正標数体上のパラメータ付きイデアルの根基計算について

On the Computation of Radicals of Parametric Ideals over a Field of Positive Characteristic

東京都立大学大学院理学研究科数理科学専攻　　田中一希 *1
KAZUKI TANAKA
Department of Mathematical Sciences, Graduate School of Science,
Tokyo Metropolitan University

Abstract

Comprehensive Gröbner systems, introduced by Weispfenning in 1992, generalize Gröbner bases for parametric ideals. Following their introduction, various algorithms for polynomial ideals have been extended to the parametric setting. In this paper, we propose an algorithm for computing the radical of parametric ideals over finite fields by combining comprehensive Gröbner systems with Matsumoto's radical computation algorithm.

1　はじめに

イデアルの根基は次で定義される．

定義 1
可換環 R とそのイデアル I に対し，

$$\sqrt{I} = \left\{ f \in R \,\middle|\, {}^{\exists} l \in \mathbb{Z}_{>0} \ \text{ s.t. } \ f^l \in I \right\}$$

を I の根基 (radical) という．

本稿では，係数にパラメータを含む多項式環のイデアル（以降，パラメトリックイデアルと呼ぶ）の根基の計算法について述べる．一般にパラメトリックイデアルの根基は，パラメータの値に応じて異なる形をとる．例えば，多項式環 $\mathbb{C}[x,y]$ のイデアル

$$I = \langle x^2 + axy + by^2,\ y^5 + a \rangle$$

について，根基 $\sqrt{I}$ は

$$\sqrt{I} = \begin{cases} \langle x, y \rangle & (a = 0), \\ \langle 2x + ay, y^5 + a \rangle & (a \neq 0,\ a^2 - 4b = 0), \\ I & (\text{otherwise}) \end{cases}$$

となる．

本稿を通して用いる記号を導入する．K を計算可能な体，L をその拡大体とし，$U = (u_1, \ldots, u_m)$ をパラメータの組，$X = (x_1, \ldots, x_n)$ を変数の組とする．$a = (a_1, \ldots, a_m) \in L^m$ に対して，U に a を

*1 〒 192-0397 東京都八王子市南大沢 1-1　E-mail: tanaka-kazuki@ed.tmu.ac.jp

代入する写像を $\pi_a : K[U][X] \to L[X]$ で表す．また，多項式の集合 $P \subset K[U]$ に対して，$V_L(P) = \{a \in L^m \mid {}^\forall p \in P,\ p(a) = 0\}$ と定め，$K = L$ のときは $V(P) = V_L(P)$ と略記する．以上の記号のもとで，本稿で扱う問題であるパラメトリックイデアルの根基計算は，次のように定式化される．

問題 1
与えられたイデアルの生成系 $F \subset K[U][X]$ に対して，各 i について

$$^\forall a \in V_L(E_i) \setminus V_L(N_i),\ \langle \pi_a(G_i) \rangle = \sqrt{\langle \pi_a(F) \rangle}$$

が成り立つようなペアの系 $\{(E_i, N_i, G_i)\}_{i=1,\dots,r}$ （$E_i, N_i \subset K[U],\ G_i \subset K[U][X]$）はどのようにすれば構成できるか．

この問題に対して有効な道具として，包括的 Gröbner 基底系がある．包括的 Gröbner 基底系は，Weispfenning [6] によって定義された，パラメトリックイデアルに対して Gröbner 基底の役割を果たす概念である．これを，パラメータを含まない場合の Gröbner 基底を用いた根基計算アルゴリズムと適切に組み合わせることにより，パラメータを含む場合にアルゴリズムを拡張できる．

係数体 K の標数が 0 の場合については，Kuramochi–Tanaka–Nabeshima [3] により，パラメトリックイデアルの根基計算アルゴリズムが既に与えられている．この結果は，Gianni–Trager–Zacharias [2] による標数 0 の場合の根基計算アルゴリズムをもとに，それを包括的 Gröbner 基底系を用いてパラメトリックな状況に拡張している．

本稿では，Matsumoto [4] による正標数の場合の根基計算アルゴリズムと包括的 Gröbner 基底系とを組み合わせることにより，$K = L = \mathbb{F}_q$ の場合におけるパラメトリックイデアルの根基計算を与える．

