２次Ｍ系列の線形複雑度について

On Linear Complexity of a Quardratic M-sequence

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

Abstract M sequence is known as good random number generating algorithm. However, its linear complexity is very small for stream cipher. On the other hand, there is a quardratic M-sequence which added the secondary term to the generation formula. Then, expecting quardartic m-sequence [1] has large complexty, we investigate its sequeces and complexity. As the results, we get: (1) one m-sequence is divided some partial sequences, (2) those linear complexity take neary periods.

1　はじめに

乱数発生アルゴリズムとしても知られるＭ系列は，良好な統計的性質を持つが，線形複雑度が低いために暗号用の乱数としては使用が困難である．本報告では，１次の生成式を持つＭ系列に積の項を追加した２次Ｍ系列 [1] について，その性質を概観するとともに，線形複雑度について調べてみる．

2　２次Ｍ系列とは

Ｍ系列は，LFSR(Linear Feedback Shift Register) によって生成される最大周期長を持つ系列のことである．LFSR の電気的出力は論理値として０と１で表される．そこでＭ系列も０と１の並んだ系列となる．

普通，Ｍ系列を生成する式は，i 番目の値を $x_i(i = 0, 1, 2, ...)$ として

$$x_n = k_{n-1}x_{n-1} + k_{n-2}x_{n-2} + ... + k_ix_i + ... \\ +k_1x_1 + k_0x_0(k_0 = 1, k_i = 0 \text{ または } 1) \quad (1)$$

となる線形一次式で与えられる．

初期値として $x_{n-1}, x_{n-2}..., x_0$ を与えると x_n が得られる．次に，添字を１個ずらして，x_n を x_{n-1}, x_{n-1} を $x_{n-2}, ...$ として，新しい x_n を得る．このようにして，次々に新しい値を得ることにより，ある系列を得る．

上式で $x_{n-1} = x_{n-2} = ... = x_0 = 0$ とすべての x_i が値０をとる場合には，x_n は０となるので，以降０以外を生成しないので，初期値としてはすべて０を除く．

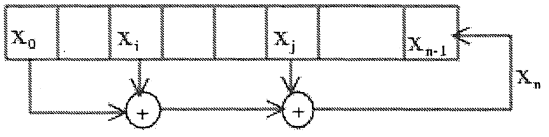

図 1: LFSR の例 $x_n = x_0 + x_i + x_j$

また，$x_{n-1}, x_{n-2}, ..., x_0$ のように連続した n 個の０と１からなる系列を n-tuple と呼ぶ．ここに，n は tuple の長さを表す．ここでは n を省略して単に tuple と呼ぶ．

(1) 式によって次々に生成される値にしたがって，新しい tuple が作られていく．tuple の長さは n なので，０と１からなる可能な組み合わせの数は 2^n 通りである．その内の，すべて０のものを除くと $2^n - 1$ 通りある．これが異なる tuple の最大の個数であり，これらすべて表れるような系列をＭ系列と呼ぶ．もし，$2^n - 1$ 通りの tuple のうち，途中で同じものが表れると，以降はその点までの繰り返しとなるので短い周期の系列になる．図１は，LFSR の例である．x_i と x_j でフィードバックがかかっている．ここで，２次のＭ系列を考えてみる．x_i は０と１のみをとるので，

