多変数多項式のパラメトリック因数分解

Parametric Factorization of Multi-variate Polynomials

横山 和弘
立教大学理学部

目的

本研究は多項式イデアルのパラメトリック (準素) 分解を最終目的とする. これは通常の準素分解をパラメータ付きの場合に拡張するもので, 以下のステップを考えることになる.

- パラメトリック最小多項式: パラメトリックイデアルのグレブナー基底に関する各 cell 上で, 定した変数の最小多項式を計算する.
- パラメトリック根基分解:
  $\Leftrightarrow$ パラメトリック最小多項式のパラメトリック無平方分解
  $\Leftrightarrow$ パラメトリック多項式のパラメトリック GCD 計算
- パラメトリック斉次分解:
  $\Leftrightarrow$ パラメトリックイデアルのパラメトリック飽和商イデアル計算
- パラメトリック既約分解/パラメトリック素 (準素) 分解:
  $\Leftrightarrow$ 一般の位置にあるパラメトリック多項式のパラメトリック因数分解

パラメトリック多項式のパラメトリック因数分解法
ICMS 2006 で提案した素朴法 (Naive Method) を発展させ, 完全なアルゴリズムとする

簡単な例による素朴法の紹介

$f(x,y) = x^2 - y^2 - ay - a$, ここで x, y は通常の変数で a はパラメーターとする. $a = 0$ または $a = 4$ のときに限り $f(x,y)$ は $\mathbb{Q}$ 上で可約である. これは以下のように示すことができる.

- 変数 $b_2, b_2, b_0, c_2, c_1, c_0$ を導入して, $f(x)$ が 1 次式の積になる因数分解を考える.

$$f(x,y) = (x + b_2y^2 + b_1y + b_0)(x + c_2y^2 + c_1y + c_0).$$

これより, a, $b_2, b_1, b_0, c_2, c_1, c_0$ を変数とする連立代数方程式が得られる.

$$\begin{cases} b_2 + c_2 = 0 & (xy^2\text{の係数}) \\ b_1 + c_1 = 0 & (xy\text{ の係数}) \\ b_0 + c_0 = 0 & (x\text{ の係数}) \\ b_2c_2 = 0 & (y^4\text{の係数}) \\ b_2c_1 + b_1c_2 = 0 & y^3(\text{の係数}) \\ b_2c_0 + b_1b_1 + b_0c_2 + 1 = 0 & y^2(\text{の係数}) \\ a + b_1c_0 + b_0c_1 = 0 & y(\text{の係数}) \\ a + b_0c_0 = 0 & (\text{定数項}) \end{cases}$$

- 導出された連立代数方程式を解くことで, 変数 $b_2, b_1, b_0, c_2, c_1, c_0$ を含まない a だけの式が計算される.

$$a^2 - 4a = 0.$$

- 結果として, $a \neq 0, 4$ のときは $f(x,y)$ は $\mathbb{Q}$ (さらには $\mathbb{Q}$ の代数閉包) 上で既約となる.
  また, $a = 0, 4$ のときはそれぞれ以下のように因数分解される.

$$\begin{aligned} f(x,y) &= x^2 - y^2 = (x-y)(x+y) \\ f(x,y) &= x^2 - y^2 - 4y - 4 = (x-y-2)(x+y+2) \end{aligned}$$

- 実際, 連立代数方程式において, 対応するイデアルのグレブナー基底を消去順序 $a \prec\prec \{b_2, b_1, b_0, c_2, c_1, c_0\}$ で計算することで a だけの制約式を計算することができる. (消去イデアル計算になっている.)

