行列の最小消去多項式候補を用いた固有ベクトル計算(II)

田島, 慎一
筑波大学数理物質系

照井, 章
筑波大学数理物質系

出版情報：COE Lecture Note. 49, pp.119-127, 2013-08-09. 九州大学マス・フォア・インダストリ研究所

行列の最小消去多項式候補を用いた固有ベクトル計算 (II)
Calculating eigenvectors of matrices using candidates for minimal annihilating polynomials II

田島 慎一*

Shinichi Tajima

筑波大学 数理物質系

Faculty of Pure and Applied Sciences, University of Tsukuba

照井　章†

Akira Terui

筑波大学 数理物質系

Faculty of Pure and Applied Sciences, University of Tsukuba

Abstract

Based on analysis of the residues of the resolvent, we have proposed an efficient algorithm for calculating eigenvector(s) of matrices. Our algorithm uses candidates for minimal annihilating polynomials, and the elements in eigenvector are represented as a polynomial in eigenvalue represented as a variable, thus we do not need to find eigenvalues by solving the characteristic equation. Whereas the previous algorithm calculates an eigenvector of the eigenvalue whose multiplicity is equal to one, the present algorithm extends the restriction such that we are now able to calculate eigenvector of eigenvalue whose multiplicity in the characteristic equation is greater than one under certain conditions.

1　はじめに

これまでに，我々は，レゾルベントの留数解析に基づき，行列の固有ベクトルを効率的に計算する算法を提案した [5]．我々の算法は，行列の最小消去多項式候補を用いるものであり，固有ベクトルの成分は固有値を変数とする多項式で表されるため，行列の特性多項式を解くことによる固有値の直接計算が不要であるという特徴をもつ．最小消去多項式候補の算法は，著者（田島）らによるレゾルベントの留数解析に基づく効率的な算法が提案されている [4]．また，我々は，この固有ベクトル算法を並列処理を用いて効率化する実装も提案している [3]．

本稿では，これまでに提案した固有ベクトル算法の拡張を提案する．これまでに提案した算法は，着目する固有値の重複度が 1 の場合に限られたが，本稿で提案する算法は，着目する固有値に属する一般固有ベクトル空間が，固有ベクトル空間に等しいという条件下で，着目する固有値の特性方程式における重複度が 1 よりも大きい場合にも固有ベクトルを計算可能にするものである．

*tajima@math.tsukuba.ac.jp

†terui@math.tsukuba.ac.jp

以下，本稿では次の内容を述べる．第 2 章では，問題設定および本稿における仮定と目的を説明する．第 3 章では，基本最小消去多項式候補がすべて真の基本最小消去多項式に等しいとあらかじめわかっている場合の固有ベクトルの算法を述べる．第 4 章では，基本最小消去多項式候補がすべて真の基本最小消去多項式に一致するかどうかが不明な場合の固有ベクトルの算法を述べる．この場合には “行列 Horner 法” を用いることにより，先に固有ベクトル候補を計算してから，基本最小消去多項式候補が真の最小消去多項式に一致するかを検査ことで，固有ベクトルをより効率的に計算可能にする．

2 問題設定

2.1 前置き (Preliminaries)

行列 A を有理数体 $\mathrm{K}=\mathbb{Q}$ 上の n 次正方行列とし，E_n を n 次単位行列とする．A の特性多項式 $\chi_A(\lambda)$ は次式の形で，整数上の既約因数分解があらかじめ求められているものとする．

$$\chi_A(\lambda)=f_1(\lambda)^{m_1}f_2(\lambda)^{m_2}\cdots f_p(\lambda)^{m_p}\cdots f_q(\lambda)^{m_q}. \tag{1}$$

本稿で提案するアルゴリズムの目的は，式 (1) のある既約因子 $f_p(\lambda)$ $(1\leq p\leq q)$ に対し，$f_p(\alpha)=0$ をみたす A の固有値 $\lambda=\alpha$ に属する固有ベクトルを求めることである．なお，本稿では $m_p\geq 1$ $(p=1,\ldots,q)$ とする．

$\boldsymbol{e}_j={}^t(0,\ldots,0,1,0,\ldots,0)$ を，第 j 成分が 1 に等しい n 次単位ベクトルとし，列のインデックスを $J=\{1,2,\ldots,n\}$ とする．n 次列ベクトル $\boldsymbol{v}$ に対し，A における $\boldsymbol{v}$ の最小消去多項式 $p(\lambda)$ は，イデアル $\{p(\lambda)\mid p(A)\boldsymbol{v}=\boldsymbol{0}\}$ のモニックな生成元として定義される．A における $\boldsymbol{e}_j$ に対する最小消去多項式を $\pi_{A,j}(\lambda)$ とするとき，$\pi_{A,j}(\lambda)$ は

$$\pi_{A,j}(\lambda)=f_1(\lambda)^{l_{j,1}}f_2(\lambda)^{l_{j,2}}\cdots f_p(\lambda)^{l_{j,p}}\cdots f_q(\lambda)^{l_{j,q}},\quad 0\leq l_{j,p}\leq m_p,\quad j\in J \tag{2}$$