2　準備

本章では，本稿で用いる基本的な道具である包括的 Gröbner 基底系と Matsumoto アルゴリズムについて簡単にまとめる．

2.1　包括的 Gröbner 基底系

まず，包括的 Gröbner 基底系の定義を述べる．

定義 2 (包括的 Gröbner 基底系, CGS)
$K[U][X]$ のイデアル $\langle F \rangle$ をパラメトリックイデアルとし，$\prec$ を単項式順序とする．また，$E, N \subset K[U]$ を有限集合とする．有限集合の組

$$\{(E_i, N_i, G_i)\}_{i=1,\dots,r} \quad (E_i, N_i \subset K[U],\ G_i \subset K[U][X])$$

が，$\langle F \rangle$ の $V(E) \setminus V(N)$ における $\prec$ に関する包括的 Gröbner 基底系 (comprehensive Gröbner system, CGS) であるとは，次の 4 条件を満たすことをいう．

(i) 次が成り立つ：

$$V(E) \setminus V(N) = \bigcup_{i=1}^{r} \big(V(E_i) \setminus V(N_i)\big).$$

(ii) 各 $i, j\ (i \neq j)$ に対して，次が成り立つ：

$$V(E_i) \setminus V(N_i) \neq \emptyset,\ \ \big(V(E_i) \setminus V(N_i)\big) \cap \big(V(E_j) \setminus V(N_j)\big) = \emptyset.$$

(iii) 任意の $a \in V(E_i) \setminus V(N_i)$ に対して，$\pi_a(G_i)$ は $\langle \pi_a(F) \rangle$ の極小 Gröbner 基底である．

(iv) 任意の $a \in V(E_i) \setminus V(N_i)$ と $g \in G_i$ に対し，$\pi_a(\mathrm{LC}\,(g)) \neq 0$ が成り立つ．

また，各 (E_i, N_i, G_i) を断片 (segment) という．

直感的には，CGS は，パラメータ空間を有限個の部分集合に分割し，各部分集合上でイデアルの Gröbner 基底の形を一様に与えたものである．CGS を計算するアルゴリズムとしては Suzuki–Sato アルゴリズム [5] 等が知られている．

2.2 Matsumoto のアルゴリズム

次に Matsumoto [4] のアルゴリズムを係数体 $K = \mathbb{F}_q$ (q は素数のべき) の場合に限って述べる．写像 $\varphi : \mathbb{F}_q[X] \to \mathbb{F}_q[X]; f(x_1, \ldots, x_n) \mapsto f(x_1^q, \ldots, x_n^q)$ を Frobenius 写像と呼ぶ．

定理 3 ([4] Chap.2)
$\mathbb{F}_q[X]$ のイデアル I に対して，次が成り立つ．
(1) $I \subseteq \varphi^{-1}(I) \subseteq \sqrt{I}$.
(2) $I \neq \sqrt{I}$ ならば $I \subsetneq \varphi^{-1}(I)$.

この定理により，イデアルの増大列

$$I \subset \varphi^{-1}(I) \subset \varphi^{-2}(I) \subset \cdots$$

が得られるが，Noether 性によりある $d \in \mathbb{Z}_{\geq 0}$ が存在して $\varphi^{-d}(I) = \varphi^{-(d+1)}(I) = \sqrt{I}$ となる．したがって，次の手順で根基が計算できる．

(1) イデアル I に対し $J = \varphi^{-1}(I)$ を計算する．

(2) I と J が一致するか判定する．

(3) 一致するならば $I = \sqrt{I}$ である．一致しない場合は I を J に更新して，最初に戻る．

よって，根基を計算するためには，Frobenius 写像の逆像の計算とイデアルの一致判定が必要である．イデアルの一致性は簡約 Gröbner 基底の性質を用いて判定できるので，あとは Frobenius 写像の逆像の計算法について考えればよい．

Frobenius 写像の逆像の計算のためには，次の定理が重要である．

定理 4 ([4] Proposition 2.5.)
I を $\mathbb{F}_q[X]$ のイデアルとする．新しい変数の組 $Y = (y_1, \ldots, y_n)$ を用意し，$\mathbb{F}_q[X, Y]$ のイデアル

$$J = \langle I \rangle_{\mathbb{F}_q[X,Y]} + \langle y_1 - x_1^q, \ldots, y_n - x_n^q \rangle$$

を定める．このとき，$\varphi^{-1}(I)$ は，$J \cap \mathbb{F}_q[Y]$ に含まれる多項式の各変数 y_i を x_i で置き換えたものにより生成されるイデアルと一致する．

