ は未定変数)
  $\mathcal{F} \leftarrow$ **para_nf**$(h, \mathcal{Z}, \succ)$; (アルゴリズム 4)
  $\mathcal{P} \leftarrow \emptyset$;
  while $\mathcal{F} \neq \emptyset$ **do**
    $\mathcal{F}$ から $(\mathbb{A}', G', g')$ をとる; $\mathcal{F} \leftarrow \mathcal{F} \backslash \{(\mathbb{A}', G', g')\}$;
    $C \leftarrow g'$ の各項の係数の集合;
    $(\mathcal{Y}, \mathcal{N}) \leftarrow$**para_solve**$(\mathbb{A}', C)$ (アルゴリズム 5) ただし, $C \subset K[t][c_{k-1}, \ldots, c_0]$;
    $\mathcal{S} \leftarrow \mathcal{S} \cup \{(\mathbb{A}'', h'') | (\mathbb{A}'', S'') \in \mathcal{Y}, h$ の $c_{k-1}, \ldots, c_0$に解 S'を代入ものは $h''\}$;
    $\mathcal{P} \leftarrow \mathcal{P} \cup \{(\mathbb{B}, G') | \mathbb{B} \in \mathcal{N}\}$;
  end-while
  $\mathcal{Z} \leftarrow \mathcal{P}$; $k \leftarrow k + 1$;
end-while

return $\mathcal{S}$;
END

4.3 考察

パラメータ付き最小多項式を計算する 2 つの方法を紹介した．ゼロ次元の場合，一般に計算法 2 が速いことが知られている．計算法 1 は消去項順序でのグレブナー基底計算が必要になるが，計算法 2 はグレブナー基底であればあれば何でもよく，その後，線形計算を行うので速いことが想像できる．

2 つのアルゴリズムは計算機代数システム Risa/Asir に実装されている．我々のプログラムの比較では，計算法 2 が速いときもあるが概して計算法 1 が速かった．計算の解析をしてみるとパラメータ付き連立 1 次方程式系の解法に時間がかかっていることが原因であることがわかった．パラメータ付き連立 1 次方程式系の解法は包括的グレブナー基底系を何度も計算しており，必要以上のパラメータ空間の分割が行われていると共に，連立 1 次方程式であるがパラメータを変数として扱っているので，包括的グレブナー基底系計算アルゴリズムにおいて非線形な多項式のグレブナー基底計算を何度も行う．このことより，計算時間に差がでたと考えられる．より良い，パラメータ付き連立 1 次方程式の解法があれば改良が期待される．

Risa/Asir のグレブナー基底計算は速いので，包括的グレブナー基底系もそれなりに計算が速い．したがって，シンプルな計算法である計算法 1 が著者の実装においては速くなっていると思われる．

5 応用

最小多項式の応用がそのままパラメータ付き最小多項式の応用となる．最小多項式の応用は論文 [1] に述べられており，また，最小多項式を用いることにより多項式関数の bifucation set の計算ができることが論文 [12] で紹介されている．ここでは，ゼロ次元イデアルの根基について考察する．ゼロ次元イデアルの根基について次の定理が知られている．

定理 7
$I = \langle f_1, \ldots, f_\ell \rangle \subset K[x]$ はゼロ次元イデアルとし，$I \cap K[x_i]$ $(1 \leq i \leq n)$ に含まれる最小次数モニックな多項式を g_i とし，$\sqrt{g_i}$ を g_i の無平方部分とする．このとき，$\sqrt{I} = \langle f_1, \ldots, f_\ell, \sqrt{g_1}, \ldots, \sqrt{g_n} \rangle$ となる．

ゼロ次元であれば，各 x_i $(1 \leq i \leq n)$ の最小多項式を求めることにより，g_i が求められる．g_i を求めた後に，無平方部分を $g_i/\gcd(g_i, \frac{\partial g_i}{\partial x_i})$ で求めることにより，イデアル I の根基の生成元を得ることができる．

これをパラメータ版に拡張するには，各 x_i $(1 \leq i \leq n)$ のパラメータ付き最小多項式を求め，その後，$g_i/\gcd(g_i, \frac{\partial g_i}{\partial x_i})$ の計算をすればよい．このとき，$\gcd(g_i, \frac{\partial g_i}{\partial x_i})$ の計算には，包括的グレブナー基底系を計算することで得られ，割り算には擬除算を使う必要がある．なぜならば，係数は環 $K[t]$ で考えているからである．

