因数分解を利用した多変数多項式の decomposition

Decompotision of multivariate polynomials using polynomial factorization

東京理科大学大学院　　徳田 陸成 [*1]
Rikuna Tokuda
Graduate school, Tokyo University of Science

東京理科大学　　武田 渉 [*2]
Wataru Takeda
Tokyo University of Science

東京理科大学　　関川 浩 [*3]
Hiroshi Sekigawa
Tokyo University of Science

Abstract

We propose algorithms for decomposing multivariate polynomials using polynomial factorization in special cases.

1　はじめに

数式処理の問題の一つとして，与えられた多項式を多項式の合成の形で表現する問題が研究されてきた．入力多項式が多変数かつ斉次の場合の問題を解くアルゴリズムは Faugère and Perret [1, 2] により提案されており，多くの問題を解くことができる．しかし，グレブナー基底計算が必要であることや，変数の個数が少ない場合には入力多項式が合成の形で表現できるか否かによらず，アルゴリズムが失敗することなど，課題がいくつか残っている．本稿では，特別な場合における因数分解を利用したアルゴリズムを提案し，また先行研究のアルゴリズムでは失敗する問題が解けることを紹介する．

2　定義

本節では，本稿を通して用いる記号，用語の定義を行う．

注意 1

以後，K を体とし，$\boldsymbol{f} = (f_1, \cdots, f_u) \in K[x_1, \cdots, x_m]^u$, $\boldsymbol{h} = (h_1, h_2) \in K[x_1, \cdots, x_m]^2$ において，各々の成分は K 線形独立であると仮定する．

[*1] 1423521@ed.tus.ac.jp
[*2] w.takeda@rs.tus.ac.jp
[*3] sekigawa@rs.tus.ac.jp

定義 1
$\boldsymbol{f} = (f_1, \cdots, f_u) \in K[x_1, \cdots, x_m]^u$ が次数 n の斉次式系であるとは，全ての $1 \leq i \leq u$ で，f_i が次数 n の斉次式であることをいう．このとき，$\boldsymbol{f}$ の次数を $\deg \boldsymbol{f} = n$ とかく．

項順序 $<$ に関する p, q の S 多項式を $S_<(p, q)$ と表す．ただし，項順序を明示する必要がないときは単に $S(p, q)$ と表す．

$\mathrm{coeff}(p, x^\alpha)$ を p の x^α における係数とする．

3 扱う問題

本稿で扱う問題は，以下の通りである．

問題 1
次数 $n = rs$ の斉次式系 $\boldsymbol{f} = (f_1, \cdots, f_u) \in K[x_1, \cdots, x_m]^u$，ただし $r, s \in \mathbb{N}_{\geq 2}$，が与えられたとき，

$$\boldsymbol{f} = \boldsymbol{g} \circ \boldsymbol{h} = (g_1(h_1, \cdots, h_d), \cdots, g_u(h_1, \cdots, h_d))$$

なる次数 r, s の斉次式系 $\boldsymbol{g} \in K[x_1, \cdots, x_d]^u$, $\boldsymbol{h} \in K[x_1, \cdots, x_m]^d$ が存在するか判定し，存在するなら $\boldsymbol{g}, \boldsymbol{h}$ を求めよ．

定義 2
$\boldsymbol{f} = \boldsymbol{g} \circ \boldsymbol{h}$ となるとき，$(\boldsymbol{g}, \boldsymbol{h})$ を $\boldsymbol{f}$ の *decomposition*，$\boldsymbol{g}, \boldsymbol{h}$ をそれぞれ *left component*，*right component* という．

主結果として，$\boldsymbol{g}$ が二変数，$\boldsymbol{h}$ が多変数の状況で，問題 1 を解くために利用できる性質を示し，その性質を用いて問題 1 を解くアルゴリズムを二通り提案する．

4 準備

decomposition アルゴリズムは，大きく以下の二つのステップに分けられる．

1. $\boldsymbol{f}$ から $\boldsymbol{h}$ を計算
2. $\boldsymbol{f}, \boldsymbol{h}$ から $\boldsymbol{f} = \boldsymbol{g} \circ \boldsymbol{h}$ を用いて $\boldsymbol{g}$ を計算

