数理解析研究所講究録 1395 巻 2004 年 126-131

代数幾何的な多変数多項式既約証明アルゴリズム

ベック和穂エリック*
東京大学情報理工学系研究科コンピュータ科学専攻
KAZUHO ERIK BECK
DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF TOKYO

Abstract

Shuhong Gao[1] により多面体論を用いた多変数多項式の既約証明アルゴリズムが考案され、多変数多項式因数分解の前処理に有効なアルゴリズムとして注目されている。ここではこれとは別に代数幾何学の定理を応用した、多項式が既約であるための十分条件を求め、それを用いた既約証明アルゴリズムを提案する。また、このアルゴリズムと [1] との簡単な比較もした。主定理からいくつかの系が導けるのでそれについても紹介する。

1 問題

K を任意の体とし、$f \in K[X_1, \cdots, X_n]$ とする。係数を K の代数閉包 $\overline{K}$ に拡張しても $f \in \overline{K}[X_1, X_2, \cdots, X_n]$ が既約であるとき f は絶対既約である、という。

問題 1 (絶対既約証明)
与えられた $f \in K[X_1, X_2, \cdots, X_n]$ は絶対既約か？

Gao は [1] において多項式の Newton 多面体を用いて多変数多項式が絶対既約であるための十分条件を与え、因数分解の前処理として定評を得ている [3]。ここでは代数幾何の定理を用い、新しい既約証明アルゴリズムを提案する。このアルゴリズムによって既約証明ができる多項式の中には Gao の方法での既約証明はできない多項式もある。

1.1 notation

今後、$f \in K[X_1, X_2, \cdots, X_n]$ を X_0 により斉次化し、$K[X_0, \cdots, X_n]$ の中での分解を考える。$K[X_0, \cdots, X_n]$ の定数でない斉次多項式の全体を $K[X_0, \cdots, X_n]_{hom}$ と書くことにする。

$\mathbb{P}^n$ を $\overline{K}$ 係数の n 次元射影空間、$V(f_1, f_2, \cdots, f_r) \subseteq \mathbb{P}^n$ を斉次多項式 $f_1, f_2, \cdots, f_r \in \overline{K}[X_0, \cdots, X_n]_{hom}$ の共通零点、$Sing(f) = V(f, \frac{\partial f}{\partial X_0}, \cdots, \frac{\partial f}{\partial X_n})$ を多項式 $f \in \overline{K}[X_0, \cdots, X_n]_{hom}$ の特異点集合とする。

2 Basic Idea

この節では代数幾何の一般論を用いて多項式が絶対既約であるための十分条件を与える。引用する定理は主に次の二つである。

*ke-beck@is.s.u-tokyo.ac.jp

定理 1
$f \in K[X_0, \cdots, X_n]_{hom} \Rightarrow \dim(V(f)) = n-1$

定理 2 (Projective Dimension Theorem)
任意の代数的集合 $V, W \subset \mathbb{P}^n_K$ に対し、

$$\dim(V \cap W) \geq \dim(V) + \dim(W) - n$$

が成立し、また右辺が非負なら $V \cap W \neq \emptyset$ である。

$f, g, h \in K[X_0, \cdots, X_n]_{hom}$, $f = gh$ とする。積の微分公式

$$f' = g'h + gh'$$

より $g = h = 0 \Rightarrow f' = 0$ が全ての微分に対して成立する。
よって、$f = gh \Rightarrow Sing(f) \supset V(g, h) \Rightarrow \dim(Sing(f)) \geq \dim(V(g, h))$ であり、
定理 1,2 から $\dim(Sing(f)) \geq (n-1) + (n-1) - n = n-2$ がわかる。
この対偶を取って、

命題 3
$\dim(Sing(f)) < n-2 \Rightarrow f$ は絶対既約

さらに、定理 2 により、

定理 4 (main theorem)
$f, g_1, \cdots, g_{n-2} \in K[X_0, \cdots, X_n]_{hom}$ とする。
$Sing(f) \cap V(g_1, \cdots, g_{n-2}) = \emptyset$ ならば f は絶対既約

