完全軸選択による行列の LU 分解の応用
– 多項式の因数分解 –

2001MM087 竹中 哲也
指導教員 鳥居 達生

1 はじめに

本研究では, 任意の実係数多項式に対して, 数値的に因数分解することを目的とする. 初めに, 連立 1 次方程式を行列表示して, 完全軸選択による行列の LU 分解により, 解を求める解法を示す. これより, 行列の階数を適確に決定できることを示し, これを多項式の因数分解に応用する. 解法はニュートン法に基づく分割統治法である [1]. しかし, 2 つの近似因子が互いに素でないとき, この解法は適用できない. そこで, 2 つの多項式の最大公約因子 (GCD) を求める計算法も提示する.

2 完全軸選択による行列の LU 分解

n 次正方行列 A を完全軸選択による LU 分解で分解すると,

$$A = P^T LUQ \tag{1}$$

となる. ただし, P, Q は完全軸選択の情報を記憶する置換行列とし, L を下三角行列, U を上三角行列とする. このとき, $|l_{ij}| \le 1,\ |u_{ij}| \le |u_{ii}|$ である.

式 (1) より, 連立 1 次方程式 $A\boldsymbol{x} = \boldsymbol{b}$ は,

$$A\boldsymbol{x} = \boldsymbol{b} \iff P^T LUQ\boldsymbol{x} = \boldsymbol{b} \tag{2}$$

となる. $\boldsymbol{y} = UQ\boldsymbol{x}$ とすると, 式 (2) より,

$$\begin{cases} P^T L\boldsymbol{y} = \boldsymbol{b} \\ UQ\boldsymbol{x} = \boldsymbol{y} \end{cases} \tag{3}$$

となる. $\boldsymbol{z} = Q\boldsymbol{x}$ とすると, 式 (3) より,

$$\begin{cases} L\boldsymbol{y} = P\boldsymbol{b} \\ U\boldsymbol{z} = \boldsymbol{y} \\ \boldsymbol{x} = Q^T\boldsymbol{z} \end{cases} \tag{4}$$

となる. 式 (4) において, 初めに, $L\boldsymbol{y} = P\boldsymbol{b}$ では, 置換行列 P による並び換えを行い, 前進代入法により, $\boldsymbol{y}$ を求める. 次に, $U\boldsymbol{z} = \boldsymbol{y}$ では, 後退代入法により, $\boldsymbol{z}$ を求める. 最後に, $\boldsymbol{x} = Q^T\boldsymbol{z}$ では, 置換行列 Q^T により, $\boldsymbol{z}$ を並び換えて, 解ベクトル $\boldsymbol{x}$ を求める. これが完全軸選択の LU 分解により, 解を求める解法である. 行選択のみによる LU 分解に比べて, この解法では, 行列 U において, 対角要素の絶対値が最大であるので, 行列の階数を適確に決定できる [2][3].

3 多項式の因数分解

3.1 互いに素である多項式の判定

2 つの多項式 $P(z), Q(z)$ が共通因子をもたないとき, $P(z), Q(z)$ は互いに素であるという.

定理 1 $P(z), Q(z)$ が互いに素であり,

$$\deg A(z) < \deg Q(z),\ \deg B(z) < \deg P(z)$$

であるとき,

$$A(z)P(z) + B(z)Q(z) = 1$$

を満たす多項式 $A(z), B(z)$ が一意的に定まる.
ここで, deg は多項式の次数を示すものとする.

3.2 多項式の行列表示

n 次多項式 $P(z)$, m 次多項式 $Q(z)$, 任意の $m+n-1$ 次多項式 $\boldsymbol{r}(z)$ を与えて,

$$A(z)P(z) + B(z)Q(z) = \boldsymbol{r}(z) \tag{5}$$

を満たす $A(z), B(z)$ を求める. ここで, 係数行列 S, ベクトル $\boldsymbol{x}$, ベクトル $\boldsymbol{r}$ を用いて, 式 (5) を行列で表すと, $S\boldsymbol{x} = \boldsymbol{r}$ となる.

