SLRA アルゴリズムによる多変数多項式の近似decomposition

An Approximate Decomposition of a Multivariate Polynomial via SLRA Algorithm

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　　関川 浩 [*2]
Hiroshi Sekigawa
Tokyo University of Science

Abstract

The approximate polynomial decomposition problem is that given a polynomial and a norm, compute the nearest decomposable polynomial with respect to the norm. In this paper, we propose an algorithm for computing an approximate decomposition of a multivariate polynomial in the 2-norm based on the SLRA problem.

1　はじめに

多項式の decomposition とは，与えられた多項式を多項式の合成の形に表現する問題である．一変数多項式に対する研究をはじめとして，有理関数や多変数多項式などへ問題が派生していった．

decomposition の派生の一つとして，近似 decomposition というものが知られている．多項式とノルムが与えられたとき，そのノルムに関して最も近い decomposable な多項式を求める問題である．

例 1

$f = 17.916x^4 + 26.3519x^3 + 35.2734x^2 + 18.8152x + 12.0927$ とする．f は *decomposable* でないが，誤差項を許容すると，$f = u \circ h + \delta,\ \|\delta\|_2 = 0.00936216$ と近似的には合成の形で表せる．ただし，u, h, δ は以下の通りである．

$$u = 1.0003x^2 + 4.0345x + 7.0231,\ h = 4.2321x^2 + 3.1124x + 1.0045,$$
$$\delta = 0.0042x^2 + 0.0035x + 0.0076.$$

浮動小数係数の多項式や，係数に何らかの理由で誤差が入った多項式の decomposition を求める際，厳密な代数的算法は誤差の影響で多くの場合破綻する．このような状況では，近似 decomposition の計算を考

[*1] E-mail: rikuna0429@gmail.com
[*2] E-mail: sekigawa@rs.tus.ac.jp

える必要がある．また，近似 decomposition には多項式の評価における演算回数の削減や多項式で表現されたデータパスの最適化 [4]，信号処理におけるモジュラーフィルタの設計 [3] など，様々な応用がある．

一変数多項式の近似 decomposition の研究はいくつか存在するが [1, 5, 8]，多変数の場合は未知の部分が多い．本論文では，以下の 2 ノルムに関する多変数多項式の近似 decomposition について考える．

問題 1
全次数 n の $f \in \mathbb{R}[x_1, \cdots, x_d]$ $(d \geq 2)$ 及び $r, s \in \mathbb{N}$ $(n = rs, r \geq 2)$ が与えられた時，次の条件を満たす $u \in \mathbb{R}[y]$，$h \in \mathbb{R}[x_1, \cdots, x_d]$ を求めよ．

- $f = u \circ h + \delta$，ただし，$\deg u = r, \deg h = s, \delta \in \mathbb{R}[x_1, \cdots, x_d]$
- $\|\delta\|_2$ が小さい

この問題を Structured Low-Rank Approximation (SLRA) という問題に帰着させることで，線形代数に基づくアルゴリズムを提案する．

2 多項式の decomposability と行列のランクについて

まず，多項式の decomposability と，ある行列のランクの関係について述べる．所望の行列は以下の命題から構成する．

命題 1 (cf. [2, 7])
$f, g \in \mathbb{R}[x_1, \cdots, x_d] \backslash (\mathbb{R}[x_1] \cup \cdots \cup \mathbb{R}[x_d])$ に対し，以下は同値である．

- $f = u \circ h$，$g = v \circ h$ なる $u, v \in \mathbb{R}[y], h \in \mathbb{R}[x_1, \cdots, x_d]$ が存在する．
- $D_f(g) = \mathbf{0}$, ただし，D_f は以下のような写像である．

$$
\begin{array}{cccc}
D_f : \mathbb{R}[x_1, \cdots, x_d] & \longrightarrow & \mathbb{R}[x_1, \cdots, x_d]^{d-1} \\
\cup\!\!\!\shortmid & & \cup\!\!\!\shortmid \\
F & \longmapsto & \begin{pmatrix} \partial_{x_1} f \partial_{x_2} F - \partial_{x_2} f \partial_{x_1} F \\ \partial_{x_1} f \partial_{x_3} F - \partial_{x_3} f \partial_{x_1} F \\ \vdots \\ \partial_{x_1} f \partial_{x_d} F - \partial_{x_d} f \partial_{x_1} F \end{pmatrix} & .
\end{array}
$$