一般に 1 の方が難しいため，先に 2 について述べる．

4.1 $\boldsymbol{g}$ の計算法

$\boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h}$ は斉次式系であるから，$\deg \boldsymbol{f} = \deg \boldsymbol{g} \cdot \deg \boldsymbol{h}$ が成り立つ．ゆえに，$\boldsymbol{f}$, $\boldsymbol{h}$ が既知なら $\deg \boldsymbol{g}$ が確定する．すると，$\boldsymbol{f} = \boldsymbol{g} \circ \boldsymbol{h}$ の係数比較により $\boldsymbol{g}$ の係数を変数とする連立線形方程式が得られるため，これを解けば $\boldsymbol{g}$ が計算できる．

例 1
$\boldsymbol{f} = (11x^4 - 26x^3y + 16x^2y^2, 4x^4 - 2x^3y - 4x^2y^2)$, $\boldsymbol{h} = (41x^2 - 54xy, xy)$ とする．このとき，$\deg \boldsymbol{g} = 2$ であるから，$\boldsymbol{g} = (a_1x^2 + a_2xy + a_3y^2, b_1x^2 + b_2xy + b_3y^2)$ とし，$\boldsymbol{f} = \boldsymbol{g} \circ \boldsymbol{h}$ から得られる以下の連立線形方程式を解けばよい．

$$\begin{cases} 11 - 1681a_3 = 0, \\ -26 - 41a_2 + 4428a_3 = 0, \\ 16 - a_1 + 54a_2 - 2916a_3 = 0, \\ 4 - 1681b_3 = 0, \\ -2 - 41b_2 + 4428b_3 = 0, \\ -4 - b_1 + 54b_2 - 2916b_3 = 0. \end{cases}$$

4.2 genericity と同値性

$\boldsymbol{h}$ の計算法において必要な概念を導入する．まずは，[1, 2] で用いられている generic という概念である．

定義 3
性質 A が *generic* であるとは，射影空間の空でない *Zariski* 開集合 O が存在して，O の任意の点に対して性質 A が成り立つことをいう．

次に，同値性についてである．

定義 4
$\boldsymbol{h}, \boldsymbol{h}' \in K[x_1, \cdots, x_m]^d$ を s 次斉次式系とする．$\boldsymbol{h}$ と $\boldsymbol{h}'$ が同値であるとは，以下が成り立つことをいう．

$$\exists A \in GL_d(K),\ \boldsymbol{h}' = \boldsymbol{h}A.$$

$\boldsymbol{f} = \boldsymbol{g} \circ \boldsymbol{h}$ とすると，$\boldsymbol{f} = \boldsymbol{g} \circ \boldsymbol{h} = \boldsymbol{g}(\boldsymbol{x}A^{-1}) \circ (\boldsymbol{h}A) =: \boldsymbol{g}' \circ \boldsymbol{h}'$ より，$(\boldsymbol{g}', \boldsymbol{h}')$ も $\boldsymbol{f}$ の decomposition になる．decomposition を考える上で定数倍の違いは無視してよいから，斉次式系をある射影空間の点と同一視し，$\boldsymbol{f}$ から $\boldsymbol{h}$ と同値な $\boldsymbol{h}'$ が generic に構成できることを示す．

5 主結果

以下が，主結果である $\boldsymbol{h}'$ の計算に利用できる性質である．

定理 5
以下，$x_1 > \cdots > x_m$ なる lex 順序を考える．

$\boldsymbol{h} = (h_1, h_2) \in K[x_1, \cdots, x_m]^2$ を s 次斉次式系，$p = G_1 \circ \boldsymbol{h},\ q = G_2 \circ \boldsymbol{h}\quad (G_i \in K[x, y],\ i = 1, 2)$ を t 次斉次式とする．また，$\mathrm{coeff}(p, x_1^t),\ \mathrm{coeff}(q, x_1^t),\ \mathrm{coeff}(h_i, x_1^s) \neq 0\quad (i = 1, 2)$ と仮定する．このとき，以下が成り立つ．

$$S(h_1, h_2)^{j+1} \mid S(S(h_1, h_2)^j p, S(h_1, h_2)^j q)\quad (j \in \mathbb{N} \cup \{0\}).$$

また，ある斉次式 $G' \in K[x, y]$ が存在して，以下のようにかける．

$$\frac{S(S(h_1, h_2)^j p, S(h_1, h_2)^j q)}{S(h_1, h_2)^{j+1}} = G' \circ \boldsymbol{h}.$$