と表される．

本稿では，固有ベクトルの計算に $\boldsymbol{e}_j$ の “最小消去多項式候補” $\pi'_{A,j}(\lambda)$ を用いる．$\pi'_{A,j}(\lambda)$ は

$$\pi'_{A,j}(\lambda)=f_1(\lambda)^{l'_{j,1}}f_2(\lambda)^{l'_{j,2}}\cdots f_p(\lambda)^{l'_{j,p}}\cdots f_q(\lambda)^{l'_{j,q}} \tag{3}$$

と表される．ここに，我々の $\pi'_{A,j}(\lambda)$ の求め方より，$\pi'_{A,j}(\lambda)$ の各既約因子の多重度は $0\leq l'_{j,p}\leq l_{j,p}$ を満たすことに注意する．

以下，$j\in J$ に対し，$\pi_{A,j}(\lambda)$ を A の “基本最小消去多項式”， $\pi'_{A,j}(\lambda)$ を A の “基本最小消去多項式候補” と呼ぶことにする．また，$f_p(\lambda)$ に対し，2 変数多項式 $\psi_p(x,y)$ を

$$\psi_p(x,y)=\frac{f_p(x)-f_p(y)}{x-y}. \tag{4}$$

で定める．このとき，$\psi_p(x,y)$ は変数 y に関して $\deg(f_p)-1$ 次の多項式であることに注意する．

以下では，ベクトル空間 $V=\mathrm{K}^n$ の有限部分集合 $S=\{\boldsymbol{v}_1,\ldots,\boldsymbol{v}_r\}$ に対し，S を含む V の最小の部分空間を $\mathrm{Span}(S)$ で表す．

2.2 仮定と目的

本稿では，行列 A とその特性多項式 $\chi_A(\lambda)$, $\chi_A(\lambda)$ の因数分解 (1)，A の基本最小消去多項式候補 (3) が与えられているもとで，$\chi_A(\lambda)$ の因子 $f_p(\lambda)$（および $f_p(\lambda)$ の零点である A の固有値 $\lambda=\alpha$）に着目する．

$f_p(\lambda)$ に対し，$l'_{j,p}$ $(j=1,\ldots,n)$ の最大値は 1 に等しい，すなわち

$$l'_p := \max_{j\in J}\{l'_{j,p}\} = 1$$

と仮定する．

注意 1
A の基本最小消去多項式 (2) に対し，$l_p = \max_{j\in J}\{l_{j,p}\}$ とおく．このとき，A の固有値 $\lambda=\alpha$ で $f_p(\alpha)=0$ をみたすものに対し，$l_p = 1$ ならば，またそのときに限り，固有値 α に属する一般固有ベクトル空間は固有ベクトル空間に等しい．∎

我々が本稿で提案する固有ベクトル算法の目的は，$f_p(\alpha)=0$ をみたす A の固有値 α に着目し，($l_p = l'_p$ を確かめた上で）固有値 α に属する固有ベクトルの（各成分を α の多項式として表した）表現をすべて求めることである．

3 基本最小消去多項式候補がすべて真の基本最小消去多項式に等しい場合

3.1 固有ベクトルの表現

まず，式 (3) の基本最小消去多項式候補 $\pi'_{A,j}(\lambda)$ がすべて，式 (2) の真の基本最小消去多項式 $\pi_{A,j}(\lambda)$ に等しい場合を扱う．

各 $\pi_{A,j}(\lambda)$ における $f_p(\lambda)$ の多重度 $l_{j,p}$ に着目する．仮定より $l_p = \max_{j\in J}\{l_{j,p}\} = 1$ $(J=\{1,\ldots,n\})$ であるので，$l_{j,p}$ は 1 または 0 に等しい．このとき，インデックスの集合 J を

$$J_0 = \{i\in J \mid l_{j,p}=0\},\quad J_1 = \{i\in J \mid l_{j,p}=1\},\quad J = J_0\cup J_1$$

と分割する．そして，$j\in J$ に対し，多項式 $g_j(\lambda)$ を，

$$g_j(\lambda) = \begin{cases} \pi_{A,j}(\lambda) & \text{for} \quad j\in J_0, \\ \pi_{A,j}(\lambda)/f_p(\lambda) & \text{for} \quad j\in J_1 \end{cases}$$

