

パラメータ付きイデアルの根基計算の実装

On the radical of a polynomial ideal with parameters

東京理科大学大学院理学研究科 倉持玲介^{*1}

RYOSUKE KURAMOCHI

GRADUATE SCHOOL OF SCIENCE, TOKYO UNIVERSITY OF SCIENCE

東京理科大學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

An algorithm for computing a radical of a parametric polynomial ideal is considered in the context of symbolic computation. The basic strategy for the computation is to reduce the problem to the zero-dimensional case by means of the extension/contraction method and its connection with comprehensive Gröbner systems. It is shown that Nabeshima-Tajime method, for computing some generic property of parametric systems, powerfully works.

1 はじめに

本研究では、パラメータ付き多項式イデアルの根基の生成元を計算する計算法を確立するとともに、計算機代数システム Risa/Asir 上に実装する。パラメータを含まない通常の多項式イデアルの根基の生成元を計算するアルゴリズムとして Gianni-Trager-Zacharias[3] が導出した方法が知られており、Becker-Weispfenning[1]において詳細が述べられている。しかし、パラメータ付き多項式イデアルの根基の生成元を計算する方法はまだ確立されていない。そこで本研究では前述の Gianni-Trager-Zacharias [3] の計算手法をパラメータ付きイデアルに拡張することで、パラメータ付きイデアルの根基の生成元の計算する手法を確立し、計算代数システムへの実装を行なった。拡張にあたって、まず計算対象のイデアルがゼロ次元である場合についてパラメータ付きイデアルへの拡張を行う。その後、ゼロ次元でないイデアルの場合を扱う。

2 準備

K を体とし、 L を K を含む代数的閉体とする。 $X = \{X_1, \dots, X_n\}$, $A = \{A_1, \dots, A_m\}$ を変数とし $X \cap A \neq \emptyset$ とする。 $\text{pp}(X)$, $\text{pp}(A)$, $\text{pp}(A, X)$ をそれぞれ X の項 (power product) の集合, A の項の集合, $A \cup X$ の項の集合とする。 \mathbb{N} を 0 を含む自然数の集合, \mathbb{Q} を有理数体, \mathbb{C} を複素数体とする。多項式 $f \in K[X]$ に対して、 \sqrt{f} を f の無平方部分とする。 $\text{pp}(A)$ における項順序を \prec_A , $\text{pp}(X)$ における項順序を \prec_X とし, $K[A][X] := (K[A])[X]$ を多項式環 $K[A]$ を係数ドメインとする多項式環とする。

$f \in K[A][X]$ のとき項順序 \prec_X に関して f の先頭項 (leading power product), 先頭係数 (leading coefficient), 先頭単項 (leading monomial) をそれぞれ $\text{lpp}_X(f)$, $\text{lc}_X(f)$, $\text{lm}_X(f)$ とする。多項式 f を $K[A, X]$

^{*1} 〒 162-0825 東京都新宿区神楽坂 1-3 E-mail: 1422513@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

の元とみなす場合には、項順序 $\prec_{A,X}$ に関して f の先頭項 (leading power product), 先頭係数 (leading coefficient), 先頭単項 (leading monomial) をそれぞれ $\text{lpp}_{A,X}(f)$, $\text{lc}_{A,X}(f)$, $\text{lm}_{A,X}(f)$ とする.

F を $K[A][X]$ の多項式の集合とする. このとき $\text{lc}_X(F) = \{\text{lc}_X(f) : f \in F\}$, $\text{lpp}_X(F) = \{\text{lpp}_X(f) : f \in F\}$ とし, F を $K[A,X]$ の多項式の集合とするとき, $\text{lc}_{A,X}(F) = \{\text{lc}_{A,X}(f) : f \in F\}$, $\text{lpp}_{A,X}(F) = \{\text{lpp}_{A,X}(f) : f \in F\}$ とする. 任意の元 $\alpha \in L^m$ に対して, 特化準同型写像 (specialization homomorphism) $\sigma_\alpha : K[A] \rightarrow L$ を定義する. この写像は自然な拡張として $\sigma_\alpha : K[A][X] \rightarrow L[X]$ と考えることもできる. このときのイデアル $I \subseteq K[A][X]$ の σ による像は $\sigma(I) := \{\sigma(f) : f \in I\} \subseteq L[X]$ である.

$f_1, \dots, f_k \in K[A]$ に対して, f_1, \dots, f_k で定義されるアフィン代数多様体を $\mathbb{V}_L(f_1, \dots, f_k)$ と定義する. つまり, $\mathbb{V}_L(f_1, \dots, f_k) = \{\bar{a} \in L^m : f_1(\bar{a}) = \dots = f_k(\bar{a}) = 0\}$ となる. また, $E, N \subset K[A]$ に対して, 本稿では, 代数的構成可能集合 $\mathbb{V}_L(E) \setminus \mathbb{V}_L(N)$ を, \mathbb{A} や \mathbb{A}' , \mathbb{A}_i ($1 \leq i \leq \ell$) または, \mathbb{B} , \mathbb{B}' , \mathbb{B}_j ($1 \leq j \leq r$) などでよく表す. R を単位元を持つ可換環としたとき, $f_1, \dots, f_k \in R$ に対して $\langle f_1, \dots, f_k \rangle := \left\{ \sum_{i=1}^k h_i f_i : h_1, \dots, h_k \in R \right\}$ とする. また, $K[X]$ のイデアル I と J に対し, I と J のイデアル商は $I : J = \{f \in K[X] : fJ \subset I\}$ であり, 飽和イデアルは $I : J^\infty = \{f \in K[X] : \text{ある } s \in \mathbb{N} \text{ について, } fJ^s \subset I\}$ である.

定義 1 (包括的グレブナー基底系)

F を $K[A][X]$ の有限部分集合, $\mathbb{A}_1, \dots, \mathbb{A}_l$ を L^m 上の代数的構造集合, G_1, \dots, G_l を $K[A][X]$ の有限部分集合とし, \prec を $\text{pp}(X)$ の項順序とする. このとき, ペアの有限部分集合 $\mathcal{G} = \{(\mathbb{A}_1, G_1), \dots, (\mathbb{A}_l, G_l)\}$ が $\langle F \rangle$ の \prec に関する $\bigcup_{i=1}^l \mathbb{A}_i$ 上の包括的グレブナー基底系 (CGS) であるとは, 以下をみたすときである.