$$x_i^2 = x_i$$

である．したがって，通常の代数の場合のように２乗の項は考えない．しかし，２個の項の積，

$$x_ix_y(i \neq j)$$

の項が考えられる．これを２次の項としてＭ系列に

[†]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）

加えたものを２次のＭ系列と呼ぶ．以下にその性質について調べる．

2.1 ２次Ｍ系列の周期について

２次Ｍ系列の場合，もとのＭ系列と同じ周期を持つ場合もあるが，n が大きくなると周期の小さな複数の系列のみとなる．以下２次Ｍ系列の振る舞いについて述べる．

ここで，もとのＭ系列の式を３項式としておく．すなわち

$$x_n = x_{n-p} + x_0 = g(n,p) \tag{2}$$

以下の議論のために i,j,k を $n-p$ でも０でもなく，かつそれらはどの２個も等しくないとする．

また，x_m から始まる長さ n の tuple を $tuple(m)$ で表す．

1. x_ix_j を加えた場合

$$x_n = x_{n-p} + x_ix_j + x_0 = g(n,p) + x_ix_j \tag{3}$$

この場合，x_i と x_j が共に１の場合のみ $x_ix_j = 1$ となり，他の場合には $x_ix_j = 0$ である．

$x_ix_j = 0$ の場合には $g(n,p)$ の生成する値がそのまま右辺の値となり，(2) 式の値に一致する．したがって，次の tuple はＭ系列のそれと一致する．

それに対して，$x_ix_j = 1$ の場合には，右辺の値は $g(n,p)$ の値の０と１を反転させたものとなる．すると，次の tuple はＭ系列で得られる tuple の順序とは別の位置の tuple となる．

tuple の中で i 番目と j 番目の値が共に１となるのは1/4の割合であるので，平均すれば，Ｍ系列を連続して４個生成する毎にことなる tuple への分岐が生ずる．図２は，LFSR の例である．x_i と x_j でフィードバックがかかっている．

2. 文献 [1] で device と呼ばれている $x_i + x_ix_j$ を加えた場合

$$x_n = g(n,p) + x_i + x_ix_j \tag{4}$$

$x_i = 1, x_j = 0$ の場合にのみ，$x_i + x_ix + j = 1$，その他は０となる．場合１と分岐する tuple は異なるが統計的な振る舞いは同様である．

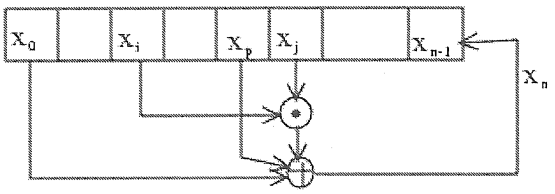

図 2: ２次の LFSR の例 $x_n = x_0 + x_p + x_ix_j$

3. $x_i + x_jx_k$ を加える場合

$$x_n = g(n,p) + x_i + x_jx_k \tag{5}$$

この場合には $x_i = 0, x_j = x_k = 1$ の場合と $x_i = x_j = 1, x_k = 0$ の場合に $x_i + x_jx_k = 1$ となり，他は０である．やはり，1/4 の tuple で分岐が生ずる．

ここでは場合２で述べた，device と呼ばれる $x_i + x_ix_j$ の項を追加した２次Ｍ系列について考察することにする．

2.2 系列の例

1. 周期がもとのＭ系列と一致する場合

もとのＭ系列を $n = 5, p = 3$ とすると生成式は次式となる．

$$x_5 = x_0 + x_2$$

初期値として $x_0 = 1, x_1 = x_2 = x_3 = x_4 = 0$ とした場合，発生される系列は周期=31 で以下となる．

1000010010110011111000110111010...(系列 1)

これより，$tuple(0) = 10000$, $tuple(1) = 00001$, $tuple(2) = 00010, ...$ である．

次に，２次の項として $x_4 + x_1x_4$ を加えた２次Ｍ系列は次式となる．

$$x_5 = x_0 + x_2 + x_4 + x_1x_4$$

上式に同一の初期値を与えて得られる系列は以下となる．

1000011101011001101111100010010...(系列 2)

もとの系列と較べると，x_6 ですでに異なっている．$x_5+x_2x_5$ を調べてみると，$x_5=1, x_2=0$ より，この項は 1 となり，元の系列の場合には 0 となるところが，1 となる．新しい tuple(=00011) はもとの系列で言えば $tuple(19)$ である．

