定数係数線形漸化式における演算子法

数列の第 n 項を n+1 項に 1 つ進める演算子を N とする。すなわち

$$Na_n = a_{n+1}$$

さらに，$c_0, c_1, c_2, \cdots, c_m$ を定数として

$$c_0 a_{n+m} + c_1 a_{n+m-1} + c_2 a_{n+m-2} + \cdots + c_m a_n = (c_0 N^m + c_1 N^{m-1} + c_2 N^{m-2} + \cdots + c_m) a_n$$

と表すとことにする。ここで N の多項式 $f(N)$ を

$$f(N) = c_0 N^m + c_1 N^{m-1} + c_2 N^{m-2} + \cdots + c_m$$

とおく。

定理

k を定数，$f(N)$，$g(N)$，$h(N)$ を N の多項式とするとき

Ⅰ　$f(N)(a_n + b_n) = f(N)a_n + f(N)b_n$

Ⅱ　$\{f(N) + g(N)\}a_n = f(N)a_n + g(N)a_n$

Ⅲ　$f(N)\{g(N)a_n\} = \{f(N)g(N)\}a_n$

ただし，ここで $\{f(N) + g(N)\}$，$\{f(N)g(N)\}$ はそれぞれ N の多項式の和，積を表す。

証明

$$f(N) = \sum_{i=0}^{m} c_i N^{m-i}, \quad g(N) = \sum_{i=0}^{m} d_i N^{m-i} \quad \text{とおく。}$$

Ⅰ　$f(N)(a_n + b_n) = (\sum_{i=0}^{m} c_i N^{m-i})(a_n + b_n) = \sum_{i=0}^{m} c_i a_{n+m-i} + \sum_{i=0}^{m} c_i b_{n+m-i} = f(N)a_n + f(N)b_n$

Ⅱ　$\{f(N) + g(N)\}a_n = \{\sum_{i=0}^{m} (c_i + d_i) N^{m-i}\}a_n = \sum_{i=0}^{m} c_i a_{n+m-i} + \sum_{i=0}^{m} d_i a_{n+m-i} = f(N)a_n + g(N)a_n$

Ⅲ　$f(N)\{g(N)a_n\} = (\sum_{j=0}^{m} c_j N^{m-j})\ (\sum_{i=0}^{m} d_i a_{n+m-i}) = \sum_{j=0}^{m} (\ \sum_{i=0}^{m} c_j d_i a_{n+2m-i-j})$

$$= \{\sum_{j=0}^{m} (\ \sum_{i=0}^{m} c_j d_i N^{n+2m-i-j})\}a_n = \{f(N)g(N)\}a_n$$

証明終り

Ⅱ，Ⅲをそれぞれ

$$f(N) + g(N) = \{f(N) + g(N)\}, \quad f(N)g(N) = \{f(N)g(N)\}$$

と書くことにする。

定理

Ⅰ　$\{f(N)g(N)\}h(N) = f(N)\{g(N)h(N)\}$　　結合法則

Ⅱ　$f(N)g(N) = g(N)f(N)$　　交換法則

Ⅲ　$f(N)\{g(N) + h(N)\} = f(N)g(N) + f(N)h(N)$　　左分配法則

Ⅳ　$\{g(N) + h(N)\}f(N) = g(N)f(N) + h(N)f(N)$　　右分配法則

証明

Ⅰ　多項式の積については結合法則が成り立つから，前定理により

$$\{f(N)g(N)\}h(N) = [\{f(N)g(N)\}h(N)] = [f(N)\{g(N)h(N)\}] = f(N)\{g(N)h(N)\}$$

Ⅱ　多項式の積については交換法則が成り立つから，前定理により

$$f(N)g(N)=\{f(N)g(N)\}=\{g(N)f(N)\}=g(N)f(N)$$

Ⅲ　多項式の積については分配法則が成り立つから，前定理により

$$f(N)\{g(N)+h(N)\}=[f(N)\{g(N)+h(N)\}]$$
$$=\{f(N)g(N)+f(N)h(N)\}=f(N)g(N)+f(N)h(N)\}$$