証明 [2, Proposition 4] と同様に，[7, Lemma 1] から従う．なお，[7, Lemma 1] において係数体は代数閉体という仮定が入っているが，f が $\mathbb{R}$ 上で decomposable であることと $\mathbb{C}$ 上で decomposable であることは同値であることに注意せよ． ∎

$n = rs$ とし，$f, h \in \mathbb{R}[x_1, \cdots, x_d] \backslash (\mathbb{R}[x_1] \cup \cdots \cup \mathbb{R}[x_d])$ は $\deg f \leq n, \deg h \leq s$ を満たすとする．また，$h(0, \cdots, 0) = 0$ とする (詳細は次の注意を参照せよ)．以下で定める行列のサイズを固定するために，もし h が sparse または i 変数多項式 $(i < d)$ であったとしても，dense な d 変数多項式とみなす．例えば，全次数 1 の多項式 $h = x_1 + x_2 \in \mathbb{R}[x_1, x_2, x_3, , x_4]$ について，$h = x_1 + x_2 + 0 \cdot x_3 + 0 \cdot x_4$ とみなす．

$D_f(h) = \mathbf{0}$ から，以下が得られる．

$$
\begin{cases}
\partial_{x_1} f \partial_{x_2} h - \partial_{x_2} f \partial_{x_1} h = 0, \\
\partial_{x_1} f \partial_{x_3} h - \partial_{x_3} f \partial_{x_1} h = 0, \\
\vdots \\
\partial_{x_1} f \partial_{x_d} h - \partial_{x_d} f \partial_{x_1} h = 0.
\end{cases}
\tag{1}
$$

(1) の両辺の係数比較によって，h の係数を変数とする同次連立線形方程式が得られる．その係数行列を M_f，h の係数ベクトルを $\boldsymbol{h}$ とすると，以下の通りである．

$$M_f \boldsymbol{h} = \boldsymbol{0}. \tag{2}$$

f が decomposable とすると，Proposition 1 より，(2) は非自明な解を持つ，すなわち M_f はランク落ちする．一方，f が indecomposable とすると，Proposition 1 より (2) は自明な解しか持たない，すなわち M_f はフルランクとなる．以上のことから，f の decomposability は M_f のランクが落ちるか否かを確認すれば判定できる．

注意 1
以後，ランク落ちするときはちょうど 1 だけ落ちると仮定する．一般にはランクが 2 以上落ちることもあるが，ちょうど 1 落ちる場合に容易に帰着できることを後の節で述べる．

$f = u \circ h + \delta$ と書けるとき，$f = u(x + h(0,\cdots,0)) \circ (h - h(0,\cdots,0)) + \delta$ より，h の定数項は 0 としてよい．ゆえに，h の未知の係数は $\binom{s+d}{d} - 1$ 個であるから，$M_f \in \mathbb{R}^{p\times q}$，$p > q = \binom{s+d}{d} - 1$ となる．よって，ランク落ちする場合のランクは $\binom{s+d}{d} - 2$ である．

3 SLRA problem

まず，本節で必要な定義について述べておく．

定義 2
$\mathbb{R}^{p\times q}$ を，以下の *Frobenius* 内積を備えた $p \times q$ 行列全体のなす空間とする．

$$\langle M_1, M_2 \rangle = \mathrm{Tr}(M_1^T M_2).$$

また，この内積から *Frobenius* ノルム $\|M\|_F = \sqrt{\langle M, M \rangle}$ が誘導される．

前節の decomposability と行列のランクの関係を用いることで，Problem 1 を解くためには以下の問題が解ければよいことが分かる．

問題 2
$f \in \mathbb{R}[x_1,\cdots,x_d]$ に対し，$\|f - \hat{f}\|_2$ が小さく，かつ $M_{\hat{f}}$ がランク落ちしているような $\hat{f} \in \mathbb{R}[x_1,\cdots,x_d]$ を求めよ．