- $\mathbb{A}_i \cap \mathbb{A}_j \neq \emptyset$,
- 各 $i \in \{1, \dots, l\}$ に対して, 任意の $\bar{a} \in \mathbb{A}_i$ と任意の $g \in G_i$ において, $\text{lpp}_X(g) = \text{lpp}_X(\sigma_{\bar{a}}(g))$ かつ $\sigma_{\bar{a}}(G_i)$ は $\langle \sigma_{\bar{a}}(F) \rangle$ の \prec に関するグレブナー基底となる.

このとき, (\mathbb{A}_i, G_i) をセグメントといい, $\bigcup_{i=1}^l \mathbb{A}_i = L^m$ のとき, 単に $\langle F \rangle$ の \prec に関する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 [5] で紹介されており, 計算機代数システム Risa/Asir [7] に実装されている.

3 パラメータ付きイデアルの計算ツール

ここでは, パラメータ付きイデアルの根基の生成元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 パラメータ付きイデアルの次元判定

パラメータ付きイデアルの次元判定のアルゴリズムを紹介する. 包括的グレブナー基底系と極大独立集合を用いることで, 各条件に対する $\langle F \rangle$ の次元を判定できる.

アルゴリズム 1 (パラメータ付き多項式イデアルの次元判定)

Specification: PARA_ZIGEN(\mathbb{A}, F)

入力: $\mathbb{A} \subset L^m$, $F : K[A][X]$ の有限部分集合.

出力: $\mathcal{Z} = \{(\mathbb{A}_1, H_1), \dots, (\mathbb{A}_r, H_r)\}$, $\mathcal{N} = \{(\mathbb{B}_1, P_1), \dots, (\mathbb{B}_\ell, P_\ell)\}$, $\mathcal{W} = \{(\mathbb{A}'_1, G_1), \dots, (\mathbb{A}'_r, G_{r'})\}$: $1 \leq i \leq r$, $\forall \bar{a} \in \mathbb{A}_i$ のとき, $\langle \sigma_{\bar{a}}(H_i) \rangle$ の次元はゼロ. $1 \leq j \leq \ell$, $\forall \bar{b} \in \mathbb{B}_j$ のとき, $\langle \sigma_{\bar{b}}(P_j) \rangle$ の次元はゼロではない. $1 \leq k \leq r'$, $\forall \bar{a} \in \mathbb{A}'_k$ のとき, $\bar{c} \in \mathbb{A}'_j$ のとき, $\langle \sigma_{\bar{c}}(G_k) \rangle$ は proper イデアルではない. ただし, $\mathbb{A} = (\bigcup_{i=1}^r \mathbb{A}_i) \cup (\bigcup_{j=1}^\ell \mathbb{B}_j) \cup (\bigcup_{k=1}^{r'} \mathbb{A}'_k)$ である.

BEGIN

Step 1: $\langle F \rangle$ を全次数項順序で \mathbb{A} 上の包括的グレブナー基底系 $\mathcal{G} = \{(\mathbb{A}_1, G_1), \dots, (\mathbb{A}_l, G_l)\}$ を計算;

Step 2: $\mathcal{Z} = \{(\mathbb{A}, G) \in \mathcal{G} : \langle \text{lpp}_X(G) \rangle \text{ を法とする極大独立集合が } \emptyset\}$;

$\mathcal{N} = \{(\mathbb{A}, G) \in \mathcal{G} : \langle \text{lpp}_X(G) \rangle \text{ を法とす W 極大独立集合が } \emptyset \text{ でない }\}$;

$\mathcal{W} = \{(\mathbb{A}, G) \in \mathcal{G} : G = \{0\} \text{ もしくは } \text{lpp}_X(G) = \{1\}\}$;

END

3.2 パラメータ付き多項式の無平方部分の計算

擬除算を用いることで、パラメータ付き一変数多項式の無平方部分を計算することができる。

アルゴリズム 2 (パラメータ付き一変数多項式の無平方部分)

Specification: GIZYOZAN(\mathbb{A}, f_{X_i}, X_i)

入力: $\mathbb{A} \subset L^m$, $f_{X_i} : K[A][X_i]$ の多項式, $X_i \in X$.

出力: $\mathcal{P} = \{(\mathbb{A}_1, g_1), \dots, (\mathbb{A}_r, g_r)\} : \forall \bar{a} \in \mathbb{A}_i (1 \leq i \leq r), \sigma_{\bar{a}}(g_i) \text{ は } \sigma_{\bar{a}}(f_{X_i}) \text{ の無平方部分となる. ただし } \mathbb{A} = \bigcup_{i=1}^r \mathbb{A}_i \text{ である.}$

BEGIN

$\mathcal{P} \leftarrow \emptyset; \mathcal{G} \leftarrow \langle f_{X_i}, \partial f_{X_i} / \partial X_i \rangle$ の包括的グレブナー基底系;

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

$(\mathbb{A}', G') \leftarrow \mathcal{G}$ から (\mathbb{A}', G') をとる; $\mathcal{G} \leftarrow \mathcal{G} \setminus \{(\mathbb{A}', G')\}$; $g' \leftarrow G'$ から g' をとる;
 $g_{X_i} \leftarrow (\text{lc}_{X_i}(g')^{\deg(f_{X_i}) - \deg(g') + 1} f_{X_i}) / g'$; $\mathcal{P} \leftarrow \mathcal{P} \cup \{(\mathbb{A}', g_{X_i})\}$

end-while

return \mathcal{P} ;

END

3.3 有理関数体上の包括的グレブナー基底系

ここでは U を X の部分集合とし, $\overline{K(U)}$ を $K(U)$ を含む代数的閉体, A をパラメータとする。このとき, $\overline{K(U)}$ 上での $\langle F \rangle$ の包括的グレブナー基底系を以下のように定義する。