で定義する．このとき，すべての $j\in J$ に対し，$g_j(\lambda)$ と $f_p(\lambda)$ は互いに素であることに注意する．

$j\in J_1$ に対し，ベクトル $\boldsymbol{v}_j$ を

$$\boldsymbol{v}_j = g_j(A)\boldsymbol{e}_j \tag{5}$$

で定義する．このとき，次の命題が成り立つ．

命題 1
$j\in J_1$ とし，α を $f_p(\alpha)=0$ をみたす A の固有値とする．式 (4) の $\psi_p(x,y)$ および式 (5) の v_j に対し，ベクトル $\psi_p(A,\lambda E)\boldsymbol{v}_j$ に $\lambda=\alpha$ を代入したベクトルは A の固有値 α に属する固有ベクトルである．

証明 式 (4) より $f_p(x)-f_p(y) = (x-y)\psi_p(x,y)$. よって $\psi_p(A,\lambda E)\boldsymbol{v}_j$ を考えると

$$(A-\lambda E)(\psi_p(A,\lambda E)\boldsymbol{v}_j) = (f_p(A)-f_p(\lambda E))\boldsymbol{v}_j.$$

が成り立つ．ここで $\lambda=\alpha$ を代入すると，$f_p(\alpha)=0$ より

$$(A-\alpha E)(\psi_p(A,\alpha E)\boldsymbol{v}_j) = f_p(A)\boldsymbol{v}_j = f_p(A)g_j(A)\boldsymbol{e}_j = \pi_{A,j}(A)\boldsymbol{e}_j = \boldsymbol{0}$$

を得る．∎

$\deg(f_p(\lambda)) = d_p = d$ とおき，$\alpha_1, \alpha_2, \ldots, \alpha_d$ を $f_p(\lambda)$ の相異なる零点とするとき，命題 1 より，$i = 1, \ldots, d$, $j \in J_1$ に対し，ベクトル $\psi_p(A, \alpha_i E)\boldsymbol{v}_j$ はすべて A の固有値 α_i に属する固有ベクトルを表す．すなわち，$j \in J_1$ に対し，$\psi_p(A, \lambda E)\boldsymbol{v}_j$ なるベクトルを 1 個求めれば，変数（記号）$\alpha_1, \alpha_2, \ldots, \alpha_d$ で表される $d = \deg(f_p)$ 個の固有値に属する固有ベクトルをすべて構成したことになる．

3.2 $f_p(\alpha) = 0$ をみたすすべての固有値に属する固有ベクトル空間（の基底）の構成

前節では，$j \in J_1$ に対し，$f_p(\alpha) = 0$ をみたす A の固有値 α に属する合計 $d = \deg(f_p)$ 個の固有ベクトルを構成する方法を示した．ところで，式 (1) より，$f_p(\alpha) = 0$ をみたす A の固有値 α の重複度は m_p である．f_p は K 上の既約多項式であり，$\deg(f_p) = d_p = d$ より，方程式 $f_p(\lambda) = 0$ は d 個の異なる根をもつ．それらの根を $\alpha_1, \ldots, \alpha_d$ とおくと，$i = 1, \ldots, d$ に対し，各 $\lambda = \alpha_i$ に属する固有ベクトル空間（これを F_{p,α_i} とおく）は m_p 次元なので，$f_p(\alpha) = 0$ をみたすすべての固有値に属する固有ベクトル空間（これを F_p とおく）の次元は $d_p m_p = dm_p$ となる．本節では，前節までの議論を踏まえ，固有ベクトル空間 F_p の基底をなす dm_p 個の固有ベクトルを計算する方法を導く．

$V = \mathrm{Span}(\boldsymbol{v}_j \mid j \in J_1)$ とする（$\boldsymbol{v}_j$ の定義は (5) を参照）．さらに，$\boldsymbol{0} \neq \boldsymbol{v}$ なる $\boldsymbol{v} \in V$ に対し，$\psi_p(A, \lambda E)\boldsymbol{v} \neq 0$ を考える．このとき，$f_p(\alpha) = 0$ をみたす α を λ に代入すると，命題 1 より

$$(A - \alpha E)\psi_p(A, \alpha E)\boldsymbol{v} = (f_p(A) - f_p(\alpha E))\boldsymbol{v} = f_p(A)\boldsymbol{v} = \boldsymbol{0}$$

が成り立つ.（ここで，$f_p(\lambda)$ は A における $\boldsymbol{v}$ の最小消去多項式であることに注意する.）すなわち，$\psi_p(A, \alpha E)\boldsymbol{v}$ は A の固有値 α に属する固有ベクトルである．よって，固有ベクトル空間 F_p の基底をなす dm_p 個の固有ベクトルは，K^n の部分空間 V から m_p 個のベクトル

$$\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_{m_p} \tag{6}$$

を適当に選び，$k = 1, 2, \ldots, m_p$ に対し，ベクトル $\psi_p(A, \lambda E)\boldsymbol{w}_k$ が

$$F_p = \mathrm{Span}(\psi_p(A, \alpha_i)\boldsymbol{w}_k \mid i = 1, \ldots, d,\ k = 1, \ldots, m_p) \tag{7}$$

をみたす，すなわち $\psi_p(A, \alpha_i)\boldsymbol{w}_k$ $(k = 1, 2, \ldots, m_p)$ が一次独立になるように構成すればよいことがわかる．では，この条件を満たすような式 (6) のベクトル $\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_{m_p}$ の選択をどのように行えばよいだろうか?

