

孫子定理の - 応用

- 代数方程式の数値的因数分解 -

名古屋大学 工学部 島田達生

梅井鉄也

杉浦 洋

1. はじめに

孫子定理 (中国剰余定理ともいう) を関数近似の方法である補間法の立場から解釈し, その結果を 1 変数多項式の数値的因数分解に応用する.

はじめに記号を定義する. $p(x)$, $q(x)$ を任意の多項式とする.

$\deg p$; $p(x)$ の次数

(p, q) ; $p(x)$ と $q(x)$ の最大公約因子. とくに

$(p, q) = 1$ ならば, p, q は互いに素.

$\|p\|$: 多項式 $p(x)$ のノルム. この定義は

$$\|p\| = \max |a_i|,$$

$$\text{ただし } p(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n.$$

多項式 $p(x)$ を, 多項式 $x(x)$ で割ったときの商と余りを,

それぞれ $Q(x)$, $R(x)$ とすれば

$$p(x) = Q(x)X(x) + R(x) \quad (1.1)$$

$$\deg R < \deg X$$

となる。この表現は一通りである。

p が X で割り切れるとき、すなわち $R=0$ のとき

$$X \mid p$$

と書く。また、 $=$ の多項式 p_1, p_2 が $X \mid p_1 - p_2$ ならば

$$p_1 \equiv p_2, \text{ mod } X$$

と書き、 p_1 と p_2 は、 X を法とした合同であること。

多項式の除算 (1.1) において、 $R \equiv p, \text{ mod } X$ であるが、余りの一意より、余り $R \in$

$$R = p(x), \text{ mod } X(x) = p, \text{ mod } X$$

と書く。

多項式 $X(x)$ の 0 点を $\alpha_1, \alpha_2, \dots, \alpha_m$ とする。重根ならば、重複度だけ並べるとする。除算 (1.1) において、 $X(x)$ の 0 点上で $p(x)$ と $R(x)$ は、次の意味で一致する。点 α_i が $X(x)$ の $\mu \geq 1$ 乗根ならば $R^{(\mu)}(\alpha_i) = p^{(\mu)}(\alpha_i)$, $0 \leq k < \mu$.

ここで $p^{(\mu)}(x)$ は、 $p(x)$ の μ 階導関数。 $R(x)$ の次数は $X(x)$ のそれより小さいことから R は、 $p(x)$ の $X(x)$ の 0 点上における補間多項式である。すなわち、代数演算

$$p, \text{ mod } X$$

は, $P(x)$ の $X(x)$ の 0 点上の Hermite 補間法である.

この知見によれば, 最早被近似関数を多項式に限定する必要はない. 形式的には, 補間法が定義できる関数族ならいい. $f(x)$ を十分滑らかな関数として, $f, \text{mod } X$ を $f(x)$ の X の 0 点上における Hermite 補間多項式とする. 後に有理式の Hermite 補間を考える.

孫子定理 多項式 P, Q, R が

$$(P, Q) = 1, \quad \deg R < \deg P + \deg Q$$

ならば

$$A(x)P(x) + B(x)Q(x) = R(x)$$

$$\deg A < \deg Q, \quad \deg B < \deg P$$

を満たす多項式 $A(x), B(x)$ は一意に存在する.

孫子定理は, 初等整数論で有名な定理であり, 素数分布研究によれば, 孫子算は 3 素数頃の本とある.

これを多項式に拡張し, 最も成功した応用例は, FFT であろう).

A, B の求め方は, いろいろある¹⁾. わかり易いと思われる一例を示す.

$(P, Q) = 1$ であるから Euclid の互除法により

$$A_0 P + B_0 Q = 1$$

$$\deg A_0 < \deg Q, \quad \deg B_0 < \deg P$$

を満たす多項式 A_0, B_0 がただ一つ存在する. この式に PQ をかけ, PQ を法として合同をとる.

$$RA_0P + RB_0Q = R \quad , \quad \text{mod } PQ$$

よって

$$\begin{aligned} RA_0P \text{ , mod } PQ &= (RA_0 \text{ , mod } Q) \cdot P \\ &= ((R \text{ , mod } Q) \cdot A_0 \text{ , mod } Q) \cdot P \\ &= AP \end{aligned}$$

よって $\deg A < \deg Q$ である.

同様に

$$\begin{aligned} RB_0Q \text{ , mod } PQ &= ((R \text{ , mod } P) \cdot B_0 \text{ , mod } P) \cdot Q \\ &= BQ \end{aligned}$$

よって $\deg B < \deg P$ である. したがって多項式 A, B は, 定理の条件を満たす.