証明には，いくつかの補題を用いる．

補題 6
$G_1, G_2 \in K[x,y]$ とすると，$G_1 \mid G_2 \Longrightarrow G_1 \circ \boldsymbol{h} \mid G_2 \circ \boldsymbol{h}$ が成り立つ．また，$\exists G \in K[x,y],\ (G_2 \circ \boldsymbol{h})/(G_1 \circ \boldsymbol{h}) = G \circ \boldsymbol{h}$ が成り立つ．

証明 $G_1 \mid G_2$ なら，$\exists G \in K[x,y],\ G_2 = G_1 G$ とかける．$x = h_1,\ y = h_2$ を代入すると，$G_1 \circ \boldsymbol{h} \mid G_2 \circ \boldsymbol{h}$ 及び $(G_2 \circ \boldsymbol{h})/(G_1 \circ \boldsymbol{h}) = G \circ \boldsymbol{h}$ が分かる． ∎

補題 7
f, g を斉次式として，f を g で割ることで得られる商と余りをそれぞれ q, r とすると，q, r はいずれも斉次式 (0 もありうる) である．

証明 割り算アルゴリズムにおける商，余りの更新の仕方から明らか． ∎

注意 2
p, q が定理 5 の仮定を満たすとき，

$$S(p,q) = \frac{1}{\mathrm{coeff}(p, x_1^t)} p - \frac{1}{\mathrm{coeff}(q, x_1^t)} q$$

であるが，記法を簡潔にするため，証明中ではこれを $\mathrm{coeff}(p, x_1^t)\mathrm{coeff}(q, x_1^t)$ 倍した

$$\mathrm{coeff}(q, x_1^t) p - \mathrm{coeff}(p, x_1^t) q$$

を $S(p,q)$ とする (定数倍の違いは結論に影響しない)．

以上の準備の下で，定理 5 を証明する．

証明 まず，$j = 0$ の場合を証明する．

$$\begin{aligned}
S(p,q) &= \mathrm{coeff}(q, x_1^t) p - \mathrm{coeff}(p, x_1^t) q \\
&= \mathrm{coeff}(q, x_1^t) G_1 \circ \boldsymbol{h} - \mathrm{coeff}(p, x_1^t) G_2 \circ \boldsymbol{h} \\
&= (\mathrm{coeff}(q, x_1^t) G_1 - \mathrm{coeff}(p, x_1^t) G_2) \circ \boldsymbol{h}, \\
S(h_1, h_2) &= \mathrm{coeff}(h_2, x_1^s) h_1 - \mathrm{coeff}(h_1, x_1^s) h_2 \\
&= (\mathrm{coeff}(h_2, x_1^s) x - \mathrm{coeff}(h_1, x_1^s) y) \circ \boldsymbol{h}.
\end{aligned}$$

補題 6 から，$\mathrm{coeff}(h_2, x_1^s) x - \mathrm{coeff}(h_1, x_1^s) y$ が $\mathrm{coeff}(q, x_1^t) G_1 - \mathrm{coeff}(p, x_1^t) G_2$ を割り切ることを示せばよい． $c = \mathrm{coeff}(h_1, x_1^s),\ d = \mathrm{coeff}(h_2, x_1^s)$ とすると，簡単な計算から

$$\mathrm{coeff}(p, x_1^t) = G_1(c,d), \qquad \mathrm{coeff}(q, x_1^t) = G_2(c,d)$$

が分かる．$\varphi = \mathrm{coeff}(q, x_1^t) G_1 - \mathrm{coeff}(p, x_1^t) G_2 = G_2(c,d) G_1 - G_1(c,d) G_2$ を $dx - cy$ で割ると，

$$\varphi = (dx - cy)\psi + m \qquad (*)$$

と表せて，m はどの項も $x = \mathrm{lm}(dx - cy)$ で割り切れないか 0 である．従って，$m \in K[y]$ である．$m \neq 0$ と仮定して矛盾を導く．補題 7 から m は斉次式なので，

$$\exists \alpha \in K \backslash \{0\},\ \exists r \in \mathbb{N},\ m = \alpha y^r$$

とかけて，$m(d) = \alpha d^r \neq 0$ である．一方，$(*)$ において $x = c,\ y = d$ を代入すると，$\varphi(c,d) = 0$ より $m(d) = 0$ となり矛盾する．よって $m = 0$ である．

一般の j の場合を示す．$e = \mathrm{lc}(S(h_1,h_2)^j)$ とすると，

$$\begin{aligned}&S(S(h_1,h_2)^j p, S(h_1,h_2)^j q)\\&= e\cdot \mathrm{coeff}(q,x^t)S(h_1,h_2)^j p - e\cdot \mathrm{coeff}(p,x^t)S(h_1,h_2)^j q\\&= eS(h_1,h_2)^j S(p,q).\end{aligned}$$