この定理と消去定理により，$F \subset \mathbb{F}_q[X]$ に対する $\varphi^{-1}(\langle F \rangle)$ の生成系は，$F \cup \{y_1 - x_1^q, \ldots, y_n - x_n^q\}$ に対して $X \gg Y$ なる順序に関する Gröbner 基底を計算し，$\mathbb{F}_q[Y]$ の元を取り出すことで計算できる．

以上により，根基は以下のアルゴリズムによって計算できる．

Algorithm 1 Radical (Matsumoto's algorithm)

Require: $F \subset \mathbb{F}_q[X]$: イデアルの生成系
Ensure: $R \subset \mathbb{F}_q[X]$: 根基 $\sqrt{\langle F \rangle}$ の生成系
1: $B \leftarrow F \cup \{y_1 - x_1^q, \ldots, y_n - x_n^q\} \subset \mathbb{F}_q[X, Y]$
2: $G \leftarrow B$ の $X \gg Y$ なる消去順序に関する Gröbner 基底
3: $H \leftarrow G \cap \mathbb{F}_q[Y]$ の各変数 y_i を x_i で置き換えたもの
4: **if** $\langle F \rangle = \langle H \rangle$ **then**
5: **return** F
6: **else**
7: **return** Radical(H)

3 $\mathbb{F}_q$ 係数のパラメトリックイデアルの根基計算アルゴリズム

本章では，前章で述べた Matsumoto のアルゴリズムを，CGS を用いてパラメトリックな状況へ拡張することで，$\mathbb{F}_q$ 係数のパラメトリックイデアルに対する根基計算アルゴリズムを与える．

Matsumoto のアルゴリズムと同様に，定理 3 からパラメトリックイデアルの根基は次の手順で計算できる．

(1) パラメトリックイデアルの生成系 $F \subset \mathbb{F}_q[U][X]$ に対し，$\varphi^{-1}(\langle F \rangle)$ の $V(E) \setminus V(N)$ における CGS $\{(E_i, N_i, G_i)\}_i$ を計算する．

(2) 各断片 (E_i, N_i, G_i) に対して，$V(E_i) \setminus V(N_i)$ において $\langle G_i \rangle$ と $\langle F \rangle$ が一致するか判定する．

(3) 一致する断片については，F が根基の生成系であるので，そこで終了する．一致しない断片については，F を G_i，E を E_i，N を N_i に更新して，それぞれ最初に戻る．

よって，根基を計算するためには，パラメトリックイデアルの Frobenius 写像の逆像の計算と，パラメトリックイデアルの一致判定が必要である．

3.1 Frobenius 写像の逆像計算

まず，パラメトリックイデアルの生成系 $F \subset \mathbb{F}_q[U][X]$ に対する Frobenius 写像の逆像 $\varphi^{-1}(\langle F \rangle)$ の計算法を与える．定理 4 および消去定理から，これは $F \cup \{y_i - x_i^q\}_i$ に対する CGS 計算に帰着される．よって，次のアルゴリズムが得られる．

Algorithm 2 ParaInverseFrobeniusMap

Require: (E, N, F): 有限集合 $E, N \subset \mathbb{F}_q[U], F \subset \mathbb{F}_q[U][X]$.
Ensure: $\mathcal{H}$: $\varphi^{-1}(\langle F \rangle)$ の $V(E) \setminus V(N)$ における CGS
1: $B \leftarrow F \cup \{y_1 - x_1^q, \ldots, y_n - x_n^q\} \subset \mathbb{F}_q[U][X, Y]$
2: $\mathcal{G} \leftarrow B$ の $V(E) \setminus V(N)$ における $X \gg Y$ なる順序に関する CGS
3: $\mathcal{H} \leftarrow \emptyset$
4: **for all** $(E_i, N_i, G_i) \in \mathcal{G}$ **do**
5: $H_i \leftarrow G_i \cap \mathbb{F}_q[U][Y]$ の各変数 y_i を x_i で置き換えたもの
6: $\mathcal{H} \leftarrow \mathcal{H} \cup \{(E_i, N_i, H_i)\}$
7: **return** $\mathcal{H}$

