

Title	多項式を要素にもつ線形連立方程式の解法：その2 (数式処理研究の新たな発展)
Author(s)	讃岐, 勝
Citation	数理解析研究所講究録 (2015), 1930: 118-123
Issue Date	2015-01
URL	<a href="http://hdl.handle.net/2433/223549">http://hdl.handle.net/2433/223549</a>
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

# 多項式を要素にもつ線形連立方程式の解法：その 2

## Finding Solutions of Linear Equation within Polynomial Entries: Part II

讃岐 勝

MASARU SANUKI

筑波大学医学医療系 & 筑波大学附属病院総合臨床教育センター

FACULTY OF MEDICINE, UNIVERSITY OF TSUKUBA,

&

CENTER FOR MEDICAL EDUCATION AND TRAINING, UNIVERSITY OF TSUKUBA HOSPITAL \*

### Abstract

本稿では、多項式要素を持つ線形連立方程式の解法について考察を行う。

## 1 はじめに

多項式を要素に持つ行列に関する線形代数について、数式処理の分野ではそれほど研究がされていない。固有値計算 [YT93], 行列式計算など限られた用途によるものだけである。本稿では、標数 0 の数体  $\mathbb{K}$  を係数に持つ  $\ell$  変数多項式  $\mathbb{K}[\mathbf{u}]^{m \times n} = \mathbb{K}[u_1, \dots, u_\ell]^{m \times n}$  を要素に持つ次の線形連立方程式を考える。

$$A\mathbf{x} = \mathbf{b}. \quad (1)$$

ここで、 $A \in \mathbb{K}[\mathbf{u}]^{m \times n}$ ,  $\mathbf{b} \in \mathbb{K}[\mathbf{u}]^m$  である。このとき、解  $\mathbf{x} = \mathbf{c}$  の要素は一般に有理関数体  $\mathbb{K}(\mathbf{u})$  となる： $\mathbf{c} \in \mathbb{K}(\mathbf{u})^n$ 。分母が 0 にならないような有理関数体の部分体を考えると、この集合はべき級数環  $\mathbb{K}\{\mathbf{u}\}$  と同一視できる。そのため、特別な事情がない限り解は  $\mathbf{x} = \mathbf{c}$  の要素は  $\mathbb{K}\{\mathbf{u}\}$  に含まれるものと仮定する： $\mathbf{c} \in \mathbb{K}\{\mathbf{u}\}^n$ 。

多項式を要素とする行列を扱う場合、数値計算のように乗算・除算を繰り返す計算を行うと数式膨張を起こし、すぐに計算が破綻する。そのため、リフティング法や補間法によって数式膨張を避けて高速に計算する次の方法がとられることが多い。

- リフティング法: GCD 計算, 因数分解など小規模サイズの問題
- 補間法: 行列式計算など大規模なサイズの問題

近似 GCD を用いて画像補正を行う方法が提案されているが [LP97], その際に入力多項式の次数が 500 次を超えるような中規模・巨大サイズの近似 GCD 計算が必要となる。[LYZ10] では構造行列に対して補間法を FFT が適用できる形にして、高速に計算を行なっている。大規模な問題の場合、有効であることがわ

---

\*sanuki@md.tsukuba.ac.jp

かるが中規模の問題に対して有効であるかは、算法を吟味していないためよくわかっていない ([讃岐 11] では特殊な場合の計算量解析のみ行なっている).

本稿では任意に与えられた線形連立方程式 (1) に対する解法について、リフティング法および補間法を用いた方法を紹介し、計算量についても言及する. 本稿の内容は [讃岐 12a, 讃岐 12b] での報告を含む.

## 2 解法

### 2.1 リフティング法に基づく [Sanuki09]

数ベクトル  $\mathbf{s} = (s_1, \dots, s_\ell)^T \in \mathbb{K}^\ell$  に対して, イデアール  $I$  を  $I = \langle \mathbf{u} - \mathbf{s} \rangle = \langle u_1 - s_1, \dots, u_\ell - s_\ell \rangle$  で定義する.  $A \bmod I^{w+1} = (a_{i,j} \bmod I^{w+1})_{i,j}$ .  $I^{w+1}$  によって打ち切られた行列を  $A^{(w)} = A \bmod I^{w+1}$  と表し,  $A^{(w+1)}$  との差分を  $\delta A^{(w+1)}$  で表す:  $A^{(w+1)} = A^{(w)} + \delta A^{(w+1)}$ .

$A^{(0)}$  が正則のとき, リフティング法は次のように実行される (正則でない場合については 3 で述べる). まず,  $A^{(0)}\mathbf{x} = \mathbf{b}^{(0)}$  を解き, その解を  $\mathbf{x} = \mathbf{c}^{(0)}$  とする.