ここで，$j=0$ の場合より $S(h_1,h_2) \mid S(p,q)$ であるから，

$$S(h_1,h_2)^{j+1} \mid S(S(h_1,h_1)^j p, S(h_1,h_2)^j q)$$

がいえる．また，$j=0$ の場合より，

$$\exists G \in K[x,y],\ \frac{S(p,q)}{S(h_1,h_2)} = G\circ \boldsymbol{h}$$

とかけるから，

$$\begin{aligned}&\frac{S(S(h_1,h_2)^j p, S(h_1,h_2)^j q)}{S(h_1,h_2)^{j+1}}\\&= \frac{eS(p,q)}{S(h_1,h_2)} = e(G\circ \boldsymbol{h}) = (eG)\circ \boldsymbol{h}.\end{aligned}$$

よって，$G' = eG$ とすればよい． ∎

5.1 $\boldsymbol{h}$ の計算法

$\boldsymbol{h}$ の計算法について述べる．$\boldsymbol{f} = \boldsymbol{g}\circ \boldsymbol{h}$ ($\boldsymbol{g} \in K[x,y]^u, \boldsymbol{h} \in K[x_1,\cdots,x_m]^2, u \in \mathbb{N}_{\geq r}$) とする．
定理 5 の $j=0$ の場合から，

$$S(f_k, f_{k+1}) = S(h_1,h_2)v_{1,k} \quad (1 \leq k \leq r-1)$$

とかけて，$v_{1,k}$ は $\boldsymbol{h}$ を right component とする合成の形でかける．定理 5 の $j=1$ の場合から，

$$S(S(f_k,f_{k+1}), S(f_{k+1},f_{k+2})) = S(h_1,h_2)^2 v_{2,k} \quad (1 \leq k \leq r-2)$$

とかけて，$v_{2,k}$ は $\boldsymbol{h}$ を right component とする合成の形でかける．同様に，定理 5 を繰り返し適用することで，

$$\mathrm{Func}(\boldsymbol{f}, r) = S(h_1,h_2)^{r-1} v_{r-1,1}$$

という形に因数分解できることが分かる．ただし，$\mathrm{Func}(\boldsymbol{f},r)$ は次ページのアルゴリズム 1 の出力である．$h_1' = S(h_1,h_2),\ h_2' = v_{r-1,1}$ とすると，構成の仕方から h_1', h_2' は h_1, h_2 の線形結合でかける．すると，ある正方行列 M により以下のように表せる．

$$(h_1', h_2') = (h_1,h_2)M.$$

$\det M = 0$ は $\boldsymbol{g}$, $\boldsymbol{h}$ の係数を変数とする代数方程式を定める．ゆえに，$\boldsymbol{h}, \boldsymbol{h}'$ が同値 ($\Leftrightarrow \det M \neq 0$) であることは generic な性質である．

注意 3
以下のアルゴリズム *1* は，以下の形の多項式を出力する．

$$\mathrm{Func}(\boldsymbol{f},3)=S(S(f_1,f_2),S(f_2,f_3)),\quad \mathrm{Func}(\boldsymbol{f},4)=S(S(S(f_1,f_2),S(f_2,f_3)),S(S(f_2,f_3),S(f_3,f_4))).$$

$\hat{\boldsymbol{f}}=(f_2,\cdots,f_u)$ とすると，$\mathrm{Func}(\boldsymbol{f},r)=S(\mathrm{Func}(\boldsymbol{f},r-1),\mathrm{Func}(\hat{\boldsymbol{f}},r-1))$ が成り立つことに注意する．

アルゴリズム 1
Input : $\boldsymbol{f}=(f_1,\cdots,f_u)\quad (u\in\mathbb{N}_{\geq r}),\ r\in\mathbb{N}$
Output : a_1
for $i=1,\cdots,r$ *do*
  $a_i\leftarrow f_i$
$k\leftarrow r-1$
while $k\neq 0$ *do*
  for $i=1,\cdots,k$ *do*
    $a_i\leftarrow S(a_i,a_{i+1})$
  $k\leftarrow k-1$
return a_1