この問題は，以下の SLRA problem に帰着させることができる．

問題 3
E を $\mathbb{R}^{p\times q}$ の *affine* 部分空間，$\mathcal{D}_r$ をランクが r の $p \times q$ 行列全体の集合とする．$M \in E$，$r \in \mathbb{N}$ が与えられたとき，$\|M - M^\star\|_F$ が小さくなるような $M^\star \in E \cap \mathcal{D}_r$ を求めよ．

注意 2
Problem 2 では 2 ノルムを最小化するのに対し，*Problem 3* では *Frobenius* ノルムを最小化している．これらの最適化問題は一致していないが，いくつかのランダムに生成した計算例でさほど悪くない出力が得られている．

Problem 2 が Problem 3 に帰着することを示す．

命題 3
$\mathbb{R}[x_1,\cdots,x_d]_{0,n} = \{f \in \mathbb{R}[x_1,\cdots,x_d] \mid \deg f \le n,\ f(0,\cdots,0)=0\}$, $E = \{M_f \mid f \in \mathbb{R}[x_1,\cdots,x_d]_{0,n}\}$ と定める．また，$\varphi : \mathbb{R}[x_1,\cdots,x_d]_{0,n} \to E$ を $\varphi(f) = M_f$ と定める．このとき，以下が成り立つ．

(i) $\mathbb{R}[x_1,\cdots,x_d]_{0,n}$ と E はともに線形空間で，φ は線形写像．

(ii) $\{M_{x^\alpha}/\|M_{x^\alpha}\|_F\}_{0<|\alpha|\le n}$ は E の正規直交基底．

(iii) φ は全単射，すなわち $\mathbb{R}[x_1,\cdots,x_d]_{0,n}$ と E は線形同型．

証明 (i) M_f の定め方から容易に示せる．

(ii) $x^\alpha \ne x^\beta, 0 < |\alpha|,|\beta| \le n$ とする．M_f の定め方から，各 i に対し，$M_{x^\alpha}, M_{x^\beta}$ の i 行目は非零成分が高々一つの行ベクトルで，ともに非零成分がある場合は互いに異なる位置にあることが示せる．よって $\langle M_{x^\alpha}, M_{x^\beta}\rangle = 0$ となる．また，$\langle M_{x^\alpha}, M_{x^\alpha}\rangle = \|M_{x^\alpha}\|_F$ であるから，$\{M_{x^\alpha}/\|M_{x^\alpha}\|_F\}_{0<|\alpha|\le n}$ は正規直交系をなす．(i) より，E は $\{M_{x^\alpha}/\|M_{x^\alpha}\|_F\}_{0<|\alpha|\le n}$ で張られる．よって，(ii) が成り立つ．

(iii) 定義から φ は全射である．$M_f = M_g$ と仮定し，(ii) の正規直交基底の各元との内積をとれば，$f = g$ が示せる．ゆえに φ は単射である．以上より，(iii) が成り立つ． ∎

$\mathrm{DEC}_{n,s} = \{f \in \mathbb{R}[x_1,\cdots,x_d]_{0,n} \mid \exists u \in \mathbb{R}[y], \exists h \in \mathbb{R}[x_1,\cdots,x_d]_{0,s}, f = u \circ h\}$ と定める．Proposition 1 より，decomposable な多項式は対応する行列がランク落ちするのであった．また，Proposition 3 により $\mathbb{R}[x_1,\cdots,x_d]_{0,n}$ と E を同一視できる．以上より，この同一視の下で，$\mathrm{DEC}_{n,s} = E \cap \mathcal{D}_{\binom{s+d}{d}-2}$ と表せる．ゆえに Problem 2 は Problem 3 に帰着される．

