テクニカルノート

M系列の位相点の計算法

山住富也† 小池慎一††

3項式M系列は工学の分野で広く利用されている．M系列を利用する場合，与えられた値だけ位相をシフトした系列を発生させたい場合があるが，従来の方法では円分位相点の計算は面倒である．また，円分位相点から外れた点の計算はできない．そこで，M系列を漸化式表現したときの添え字間の演算に注目し，円分位相点の簡明な演算方式を示した．さらに，この計算法を使い，任意の値だけ位相をシフトしたM系列の構成が簡単にできることを示した．

An Algorithm for Computing Phases of an M-sequence

TOMIYA YAMAZUMI† and SHIN-ICHI KOIKE††

A trinomial M-sequence is generally used in technology engineering. However, near cyclotomic phases in a period such as $\frac{1}{2}$ or $\frac{1}{4}$, tuples which are similar to an initial tuple appear. This property is not good for random sequence. On using the M-sequence shifted by arbitrary value, a calculation of cyclotomic phase is too difficult. And the phase out of cyclotomic phase can't be calculate. So, we notice the suffix on the linear recurrence formula, and suggeste the calcutation method of cyclotomic phase.

1. はじめに

M系列の円分位相点の計算法については，柏木ら[1),2)]や山住ら[3)]に報告がある．しかし，計算が面倒であり，また，円分位相点から外れた点の計算はできない．本報ではM系列を漸化式表現したときの添え字間の演算に注目し，任意の位相点の簡明な演算方式を提案する．

M系列は，そのランダムネスに注目して統計的乱数や制御系の動特性の解析，メモリなどのビット・テスト・パターン生成などいろいろな分野で利用されている．しかし，周期の $\frac{1}{2}$ や $\frac{1}{4}$ の円分位相点付近では，系列の初めの数個の要素の和で表されることが知られている[1)]．これは，$\frac{1}{2}$ や $\frac{1}{4}$ 円分位相点付近では系列の初めのタップルと似たタップルが出現することを意味し，その付近の部分系列はランダムな系列としては望ましくない．

このことから $\frac{3}{4}$ や，さらには $\frac{5}{8}$ 位相点なども同様な傾向があると予想される．しかし，その計算は従来の方法では容易ではない．ここで提案する計算法によれば標準精度の整数演算のみで簡明なアルゴリズムで計算でき，かつ，同様の傾向があることが数値的に確かめられた．

また，任意の値だけ位相をシフトしたM系列を利用するような応用においても，シフトしたM系列を構成することが簡単にできる．このように，この計算法はM系列を利用するうえで有用である．

2. 数学的準備

線形漸化式で表現される3項式M系列は以下のように与えられる．

$$x_n = x_{n-p} + x_{n-q} \tag{1}$$

ここに，$p, q\,(p > q)$ は原始3項式の次数である．各項の値は0，1で，演算は $GF(2)$ 上でなされる．容易に示されるように，整数 k に対して

$$x_n = x_{n-2^k p} + x_{n-2^k q} \tag{2}$$

が成立する．また，n を改めて $n+h$ とおくことにより，

$$x_{n+h} = x_{n+h-p} + x_{n+h-q} \tag{3}$$

† 名古屋文理大学情報文化学部情報文化学科
Department of Information Culture, Nagoya Bunri University
†† 愛知工業大学計算センター
Computing Center, Aichi Institute of Technology

が成立する☆．ここに h は正整数である．さらに，M系列の周期は

$$T = 2^p - 1 \tag{4}$$

で与えられる．したがって，要素 x_n の添え字 n は周期 T を法として計算される．

要素 x_n の添え字に注目して，式(1)を

$$[n] = [n-p, n-q] \tag{5}$$

と表す．すなわち，$[n]$ は，添え字 n を持つ要素 x_n を意味する．以下，この表現に従って，表記規則および演算規則について述べる．

2.1 表記規則

(1) 要素

M系列の要素を，添え字を [と] ではさんで表す．項が複数の要素の和からなる場合には，それらをカンマ「,」で区切って並べ，両端を [と] で囲む．

(例)

