数理解析研究所講究録
第1955巻 2015年 198-204

最小消去多項式を用いた一般固有ベクトル空間の基底計算法

小原功任*
KATSUYOSHI OHARA
金沢大学理工研究域
FACULTY OF MATHEMATICS AND PHYSICS,
INSTITUTE OF SCIENCE AND ENGINEERING,
KANAZAWA UNIVERSITY

田島慎一†
SHINICHI TAJIMA
筑波大学数理物質系
INSTITUTE OF MATHEMATICS,
FACULTY OF PURE AND APPLIED SCIENCES,
UNIVERSITY OF TSUKUBA

1 はじめに

体 $K=\mathbf{Q}$ 上の n 次正方行列 A を考えよう．いま，行列 A のある固有値 λ に注目する．λ の定義多項式 $f(x)$ は行列 A の特性多項式 $\chi_A(x)$ の既約因子となっている．行列 A をベクトル空間 $\mathbf{C}^n$ における線型変換とみて，線型変換 $A-\lambda$ のカーネル $E(\lambda)=\{\boldsymbol{v}\in\mathbf{C}^n \mid (A-\lambda)\boldsymbol{v}=\mathbf{0}\}$ を λ に関する固有ベクトル空間とよぶ．一方，線形変換 $A-\lambda$ によって不変な最大の真部分ベクトル空間 $V(\lambda)\subset\mathbf{C}^n$ を λ に関する一般固有ベクトル空間とよぶ．本研究では，行列 A の特性多項式 $\chi_A(x)$ が既知のとき，一般固有ベクトル空間 $V(\lambda)$ の基底の効率的に構成するアルゴリズムを与える．

数式処理システム上での効率的計算のために注意しておきたいことは，われわれが求める対象は，$\mathbf{C}$-ベクトル空間 $V(\lambda)$ の基底ではあるが，それを K における計算のみを用いて実現したいということである．多項式を要素として含む行列の演算や多項式の乗算・除算は，数のそれにくらべてずっと計算量が大きいことはよく知られている．したがって多項式を要素として含む行列の掃き出しなどは，効率的算法にはそぐわない．われわれはその目的を達成するための手法として，最小消去多項式を用いる．本研究は，一般固有ベクトル空間の構造，すなわち正方行列 A のジョルダン鎖を求める算法 ([4, 1, 2]) から発展したものである．

2 最小消去多項式とその性質

正方行列 $A\in M_n(K)$ の最小多項式 $\pi_A(x)$ は，イデアル $\{f(x)\in K[x] \mid f(A)=O\}\subset K[x]$ のモニックな生成元であって，どのような列ベクトル $\boldsymbol{u}\in K^n$ に対しても，$\pi_A(A)\boldsymbol{u}=\mathbf{0}$ を満たす．逆に列ベクトル $\boldsymbol{u}\in K^n$ に対し，イデアル $\mathrm{Ann}_{K[x]}(A,\boldsymbol{u})=\{f(x)\in K[x] \mid f(A)\boldsymbol{u}=\mathbf{0}\}\subset K[x]$ を考え，そのモニックな生成元をベクトル $\boldsymbol{u}$ に関する A の**最小消去多項式**と呼び，$\pi_{A,\boldsymbol{u}}(x)$ で表わす．第 i 基本ベクトル $\boldsymbol{e}_i$ に関する最小消去多項式 $\pi_{A,i}(x)=\pi_{A,\boldsymbol{e}_j}(x)$ を**第 i 基本最小消去多項式**と呼ぶ．その定義から，次が従う．

*ohara@se.kanazawa-u.ac.jp
†tajima@math.tsukuba.ac.jp

補題 1. 最小消去多項式に関して次が成り立つ.

(1) $\pi_{A,\boldsymbol{u}}(x)$ は $\pi_A(x)$ を割りきる.

(2) すべての基本最小消去多項式の最小公倍多項式は最小多項式と一致する.

さらに，行列 A の固有値 λ に着目すると，次のことも容易に得られる.

