パラメータ付きのイデアル操作の計算について
On Computations of Ideal Operations with Parameters

東京理科大学　石原侑樹
yishihara@rs.tus.ac.jp

RIMS 共同研究 (公開型)
Computer Algebra - Theory and its Applications,
2022/12/20

Overview of Slides

Overview of Slides

研究背景-1

$f_1, \ldots, f_s$: 多項式
$\langle f_1 \ldots, f_s \rangle$: $f_1, \ldots, f_s$ から生成されるイデアル i.e.

$$\langle f_1 \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_i : \text{多項式} \right\}$$

イデアル操作 ＝ 1 つ以上のイデアルから新しいイデアルを生成する操作

Example

$I = \langle x^2 \rangle,\ \ J = \langle x^3, y \rangle$

- $I + J = \langle x^2, y \rangle$
- $I \cap J = \langle x^3, x^2 y \rangle$
- $I : J = \langle x^2 \rangle$
- $\sqrt{I} = \langle x \rangle$

研究背景-2

イデアル操作の多くはグレブナー基底を用いて計算することができる

共通部分の場合

多項式環 $K[X]=K[x_1,\ldots,x_n]$ において，I，J をイデアル，t を新しい変数とすると，

$$I\cap J=(I\cdot t+J\cdot(1-t))\cap K[X]$$

が成り立つ．よって，G をブロック順序 $t>>X$ に関する $I\cdot t+J\cdot(1-t)$ のグレブナー基底とすると，消去定理から

$$I\cap J=\langle G\cap K[X]\rangle.$$

Example

$I=\langle x^2\rangle$，$J=\langle x^3,y\rangle$ の時，$I\cdot t+J\cdot(1-t)=\langle tx^2,x^3(1-t),y(1-t)\rangle$ の辞書式順序 $t<x<t$ に関する簡約グレブナー基底は $G=\{x^3,x^2y,ty-y,tx^2\}$ であり，$I\cap J=\langle x^3,x^2y\rangle$

本研究の目的

目的 1 パラメータを含むイデアル操作の効率的なアルゴリズムを開発する

目的 2 目的 1 で考案したアルゴリズムを部品として，
パラメータを含むイデアルの準素分解のアルゴリズムを開発する

パラメータを含むイデアル操作を考える利点

- パラメータの値で場合を分けをした包括的なイデアル操作が分かる

Example

$A=\{a\}$：パラメータ，$X=\{x,y\}$：主変数，$I=\langle x+a\rangle$，$J=\langle x^2,y\rangle$ とした時には，

- $a=0$ ならば，$I\cap J=\langle x^2,xy\rangle$
- $a\neq 0$ ならば，$I\cap J=\langle x^2(x+a),(x+a)y\rangle$

$V(f_1,\ldots,f_s)=\{b\in K^m\mid f_1(b)=\cdots=f_s(b)=0\}$ とすれば，

前者は $V(a)$，後者は $K\setminus V(a)$ となる．

先行研究

先行研究

Nabeshima-Tajima Nabeshima, K., Tajima, S. Testing Zero-Dimensionality of Varieties at a Point. Math.Comput.Sci. 15, 317-331 (2021)

Yokoyama Yokoyama, K. Stability of Parametric Decomposition. In: Iglesias, A., Takayama, N. (eds) Mathematical Software - ICMS 2006. ICMS 2006. Lecture Notes in Computer Science, vol 4151. (2006)

[Nabeshima-Tajima] においては，Appendix でパラメータ付きのイデアル商と飽和イデアルの計算を紹介している．

[Yokoyama] においては，パラメータ付きのイデアルの根基イデアルの計算や，$\mathbb{C}$ におけるパラメータ準素分解のアルゴリズムについて考察している．

本発表の目的と主結果

本発表の目的

- いくつかのパラメータ付きイデアル操作の既知のアルゴリズムを紹介
- 有理数係数のパラメータ付きイデアルの「計算可能な準素分解」を紹介（発表者が新しく定義）

主結果

- Comprehensive Gröbner System (CGS) を用いて，（実行可能な）パラメータ準素分解の計算アルゴリズムを考案
- ヒルベルトの既約性定理を用いて，イデアルのパラメータに値を代入した後の（準）素イデアル性について考察

