２元および多元M系列を基にした新乱数生成法

小清水　誠*　・　森山　純臣**

New Random Number Generator Based on Binary and Multi-Level M-sequences

Makoto KOSHIMIZU　Yoshitomi MORIYAMA

Abstract - H. Pangratz considered the pseudo-random number generator based on binary and quinary maximal-length sequences, and calculated the autocorrelation function. Recently, the generation of pseudo-random binary sequences with good randomness from a Product M-sequences of low degree using a scrambler is presented. In this paper, we propose new random number generator which used 2&5&3&7-level M-sequence generator. 10-level random number are made using each one generator of every. The empirical tests are made using chi-square statistic on two generators, Pangratz 's and our's.
Keywords : pseudo-random number, M-sequences, scrambler

１．はじめに

乱数生成法には合同法がよく知られているが，２元の最大長周期系列（M系列）を用いた生成法をR.C.Tausworthe[1]が発表している。また，H.Pangratz等[2]は２元M系列と５元M系列をもとに10進乱数列を発生させて，理論的に自己相関値を求めている。その後，著者の一人が２元と３元M系列を基に４元と６元の系列を求めて，10進乱数列を求める方法を提案している[3]。本論文では，３元M系列と７元M系列を発生させ,これらを３:７の割合で採用することにより，10進乱数列を求める方法を提案している。さらに，この生成法とPangratzの方法による系列について,乱数として実用できるか，いくつかのランダム性の検証を行っている。

２．生成法

２元・３元・５元および７元M系列Generatorから得られるM系列をそれぞれu(n),v(n),w(n),s(n)とする。

図１に示すように，まずH.Pangratzの生成式（１）もしくは（２）を使用しu(n)とw(n)からx(n)を求める。

$$x(n) = 5u(n) + w(n) \qquad -(1)$$

$$x(n) = u(n) + 2w(n) \qquad -(2)$$

次に，上式よりもとめたx(n)を利用し，v(n)とs(n)から10進乱数列を求める。v(n)とs(n)は，それぞれ３元と７元のM系列である為，10進数列を求める場合v(n):s(n)を３：７で採用しなければならない。そのため，図１中の10-Level Generatorで10進乱数列y(n)を式（３）より求める。

$$y(n) = \begin{cases} v(n) + 7 & if\ \ x(n)\%3 = 1 \\ s(n) & othere \end{cases} \qquad -(3)$$

ここで％は，剰余計算をあらわすこととする。H.Pangratzの生成式より得られる，x(n)は０～９の整数である。よって，x(n)を３で割ったあまりが１の場合とそれ以外の場合を区別させることによりv(n):s(n)を３：７で採用することができる。
また，表１～３に３元・５元および７元M系列Generatorのフィードバック Tap位置(j)，係数Cm,Cjを示す。長周期な多元M系列を求める場合，計算にか

*釧路高専技術室　**釧路高専電子工学科

なりの日数を必要とするめ，さらに長周期なM系列を求める際の参考にしていただきたい。

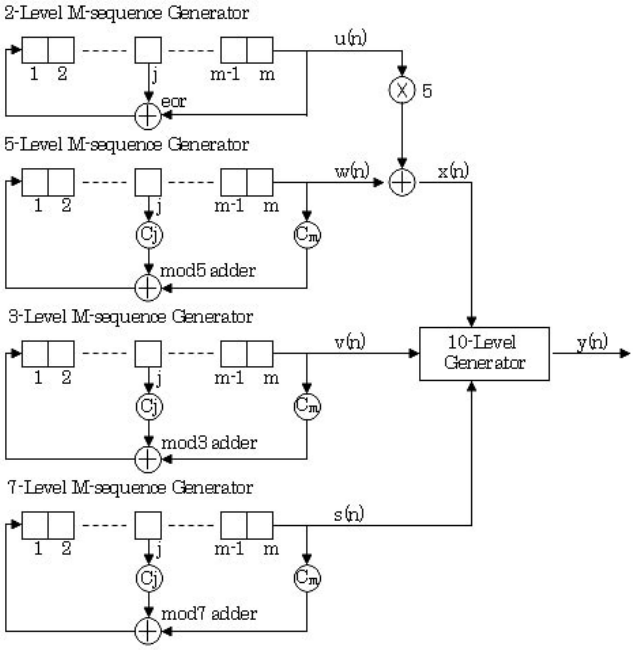

図１．10-level generator which used 2&5&3&7-level M-sequence generator

表１．3-Level M-Sequence generator of trinomials

BitL	j	Cj	Cm
3	1	2	1
3	2	2	1
5	1	2	1
5	4	2	1
7	2	2	1
7	5	2	1
9	4	2	1
9	5	2	1
11	2	2	1
11	3	2	1
11	8	2	1
11	9	2	1
13	1	2	1
13	4	2	1
13	6	2	1
13	7	2	1
13	9	2	1
13	12	2	1
15	2	2	1
15	7	2	1
15	8	2	1
15	13	2	1
17	1	2	1
17	16	2	1
19	2	2	1
19	8	2	1
19	11	2	1
19	17	2	1