定義 2

F を $(K(U)[A])[X]$ の有限部分集合とし, $\mathbb{A}_1, \dots, \mathbb{A}_r$ を $\overline{K(U)}^m$ 上の代数的構造集合とする。 G_1, \dots, G_r を $K(U)[A][X]$ の有限部分集合とする。 \prec を $\text{pp}(X)$ の項順序とする。ペアの集合 $\mathcal{G} = \{(\mathbb{A}_1, G_1), \dots, (\mathbb{A}_r, G_r)\}$ が次を満たすとき, \mathcal{G} を $\langle F \rangle$ の \prec に関する $\bigcup_{i=1}^r \mathbb{A}_i$ 上の包括的グレブナー基底系という。

- $i \neq j, \mathbb{A}_i \cap \mathbb{A}_j = \emptyset$,
- 各 $i \in \{1, \dots, r\}$ に対して, 任意の $\bar{a} \in \mathbb{A}_i$ と任意の $g \in G_i$ において, $\text{lpp}_X(g) = \text{lpp}_X(\sigma_{\bar{a}}(g))$ かつ $\sigma_{\bar{a}}(G_i)$ は $\langle \sigma_{\bar{a}}(F) \rangle$ の \prec に関するグレブナー基底となる。

定義 2 は, 通常の包括的グレブナー基底系計算アルゴリズムで計算可能である。

3.4 パラメータ付き多項式イデアルの共通部分

パラメータ付き多項式イデアルの共通部分を計算する方法について紹介する。新しい変数 t を用いてグレブナー基底を計算することで, 2つの多項式イデアルの共通部分を求めることができる。([2])

定理 3

$I = \langle f_1, \dots, f_r \rangle$ と $J = \langle g_1, \dots, g_s \rangle$ を $K[X]$ のイデアルとし, t を新しい変数とする。 $K[X, t]$ のイデアル $\langle tf_1, \dots, tf_r, (1-t)g_1, \dots, (1-t)g_s \rangle$ の $X \ll t$ となるブロック順序に関するグレブナー基底を G とする。このとき, $G \cap K[X]$ は $I \cap J$ の基底となる。

包括的グレブナー基底系を用いることにより、パラメータ付きイデアルに拡張できる。

アルゴリズム 3 (パラメータ付き多項式イデアルの共通部分)

Specification: PARA_INTERSECTION(\mathbb{A}, F, G)

入力: $\mathbb{A} \subset L^m$, $F, G : K[A][X]$ の有限部分集合.

出力: $\mathcal{R} = \{(\mathbb{A}_1, G_1), (\mathbb{A}_2, G_2), \dots, (\mathbb{A}_\ell, G_\ell)\} : \forall \bar{a} \in \mathbb{A}_i$ のとき, $\langle \sigma_{\bar{a}}(F) \rangle \cap \langle \sigma_{\bar{a}}(G) \rangle = \langle \sigma_{\bar{a}}(G_i) \rangle$, ただし, $1 \leq i \leq \ell$ であり, $\mathbb{A} = \bigcup_{i=1}^\ell \mathbb{A}_i$ である.

BEGIN

$\mathcal{R} \leftarrow \emptyset$; $\prec \leftarrow$ 新しい変数を t とし, $X \ll t$ となるブロック順序;

$\mathcal{G} \leftarrow \langle \{tf : f \in F\} \cup \{(1-t)g : g \in G\} \rangle \subset K[A][X, t]$ の \prec に関する包括的グレブナー基底系;

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

$(\mathbb{A}', G') \leftarrow \mathcal{G}$ から (\mathbb{A}', G') をとる; $\mathcal{G} \leftarrow \mathcal{G} \setminus \{(\mathbb{A}', G')\}$; $\mathcal{R} \leftarrow \mathcal{R} \cup \{(\mathbb{A}', G' \cap K[A][X])\}$;

end-while

return \mathcal{R} ;

END

定理 3 を用いることで、上のアルゴリズムで包括的グレブナー基底系 \mathcal{G} の各セグメント毎に、 t を変数にもつ多項式を除くことができる。したがって、このアルゴリズムによりパラメータ付き多項式イデアルの共通部分は計算することができる。

3.5 パラメータ付き多項式イデアルの最小公倍元の計算

パラメータ付き多項式イデアルの最小公倍元を計算する方法について紹介する。通常の多項式イデアルに対しての最小公倍元の計算方法として『 $f, g \in K[X]$ とする。このとき, $\langle f \rangle \cap \langle g \rangle = \langle \text{lcm}\{f, g\} \rangle$ となる』ことが知られている。アルゴリズム 3 を用いることで、これをパラメータ付き多項式の場合に拡張することができる。

アルゴリズム 4 (パラメータ付き多項式イデアルの最小公倍元)

Specification: PARA_LCM(\mathbb{A}, F)

入力: $\mathbb{A} \subset L^m$, $F : K[A][X]$ の有限部分集合.

出力: $\{(\mathbb{A}_1, \{f_1\}), (\mathbb{A}_2, \{f_2\}), \dots, (\mathbb{A}_\ell, \{f_\ell\})\} : \forall \bar{a} \in \mathbb{A}_i$ のとき, $\text{lcm}\{\sigma_{\bar{a}}(F)\} = \sigma_{\bar{a}}(f_i)$ となる. ただし $1 \leq i \leq \ell$ であり, $\mathbb{A} = \bigcup_{i=1}^\ell \mathbb{A}_i$ である.

BEGIN

$\mathcal{G} \leftarrow \emptyset$; $f \leftarrow F$ から f をとる; $F \leftarrow F \setminus \{f\}$; $\mathcal{H} \leftarrow \{(\mathbb{A}, \{f\})\}$;

while $F \neq \emptyset$ **do**

$g \leftarrow F$ から g をとる; $F \leftarrow F \setminus \{g\}$;

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

$(\mathbb{A}', \{f'\}) \leftarrow \mathcal{H}$ から $(\mathbb{A}', \{f'\})$ をとる; $\mathcal{H} \leftarrow \mathcal{H} \setminus \{(\mathbb{A}', \{f'\})\}$;

$\mathcal{L} \leftarrow \text{PARA_INTERSECTION}(\mathbb{A}', \{f'\}, \{g\})$; $\mathcal{G} \leftarrow \mathcal{G} \cup \mathcal{L}$

end-while

$\mathcal{H} \leftarrow \mathcal{G}$;

end-while

return \mathcal{H} ;

END

F の各要素について共通部分を計算することで, F の最小公倍元を計算することができる. したがって, このアルゴリズムによりパラメータ付き多項式イデアルの最小公倍元を計算することができる.