補題 2. $f(x)$ を 固有値 λ の最小多項式とする．このとき

(1) 既約多項式 $f(x)$ について，$\pi_A(x) = f(x)^m h(x)$ ならば，$f(x)^m$ で割りきれる基本最小消去多項式が存在する.

(2) 既約多項式 $f(x)$ について，$\pi_{A,i}(x) = f(x)^m g(x)$ ならば，$\boldsymbol{p} = g(A)\boldsymbol{e}_i$ の最小消去多項式は $\pi_{A,\boldsymbol{p}} = f(x)^k$ である.

(3) $\Psi_f(A, \lambda E)(A - \lambda E) = f(A)$ を満たす対称多項式 $\Psi_f(x, y) \in K[x, y]$ が存在する.

3 一般固有ベクトル空間の性質

以下，固有値 λ の最小多項式 $f(x)$ について，$\pi_A(x) = f(x)^m h(x)$，$\gcd(f, h) = 1$ が成り立つとする．このとき，固有値 λ に付随する一般固有ベクトル空間は,

$$V(\lambda) = \{\boldsymbol{u} \in \mathbf{C}^n \mid (A - \lambda)^m \boldsymbol{u} = \boldsymbol{0}\}$$

であることに注意しよう．$V^{(k)}(\lambda) = \{\boldsymbol{u} \in \mathbf{C}^n \mid (A - \lambda E)^k \boldsymbol{u} = \boldsymbol{0}\}$，$(1 \leq k \leq m)$ と置くと，$V(\lambda)$ は,

$$E(\lambda) = V^{(1)}(\lambda) \subset V^{(2)}(\lambda) \subset \cdots \subset V^{(m)}(\lambda) = V(\lambda)$$

といった構造をもつことが分かる．この構造にそって基底を構成することが目標である.

一方，K-ベクトル空間

$$\ker f(A)^m = \{\boldsymbol{u} \in K^n \mid f(A)^m \boldsymbol{u} = \boldsymbol{0}\}$$

を考える．$\ker f(A)^m$ は次の構造をもつ.

$$\ker f(A) \subset \ker f(A)^2 \subset \cdots \subset \ker f(A)^m$$

最小消去多項式の定義から，$\pi_{A,\boldsymbol{p}}(x) = f(x)^k$ であることと，$\boldsymbol{p} \in \ker f(A)^k \setminus \ker f(A)^{k-1}$ であることは同値である．しかも $\boldsymbol{v} = \Psi_f(A, \lambda E)^k \boldsymbol{p}$ は，補題 2 より,

$$\boldsymbol{v} \in V^{(k)}(\lambda) \setminus V^{(k-1)}(\lambda)$$

を満たす．実際，$\ker f(A)^m$ と $V(\lambda)$ には次の関係がある.

補題 3. $\mathbf{C}$-ベクトル空間としての同型 $\ker f(A)^m \otimes \mathbf{C} \simeq V(\lambda)$ が存在する.

この補題より，一般固有ベクトル空間 $V(\lambda)$ の基底を構成するには,

(1) $\ker f(A)^m$ の基底を構成する.

(2) $V(\lambda)$ の基底を構成する.

の 2 段階で実行可能であることが分かる.

4 $\ker f(A)^m$ とクリロフ巡回部分空間

この節では，K-ベクトル空間 $\ker f(A)^m$ の構造を調べていくこととする．$\deg f(x) = d$ と置く．いま，$\boldsymbol{p} \in \ker f(A)^m \setminus \ker f(A)^{m-1}$ をとると，その最小消去多項式は $f(x)^m$ に等しい．A と $f(A)$ が可換であることから，$\boldsymbol{p}$, $A\boldsymbol{p}$, $A^2\boldsymbol{p}$, ... はすべて $\ker f(A)^m$ に属する．$\boldsymbol{p}$ が生成するクリロフ巡回部分空間

$$L_A(\boldsymbol{p}) = \sum_{i \geq 0} KA^i\boldsymbol{p} = K\boldsymbol{p} \oplus KA\boldsymbol{p} \oplus \cdots \oplus KA^{md-1}\boldsymbol{p} \subset \ker f(A)^m \subset K^n$$