- $[n]$：要素 x_n を意味する．
- $[n_1, n_2]$：2個の要素 x_{n_1} と x_{n_2} の和を意味する．

(2) シフト演算

要素 $[n]$ の整数 r だけのシフト演算を

$$[n+r] = [n] + [r] \tag{6}$$

と，要素の算術和 + で表す．

(3) 逆数

$$\left[\frac{1}{m}\right] = \left[\frac{nT+1}{m}\right] \tag{7}$$

ここに T はM系列の周期で，式(4)より $T = 2^p - 1$ である．また n は任意の整数である．

m が 2^k $(0 \le k < p)$ であるとき，m が2のべき乗で表されるとき，$\frac{1}{m}$ は $n = 1$ に対して割り切れて整数値をとる．これを円分位相点という．その他の m に対しては，ある適当な n をとれば割り切れて整数値をとる．

[例] $p = 6$，$q = 1$ の場合，$m = 5$ の場合，$T = 63$ と $n = 8$ に対して，$[\frac{1}{5}] = [\frac{8\times63+1}{5}] = [\frac{505}{5}] = [38]$ となる．これは円分位相点ではない．

2.2 演算規則

次に演算規則についてまとめておく．

(1) 交換則

$$[a, b] = [b, a] \tag{8}$$

$[a] = [b, c]$ のとき

$$[b] = [a, c] \tag{9}$$

(2) 分配則

$$[a, b] + [c] = [a + c, b + c] \tag{10}$$

$$\begin{aligned}[a, b] + [c, d] &= [a + [c, d], b + [c, d]] \\ &= [a + c, a + d, b + c, b + d]\end{aligned} \tag{11}$$

証明

前半について．$[p] = [a, b]$ とおくと，$[a, b] + [c] = [p] + [c] = [p + c]$，これは c だけのシフトを表すので，右辺に一致する．後半についても同様にして，前半の計算を2回繰り返せばよい．

(3) 置換則

$[n] = [n_1, n_2]$ のとき

$$[p, n_1, n_2] = [p, n] \tag{12}$$

特に，$n_1 = n_2$ のとき，$[n_1, n_2] = [n_1, n_1] = [\,]$ となり，式(12)は

$$[p, n_1, n_2] = [p] \tag{13}$$

と縮約される．

また，$[p] = [n_1, n_2]$ のとき

$$[p, n_1, n_2] = [p, p] = [\,] \tag{14}$$

となる．

証明

式(14)は $2x_p$ となり，この要素は消滅する．

2.3 2倍公式・1/2倍公式

$[n] = [n_1,\ n_2]$ のとき

$$[2n] = [2n_1,\ 2n_2], \tag{15}$$

$$\left[\frac{n}{2}\right] = \left[\frac{n_1}{2}, \frac{n_2}{2}\right] \tag{16}$$

が成立する．

証明

2倍公式について

与式より，$[2n] = [n] + [n] = [n_1, n_2] + [n_1, n_2] = [2n_1, 2n_2]$ を得る．

1/2倍公式について

2倍公式を $p - 1$ 回用いて，左辺 $= [2^{p-1}n] = [\frac{T+1}{2}n] = [\frac{n}{2}]$，右辺についても同様にして得られる．

3. 円分位相点の計算

円分位相点とは，r を正整数としてM系列の $\frac{T+1}{2^r}$ だけ位相のずれた点を意味する[1]．位相は法 T で計算されるので，以降，単に $\frac{1}{2^r}$ で表す．

r が小さい値（1，2，3程度）の場合 $\frac{1}{2^r}$ 円分位相点の要素の計算については柏木ら[1]，山住ら[3]によりなされている．しかし，その導出はかなり面倒であり，M系列のパラメータである p，q の値に依存する．

☆ 式(2)，(3)は一般のM系列についても成立するが，数値例の都合で本報では3項式で説明する．

ここでは，前章で定義した表記および規則を用いた導出方式を述べる．

3.1 $\frac{1}{2}$ 倍公式を用いる方法

M系列の式を前章の表記で表せば $[n]=[n-p,n-q]$ となる．$p-n+1$ のシフト演算と交換則を用いて

$$[1]=[p+1,p-q+1]$$

を得る．これを用いて

$$\left[\frac{1}{2}\right]=\left[\frac{1}{2}\times(p+1),\frac{1}{2}\times(p-q+1)\right] \quad (17)$$