3.6 パラメータ付き多項式イデアルの飽和

パラメータ付き多項式イデアルの飽和を計算する手法について述べる. まず, 通常のイデアルに対する飽和の計算方法として以下が知られている.

定理 4

$I = \langle f_1, \dots, f_s \rangle$ を $K[X]$ のイデアルとし, $f \in K[X]$ を固定する. t を新しい変数とし, $J = \langle f_1, \dots, f_s, 1 - tf \rangle \subset K[X, t]$ とおく. このとき, $I : f^\infty = J \cap K[X]$ となる.

この定理をパラメータ付き多項式イデアルに対し拡張する.

アルゴリズム 5 (パラメータ付き多項式イデアルの飽和)

Specification: PARA_SAT(\mathbb{A}, F, f)

入力: $\mathbb{A} \subset L^m$, $F : K[A][X]$ の有限部分集合, $f : K[A][X]$ の多項式.

出力: $\langle F \rangle$ と f の \mathbb{A} 上の $\langle F \rangle : f^\infty$ の包括的グレブナー基底系 \mathcal{R} .

BEGIN

$\mathcal{R} \leftarrow \emptyset$; $\prec \leftarrow$ 新しい変数 t について, $X \ll t$ となるブロック順序;

$\mathcal{G} \leftarrow \langle F \cup \{1 - tf\} \rangle \subset K[A][X, t]$ の \prec に関する包括的グレブナー基底系;

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

$(\mathbb{A}', G') \leftarrow \mathcal{G}$ から (\mathbb{A}', G') をとる; $\mathcal{G} \leftarrow \mathcal{G} \setminus \{(\mathbb{A}', G')\}$; $\mathcal{R} \leftarrow \mathcal{R} \cup \{(\mathbb{A}', G' \cap K[A][X])\}$;

end-while

return \mathcal{R} ;

END

定理 4 を用いることで, 上記のアルゴリズムで $\langle F \cup \{1 - tf\} \rangle$ の包括的グレブナー基底系 \mathcal{G} の各セグメント毎に, t を変数にもつ多項式を除くことができる. したがって, 上記のアルゴリズムによりパラメータ付き多項式イデアルの飽和は計算することができる.

4 パラメータを含まないイデアルの根基

パラメータを含まない多項式イデアルの根基の生成元の計算について述べる.

定義 5

F を $K[X]$ の多項式集合とする. このとき, 集合 $\{f \in K[X] \mid \text{ある } s \in \mathbb{N} \text{ について, } f^s \in \langle F \rangle\}$ を $\langle F \rangle$ の根基とし, $\sqrt{\langle F \rangle}$ と定義する.

この多項式イデアルの根基を計算する手法については, Becker-Weispfenning [1] の 8 章に述べられている. また, 本稿の研究対象であるパラメータ付きイデアルに対する根基を次のように定義する.

定義 6 (パラメータ付き根基)

F を $K[A][X]$ の有限部分集合とし, $\mathbb{A}_1, \dots, \mathbb{A}_l \subset L^m$, $G_1, G_2, \dots, G_l \subset K[A][X]$ とする. ペアの集合 $\mathcal{R} = \{(\mathbb{A}_1, G_1), \dots, (\mathbb{A}_l, G_l)\}$ が以下を満たすとき, \mathcal{R} を $\langle F \rangle$ の $\bigcup_{i=1}^l \mathbb{A}_i$ 上のパラメータ付き根基と呼ぶ.

- $\mathbb{A}_i \cap \mathbb{A}_j = \emptyset$. ($i \neq j$)

- 各 i ($1 \leq i \leq l$) に対して, 任意の $\bar{a} \in \mathbb{A}_i$, $\sigma_{\bar{a}}(G_i)$ が $\sqrt{\langle \sigma_{\bar{a}}(F) \rangle}$ の根基となる.

例 1

$I = \langle ax^2y^2, (x+y)^2 \rangle$ とする。このとき x, y を主変数, a をパラメータとすると, パラメータ付き根基は $\mathcal{R} = \{(\mathbb{V}_{\mathbb{C}}(a), \{x+y\}), (\mathbb{C} \setminus \mathbb{V}_{\mathbb{C}}(a), \{x, y\})\}$ である。つまり, $a = 0$ のとき \sqrt{I} の生成元は $\{x+y\}$ となり, $a \neq 0$ のとき \sqrt{I} の生成元は $\{x, y\}$ となる。

4.1 ゼロ次元の場合

ゼロ次元のイデアルに対し, 以下の定理によって根基の生成元が計算できる。

定理 7 (ゼロ次元イデアルの根基)

K を完全体, F を $\langle F \rangle$ がゼロ次元イデアルとなる $K[X]$ の多項式の集合とする。 $1 \leq i \leq n$ について, f_i を $\langle F \rangle \cap K[X_i]$ の一意な最小次数モニック多項式, g_i を f_i の無平方部分とすると, $\sqrt{\langle F \rangle} = \langle F \cup \{g_1, \dots, g_n\} \rangle$ となる。

これより, ゼロ次元のイデアルに対する根基計算アルゴリズムは以下のように構成できる。

アルゴリズム 6 (ゼロ次元イデアルの根基)

Specification: ZRADICAL(F)

入力: $F : \langle F \rangle$ がゼロ次元イデアルとなる $K[X]$ の有限部分集合。

出力: $\sqrt{\langle F \rangle}$ の有限基底。

BEGIN

$G \leftarrow F;$

for $i = 1$ to n do

$f_{X_i} \leftarrow \langle F \rangle \cap K[X_i]$ の最小次数のモニック生成元; $g_{X_i} \leftarrow f_{X_i}$ の無平方部分; $G \leftarrow G \cup \{g_{X_i}\}$;

end-for

return G ;

END

このアルゴリズムを包括的グレブナー基底系を用いることにより, 次のようにパラメータ付きイデアルに拡張した。無平方部分の計算には 3.2 の擬除算を用いた。

アルゴリズム 7 (ゼロ次元イデアルのパラメータ付き根基)

Specification: PARAZERO(\mathbb{A}, F, N)

入力: $\mathbb{A} \subset L^m$, $F : K[A][X]$ の有限部分集合, \mathbb{A} 上で $\langle F \rangle$ はゼロ次元, $N \in \mathbb{N}$.