を考えよう．$f(A)^k\boldsymbol{p} \in \ker f(A)^{m-k}$ に注意して，記号

$$S(\boldsymbol{q}) = K\boldsymbol{p} \oplus KA\boldsymbol{p} \oplus \cdots \oplus KA^{d-1}\boldsymbol{p}, \qquad (\boldsymbol{q} \in K^n)$$

を導入すると，直和分解

$$\begin{aligned} L_A(\boldsymbol{p}) &= S(\boldsymbol{p}) \oplus S(f(A)\boldsymbol{p}) \oplus S(f(A)^2\boldsymbol{p}) \oplus \cdots \oplus S(f(A)^{m-1}\boldsymbol{p}) \\ &= S_1(\boldsymbol{p}) \oplus S_2(\boldsymbol{p}) \oplus S_3(\boldsymbol{p}) \oplus \cdots \oplus S_m(\boldsymbol{p}) \end{aligned}$$

が得られる．ただし，$S_k(\boldsymbol{p}) = S(f(A)^{k-1}\boldsymbol{p})$ とする．しかも，

$$S_{m-k+1}(\boldsymbol{p}) \oplus \cdots \oplus S_m(\boldsymbol{p}) = L_A(f(A)^k\boldsymbol{p}) \subset \ker f(A)^k$$

であることも容易に分かる．つまりこの直和分解は $\ker f(A)^m$ の構造にそっている．また，$L_A(\boldsymbol{p}) = S_1(\boldsymbol{p}) \oplus L_A(f(A)\boldsymbol{p})$ であるから，$S_1(\boldsymbol{p})$ の基底を構成する手続きと，$L_A(f(A)\boldsymbol{p})$ の生成系を得る手続きが実現できれば，帰納的に，$L_A(\boldsymbol{p})$ の基底も構成できる．これは補題 2 から得られる $\boldsymbol{p} \in \ker f(A)^m \setminus \ker f(A)^{m-1}$ から出発して，$\ker f(A)^k$ の基底を有理数計算のみで得ることを意味する．

次に，基本最小消去多項式から $\ker f(A)^m$ の基底を構成する方法を述べる．すべての基本最小消去多項式とその既約分解が既知であるとし，$\pi_{A,i}(x) = f(x)^{m_i}g_i(x)$ と表す．$f(x)$ と $g_i(x)$ は互いに素であるとする．また，$\boldsymbol{p}_i = g_(A)\boldsymbol{e}_i$ としよう．すると，$\pi_{A,\boldsymbol{p}_i} = f(x)^{m_i}$ である．記号，$J_k = \{i \mid m_i = k\}$ を導入すると，添字集合の分解

$$\{1, 2, \ldots, n\} = J_0 \cup J_1 \cup \cdots \cup J_m$$

が得られる．線型変換 $f(A)^{m-1}$ による $\ker f(A)^m$ の像は $f(A)^{m-1}(\ker f(A)^m) = \sum_{i \in J_m} K\boldsymbol{p}_i$ である．このとき，完全系列

$$0 \longrightarrow \ker f(A)^m \xrightarrow{f(A)^{m-1}} f(A)^{m-1}(\ker f(A)^m) \xrightarrow{f(A)} 0$$

が存在するので，$\ker f(A)^m$ における $\ker f(A)^{m-1}$ の補空間の基底を求めるには，$f(A)^{m-1}(\ker f(A)^m)$ の基底を調べればよい．ベクトルの集合 $\{f(A)^{m-1}\boldsymbol{p}_i \mid i \in J_m\}$ に対して，掃出しを実行すると，添字のある部分集合 $J'_m \subset J_m$ により，$\{f(A)^{m-1}\boldsymbol{p}_i \mid i \in J'_m\}$ は $f(A)^{m-1}(\ker f(A)^m)$ の基底となる．よって，$\{\boldsymbol{p}_i \mid i \in J'_m\}$ が求める補空間の基底である．さらに，$\boldsymbol{p}_j$ $(j \in J_m \setminus J'_m)$ に対しては線形関係式

$$\left[f(A)^{m-1}\boldsymbol{p}_j + \sum_{i \in J'_m} c_{ji} f(A)^{m-1}\boldsymbol{p}_i \right] = f(A)^{m-1} \left[\boldsymbol{p}_j + \sum_{i \in J'_m} c_{ji}\boldsymbol{p}_i \right] = \boldsymbol{0}$$

