

M 系列の部分的性質を考慮した一様乱数の発生

熊本大学工学部 柏木 潤

Hiroshi Kashiwagi

M 系列は一周期にわたる性質をみると、大変バランスがとれていて真に不規則な系列に似ている。しかし乱数発生などに高次の M 系列（例えば 100 次）を用いると、周期は殆んど無限大であり、実際我々が使用するのは周期のほんの一部でしかない。従って、もし不適当な初期値を用いると当分の間、極めて不規則性の悪い系列しか得られないということが起り得る。実際 all 1 や特性 M 系列の初期値 (C.M. と略記) を初期値として用いると不規則性が極めて悪い。そこで M 系列の部分的性質を調べておき、周期のどの部分（位相）を用いるのがよいかを調べておく必要がある。筆者は、部分的性質として、(1) M 系列の部分的自己相関関数、(2) 連の自己相関関数（長さが 3 の連があれば、それを数値の 3 と表わし、その自己相関をとったもの）、(3) 連の長さの分布、(4) Tausworthe 系列の分布をとり、いくつかの位相における部分的性質を調べてみた。その結果、周期を N として、 $(N+1)/2^i$ の点を円分位相点と定義すると、円分位相点における部分的性質は i の順序に類似していることが分った¹⁾。従って、使用すべき位相

としては, all 1 や C.M. を避けるだけでなく, その円分位相乗のいくつかも避けるべきであることが分る。また部分的不規則性を調べるのに, ある位相乗より m タップルを M 個とり出したとき, 1 タップル当りのエントロピー H_m を (1) 式で, また不規則度 R を (2) 式で定義する。

$$H_m = -\frac{1}{m} \sum_{i=1}^m p_i \log_2 p_i \quad \dots (1)$$

ただし, p_i はある m タップルが生ずる確率であり, 実際は相対度数 f_i/M (f_i はある m タップルが M 個中に生ずる回数) で近似する。

$$R = \sum_{i=1}^r i H_i / \sum_{i=1}^r i \quad \dots (2) \quad \left[\begin{array}{l} \text{ただし 実際上 } n \text{ 次 } M \\ \text{系列に } n \text{ まで} \\ n \geq 16 \text{ のとき } r=16 \\ n < 16 \text{ のとき } r=n \end{array} \right]$$

特性多項式 $f(x) = x^{129} + x^5 + 1$ および $f(x) = x^{129} + x^{40} + x^2 + x + 1$ に対して, 周期を 512 等分して各乗における不規則度 R を描いたのが Fig. 1, Fig. 2 である。いづれも C.M. の円分位相乗で R が小さいと, および $f(x)$ が 3 項式のときは周期の全体にわたって R が小さいことが分る。サンプル個数 M は, 大きくすると部分的性質が平均化されてしまう (例えば $M=2^n-1$ ととれば, 一周期全体にわたる性質から常に $H_m = 1$ となる) ので, 部分的性質をみるには M はある程度小さくする必要が

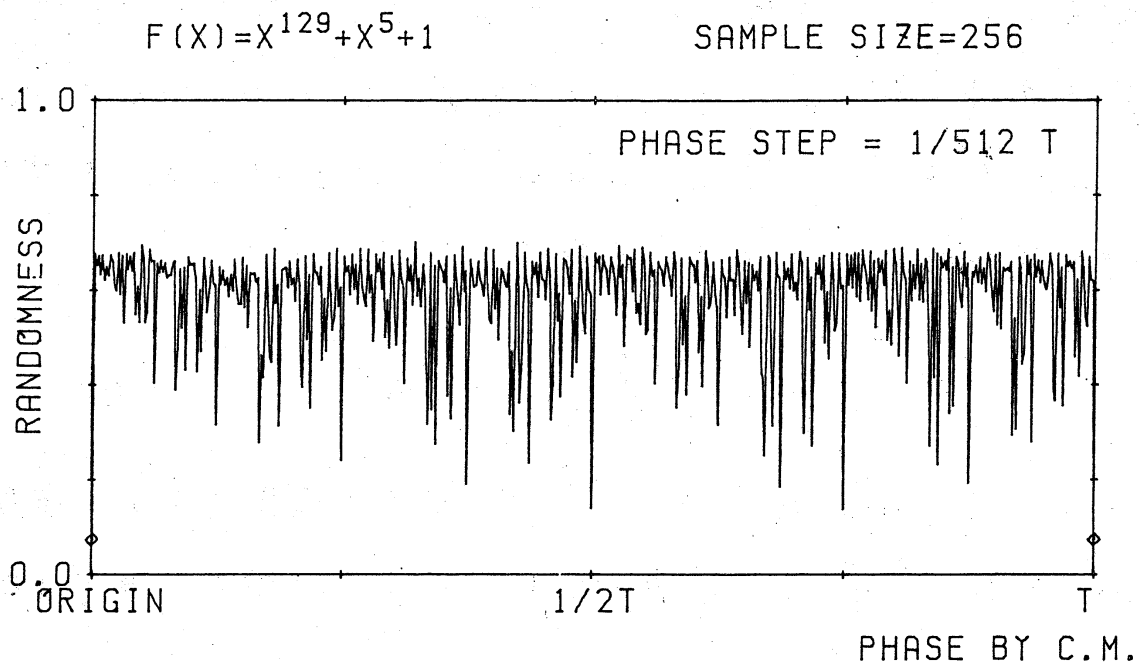


FIG. -1 RANDOMNESS OF M-SEQ.