（注）以上の結果はこれから論文として投稿を考えているため，修正の可能性あり

Overview of Slides

記号の定義

- K: 体，$\overline{K}$: K の代数閉包
- $A = \{a_1, \ldots, a_m\}$: パラメータ，$X = \{x_1, \ldots, x_n\}$: 主変数
- $K[A, X]$: 多項式環
- $a \in K^m$ に対し，$\phi_a: K[A, X] \to K[X]$: a を代入する写像 i.e. $\phi_a(f(A, X)) = f(a, X)$
- $I \subset K[A, X]$: パラメータ付きのイデアル
- $\mathcal{I}$: $K[A, X]$ のパラメータ付きイデアル全体の集合
- $\mathcal{F}: \prod_{i=1}^{r} \mathcal{I} \to \mathcal{I}$: イデアル操作

  例：$\mathcal{F}(I) = \sqrt{I}$，$\mathcal{F}(I, J) = I \cap J$，$\mathcal{F}(I, J) = I : J$ など

「イデアル操作を計算」
||
「イデアル操作の結果のイデアルのグレブナー基底（系）を求める」

イデアル操作の例

I と J を $K[A, X]$ のイデアルとする．

- イデアル和 $I + J = \{f + g \in K[A, X] \mid f \in I, g \in J\}$
- イデアル積 $IJ = \langle fg \in K[A, X] \mid f \in I, g \in J\rangle$
- 共通部分 $I \cap J = \{f \in K[A, X] \mid f \in I$ かつ $f \in J\}$
- イデアル商 $I : J = \{f \in K[A, X] \mid fJ \subset I\}$
- 飽和イデアル $I : J^\infty = \{f \in K[A, X] \mid \exists m, f^m J \subset I\}$
- 根基 $\sqrt{I} = \{f \in K[A, X] \mid \exists m, f^m \in I\}$
- equidimensional hull $\mathrm{hull}(I) = \bigcap_{Q \in \mathcal{Q}, \dim Q = \dim I} Q$．ここで $\mathcal{Q}$ は I の最短準素分解
- $IK[A, X]_{K[U]^\times} \cap K[A, X]$: 独立集合 U による I の局所化

包括的グレブナー基底系

Definition (包括的グレブナー基底系．[2]，[1])

$F = \{f_1(A, X), \ldots, f_k(A, X)\}$ を $K[X, A]$ の有限集合，$S_1, \ldots, S_l$ を $\overline{K}^m$ の分割，$\{G_1, \ldots, G_l\}$ を $K[A, X]$ の有限集合の集合とする．各 i について，任意の $a \in S_i$ に対して，$\phi_a(G_i)$ がイデアル $\langle f_1(a, X), \ldots, f_k(a, X)\rangle_{\overline{K}[X]}$ のグレブナー基底であるとき，$\mathcal{G} = \{(S_1, G_1), \ldots, (S_l, G_l)\}$ は F の包括的グレブナー基底系（**Comprehensive Gröbner System**）と呼ばれる．

Example

$A = \{a\}$，$X = \{x, y\}$，$F = \{ax^2 + y, y^2\}$ に対し，

$$\mathcal{G} = \{(V(a), \{y\}), (\mathbb{C} \setminus V(a), \{ax^2 + y, y^2\})\}$$

は F の包括的グレブナー基底系である．

[1] 佐藤洋祐. 包括的グレブナー基底 (系) 入門. 数式処理. **14** (1)，3-15，日本数式処理学会 (2007).

