愛知工業大学研究報告
第４１号Ｂ，平成１８年

スイッチ付きＭ系列の周期について

On a Period of M-Sequences with Switching Term

小池慎一 †, 山住富也 ††
Shin-ichi KOIKE, Tomiya YAMAZUMI

Abstract Let two M-sequences be $x(n|p_1,q_1)$ and $y(n|p_2,q_2)$ and define $z_n = z_{n-p_1} + x_{z-q_1} + f(n)$, where $f(n)$ is as follows: $f(n) = y_{n-k}$ or $f(n) = y_{n-k_1}y_{n-k_2},\ldots$. Sequence y_n is M-sequence switching term. When T_1 and T_2 are two periods of $x(n|p_1,q_1)$ and $y(n|p_2,q_2)$, a period z_n is $2T_1$ (case of x equals y) or T_1T_2 (else). Generating the sequece and estimating characteristic polynomial for some intervals of it, we get order p_1p_2 functions, by exapmle $1+x^2+x^4+x^7$, where $p_1=4$, $q_1=1$, $p_2=3$, $q_2=1$. These polynomials take different forms for each intervals.

1 はじめに

3 項式Ｍ系列は

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

で与えられる．ここに x_i は GF(2) の要素であり,0 または 1 の値をとる．加算は mod 2 で行われる．また，その周期は $T=2^n-1$ である．

この系列に別の M-系列の項からなる式を付加する．それを $f(n)$ とすると

$$x_n = x_{n-p} + x_{n-q} + f(n) \tag{2}$$

と表される．$f(n)$ が 1 項からのみなる場合には例えば $f(n)=y_{n-k}$ である.$f(n)$ の値が 1 を取る場合，それがない場合の系列 x_n の値の 0 と 1 が反転する．これは本来の系列の tuple が別の位置に分岐 (switching) したのと同様の効果をもつ，この系列をスイッチ項付きＭ系列と呼ぶ [1]. 以降, 単に' スイッチ付きＭ系列' と呼ぶ.

本報では，この系列の周期の構造を明らかにし，かつその特性多項式の推定が困難であることを数値例で示す.

†愛知工業大学経営情報科学部（豊田市）
††名古屋文理大学情報文化学部（稲沢市）

2 スイッチ付きM-系列の周期

2.1 準備

スイッチ付き M-系列の周期について述べるための準備として,3 項 M-系列の漸化式の性質について述べる.

[性質 1-1] 展開ごとに，項の数は 1 だけ増加するか 1 だけ減少する.

[証明] (1) 式の M-系列を以下の形式で表す [2].

$$[n] = [n-q, n-p] \tag{3}$$

n を右辺に移項する.

$$[\,] = [n, n-q, n-p] \tag{4}$$

これは 3 個の添え字が右辺に見られるような関係にある場合には，それらの項は消去されることを意味する.

(3) 式の右辺の最大の項について展開して

$$[n-q] = [n-2q, n-q-p, n-p] \tag{5}$$

を得る．以下同様にして最大の項について展開を繰り返すと，ある時点で

$$[n-i] = [n-j_1, n-j_2, ..., n-j_k] \quad (j_1 < j_2 < \cdots < j_k) \tag{6}$$

の形をとる．この場合 k 個の項がある.

これを (3) 式を用いて右辺の最大の項で展開するわけであるが，

1. $j_2, j_3, ..., j_k$ の中に $j_1 - q$ または $j_1 - p$ に等しいものが存在する場合，展開された結果，項の数は１個減ずる．

2. 存在しない場合には，１個の項を展開して２個の項を得るので，項の数は１個増加する．

なお，1において，$j_2, j_3, ..., j_k$ の中に $j_1 - p$ と $j_1 - q$ に等しい項が２個存在する場合はない．何故ならば，もし存在すれば，(4) 式により，すでに消去されているからである．■