ページ制限の都合上，詳しいアルゴリズムは割愛するが，パラメータ付き最小多項式を用いることにより，ゼロ次元イデアルの根基の生成元を計算することができる．

例 2
$a.b$ をパラメータ，x, y を変数とする．多項式 $F = \{x^2y + bx + a, x^3y + ax^2y + x\} \subset \mathbb{Q}[a, b][x, y]$ を考える，このとき，$\langle F \rangle$ のパラメータ付根基イデアルの生成元は次となる．

1. パラメータが $\mathbb{V}(a-1, b)$，$\mathbb{V}(a) \setminus \mathbb{V}(b(a-1))$，$\mathbb{V}(a, b)$ に属するとき，$\langle F \rangle$ はゼロ次元とならない．
2. パラメータが $\mathbb{V}(b) \setminus \mathbb{V}(a(a-1))$ に属するとき，$\langle F \rangle$ の根基の生成元は $\{a^3y + a^2 - 2a + 1, (a-1)x + a^2\}$ である．

3. パラメータが $\mathbb{V}(a-1)\setminus\mathbb{V}(b^2-4b)$ に属するとき，$\langle F\rangle$ の根基の生成元は $\{y-b, bx^2+bx+1\}$ である．

4. パラメータが $\mathbb{V}(b-4,a-1)\setminus\mathbb{V}(b)$ に属するとき，$\langle F\rangle$ の根基の生成元は $\{y-4, 2x+1\}$ である．

5. パラメータが $\{\mathbb{V}(9a^2-10a+1, b-4)\}\setminus\mathbb{V}(ba^2-ba)$ に属するとき，$\langle F\rangle$ の根基の生成元は $\{y-126a+122, (18a-18)x-a+1\}$ である．

6. パラメータが $\mathbb{V}((b^2-2b+1)a^2+(-2b-2)a+1)\setminus\mathbb{V}((b^2-4b)a^2+(-b^2+4b)a)$ に属するとき，$\langle F\rangle$ の根基の生成元は $\{2y+(-b^4-b^3+5b^2-3b)a+b^3+10b^2+5b, (2b^3-8b^2)x+(b^3-3b^2-4b)a-b^2+4b\}$ である．

7. パラメータが $\mathbb{C}^2\setminus\mathbb{V}((b^3-2b^2+b)a^4+(-b^3-3b)a^3+(2b^2+3b)a^2-ba)$ に属するとき，$\langle F\rangle$ の根基の生成元は $\{(ba^2-ba)x+a^4y+a^3+(-b-2)a^2+a, a^3y^2+((-b+1)a^2+(-b-2)a+1)y+b^2\}$ である．

参 考 文 献

[1] Abbott, J. Bigatti, A.M., Palezzato, E. and Robbiano, L.: Computing and using minimal polynomials. J. Symb. Comp., **100**, 137–163, (2020).

[2] Becker. T. and V. Weispfenning: Gröbner Bases, A Computational Approach to Commutative Algebra (GTM 141), Springer, 1993.

[3] Kapur, D., Sun, Y. and Wang, D. : A new algorithm for computing comprehensive Gröbner systems. Proc. ISSAC 2010, 29–36, ACM, (2010).

[4] Kapur, D., Sun, Y. and Wang, D. : An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system. J. Symb. Comp., **49**, 74–44, (2013).

[5] Lu, D., Sun, Y. and Wang, D. : A survey on algorithms for computing comprehensive Gröbner systems and comprehensive Gröbner bases. J. Syst. Sci. Complex, **32**, 234–255, (2019)

[6] Montes, A. : The Gröbner Cover. Springer Nature Switzerland AG 2018

[7] Nabeshima, K.: Generic Gröbner basis of a parametric ideal and its application to a comprehensive Gröbner system, Applicable Algebra in Engineering, Communication and Computing, **35**, 55–70, (2024)

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

[9] 野呂正行，横山和弘: グレブナー基底の計算 基礎篇-計算機代数入門．東京大学出版会 (2003).

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

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

[12] 田島慎一, 鍋島克輔： 多項式函数の bifurcation set の計算法 I, 数理解析研究所講究録, 第 2255 号, 88-95. (2023).

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