$f_p(\lambda)$ が A における $\boldsymbol{v}$ の最小消去多項式であることから，ベクトル $\boldsymbol{v}$, $A\boldsymbol{v}$, $A^2\boldsymbol{v}$, $\ldots$, $A^{d-1}\boldsymbol{v}$ は一次独立である．そこで，$\boldsymbol{v} \in V$ に対し

$$L_A(\boldsymbol{v}) = \mathrm{Span}(\boldsymbol{v}, A\boldsymbol{v}, A^2\boldsymbol{v}, \ldots, A^{d-1}\boldsymbol{v})$$

とおく．このとき，次の命題が成り立つ．

命題 2
$\boldsymbol{u}, \boldsymbol{w} \in V$（ただし $\boldsymbol{u}, \boldsymbol{v} \neq \boldsymbol{0}$）とする．このとき，以下は同値:

1. $\mathrm{Span}(\psi_p(A, \alpha_i)\boldsymbol{u} \mid i = 1, \ldots, d) = \mathrm{Span}(\psi_p(A, \alpha_i)\boldsymbol{w} \mid i = 1, \ldots, d)$,
2. $L_A(\boldsymbol{u}) = L_A(\boldsymbol{w})$,
3. $\boldsymbol{w} \in L_A(\boldsymbol{u})$,
4. $\boldsymbol{u} \in L_A(\boldsymbol{w})$.

証明 $\boldsymbol{u} \in V$ に対し，上記より $\boldsymbol{u}$, $A\boldsymbol{u}$, $A^2\boldsymbol{u}$, $\ldots$, $A^{d-1}\boldsymbol{u}$ は一次独立．また $k = 0, \ldots, d-1$ に対し

$$\psi_p(A, \lambda E)(A^k \boldsymbol{u}) = A^k(\psi_p(A, \lambda E)\boldsymbol{u})$$

が成り立つ．ところが，$f_p(\alpha) = 0$ をみたす A の固有値 α に対し，$\psi_p(A, \alpha E)\boldsymbol{u}$ は α に属する A の固有ベクトルであるので，$k = 0, \ldots, d-1$ に対し

$$\psi_p(A, \alpha E)(A^k \boldsymbol{u}) = A^k(\psi_p(A, \alpha E)\boldsymbol{u}) = \alpha^k(\psi_p(A, \alpha E)\boldsymbol{u}) \tag{8}$$

が成り立つ．すなわち，$\boldsymbol{0} \neq \boldsymbol{w} \in L_A(\boldsymbol{u})$ に対し，$\psi_p(A, \alpha E)\boldsymbol{w}$ は $\psi_p(A, \alpha E)\boldsymbol{u}$ のスカラー倍に過ぎないことがわかる．よって 3. と 1. は同値．

一方，$\boldsymbol{w}$, $A\boldsymbol{w}$, $A^2\boldsymbol{w}$, $\ldots$, $A^{d-1}\boldsymbol{w}$ についても (8) と同様に

$$\psi_p(A, \alpha E)(A^k \boldsymbol{w}) = A^k(\psi_p(A, \alpha E)\boldsymbol{w}) = \alpha^k(\psi_p(A, \alpha E)\boldsymbol{w})$$

が成り立つ．$\psi_p(A, \alpha E)\boldsymbol{u}$ も $\psi_p(A, \alpha E)\boldsymbol{w}$ のスカラー倍に過ぎないことに注意すると 3. と 4. が同値，ゆえに（3. および 4. と）2. も同値であることがわかる．∎

命題 2 より，式 (7) をみたすような式 (6) のベクトル $\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_{m_p} \in V$ として

$$V = L_A(\boldsymbol{w}_1) \oplus L_A(\boldsymbol{w}_2) \oplus \cdots \oplus L_A(\boldsymbol{w}_{m_p})$$

をみたす $\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_{m_p}$ を選べばよいことがわかる．

3.3 固有ベクトル計算の手順

前節までの議論を踏まえ，基本最小消去多項式候補 $\pi'_{A,j}(\lambda)$ がすべて真の基本最小消去多項式 $\pi_{A,j}(\lambda)$ に一致していることがわかっている場合に、$f_p(\alpha) = 0$ をみたす A の固有値 α に属する固有ベクトル（空間の基底）を計算する方法を以下の通り示す．

アルゴリズム **1**
(基本最小消去多項式候補がすべて真の基本最小消去多項式に一致していることがわかっている場合の固有ベクトルの算法)