パラメトリック因数分解の設定を与える．このような設定に変換するには，パラメトリックイデアルの逐次構成法を適用すればよい．

設定

- $A = \{a_1, \ldots, a_m\}$ をパラメーターの集合，$X = \{x_1, \ldots, x_n\}$ を変数の集合とする．また，K を体とし，$\overline{K}$ をその代数閉包とする．
- パラメトリック多項式 $f(A, X)$ に対して，ある $z \in X$ を選んで主変数とし，$f(A, X)$ を変数を z とする $K[A, Y]$ 上の多項式と考える．ここで $Y \subset X \setminus \{z\}$ である．(Y は空でもよい.) 簡単のために $f(A, X)$ を $f(z)$ と表す．
- 簡単のために，$f(z) = f(A, X)$ は $K[A, X]$ 上で既約とし，$f(z)$ は変数 z に関してモニックとする．

以下では，素朴法を一般の形で説明する．そこで，
$f(z) = z^d + f_{d-1}(A, Y)z^{d-1} + \cdots + f_0(A, Y)$, $Y = \{y_1, \ldots, y_r\}$, とする．

素朴法の概要

- 以下の因数分解を考える．(既約分解でなくてよい)

$$f(z) = g_1(z) \cdots g_s(z), \tag{1}$$

- 各因子 $g_1(z), \ldots, g_s(z)$ の係数をすべて独立な変数 $b^{(1)}_{d_1-1,e_{D_1,\ldots,D_r}}$, $\ldots$, $b^{(1)}_{0,e_{0,\ldots,0}}, \ldots, b^{(s)}_{d_s-1,e_{D_1,\ldots,D_r}}, \ldots, b^{(s)}_{0,e_{0,\ldots,0}}$ に置き換える．すなわち，

$$\begin{cases} g_1(z) &= z^{d_1} + \sum_{k<d_1, i_1 \le D_1, \ldots, i_r \le D_r} b^{(1)}_{k,e_{i_1,\ldots,i_r}} y_1^{i_1} \cdots y_r^{i_r} z^k \\ g_2(z) &= z^{d_2} + \sum_{k<d_2, i_1 \le D_1, \ldots, i_r \le D_r} b^{(2)}_{k,e_{i_1,\ldots,i_r}} y_1^{i_1} \cdots y_r^{i_r} z^k \\ \vdots & \qquad\qquad \vdots \\ g_s(z) &= z^{d_s} + \sum_{k<d_s, i_1 \le D_1, \ldots, i_r \le D_r} b^{(s)}_{k,e_{i_1,\ldots,i_r}} y_1^{i_1} \cdots y_r^{i_r} z^k, \end{cases}$$

である．ここで $d_1 + \cdots + d_s = d$, $D_j = \deg_{y_j}(f)$ である．以下では，次数のリスト $\mathbf{d} = (d_1, \ldots, d_s)$ を因数分解の型と呼ぶことにする．

- 分解イデアル: 等式 (1) をパラメータ係数の多項式に置き換えることで，連立代数方程式が得られる．これに対応する多項式環 $K[A, B]$ のイデアルを $\mathcal{J}_{\mathbf{d}}$ とおく．ここで，B は導入されたパラメーターの集合とする．このイデアル $\mathcal{J}_{\mathbf{d}}$ をここでは，因数分解の型 $\mathbf{d}$ の分解イデアルと呼ぶ．
- 分解イデアルの非自明性: 因数分解 (1) が実現可能かどうかはイデアル $\mathcal{J}_{\mathbf{d}}$ が自明でないかどうかと同値である．よって，これより，パラメーター A に関する制約式を得ることができる．
  ここで，イデアルが自明でないことは，代数閉包上で (A, B) に関する解が存在することである．よって，可能な因数分解 (1) は基本的には代数閉体上の分解に対応することになる．
- 消去イデアルによる制約条件の導出: 消去イデアル $\mathcal{E}_{\mathbf{d}} = K[A] \cap \mathcal{J}_{\mathbf{d}}$ が自明でないときには，消去定理を用いることで，消去イデアルのグレブナー基底 G_A がパラメーター A の本質的な条件を与える．
  得られた条件の正当性は，$f(A, X)$ と G_A で生成されるイデアルの素分解を計算することで確認できる．

消去イデアル $\mathcal{E}_{\mathbf{d}} = K[A] \cap J_{\mathbf{d}}$ が自明の場合を考えよう．例えば，f が 2 変数 (重み付き) 斉次多項式の場合には，f はどのようなパラメータの値でも，$\overline{K}$ 上で 1 次式の積に分解される．(例 3 を参照.)