を得る．

以下，順に $\frac{1}{2}$ 倍公式を適用し，$\left[\frac{1}{T+1}\right]$ を得る．

なお，この計算アルゴリズムを付録に示す．

3.2 2倍公式を用いる方法

$\left[\frac{1}{T+1}\right]=[1]$ から始めて，$\left[\frac{2}{T+1}\right]=\left[2\times\frac{1}{T+1}\right]=[2\times1]=[2]$，と順次2倍公式を適用する．右辺の [と] で囲まれた値が p を超えた場合には，置換および縮約則を用いてその値が0から $p-1$ の範囲に入るように変形しておく．

3.3 数 値 例

$p=6$，$q=1$ の場合

- $\frac{1}{2}$ 公式を用いた場合

  M系列の漸化式より $[1]=[7,6]$ が得られる．これから出発して

$$\left[\frac{1}{2}\right]=\left[\frac{7}{2},\frac{6}{2}\right]=\left[\frac{8,6,2}{2}\right]=[4,3,1]$$

$$\left[\frac{1}{4}\right]=\left[\frac{4,3,1}{2}\right]=\left[2,1+\frac{1}{2},\frac{1}{2}\right]$$
$$=[2,[5,4,2],[4,3,1]]=[5,3,1]$$

$$\left[\frac{1}{8}\right]=\left[\frac{5,3,1}{2}\right]=\left[2+\frac{1}{2},1+\frac{1}{2},\frac{1}{2}\right]$$
$$=[[6,5,3],[5,4,2],[4,3,1]]$$
$$=[6,2,1]=[5,2,1,0]$$

  以下省略．これ以下は直接計算した方が早い．

- 2倍公式を用いた場合

$$\left[\frac{1}{64}\right]=[1]$$

$$\left[\frac{1}{32}\right]=\left[2\times\frac{1}{64}\right]=[2\times1]=[2]$$

$$\left[\frac{1}{16}\right]=\left[2\times\frac{1}{32}\right]=[4]$$

$$\left[\frac{1}{8}\right]=[8]=[7,2]=[6,2,1]=[5,2,1,0]$$

$$\left[\frac{1}{4}\right]=\left[2\times\frac{1}{8}\right]$$
$$=[2\times5,2\times2,2\times1,2\times0]$$
$$=[10,4,2,0]=[5,3,1]$$

$$\left[\frac{1}{2}\right]=\left[2\times\frac{1}{4}\right]=[10,6,2]$$
$$=[5,4,3,2,1,0,6,2]=[4,3,1]$$

4. 一般の位相点の計算

要素 $[n]$ $(n<T)$ の位相は n を2進数に分解することにより容易に得られる．

いま，$n=\sum_{r=0}^{p-1}k_r2^r$ $(k_r=0,1)$ と表せたとすると，

$$[n]=\sum_{r=0,k_r\neq0}^{p-1}[2^r]$$

である．ここで，$2^r=\frac{1}{2^{p-r}}$ より，$k_r\neq0$ なる項についての円分位相点の和で表される．

4.1 数 値 例

$p=6$，$q=1$ の場合

- 周期の $\frac{3}{4}$ 位相を求める．

$$\left[\frac{3}{4}\right]=\left[\frac{1}{2}\right]+\left[\frac{1}{4}\right]$$
$$=[4,3,1]+[5,3,1]$$
$$=[3,2,1,0]$$

- 43の位相を求める．

  $43=2^5+2^3+2+1$ より

$$[43]=\left[\frac{1}{2}\right]+\left[\frac{1}{8}\right]+\left[\frac{1}{32}\right]+\left[\frac{1}{64}\right]$$
$$=[4,3,1]+[5,2,1,0]+[2]+[1]$$
$$=[4,0]$$

4.2 計算量について

各々の円分位相点は p 個以内の要素で表される．2個の円分位相点の和は，たかだか p^2 個以内の要素で，計算回数も p^2 回以内である．演算の途中では同じ要素どうしが縮約されるため，$2p$ 個以内の要素で表現される．要素の値が p 以上になる場合は，置換則を用いて0から $p-1$ の範囲に値が収まるように変形しておく．すなわち，計算領域としては，$2p$ 個の整数を要する．要素どうしの演算のみであるので，多倍長の整数演算は必要とされない．

一般の位相の計算は，最高で p 個の円分位相点の和となる．よって，計算回数としては，上述のように2個ずつ円分位相点の和を繰り返すので，多くとも p^2 回の計算を $p-1$ 回行えばよい．

4.3 数 値 例

引用文献と比較する意味で，$p=127$，$q=63$ と $p=521$，$q=168$ のM系列について位相点の計算例を**表1，2**に示す．

この結果から，従来，$\frac{3}{8}$ とか $\frac{5}{8}$ などの位相を求め

表1 円分位相点における要素 ($p=127$, $q=63$)
Table 1 Elements on the cyclotomic phase ($p=127$, $q=63$).