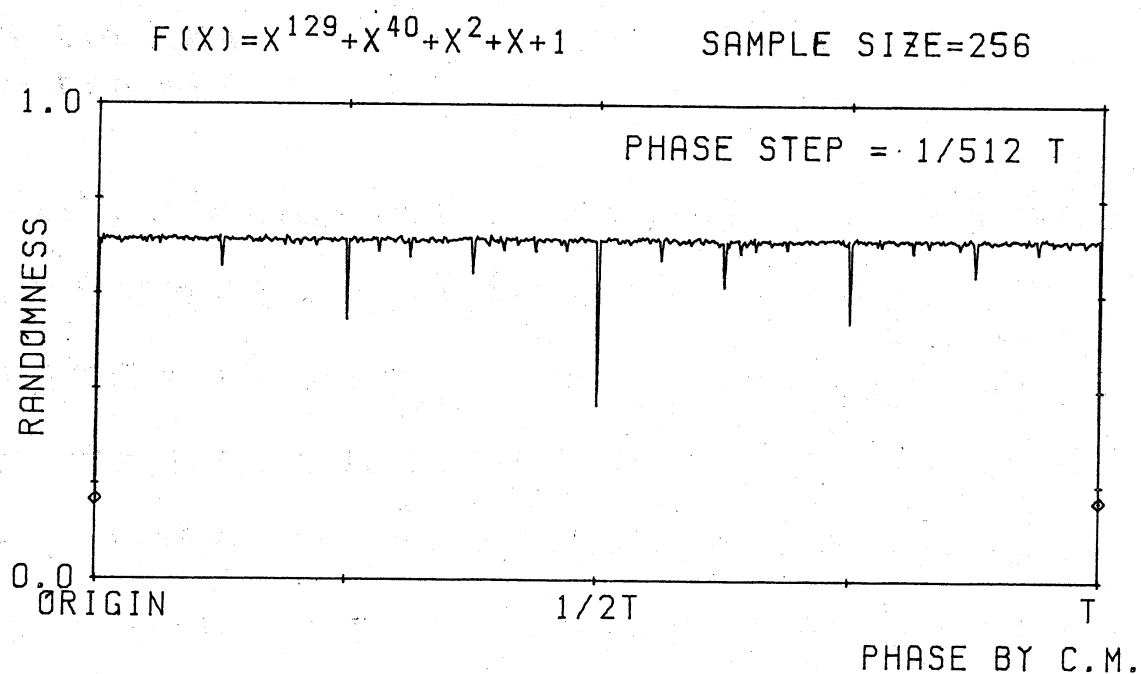


FIG. -2 RANDOMNESS OF M-SEQ.

ある。こゝでは $M=256$ ととっている。 M が 2^m より小さいときは、 H_m の上限は 1 より小さくなり、従って R の上限も 1 より小さくなる。即ち、 $M=2^k$ ($k < m$) ととったとき、

$$H_m \leq -\frac{1}{m} \cdot 2^k \times \frac{1}{2^k} \log_2 \frac{1}{2^k} = \frac{k}{m} \quad \dots (3)$$

従って

$$R \leq \frac{1+2+\dots+k-1+(r-k+1)k}{1+2+\dots+r} \quad \dots (4)$$

となる。 $n \geq 16$ のときは $r=16$ であるから

$$R \leq \frac{1}{272} \cdot (33-k) \cdot k \quad \dots (5)$$

となる。 $M=256=2^8$ のときは、 $R \leq 0.735$ となり、Fig. 1, 2 とよく一致している。

このように部分的性質を調べた結果、乱数発生という目的のためには、次のことが云える。

(1) 特性多項式は 3 項式を避けて 5 項式を用いる。例えば、89 次のときに用いるべき 5 項式としては次のようなものがある。ベキのみを示すと、

$$(89, 72, 55, 38, 0), (89, 86, 41, 38, 0), (89, 32, 12, 1, 0)$$

$$(89, 28, 8, 1, 0)$$

これらはいずれも筆者の研究室で見出されたものである。⁴⁾

(2) all 1, C.M. およびその円分位相臭 (主に $\frac{1}{2}, \frac{1}{4}$ 臭) を避けて, 例之ば C.M. から $\frac{1}{3}, \frac{1}{5}, \frac{1}{7}$ 臭などを用いる. このためには, $x^{\frac{1}{3}} \bmod f(x)$ などの剰余多項式を予め求めておく必要がある. 剰余多項式の求め方については文献(3)の方法を用いると便利である.