出力: $N = 1$ のとき $\langle F \rangle$ の \mathbb{A} 上のパラメータ付き根基 \mathcal{Z} .

BEGIN

if $N = n + 1$ then return $\{(\mathbb{A}, F)\}$; end-if

$\mathcal{Z} \leftarrow \emptyset$; $\mathcal{G} \leftarrow$ 消去順序で $\langle F \rangle \cap K[X_N]$ の \mathbb{A} 上の包括的グレブナー基底系を計算

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

$(\mathbb{A}', G') \leftarrow \mathcal{G}$ から (\mathbb{A}', G') をとる; $\mathcal{G} \leftarrow \mathcal{G} \setminus \{(\mathbb{A}', G')\}$; $g' \leftarrow G' \cap K[A][X_N]$

$\mathcal{B} \leftarrow$ アルゴリズム 2 を用いて g' のパラメータ付き無平方部分を計算;

 while $\mathcal{B} \neq \emptyset$ do

$(\mathbb{B}, b) \leftarrow \mathcal{B}$ から (\mathbb{B}, b) をとる; $\mathcal{B} \leftarrow \mathcal{B} \setminus \{(\mathbb{B}, b)\}$; $\mathcal{Z} \leftarrow \text{PARAZERO}(\mathbb{B}, F \cup \{b\}, N+1) \cup \mathcal{Z}$;

 end-while

end-while

```

return  $\mathcal{Z}$ ;
END

```

例 2

a, b をパラメータ, x, y を変数とする. $\prec_{x,y}$ を $y \prec x$ となる次数付き逆辞書式項順序とする. $F = \{x^2 + axy, xy^2 - bx + y\} \subset \mathbb{Q}[a, b][x, y]$ とする. $\langle F \rangle$ の \prec に関する包括的グレブナー基底系 \mathcal{G} を計算する.

$$\mathcal{G} = \{(\mathbb{C}^2 \setminus \mathbb{V}_C(a), \{bx + ay^3 - y, x^2 - a^2y^2, yx + ay^2\}), (\mathbb{V}_C(a) \setminus \mathbb{V}_C(b), \{y^2, bx - y\}), (\mathbb{V}_C(a, b), \{x^2, y\})\}.$$

このとき, すべてのセグメントはゼロ次元となるので, これらのセグメントに対して **PARAZERO** を適用する. まず $(\mathbb{C}^2 \setminus \mathbb{V}_C(a), \{bx + ay^3 - y, x^2 - a^2y^2, yx + ay^2\})$ について計算を行う. $\mathbb{C}^2 \setminus \mathbb{V}_C(a)$ 上で $x \prec y$ となる辞書式項順序に関する包括的グレブナー基底系を計算すると, $\{(\mathbb{C}^2 \setminus \mathbb{V}_C(a), \{x^4 + (-ba^2 - a)x^2, x^3 - ba^2x + a^2y\})\}$ となる. 同様に, $\mathbb{C}^2 \setminus \mathbb{V}_C(ab + 1)$ 上で $y \prec x$ となる辞書式項順序に関する包括的グレブナー基底系を計算すると, $\{(\mathbb{C}^2 \setminus \mathbb{V}_C(ab + 1), \{a^4y^3 + (-ba^4 - a^3)y, ax + a^2y\})$ となる. 包括的グレブナー基底系の結果より, x, y についての 1 変数多項式はそれぞれ x については, $\mathbb{C}^2 \setminus \mathbb{V}_C(a)$ のとき, $f_x = x^4 + (-a^2b - a)x^2$ となり, y については, $\mathbb{C}^2 \setminus \mathbb{V}_C(ab + 1)$ のとき, $f_y = ay^3 + (-ab - 1)y$ となる. これらの一変数多項式に対し包括的グレブナー基底系を用いて最大公約元を計算すると, x については, $\mathbb{V}_C(ab + 1)$ のとき, $\gcd(f_x, \partial f_x / \partial x) = x^3$ となり, $\mathbb{C}^2 \setminus \mathbb{V}_C(a^2b + a)$ のとき, $\gcd(f_x, \partial f_x / \partial x) = x$ となる. y については, $\mathbb{V}_C(ab + 1)$ のとき, $\gcd(f_y, \partial f_y / \partial y) = y^2$ となり, $\mathbb{C}^2 \setminus \mathbb{V}_C(a^2b + a)$ のとき, $\gcd(f_y, \partial f_y / \partial y) = 1$ となる. これらの最大公約元から f_x についての無平方部分 $f_x / \gcd(f_x, \partial f_x / \partial x)$ を計算すると, $\mathbb{V}_C(ab + 1)$ のとき, x となり, $\mathbb{C}^2 \setminus \mathbb{V}_C(a^2b + a)$ のとき, $x^3 + (-a^2b - a)x$ となる. 次に, f_y についての無平方部分 $f_y / \gcd(f_y, \partial f_y / \partial y)$ を計算すると, $\mathbb{V}_C(ab + 1)$ のとき, y となり, $\mathbb{C}^2 \setminus \mathbb{V}_C(a^2b + a)$ のとき, $ay^3 + (-ab - 1)y$ となる. 同様の計算を他のセグメントにも行うと次を得る.

$$\{(\mathbb{V}_C(a, b), \{y, x\}), (\mathbb{V}_C(a) \setminus \mathbb{V}_C(b), \{y, x\}), (\mathbb{V}_C(ab + 1) \setminus \mathbb{V}_C(a), \{y, x\}), \\ (\mathbb{C}^2 \setminus \mathbb{V}_C(a^2b + a), \{ay^3 + (-ab - 1)y, ax + a^2y, x^3 + (-a^2b - a)x\})\}.$$

4.2 ゼロ次元でない場合

ゼロ次元でない場合の計算方法について述べる. イデアルがゼロ次元でない場合, イデアルをゼロ次元に帰着させることが必要になる. このような手法として, 極大独立集合を用いる手法が有効である. ここで $U = \{u_1, \dots, u_r\}$ をイデアル $I \subset K[X]$ を法とする極大独立集合としたとき, I は $K(U)[X \setminus U]$ でゼロ次元イデアルとなる. また, $K(U)$ は変数 U を持つ有理関数体である.