[Step 1] $J = \{1, 2, \ldots, n\}$ を

$$J_0 = \{j \in J \mid l_{j,p} = 0\}, \quad J_1 = \{j \in J \mid l_{j,p} = 1\}, \quad J_0 \cup J_1 = J$$

に分割する．

[Step 2] $j \in J_1$ に対し $\boldsymbol{v}_j = g_j(A)\boldsymbol{e}_j$ を計算する．

[Step 3] $V = \mathrm{Span}(\boldsymbol{v}_j \mid j \in J_1\}$ の基底（ベクトル）

$$\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{dm_p}\} = B$$

を，$\{\boldsymbol{v}_j \mid j \in J_1\}$ に対する掃き出し法によって求める．

[Step 4] 1. V の基底ベクトルの集合 B から最も “単純な” 形のベクトルを選び，これを $\boldsymbol{u}_1$ とする．これに対し

$$L_A(\boldsymbol{u}_1) = \mathrm{Span}(\boldsymbol{u}_1, A\boldsymbol{u}_1, \ldots, A^{d-1}\boldsymbol{u}_1)$$

を計算し，掃き出し法で $L_A(\boldsymbol{u}_1)$ の基底 B_1 を求める．

2. B の要素であり，かつ $L_A(\boldsymbol{u}_1)$ に属さないものから最も “単純な” 形のベクトルを選び，これを $\boldsymbol{u}_2$ とする．これに対し

$$L_A(\boldsymbol{u}_2) = \mathrm{Span}(\boldsymbol{u}_2, A\boldsymbol{u}_2, \ldots, A^{d-1}\boldsymbol{u}_2)$$

を計算し，さらに $L_A(\boldsymbol{u}_1) \oplus L_A(\boldsymbol{u}_2)$ に掃き出し法を適用し，$L_A(\boldsymbol{u}_1) \oplus L_A(\boldsymbol{u}_2)$ の基底 B_2 を求める．

3. B の要素であり，かつ $L_A(\boldsymbol{u}_1) \oplus L_A(\boldsymbol{u}_2)$ に属さないものから最も “単純な” 形のベクトルを選び，これを $\boldsymbol{u}_3$ とする．これに対し

$$L_A(\boldsymbol{u}_3) = \mathrm{Span}(\boldsymbol{u}_3, A\boldsymbol{u}_3, \ldots, A^{d-1}\boldsymbol{u}_3)$$

を計算し，さらに $L_A(\boldsymbol{u}_1) \oplus L_A(\boldsymbol{u}_2) \oplus L_A(\boldsymbol{u}_3)$ に掃き出し法を適用し，$L_A(\boldsymbol{u}_1) \oplus L_A(\boldsymbol{u}_2) \oplus L_A(\boldsymbol{u}_3)$ の基底 B_3 を求める．

4. 以下，同様にして，$k = 4, \ldots, m_p - 1$ に対し，$L_A(\boldsymbol{u}_1) \oplus \cdots \oplus L_A(\boldsymbol{u}_k)$ の基底 B_k を求める．

5. 最後に，B の要素であり，かつ $L_A(\boldsymbol{u}_1) \oplus \cdots \oplus L_A(\boldsymbol{u}_{m_p-1})$ に属さないものから最も “単純な” 形のベクトルを選び，これを $\boldsymbol{u}_{m_p}$ とおく．このステップにおいては，$L_A(\boldsymbol{u}_{m_p})$ 等の計算は不要である点に注意する．

[Step 5] 上のステップで得られた $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{m_p}$ に対し

$$\psi_p(A, \lambda E)\boldsymbol{u}_k, \quad k = 1, \ldots, m_p$$

を計算する．これが求める固有ベクトルを与える．∎

4 基本最小消去多項式候補がすべて真の基本最小消去多項式に一致するかどうかが不明な場合

4.1 基本的なアルゴリズム

これ以降では，式 (3) の基本最小消去多項式候補 $\pi'_{A,j}(\lambda)$ が与えられているが，これらすべてが式 (2) の真の基本最小消去多項式 $\pi_{A,j}(\lambda)$ に一致するかどうかがまだ不明であるとする．ほとんどの場合 $\pi'_{A,j}(\lambda) = \pi_{A,j}(\lambda)$ $(i \in J)$ が成り立つことが期待できるが，何らかの方法で $\pi'_{A,j}(\lambda)$ $(i \in J)$ が真の最小消去多項式を与えていることを確かめる必要がある．

そこで，上述のアルゴリズム 1 に，すでに与えられている基本最小消去多項式候補 $\pi'_{A,j}(\lambda)$ が真の基本最小消去多項式に等しいかどうかを検査する計算を加えたアルゴリズムを以下の通り示す．

アルゴリズム **2**
(基本最小消去多項式候補が真の基本最小消去多項式に一致しているかどうかの検査を固有ベクトルの算法)