tuple の系列で表すと，この系列は

$$0, 1, 19, 12, 24, 25, ..., 30, 0, 1..$$

となる．これはもとの系列を入れ替えたものである．

2. 部分列を生成する場合

2 次 M 系列の周期は，加える 2 次の項により，元の系列と一致する場合もあるが，多くは一致しない．すなわち，部分列となる．

上の例で，2 次の項を $x_1+x_1x_3$ とした場合，生成式は以下となる．

$$x_5 = x_0 + x_2 + x_1 + x_1x_3$$

上式により，以下の 3 個の部分列を得る

部分列 1	周期 = 18	100001001111100101
部分列 2	周期 = 9	010001101
部分列 3	周期 = 4	1101

$n = 15, p = 7, i = 1$ の場合，$j = 2, 3, .., 14 (j \neq 8)$ について部分列の先頭の tuple の番号と周期を表 1 に示す．この場合の tuple は上の小さい例と同様に，初期値として $x_0 = 1, x_1 = x_2 = ... = x_{14} = 0$ から始めた場合に得られる tuple を基準にして記述してある．この場合，表から分かるように，周期が $2^{15}-1 = 32767$ となるものはない．

3 線形複雑度について

0,1 の値からなる m 個の系列が与えられたとき，それを生成できる LFSR の最小段数が線形複雑度である．M 系列の場合にはその次数となる．ここでは，n がその値である．段数が L の LFSR は $2L-1$ 個のデータがあれば，その構成は決定される．したがって，ストリーム暗号などに疑似乱数として使用する場合，線形複雑度が小さいと容易に推定されてしまう．M 系列の場合には，次数が n であると，$2n-1$ 個のデータが知られてしまえば，式 (1) は推定されてしまう．この値は一般に周期 2^n-1 に較べれば小さな値であるので，M 系列を用いる場合，Geffe 型の乱数などのように，複数個の M 系列を組み合わせて用いて線形複雑度を上げる工夫がなされる．

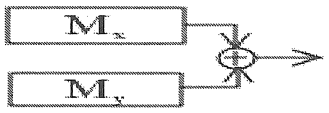

図 3: 2 個の M 系列の和の生成器

線形複雑度の推定には Berlekamp-Massey のアルゴリズム (以下 BM と略す) が知られている [2]．例えば，$n = 15, p = 7$ の M 系列のはじめの $2n-1 = 29$ 個のデータにより，推定式は

$$x^{15} + x^8 + 1 = 0$$

として得られる．すなわち，線形複雑度は 15 である．M 系列である場合には，次数の 2 倍-1 個のデータが入手できれば，生成式の推定は BM により簡単に出来てしまう．このように，線形複雑度がが小さければ，推定に必要なデータ数も少なくてすんでしまう．

そこで，線形複雑度を上げる方法がいろいろ考えられている．以下に例を 2 個示す．

- ［例 A］　2 個の M 系列の和の系列

  2 個の M 系列 M_x，M_y を

  $$x_3 = x_2 + x_0$$
  $$y_4 = y_3 + y_0$$

  とした場合，これらの和

  $$u_n = x_n + y_n$$

  の系列を混合 M 系列と言う [3]．15 個のデータを用いて BM で線形複雑度を求めると

  $$u^7 + u^5 + u^3 + u^2 + 1 = 0$$

  を得る．この多項式は，上の式の多項式表現の積であり，理論値と一致する．このように簡単に推定されてしまう．図??に，和の系列を示す．

- ［例 B］　Geffe 型系列の場合

表 1: 部分系列の周期 ($n = 15, p = 7, i = 1$)

j=2		j=3		j=4		j=5		j=6		j=7	
start	period	start	period	start	period	start	period	start	period	start	period
14	120	14	120	14	5163	14	24276	14	16165	14	20488
29	3717	28	28666	21	24230	29	4534	21	12937	35	197
44	291	115	365	57	2411	42	1969	56	2148	49	4628
45	22612	127	3294	196	217	197	1423	77	844	70	2322
59	5745	1502	177	635	137	424	234	257	256	87	780
1857	120	3925	120	669	173	973	290	865	248	100	2069
4923	141	7908	25	806	142			2596	108	217	564
8190	2			1170	147			3076	59	340	1066
8647	19			1729	106			8190	2	423	205
				2764	39					1000	146
				8190	2					1058	31
										1090	77
										1904	74
										2282	53