アルゴリズム 8 (ゼロ次元でないイデアルの根基)

Specification: RADICAL(F)

入力: $F : K[X]$ の有限部分集合.

出力: $\sqrt{\langle F \rangle}$ の有限基底 G .

BEGIN

$G \leftarrow \{1\};$

if $1 \notin \langle F \rangle$ **then**

$U \leftarrow \langle F \rangle$ を法とする極大独立集合; $Z \leftarrow F$; $Y \leftarrow X \setminus U$;

while $Y \neq \emptyset$ **do**

$X_i \leftarrow Y$ から X_i をとる; $Y \leftarrow Y \setminus \{X_i\}$; $f_{X_i} \leftarrow \langle F \rangle \cap K(U)[X_i]$ の最小次数のモニック生成元;
 $g_{X_i} \leftarrow f_{X_i}$ の無平方部分; $Z \leftarrow Z \cup \{g_{X_i}\}$

```

end-while
 $C \leftarrow \text{CONT}(Z, U); f \leftarrow \text{EXTCONT}(F, U)$  より求まる  $f$ ;
 $G \leftarrow \langle \text{RADICAL}(F \cup \{f\}) \rangle$  と  $\langle C \rangle$  の共通部分の生成元を計算; (再帰する)
end-if
return  $G$ ;
END

```

次に、このアルゴリズムをパラメータ付きイデアルに拡張を行う。主な変更点は、ゼロ次元の場合と同様に計算過程で必要であったグレブナー基底の計算を、全て包括的グレブナー基底系に変更することである。ただし、この際にゼロ次元の場合とは異なる問題点がある。パラメータ付きイデアルの根基の計算では、 $K(U)[A][X \setminus U]$ の多項式にパラメータ A が含まれるとき、

$$X \setminus U : \text{主変数}, A : \text{パラメータ}, U : K(U) \text{ 上の変数}$$

と 3 種類の変数を扱うことが必要となる。どのようにして包括的グレブナー基底系を構成すればよいかが問題となる。この問題を解決するため、本研究では鍋島-田島 (2023)[6] の手法を用いて包括的グレブナー基底系の計算を行う。この手法は包括的スタンダード基底の計算手法として述べられているが、包括的グレブナー基底系についても同様の手法で計算可能となっている。

鍋島-田島 (2023) の方法 [6]

Step1. A は $\overline{K(U)}$ 上の値をとるものとし、 $K(U)[A][X \setminus U]$ 上で包括的グレブナー基底系を構成する。

Step2. パラメータ空間を L 上に制限する操作を行う。

Step1 の包括的グレブナー基底系は 3 章の定義 2 を用いて計算を行う。この計算はこれまで述べた通常の包括的グレブナー基底系のアルゴリズムで計算可能となっている。次にこの計算した包括的グレブナー基底系を制限するためには、以下の定理を用いる。

定理 8 (鍋島-田島 [6])

$E \subset K[U][A]$, $h \in K[U][A]$ とし、 $\mathbb{A} = \mathbb{V}_{\overline{K(U)}}(E) \setminus \mathbb{V}_{\overline{K(U)}}(h)$ とする。このとき、

1. もし $E \subset K[A]$ ならば、 $\mathbb{A} \cap L^m = \mathbb{V}_L(E) \setminus \mathbb{V}_L(h)$ である。
2. $T = \{c_\alpha : \sum_{\alpha \in \mathbb{N}} c_\alpha u^\alpha \in E, c_\alpha \in K[A]\} \subset K[A]$ (つまり、 E の各項の係数の集合) とする。このとき、 $\mathbb{V}_L(E) = \mathbb{V}_L(T)$ となる。

例 3

t_1, t_2 をパラメータとし、 $\mathbb{V}_{\overline{\mathbb{C}(u_1, u_2)}}(t_1^2 u_1^2 u_2 + (t_2 + 1)u_2 + t_1) \subset (\overline{\mathbb{C}(u_1, u_2)})^2$ を \mathbb{C}^2 で制限する。各項の係数に着目すると、 $\mathbb{V}_{\overline{\mathbb{C}(u_1, u_2)}}(t_1^2 u_1^2 u_2 + (t_2 + 1)u_2 + t_1) \cap \mathbb{C}^2 = \mathbb{V}_{\mathbb{C}}(t_1^2, t_2 + 1, t_1) = \mathbb{V}_{\mathbb{C}}(t_1, t_2 + 1)$ となる。

有理関数体上の包括的グレブナー基底系と定理 8 を用いると次のアルゴリズムを得る。

アルゴリズム 9 (有理関数体上の包括的グレブナー基底系)

Specification: QPGBMAIN(\mathbb{A}, F, U, \prec)

入力: $\mathbb{A} \subset L^m$, $F : K(U)[A][X \setminus U]$ の有限部分集合, $U \subset X$, $\prec : \text{pp}(X \setminus U)$ 上の項順序。

出力: $\langle F \rangle \subset K(U)[A][X \setminus U]$ の \mathbb{A} 上の包括的グレブナー基底系 \mathcal{Q} .

BEGIN

$\mathcal{Q} \leftarrow \emptyset$;

```

 $\mathcal{G} \leftarrow \langle F \rangle \subset K(U)[A][X \setminus U]$  の  $\mathbb{A}$  上での  $\prec$  に関する包括的グレブナー基底系;
while  $\mathcal{G} \neq \emptyset$  do
   $(\mathbb{A}', G') \leftarrow \mathcal{G}$  から  $(\mathbb{A}', G')$  をとる;  $\mathcal{G} \leftarrow \mathcal{G} \setminus \{(\mathbb{A}', G')\}$ ;  $\mathbb{A}'' \leftarrow \mathbb{A}'$  を  $L^m$  上に制限;  $\mathcal{Q} \leftarrow \mathcal{Q} \cup \{(\mathbb{A}'', G')\}$ ;
end-while
return  $\mathcal{Q}$ ;
END

```

このようにして鍋島-田島の方法 [6] を用いることで、ゼロ次元でないパラメータ付きイデアルの根基計算においても L^m 上の包括的グレブナー基底系を計算することができる。以下、アルゴリズム 10 と 11 はパラメータ付きイデアルの根基計算に必要とされる。