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

イデアル操作の包括的グレブナー基底系

Definition

$\mathcal{F}$ をイデアル操作，$(I_1, \ldots, I_r)$ を $\overline{K}[A, X]$ の r 個のイデアルの組とする．また，$S_1, \ldots, S_l$ を $\overline{K}^m$ の分割，$\{G_1, \ldots, G_l\}$ を $K[A, X]$ の有限集合の集合とする．各 i について，任意の $a \in S_i$ に対して，$\phi_a(G_i)$ がイデアル $\mathcal{F}(\phi_a(I_1), \ldots, \phi_a(I_r))$ のグレブナー基底である時，
$\mathcal{G} = \{(S_1, G_1), \ldots, (S_l, G_l)\}$ を $(I_1, \ldots, I_r)$ に関する $\mathcal{F}$ の包括的グレブナー基底系と呼ぶ．

Example

$\mathcal{F}$ を共通部分のイデアル操作とする．すなわち，$\mathcal{F} \colon \mathcal{I} \times \mathcal{I} \to \mathcal{I}$, $\mathcal{F}(I, J) = I \cap J$．$A = \{a\}$，$X = \{x, y\}$，$I = \langle x + a \rangle$，$J = \langle x^2, y \rangle$ とした時には，

- $a = 0$ ならば，$\phi_a(I) \cap \phi_a(J) = \langle x^2, xy \rangle$
- $a \neq 0$ ならば，$\phi_a(I) \cap \phi_a(J) = \langle x^2(x + a), (x + a)y \rangle$

となり，$\mathcal{G} = \{(V(a), \{x^2, xy\}, \{(\mathbb{C} \setminus V(a), \{x^2(x + a), (x + a)y\})\})\}$ が $\mathcal{F}$ の $(\langle x + a \rangle, \langle x^2, y \rangle)$ に関する包括的グレブナー基底系となる．

イデアル操作の包括的グレブナー基底系の計算-1

イデアル操作がグレブナー基底を使って計算できる場合，包括的グレブナー基底系を使って計算できる．

共通部分の場合
$K[A, X]$ において，I，J をイデアル，t を新しい変数とすると，

$$I \cap J = (I \cdot t + J \cdot (1 - t)) \cap K[X]$$

が成り立つ．よって，$\mathcal{G} = \{(S_1, G_1), \ldots, (S_l, G_l)\}$ をブロック順序 $t >> X >> A$ に関する $I \cdot t + J \cdot (1 - t)$ の包括的グレブナー基底系とすると，

$$\{(S_1, G_1 \cap K[A, X]), \ldots, (S_l, G_l \cap K[A, X])\}$$

は (I, J) に関する共通部分の包括的グレブナー基底系である．

イデアル操作の包括的グレブナー基底系の計算-2

イデアル商の場合
$K[A, X]$ において，I をイデアル，f を 0 でない多項式とすると，

$$I : \langle f \rangle = (I \cap \langle f \rangle) \cdot f^{-1}$$

が成り立つ．よって，$S_0 = \{a \in \overline{K}^m \mid \phi_a(f) = 0\}$ とし，
$\mathcal{G} = \{(S_1, G_1), \ldots, (S_l, G_l)\}$ を $(I, \langle f \rangle)$ に関する共通部分の包括的グレブナー基底系とすると，

$$\{(S_0, \{0\}), (S_1 \setminus S_0, G_1), \ldots, (S_l \setminus S_0, G_l)\}$$

は $(I, \langle f \rangle)$ に関するイデアル商の包括的グレブナー基底系である．
$J = \langle f_1, \ldots, f_s \rangle$ に対し，

$$I : J = (I : \langle f_1 \rangle) \cap \cdots \cap (I : \langle f_s \rangle)$$

が成り立つため，$I : J$ の包括的グレブナー基底系も同様に計算できる．

Overview of Slides

目標：パラメータを含むイデアルの準素分解を包括的に計算する

I : $K[A,X]$ のイデアル（$A=\{a_1,\dots,a_m\}$）．次の 2 つの条件を満たす $(\mathbb{A}_1,\mathcal{Q}_1),\dots,(\mathbb{A}_l,\mathcal{Q}_l)$ を計算する．

1. $\mathbb{A}_1\cup\cdots\cup\mathbb{A}_l=K^m$
2. 各 i に対し，任意の点 $a_i\in\mathbb{A}_i$ に対し，$\phi_a(\mathcal{Q}_i)$ は $\phi_a(I)$ の準素イデアル分解

可能であるならば，$\mathbb{A}_1,\dots,\mathbb{A}_l$ は構成的集合（$V(J_1)\setminus V(J_2)$）．

Remark

$\phi_a : K[A,X]\to K[X]$ は a を代入する写像で，$\phi_a(\mathcal{Q}_i)=\{\phi_a(Q)\mid Q\in\mathcal{Q}_i\}$

Example

$I=\langle(ax+1)y\rangle\subset K[a,x,y]$.