表２．5-Level M-Sequence generator of trinomials

BitL	j	Cj	Cm
3	1	1	2
3	1	3	2
3	1	2	3
3	1	4	3
3	2	3	2
3	2	4	2
3	2	3	3
3	2	4	3
5	1	3	2
5	1	2	3
5	2	3	2
5	2	3	3
5	3	1	2
5	3	4	3
5	4	4	2
5	4	4	3
7	1	1	2
7	1	3	2
7	1	2	3
7	1	4	3
7	3	3	2
7	3	2	3
7	4	4	2
7	4	4	3
7	6	3	2
7	6	4	2
7	6	3	3
7	6	4	3
11	1	1	2
11	1	4	3
11	2	3	2
11	2	3	3
11	3	3	2
11	3	2	3
11	5	1	2
11	5	3	2
11	5	2	3
11	5	4	3
11	6	3	2
11	6	4	2
11	6	3	3
11	6	4	3
11	8	4	2
11	8	4	3
11	9	1	2
11	9	4	3
11	10	3	2
11	10	3	3
13	6	4	2
13	6	4	3
13	7	3	2
13	7	2	3

表３．7-Level M-Sequence generator of trinomials

BitL	j	Cj	Cm
3	1	3	4
3	1	5	4
3	1	6	4
3	2	3	2
3	2	5	2
3	2	6	2
5	1	2	2
5	1	5	2
5	1	1	4
5	1	6	4
5	2	6	2
5	2	5	4
5	3	3	2
5	3	3	4
5	4	2	2
5	4	5	2
5	4	1	4
5	4	6	4
7	2	3	2
7	2	5	2
7	2	6	2
7	7	3	4
7	7	5	4
7	7	6	4
9	2	3	2
9	2	5	2
9	2	6	2
9	7	3	4
9	7	5	4
9	7	6	4
11	1	2	2
11	1	3	2
11	1	1	4
11	1	5	4
11	10	2	2
11	10	3	2
11	10	1	4
11	10	5	4
13	6	4	2
13	6	4	3
13	7	3	2
13	7	2	3

３．検定

H. Pangratz の論文では，１桁の数の自己相関値については計算されているが，乱数としての性質は調べられていない。そこで本研究での生成法と比較するために，文献[3] のデータを参考にランダム性を調べることにした。z(n)の10進出力を５桁とり，区間[0,1)の１個の実乱数として10万個ずつ10区間（#1～#10）について２種類の検定を行った。10進乱数列の生成には23Bitの２元M系列Generator（j=18,Cj=1,Cm=1），13Bitの５元M系列Generator(j=6,Cj=4,Cm=3),17Bitの３元M系列Generator（j=1,Cj=2,Cm=1），11Bitの７元M系列Generator（j=1,Cj=2,Cm=2）を用いている。

３．１　頻度検定

区間[0,1)を25の等しい区間に分け，各区間ごと実乱数のカイ２乗を求めた結果を表４に示す。両生成法ともにχ^2_{24}（0.05）=36.4以下の値を示し，“生成される数列が区間[0,1)上に等確率で現れる。”は有意水準5%で受け入れられ,等出現性が保証されることがわかる。なお，図２は生成される２数を１組の座標と考えて，視覚的に２次元表示したものである。これらからも，両生成法の等頻度性がうかがわれる。

表4. Frequency test

section	2&5-Level Generator	2&5&3&7-Level Generator
#1	15.60	17.32
#2	23.19	17.34
#3	18.61	17.48
#4	16.62	17.54
#5	17.14	17.80
#6	27.81	17.90
#7	16.98	17.88
#8	25.93	17.98
#9	18.11	17.87
#10	20.50	17.78