== 次の問題を解く.

問題. 有理式 P/Q と多項式 X とする. $(Q, X) = 1$ とし $P/Q \text{ , mod } X$ を求めよ.

解法. $\deg P, \deg Q < \deg X$ と一般性を失わずに.

$(Q, X) = 1$ であるから, 跡定理より

$$SQ + TX = P \quad , \quad \deg S < \deg X, \deg T < \deg Q$$

を満たす多項式 S, T を求める. 明らかに

$$S = P/Q \text{ , mod } X$$

である。これが有理式 P/Q の X の 0 乗の補間多項式である。

解法では、 X の 0 乗を陽に必要としないことに注意。

以後簡単のため S を X 上の補間式という。

とくに $X(x) = x^N - 1$, $N = 2^n$ ならば、 $S(x)$ は、^(次のように) FFT によって高速に求まる。

$P(x)$, $Q(x)$ に ^(N 回) FFT を適用し、 $x^N - 1$ の 0 乗上で、これを標本化する。標本点上で、 N 回の除算 $P(x_k)/Q(x_k)$ ($x_k^N - 1 = 0$) を行なう。こうして得られた標本に N 回 FFT を適用すれば $S(x)$ が得られる。すなわち、たゞみのみ演算と同じ手順である。

つまり $SQ + T \cdot (x^N - 1) = P$ の T を求める。両辺 x^{N+1} と合同をとれば、 $x^N - 1, \text{mod } x^{N+1} = 2$ に注意すれば

$$T = \frac{1}{2} (SQ - P), \text{mod } x^{N+1}$$

$$= \frac{1}{2} (SQ, \text{mod } (x^{N+1}) - P)$$

となる。したがって中乗公式に基づく N 回 FFT を 3 回使えばよいことになる。矢張り手順としては項数 N の循環型たゞみのみ演算と下いである。

2. Bairstow 法の拡張

周知のように、Bairstow 法は、実係数多項式の 2 次因子をとり出す方法である。まず Bairstow 法に対し、独自の解

能え与えよう. $f(x)$ を与えられた多項式とする. $X(x)$ を試みの二次因子とし $f \in X$ が割つたときの商と余りを Q, R とすれば $f = QX + R$ となる. Q を補助関数とし, 有理式 $f/Q \in X$ 上へ補間し, それを $S(x)$ とおけば

$$S(x) = \frac{f}{Q}, \text{ mod } X = \frac{R}{Q}, \text{ mod } X$$

となる. ただし $(Q, X) = 1$ を仮定した. $X+S$ を新しい二次因子 X とおき, 同様の操作を繰り返す. これが Bairstow 法である. $\varepsilon > 0$ を十分小とする. $\|R\| < \varepsilon$ ならば, これが二次係数であることも次によって簡単にわかる.

$(Q, X) = 1$ であるから $SQ + TX = R$ において $\|S\|, \|T\|$ は, ε にも $O(\varepsilon)$ である.

一方, $f = QX + R = QX + SQ + TX = Q(X+S) + TX$ において, $f, \text{ mod } (X+S)$ を評価すれば

$$f \equiv TX \equiv -TS, \text{ mod } (X+S)$$

したがって, $\|TS\| \leq \|T\| \|S\| = O(\varepsilon^2)$.

以上において, 試みの因子 $X(x)$ の次数 n は, 本質的な制限ではない. X の次数は任意であってよい. $n < \lfloor \deg f / 2 \rfloor$ にとったとき, これは分割統治法とよばれる算法となる. Freeman は, $X(x)$ の係数に関する非線形方程式を Newton 法で解いている¹⁾. 著者の上述の導出も,

結果的には同じであるが記述が簡単である。

再び元の問題に立ち返る。試みの因子 X の次数を適当に大きくして $f = QX + R$ と表わしたとき, $\deg Q, \deg R$ は, ともに $\deg X$ より小さくなる。このとき $QX + R = 0$ は X に関する 1 次式とみなす。(Q と R の次数の制限はなくてもよい)。