注意 3
$\mathrm{DEC}_{n,s}$ の定め方から定数項が 0 の多項式に対する近似 *decomposition* を考えることになるが，定数項が 0 でない場合も容易に計算できる．実際，$f = u \circ h + \delta$ と書けるとき，$f - f(0,\cdots,0) = (u - f(0,\cdots,0)) \circ h + \delta$ となるから，$f - f(0,\cdots,0)$ に対する近似 *decomposition* (u,h) を求めた後，$u' = u + f(0,\cdots,0)$ とすれば (u',h) が f の近似 *decomposition* となる．

4 SLRA problem に基づく近似 decomposition アルゴリズム

Problem 3 を解くアルゴリズムとして，NewtonSLRA [9] という反復法が知られている．本節ではその変種である relaxed NewtonSLRA [6] を用いる．これは近似 GCD の計算用にデザインされたものであるが，近似 decomposition の計算にも問題なく使用できる．

以下が relaxed NewtonSLRA の一回分の反復である．中身の記号等の詳細については元論文 [6] を参照されたい．

Algorithm 1 One iteration of relaxed NewtonSLRA

Require: $M \in E \subset \mathbb{R}^{p\times q}, r \in \mathbb{N}$ such that $p > q, r = q-1$ and $\{B_1,\cdots,B_t\}$ is an orthonormal basis of E^0

Ensure: $\Pi_{E\cap\mathcal{T}_{M,\tilde{M}}\mathcal{D}_r}(M)$, where $\tilde{M} = \Pi_{\mathcal{D}_r}(M)$

1: $U\Sigma V^T \leftarrow$ the singular value decomposition of M and let $U = (\vec{u}_1,\cdots,\vec{u}_p)$ and $V = (\vec{v}_1,\cdots,\vec{v}_q)$
2: $\tilde{M} \leftarrow U_r\Sigma_r V_r^T$, where $U_r = (\vec{u}_1,\cdots,\vec{u}_r), V_r = (\vec{v}_1,\cdots,\vec{v}_r)$ and Σ_r is the top-left $r\times r$ submatrix of Σ
3: $A \leftarrow (a_{1,l})^{1\times t}, a_{1,l} = \langle \vec{u}_{r+1}\vec{v}_q^T, B_l\rangle$
4: $\vec{b} \leftarrow (b_1) \in \mathbb{R}^1, b_1 = \langle \vec{u}_{r+1}\vec{v}_q^T, \tilde{M} - M\rangle$
5: **return** $M + \sum_{l=1}^t (A^\dagger \vec{b})_l B_l$

注意 4
通常の *NewtonSLRA* を用いると局所最適解に収束することが多いため，局所最適解への収束を防ぐ工夫の入った *relaxed NewtonSLRA* を用いている．なお，講演後に *[6]* の著者にお聞きした事だが，*NewtonSLRA* 内の最小二乗解の計算 *(Algorithm 1* では *Step 5* の $A^\dagger\vec{b}$ の計算に相当*)* において，*tolerance* を調節すれば同様に局所最適解へ収束することを防ぐことができる．

Algorithm 1 を用いて，近似 decomposition アルゴリズムを構成する．アルゴリズムの入力として以下が必要であった．

- 初期値行列 M
- 出力行列のランク r
- E に付随する線形空間 E^0 の正規直交基底 $\{B_1, \cdots, B_t\}$

問題設定と Proposition 3 より，$M = M_f, r = \binom{s+d}{d} - 2, \{B_1, \cdots, B_t\} = \{M_{x^\alpha}/\|M_{x^\alpha}\|_F\}_{0<|\alpha|\le n}$ とすればよい (E は線形空間なので $E = E^0$ である)．これで Algorithm 1 が利用できる．