- $\mathbb{A}_1=K^2\setminus V(a)$, $\mathcal{Q}_1=\{\langle ax+1\rangle,\langle y\rangle\}$
- $\mathbb{A}_2=V(a)$, $\mathcal{Q}_2=\{\langle y\rangle\}$

問題点：一般には解決できないと思われる

$\mathbb{A}_1,\dots,\mathbb{A}_l$ が構成的集合で書けるとは限らない

Example

$I=\langle x^2-a\rangle\subset\mathbb{Q}[a,x]$.

- $\mathbb{A}_1=\{a\in\mathbb{Q}\mid a$ は正の平方数 $\}$, $\mathcal{Q}_1=\{\langle x+\sqrt{a}\rangle,\langle x-\sqrt{a}\rangle\}$
- $\mathbb{A}_2=\{a\in\mathbb{Q}\mid a$ は正の平方数でない $\}$, $\mathcal{Q}_2=\{\langle x^2-a\rangle\}$

解決策：目標 (2) の「任意の」の条件を緩めて「実行可能」な分解を考える

I : $K[A,X]$ のイデアル．次の 2 つの条件を満たす $(\mathbb{A}_1,\mathcal{Q}_1),\dots,(\mathbb{A}_l,\mathcal{Q}_l)$ を計算する．

1. $\mathbb{A}_1\cup\cdots\cup\mathbb{A}_l=K^m$
2. 各 i に対し，ほとんどの $a_i\in\mathbb{A}_i$ に対し，$\phi_a(\mathcal{Q}_i)$ は $\phi_a(I)$ の準素イデアル分解

$\Longrightarrow$ 上記の分解を feasible decomposition と呼ぶことにする．

Definition (Zariski-feasible decomposition)

I : $K[A,X]$ のイデアル．$\mathbb{A}_1,\dots,\mathbb{A}_l\subset K^m$, $\mathcal{Q}_i$: イデアルの有限集合．$(\mathbb{A}_1,\mathcal{Q}_1),\dots,(\mathbb{A}_l,\mathcal{Q}_l)$ は次の 2 つの条件を満たすとき，I の Zariski-feasible decomposition と呼ぶことにする．

1. $\mathbb{A}_1\cup\cdots\cup\mathbb{A}_l=K^m$
2. 各 i に対し，$\mathbb{A}_i$ の Zariski-dense な部分集合 $\mathbb{O}_i$ が存在して，任意の $a_i\in\mathbb{O}_i$ に対し，$\phi_a(\mathcal{Q}_i)$ は $\phi_a(I)$ の準素イデアル分解
3. $\mathbb{A}_1,\dots,\mathbb{A}_l$ は構成的集合

Example

$I=\langle x^2-a\rangle\subset\mathbb{Q}[a,x]$.

- $\mathbb{A}_1=\mathbb{Q}$, $\mathcal{Q}_1=\{\langle x^2-a\rangle\}$, $\mathbb{O}_1=\{a\in\mathbb{Q}\mid a$ は正の平方数でない $\}$

Zariski-feasible decomposition の存在はヒルベルトの既約性定理から保証される（と思われる）

Theorem (ヒルベルトの既約性定理 (1892))

既約多項式 $f(A,X)\in\mathbb{Q}[A,X]$ を既約多項式とすると，ある無限個の $a\in\mathbb{Q}^r$ に対して，$f(a,X)$ は既約多項式となる．特に，*Zariski-dense* な集合 $\mathcal{O}\subset\mathbb{Q}^r$ の任意の元 a に対し，$f(a,X)$ は既約となる．

Corollary

P: $\mathbb{Q}[A,X]$ の素イデアル．*Zariski-dense* な集合 $\mathcal{O}\subset\mathbb{Q}^r$ が存在して，任意の元 $a\in\mathcal{O}$ に対し，$\phi_a(P)$ は $K[X]$ の素イデアル．