定理 1 より, $P(z), Q(z)$ が互いに素であるとき, 行列 S は正則である. したがって, 次の定理が成り立つ.

定理 2 定理 1 と同じ仮定の下で, 式 (5) を満たす多項式 $A(z), B(z)$ は一意的に定まる.

定理 2 より, 式 (5) を行列表示した $S\boldsymbol{x} = \boldsymbol{r}$ において, 完全軸選択による行列の LU 分解で解くと, $A(z), B(z)$ が一意的に求まる.

3.3 分割統治法による多項式の因数分解

高次多項式 $f(z)$ を分割統治法により, 因数分解する. 初期値として, 2 つの多項式 $X(z), Y(z)$ を近似因子として与えて,

$$f(z) \cong X(z)Y(z)$$

とする. ここで, $f(z), Y(z), X(z)$ の最高べきの係数を 1 として,

$$\deg f = \deg X + \deg Y$$

を仮定する. そして, 残差を,

$$R(z) = f(z) - X(z)Y(z)$$

と定義する. ただし, $R(z) \ne 0$ とする.
このとき, $\deg R(z) < \deg f(z)$ が成り立つ.

ここで, $f(z), R(z)$ を f, R とし, $X(z), Y(z)$ を X, Y とし, $\Delta X(z), \Delta Y(z)$ を $\Delta X, \Delta Y$ と表す.

$$f = (X + \Delta X)(Y + \Delta Y)$$

とすると, $f = XY + R$ より,

$$(X + \Delta X)(Y + \Delta Y) = XY + R$$

となる. これを展開して,

$$XY + X\Delta Y + Y\Delta X + \Delta X\Delta Y = XY + R.$$

ここで, 積 $\Delta X\Delta Y$ は $\Delta X, \Delta Y$ に比べて十分小さいと仮定して, 2 次の項 $\Delta X\Delta Y$ を無視すると,

$$X\Delta Y + Y\Delta X = R$$

となる. ここで, 完全軸選択による行列の LU 分解を行い, $\Delta X, \Delta Y$ を求める. そして,

$$X \leftarrow X + \Delta X$$
$$Y \leftarrow Y + \Delta Y$$

として, この操作を繰り返すと残差 $R(z)$ が 0 に 2 次収束していき, $f(z)$ が $X(z)$ と $Y(z)$ に因数分解される. これがニュートン法に基づく分割統治法である [2].

4 最大公約因子 (GCD) を求める解法

2 つの多項式が互いに素でないとき, 定理 1 と定理 2 が成立しないため, 前述の分割統治法で因数分解することができない. そこで, まず 2 つの多項式の最大公約因子 (GCD) を求める必要がある. n 次多項式 $f(z)$ と, m 次多項式 $g(z)$ を与える. $f(z)$ と $g(z)$ の最大公約因子を $d(z)$ として, $f(z)$ と $d(z)$ の商を $f_1(z)$, $g(z)$ と $d(z)$ の商を $g_1(z)$ とすると,

$$\begin{aligned} A(z)f(z) + B(z)g(z) &= A(z)d(z)f_1(z) + B(z)d(z)g_1(z) \\ &= d(z)\{A(z)f_1(z) + B(z)g_1(z)\} \end{aligned}$$

となる. このとき, $f_1(z)$ と $g_1(z)$ は互いに素であるので, 定理 1 より, $A(z)f_1(z) + B(z)g_1(z) = 1$ を満たす $A(z), B(z)$ が一意的に決まる. この $A(z), B(z)$ を用いると,

$$A(z)f(z) + B(z)g(z) = d(z) \tag{6}$$

となり, 最大公約因子 $d(z)$ を求めることができる. 以上のことを, 数値的に計算するために, 行列を用いて考える.