アルゴリズム 10 (パラメータ付きイデアルの縮小)

Specification: **PARA_CONT**(\mathbb{A}, F, U)

入力: $\mathbb{A} \subset L^m$, $F : K(U)[A][X \setminus U]$ の有限部分集合, $U : X$ の極大独立集合, $\prec : \text{pp}(X \setminus U)$ 上の項順序。
出力: $\mathcal{C} = \{(\mathbb{A}_1, G_1), \dots, (\mathbb{A}_r, G_r)\} : \forall \alpha \in \mathbb{A}_i (1 \leq i \leq r), \sigma_\alpha(G_i)$ は $\langle \sigma_\alpha(F) \rangle \subset L[X]$ の生成元となる。ただし $\mathbb{A} = \bigcup_{i=1}^r \mathbb{A}_i$ である。

BEGIN

$\mathcal{C} \leftarrow \emptyset$; $\mathcal{H} \leftarrow \text{QPGBMAIN}(\mathbb{A}, F, U, \prec)$;

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

$(\mathbb{A}', G') \leftarrow \mathcal{H}$ から (\mathbb{A}', G') をとる; $\mathcal{H} \leftarrow \mathcal{H} \setminus \{(\mathbb{A}', G')\}$; $LC \leftarrow \{\text{lc}_{X \setminus U}(g') : g' \in G'\}$;

$\mathcal{G} \leftarrow \text{PARA_LCM}(\mathbb{A}, LC)$;

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

$(\mathbb{A}'', f) \leftarrow \mathcal{G}$ から (\mathbb{A}'', f) をとる; $\mathcal{G} \leftarrow \mathcal{G} \setminus \{(\mathbb{A}'', f)\}$;

$\mathcal{Z} \leftarrow \langle G' \rangle : f^\infty$ の \mathbb{A}' 上の包括的グレブナー基底系; $\mathcal{C} \leftarrow \mathcal{Z} \cup \mathcal{C}$;

end-while

end-while

return \mathcal{C} ;

END

アルゴリズム 11 (パラメータ付きイデアルの EXTCONT)

Specification: **PARA_EXTCONT**(\mathbb{A}, F, U)

入力: $\mathbb{A} \subset L^m$, $F : K[A][X]$ の有限部分集合, $U : X$ の極大独立集合, $\prec : \text{pp}(X \setminus U)$ 上の項順序。

出力: $\mathcal{F} = \{(\mathbb{A}_1, f_1), \dots, (\mathbb{A}_r, f_r)\} : \forall \bar{a} \in \mathbb{A}_i (1 \leq i \leq r), \sqrt{\langle \sigma_{\bar{a}}(F) \rangle} = \sqrt{\langle \sigma_{\bar{a}}(F), \sigma_{\bar{a}}(f_i) \rangle} \cap \sqrt{\langle \sigma_{\bar{a}}(F) \rangle^{ec}}$.

BEGIN

$\mathcal{F} \leftarrow \emptyset$; $\mathcal{H} \leftarrow \text{QPGBMAIN}(\mathbb{A}, F, U, \prec)$;

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

$(\mathbb{A}', G') \leftarrow \mathcal{H}$ から (\mathbb{A}', G') をとる; $\mathcal{H} \leftarrow \mathcal{H} \setminus \{(\mathbb{A}', G')\}$; $LC \leftarrow \{\text{lc}_{X \setminus U}(g') : g' \in G'\}$;

$\mathcal{L} \leftarrow \text{PARA_LCM}(\mathbb{A}', LC)$; $\mathcal{F} \leftarrow \mathcal{F} \cup \mathcal{L}$;

end-while

return \mathcal{F} ;

END

以上の拡張より、ゼロ次元でないイデアルについてパラメータ付き根基を計算するアルゴリズムは以下のように記述できる。

アルゴリズム 12 (ゼロ次元でないイデアルのパラメータ付き根基)

Specification:PARA_NONZERO(\mathbb{A}, F)

入力: $\mathbb{A} \subset L^m$, $F : K[A][X]$ の有限部分集合, \mathbb{A} 上で $\langle F \rangle$ はゼロ次元でない.

出力: $\mathcal{N}Z : \langle F \rangle$ の \mathbb{A} 上のパラメータ付き根基.

BEGIN

$\mathcal{G} \leftarrow \mathbb{A}$ 上の $\langle F \rangle$ の包括的グレブナー基底系; $\mathcal{N}Z \leftarrow \{(\mathbb{A}_1, \{1\}) : (\mathbb{A}_1, G_1) \in \mathcal{G}, G_1 = \{1\}\}; \mathcal{G} \leftarrow \mathcal{G} \setminus \mathcal{N}Z;$

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

$(\mathbb{A}_2, G_2) \leftarrow \mathcal{G}$ から (\mathbb{A}_2, G_2) をとる; $\mathcal{G} \leftarrow \mathcal{G} \setminus \{(\mathbb{A}_2, G_2)\}; U \leftarrow \langle \text{lpp}_X(G_2) \rangle$ を法とする極大独立集合;

$\mathcal{Z} \leftarrow \text{PARAZERO_RATIONAL}(\mathbb{A}_2, G_2, U);$

while $\mathcal{Z} \neq \emptyset$ do

$(\mathbb{A}', Z) \leftarrow \mathcal{Z}$ から (\mathbb{A}', Z) をとる; $\mathcal{Z} \leftarrow \mathcal{Z} \setminus \{(\mathbb{A}', Z)\}; \mathcal{C} \leftarrow \text{PARA_CONT}(\mathbb{A}', Z, U);$