すなわち多項式 $f(x)$ の因数分解は, 一般性を失うことなく 1 次式

$$QX + R = 0 \pmod{f}, \quad \deg Q, \deg R < \deg X \quad (2.1)$$

を解くことに帰着できる。

孫子定理を用いて連立 1 次方程式列 S_k, T_k, Q_k をつくります。

算法 1. 初期値 $Q_0 = Q$

$$S_k Q_k + T_k X = R$$

$$Q_{k+1} = Q + T_k$$

$$k = 0, 1, 2, \dots$$

孫子定理より $(Q_k, X) = 1$ ならば, 上の漸化式は支障なく進行する。

いま, $X_{k+1} = X + S_k$ とおく。

定理. X_k, Q_k が, それぞれ X_∞, Q_∞ に収束したとすれば $QX + R = Q_\infty X_\infty$ が成り立つ。すなわち X_∞ は

1 次式 (2.1) の解である。

証明. 演算子定理を用ゐる.

$$\begin{aligned} QX + R &= QX + S_k Q_k + T_k X \\ &= (Q + T_k) X + S_k Q_k \\ &= Q_{k+1} X + S_k Q_k \end{aligned}$$

Q_k, X_k の収束を仮定して S_k の極限を S_∞ とすれば
上式の右辺は $Q_\infty (X + S_\infty) = Q_\infty X_\infty$ に収束する.
(証明終)

次は, 収束次数の問題である. これに必要は補題から述べる.

補題 1. 算法 1 における $S_k Q_k + T_k X = R, k=0, 1, 2, \dots$
に於いて $\|R\| < \varepsilon, \|X\| = O(1), \|Q_0\| = O(1)$ かつ

$$\|S_k\| = O(\varepsilon), \|T_k\| = O(\varepsilon)$$

$$\|T_k - T_{k-1}\| = O(\varepsilon^k), \|S_k - S_{k-1}\| = O(\varepsilon^k)$$

とすると, 十分小 $\varepsilon > 0$ は十分小とする.

証明 $S_{k+1} Q_{k+1} + T_{k+1} X = R$ と k を 1 減じた式と逐々差引
けば

$$(T_{k+1} - T_k) X + S_{k+1} (Q + T_k) - S_k (Q + T_{k-1}) = 0$$

$$(T_{k+1} - T_k) X + (S_{k+1} - S_k) Q_k = -S_k (T_k - T_{k-1}).$$

$k=0$ のとき $\left(\begin{array}{l} \|R\| < \varepsilon \\ (Q_0, X) = 1 \end{array} \right)$ より $\|S_0\| = O(\varepsilon), \|T_0\| = O(\varepsilon)$
とある. また, 各 k に於いて, $(Q_k, X) = 1$ を仮定して

$\|S_k\| = O(\varepsilon), \|T_k\| = O(\varepsilon)$. 上の $T_k - T_{k-1}$ に関する漸

化式に於いて $T_1 = 0$ とおき、帰納法により、 $\|T_k - T_{k-1}\| = O(\varepsilon^k)$,
 $\|S_k - S_{k-1}\| = O(\varepsilon^k)$ を証明できる. (証明終)

定理 多項式列 X_k の収束次数は 1 である.

証明. $f = QX + R \equiv \text{mod } X_k$ の意味を評価する.

$$QX + R = QX + S_k Q_k + T_k X$$

$$X_{k+1} = X + S_k \text{ であるから}$$

$$\begin{aligned} QX + R, \text{ mod } X_{k+1} &= Q_{k+1}(-S_k) + S_k Q_k \\ &= -S_k (T_k - T_{k-1}) \end{aligned}$$

したがって, 補題 1 より

$$\begin{aligned} \|QX + R, \text{ mod } X_k\| &\leq \|S_k\| \|T_k - T_{k-1}\| \\ &= O(\varepsilon) \cdot O(\varepsilon^k) = O(\varepsilon^{k+1}) \end{aligned}$$

が得られる. (証明終)

1 次収束する方法をリスタート方式を使えば, 高次収束となる. すなわち $X_0 = X$ とおき $X_k = X + S_{k-1}$, $k = 1, 2, \dots, m$ をつくる. X_m をあらためて X_0 とおき, これを反復すれば $m+1$ 次収束となる.

X を 1 次因子とするとき, $m = 1, 2, 3$ に対応する算法は Newton 法, Halley 法, Kins 法となる.

FFT を使い高速算法となるのは X が円周等分多項式でその次数が 2 のべき乗の場合にある. 数値実験は, 以下に示すように.

分割統治法の著者の実験例は、文献 2) にある。

参考文献

- 1) Freeman, T. L ; A divide and conquer method for polynomial zeros, J. Comput. Appl. Math. 30, pp. 71-79 (1990)
- 2) 園田信吾, 榑井欽也, 杉浦洋, 島元達生 ; 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).