[Step 1] $J'_0 = \{j \in J \mid l'_{j,p} = 0\}$, $J'_1 = \{j \in J \mid l'_{j,p} = 1\}$ とおく．仮定より $\max\{l'_{j,p} = 1 \mid i \in J\} = 1$ であるので $J'_0 \cup J'_1 = J$ が成り立つ．

各 $j \in J'_0$ に対し $\pi'_{A,j}(\lambda) = g_j(\lambda)$ （$g_j(\lambda)$ は $f_p(\lambda)$ と互いに素）と表せる．そこで，$j \in J'_0$ に対し $g_j(A)\boldsymbol{e}_j$ を計算し，$g_j(A)\boldsymbol{e}_j = \boldsymbol{0}$ が成り立つことを確かめる．

[Step 2] $j \in J_1'$ に対し $\boldsymbol{v}_j = g_j(A)\boldsymbol{e}_j$ を計算する．(ここに，$\pi'_{A,j}(\lambda) = f_p(\lambda)g_j(\lambda)$, g_j は f_p と互いに素.)

ここで，基本最小消去多項式候補が真の基本最小消去多項式に一致するかどうかを以下の手順で確かめる．$j \in J_1'$ に対し，整数 c_j を無作為に選び，$\boldsymbol{v} = \sum_{j \in J_1'} c_j \boldsymbol{v}_j$ とおき，

$$f_p(A)\boldsymbol{v} = \boldsymbol{0} \tag{9}$$

が成り立つことを確かめる．

もし $f_p(A)\boldsymbol{v} \neq \boldsymbol{0}$ ならば，少なくとも 1 つのベクトル $\boldsymbol{v}_j$ $(j \in J_1')$ が $f_p(A)$ で $\boldsymbol{0}$ に写らないことがわかる．すなわち，基本最小消去多項式 $\pi'_{A,j}(\lambda)$ で真の基本最小消去多項式 $\pi_{A,j}(\lambda)$ に一致しないものが存在することがわかる．

以下のステップは，式 (9) が成り立つ場合に実行する．

[Step 3] $V = \mathrm{Span}(\boldsymbol{v}_j \mid j \in J_1'\}$ の基底（ベクトル）

$$\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{dm_p}\} = B$$

を，$\{\boldsymbol{v}_j \mid j \in J_1'\}$ に対する掃き出し法によって求める．

[Step 4]

1. V の基底ベクトルの集合 B から最も "単純な" 形のベクトルを選び，これを $\boldsymbol{u}_1$ とする．これに対し，$\boldsymbol{u}_1, A\boldsymbol{u}_1, \ldots, A^{d-1}\boldsymbol{u}_1$ を求めた上で，$f_p(A)\boldsymbol{u}_1 = \boldsymbol{0}$ を確かめる．もし $f_p(A)\boldsymbol{u}_1 = \boldsymbol{0}$ が成り立つ場合は
$$L_A(\boldsymbol{u}_1) = \mathrm{Span}(\boldsymbol{u}_1, A\boldsymbol{u}_1, \ldots, A^{d-1}\boldsymbol{u}_1)$$
を計算し，掃き出し法で $L_A(\boldsymbol{u}_1)$ の基底 B_1 を求める．
2. B の要素であり，かつ $L_A(\boldsymbol{u}_1)$ に属さないものから最も "単純な" 形のベクトルを選び，これを $\boldsymbol{u}_2$ とする．これに対し，$\boldsymbol{u}_2, A\boldsymbol{u}_2, \ldots, A^{d-1}\boldsymbol{u}_2$ を求めた上で，$f_p(A)\boldsymbol{u}_2 = \boldsymbol{0}$ を確かめる．もし $f_p(A)\boldsymbol{u}_2 = \boldsymbol{0}$ が成り立つ場合は
$$L_A(\boldsymbol{u}_2) = \mathrm{Span}(\boldsymbol{u}_2, A\boldsymbol{u}_2, \ldots, A^{d-1}\boldsymbol{u}_2)$$
を計算し，さらに $L_A(\boldsymbol{u}_1) \oplus L_A(\boldsymbol{u}_2)$ に掃き出し法を適用し，$L_A(\boldsymbol{u}_1) \oplus L_A(\boldsymbol{u}_2)$ の基底 B_2 を求める．
3. 以下，同様にして，$k = 3, \ldots, m_p - 1$ に対し，$L_A(\boldsymbol{u}_1) \oplus \cdots \oplus L_A(\boldsymbol{u}_k)$ の基底 B_k を求める．
4. 最後に，B の要素であり，かつ $L_A(\boldsymbol{u}_1) \oplus \cdots \oplus L_A(\boldsymbol{u}_{m_p-1})$ に属さないものから最も "単純な" 形のベクトルを選び，これを $\boldsymbol{u}_{m_p}$ とおく．そして $f_p(A)\boldsymbol{u}_{m_p}$ が成り立つことを確かめる．