$\mathcal{F} \leftarrow \text{PARA_EXTCONT}(\mathbb{A}_2, G_2, U)$

while $\mathcal{F} \neq \emptyset$ do

$(\mathbb{A}'', f') \leftarrow \mathcal{F}$ から (\mathbb{A}'', f') をとる; $\mathcal{F} \leftarrow \mathcal{F} \setminus \{(\mathbb{A}'', f')\};$

while $\mathcal{C} \neq \emptyset$ do

$(\mathbb{B}, C) \leftarrow \mathcal{C}$ から (\mathbb{B}, C) をとる; $\mathcal{C} \leftarrow \mathcal{C} \setminus \{(\mathbb{B}, C)\};$

if $\mathbb{B} \cap \mathbb{A}'' \neq \emptyset$ then

$\mathcal{L} \leftarrow \text{PARA_NONZERO}(\mathbb{B} \cap \mathbb{A}'', F \cup \{f'\});$

end-if

while $\mathcal{L} \neq \emptyset$ do

$(\mathbb{B}', L) \leftarrow \mathcal{L}$ から (\mathbb{B}', L) をとる; $\mathcal{L} \leftarrow \mathcal{L} \setminus \{(\mathbb{B}', L)\};$

$\mathcal{A} \leftarrow \text{PARA_INTERSECTION}(\mathbb{B}', L, C); \mathcal{N}Z \leftarrow \mathcal{N}Z \cup \mathcal{A};$

end-while

end-while

end-while

end-while

return $\mathcal{N}Z;$

END

アルゴリズム 13 ($K(U)[X \setminus U]$ 上のゼロ次元イデアルのパラメータ付き根基)

Specification:PARAZERO_RATIONAL(\mathbb{A}, F, U)

入力: $\mathbb{A} \subset L^m$, $F : K(U)[A][X \setminus U]$ の有限部分集合, $\forall \bar{a} \in \mathbb{A}$, $\langle \sigma_{\bar{a}}(F) \rangle$ は $L(U)[X \setminus U]$ 上でゼロ次元, $U \subset X$.

出力: $\mathcal{H} : \langle F \rangle \subset K(U)[X \setminus U]$ の \mathbb{A} 上のパラメータ付き根基.

BEGIN

$\mathcal{H} \leftarrow \{(\mathbb{A}, F)\}; Y \leftarrow X \setminus U;$

while $Y \neq \emptyset$ do

$Z \leftarrow Y$ から Z をとる; $Y \leftarrow Y \setminus \{Z\};$

$\mathcal{G} \leftarrow \text{QPGBMAIN}(\mathbb{A}, F, U, \prec)$, ここで, \prec は $Z \ll (X \setminus U) \setminus Z$ となるブロック項順序;

$\mathcal{G}' \leftarrow \{(\mathbb{A}, g) : g \in G \cap K(U)[Z], (\mathbb{A}, G) \in \mathcal{G}\};$

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

$(\mathbb{A}', g') \leftarrow \mathcal{G}'$ から (\mathbb{A}', g') をとる; $\mathcal{G}' \leftarrow \mathcal{G}' \setminus \{(\mathbb{A}', g')\}; \mathcal{B} \leftarrow \text{GIZYOZAN}(\mathbb{A}', g', Z);$

```

while  $\mathcal{B} \neq \emptyset$  do
     $(\mathbb{B}, b) \leftarrow \mathcal{B}$  から  $(\mathbb{B}, b)$  をとる;  $\mathcal{B} \leftarrow \mathcal{B} \setminus \{(\mathbb{B}, b)\}$ ;  $\mathcal{P} \leftarrow \emptyset$ ;
    while  $\mathcal{H} \neq \emptyset$  do
         $(\mathbb{B}', G') \leftarrow \mathcal{H}$  から  $(\mathbb{B}', G')$  をとる;  $\mathcal{H} \leftarrow \mathcal{H} \setminus \{(\mathbb{B}', G')\}$ ;
        if  $\mathbb{B} \cap \mathbb{B}' \neq \emptyset$  then
             $\mathcal{P} \leftarrow \mathcal{P} \cup \{(\mathbb{B} \cap \mathbb{B}', G' \cup \{b\})\}$ ;
        end-if
    end-while
     $\mathcal{H} \leftarrow \mathcal{P}$ ;
    end-while
end-while
end-while
return  $\mathcal{H}$ ;
END

```

本研究において、アルゴリズム 13 は計算機代数システム Risa/Asir 上に実装されている。

例 4

a をパラメータ, x, y, z を変数とする. $F = \{ax^2z + xy^2, (y + xz)^2 + ax^3z^2\} \subset \mathbb{Q}[a][x, y, z]$ について, $\langle F \rangle$ のパラメータ付き根基を考える. 実装されたプログラムは次の, パラメータ付き根基を出力する.

$$\{(\mathbb{C} \setminus \mathbb{V}_{\mathbb{C}}(a), \{azx + y^2, az^2x^3 + (-2azy + z^2)x^2 + 3azzx + 2ay\}), (\mathbb{V}_{\mathbb{C}}(a), \{y, zx\})\}.$$

本研究ではパラメータ付き多項式イデアルに対する根基計算を行う計算方法を確立し, Risa/Asir 上にアルゴリズムの実装を行なった. 特にゼロ次元でないパラメータ付き多項式イデアルの根基計算においては, 多項式環を拡大した後の包括的グレブナー基底系を計算するために鍋島-田島の手法 [6] を用いることが有効であることが分かった.

参考文献

- [1] Thomas Becker, Volker Weispfenning. *Gröbner Bases A Computational Approach to Commutative Algebra*. Springer-Verlag, New York, Inc., 1993.
- [2] David Cox, Jhon Little, Donal O'Shea. *Ideals, Varieties, and Algorithms(2nd edition)*. Springer-Verlag, New York, Inc., 1997.
- [3] Patrizia Gianni, Barry Trager, Gail Zacharias. *Gröbner bases and primary decomposition of polynomial ideals*. J. Symbolic Computation Vol. 6, 149-167, 1988
- [4] Michael Kalkbrener. *On the stability of Gröbner bases under specializations*. J. Symbolic Computation Vol. 24, 51-58, 1997.
- [5] Deepak Kapur, Yao Sun, Dingkang Wang. *An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system*. J. Symbolic Computation ,Vol. 49, 27-44, 2013.
- [6] Katsusuke Nabeshima, Shinichi Tajima. *CSSg method for several genericities of parametric systems*. Japan J. Industrial and Applied Mathematics Vol. 40, 315–337, 2023.
- [7] Masayuki Noro, Taku Takehima *Risa/Asir - a computer algebra system*. ISSAC 1992 (ed. P. S. Wang), ACM , 387–396, 2013.
<http://www.math.kobe-u.ac.jp/Asir/asir.html>