これをアルゴリズムの形に書き直すと、

アルゴリズム 1
入力: $f \in K[X_1, \cdots, X_n] (n \geq 2)$
出力: 既約証明に成功すれば「既約」失敗すれば「失敗」

1. f が斉次式でなければ新しい変数で斉次化、斉次式なら 1 変数少ない多項式の斉次化とみなす
2. f、f の各変数での微分、任意の $n-2$ 個の斉次多項式による連立方程式を作る
3. 方程式に解がなければ「既約」、あったら「失敗」

例 1
K を 5 以外の標数の体とすると、4 変数多項式 $f = A^5 + B^5 + C^5 + D^5 + ABC + 1$ は絶対既約である。

Proof 新たな変数による f の斉次化、その各変数による偏微分で方程式を作る。

$$\begin{aligned} \tilde{f} = A^5 + B^5 + C^5 + D^5 + E^5 + ABCE^2 &= 0 \\ f_A = 5A^4 + BCE^2 &= 0 \\ f_B = 5B^4 + ACE^2 &= 0 \\ f_C = 5C^4 + ABE^2 &= 0 \\ f_D = 5D^4 &= 0 \\ f_E = 5E^4 + 2ABCE &= 0 \end{aligned}$$

これに、自分で与えた $4-2=2$ 個の方程式、

$$B=C$$
$$D=E$$

を加えた方程式系に $(0,0,0,0,0)(\notin \mathbb{P}^4)$ 以外の解がないことから、定理 4 より証明終。

任意に取れる $n-2$ 個の多項式をこの例のように 1 次式でとっておけば、これは $n-2$ 変数への代入と等価であり、この場合連立方程式は 3 変数の斉次式のみで与えられる。従ってこのアルゴリズムは変数の多さに直接影響は受けない。

3 証明能力の検証

3.1 証明不可能な多項式の一般系

命題 5
$f=f_1^2p+f_1f_2q+f_2^2r(f_1,f_2$は定数でない多項式) の形の f に対して $\dim(Sing(f))\geq n-2$

Proof $f'=(2f_1'p+f_1p'+f_2'q+f_2q')f_1+(f_1q+2f_2'r+f_2r')f_2$ であり、$Sing(f)\supseteq V(f_1,f_2)$ よって、$\dim Sing(f)\geq \dim V(f_1,f_2)\geq n-2$

この命題によって今回のアルゴリズムでこのような多項式の既約証明を行うことはできない。Asir 内の asir2000/lib/fctrdata の因数分解テスト用多項式の既約成分で計算機実験を行ったところ、ほぼ全てが命題 5 の形であり、既約証明はできなかった。よって 3.2 節ではこのような形でない多項式の既約証明がどの程度可能か実験により検証する。

3.2 計算機実験

アルゴリズム 1 は既約であることの十分条件しか計算しない。その証明能力を見るために今回は代入を行わず、純粋に特異点の次元のみを計算することにした。特異点の次元が低い多項式のほうが既約証明がやりやすいことになる。今回は計算時間に関する考察はしていない。

アルゴリズム 1 は方程式に解がないことにより既約証明を行う。経験則では、解を持ってしまう場合は

$$(x,y,z)=(1,0,0)\Longrightarrow xy+z^2=xyz+xz^2+y^3=z^2+xy=0$$

のように方程式に現れる全ての項が 0 になってしまう場合が圧倒的で、それは 1 変数 (上の例では x) のべきだけの項が方程式のどこにも現れないことによる。そこでもともとの多項式がいくつの 1 変数のべきの項を持つかに注目し多項式を生成、その特異点の次元を計算した。表 1 は 24 個の多項式に対する実験結果である。

なるべく正確に次元を求めるため代入はできる限り行わないようにした。不等式で示してあるものは計算時間がかかり過ぎたためやむを得ずいくつかの代入を行って計算、評価したものである。時間がかかり過ぎないよう次数は 6~12、項数は 5~17 程度のものが主である。変数の数は斉次化する前のものを示し、特異点がないときは $\dim(Sing(f))=-1$ とした。ここで扱った多項式に対しては全て $n-d>3$ であり、この表は全ての多項式が既約であることを示している。また、1 変数のべきの項を多く含む多項式のほうが特異点の次元が低くなっていることも見て取れる。