円分位相	要素
$\frac{1}{8}$	120, 112, 104, 96, 88, 80, 72, 64, 57, 56, 49, 48, 41, 40, 33, 32, 25, 24, 17, 16, 9, 1
$\frac{1}{4}$	112, 96, 80, 64, 49, 48, 33, 32, 17, 1
$\frac{3}{8}$	120, 112, 88, 80, 57, 56, 49, 48, 25, 17
$\frac{1}{2}$	96, 64, 33, 1
$\frac{5}{8}$	104, 96, 88, 80, 41, 33, 25, 17
$\frac{3}{4}$	112, 96, 49, 33
$\frac{7}{8}$	120, 112, 57, 49

表2 円分位相点における要素 ($p=521$, $q=168$)
Table 2 Elements on the cyclotomic phase ($p=521$, $q=168$).

円分位相	要素
$\frac{1}{8}$	456, 435, 414, 393, 372, 351, 330, 309
$\frac{1}{4}$	391, 349, 307, 265
$\frac{3}{8}$	326, 305, 242, 221
$\frac{1}{2}$	261, 177
$\frac{5}{8}$	196, 175, 154, 133
$\frac{3}{4}$	131, 89
$\frac{7}{8}$	66, 45

るのは式の変形が人によるため面倒であったが，機械的に得ることができた．表に示された位相では，p に比べて $\frac{1}{6}$ から $\frac{1}{260}$ 個程度の要素からなるので，その位相のあたりではランダム性が低いといえる．

5. むすび

M系列の位相が $\frac{1}{2}, \frac{1}{4}, \ldots$ では，少ない要素の和で表されることが知られている．その計算は面倒であった．本報の方法は簡潔であり，かつ計算量も少なくてすむ．また，任意の位相についても計算が可能であることから，M系列を位相差を指定して利用する場合には有用である．

今後の課題としては任意のM系列の実現値，たとえば，すべて1であるとか，0101...01 となるようなタップルを与えて，位相を逆算する方法の開発が待たれる．

参考文献

1) 柏木 濶，原田博之：M系列の円分位相，計測自動制御学会論文集，Vol.18, No.10, pp.999–1004 (1982).
2) 柏木 濶，森内 勉：GF(2) 上の多項式を法とする演算の高速化，計測自動制御学会論文集，Vol.18, No.3, pp.300–303 (1982).
3) 山住富也，小池慎一：3項式M系列の円分位相点の計算法について，電気関係学会東海支部連合大会，p.639 (1998).

付録 3.1 の円分位相点の計算アルゴリズム

円分位相点を $\left[\frac{1}{2^r}\right]$ とする．

while $1 \geq i \geq r$
  if $i=1$ **then**
    式 (17) より右辺の要素を計算する;
    if 右辺第1要素の分子=奇数 **then**
      右辺第1要素の分子 $[p+1]$ を $[p+q+1, q+1]$ で置換する;
    else if 右辺第2要素の分子=奇数 **then**
      右辺第2要素の分子 $[p-q+1]$ を $[p-2q+1, 1-q]$ で置換する;
    endif
  endif
  if $2 \leq i \leq r$ **then**
    if 要素の値=偶数 $(2l)$ **then**
      要素を2で割る：$\frac{1}{2}(2l) \rightarrow l$;
    else if 要素の値=奇数 $(2l+1)$ **then**
      $\frac{1}{2}(2l+1) \rightarrow l+\frac{1}{2}$ として，$\frac{1}{2}$ 円分位相点を l だけシフト演算する;
    endif
  endif
  同じ要素がある場合は縮約する;
  要素の値が p を超えるか，負となる場合，式 (5) を用いて範囲を狭める;
end while

(平成11年2月1日受付)
(平成11年7月1日採録)

山住 富也（正会員）
昭和38年生．平成3年中部大学大学院工学研究科後期博士課程電気工学専攻修了．現在，名古屋文理大学情報文化学部情報文化学科講師．工学博士．

小池 慎一（正会員）
昭和16年生．昭和44年名古屋工業大学工学研究科修士課程修了．現在，愛知工業大学計算センター助教授．