[Step 5] 上のステップで得られた $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{m_p}$ に対し

$$\psi_p(A, \lambda E)\boldsymbol{u}_k, \quad k = 1, \ldots, m_p$$

を計算する．これらが求める固有ベクトルを与える．∎

注意 2

基本最小消去多項式候補が真の基本最小消去多項式に一致しているかどうかを検査する方法として，すべての $j \in J_1'$ に対し $\pi'_{A,j}(A)\boldsymbol{e}_j = f_p(A)\boldsymbol{v}_j = \boldsymbol{0}$ を求める方法が考えられる．しかしながら，この検査は，アルゴリズム 2 で与えた通り，$V = \mathrm{Span}(\boldsymbol{v}_j \mid j \in J_1')$ の基底 $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{m_p d}\}$ $(d = d_p)$ から選んだ m_p 個のベクトル $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{m_p}$ のみに対して $\pi'_{A,j}(A)\boldsymbol{b}_k = f_p(A)\boldsymbol{b}_k = \boldsymbol{0}$ を確かめれば十分である（なぜなら，命題 1, 2 より，$\boldsymbol{0} \neq \boldsymbol{w} \in L_A(\boldsymbol{u}_k)$ をみたすすべてのベクトル $\boldsymbol{w}$ に対し，$\boldsymbol{u}_k$ の最小消去多項式が $f_p(\lambda)$ であれば，$\boldsymbol{w}$ の最小消去多項式も $f_p(\lambda)$ になるからである）．これにより，最小消去多項式候補が真の最小消去多項式になることを確かめる手間が $1/d$ に抑えられたことになる．∎

4.2　アルゴリズムの効率化

アルゴリズム 2 は，以下の点で効率化が可能である．

1. [Step 1] および [Step 2] において $\boldsymbol{v}_j$ を求める計算は j 毎に独立した計算なので，並列化が可能である．

2. [Step 4] および [Step 5] に着目する．[Step 4] では，ある $\boldsymbol{u}_k$ に対し，$\boldsymbol{u}_k, A\boldsymbol{u}_k, \ldots, A^{d-1}\boldsymbol{u}_k$ を求めた上で，$f_p(A)\boldsymbol{u}_k = \boldsymbol{0}$ が成り立つことを確かめ，$L_A(\boldsymbol{u}_k) = \mathrm{Span}(\boldsymbol{u}_k, A\boldsymbol{u}_k, \ldots, A^{d-1}\boldsymbol{u}_k)$ の基底を求めている．ここで計算される $\boldsymbol{u}_k, A\boldsymbol{u}_k, \ldots, A^{d-1}\boldsymbol{u}_k$ を記憶しておくことで，[Step 5] の $\psi_p(A, \lambda E)\boldsymbol{u}_k$ の計算に再利用することが可能であるが，加算の回数が多くなる．

   ところが，[Step 5] の $\psi_p(A, \lambda E)\boldsymbol{u}_k$ の計算を “行列 Horner 法” を用いて行った後，Horner 法の計算をさらにもう 1 度行うことで $f_p(A)\boldsymbol{u}_k$ を計算できる（詳細は照井・田島 [5] を参照）．

ここでは，特に上記 2. を考慮することにより，アルゴリズム 2 を以下の形で効率化する．

アルゴリズム **3**
(基本最小消去多項式候補が真の基本最小消去多項式に一致しているかどうかの検査を固有ベクトルの算法: 改良版)

[Step 1], [Step 2], [Step 3] はアルゴリズム 2 と同一であるので省略．

[Step 4]

1. V の基底ベクトルの集合 B から最も “単純な” 形のベクトルを選び，これを $\boldsymbol{u}_1$ とする．$\psi_p(A, \lambda E)\boldsymbol{u}_1$ を計算し，メモリに保存する．この結果を用いて $f(A)\boldsymbol{u}_1 = \boldsymbol{0}$ を確かめる．もし $f_p(A)\boldsymbol{u}_1 = \boldsymbol{0}$ が成り立つ場合は
$$L_A(\boldsymbol{u}_1) = \mathrm{Span}(\boldsymbol{u}_1, A\boldsymbol{u}_1, \ldots, A^{d-1}\boldsymbol{u}_1)$$
を計算し，掃き出し法で $L_A(\boldsymbol{u}_1)$ の基底 B_1 を求める．