表 1: 多変数多項式とその特異点の次元

多項式	F01	F02	F03	F04	F05	F06	F07	F08	F09	F10	F11	F12
変数の数 n	5	5	5	5	5	5	5	5	5	5	5	5
べきの項の数	0	0	0	0	0	3	3	3	3	3	6	6
$d = \dim(Sing(f))$	2	≤ 2	2	2	2	1	1	≤ 1	1	1	≤ 0	-1
$n-d$	3	≥ 3	3	3	3	4	4	≥ 4	4	4	≥ 5	6
多項式	F13	F14	F15	F16	F17	F18	F19	F20	F21	F22	F23	F24
変数の数 n	5	5	5	10	10	10	10	10	10	10	10	10
べきの項の数	6	6	6	0	0	0	5	5	5	11	11	11
$d = \dim(Sing(f))$	≤ 0	≤ 0	-1	≤ 7	7	≤ 7	≤ 5	4	3	≤ 2	≤ 1	0
$n-d$	≥ 5	≥ 5	6	≥ 3	3	≥ 3	≥ 5	6	7	≥ 8	≥ 9	10

4 Newton 多面体による方法との比較

現在有用といわれている既約証明アルゴリズムに Gao [1] による多項式の Newton 多面体を用いたものがある。この節ではその原理となる既約性十分条件を簡単に紹介し、定理 4 の条件との比較をする。

$f = \Sigma a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n} \in K[X_1, X_2, \cdots, X_n], (a_{i_1 \cdots i_n} \in K)$ を任意の体上の多項式とし、各単項式 $a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n}$ を $\mathbb{R}^n$ の座標 $(i_1, \cdots, i_n) \in \mathbb{Z}^n$ とみなす。

f の Newton 多面体を

$$P(f) = conv\{\{(i_1, \cdots, i_n) | a_{i_1 \cdots i_n} \neq 0\}\}$$

によって定義する。次の命題はよく知られている。

命題 6

$f = gh \in K[X_1, X_2, \cdots, X_n] \Rightarrow P(f) = P(g) + P(h)$

ただし右辺の "+" は多面体のミンコフスキー和 (ベクトルの足し算) を意味する。

定義 7

頂点の座標が全て整数であるような多面体を整多面体という

定義 8

整多面体が *indecomposable* であるとは、1 次元以上の 2 つの整多面体のミンコフスキー和として表されないことをいう

命題 9 (Newton 多面体による既約性十分条件)

$\forall X_i \not| f$ かつ $P(f)$ が *indecomposable* $\Rightarrow f$ は絶対既約

例 2

$P(X^2Y + Z^3)$ は *indecomposable* であり、$X^2Y + Z^3$ は絶対既約である。ところが $X^2Y + Z^3$ は 5 の条件を満たし、命題 3、定理 4 による既約証明はできない

例 3

例 1 で既約証明を行った $f = A^5 + B^5 + C^5 + D^5 + ABCE^2 + E^5$ は、$P(f) = P((A + B + C + D + E)^5)$ であり、Newton 多面体による方法で f の既約証明は行えない。

このように、それぞれの絶対既約のための十分条件には包含関係がなく、お互いにもう一方の方法では既約証明できない多項式のうちで既約証明可能な多項式が存在する。

例3のように全ての変数に関するべきの項を含む多項式の既約証明はNewton多面体による方法では不可能だが、3.2節で見たようにこれはアルゴリズム1がもっとも得意とする多項式である。

