愛知工業大学研究報告
第 43 号　平成 20 年

スイッチ項付きM系列の性質について

On M-Sequence with Switching Term

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

Abstract　Using a M-sequence and 0-1 switching sequence, a new sequence is generated with $x_n=x_{n-p}+x_{n-q}+s_j$ mod 2. The sequence is considered as tuple sequence. Where the tuple is a vector $(x_i, x_{i+1}, ..., x_{i+p-1})$, $x_i \in$ M-sequence. The switching sequence disturbs original sequence , then we get another tuple's random sequence. This sequence has period T_2 or T_1T_2. The period is determined by phase of switching term for mother M-sequence.

We have good statistical property for some examples. But if sw sequence having 1's-term are very few, then statistical property is not good.

1. はじめに

３項式M系列

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

の周期は$T = 2^p - 1$で与えられる. 適当なp, qを選べば十分に長い周期のものも得られる．しかし，生成式(1)は線形であり，容易にそのパラメタは推定される．それを防ぐために，別のM系列を用意して，式(1)で生成される系列を攪乱することにより, 周期が長くパラメタの推定も困難であることを報告してきた．[1,2]

これまでは, 系列の出現する値に注目してその性質を論じてきたが，ここでは，式(1)で生成される系列を大きさpの tuple の系列とみて性質を調べてみた．その結果，攪乱する系列はM系列である必要はなく，任意に与えた 0, 1 からなる周期系列でよいことが分かった.

2. tuple の系列と見たM系列

式(1)で生成される系列$x_0, x_1, x_2, \cdots, x_{n-1}, \cdots$を$p$個ずつの tuple の系列とみなす．すなわち，

$$(x_0, x_1, \cdots, x_{p-1}), (x_1, x_2, \cdots, x_p), \cdots \\ , (x_{T-1}, x_T, \cdots, x_{T+p-2}), \cdots. \tag{2}$$

ここで，おのおのの'(' と')' で囲まれた tuple を$t_i, i = 1, 2, \cdots$で表すと，式(2)の系列は

$$t_1, t_2, \cdots, t_T, \cdots \tag{3}$$

で表される．M系列のパラメタp, qおよび初期系列が与えられれば, 式(3)のおのおのの tuple の内容は確定する．別の言い方をすれば，tuple の内容は初期系列により異なってくる.

異なる tuple の個数は式(1)で与えられるM系列の周期T個だけある．$T+1$番目の tuple は1番目の tuple に等しい．すなわち

$$t_i = \begin{cases} t_T, & (i \bmod T = 0) \\ t_{i \bmod T}, & (i \bmod T \neq 0) \end{cases}. \tag{4}$$

M系列の生成式(1)にこの系列を攪乱する目的で　生成される系列からの出力値sを加える．すなわち，

$$x_n = x_{n-p} + x_{n-q} + s \quad (p > q, s = 0, 1). \tag{5}$$

式(5)のsの値が 0 の場合には, 式(5)は式(1)と等しい．しかし，１の場合には左辺のx_nの 0,1 は反転する．これ

†　愛知工業大学　経営上科学部情報科学科（豊田市）
††名古屋文理大学　情報文化学部情報メディア学科（稲沢市）

を tuple の立場からみると 0 の場合には現在の tuple の式(1)に基づく次の tuple が生成されるのに対して 1 の場合には別の tuple が生成される．これを以下の式で表す．

$$succ(t_i, s) = \begin{cases} t_i, & (s=0) \\ t_j, & (s=1) \end{cases} \qquad (6)$$

スイッチ項を加えることにより，通常のM系列では生じない以下のようなことが起きる．

■性質１　すべてが 0 からなる tuple の生成

tuple の先頭(左端)の値のみが 1 で残りは 0 の tuple の場合，それを t_j とすると

$$succ(t_j, 0) = (0,0,\cdots,0) = t_0 \quad (say) \qquad (7)$$

となる．ここで，すべてが 0 の tuple を t_0 とおいた．

tuple t_0 は通常のM系列では唯一生成されない tuple である．

次に，M系列では，同一の tuple が連続して生成されることはないが，式(5)において $s=1$ の場合にはそれが生ずる．すなわち，tuple のすべての要素が 1 の場合には式(5)の右辺が $1+1+1=1 \bmod 2$ となるので，続く tuple は同一のものとなる．

■性質２　すべて 1 からなる tuple の連続

tuple の要素がすべて 1 の場合続く tuple も同一の tuple となる．

式で表せばすべてが 1 からなる tuple を t_j とした場合

$$succ(t_j, 1) = t_j \qquad (8)$$

となる．

3. スイッチ系列と周期

最初に，M系列を tuple の系列と見た小さい数値例を示す．

サンプルは $p=3, q=1, T=7, t_1=(100)$ の系列である．tuple としては添え字が 1 から 7 までの 7 個ある．これに，スイッチ系列の値が 0 と 1 の場合の tuple の遷移を以下に表に示す．t_4 は $(1,1,1)$ であって，すべてが 1 の tuple である．