j=9		j=10		j=11		j=12		j=13		j=14	
start	period	start	period	start	period	start	period	start	period	start	period
14	8923	14	7378	14	16162	14	30982	14	28794	14	4477
28	23535	28	13649	21	2175	111	467	28	1203	21	8356
144	101	51	10687	42	2158	196	1139	89	1385	42	7833
299	190	71	645	70	9974	211	60	145	686	84	10235
7836	18	162	371	156	19	1050	99	151	529	144	970
		3045	35	219	101	2876	18	470	90	495	23
		8190	2	271	569	8190	2	1493	20	506	610
				303	429			2805	30	776	161
				314	118			3626	30	888	80
				381	615					1109	20
				443	120						
				541	19						
				554	60						
				737	11						
				866	120						
				1420	27						
				3205	60						
				6278	19						
				18438	11						

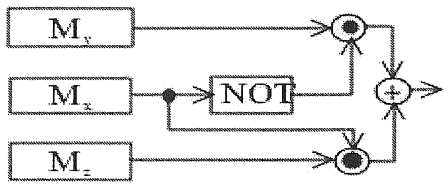

図 4: Geffe 型生成器

Geffe 型の系列は，3 個の M 系列を用いる [4]. すなわち

$$\begin{aligned} x_3 &= x_0 + x_1 \\ y_4 &= y_0 + y_1 \\ z_5 &= z_0 + z_3 \end{aligned}$$

それらを M_x, M_y, M_z とおき，おのおのの LFSR の出力を x_n, y_n, z_n とした場合，

$$v_n = (x_n \wedge \overline{y_n}) \oplus (y_n \wedge z_n)$$

を新しい系列とする．この場合，解析的には 17 次の線形多項式で実現されることが分かっている．実際，BM で直接線形複雑度を求めると

$$\begin{aligned} v^{17} + v^{14} + v^{13} + v^{11} + v^9 + v^7 & \\ + v^6 + v^4 + v^2 + v + 1 &= 0 \end{aligned}$$

を得る．この結果は，理論値に一致する．

この場合は，線形複雑度が大きくなっているので，33 個のデータがないと推測されない．しかし，周期 105 に較べれば十分小さな値で推測可能である．図 4 に，Geffe 型生成器を示す．

次に表 1 で与えられた $n = 15, p = 7, i = 1, j = 2$ の場合の系列について実際に BM により線形複雑度を求めてみる．初期値として 100000000000000 を与えた場合，45 番目の tuple から始まる系列は周期 22612 を持つ．この場合に BM により線形複雑度を求めてみると 22608 となる．これは，ほぼ周期に等しい．この値を得るために用いたデータは 45215 個であり，1 周期を超えているので，その意味では線形複雑度を求めて推測する意味はない．

言い換えると，ここで述べている 2 次の M 系列では，線形複雑度の推測はできない．その意味で，暗号には適していると言えよう．

この例は次数が $n = 15$ と小さい．しかし，$n = 521, p = 353$ などのような大きな次数を持つ系列では BM で線形複雑度推定することは事実上出来ないであろう，と予想する (推定するためには $2 \times (2^{521} - 1)$ 個程度のデータが必要).

4 まとめ

2 次 M 系列の線形複雑度は十分に大きいと言えそうである．問題点としては 2 次の項を加えることにより，系列は部分列に分割されてしまう．部分列の大きさについては，今のところ，何らかの方法で調べる以外ない．n が大きい場合には，調べるだけで時間が掛かってしまうので，実用的に使うための工夫が必要である．

参考文献

[1] A.H.Chan, R.A.Games, J.J.Rushana, "On Quadratic M-Sequences", URL http://www.ccs.neu.edu/home/jjr/q_mseq.ps

[2] 岡本龍明, 山本博資, "現代暗号", p45-63, 産業図書 (1997)

[3] 山住富也, 小池慎一, "混合M系列の性質について, 電気関係学会東海支部, p.552 (2003)

[4] 山住富也, 小池慎一, "単一の M 系列を入力とする Geffe 型コンバイナの性質について", 電気関係学会東海支部, p.661 (2001)

(受理　平成 16 年 3 月 19 日)