このような場合には，別の方法でパラメトリック因数分解を記述することになる．(例 7 を参照.)

例 1 (1 パラメーターの典型例)

$K=\mathbb{Q}$, $A=\{a\}$, $X=\{z,y\}$ とし, f を以下とする.

$$\begin{aligned} f &= x^4+(-y^2+y)x^3+(-y^3+3y^2+y+a^2-4)x^2+(-y^4+2y^3 \\ &\quad +(-a^2+a+1)y^2-3y-a+1)x-y^5+y^4+(a^2-a+3)y^3 \\ &\quad +(a-3)y^2-2y+a^2-2a+2. \end{aligned}$$

調べる因数分解の型は $(1,3),(2,2),(1,1,2),(1,1,1,1)$ である.

- 型 $(1,3)$: 分解イデアル $\mathcal{J}_{(1,3)}$ の項順序 $a \prec\prec B$ に対するグレブナー基底は $\{a,(b_{0,0}^{(1)})^2-b_{0,0}^{(1)}-2,b_{0,0}^{(1)}+3b_{0,1}^{(1)}-2,\ldots\}$.
  となる. よって, $a=0$ が型 $(1,3)$ を実現するための条件となる.
- 型 $(2,2)$: 分解イデアル $\mathcal{J}_{(1,3)}$ の項順序 $a \prec\prec B$ に対するグレブナー基底は $\{a^2-a,(b_{0,0}^{(1)}+1)a,(b_{0,0}^{(1)})^2+3b_{0,0}^{(1)}+2,\ldots\}$
  となる. よって, $a=0,1$ のときに, f が 2 つの 2 次因子に分解される.
- 型 $(1,1,2)$: 型 $(1,3)$ と型 $(2,2)$ の条件を合わせると, $a=0$ は型 $(1,1,2)$ を実現するための条件である. 型 $(1,1,1,1)$ は起こり得ない.

例 2 (2 パラメーターの例)

$K=\mathbb{Q}$, $A=\{a_1,a_2\}$, $X=\{z,y\}$ とし,

$$f=x^3+(-y^2+a_1y+a_2)x^2-a_1y^2x+a_1y^4-a_1^2y^3-a_2y^2.$$

とする. 可能な因数分解の型は $(3),(1,2),(1,1,1)$ である.

型 $(1,3)$ に対する分解イデアル $\mathcal{J}_{1,3}$ のグレブナー基底は以下となる.

$$\{a_2a_1^2-a_2a_1,(a_2^3+a_2^2)a_1-a_2^3-a_2^2,b_{0,0}^{(1)}a_1^3-b_{0,0}^{(1)}a_1^2,\ldots\}$$

このとき消去イデアルは非自明で

$$\mathcal{E}_{(1,3)}=\langle a_2a_1^2-a_2a_1,(a_2^3+a_2^2)a-a_2^3-a_2^2\rangle$$

となり, 素因子は $\langle a_1-1\rangle,\langle a_2\rangle,\langle a_1,a_2+1\rangle$ である. よって, $a_1=1$, $a_2=0$ または $a_1=0\wedge a_2=-1$ のときに f は 1 次因子を持つ.

$$f(z)=\begin{cases}(x-y)(x+y)(x-y^2+y+a_2) & (a_1=1 \text{ のとき})\\ (x-y^2+a_1y)(x^2-a_1y^2) & (a_2=0 \text{ のとき})\\ (x-1)(x^2-y^2x-y^2) & ((a_1,a_2)=(0,-1) \text{ のとき})\end{cases}$$

2 番目の場合に因子に a_1 が現れるので, 型 $(1,1,1)$ のチェックが必要になる. (2 番目の因子 $x^2-a_1y^2$ は斉次である.)