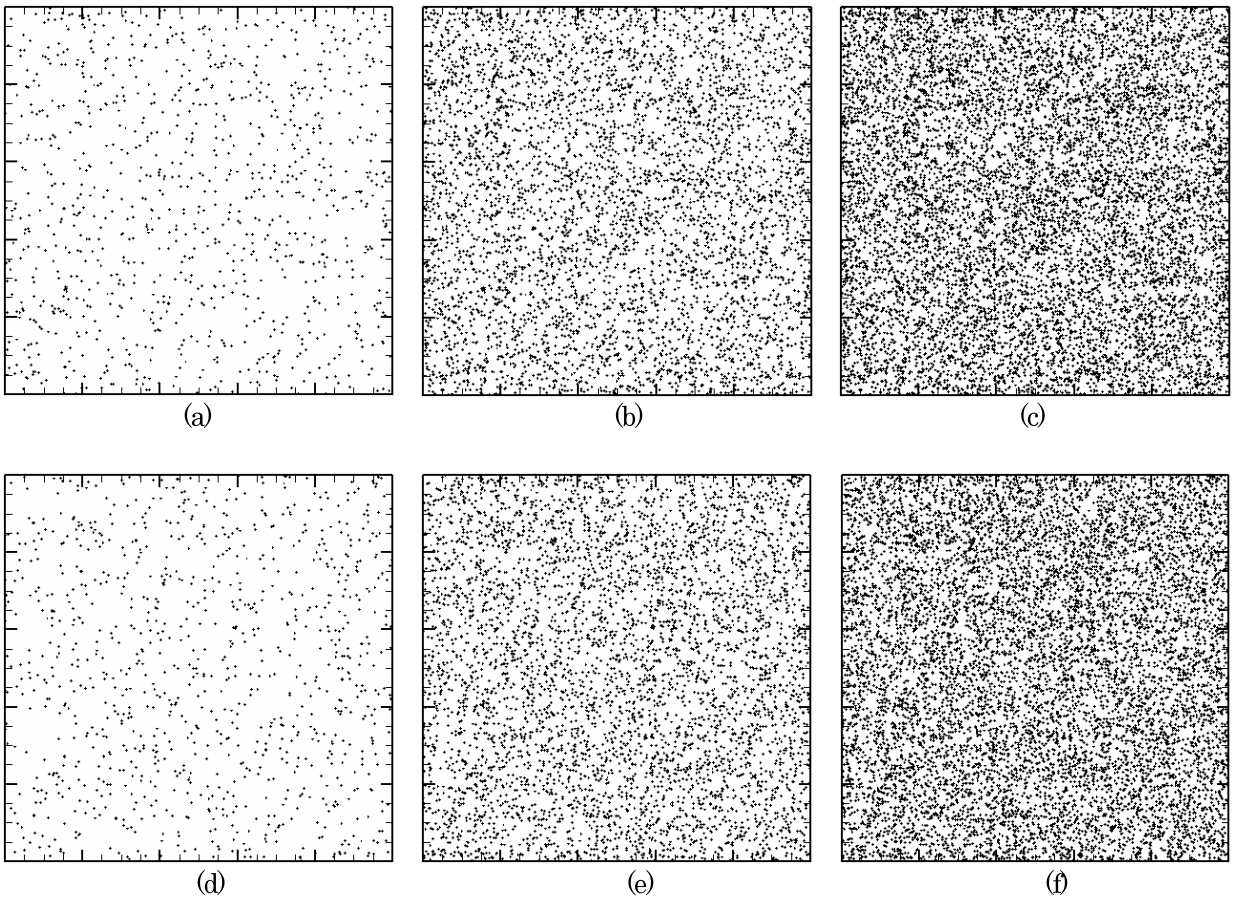

図２．2&5-Level Generator　　: (a) 1000,(b) 5000,(c) 10000 points plotted in 2-space.
2&5&3&7-Level Generator : (d) 1000,(e) 5000,(f) 10000 points plotted in 2-space.

３．２　連検定

#1 から#10 までの各々10 万個の乱数について，長さｒの連の数をかぞえ理論値と比較している。表５は，#1 の上昇，下降及び総合の連の数を表しているが，全体的に理論値と一致しているのがわかる。表６は 10 区間（#1～#10）についてのカイ２乗を示しているが，両生成法とも χ^2_6 (0.05) =12.6 以下であり，等出現性が保証される。

表 5. Run test of #1

Run Length	Observed Up	Observed Down	Predicted Up(Down)	Oberved Total	Predicted Total
1	20647	20900	20833	41547	41666
2	9304	9108	9166	18412	18333
3	2662	2630	2638	5292	5277
4	588	561	575	1149	1150
5	93	92	101	185	203
6	16	19	15	35	30
7	2	1	2	3	4
χ^2	4.95	3.32		3.40	

表 6. Run test

section	2&5-Level Generator	2&5&3&7-Level Generator
#1	8.39	3.40
#2	6.68	3.39
#3	8.87	3.41
#4	5.13	3.39
#5	6.30	3.41
#6	7.20	3.42
#7	6.69	3.62
#8	8.74	3.65
#9	1.84	3.61
#10	8.83	3.63

４．あとがき

両生成法とも，２種類の検定ですべて合格であり，乱数として使用することが可能であると考えられる。しかし，H. Pangratz の乱数発生法で生成した 10 進擬似乱数列では，頻度検定および連検定での χ^2 値にばらつきがあるが，本研究で提案した 10 進擬似乱数列ではほぼ一定の値し示している。その結果より，より理想的な乱数列が得られたと考えられる。

さらに，それぞれの Generator のフィードバックの位置を増やした場合に，期待した結果がえられるかどうか，また理論的な周期や自己相関関数を求めることなどが残されている。

５．参考文献

1) Tausworthe, R.C.:"Random numbers generated by linear recurrence modulo two", Math. COMP. 19, 1965, 201-209.
2) Pangratz, H. and Weinrichter, H. : "Pseudo-Random Number Generator Based on Binary and Quinary Maximal-Length Sequences", IEEE Trans. COM. Vol.c28, 1979.
3) 森山純臣, 中村隆, 山田昌尚:"２進および３進M系列をもとにした新乱数生成法", 釧路工業高等専門学校紀要第 23 号, 51-54, 1989.