が存在するということだから，$\boldsymbol{p}_j + \sum_{i \in J'_m} c_{ji}\boldsymbol{p}_i \in \ker f(A)^{m-1}$ であり，

$$\left\{ \boldsymbol{p}_j + \sum_{i \in J'_m} c_{ji}\boldsymbol{p}_i \mid j \in J_m \setminus J'_m \right\} \cup \left\{ \boldsymbol{p}_k \mid k \in J_{m-1} \right\}$$

が $\ker f(A)^{m-1}$ を張ることが分かる．よって，$\ker f(A)^m$ に対して行った手順が $\ker f(A)^{m-1}$ に対しても実行できる．これまでに述べた手続きを順番に繰り返すことで，

$$\ker f(A) \subset \ker f(A)^2 \subset \cdots \subset \ker f(A)^m$$

に対応する $\ker f(A)^m$ の基底が構成される．

5 一般固有ベクトル空間 $V(\lambda)$ の基底

前節までの議論で，$\ker f(A)^m$ の基底を構成できることが分かった．また，対応

$$\ker f(A)^k \setminus \ker f(A)^{k-1} \ni \boldsymbol{p} \mapsto \Psi_f(A, \lambda E)^k \boldsymbol{p} \in V^{(k)}(\lambda) \setminus V^{(k-1)}(\lambda)$$

により，一般固有ベクトルの構成法も分かっている．しかしながら，$\ker f(A)^m$ と $V(\lambda)$ は同じものではなく，係数拡大による同型 $\ker f(A)^m \otimes \mathbf{C} \simeq V(\lambda)$ であるので，$V(\lambda)$ の基底構成には注意を要する．このことを再びクリロフ巡回部分空間に戻って説明しよう．

直和分解 $L_A(\boldsymbol{p}) = S_1(\boldsymbol{p}) \oplus \cdots \oplus S_m(\boldsymbol{p})$ に注意しよう．成分 $S_m(\boldsymbol{p})$ は，$\boldsymbol{q} = f(A)^{m-1}\boldsymbol{p}$ とすれば，

$$S_m(\boldsymbol{p}) = S(\boldsymbol{q}) = \bigoplus_{i=0}^{d-1} KA^i\boldsymbol{q}$$

と表される．$\boldsymbol{q}$ に対応する固有ベクトル $\boldsymbol{v} = \Psi(\lambda E, A)\boldsymbol{q}$ を考えると，各一次元空間 $KA^i\boldsymbol{q}$ には，$\mathbf{C}A^i\boldsymbol{v} = \mathbf{C}\lambda^i\boldsymbol{v} = \mathbf{C}\boldsymbol{v}$ が対応するため，$\S_m(\boldsymbol{p}) \otimes \mathbf{C} \simeq \mathbf{C}\boldsymbol{v}$ なる同型が得られる．つまり係数拡大により，$\boldsymbol{q}, A\boldsymbol{q}, \ldots, A^{d-1}\boldsymbol{q}$ は同一視されることとなるので，係数拡大することは，巡回空間を考えることに対応する．よって，基底を構成する場合は，巡回空間の生成元の合併 $\bigcup S_1(\boldsymbol{q})$ について掃出しを行わなければならない．(最後に代表元を選ぶ)

基底に対応することが分かっている $\boldsymbol{p} \in \ker f(A)^k \setminus \ker f(A)^{k-1}$ が与えられているとき，次の手順で $V(\lambda)$ の基底に含まれるベクトルを求める．

(1) $\Psi_f(x,y)^i \mod f(y), (i = 1, \ldots, m)$ を漸化式で求めておく．

$$\Psi_f(x,y)^i \mod f(y) = \sum_{j=0}^{\deg f - 1} y^j a_{ij}(x)$$

(2) 次のベクトルを一般固有ベクトルとする．

$$\boldsymbol{v} = \Psi_f(A, \lambda E)^k \boldsymbol{p} = \sum_{j=0}^{\deg f - 1} \lambda^j a_{kj}(A)\boldsymbol{p}$$