例 3 (斉次の例)

例 2 の因子 x^2-ay^2 を考える. 型 $(1,1)$ に対して, 分解イデアル $\mathcal{J}_{1,1}$ の項順序 $a \prec\prec B$ に関するグレブナー基底は以下となる.

$$\{b_{0,0}^{(1)}a,(b_{0,2}^{(1)})^2,-b_{0,1}^{(1)}-b_{0,1}^{(2)},\ldots\}$$

このとき, 分解イデアルは唯一の孤立素因子 P を持ち, グレブナー基底は以下となる.

$$\{a-(b_{0,1}^{(2)})^2,b_{0,0}^{(1)},b_{0,0}^{(2)},b_{0,1}^{(1)}+b_{0,1}^{(2)},b_{0,2}^{(1)},b_{0,2}^{(2)}\}$$

よって, P は $\{b_{0,1}^{(2)}\}$ を MIS に持ち, a はその多項式 $(b_{0,1}^{(2)})^2$ として表される. ($\{a\}$ も MIS である.)

すなわち, $\mathbb{Q}$ 上で因数分解の型 $(1,1)$ を実現する a の値は $\{c^2\mid c\in\mathbb{Q}\}$ である.

実際, f において a に c^2 を代入することで (c は $\mathbb{Q}$ を動く), $f(c^2,x,y)$ は $\mathbb{Q}$ 上で 2 個の 1 次因子 $x-cy,x+cy$ に分解される.

1 個のパラメーターを持つ場合

パラメトリック因数分解の完全なアルゴリズムを構成するための第一歩として, 最も基本となる, 2 変数 z,y で 1 個のパラメーター a を考える.

注意 4 (2 変数への帰着)

効果的/実際的ヒルベルトの既約定理 (Kaltofen,1985) により, 3 変数以上の多項式の既約性判定は 2 変数多項式の既約性判定に帰着される.

$\Rightarrow$ 元の因数分解は 2 変数への帰着したときの因数分解になる. (さらなる分解になる可能性もある)

以下ではパラメトリック多項式 $f(a,z,y)$ は $K[a,z,y]$ 内で既約であり, 主変数 z に関してモニックとする. また, 因数分解の型として $\mathbf{d}=(d_1,\ldots,d_s)$ を考える.

自明でない消去イデアルの存在には, 絶対既約性が必要となる.

定義 5 (絶対既約性)

パラメトリック多項式 $f(a,z,y)$ は $K[a,z,y]$ で既約であり, 主変数 z に関してモニックとする. $f(a,z,y)$ が絶対既約であるとは, $f(a,z,y)$ が a を変数とする有理関数体 $K(a)$ の任意の有限次拡大上で既約であるときにいう.

上記の絶対既約性の判定法として Kaltofen (1983) によるものがある.
(ここでは係数体を $K(a)$ として適用している.)
以下では, 簡単のため $f(a,z,y)$ は定義 5 のものとする.

絶対既約性判定法

ある $\beta \in K$ に対して, $f(a,z,\beta)$ は無平方であり, その K 上の既約因子を $g_1,\ldots,g_s$ とする. このとき, $f(a,z,y)$ が絶対既約であることの必要十分条件は, $f(a,z,y)$ は各拡大体 $K(a)[w]/\langle g_i(a,w)\rangle$, $(i=1,\ldots,s)$, 上で既約であることである.

絶対既約な場合には完全なパラメトリック因数分解が実現される.

定理 6 (絶対既約の場合のパラメトリック分解)

$f(a,z,y)$ は絶対既約かつモニックなパラメトリック多項式とする. f の分解の型 $\mathbf{d}=(d_1,\ldots,d_s)$ に対する分解イデアル $\mathcal{J}_\mathbf{d}$ が自明でないとき以下が成り立つ.

- $\mathcal{J}_\mathbf{d}$ は 0 次元であり, その零点集合 $V_{\overline{K}}(J_\mathbf{d})$ は有限集合である.
- 消去イデアル $\mathcal{E}_\mathbf{d}=K[a]\cap\mathcal{J}_\mathbf{d}$ は自明でない.
- 各零点 ($V_K(\mathcal{E}_\mathbf{d})$ の元) から因数分解の型を実現するパラメーター a の K 上の値をすべて求めることができる.

- 分解イデアルが自明であれば, いかなる $\overline{K}$ での a の値に対しても $f(a,z,y)$ は既約である.
- 分解イデアルが自明でない場合には, 有限個の a の値を除いて $f(a,z,y)$ は $\overline{K}$ 上で既約である. すなわち, K 上でも既約である.

