愛知工業大学研究報告
第４０号Ｂ，平成１７年

スイッチ項を持つM系列の統計的性質について

On Statistical Properties for M-Sequence with a Switching Term

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

Abstract A order n's M-sequence has $T(=2^n-1)$'s n-tuples, say M-sequence is n-tuple's sequence. By adding 2nd order term on the sequence, we take a nonlinear sequence. When the 2nd order term's value is 1, the following tuple is changed, so we call the term as "switching term". This sequence is nonlinear, then difficult to estimate it. In this paper, we show some statistical characteristics, uniform-, poker-, run-tests. In these test the characteristics aren't significant at 5%.

1 はじめに

先に２次Ｍ系列としてＭ系列の式に積の項を追加したものが非線形である故に,Barlekamp の推定式では生成式が推測されないことを示した [1]. また, ２次の項の働きをよく見ると, 系列を n-tuple の列に置き換えて見た場合, 系列をスキップすることに注目して, この２次の項の働きをスイッチと見なし, スイッチ付きＭ系列として報告した. ここでは, このスイッチ付きＭ系列の統計的性質を調べて報告する.

2 スイッチ項付きM系列

3 項式 M 系列は

$$x_n = x_q + x_0 \tag{1}$$

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 mod2 で行われる.

Ｍ系列はよく知られているように, 周期は $T=2^n-1$ であり,$x_0, x_1, ..., x_{n-2}$ の系列の中ですべてが 0 の n-tuple を除いたすべての n-tuple が出現する.

この系列に２次の積の項を追加したする. すなわち

$$x_n = x_q + x_0 + x_i x_j \tag{2}$$
$$(i, j \neq q, i \neq j, n-1 \geq i, j \geq 1)$$

すると積 $x_i x_j$ が 1 の値を取る場合に, 本来の系列の式の右辺に 1 が加わることになるので, 次の値の 0,1 が反対になる.n-tuple で言えば, 別の n-tuple となる. 系列を n-tuple を並べたもので考えると, 系列の流れが不連続に分岐することになる. この分岐をスイッチ (switch) と見なし, スイッチ項付きＭ系列と呼ぶ. 以降, 単に' スイッチ付きＭ系列' と呼ぶ.

3 tupleの系列として見た場合の系列と推移行列

Ｍ系列を n-tuple(以下 n-tuple を単に tuple と呼ぶ) の系列で考えてみる. 例えば,$n=4$ のＭ系列

$$x_4 = x_3 + x_0$$

は, 系列 000111101011001... を生成する.tuple で表すと,0001,0011,0111,1111,1110,... となる. ここで,tuple の数字の並びを２進数として読むと,1,3,7,15,14,... となる.tuple の推移は $1 \to 3 \to 7 \to 15 \to 14 \to$ となる. なお,tuple 0000 は２進数では 0 で tuple の推移は $0 \to 0$ である.

式 (1) で表されるＭ系列において, 先頭 bit が 1, 続く $n-1$ 個の bit が 0 からなる tuple, 例えば $n=4$ の場合は 0001 から出発して,tuple の列に順に 0,1,2... と番号を振る. 系列の初期値を表すのに, この tuple 列の番号を用いる. 例えば, 3 番目の tuple が 1111 であれば' 初期値として 1111 を用いる' と言う代わりに,' 3 番目の tuple を初期値とする' と言う.

†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）

tuple の推移を行列 M で表す [2]. 行と列の番号を 0,1,2,... として, それを tuple の 2 進数の値に対応させる.tuple i から tuple j への推移を行列の要素 $m_{ij}=1$ とする. 推移のない要素の場合には $m_{ij}=0$ とする. 上の例を行列で表せば以下のようになる.

$$M_1=\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0
\end{bmatrix}$$

この行列を 15 回掛けると単位行列 I になる. すなわち

$$M^{15}=I$$

形式的に

$$M=I^{-15}$$

と書ける.

系列が LFSR で生成される場合, 推移可能な tuple は tuple の値 $\times 2 \pmod{2^n}$ に 0 または 1 を加えた tuple である. したがって, 行列の要素 $x_{ij}=1$ となる位置には制限がある.