Ⅳ　Ⅱ，Ⅲより明らか

証明終り

演算子法の応用

定数係数線形漸化式は

$$f(N)a_n=0$$

の形に表される。

例　$a_1=1, a_2=4,\quad a_{n+2}-5a_{n+1}+6a_n=0\ (n=1,2,3,\cdots)$　を一般項を求める。

解

漸化式は　$(N^2-5N+6)a_n=0$　…①

変形して　$(N-2)(N-3)a_n=0$　…②

整式 N^{n-1} を整式 $(N-2)(N-3)$ で割った商を $Q(N)$ とすると

$$N^{n-1}=(N-2)(N-3)Q(N)+sN+t$$

と表される。$N=2,3$ を代入して

$$2^{n-1}=2s+t,\quad 3^{n-1}=3s+t$$

これを解いて

$$s=-2^{n-1}+3^{n-1},\quad t=3\cdot 2^{n-1}-2\cdot 3^{n-1}$$

よって

$$a_n=N^{n-1}a_1=(N-2)(N-3)Q(N)a_1+sNa_1+ta_1$$
$$=Q(N)(N-2)(N-3)a_1+(-2^{n-1}+3^{n-1})Na_1+(3\cdot 2^{n-1}-2\cdot 3^{n-1})a_1$$
$$=(-2^{n-1}+3^{n-1})a_2+(3\cdot 2^{n-1}-2\cdot 3^{n-1})a_1$$
$$=2\cdot 3^{n-1}-2^{n-1}$$

別解　②より，$(N-3)a_n=0$　を満たす a_n は①を満たすから，$a_n=3^{n-1}$ は①を満たす。

また，②は　$(N-3)(N-2)a_n=0$　と変形できるから，同様にして，$a_n=2^{n-1}$ は①を満たす

漸化式は線形であるから，s，t を定数として，$a_n=s\cdot 2^{n-1}+t\cdot 3^{n-1}$ は①を満たす。

ここで，$a_1=1, a_2=4$ であるから　$s=-1, t=2$

よって　$a_n=2\cdot 3^{n-1}-2^{n-1}$

定理　$f(N)$ が因数 $(N-r)^m$ を持つとき，$a_n=n^i r^n\quad (i=0,1,2,\cdots,m-1)$　は　$f(N)a_n=0$　を満たす。

証明

$f(N)a_n = g(N)(N-r)^m a_n$ となるから $(N-r)^{i+1}n^i r^n = 0 \quad (i = 0, 1, 2, \cdots)$ であることを示せばよい。

(Ⅰ) i=0 のとき $(N-r)r^n = r^{n+1} - r^{n+1} = 0$ より成り立つ。

(Ⅱ) i≦k－1 のとき命題が成り立つと仮定すると，

$$(N-r)^{i+1}n^i r^n = 0 \quad (i = 0, 1, 2, \cdots, k-1)$$

このとき

$$(N-r)^{k+1}n^k r^n = (N-r)^k (N-r)n^k r^n = (N-r)^k (Nn^k r^n - rn^k r^n)$$

$$= (N-r)^k \{(n+1)^k r^{n+1} - n^k r^{n+1}\} = (N-r)^k \sum_{i=0}^{k-1} {}_kC_i n^i r^{n+1} = r\sum_{i=0}^{k-1} {}_kC_i (N-r)^k n^i r^n = 0$$

よって，i≦k のときも命題は成り立つ。

(Ⅰ)，(Ⅱ)より，すべての負でない整数 i について命題は成り立つ。

証明終り

例　漸化式　$(N-3)(N-2)^3 a_n = 0$　の一般解は，$a_n = s \cdot 3^{n-1} + (t \cdot n^2 + u \cdot n + v) \cdot 2^{n-1}$

定数係数線形漸化式の高速計算法

例　フィボナッチ数列の項の高速計算法

$$a_1 = 1, a_2 = 1, \quad a_{n+2} = a_{n+1} + a_n$$

で定義される数列がフィボナッチ数列である。

第 1000 項を求めたい。

$$N^2 a_n = (N+1)a_n$$

$$a_{1000} = N^{999} a_1$$

である。

このとき　999 を 2 進数で表すと　1111100111　となる。

よって

$$N^{999} = N^{2^9+2^8+2^7+2^6+2^5+2^2+2^1+2^0}$$

であるから

$$N^{999} = (((((((((N^2N)^2N)^2N)^2N)^2)^2)^2)N)^2N)^2N$$

である。(バイナリー法)