絶対既約でない場合

$f(a,z,y)$ が絶対既約でなく, 因数分解の型 $\mathbf{d}$ に対する分解イデアル $\mathcal{J}_\mathbf{d}$ が自明でない場合には以下が成り立つ.

- 消去イデアル $\mathcal{E}_\mathbf{d}$ は自明となり, その Zariski 閉包は $\overline{K}$ となる.
- この場合に a の満たすべき代数制約式はない.

一方, $\mathcal{J}_\mathbf{d}$ の $K[a,B]$ における素因子を計算すれば, 以下となる.

- 0 次元でない素因子 P は 1 次元であり, その MIS を B の元からとることができる. そこで MIS を $\{b\}$ とすれば, $K(b)[\{a\}\cup B\setminus\{b\}]$ における P の拡大イデアル P^e は 0 次元である.
- よって, a は $K(b)$ 上で代数的となり, a は代数関数として表される. とくに, 幸運な場合には b の有理関数として表される.
- この代数関数表現や有理関数表現を a の値と考えることもできる.
  $\Rightarrow$ これを使ってパラメトリック因数分解を定式化できる.

例 7 (絶対既約でない例)

$f(a,z,y)=(z-y+1)^3+a(z-y+a)$ に対して, $y=0$ とすると,

$$g(a,z)=f(a,z,0)=z^3+3z^2+(a+3)z+a^2+1$$

である. $g(a,z)$ は $\mathbb{Q}$ 上既約であるので, $\mathbb{Q}(a)$ 上で既約である. しかし, $f(a,z,y)$ は $\mathbb{Q}(a)[w]/\langle g(a,w)\rangle$ 上で可約となる. 実際, イデアル $\langle f(a,x,y),g(a,w)\rangle$ の素分解計算より, 以下の分解が得られる.

$$\begin{aligned} f(a,z,y) \equiv\ & (z-y-w)(z^2+(-2y+w+3)z+y^2+(-w-3)y \\ & +w^2+3w+a+3) \pmod{w^3+3w^2+(a+3)z+a^2+1} \end{aligned}$$

以下が型 $(1,3)$ に対する分解イデアル $\mathcal{J}_{(1,3)}$ のグレブナー基底となる.

$$\{a^2-b_{0,0}^{(1)}a-(b_{0,0}^{(1)})^3+3(b_{0,0}^{(1)})^2-3b_{0,0}^{(1)}+1,\ -a-(b_{0,0}^{(1)})^2+3b_{0,0}^{(1)}+b_{0,0}^{(2)}-3,\ldots\}$$

分解イデアルは 1 個の 1 次元孤立素因子 P と 2 個の 0 次元埋没素因子を持つ. また, $b_{0,0}^{(1)}$ が P の MIS であり, a は $b_{0,0}^{(1)}$ の代数関数として表される. 具体的には $c=b_{0,0}^{(1)}$ とおくと, 以下となる.

$$a=\frac{c\pm\sqrt{4c^3-11c^2+12c-4}}{2}.$$

例 8 (1 変数の場合)

1 変数の場合として $f(a,x) = x^3 - ax^2 + (a-3)x + 1$ を考える. f は位数 3 の巡回群をガロア群に持つ generic 多項式である.

因数分解の型 $(1,2)$ に対して, 分解イデアル $\mathcal{J}_{1,2}$ は唯一の孤立素因子 P を持ち, 以下のグレブナー基底を持つ.

$$\{((b_0^{(1)})^2+b_0^{(1)})a+(b_0^{(1)})^3-3b_0^{(1)}-1, (b_0^{(1)}+1)a+(b_0^{(1)})^2+b_0^{(2)}+3, a+b_0^{(1)}+b_1^{(2)}\}$$

ここで, P は $\{b_0^{(1)}\}$ を MIS として持ち, $\mathbb{Q}(b_0^{(1)})[a, b_0^{(2)}, b_1^{(2)}, b_0^{(2)}]$ での拡大イデアル P^e も同じグレブナー基底を持つ.