さて，近似 decomposition の計算法について述べる．まず，Algorithm 1 を十分な回数反復することで M_f からランク落ちした近接行列 $M_{\hat{f}}$ を計算する．すると，$M_{\hat{f}}\boldsymbol{h} = \boldsymbol{0}$ の非自明な解，すなわち $\ker M_{\hat{f}}$ の基底を求めることで h が計算できる．次に，f, h から $\|f - u \circ h\|_2$ を最小化する u を求める．$f = u \circ h$ から，u の係数を変数とする連立線形方程式 $A\boldsymbol{u} = \boldsymbol{b}$ が得られる．この連立方程式の最小二乗解 $\boldsymbol{u} = A^\dagger\boldsymbol{b}$ を求めれば，$\|f - u \circ h\|_2$ を最小化する u が計算できる．

以上をまとめると，以下の近似 decomposition アルゴリズムが構成できる．

Algorithm 2 AppDecomp
Require: (f, n, s) as in Problem 1
Ensure: (u, h) as in Problem 1
1: Construct M_f from (f, n, s)
2: Compute a rank deficient matrix $M_{\hat{f}}$ from M_f by Algorithm 1
3: Compute h from a linear system $M_{\hat{f}}\boldsymbol{h} = \boldsymbol{0}$
4: Compute u by solving the least-squares problem
5: **return** (u, h)

注意 5
Proposition 1 は一変数多項式に対しては成り立たないため，このアルゴリズムでは一変数多項式の近似 *decomposition* を計算することはできない．一変数の場合は *[1, 5]* のアルゴリズムを用いればよい．

例 2
$n = 4, s = 2$ とし，f を以下の通りとする．f は *decomposable* な多項式の係数に平均 0, 分散 10^{-6} の正規分布からのノイズを加えたものである．

$$\begin{aligned} f =& 131.225x^4 - 133.654x^3 - 14.9802x^2y + 335.763x^2z + 4.9437x^2 + 7.62874xy - 170.989xz + \\ & 14.8132x + 0.427524y^2 - 19.1649yz + 1.6603y + 214.778z^2 - 37.2136z. \end{aligned}$$

$M_f \in \mathbb{R}^{70\times 9}$ を構成し，*Algorithm 1* を反復することでランク落ちした近接行列 $M_{\hat{f}}$ が得られる．$\ker M_{\tilde{f}}$ の基底を計算すると，

$$h = 0.299079x - 0.58729x^2 + 0.0335216y - 0.751345z$$

が得られる．すると，f, h から最小二乗法によって u は以下のように計算できる．

$$u = 380.462x^2 + 49.5293x.$$

$\|f - u \circ h\|_2 = 3.6123 \times 10^{-6}$ と，絶対誤差は与えたノイズの分散と同程度であることが分かる．

5　ランクが 2 以上落ちる場合

近接行列のランクが 2 以上落ちる場合の対処法について述べる．$f = u \circ h + \delta, \deg f = n, \deg h = s$ とする．(f, n, s) から M_f を構成すると，h が decomposable であれば，$M_{\hat{f}}$ は 2 以上ランク落ちする．この場合，$\ker M_{\hat{f}}$ は h と h の right component に対応する係数ベクトルを含むため，$\ker M_{\hat{f}}$ の基底が h の係数を与えるとは限らない．

この場合，s の約数 s' をとり，(f, n, s') から M_f を再構成する．この操作を繰り返すと，$\ker M_{\hat{f}}$ が h の indecomposable な right component に対応する係数ベクトルのみを含むようになるため，近接行列のランクがちょうど 1 落ちるような M_f が得られる．

上記の操作のためには，近接行列がどれだけランク落ちしているのか確認する必要がある．ランクは M_f の特異値の最大 gap から推定することができる．Algorithm 1 でまず特異値分解をするため，追加でランクの推定も行えばよい．

例 3
$n = 4, s = 2$ とし，f を以下の通りとする．f は *decomposable* な多項式の係数に平均 0, 分散 10^{-4} の正規分布からのノイズを加えたものである．

$$\begin{aligned} f =& 4.12149x^4 + 108.574x^3y + 0.0233258x^3 + 1072.59x^2y^2 + 0.45727x^2y + 0.00194601x^2 + 4709.29xy^3 + \\ & 3.01126xy^2 + 0.0273166xy - 0.0000256633x + 7753.7y^4 + 6.61033y^3 + 0.0893366y^2 - 0.000060814y. \end{aligned}$$