消去定理から，このアルゴリズムの出力は CGS になることに注意する．

3.2 パラメトリックイデアルの一致判定

次に，2 つのパラメトリックイデアルが一致するか判定する方法を与える．ただし，アルゴリズムの形から，(E, N, G) を CGS の断片とし，$(\tilde{E}, \tilde{N}, \tilde{G})$ を ParaInverseFrobeniusMap(E, N, G) の断片としたときに限って，これらが表すパラメトリックイデアルが一致するか判定する方法を与えればよい．これらの断片は以下の 4 条件を満たす．

(i) 任意の $a \in V(E) \setminus V(N)$ に対して，$\pi_a(G)$ は $\langle \pi_a(I) \rangle$ の Gröbner 基底である．

(ii) 任意の $a \in V(E) \setminus V(N)$ と $g \in G$ に対して，$\pi_a(\mathrm{LC}\,(g)) \neq 0$ である．

(iii) 任意の $a \in V(\tilde{E}) \setminus V(\tilde{N})$ に対して $\langle \pi_a(G) \rangle \subset \langle \pi_a(\tilde{G}) \rangle$ が成り立つ．

(iv) $V(E) \setminus V(N) \supset V(\tilde{E}) \setminus V(\tilde{N})$ が成り立つ．

(E, N, G) が CGS の断片であることから (i)，(ii) が従い，これにより任意の $f \in \mathbb{F}_q[U][X]$ に対して，normal form $\mathrm{NF}_G(f)$ が計算できる．また，定理 3 より (iii) が従う．

以上のことから，一致判定のためには逆の包含関係 $\langle \pi_a(G) \rangle \supset \langle \pi_a(\tilde{G}) \rangle$ が成り立つかどうかを判定できればよく，そのためには各 $g \in \tilde{G}$ に対して $\mathrm{NF}_G(g) = 0$ であることを確認すればよい．しかし，以下の例のような場合に注意が必要である．

例 1
$G = \{x^3 + y + a, y^2 + bx\} \subset \mathbb{F}_3[a, b][x, y]$ とし，*CGS* の断片 $(\{a - b\}, \{1\}, G)$ とパラメトリック多項式 $f = x^3y - b^3x + by \in \mathbb{F}_3[a, b][x, y]$ を考える．このとき，

$$\mathrm{NF}_G(f) = (-b^3 + b)x + (-a + b)y$$

となるが，$(a, b) \in V(a - b) \subset \mathbb{F}_3^2$ なので $\mathrm{NF}_G(f) = 0$ である．

このように，パラメトリックの場合には，normal form が見かけの上では 0 にならないが，パラメータの条件や Fermat の小定理から実際には 0 になることがある．この問題を解消するため，与えられたパラメータ空間においてパラメトリック多項式が 0 になるかを判定する方法を与える．

補題 5
$r \in \mathbb{F}_q[U][X]$ をパラメトリック多項式，$E, N \subset \mathbb{F}_q[U]$ を有限集合とする．$H \subset \mathbb{F}_q[U]$ を r の係数全体の集合とし，$\Psi = \{u_1^q - u_1, \ldots, u_m^q - u_m\}$ とおく．このとき，次は同値である．

(i) 任意の $a \in V(E) \setminus V(N)$ に対し，$\pi_a(r) = 0$ が成り立つ．

(ii) 任意の $h \in H, v \in N$ に対し，$hv \in \langle E \cup \Psi \rangle$ が成り立つ．

この補題は Gao らによる有限体上の零点定理 [1, Theorem 2.2] を用いて証明できる．これにより，次のアルゴリズムを得る．

Algorithm 3 IsZeroInLocallyClosedSet

Require: $r \in \mathbb{F}_q[U][X]$，$E, N \subset \mathbb{F}_q[U]$：有限集合.

Ensure: 「任意の $a \in V(E) \setminus V(N)$ に対し，$\pi_a(r) = 0$ が成り立つ」の真偽.

1: $H \leftarrow r$ の係数全体の集合
2: $\Psi \leftarrow \{u_1^q - u_1, \ldots, u_m^q - u_m\}$
3: $G \leftarrow \langle E \cup \Psi \rangle$ の Gröbner 基底
4: **for all** $(h, v) \in H \times N$ **do**
5: $\quad \tilde{r} \leftarrow \mathrm{NF}_G(hv)$
6: $\quad$ **if** $\tilde{r} \neq 0$ **then**
7: $\quad\quad$ **return False**
8: **return True**

以上で normal form が見かけ上 0 にならない問題は解決した．これにより，次のパラメトリックイデアルの一致判定のアルゴリズムを得る.