次に, スイッチ付き M 系列の例として上の系列に x_1x_2 を加えたものを調べる.

$$x_4=x_3+x_0+x_1x_2$$

この系列は長さ 9 の 000111001, 長さ 5 の 01011, 長さ 1 の 1 の 3 個の異なる周期を持つ系列を生成する. これを行列で 0000 の tuple を加えて行列で表すと以下のようになる.

$$M_2=\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0
\end{bmatrix}$$

この行列 M の行 6 と 12, 列 6 と 12, 行 5 と 14, 列 5 と 14 を入れ替えると, 以下の行列 M_3 を得る.

$$M_3=\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{bmatrix}$$

これをよく見ると対角要素が 1 であるものを別にすれば, 非 0 の要素を持つ以下の 2 個の部分行列が見られる.

$$P_1 = \begin{bmatrix} 0\,0\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1 \\ 0\,0\,0\,0\,1\,0\,0\,0\,0 \\ 1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0 \end{bmatrix}$$

$$P_2 = \begin{bmatrix} 0\,0\,0\,0\,1 \\ 0\,0\,1\,0\,0 \\ 0\,0\,0\,1\,0 \\ 1\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0 \end{bmatrix}$$

部分列に分解される系列は推移行列で表せば上のように分解されることがわかる.

P_1 を 9 回掛けると単位行列 I_9 に,P_2 を 5 回掛けると単位行列 I_5 を得る. したがって, 形式的に

$$P_1 = I_9^{-9},\ P_2 = I_5^{-5}$$

となる.

推移行列から,m_{ij} の値を書き換えて $M^n = I$ となるような行列に作りかえれば, その tuple の系列は行列の大きさの周期を持つ. しかし, それは LFSR で実現できるとは限らない. また, スイッチ項 x_ix_j が異なれば推移行列は別の値を取る.

4 統計的検定

スイッチ項を付加したM系列の周期は最大周期 2^n-1 より小さい. したがって, 2 次の性質を持ち生成式を推測されにくいと言う利点はあるが, 周期が短い部分列が含まれることが欠点である.

そこで, 生成された系列が一回りしたらスイッチ項自体を切り替える方法を考えた [3]. その周期については, おおむね 10 倍程度になることが実験的に確かめられた (本論文で用いたデータでは, 後の表に示されるようにおおむね 10-20 倍である).0 と 1 の出現頻度についてもほぼ半々で満足すべきものであった.

しかし, その他の統計的性質については調べられていなかったので, 次節に示すような方法で発生させた系列について, ポーカー検定, 連の検定による調査を行った. 以下にその結果を述べる.

4.1 系列の生成方法

調査したのは $n = 10$ および $n = 11$ の 2 種類のスイッチ付 M 系列である. すなわち,

$$x_{10} = x_2 + x_0 + x_ix_j \tag{3}$$

$$x_{11} = x_3 + x_0 + x_ix_j. \tag{4}$$

具体的な系列の生成方式を $n = 11$ の場合について以下に述べる.$n = 10$ の場合も同様である.

まず, 式 (4) において, 初期 tuple をランダムに与える.

スイッチ項 x_ix_j は初めに $i = 1, j = 2$ とし, 1 周期生成された時点, すなわち同じ tuple が出現したところで j を 1 ずつ $2 \le j \le 10 (j \ne q = 3)$ の範囲で書き換えながら系列を発生する.

ここで, 1 つのスイッチに対し同じ tuple が系列の中で初期値と 1 周期発生時点の 2 度出現する. そこで, スイッチ項 x_ix_j を書き換えるときに最後の tuple は捨て, その直前の tuple を初期値として, 改めて系列を発生する.

$j = 10$ まで生成したところで,$i = 2, j = 3$ とし, 同様に $3 \le j \le 10 (j \ne 3)$ の範囲で書き換える. 以下,$i = 9, j = 10$ までスイッチ項のすべての組み合わせについて連続的に生成し, スイッチ付 M 系列の 1 周期とする.

4.2 検定について

スイッチ付 M 系列の統計的性質を調べるため, 3 種類の検定 (1 次元度数検定, ポーカー検定, 連の検定) を行う. 各検定において, 初期値の異なる系列 100 通りを発生し, それぞれ χ^2 値の適合度検定 (有意水準 5%) を行う.

- 1 次元度数検定
  1 周期全体について 0,1 の出現頻度を数え上げ,χ^2 値を求めて適合度検定を行う.