[性質 1-2] M-系列の周期を T とすると，展開して $[n] = [n - T]$ を得るためには，偶数回の展開が必要である．
[証明] 長さが１の１個の項を展開して最終的にやはり長さが１の１個の項を得る．そのためには，長さが１だけ増加する展開の個数と，１だけ減少する展開の個数が等しくなる必要がある．したがって，その回数は偶数回となる．■

[性質 2] 互いに素な整数値をとる２個の M-系列を考える．それらの周期を $T_1, T_2 (T_1 > T_2)$ とする．このとき，周期 T_1 の M-系列を T_2 個並べると，周期 T_1 のおのおのの系列の中の n 番目の添え字は，周期 T_2 の中の添え字として見た場合，すべて異なる値をとる．ここに n は $T_1 > n \geq 0$ の値をとる．
[証明] 周期 T_1 をもつ系列を連続して T_2 個生成する．そのとき m 番目の系列の n 番目の添え字を通算の添え字として k_m で表すと，

$$k_m = n + mT_1, (m = 0, 1, ..., T_2 - 1).$$

k_m が T_2 の周期を持つ系列の中では何番目の添え字であるかを調べる．

簡単のために $T_1 \bmod T_2 = t_1$ とおく．すると

$$k_m \bmod T_2 = n \bmod T_2 + mt_1 \bmod T_2$$

ここで右辺 $n + mt_1 \bmod T_2$ は，$m < T_2$ なので m の値により $0, 1, 2, ..., T_2 - 1$ のいずれかの値をとり重複はない．■

[数値例] 性質２の数値例として $T_1 = 31, T_2 = 15, n = 3$ の場合について表１に示す．周期が T_2 の系列についていずれも添え字の重複はない．

表 1: $T_1 = 31, T_2 = 15, n = 3$ の場合

m	k_m	$k_m \bmod T_2$
0	3	3
1	34	4
2	65	5
3	96	6
4	127	7
5	158	8
6	189	9
7	220	10
8	251	11
9	282	12
10	313	13
11	344	14
12	375	0
13	406	1
14	437	2

2.2 スイッチ項の系列と母系列の p, q が同一の場合

はじめにスイッチ項を生成する M-系列と母系列の M-系列のパラメータ p と q が同一の場合には周期が２倍の系列を生成することを示す．

[性質 3-1] スイッチ項の系列と母系列の $p, q (p > q)$ が同一の３項 M-系列の場合，生成される系列の周期はもとの系列の周期 $T = 2^p - 1$ の２倍となる．
[証明] スイッチ項を生成する M-系列の一般項を x_n，スイッチ項を $f(n)$ とすると以下のように表される．

$$x_n = x_{n-p} + x_{n-q} \quad (7)$$

$$y_n = y_{n-p} + y_{n-q} + f(n) \quad (8)$$

(8) 式の右辺の最大の添え字を持つ項 y_{n-q} を漸化式にしたがって展開すると

$$y_n = y_{n-q-p} + y_{n-2q} + f(n-q) + y_{n-p} + f(n) \quad (9)$$

を得る．右辺の y の項のうち，添え字の等しい項があればそれは消える．また，項 $f(\cdot)$ の引数は展開された y の添え字，すなわち $n - q$ となる．

この展開を繰り返すと，もとの系列の周期が T であることから，y_n の項は y_{n-T} の項になり，

$$y_n = y_{n-T} + f(n) + f(n-q) + ... + f(n-T+r)$$

を得る．ここに $f(n-T+r)$ の r は p または q である．

右辺の y_{n-T} についてこの手続きを繰り返すと

$$\begin{aligned} y_{n-T} &= y_{n-2T}+f(n-T)+(n-T-q) \\ &\quad +\ldots+f(n-2T+r) \end{aligned}$$