Algorithm 4 ParaIdealMatch

Require: (E, N, G) CGS の断片，$(\tilde{E}, \tilde{N}, \tilde{G})$：ParaInverseFrobeniusMap$(E, N, G)$ の断片.

Ensure: 「任意の $a \in V(\tilde{E}) \setminus V(\tilde{N})$ に対して，$\langle \pi_a(G) \rangle = \langle \pi_a(\tilde{G}) \rangle$ である」の真偽.

1: **for all** $g \in \tilde{G}$ **do**
2: $\quad r \leftarrow \mathrm{NF}_G(g)$
3: $\quad$ **if not** IsZeroInLocallyClosedSet$(r, \tilde{E}, \tilde{N})$ **then**
4: $\quad\quad$ **return False**
5: **return True**

3.3 パラメトリックイデアルの根基計算アルゴリズム

以上を組み合わせることで，パラメトリックイデアルの根基を計算するアルゴリズムを構成する．一致判定のアルゴリズム ParaIdealMatch は入力が CGS の断片であることを要求するため，本アルゴリズムでは前処理としてまず F の CGS を計算する．その後，得られた各断片 (E_i, N_i, G_i) に対して，主要部である ParaRadicalMain を適用する.

Algorithm 5 ParaRadical

Require: $F \subset \mathbb{F}_q[U][X]$: パラメトリックイデアルの生成系

Ensure: $\mathcal{R}$: $\sqrt{\langle F \rangle}$ の CGS

1: $\mathcal{R} \leftarrow \emptyset$; $\mathcal{G} \leftarrow F$ の CGS
2: **for all** $(E_i, N_i, G_i) \in \mathcal{G}$ **do**
3: $\quad \mathcal{R} \leftarrow \mathcal{R} \cup$ ParaRadicalMain(E_i, N_i, G_i)
4: **return** $\mathcal{R}$

Algorithm 6 ParaRadicalMain

Require: (E, N, G): CGS の断片

Ensure: $\mathcal{R}$: $V(E) \setminus V(N)$ における $\sqrt{\langle G \rangle}$ の基底系

1: $\mathcal{R} \leftarrow \emptyset$
2: $\mathcal{H} \leftarrow \mathrm{ParaInverseFrobeniusMap}(E, N, G)$
3: **for all** $(E_i, N_i, G_i) \in \mathcal{H}$ **do**
4: **if** $\mathrm{ParaIdealMatch}((E, N, G), (E_i, N_i, G_i))$ **then**
5: $\mathcal{R} \leftarrow \mathcal{R} \cup \{(E_i, N_i, G)\}$
6: **else**
7: $\mathcal{R} \leftarrow \mathcal{R} \cup \mathrm{ParaRadicalMain}(E_i, N_i, G_i)$
8: **return** $\mathcal{R}$

4 さいごに

本稿では，包括的 Gröbner 基底系と Matsumoto のアルゴリズムを組み合わせることにより，有限体上のパラメトリックイデアルの根基を計算するアルゴリズムを構成した．今回は係数体を有限体に限定して議論を行ったが，より一般の正標数体への拡張が今後の課題である．

参 考 文 献

[1] Gao, S., Platzer, A., Clarke, E. M. (2011) Quantifier Elimination over Finite Fields Using Gröbner Bases. LNCS Vol. 6742, 140-157. Springer, Berlin Heidelberg.

[2] Gianni, P., Trager, B., Zacharias, G. (1988) Gröbner Bases and Primary Decomposition of Polynomial Ideals. *J. of Symbolic Computation* Vol.6, 149-167.

[3] Kuramochi, R., Tanaka, K., Nabeshima, K. (2024) On the Radical of a Polynomial Ideal with Parameters. *Proc. of CASC* 2024. LNCS Vol.14938, 193-214. Springer, Cham.

[4] Matsumoto, R. (2001) Computing the Radical of an Ideal in Positive Characteristic. *J. of Symbolic Computation* Vol.32, 263-271.

[5] Suzuki, A., Sato, Y. (2006) A Simple Algorithm to Compute Comprehensive Gröbner Bases. *Proc. of ISSAC* 2006, 326-331.

[6] Weispfenning, V. (1992) Comprehensive Gröbner Bases. *J. of Symbolic Computation* Vol.14-1, 1-29.