  χ^2 値は以下の式で計算する.

$$\chi^2 = \sum_{i=1}^{k} \frac{(n_i - np_i)^2}{np_i} \tag{5}$$

  ここで, クラス数 $k = 2$, 自由度は $k - 1 = 1$ で,5%有意水準 $\alpha_{0.05} = 3.84$,n はサンプル数 (1

表 1: 一次元度数検定 ($\alpha_{0.05} = 3.84$),$n = 11, q = 2$

No.	開始 tuple	周期	実測値の χ^2 値
1	130	35306	0.01
2	747	37343	0.35
3	1090	36634	0.01
4	1421	36599	0.01
5	976	35382	0.09
6	1219	36062	0.01
7	274	34182	0.46
8	431	36083	0.52
9	421	39771	0.15
10	816	33649	0.28
11	229	34683	0.77
12	1524	34796	0.15
13	362	37514	0.28
14	69	36097	0.45
15	1360	37344	0.01
16	1318	36318	0.85
17	110	39564	0.22
18	1993	35663	0.96
19	483	35926	0.01
20	508	34851	0.52
21	736	37142	0.10
22	1049	35486	0.08
23	1703	33699	0.81
24	509	38688	0.63
25	898	38934	0.21

表 2: ポーカー検定 ($\alpha_{0.05} = 5.99$),$n = 11, q = 2$

No.	開始 tuple	周期	実測値の χ^2 値
1	130	35306	2.65
2	747	37343	0.09
3	1090	36634	0.67
4	1421	36599	2.11
5	976	35382	0.95
6	1219	36062	0.82
7	274	34182	5.29
8	431	36083	0.17
9	421	39771	0.65
10	816	33649	1.61
11	229	34683	2.13
12	1524	34796	0.10
13	362	37514	1.75
14	69	36097	1.18
15	1360	37344	0.40
16	1318	36318	0.09
17	110	39564	2.29
18	1993	35663	0.88
19	483	35926	2.71
20	508	34851	0.65
21	736	37142	3.02
22	1049	35486	4.42
23	1703	33699	1.52
24	509	38688	0.01
25	898	38934	7.04*

周期）,$p_i (i = 0, 1)$ は 0.5,n_i は 0,1 の出現頻度である.

- ポーカー検定
  系列の連続する 5 個を 1 つの組みとし, ポーカーの手役の出現頻度を数え,χ^2 値を求めて適合度検定を行う.5 個の値はすべて 0 か 1 なので, 手役は 5-cards(aaaaa), 4-cards(aaaab), full-house(aaabb) の 3 種類となり, クラス数 $k = 3$ である. 各手役の出現率 $p_i (i = 1, 2, 3)$ は, 順に p_1=6.25%, p_2=31.25%, p_3=62.5%, 自由度は $k - 1 = 2$ で 5%有意水準 $\alpha_{0.05} = 5.99$ である.χ^2 値は式 (5) において,5bit1 組なのでサンプル数 n は 1 周期の 1/5,n_i は各手役の出現度数となる.

- 連の検定
  スイッチ付 M 系列の値 16 個を並べて 1 つの整数を生成する. ただし, 整数の隣り合う bit は位相差をそれぞれ 16bit となるようにする. このようにして作られた整数の上昇連（直前の値より大きい値となる）の長さを調べる. 連の長さは 1,2,3 および 4 以上の 4 種類とし, 出現頻度を数え,χ^2 値を求めて適合度検定を行う. 長さ i の連の出現率 $p_i (i = 1, 2, 3, 4)$ は, 長さ 1 の連から順に,p_1 =33.4%, p_2=41.7%, p_3=18.3%, p_4=6.6%である. クラス数 $k = 4$ で, 自由度は $k - 1 = 3$,5%有意水準 $\alpha_{0.05} = 7.81$. である.χ^2 値は式 (5) において,16bit 1 組なのでサンプル数 n は 1 周期の 1/16,n_i は長さ i の連の出現度数となる.

4.3 検定の結果

はじめに, 周期について検討する. 表 1 より,$n = 11$ の場合周期の最小=34182, 周期の最大=39564 であり,

表 3: 連の検定 ($\alpha_{0.05} = 7.81$),$n = 11, q = 2$

No.	開始 tuple	周期	実測値の χ^2 値
1	130	35306	2.12
2	747	37343	0.41
3	1090	36634	2.69
4	1421	36599	0.89
5	976	35382	0.41
6	1219	36062	2.27
7	274	34182	1.27
8	431	36083	0.17
9	421	39771	1.21
10	816	33649	0.55
11	229	34683	1.93
12	1524	34796	0.52
13	362	37514	1.78
14	69	36097	1.35
15	1360	37344	0.52
16	1318	36318	0.90
17	110	39564	0.23
18	1993	35663	1.75
19	483	35926	1.30
20	508	34851	0.11
21	736	37142	0.83
22	1049	35486	1.67
23	1703	33699	1.47
24	509	38688	1.45
25	898	38934	0.58