を得る．ところが，$f(\cdot)$ の項は周期 T の M-系列により生成された項の式であるので，$f(i)=f(i-T)$ である．したがって，$f(i)+f(i-T)=0\ (n-T>i>n-2T)$，すなわち $f(\cdot)$ の項は相殺されて消える．よって，

$$y_n = y_{n-2T}. \tag{10}$$

これより，y の周期は $2T$ であることがわかる．■

[数値例] $p=4, q=3, f(n)=x_{n-2}$ の場合について例を示す．

$$y_n = y_{n-3}+y_{n-4}+x_{n-2} \tag{11}$$

この生成式にしたがい y_{30}，つまり $2T$ 番目の項を展開する．

$$\begin{aligned} y_{30} &= y_{27}+y_{26}+x_{28} \\ &= y_{26}+y_{24}+y_{23}+x_{28}+x_{25} \\ &= y_{24}+y_{22}+x_{28}+x_{25}+x_{24} \\ &= y_{22}+y_{21}+y_{20}+x_{28}+x_{25}+x_{24}+x_{22} \\ &= y_{21}+y_{20}+y_{19}+y_{18}+x_{28}+x_{25} \\ &\quad +x_{24}+x_{22}+x_{20} \\ &= y_{20}+y_{19}+y_{17}+x_{28}+x_{25}+x_{24} \\ &\quad +x_{22}+x_{20}+x_{19} \\ &= y_{19}+y_{16}+x_{28}+x_{25}+x_{24}+x_{22} \\ &\quad +x_{20}+x_{19}+x_{18} \\ &= y_{15}+x_{28}+x_{25}+x_{24}+x_{22}+x_{20} \\ &\quad +x_{19}+x_{18}+x_{17} \\ &= y_{12}+y_{11}+x_{25}+x_{24}+x_{22}+x_{20} \\ &\quad +x_{19}+x_{18}+x_{17}x_{28} \\ &= y_{11}+y_{9}+y_{8}+x_{24}+x_{22}+x_{20} \\ &\quad +x_{19}+x_{18}+x_{17} \\ &= y_{9}+y_{7}+x_{22}+x_{20}+x_{19}+x_{18}+x_{17} \\ &= y_{7}+y_{6}+y_{5}+x_{20}+x_{19}+x_{18}+x_{17} \\ &= y_{6}+y_{5}+y_{4}+y_{3}+x_{19}+x_{18}+x_{17} \\ &= y_{5}+y_{4}+y_{2}+x_{18}+x_{17} \\ &= y_{4}+y_{1}+x_{17} \\ &= y_0 \end{aligned}$$

よって，$y_{30}=y_0$ となり，スイッチ付き系列の周期は母系列の周期 T の 2 倍となる．

2.3 スイッチ項の系列と母系列の p, q が異なる場合

スイッチ項の系列と母系列の p, q が異なり，かつそれらの周期が互いに素である場合について考察する．

[性質 4] 周期が互いに素な系列で，スイッチ付き系列を生成した場合の周期が個々の周期の積になる．

[証明] 2 個の M 系列のパラメータを $p_1, q_1(p_1>q_1)$，$p_2, q_2(p_2>q2)$ とする．スイッチ付き系列を

$$y_n = y_{n-p_1}+y_{n-q_1}+f(n) \tag{12}$$

とする．ここに，$f(n)$ は，x_n の系列の算術式である．

スイッチ項を生成する系列を

$$x_n = x_{n-p_2}+x_{n-q_2}\ (p_2>q_2)$$

とおく．(12) 式からスイッチ項 $f(n)$ を除いた母系列の周期は $T_1=2^{p_1}-1$，スイッチ項の系列 x_n の周期は $T_2=2^{p_2}-1$ であり，T_1 と T_2 は互いに素であるとする．

ここで，$N=T_1T_2$ として，(12) 式の右辺の y_i の項の最大なものについて，逐次展開していく．$f(n)$ については，展開ごとに展開される項の添え字を引数として持つ項が生成される．

最終的には

$$y_N = y_{T_1T_2} = y_0+\Sigma\ f(i)$$

の形の式を得る．

上式の和の中の関数 $f(\cdot)$ の引数について調べる．

展開は y_i の右辺の最大の添え字を持つ項についてなされる．その添え字に対応して $f(i)$ が加えられていく．

[性質 1-2] で調べたように，y_i の項は周期 T_1 内で相殺され最後に y_0 のみが残る．他方 [性質 2] で得られたように，周期 T_1 で数えた n 番目の項に対応するスイッチ項の関数 $f(k_m)$ は，周期 T_2 の系列内では 0 から T_2-1 の添え字に対応する．展開は偶数回なされるので，$f(k_m \bmod T_2)$ の項も偶数個存在する．すなわち，和 $\sum f(i)=0$.