$k-1$  次まで構成できたと仮定する:  $\mathbf{x} \equiv \mathbf{c}^{(k)}$ .

$$A\mathbf{c}^{(k-1)} \equiv \mathbf{b} \pmod{I^k}. \quad (2)$$

このとき,  $A\mathbf{c}^{(k)} \equiv \mathbf{b} \pmod{I^{k+1}}$  をみたす  $\mathbf{c}^{(k)} = \mathbf{c}^{(k-1)} + \delta\mathbf{c}^{(k)}$  は次の式から計算する.

$$(A^{(0)} + \delta A^{(1)} + \dots + \delta A^{(k+1)})(\mathbf{c}^{(0)} + \delta\mathbf{c}^{(1)} + \dots + \delta\mathbf{c}^{(k+1)}) \equiv \mathbf{b} \pmod{I^{k+1}} \quad (3)$$

から全次数  $k+1$  の斉次項のみを取り出すことにより次を得る.

$$A^{(0)}\delta\mathbf{c}^{(k+1)} + \delta A^{(1)}\delta\mathbf{c}^{(k)} + \dots + \delta A^{(k+1)}\mathbf{c}^{(0)} = \delta\mathbf{b}^{(k+1)} \quad (4)$$

$$\delta\mathbf{c}^{(k+1)} = (A^{(0)})^{-1} \left( \delta\mathbf{b}^{(k+1)} - \sum_{i=1}^{k+1} \delta A^{(i)}\delta\mathbf{c}^{(k+1-i)} \right). \quad (5)$$

$A^{(0)}$  は数値行列であり, 逆行列の計算は容易である. また, リフティングを行う際に逆行列の計算は 1 回のみであり, その他に必要な計算は行列とベクトルの積およびベクトル同士の和である.

### 2.2 補間法に基づく

補間法に基づく方法は次のステップで計算される.

1. 補間点の個数  $R$  を計算
2.  $R$  個の補間点  $\mathbf{s}_i = (s_{i,1}, \dots, s_{i,\ell})$  を与えられた線形方程式  $A\mathbf{x} = \mathbf{b}$  に代入し, 数値要素の線形方程式を解く.

$$A|_{\mathbf{u}=\mathbf{s}_i} \mathbf{x} = \mathbf{b}|_{\mathbf{u}=\mathbf{s}_i}$$

このとき得られた解を  $\mathbf{x} = \mathbf{d}_i^{(0)} = (d_{i,1}^{(0)}, \dots, d_{i,m}^{(0)})^T \in \mathbb{K}^m$  とする. このとき  $A\mathbf{x} = \mathbf{b}$  の解  $\mathbf{x}$  の  $j$  番目の要素  $x_j$  は次の線形方程式のよって計算できる.

$$\begin{pmatrix} 1 & s_{1,1} & \cdots & s_{1,\ell} & s_{1,1}^2 & s_{1,1}s_{1,2} & \cdots & s_{1,\ell}^{k_\ell} \\ 1 & s_{2,1} & \cdots & s_{2,\ell} & s_{2,1}^2 & s_{2,1}s_{2,2} & \cdots & s_{2,\ell}^{k_\ell} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & s_{R,1} & \cdots & s_{R,\ell} & s_{R,1}^2 & s_{R,1}s_{R,2} & \cdots & s_{R,\ell}^{k_\ell} \end{pmatrix} \begin{pmatrix} q_j^{(0,0,\dots,0)} \\ q_j^{(1,0,\dots,0)} \\ \vdots \\ q_j^{(0,0,\dots,1)} \\ q_j^{(2,0,\dots,0)} \\ \vdots \\ q_j^{(1,1,\dots,0)} \\ \vdots \\ q_j^{(0,0,\dots,k_\ell)} \end{pmatrix} = \begin{pmatrix} c_{1,j} \\ c_{2,j} \\ \vdots \\ c_{R,j} \end{pmatrix}.$$

ただし,  $x_j = q_j^{(0,0,\dots,0)} + \sum_{(i_1,\dots,i_\ell)} q_j^{(i_1,\dots,i_\ell)} u_1^{i_1} \cdots u_\ell^{i_\ell}$  with  $q_j^{(i_1,\dots,i_\ell)} \in \mathbb{K}$  である.

### 3 リフティング法における悪条件性

$A^{(0)}\mathbf{x} = \mathbf{b}^{(0)}$  が可解でない場合, リフティング法による方法は破綻する. 破綻する場合は数値要素における線形代数から 1)  $A^{(0)}$  が特異な場合, 2)  $A^{(0)}$  が正則でないに限る.