多項式 $Y(z)$ を用いて, 次の式

$$A(z)f(z) + B(z)g(z) = Y(z) \tag{7}$$

を行列で表すと, $S\boldsymbol{x} = Y$ となる. ただし, $N = m + n$ とする. ここで, Y の第 1 成分, 第 2 成分,$\cdots$ と初めからできるだけ 0 にするような $\boldsymbol{x}$ の値を求める。ただし, $Y \neq 0$ とする.

S が正則であるときは, $Y = (0\ \cdots\ 0\ \ 1)^T$ として, $\boldsymbol{x}$ を求めると, $A(z), B(z)$ が一意的に決まる.

定理 3 行列 S の退化次数と最大公約因子 $d(z)$ の次数は一致する.

S が非正則であるときを考える. 完全軸選択による行列の LU 分解を行うと,

$$S = P^T LDUQ$$

となる. このとき, 行列の階数を r, 退化次数を $l = N - r$ とする. ここで, $\boldsymbol{y} = DUQ\boldsymbol{x}$ とすると,

$$S\boldsymbol{x} = P^T L\boldsymbol{y}$$

となる. このとき, ベクトル $\boldsymbol{y}$ の第 $r+1$ 成分から第 N 成分までは 0 となる. ここで, 式 (7) の右辺ベクトル Y を第 1 成分, 第 2 成分, $\cdots$, 第 $r-1$ 成分まで 0 にするように, $\boldsymbol{y}$ を決定する. そのために, $M = (\boldsymbol{z}_r, \boldsymbol{z}_{r+1}, \cdots,\ \boldsymbol{z}_N)$ とし, I_{l+1} は $l+1$ 次の単位行列を表すものとして,

$$P^T LM = \begin{pmatrix} 0 \\ I_{l+1} \end{pmatrix}$$

を満たす M を前進代入法により求める. 行列 M の第 1 行から第 r 行までを行列 M_1 とし, 残りの第 $r+1$ 行から第 N 行までを行列 M_2 として分割する. このとき, $M_1 \in R^{r\times(l+1)}$, $M_2 \in R^{l\times(l+1)}$ となる. そして, $\boldsymbol{d} \in R^{l+1}$ として,

$$\begin{aligned} \boldsymbol{y} &= M\boldsymbol{d} \\ &= \begin{pmatrix} M_1\boldsymbol{d} \\ M_2\boldsymbol{d} \end{pmatrix} \end{aligned}$$

とすると, $\boldsymbol{y}$ の第 $r+1$ 成分から第 N 成分までは 0 であるので,

$$M_2\boldsymbol{d} = 0,\ (\boldsymbol{d} \neq 0)$$

となる $\boldsymbol{d}$ を完全軸選択による LU 分解で求める. 定理 3 より, ベクトル $\boldsymbol{d}$ の最高べきの係数は 0 でないので, この係数が 1 となるように調節して, 最大公約因子を求める. このとき, $\boldsymbol{d}$ は最大公約因子の係数を与えるものである.

式 (6) の $A(z), B(z)$ の計算法は省略する.

5 おわりに

完全軸選択による LU 分解を行うことで, 行列の階数を適確に決定できた. これを応用し, 分割統治法により多項式の因数分解を行うことができた. また, 2 つの近似因子が互いに素でない場合, 最大公約因子も求めることができた. より多くの例題につき数値実験を行い, 問題を発見し, それを解決するために理論やプログラムを改良していくことが今後の課題である.

参考文献

[1] 園田信吾, 櫻井鉄也, 杉浦洋, 鳥居達生: 分割統治法による多項式の数値的因数分解, 日本応用数理学会論文誌, Vol.1 No.4, pp.277〜290 (1991).

[2] 杉浦洋：数値計算の基礎と応用-数値解析学への入門-, サイエンス社, (1997).

[3] G.W.Stewart：Matrix Algorithms, siam, (1998).