(f, n, s) から M_f を構成し，M_f の特異値を求めると，以下のようになる．

$$\begin{aligned} &\mathrm{SingularValue}(M_f) = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5), \\ &\text{where } \sigma_1 = 69138.7, \sigma_2 = 34540.1, \sigma_3 = 32288.9, \sigma_4 = 0.00147171, \sigma_5 = 0.000677187. \end{aligned}$$

特異値の gap は隣接特異値間の商で測る．最大 gap は $\sigma_3/\sigma_4 \approx 2.19397 \times 10^7$ であり，第 3 特異値と第 4 特異値の間で生じている．ゆえに $M_{\hat{f}}$ のランクを 3 と推定する．M_f のランクは 5 であるから，ランクは 2 落ちると推定できる．よって，(f, n, s) の代わりに s の約数 1 をとって，$(f, n, 1)$ に対し Algorithm 2 を実行すると，以下の通り近似 decomposition が計算できる．

$$\begin{aligned} u &= 8115.35x^4 + 6.8403x^3 + 0.091447x^2 - 0.0000639774x, \\ h &= 0.150119x + 0.988668y, \quad \|f - u \circ h\|_2 = 0.000339612. \end{aligned}$$

6　おわりに

SLRA problem に基づく多変数多項式の近似 decomposition アルゴリズムを提案した．Algorithm 2 は線形代数の計算が主のアルゴリズムとなっている．しかし，M_f のサイズは変数の数に対し指数的であるから，入力多項式によっては巨大な行列の操作が伴い，現状のままではメモリの圧迫や計算時間の増加は避けられない (例えば，10 変数 6 次の多項式 f に対する M_f は約 1GB の行列となる)．今後の課題として，Algorithm 1 に補間法を組み込み，巨大な行列の演算を回避する手法について考える必要がある．

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を受けたものである.

参 考 文 献

[1] Robert M. Corless, Mark Giesbrecht, David J. Jeffrey, and Stephen M. Watt. Approximate polynomial decomposition. In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC)*, pages 213–219. ACM, New York, 1999.

[2] Guillaume Chèze. A recombination algorithm for the decomposition of multivariate rational functions. *Math. Comp.*, 82(283):1793–1812, 2013.

[3] Sefa Demirtas and Alan V. Oppenheim. A functional composition approach to filter sharpening and modular filter design. *IEEE Trans. Signal Process.*, 64(14):3667–3676, 2016.

[4] Samaneh Ghandali, Bijan Alizadeh, Masahiro Fujita, and Zainalabedin Navabi. Automatic high-level data-flow synthesis and optimization of polynomial datapaths using functional decomposition. *IEEE Trans. Comput.*, 64(6):1579–1593, 2015.

[5] Mark Giesbrecht and John May. New algorithms for exact and approximate polynomial decomposition. In Dongming Wang and Lihong Zhi, editors, *Symbolic-numeric computation*, Trends Math., pages 99–112. Birkhäuser, Basel, 2007.

[6] Kosaku Nagasaka. Approximate GCD by relaxed NewtonSLRA algorithm. *ACM Commun. Comput. Algebra*, 55(3):97–101, 2021.

[7] Anatoliy P. Petravchuk and Oleksandr G. Iena. On closed rational functions in several variables. *Algebra Discrete Math.*, (2):115–124, 2007.

[8] Hiroshi Sekigawa. An approximation algorithm for the nearest decomposable polynomial in the Hamming distance. *ACM Commun. Comput. Algebra*, 57(3):119–122, 2023.

[9] Éric Schost and Pierre-Jean Spaenlehauer. A quadratically convergent algorithm for structured low-rank approximation. *Found. Comput. Math.*, 16(2):457–492, 2016.