5 いくつかの系と拡張

この節では第2節とほぼ同様の考察により既約証明以外のいくつかの問題を解けることを見る。既約証明のときと同様、十分条件のみ計算することができる。

5.1 mod p で還元したときの既約性

問題 2

$f \in \mathbb{Q}[X_0, \cdots, X_n]_{hom}$ とする。f をある素数 p で還元したとき f は絶対既約か？

必要なら f を整数倍し全ての係数が整数であるとする。

命題 10

$f \in \mathbb{Z}[X_0, \cdots, X_n]_{hom}$ とする。イデアル $I \subset \mathbb{Z}[X_0, \cdots, X_n]$ を

$$I = (f, \frac{\partial f}{\partial X_0}, \cdots, \frac{\partial f}{\partial X_n}, g_1, \cdots, g_{n-2}) \quad (g_i \in \mathbb{Z}[X_0, \cdots, X_n]_{hom})$$

$\sqrt{I} = (m_0 X_0, \cdots, m_n X_n), p \nmid m_0 \cdots m_n$ とする。このとき $f \bmod p$ は絶対既約

Proof I の各生成元を mod p で還元し、それらを生成元とする $\mathbb{F}_p[X_0, \cdots, X_n]$ のイデアルを J とすると、$\sqrt{I} = (m_0 X_0, \cdots, m_n X_n)$ より $p \nmid m_0 \cdots m_n \Rightarrow J = (X_0, \cdots, X_n)$ であり、定理4から $f \bmod p$ は絶対既約である。

5.2 絶対既約な多変数多項式の生成

解がないことの証明に用いる多項式が少なくてすむときに絶対既約な多項式を無限個生成することができる:

系 11

$f \in K[X_0, \cdots, X_n]_{hom}, I = (\frac{\partial f}{\partial X_0}, \cdots, \frac{\partial f}{\partial X_r}, g_1, \cdots, g_{n-2})$ とする。$V(I) = \emptyset$ が成立すれば、
$deg(h) = deg(f)$ のような任意の $h \in K[X_{r+1}, \cdots, X_n]_{hom}$ に対し、$f + h$ は絶対既約である。

Proof $V(\frac{\partial}{\partial X_0}(f+h), \cdots, \frac{\partial}{\partial X_r}(f+h), g_1, \cdots, g_{n-2}) \subset V(\frac{\partial}{\partial X_0} f, \cdots, \frac{\partial}{\partial X_r} f, g_1, \cdots, g_{n-2})) = \emptyset$
定理4から $f + h$ は絶対既約

5.3 既約成分の上界

命題 12

S を f と f の r 階以下の微分からなる集合、$g_1, \cdots, g_{n-(r+1)} \in K[X_0, \cdots, X_n]_{hom}$ とする。このとき、$V(S) \cap V(g_1, \cdots, g_{n-(r+1)}) = \emptyset$ であれば f の既約成分の個数は r 個以下。

Proof $f = f_1 \cdots f_{r+1}$ とする。積の微分公式より $S \subset (f_1, \cdots, f_{r+1})$ よって $\dim(V(S)) > n - (r+1)$ 。定理 2 から $V(S) \cap V(g_1, \cdots, g_{n-(r+1)}) \neq \emptyset$ 対偶により結論を得る。

r が増えると代入多項式 g_i の数が減り、計算時間が増大することが予想される。

6 結論

今回は代数幾何の定理を応用し、多変数多項式が絶対既約であるための十分条件 (命題 3、定理 4) とそれを用いた既約証明アルゴリズムを構成し、これを用いて Gao による Newton 多面体を用いた証明方法では示せない多項式の既約証明もできることを示した。

またこの条件がどれだけ有用かを見るために命題 5 のような形でない多項式がどれだけ命題 3 の条件を満たしているかについて実験を行い、実験で扱った全ての多項式が命題 3 の条件を満たしていることを確かめ、命題 3 の条件の有用性を示した。既約証明がしやすい多項式の特徴も与えた。

アルゴリズム 1 で代入すべき多項式の考察、計算時間の解析、5 節で紹介した内容に関する詳しい考察などは今後の課題とする。

参 考 文 献

[1] S.Gao. *Absolute Irreducibility of Polynonmials via Newton Polytopes*, J. of Algebra 237, 501–520 (2001)

[2] R. Hartshorne, Algebraic Geometry, Springer-Verlag GTM 52, Berlin, New York, 1977.

[3] Erick Kaltofen, *Polynomial Factorization:a success story*,Proceedings,ISSAC'03