Corollary

P: $\mathbb{Q}[A,X]$ の準素イデアル．*Zariski-dense* な集合 $\mathcal{O}\subset\mathbb{Q}^r$ が存在して，任意の元 $a\in\mathcal{O}$ に対し，$\phi_a(P)$ は $K[X]$ の準素イデアル．

包括的グレブナー基底系 (CGS) を用いて Zariski-feasible decomposition を計算することを考える

準素分解の定義

Definition

I: イデアル．イデアルの有限集合 $\{Q_1, \dots, Q_s\}$ は次の条件を満たすとき，I の準素イデアル分解と呼ばれる．

1. 各 Q_i は準素イデアル．
2. $I = Q_1 \cap \cdots \cap Q_s$

さらに，次の条件を満たすとき，I の最短準素イデアル分解と呼ばれる

3. $\sqrt{Q_i} \neq \sqrt{Q_j}$ $(i \neq j)$
4. $\bigcap_{j \neq i} Q_j \not\subset Q_i$

$\Longrightarrow$ a を代入したときに，上記の 4 つの条件を満たすか確認することが重要

それぞれの条件の対処法

1. 各 Q_i は準素イデアル $\Longrightarrow$ ヒルベルトの既約性定理．
2. $I = Q_1 \cap \cdots \cap Q_s$ $\Longrightarrow$ 共通部分に関する CGS
3. $\sqrt{Q_i} \neq \sqrt{Q_j}$ $(i \neq j)$ $\Longrightarrow$ 包含関係に関する CGS
4. $\bigcap_{j \neq i} Q_j \not\subset Q_i$ $\Longrightarrow$ 包含関係に関する CGS

$\mathcal{Q}$ を I の最短準素分解とすると，$\phi_a(\mathcal{Q})$ が $\phi_a(I)$ の最短準素分解になるためには，次の 4 つの条件を満たさなければならない．

1. 各 $\phi_a(Q_i)$ は準素イデアル
2. $\phi_a(I) = \phi_a(Q_1) \cap \cdots \cap \phi_a(Q_s)$ $\Longrightarrow$ 共通部分に関する CGS
3. $\sqrt{\phi_a(Q_i)} \neq \sqrt{\phi_a(Q_j)}$ $(i \neq j)$ $\Longrightarrow$ 根基に関する CGS
4. $\bigcap_{j \neq i} \phi_a(Q_j) \not\subset \phi_a(Q_i)$ $\Longrightarrow$ 共通部分と包含関係に関する CGS

Remark

上の 4 つの条件がそれぞれ独立に成り立たないような例が作れる

共通部分と代入

一般に，

$$\phi_a(I \cap J) \subset \phi_a(I) \cap \phi_a(J)$$

であるが，逆の包含は成り立つとは限らない．新しい変数を t として，イデアル

$$F(t) = tI + (1-t)J \subset K[t, A, X]$$

のブロック順序 $t \gg X >\gg A$ のグレブナー基底を $G(t)$ とし，$G(t)$ の各元の $K(A)[t, X]$ における先頭係数の積を $h = \prod_{f \in G(t)} \mathrm{lc}(f)$ とする．また，$\mathbb{A} = K^m \setminus V(h)$ とする．このとき，任意の元 $a \in \mathbb{A}$ に対し，

$$\phi_a(I \cap J) = \phi_a(I) \cap \phi_a(J)$$

が成り立つ．

Proposition

I: イデアル，$Q_1, \dots, Q_s$: I の準素分解．このとき，ある多項式 $h \neq 0$ が存在して，任意の元 $a \in K^m \setminus V(h)$ に対し，

$$\phi_a(I) = \phi_a(Q_1) \cap \cdots \cap \phi_a(Q_s).$$

Proof.