表 4: 一次元度数検定 ($\alpha_{0.05} = 3.84$),$n = 10, q = 3$

No.	開始 tuple	周期	実測値の χ^2 値
1	130	13796	0.34
2	752	13565	0.29
3	67	13168	0.01
4	403	15692	0.01
5	979	15535	0.01
6	204	10961	0.69
7	277	14383	7.71
8	442	14929	0.01
9	436	12529	0.55
10	820	13435	1.70
11	236	13782	0.01
12	502	15654	0.23
13	373	12995	0.41
14	78	13745	0.29
15	337	12180	2.26
16	297	14436	0.72
17	123	15450	0.14
18	980	12775	0.01
19	495	13569	0.10
20	521	11892	0.11
21	751	14032	0.55
22	29	13330	0.20
23	686	13787	0.50
24	524	15014	0.33
25	911	12641	0.54

元のM系列の周期2048の16.7～19.3倍である. 他方, 表4より,$n = 10$の場合, 周期の最小=10961, 周期の最大=15962であり, もとのM系列の周期1024の10.7～15.6倍である.$n = 11$の方が倍率が大きいのは, スイッチ項が$n = 10$の場合より多いことに寄る妥当な結果である.

1次元度数検定の結果（始めの25個）を表1と表4に示す. ここで, 開始tupleとは式(3)の初期値であり,3節で定義したtuple列の番号である.

$n = 11, n = 10$いずれの場合もχ^2値は5%有意水準$\alpha_{0.05} = 3.84$以内に収まっているので,0,1の出現頻度について偏りは見られない.

次にポーカー検定の結果を表2と表5に示す.100個のχ^2値のうち5%有意水準$\alpha_{0.05} = 5.99$を越えたものは$n = 11$の場合7個(7%),$n = 10$の場合2個(2%)で,5bitごとの組み合わせの検定についても, 特に有意差は見られない.

連の検定の結果を表3と表6に示す.$n = 11$の場合,100個のχ^2値のうち5%有意水準$\alpha_{0.05} = 7.81$を越えたものはなく, 時系列の出現パターンについても有意差は見られない. 対して,$n = 10$の場合,5%有意水準を越えたものが18個(18%)検出された. 今後の検討課題である.

5 まとめ

スイッチ付M系列を, 系列が一回りしたらスイッチ項を次々と書き換えることにより得られる長周期の系列について性質を調べた.

その結果, 1次元度数検定, ポーカー検定については有意差は見られなかった. 連の検定については$n = 10$の場合について有意差が認められたので検討課題である.

表 5: ポーカー検定 ($\alpha_{0.05} = 5.99$),$n = 10, q = 3$

No.	開始 tuple	周期	実測値の χ^2 値
1	130	13796	1.67
2	752	13565	1.51
3	67	13168	1.48
4	403	15692	0.34
5	979	15535	0.40
6	204	10961	2.60
7	277	14383	1.93
8	442	14929	2.38
9	436	12529	0.11
10	820	13435	0.15
11	236	13782	2.81
12	502	15654	1.49
13	373	12995	1.61
14	78	13745	1.09
15	337	12180	2.33
16	297	14436	1.98
17	123	15450	0.49
18	980	12775	0.90
19	495	13569	0.67
20	521	11892	2.01
21	751	14032	3.34
22	29	13330	1.12
23	686	13787	2.12
24	524	15014	0.12
25	911	12641	1.75

表 6: 連の検定 ($\alpha_{0.05} = 7.81$),$n = 10, q = 3$

No.	開始 tuple	周期	実測値の χ^2 値
1	130	13796	5.65
2	752	13565	4.68
3	67	13168	4.49
4	403	15692	2.91
5	979	15535	8.25*
6	204	10961	2.96
7	277	14383	1.08
8	442	14929	5.41
9	436	12529	8.77*
10	820	13435	3.93
11	236	13782	0.47
12	502	15654	3.40
13	373	12995	0.07
14	78	13745	1.71
15	337	12180	10.92*
16	297	14436	0.57
17	123	15450	0.22
18	980	12775	7.20
19	495	13569	0.63
20	521	11892	3.75
21	751	14032	2.53
22	29	13330	1.21
23	686	13787	3.72
24	524	15014	1.53
25	911	12641	0.91

また今後は, 系列を発生するスイッチ項の書き換え方法についても検討する.

参考文献

[1] 小池慎一, 山住富也, "２次M系列の線形複雑度について", 愛知工業大学研究報告　No.39, pp.142-145, (2004)

[2] D. Ferreo,R.Gonzalo,M. Soriano "Some Properties ofNon-Linear Feedback Shift Registers with Maximum Period", Sixth International Conference on Telecommunications Systems. Nashville (1998)

[3] 山住富也, 小池慎一, "スイッチ付M系列について", 電子関係学会東海支部, o-351, (2004)

(受理　平成 17 年 3 月 17 日)