#### 3.1 $A^{(0)}$ が特異なとき

$A^{(0)}$  の逆行列が存在しないため一般逆行列は存在する.  $A^{(0)}$  の一般逆行列  $(A^{(0)})^+$  とは次の性質を満たす行列である ( $A^{(0)}$  に逆行列が存在する場合も上の性質は満たされる).

$$(A^{(0)})^+ A^{(0)} (A^{(0)})^+ = (A^{(0)})^+ \quad (6)$$

$$A^{(0)} (A^{(0)})^+ A^{(0)} = A^{(0)} \quad (7)$$

$$\left( (A^{(0)})^+ A^{(0)} \right)^T = (A^{(0)})^+ A^{(0)} \quad (8)$$

$$\left( A^{(0)} (A^{(0)})^+ \right)^T = A^{(0)} (A^{(0)})^+ \quad (9)$$

$$(10)$$

逆行列と異なり一意性は満たされないことに注意が必要である. 一般逆行列の計算法には LU 分解を用いる方法, 特異値分解を用いる方法などがある [斉藤-牧野 96]. 一般逆行列を用いると方程式 (4) の解は次でかける.

$$\delta \mathbf{x} = (A^{(0)})^+ \delta \mathbf{s}^{(w)} - (E - (A^{(0)})^+ A^{(0)}) \delta \mathbf{s}^{(w)}.$$

ただし,  $\delta \mathbf{s}^{(w)} = \delta \mathbf{b}^{(w)} - \sum_{j=1}^w \delta A^{(j)} \delta \mathbf{x}^{(w-j)}$  である.

##### 3.1.1 初期値問題

リフティングを用いて得られた解は初期値  $\mathbf{c}^{(0)}$  と  $A^{(0)}$  の逆行列または一般逆行列によって決定する. 逆行列は一意に存在するので  $\mathbf{c}^{(0)}$  も一意に決定するためリフティングによって得られた  $\mathbf{c}^{(w)}$  は  $A\mathbf{x} = \mathbf{b}$  を満

たす。一方、一般逆行列を用いた方法では  $Ax = b$  が一意な解を持つとしても  $A^{(0)}x = b^{(0)}$  の解は無数個存在するので、リフティングの種となる  $d^{(0)}$  を  $c^{(0)} \equiv d^{(0)} \pmod{I}$  となるように選ぶ必要がある。

次の方法により初期値を決定する。  $A^{(0)}$  のランクを計算するとき  $r$  だけランクが落ちているとする。このとき、一般逆行列により得られた解  $d^{(0)}$  は  $r$  だけ自由度があり、  $r$  個のパラメータによって一般解を表現できる： $d^{(0)} + p_r$ 。このとき、  $\delta d^{(1)}$  はリフティング法の性質から  $p_r$  の次数が 1 であるベクトルで表現され、  $\delta d^{(w)}$  の場合についても同様に次数が 1 であるベクトルで表現される。もとの方程式の変数に値を入れることで  $r$  個のパラメータからなる線形連立方程式が得られ、多くの場合可解である。

### 例 1

次の連立方程式を解く。

$$\begin{pmatrix} 1+u & 2+u+v \\ 2+v & 4+v \end{pmatrix} x = \begin{pmatrix} 3+u+2u+2uv+u^2 \\ 6+4u-2v+2uv \end{pmatrix}.$$

行列  $A^{(0)}$  は特異でありランクは 1 である。上の方程式の解は  $c$  である。

$$c = \begin{pmatrix} -1+v \\ 2+u \end{pmatrix}.$$

特異値分解による一般逆行列を用いて  $A^{(0)}x = b$  を解くと  $d^{(0)} = (1, 1)^T$  が得られ一般解は次でかけることがわかる（ランクが 1 落ちるのでパラメータは 1 つである）。

$$d^{(0)} = \begin{pmatrix} 1-2a \\ 1+a \end{pmatrix}$$

与えられた方程式の変数に適当な値を代入すると、パラメータからなる線形方程式が得られ、適切な  $a = 1$  がすぐに得られる（一般の場合についても、パラメータからなる可解な線形方程式が得られる）。 ■

## 3.2 $A^{(0)}$ が零行列の場合

この場合、一般逆行列が存在しないため、  $A^{(0)}x = b^{(0)}$  からリフティングに必要な種を生成することができない。初期値  $c^{(0)}$  を次のように生成する。

まず、  $b^{(0)}$  が零ベクトルでない場合、  $A^{(0)}x = b^{(0)}$  の解は存在しないので  $b^{(0)} = 0$  の場合のみ考えれば良い。  $b^{(0)} = 0$  のとき、  $A^{(0)}x = b^{(0)}$  の解はベクトル空間に一致する。このため、次のように問題を一般化できる。  $A^{(w-1)} = 0$  かつ  $\delta A^{(w)} \neq 0$  の  $A$  を要素に持つ線形連立方程式を考える。  $b^{w-1} = 0$  であることも仮定する。このとき、  $\delta A^{(w)}x = \delta b^{(w)}$  の解は数値要素でありこの解を  $x = c^{(0)}$  とリフティングの種とする。実際の求め方については、補間点  $u = s \in \mathbb{K}^m$  を代入した数値要素の線形連立方程式を解くことによって初期点を定める。