5.2 定理 5 の仮定について

定理 5 を適用するには，$\boldsymbol{f}$, $\boldsymbol{h}$ が以下の仮定を満たす必要がある．

1. $\mathrm{coeff}(f_j,x_1^n)\neq 0\quad (j=1,\cdots,u)$
2. $\mathrm{coeff}(h_j,x_1^s)\neq 0\quad (j=1,2)$

以下の命題は，1 の条件を満たすことのみ確認すればよいことを意味する．

命題 8
$\boldsymbol{f}=\boldsymbol{g}\circ\boldsymbol{h}$ が *1* を満たすとすると，*2* を満たす $\boldsymbol{f}$ の *right component* $\boldsymbol{h}'$ が存在する．

証明 以下の変換 S_1,S_2,T_1,T_2 を考える．

$$S_1:(x,y)\mapsto(x+y,y),\qquad S_2:(x,y)\mapsto(x-y,y),$$
$$T_1:(x,y)\mapsto(x,y+x),\qquad T_2:(x,y)\mapsto(x,y-x).$$

$S_1\circ S_2=T_1\circ T_2=(x,y)$ が成り立つことに注意する．2 を満たさない場合を 3 つの場合に分けて考える．

- $\mathrm{coeff}(h_1,x^s)=0,\ \mathrm{coeff}(h_2,x^s)\neq 0$ のとき：
  $f=\boldsymbol{g}\circ\boldsymbol{h}=(\boldsymbol{g}\circ S_1)\circ(S_2\circ\boldsymbol{h})$ とかけて，$S_2\circ\boldsymbol{h}=(h_1-h_2,h_2)$ である．$\mathrm{coeff}(h_1-h_2,x^s)=\mathrm{coeff}(-h_2,x^s)\neq 0,\ \mathrm{coeff}(h_2,x^s)\neq 0$ なので，$S_2\circ\boldsymbol{h}$ は 2 を満たす．
- $\mathrm{coeff}(h_1,x^s)\neq 0,\ \mathrm{coeff}(h_2,x^s)=0$ のとき：
  上と同様の議論により，$T_2\circ\boldsymbol{h}$ は 2 を満たす．
- $\mathrm{coeff}(h_1,x^s)=0,\ \mathrm{coeff}(h_2,x^s)=0$ のとき：
  定理 5 の証明から，$\mathrm{coeff}(f_1,x^n)=g_1(c,d)$ である．ここで，$c=\mathrm{coeff}(h_1,x^s),\ d=\mathrm{coeff}(h_2,x^s)$ である．今，$c=d=0$ であり，g_1 は斉次だから，$0\neq\mathrm{coeff}(f_1,x^n)=0$ となり矛盾するので，この状況は起こり得ない．

∎

$\boldsymbol{f}$ が 1 を満たさないときの二つの対処法を述べる．

- 変数変換
  $a \in K,\ 2 \leq i \leq m$ に対し，$\boldsymbol{f}' = \boldsymbol{f}(x_1, \cdots, x_{i-1}, x_i + ax_1, x_{i+1}, \cdots, x_m)$ とする．$\boldsymbol{f}'$ の decomposition $(\boldsymbol{g}', \boldsymbol{h}')$ が存在するなら，$\boldsymbol{h} = \boldsymbol{h}'(x_1, \cdots, x_i - ax_1, \cdots, x_m)$ とすると，$(\boldsymbol{g}', \boldsymbol{h})$ は $\boldsymbol{f}$ の decomposition になる．ゆえに，$\boldsymbol{f}$ が 1 を満たさないときは，適当な a, i をとり，1 を満たすような $\boldsymbol{f}'$ の decomposition を考えればよい．ただし，係数体の位数が小さいときは必ずしもこのような a, i がとれるとは限らない．

- 項順序の取り替え
  定理 5 において $x_1 > \cdots > x_m$ なる lex 順序を考えていたが，例えば $x_2 > \cdots > x_m > x_1$ なる lex 順序でも，同様のことが成り立つ (係数の条件において，x_1 を x_2 に置き換えればよい)．ゆえに，$\mathrm{coeff}(f_j, x_i^n) \neq 0 \quad (j = 1, \cdots, u)$ なる変数 x_i を先頭とするような lex 順序を考えればよい．

6 アルゴリズム

定理 5 を用いて，二通りの decomposition アルゴリズムが構成できる．

アルゴリズム 2
Input : $\boldsymbol{f} \in K[x_1, \cdots, x_m]^u, r, s \in \mathbb{N}_{\geq 2}$,
　　where $\boldsymbol{f} = \boldsymbol{g} \circ \boldsymbol{h}$ $(\boldsymbol{g} \in K[x, y]^u,\ \boldsymbol{h} \in K[x_1, \cdots, x_m]^2,\ u \in \mathbb{N}_{\geq r})$
Output : $\boldsymbol{h}'$