よって, a は $b_0^{(1)} \neq 0, -1$ の場合には, $b_0^{(1)}$ の有理関数

$$\frac{-(b_0^{(1)})^3 + 3b_0^{(1)} + 1}{(b_0^{(1)})^2 + b_0^{(1)})}$$

として表される. 実際, f において a に $\frac{-c^3+3c+1}{c^2+c}$ を代入すると f は $\mathbb{Q}$ 上で 3 個の 1 次因子 $x+c$, $x-1-\frac{1}{c}$, $x-\frac{1}{c+1}$ の積に分解される. ここで c は $\mathbb{Q} \setminus \{0,-1\}$ を動くものとする.

効率的なアルゴリズムのために因数分解の型に注目する.

定義 9 (原始的な型)

因数分解の型 $\mathbf{d} = (d_1, \ldots, d_s)$ が原始的であるとは, $\mathbf{d}$ の細分となる因数分解の型が存在しないときにいう.

注意 10

固定した次数 d に対して, 原始的な型は以下となる.

$$(1,d-1),(2,d-2),\ldots,\left(\frac{d-1}{2},\frac{d+1}{2}\right) \quad (d \text{ が奇数の場合})$$

$$(1,d-1),(2,d-2),\ldots,\left(\frac{d}{2},\frac{d}{2}\right) \quad (d \text{ が偶数の場合})$$

原始的な型についてそれを実現するパラメータ値を求めれば, それらより, すべての型について実現するパラメーター値がわかることに注意する.

K 上のパラメトリック因数分解アルゴリズム

入力: パラメトリック多項式 $f(a,z,y)$, ただし $f(a,z,y)$ は絶対既約かつ z に関してモニックである.

(1) $f(a,z,y)$ の z に関する次数に対する原始的な型を生成する.

(2) 各原始的な型 $\mathbf{d}$ に対して, 分解イデアル $J_{\mathbf{d}}$ を計算する.

(i) $J_{\mathbf{d}}$ が自明でないとき:
- 消去イデアル $\mathcal{E}_{\mathbf{d}} = K[a] \cap J_{\mathbf{d}}$ を計算する.
- $\mathcal{E}_{\mathbf{d}}$ の生成元 $g(a)$ の K 上の根を計算する.
- $g(a)$ の各根 α に対して, $f(\alpha,z,y)$ を K 上で因数分解する.

(ii) $J_{\mathbf{d}}$ が自明なとき: 型 $\mathbf{d}$ を実現する a の値は存在しない.

(3) 原始的な型を実現するパラメーター値における因数分解の結果を統合する.

むすび

Yokoyama (2006) の続きとして, そこで提案された素朴法に基づく完全なパラメトリック因数分解アルゴリズの実現に向けての進捗を報告した.

要点 11 (素朴法に関する理論的結果について)

- パラメーターが 1 個の場合には因数分解するパラメトリック多項式が絶対既約であれば, 各因数分解の型に対して, それを実現するパラメーターの値をすべて求めることができることが明らかになった.
- パラメトリック多項式が絶対既約でないときには, 因数分解の型を実現するパラメーター値の表し方を代数関数を使うことで可能である.
  $\Rightarrow$ この表し方が実際的であるかどうかは次の研究課題である.

要点 12 (素朴法の実際性について)

- パラメトリック多項式の因数分解については, 標準的なテスト用のものがないので, 計算機実験はスナップショットにすぎない.
- ランダムなパラメトリック多項式は分解イデアルがほぼ自明になる. 実験の多項式は作為的に作成したものを使った.
- 次数が小さい場合には素朴法で計算ができている.
- 素朴法の効率性は分解イデアルのグレブナー基底計算の効率性に依存している.
- 素朴法における追加の変数 B の個数は $O(d_x d_y)$ である. (ここで d_x, d_y はそれぞれ多項式の x 次数と y 次数を表す.)
  計算の効率化には不要な変数を削る等の改良が必要である.
- 実際性においては, 入力多項式が疎であることも重要と思われる.

ご清聴をありがとうございます.