したがって，

$$y_{T_1T_2} = y_0$$

となり，周期は T_1T_2 である．■

3　系列の特性多項式の性質について

(7),(8) 式で与えられるようなスイッチ付き系列とよく似ているものに混合系列がある．
x_n, y_n を 2 個の系列, その和を z_n とすると，

$$\begin{aligned} x_n &= x_{n-p_1} + x_{n-q_1} \\ y_n &= y_{n-p_2} + y_{n-q_2} \\ z_n &= x_n + y_n \end{aligned}$$

x_n と y_n の特性方程式を

$$\begin{aligned} f_1(x) &= 1 + x^{p_1-q_1} + x^{p_1} \\ f_2(x) &= 1 + x^{p_2-q_2} + x^{p_2} \end{aligned}$$

とおく．$f_1(x)$ は p_1 次の多項式,$f_2(x_0)$ は p_2 次の多項式である．これらを加え合わせた混合系列の特性多項式は

$$f_3(x) = f_1(x) f_2(x)$$

であることが知られている．なお周期は T_1T_2 である．

それに対して, スイッチ付き系列の場合に生成された系列データに対して Berlekamp-Massey の推定式を求めてみる．例として 3 次のスイッチ項を持つ 4 次の系列で推定に用いるデータを重複しない別々の 3 区間で計算してみる．すると以下に示すように 3 種類の特性多項式が得られた．

スイッチ項を生成する M-系列の特性多項式を $f_1(\cdot)$, 母系列を生成する系列の特性多項式を $f_2(\cdot)$ とすると

$$\begin{aligned} f_1(x) &= 1 + x^2 + x^3 \\ f_2(x) &= 1 + x^3 + x^4 \end{aligned}$$

である．

上式によるスイッチ付き M-系列で生成されたデータを読み込んで推定すると, 以下の別々の特性多項式が得られた．

$$\begin{aligned} f_3(x) &= 1 + x + x^2 + x^3 + x^7 \\ f_4(x) &= 1 + x + x^3 + x^4 + x^5 + x^6 + x^7 \\ f_5(x) &= 1 + x^2 + x^4 + x^7 \end{aligned}$$

これらは次数はいずれも 7 次であるが, 式の形は異なる．区間によって別々の特性多項式を持つ系列とでも言うような性質である．言うまでもなく, $f_1(\cdot), f_2(\cdot)$ をもつ系列から得られる混合系列の特性多項式 $1 + x^2 + x^3 + x^5 + x^7$ とも異なる．

4　結論および考察

前報 [1],[3] で実験的に得られていたスイッチ付き M-系列の周期についてその仕組みを明らかにした．すなわち，スイッチ項の系列と母系列に同じ系列を用いた場合に元の系列の 2 倍, 異なる系列を用いた場合にはそれらの周期の積になる．

他方，Berlekamp-Massey により推定された特性多項式は, スイッチ項と母系列を生成する M-系列の特性多項式の次数の和になるが, 式そのものは別のものとなることが数値例で示された．

今後，この系列の特性多項式の性質についてさらに調べたい．

参考文献

[1] 小池慎一, 山住富也, "スイッチ項を持つM系列の統計的性質について", 愛知工業大学研究報告 No.40, pp.237-242, (2005)

[2] 小池慎一, 山住富也, "M系列の位相点の計算法", 情報処理学会論文誌　No.40, pp.3608-3611, (1999)

[3] 山住富也, 小池慎一, "スイッチ付M系列について (2)", 電子関係学会東海支部, o-281, (2005)

(受理　平成 18 年 3 月 18 日)