ここで

$$N^2 \equiv N+1 \quad (\mathrm{mod} \quad N^2 - N - 1)$$

を繰り返し用いれば，N^{999} は定数 s，t を用いて

$$N^{999} \equiv sN + t \quad (\mathrm{mod} \quad N^2 - N - 1)$$

の形に表される。よって

$$a_{1000} = N^{999} a_1 = (sN+t)a_1 = sa_2 + ta_1 = s + t$$

となる。このとき N^{999} を計算するのに，2 乗を 9 回，乗算を 7 回行う。

さらに，$a_{1001} = N^{999} a_2 = N^{1000} a_1$ を求めれば，これ以降の項が漸化式により求まる。

一般的に，数列$\{a_n\}$の定数係数線形漸化式は次のように表される。

$$a_{n+m} = c_1 a_{n+m-1} + c_2 a_{n+m-2} + \cdots + c_m a_n$$

ここで，演算子 N を用いると

$$N^m a_n = (c_1 N^{m-1} + c_2 N^{m-2} + \cdots + c_m) a_n$$

となる。よって

$P(N) = N^m - (c_1 N^{m-1} + c_2 N^{m-2} + \cdots + c_m)$　とおくと　$P(N) a_n = 0$

また，$\{a_n\}$の第 M 項は

$$a_M = N^{M-1} a_1$$

と表される。ここで，$M-1$を 2 進数展開して，バイナリー法を用いる。
このとき

$$N^m \equiv c_1 N^{m-1} + c_2 N^{m-2} + \cdots + c_m \qquad (\mathrm{mod} \quad P(N))$$

を繰り返し用いれば，$s_1, s_2, \cdots, s_m$を定数として

$$N^{M-1} \equiv s_1 N^{m-1} + s_2 N^{m-2} + \cdots + s_m \quad (\mathrm{mod} \quad P(N))$$

の形に表されるから

$$a_M = N^{M-1} a_1$$

$$= (s_1 N^{m-1} + s_2 N^{m-2} + \cdots + s_m) a_1$$

$$= s_1 a_m + s_2 a_{m-1} + \cdots + s_m a_1$$

となる。

よって，漸化式により$a_{m+1}, a_{m+2}, a_{m+3}, \cdots, a_{2m}$を求めるか，$N^{M-1}, N^M, \cdots, N^{M+m-2}$を$P(N)$で割った余りを求めれば，$a_M, a_{M+1}, a_{M+2}, \cdots, a_{M+m-1}$ が求められ，これ以降の項が漸化式により求まる。
このアルゴリズムは，特に有限体上の漸化式において有効である。m が大きいとき，1 回の乗算の計算量は m のオーダー，1 回の 2 乗の計算量はm^2のオーダーである。2 乗の回数は$\log_2 M$回程度であるから，全体の計算量は$m^2 \log_2 M$のオーダーである。ただし，GF(2)上の漸化式で，かつ，3 項間漸化式のように項の数が少ない場合は，全体の計算量は$m \log_2 M$のオーダーである。

上記の高速計算法は，漸化式を行列を用いて表し，ケーリー・ハミルトンの定理を利用する方法と同等であるが，演算子法はそれよりも簡明である。
行列を用いる方法では，漸化式

$$a_{n+m} = c_1 a_{n+m-1} + c_2 a_{n+m-2} + \cdots + c_m a_n$$

を行列を用いて表すと

$$\begin{pmatrix} a_{n+m} \\ a_{n+m-1} \\ a_{n+m-2} \\ \vdots \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_m \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n+m-1} \\ a_{n+m-2} \\ a_{n+m-3} \\ \vdots \\ a_n \end{pmatrix}$$

ここで

$$A=\begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_m \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},\quad X_n=\begin{pmatrix} a_{n+m-1} \\ a_{n+m-2} \\ a_{n+m-3} \\ \vdots \\ a_n \end{pmatrix}$$

とおくと，

$$X_{n+1}=AX_n$$

となるから

$$X_M=A^{M-1}X_1$$

A の固有方程式は漸化式の特性方程式と一致するから，ケーリー・ハミルトンの定理により

$$A^m=c_1A^{m-1}+c_2A^{m-2}+\cdots+c_mE$$

バイナリー法によりこれを繰り返し用いれば

$$A^{M-1}=s_1A^{m-1}+s_2A^{m-2}+\cdots+s_mE$$

と表される。したがって，

$$X_M=A^{M-1}X_1=(s_1A^{m-1}+s_2A^{m-2}+\cdots+s_mE)X_1$$