$s=0$ の列が通常のM系列の tuple の系列になる．t_0 は出現しない．

$s=1$ の列は

$$t_1 \to t_0 \to t_2 \to t_7 \to t_6 \to t_3 \to t_5 \to t_1 \to$$

となり，t_4 が出現しない．

スイッチ系列は 0 と 1 とがある比率で交互に出現するので，上記の例は特別な場合であるが，t_0 と t_4 が式(7)，式(8)に示される特別な性質を持つことが暗示される．

表１　tuple の遷移 (p=3,q=1)
初期 tuple= (1,0,0)

現在の tuple t_i	次の tuple t_i	
	s=0	s=1
t_0	t_0	t_2
t_1	t_2	t_0
t_2	t_3	t_7
t_3	t_4	t_5
t_4	t_5	t_4
t_5	t_6	t_1
t_6	t_7	t_3
t_7	t_1	t_6

式(5)において，式(1)のM系列を母系列とよび，その周期を T_1 とする．また，スイッチ系列の周期を T_2 とする．ここには $T_2 > T_1$ とする．上のM系列を $T_1=7$ の母系列とし，$T_2=15$ のスイッチ系列を 000100010100010 とする．式(5)によって生成される系列の tuple は

$$t_1 \to t_2 \to t_3 \to t_4 \to t_4 \to t_5 \to \cdots \to t_7 \to t_1 \to \cdots$$

となり，周期は 15 である．すなわち，スイッチ系列のそれに同じとなる．

同じスイッチ系列を 3 だけ進めて 100010100010000 とすると，生成される系列は

$$t_1 \to t_0 \to t_0 \to t_0 \to t_0 \to t_2 \to \cdots \to t_7 \to t_1 \to \cdots$$

となる．周期は$7\times15=105$となる．
複数の数値例から以下のようなことが言える．

■性質３

母系列の周期T_1，スイッチ系列の周期T_2とする．ここにT_1とT_2は互いに素とする．
スイッチ系列を

$$s_0, s_1, s_2, \cdots, s_{T_2-1}, \cdots$$

とする．T_1+1の tuple とT_2のスイッチ系列の項の組み合わせはそれらの積$(T_1+1)\times T_2$個ある．

式(5)の系列においてそのすべてが出現すれば生成される系列の周期は$(T_1+1)\times T_2$になるはずであるが，実際は$T_1\times T_2$あるいはT_2となる．

どちらになるかは，スイッチ系列と母系列の初期値によって定まり予見は出来ない．

4. 統計的性質について

スイッチ系列により攪乱されるM系列の統計的性質については，攪乱する系列がM系列である場合についてはすでに報告されている．[2)]

ここでは，スイッチ系列についてランダム性を前提としない場合について調べる．

スイッチ系列がすべて０あるいは１の場合もスイッチとしての意味がないので除外する．

スイッチ系列が文字通りスイッチとして働き tuple の並びを攪乱するのはその値が１の場合である．

M系列を

$$y_n = y_{n-p_s} + y_{n-q_s}$$

として，スイッチ項を

$$s = y_{n-k} y_{n-l} \quad (0 \le k, l \le p_s)$$

あるいは

$$s = y_{n-k}(1 + y_{n-l}) \quad (0 \le k, l \le p_s)$$

などである．１の出現比率は概ね$1/4$となる．
そこで，１の出現比率をこの$1/4$程度になる系列について調べる．

また，母系列とスイッチ系列の２個の周期T_1とT_2の自己相関も調べてみる．これらの値が小さい場合には相関が大きくでるであろうが，大きい場合には相関は０に近いと予想される．

■スイッチ系列が一定パターンの場合

式(5)において，母系列を p=4, q=1（T_1=15）と p=6, q=1（T_1=63）の場合について，χ^2 値と自己相関係数を求めた．

スイッチ項 s は周期T_2がそれぞれ 31 と 127 のビット列で，00010001…のように，4 ビットごとに等間隔で１となる系列とした．ただし，T_2=31 の場合，系列の最後は……001000，T_2=127 の場合，同じく…001000 となる．生成された系列全体の周期は$T_1\times T_2$となり，それぞれ 465(=15×31)，8001(=63×127)である．

表 2，３にχ^2値と自己相関係数を示す．

χ^2検定は 3 種類（頻度，poker，run）行った．χ^2値の 5%有意水準は，それぞれ$\alpha_{0.05}$=3.84，$\alpha_{0.05}$=5.99，$\alpha_{0.05}$=7.82 である．