新しい変数を $T = \{t_1, \dots, t_s\}$ として，イデアル

$$F(T) = t_1 Q_1 + t_2 Q_2 + \cdots + t_s Q_s + \langle t_1 + t_2 + \cdots + t_s - 1 \rangle \subset K[T, A, X]$$

のブロック順序 $T \gg X \gg A$ のグレブナー基底を $G(T)$ とし，$G(T)$ の各元の $K(A)[T, X]$ における先頭係数の積を $h = \prod_{f \in G(t)} \mathrm{lc}(f)$ とする．また，$\mathbb{A} = K^m \setminus V(h)$ とする．このとき，任意の元 $a \in \mathbb{A}$ に対し，

$$\phi_a(I) = \phi_a(Q_1) \cap \cdots \cap \phi_a(Q_s)$$

が成り立つ．

$\square$

包含関係と代入

一般に，

$$I \not\subset J \implies \phi_a(I) \not\subset \phi_a(J)$$

は成り立つとは限らない．$I \not\subset J$ とし，J の $X \gg A$ に関するグレブナー基底を G とする．$I = \langle f_1, \dots, f_m \rangle$ に対し，$f_i \notin J$ を満たす f_i を G で割った余りを r_i とし，各 r_i の $K(A)[T, X]$ における先頭係数の積を $h = \prod \mathrm{lc}(r_i)$ とする．また，$\mathbb{A} = K^m \setminus V(h)$ とする．このとき，任意の元 $a \in \mathbb{A}$ に対し，

$$\phi_a(I) \not\subset \phi_a(J)$$

が成り立つ．

Proposition

I: イデアル，$\{Q_1, \dots, Q_s\}$: I の準素分解．このとき，ある多項式 $h \neq 0$ が存在して，任意の元 $a \in K^m \setminus V(h)$ に対し，

2. $\phi_a(I) = \phi_a(Q_1) \cap \dots \cap \phi_a(Q_s)$
3. $\sqrt{\phi_a(Q_i)} \neq \sqrt{\phi_a(Q_j)}$ $(i \neq j)$
4. $\bigcap_{j \neq i} \phi_a(Q_j) \not\subset \phi_a(Q_i)$

が成り立つ．また，$K^m \setminus V(h)$ のある *Zariski-dense* な集合 $\mathbb{O}$ が存在して，任意の元 $a \in \mathbb{O} \subset K^m \setminus V(h)$ に対し，$\{\phi_a(Q_1), \dots, \phi_a(Q_s)\}$ は $\phi_a(I)$ の最短準素分解となる．

Remark

$I + \langle h \rangle$ に繰り返し適用していけば，*Zariski-feasible decomposition* が計算できる．

アルゴリズム

入力：イデアル $I \subset \mathbb{Q}[A, X]$
出力：I の Zariski-feasible decomposition

1. $J \leftarrow I$, $\mathbb{B} \leftarrow \mathbb{Q}^m$, $i \leftarrow 1$
2. J の最短準素分解を $\mathcal{Q}_i$ とする．$i \geq 2$ のとき，
   $\mathbb{B} \leftarrow \mathbb{Q}^m \setminus (\mathbb{A}_1 \cup \dots \cup \mathbb{A}_{i-1})$ とする．
3. 次を満たす多項式 h を計算；「任意の $a \in \mathbb{B} \setminus V(h)$ に対し，$\phi_a(\mathcal{Q}_i)$ は $\phi_a(J)$ に対し，最短準素分解の条件 (2)-(4) を満たす.」
   また，$\mathbb{A}_i \leftarrow \mathbb{B} \setminus V(h)$ とする．
4. $h \in J$ の場合には，$\{(\mathbb{A}_1, \mathcal{Q}_1), \dots, (\mathbb{A}_s, \mathcal{Q}_s)\}$ を返す．そうでない場合には，$J \leftarrow J + \langle h \rangle$，$i \leftarrow i + 1$ として，2 に戻る．

まとめ

まとめ

- いくつかのパラメータ付きのイデアル操作のアルゴリズムを紹介
- $\mathbb{Q}$ 上のパラメータ付き準素分解を計算できる範囲で定義
- 包括的グレブナー基底系の理論を応用してアルゴリズムを考案

今度の課題

- パラメータ準素分解の良い応用を見つける
- 実数の範囲でのパラメータ準素分解を考える