2. B の要素であり，かつ $L_A(\boldsymbol{u}_1)$ に属さないものから最も “単純な” 形のベクトルを選び，これを $\boldsymbol{u}_2$ とする．これに対し，$\psi_p(A, \lambda E)\boldsymbol{u}_2$ を計算し，メモリに保存する．この結果を用いて $f(A)\boldsymbol{u}_2 = \boldsymbol{0}$ を確かめる．もし $f_p(A)\boldsymbol{u}_2 = \boldsymbol{0}$ が成り立つ場合は
$$L_A(\boldsymbol{u}_2) = \mathrm{Span}(\boldsymbol{u}_2, A\boldsymbol{u}_2, \ldots, A^{d-1}\boldsymbol{u}_2)$$
を計算し，さらに $L_A(\boldsymbol{u}_1) \oplus L_A(\boldsymbol{u}_2)$ に掃き出し法を適用し，$L_A(\boldsymbol{u}_1) \oplus L_A(\boldsymbol{u}_2)$ の基底 B_2 を求める．

3. 以下，同様にして，$k = 3, \ldots, m_p - 1$ に対し，$\psi_p(A, \lambda E)\boldsymbol{u}_k$ を計算し，メモリに保存した上で，この結果を用いて $f(A)\boldsymbol{u}_k = \boldsymbol{0}$ を確かめる．もし $f_p(A)\boldsymbol{u}_k = \boldsymbol{0}$ が成り立つ場合は
$$L_A(\boldsymbol{u}_k) = \mathrm{Span}(\boldsymbol{u}_k, A\boldsymbol{u}_k, \ldots, A^{d-1}\boldsymbol{u}_k)$$
を計算し，さらに $L_A(\boldsymbol{u}_1) \oplus \cdots \oplus L_A(\boldsymbol{u}_k)$ に掃き出し法を適用し，基底 B_k を求める．

4. 最後に，B の要素であり，かつ $L_A(\boldsymbol{u}_1) \oplus \cdots \oplus L_A(\boldsymbol{u}_{m_p-1})$ に属さないものから最も “単純な” 形のベクトルを選び，これを $\boldsymbol{u}_{m_p}$ とおく．そして $\psi_p(A, \lambda E)\boldsymbol{u}_{m_p}$ を計算し，メモリに保存した上で，この結果を用いて $f_p(A)\boldsymbol{u}_{m_p} = \boldsymbol{0}$ が成り立つことを確かめる．

[Step 5] 上のステップで得られた $\psi_p(A, \lambda E)\boldsymbol{u}_k$ $(k = 1, \ldots, m_p)$ を A の固有ベクトルとして出力する．∎

5 まとめ

本稿では，レゾルベントの留数解析に基づき，行列の固有ベクトルを効率的に計算する算法として，我々がこれまでに提案した算法の拡張を提案した．これまでに提案した算法では，着目する固有値の重複度が 1 の場合に限られたが，本稿で提案する算法では，着目する固有値に属する一般固有ベクトル空間が，固有ベクトル空間に等しいという条件下で，着目する固有値の特性方程式における重複度が 1 よりも大きい場合にも固有ベクトルを計算可能にした．

実際の固有ベクトル算法としては，まず，基本最小消去多項式候補がすべて真の基本最小消去多項式に等しいとあらかじめわかっている場合の算法を提案し，次に基本最小消去多項式候補がすべて真の基本最小消去多項式に一致するかどうかが不明な場合の算法を提案した．そして，特に後者においては，“行列 Horner 法” を用いることにより，先に固有ベクトル候補を計算してから，基本最小消去多項式候補が真の最小消去多項式に一致するかどうかを検査することで，固有ベクトルをより効率的に計算可能にすることを示した．

現在の課題は以下の通りである．提案したアルゴリズム内には “基底ベクトルの集合から最も ‘単純な’ ベクトルを選ぶ” 手順があるが，“単純” の基準をどのようにとるかは今後の検討課題である．また，各基底ベクトルに対し，格子算法 ([1], [2]) などによるベクトルの簡約を行うことがその後の計算の効率化に結びつくか等についても今後検討の余地がある．

今後は，以上の課題とともに，第 4.2 節で述べたように，並列処理なども含めた固有ベクトル計算の効率化を計り，算法の実装と検証を行いたいと考えている．

参　考　文　献

[1] Murray R. Bremner. *Lattice Basis Reduction.* CRC Press, 2012.

[2] Phone Q. Nguyen and Brigitte Vallée, editors. *The LLL Algorithm.* Information Security and Cryptography. Springer, 2010.

[3] 田島慎一, 小原功任, 照井章. 行列 Horner 法の並列化の実装について. 数式処理研究の新たな発展, 数理解析研究所講究録. 京都大学数理解析研究所, 印刷中.

[4] 田島慎一, 奈良洸平. 最小消去多項式候補とその応用. *Computer Algebra — Design of Algorithms, Implementations and Applications*, 数理解析研究所講究録, 第 1815 巻, pp. 1–12. 京都大学数理解析研究所, 2012 年 10 月.

[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. *Computer Algebra — Design of Algorithms, Implementations and Applications*, 数理解析研究所講究録, 第 1815 巻, pp. 13–22. 京都大学数理解析研究所, 2012 年 10 月.