最後のステップでは，行列多項式とベクトルの積を拡張ホーナー法で求める．

以上を整理すると，次のアルゴリズムが得られる．

アルゴリズム 1 (一般固有ベクトル空間の基底).
入力: A: 正方行列, $\chi_A(x)$: 特性多項式, $f(x)$: 固有値 λ の最小多項式.
出力: $V(\lambda)$ の基底 B

(1) 基本最小消去多項式 $\{\pi_{A,1}(x), \ldots, \pi_{A,n}(x)\}$ を計算.

(2) **for** $i = 1, \ldots, n$; **do**
$\pi_{A,i}(x) = f(x)^{m_i} g_i(x)$ かつ $\gcd(f(x), g_i(x)) = 1$ のとき,
$\boldsymbol{p}_i \leftarrow g_i(A)\boldsymbol{e}_i$
done

(3) $\{1, \ldots, n\} = J_0 \cup \cdots \cup J_m$, ここで $J_k = \{j \mid m_j = k\}$

(4) **for** $i = 1, \ldots, n$; **do**
for $k = 0, \ldots, m_i - 1$; **do**
$\boldsymbol{p}_i^{(k)} \leftarrow f(A)^k \boldsymbol{p}_i$
done
done

(5) $W_m \leftarrow \emptyset$
for $k = m, m-1, \cdots, 1$; **do**
$P' \leftarrow \{\boldsymbol{p}_i \mid i \in J_k\} \cup W_k$,
行列 $(f(A)^{k-1}\boldsymbol{u})_{\boldsymbol{u} \in P'}$ を掃出して,
$Q \leftarrow \{\boldsymbol{u} \in P' \mid f(A)^{k-1}\boldsymbol{u}$ は一次独立 $\}$
$W_{k-1} \leftarrow \{\boldsymbol{w} \in K^n \mid \boldsymbol{w} = \sum_{i=1}^n c_i \boldsymbol{p}_i \neq \boldsymbol{0},\ f(A)^{k-1}\boldsymbol{w} = \boldsymbol{0}\}$,
行列 $(\mathrm{Cycl}(f(A)^{k-1}\boldsymbol{u}))_{\boldsymbol{u} \in Q}$ を掃出して,
$R_i \leftarrow \{\boldsymbol{u} \in Q \mid \boldsymbol{u}$ は消去されなかった $\}$
done

(6) $B \leftarrow \bigcup_{i=1}^m \{\Psi_f(A, \lambda E)^k \boldsymbol{u} \mid \boldsymbol{u} \in R_i\}$

6 Example

例 1.

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ -5 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ -3 & 0 & 0 & 0 & 0 & 1 \\ 6 & 3 & -25 & -10 & -11 & -2 \end{pmatrix}, \qquad \chi_A(x) = f(x)^3, \quad \pi_A(x) = f(x)^2$$

ただし $f(x) = x^2 + x + 5$ である. このとき基本最小消去多項式は

$$\pi_{A,1}(x) = f(x)^2, \quad \pi_{A,2}(x) = f(x), \quad \pi_{A,3}(x) = \pi_{A,4}(x) = \pi_{A,5}(x) = \pi_{A,6}(x) = f(x)^2$$

で与えられる. $f(x)$ の共役な二つの根を λ_1, λ_2 とすると, A のジョルダン鎖は,

$$A \sim [J_2(\lambda_1) \oplus J_1(\lambda_1)] \oplus [J_2(\lambda_2) \oplus J_1(\lambda_2)]$$