$c^{(p-1)}$  まで定まると仮定する。このとき、  $\delta c^{(p)}$  について次の関係を満たす。

$$\begin{aligned} \delta A^{(w+p)}c^{(0)} + \delta A^{(w+p-1)}c^{(1)} + \dots + \delta A^{(w)}\delta c^{(p)} &= \delta b^{(w+p)} \\ \delta A^{(w)}\delta c^{(p)} &= \delta b^{(w+p)} - \sum_{i=1}^p \delta A^{(w+i)}c^{(p-i)}. \end{aligned}$$

$\delta A^{(w)}$  は数式を要素とするため、逆行列の計算は大変である。そのため変数に数値を代入して計算を行う。計算には  $\delta A^{(w)}(s)$  の逆行列が必要であるが、  $c^{(0)}$  の生成の時にすでに計算済みである。

## 4 計算量

### 4.1 リフティング法に基づく

計算のステップは次の通りである.

- $w = 0$  のとき
  - 逆行列または一般逆行列の計算: 逆行列および一般逆行列の計算量は一般に  $O(m^3)$  以上である.
- $w \geq 1$  のとき
  - 行列とベクトルの積:  $w$  回, 行列とベクトルの積を計算するため, 計算量は  $O(w \cdot m^2)$  である.
  - ベクトル同士の和:  $w + 1$  個のベクトルの和を計算する.

それゆえ, 全体の計算量は  $O(m^3)$  で抑えることができる.

### 4.2 補間法に基づく

計算のステップおよび計算量は次の通りである.

1. 補間点の代入:  $R \times m \times n_{\text{subs}}(P)$ . ただし,  $P$  は行列  $A$  の要素に対応する.
2. 補間点を代入して得られる線形方程式を解く:  $R \times O(m^3)$ .
3. 与えられた方程式を解く,  $n \times O(R^3)$ .

それゆえ, 全体の計算量は  $O(m^3)$  である.

## 5 まとめ

本研究では, 数式を要素に持つ線形連立方程式の解法について高速だと思われる「リフティングを用いた方法」と「補間法」の2つについて比較を行った. サイズが十分大きな場合には補間法が有効であることは多くの研究から実証済みであるが, 応用が十分にある中規模サイズの問題に対してリフティングを用いた方法も理論的な計算量の観点から有効であることを示した(逆行列を用いるため, サイズが大きい場合には有効ではない). 本研究では理論的な解析のみであったが, 今後は実験を含めた実際の問題を扱って研究を行う必要がある.

## 参考文献

- [LP97] B. Liang and S. U. Pillai. Two-dimensional blind deconvolution using a robust GCD approach. *Proc. International Conf. On Image Proces.*, 1997, 424–427.
- [LYZ10] Z. Li, Z. Yang, and L. Zhi. Blind image deconvolution via fast approximate GCD *Proc. of ISSAC'10*, ACM Press, 2010, 155–162.
- [斉藤-牧野 96] 齊藤敏明・牧野野夫, 一般逆行列の計算アルゴリズムとその証明, 京都大学数理解析研究所講究録 941 巻, 1996, 156–169

- [Sanuki09] M. Sanuki. *Computing multivariate approximate GCD based on Barnett's theorem*, Proc. of Symbolic-Numeric Computation 2009 (SNC 2009), H. Sekigawa & H. Kai (Eds.), 2009, 149-157, Kyoto, Japan, 3-5 August 2009.
- [讃岐 11] 讃岐 勝, 近似代数による画像処理の実践, “Computer Algebra - The Algorithms, Implementations and the Next Generation -”, 京都大学数理解析研究所.
- [讃岐 12a] 讃岐 勝, 多項式を要素にもつ線形連立方程式の解法, Risa/Asir Conference 2012, 神戸大学, 2012年3月.
- [讃岐 12b] 讃岐 勝, 多項式要素からなる線形連立方程式の数式処理による解法, 第41回数値解析シンポジウム講演予稿集, 2012, 13-16.
- [SKK00] T. Sasaki, T. Kitamoto and F. Kako. On cancellation error in Newton's method for power series roots of multivariate polynomial, preprint, 2000, 32 pages.
- [YT93] K. Yokoyama and T. Takeshima. On Hensel construction of eigenvalues and eigenvectors of matrices with polynomial entries. *Proc. of ISSAC'93, ACM Press*, 1993, 218-224.