1. 必要なら，*5.2* 節の対処法を適用する
2. $\mathrm{Func}(\boldsymbol{f}, r)$ を計算
3. $\mathrm{Func}(\boldsymbol{f}, r) = S(h_1, h_2)^{r-1} v$ と因数分解し，$h_1' = S(h_1, h_2),\ h_2' = v$ と定める
4. *return* (h_1', h_2')

アルゴリズム 3
Input : $\boldsymbol{f} \in K[x_1, \cdots, x_m]^u, r, s \in \mathbb{N}_{\geq 2}$,
　　where $\boldsymbol{f} = \boldsymbol{g} \circ \boldsymbol{h}$ $(\boldsymbol{g} \in K[x, y]^u,\ \boldsymbol{h} \in K[x_1, \cdots, x_m]^2,\ u \in \mathbb{N}_{\geq 2})$
Output : $\boldsymbol{h}'$

1. $<, \prec : S_<(f_1, f_2) \neq S_\prec(f_1, f_2)$ なる項順序
   必要なら，*5.2* 節の対処法を適用する
2. $S_<(f_1, f_2),\ S_\prec(f_1, f_2)$ を計算
3. これらを因数分解し，$h_1' = S_<(h_1, h_2),\ h_2' = S_\prec(h_1, h_2)$ と定める
4. *return* (h_1', h_2')

アルゴリズム 2, 3 の違いは以下の通りである．

- アルゴリズム 2
  - 入力リスト長が r 以上でなければならない
  - 因数分解が一回で済む
- アルゴリズム 3
  - 入力リスト長が 2 以上であればよい
  - 因数分解が二回必要になる

共通する性質として，ほとんどの場合に $\boldsymbol{f}$ の right component を計算できる．

系 9
アルゴリズムの出力を $\boldsymbol{h}'$ とすると，$\boldsymbol{h}'$ が $\boldsymbol{f}$ の *right component* であることは *generic* な性質である．

証明 5.1 節の議論より従う． ∎

6.1 計算例

先行研究のアルゴリズムでは計算できない例を計算する．$\boldsymbol{f} = (x^4 + x^3y + 2x^2y^2 + xy^3 + y^4, x^4 + 3x^3y + 3x^2y^2 + 3xy^3 + y^4) \in \mathbb{Q}[x, y]^2$ は二つの二次斉次式系を合成したものである．$\boldsymbol{f}$ に先行研究のアルゴリズムを適用すると失敗する (四次式の decomposition の計算では五変数以上であることを必要とする)．

アルゴリズム 2 で $\boldsymbol{f}$ の decomposition を計算しよう．$\mathrm{Func}(\boldsymbol{f}, 2)$ は以下のように因数分解できる．

$$\mathrm{Func}(\boldsymbol{f}, 2) = -xy(2x^2 + xy + 2y^2).$$

$\boldsymbol{h}' = (-xy, 2x^2 + xy + 2y^2)$ と定める．$\boldsymbol{f} = \boldsymbol{g}' \circ \boldsymbol{h}'$ から得られる連立線形方程式を解くと，以下のように g' が計算できる．

$$\boldsymbol{g}' = \Big(-\frac{x^2}{4} + \frac{y^2}{4}, -\frac{x^2}{4} - xy + \frac{y^2}{4}\Big).$$

$(\boldsymbol{g}', \boldsymbol{h}')$ は $\boldsymbol{f}$ の decomposition である．

7 おわりに

本稿では，$\boldsymbol{g}$ が二変数，$\boldsymbol{h}$ が多変数の状況で，二通りの decomposition アルゴリズムを提案した．今後の課題として，いずれのアルゴリズムでも対応できない入力リスト長が 1 の場合の対処法と，g が三変数以上の場合への結果の拡張について考える．

謝　辞

本研究は共同利用・共同研究拠点である京都大学数理解析研究所の支援と科研費 21K11760 の助成を受けたものである．

参 考 文 献

[1] Jean-Charles Faugère and Ludovic Perret. “An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography.” *Journal of Symbolic Computation* 44.12 (2009): 1676–1689.

[2] Jean-Charles Faugère and Ludovic Perret. “High order derivatives and decomposition of multivariate polynomials.” *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation* (2009): 207–214.