また，自己相関係数については間隔を，すぐ隣の項(lag=1)，母系列の周期(lag=T_1)，スイッチ系列の周期(lag=T_2)の 3 パターンについて求めた．

表２　χ^2値と自己相関係数（p=4,q=1，T_1=15）
スイッチ項 s の周期T_2=31（１の出現比率 1/4）

sの初期値	1000	0100	0010	0001
χ^2 値				
頻度	0.0216	0.0216	0.0216	0.0216
poker	0.821	0.252	0.252	0.252
run	10.3*	1.70	3.97	0.500
自己相関				
lag=1	−0.0172	−0.0129	−0.0129	−0.0172
63	−0.0302	−0.0302	−0.0302	−0.0431
127	−0.0647	−0.0647	−0.0604	−0.0819
0,1 の発生頻度				
0の個数	231	231	231	231
1の個数	234	234	234	234

母系列が p=4 の場合（表 2），p=6 の場合に比べて系列全体の周期が短いため，0,1 の発生頻度の差が χ^2 値や自己相関係数に影響し，大きな値となっている．run 検定では 5%有意水準を超えるパターンもある．

表 3 χ^2 値と自己相関係数（p=6,q=1, T_1=63）
スイッチ項 s の周期 T_2=127（1 の出現比率 1/4）

sの初期値	1000	0100	0010	0001
χ^2 値				
頻度	0.00125	0.00125	0.00125	0.0125
poker	0.307	0.556	1.30	0.288
run	0.198	0.324	3.42	4.33
自己相関				
lag=1	−0.0015	−0.0012	−0.0012	−0.0015
63	−0.00775	−0.00775	−0.00775	−0.00875
127	−0.0158	−0.0158	−0.0155	−0.0172
0,1 の発生頻度				
0の個数	3999	3999	3999	3999
1の個数	4002	4002	4002	4002

一方，p=6 の場合は χ^2 検定で有意差は見られないことから，頻度や出現パターンの偏りは見られない．自己相関も 0 に近い値となったことから良好な乱数が得られた．

次に，スイッチ項 s の周期 T_2 が 127 で，1 の出現比率が約 1/8 となるよう，00000001…と 8 ビットごとに等間隔で 1 となる系列について，同様の検定を行った．母系列は p=6, q=1 で系列全体の周期は 8001 である．検定の結果を表 4 に示す．

1 の発生頻度が 1/4 の場合（表 3）と比べて 1/2 となり，スイッチ系列 s の初期値によっては run 検定で 5%有意水準を超える場合が 3 とおりある．

スイッチ項の系列が 0 が多くなると，生成された系列で 0 の出現比率が多くなるなどのパターン偏りが生ずるので，1 の比率は 1/4 程度にするほうがよいと考えられる．

5. 結論

任意に与えた 0, 1 からなる周期系列をスイッチ系列として，M系列に付加して生成される系列の性質を調べた．スイッチ系列として，M系列ではなく 10001000…のようなほぼ等間隔で 1/4 の割合で 1 が出現するような周期系列を用いた場合にも，乱数として良好な性質を示すことが分かった．しかし，1 の発生頻度が 1/8 程度と少ない場合には乱数としてよくなかった．

表 4 χ^2 値と自己相関係数（p=6,q=1, T_1=63）
スイッチ項 s の周期 T_2=127（1 の出現比率 1/8）

sの初期値	10000000	01000000	00100000	00010000
χ^2 値				
頻度	0.00125	0.00125	0.00125	0.00125
poker	0.748	0.784	1.84	0.531
run	6.59	5.05	19.5*	1.90
自己相関				
lag=1	−0.0005	−0.00025	−0.00025	−0.00025
63	−0.008	−0.00825	−0.00825	−0.007
127	−0.017	−0.0152	−0.0168	−0.0155
0,1 の発生頻度				
0の個数	3999	3999	3999	3999
1の個数	4002	4002	4002	4002

sの初期値	00001000	00000100	00000010	00000001
χ^2 値				
頻度	0.00125	0.00125	0.00125	0.00125
poker	1.12	5.68	0.012	2.64
run	2.77	6.38	30.6*	9.31*
自己相関				
lag=1	−0.0025	−0.00025	−0.00025	−0.0005
63	−0.00725	−0.00775	−0.009	−0.00825
127	−0.0145	−0.0148	−0.016	−0.0152
0,1 の発生頻度				
0の個数	3999	3999	3999	3999
1の個数	4002	4002	4002	4002

参考文献

1) 小池，山住，”スイッチ付きM系列の周期について”，愛知工業大学研究報告 No.41B, pp. 203-206 (2006)

2) 山住，小池，“スイッチ系列により攪乱される系列の性質について”電気関係学会東海 O-011 (2007)

（受理 平成 20 年 3 月 19 日）