となっている．また，$V(\lambda_1), V(\lambda_2)$ はまったく同一の構造を持ち，

$$\boldsymbol{v}_1 = \begin{pmatrix} 1 \\ \lambda_1 \\ 0 \\ 0 \\ 0 \\ 3 \end{pmatrix}, \quad \boldsymbol{v}_2 = \begin{pmatrix} 25\lambda_1 + 25 \\ -125 \\ -3\lambda_1 + 12 \\ 15\lambda_1 + 15 \\ -75 \\ 75 \end{pmatrix}, \quad \boldsymbol{v}_3 = \begin{pmatrix} \lambda_1 - 9 \\ -10\lambda_1 - 5 \\ 0 \\ -3 \\ -6\lambda_1 \\ 12\lambda_1 + 18 \end{pmatrix}$$

と置くと，$V(\lambda_1)$ の基底は $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3\}$ で与えられる．しかも，$V^{(1)}(\lambda_1) = \mathbf{C}\boldsymbol{v}_1 \oplus \mathbf{C}\boldsymbol{v}_2$ となっている．

例 2.

$$A = \begin{pmatrix} 2 & 1 & 1 & 0 & -8 & 4 \\ -11 & -3 & -2 & 1 & 46 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & -5 & -1 & -2 & -2 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}, \qquad \chi_A(x) = \pi_A(x) = f(x)^2 g(x)$$

ただし $f(x) = x^2 + x + 5$, $g(x) = x^2 + 1$ とする．このとき基本最小消去多項式は，

$$\pi_{A,1}(x) = \pi_{A,2}(x) = f(x), \quad \pi_{A,3}(x) = \pi_{A,4}(x) = f(x)^2, \quad \pi_{A,5}(x) = f(x)^2 g, \quad \pi_{A,6}(x) = g(x),$$

である．$f(x)$ の根をそれぞれ λ_1, λ_2 で，$g(x)$ の根をそれぞれ μ_1, μ_2 で表すとき，A のジョルダン鎖は，

$$A \sim J_2(\lambda_1) \oplus J_2(\lambda_2) \oplus J_1(\mu_1) \oplus J_1(\mu_2)$$

となっている．また，

$$\boldsymbol{v}_1 = \begin{pmatrix} \lambda_1 + 3 \\ -11 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \boldsymbol{v}_2 = \begin{pmatrix} 2\lambda_1 + 2 \\ -4\lambda_1 - 14 \\ \lambda_1 - 9 \\ -10\lambda_1 - 5 \\ 0 \\ 0 \end{pmatrix}, \quad \boldsymbol{v}_3 = \begin{pmatrix} 60\mu_1 - 32 \\ 0 \\ 0 \\ -30\mu_1 + 16 \\ 15\mu_1 - 8 \\ -8\mu_1 - 15 \end{pmatrix}$$

と置くと，$V(\lambda_1)$ の基底は $\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$, $V(\mu_1)$ の基底は $\{\boldsymbol{v}_3\}$ で与えられる．また，$V^{(1)}(\lambda_1) = \mathbf{C}\boldsymbol{v}_1$ である．

参 考 文 献

[1] 小原功任, 田島慎一: 最小消去多項式候補を用いた行列の一般固有空間の構造の計算法について, COE Lecture Note **49**(2013), Kyushu University, 113–118.

[2] 小原功任, 田島慎一: 最小消去多項式候補を用いた行列の一般固有空間の構造の計算アルゴリズム, 京都大学数理解析研究所講究録 **1907**(2014), 62–70.

[3] 小原功任, 田島慎一: 行列の最小消去多項式とその候補の計算法, 日本数学会 2013 年度年会, 代数学分科会講演アブストラクト.

[4] 田島慎一: 一般固有ベクトル空間の構造を求める計算法について京都大学数理解析研究所講究録 **1843**(2013), 146–154.

[5] 照井章, 田島慎一: 行列の最小消去多項式候補を利用した固有ベクトル計算 (III), 京都大学数理解析研究所講究録 **1907**(2014), 50–61.

[6] K. Ohara, S. Tajima, A. Terui: Developing linear algebra packages on Risa/Asir for eigenproblems, The proceedings of ICMS 2014, Lecture Notes in Computer Science **8592**(2014), 321–324.

[7] S. Tajima, K. Ohara, A. Terui: An extension and efficient calculation of the Horner's rule, The proceedings of ICMS 2014, Lecture Notes in Computer Science **8592**(2014), 346–351.