さて実際に乱数発生プログラムを作ってみよう. 特性多項式は, 不規則度を調べた結果, 前述の四つの中では, $(89, 32, 12, 1, 0)$ が良かったので, これを用いることにする. C.M. より $\frac{1}{3}, \frac{1}{5}, \frac{1}{7}$ 臭について, それぞれ 100 万個のデータについて, 1 万個ずつ 100 組に分けて, 一様性, 組合せ, 連 (above/below), 連 (up/down) について検定を行った結果を Fig. 3 に示す. 連の性質がやや悪いが, 一様性と組合せについてはほぼ満足できることが分る. そこで, これに $\frac{1}{11}$ 臭を加えて, C.M. より $\frac{1}{3}, \frac{1}{5}, \frac{1}{7}, \frac{1}{11}$ 臭の合計 4 臭および各々の位相臭から $i/8$ 位相臭 ($i=0, 1, \dots, 7$), 計 32 の位相臭について, 初期パラメータ IX によって選択し, 更にその臭より IX 回空回しをすることによって初期化を行なうことにする. 即ち, IX の下位 3 ビットによって $i/8$ 臭のいずれをとるかを決め, その上の 2 ビットによって $\frac{1}{3} \sim \frac{1}{11}$ 臭のいずれにするかを定める. 実際の M 系列の発生は TLP 法を用いるのが便利である. TLP 法では, M 系列を $a_i (=0 \text{ or } 1)$ とす

	有意水準 5% 不合格	有意水準 1% 不合格
一様性	68,74,75,92	75,92
組み合わせ	13,21,22,26,27 29,42,47,55,71 76,88,99	26,27,29
連 ABOVE/BELOW	6,10,14,32,37 42,43,58,99	6,10,14,32,42 43,58,99
連 UP/DOWN	4,14,25,40,64 80,84,96	4,25,40,64,80 84,96

左表の
数字は
組の番号

Fig. 3 (a) 特性M系列の初期値から T/3 位相点より100 万個の検定結果

	有意水準 5% 不合格	有意水準 1% 不合格
一様性	16,17,45,60,64	60,64
組み合わせ	6,67,91	
連 ABOVE/BELOW	13,14,21,26,30 43,46,52,67,69 70,81,90,95,96	14,21,26,30,43 52,67,81,90,95 96
連 UP/DOWN	4,11,20,24,32 67,75	4,11,20,32,67 75

左表の
数字は
組の番号

Fig. 3 (b) 特性M系列の初期値から T/5 位相点より100 万個の検定結果

	有意水準 5% 不合格	有意水準 1% 不合格
一様性	19,22,42,59,66 93,98	59
組み合わせ	2, 3, 7,18,21 38,50,51,56,61 63,90	2, 3,61,90
連 ABOVE/BELOW	8, 9,16,25,32 62,63,76,77,91 100	8, 9,16,62,63 76,77,91
連 UP/DOWN	19,21,30,47,54 66,77,85,88	19,21,30,66,77 85,88

左表の
数字は
組の番号

Fig. 3 (c) 特性M系列の初期値からT/7 位相点より100 万個の検定結果

るとき,

$$\begin{array}{cccccc}
 w_0 & w_1 & w_2 & & w_{n-1} & w_n \\
 a_0 & a_1 & a_2 & \cdots & a_{n-1} & a_n \cdots \\
 a_r & a_{r+1} & a_{r+2} & \cdots & a_{r+n-1} & a_{r+n} \cdots \\
 a_{2r} & a_{2r+1} & a_{2r+2} & \cdots & a_{2r+n-1} & a_{2r+n} \cdots \\
 \vdots & \vdots & \vdots & & \vdots & \vdots \\
 a_{(L-1)r} & a_{(L-1)r+1} & a_{(L-1)r+2} & \cdots & a_{(L-1)r+n-1} & a_{(L-1)r+n} \cdots
 \end{array}$$

と並べ,

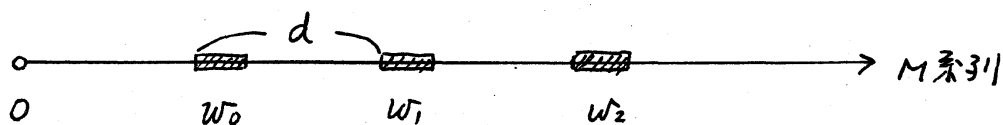
$$w_i = 0. a_i a_{i+r} a_{i+2r} \cdots a_{i+(L-1)r} \quad (\text{base } 2)$$

によって一様乱数 w_i を発生すると, w_i は特性多項式によ

る漸化式を満足するので、 L を計算機の語長 (16 or 32) にしておくと、語ごとの排他的論理和によって次々に w_i が発生されるから便利である。⁵⁾ 問題は $w_0 \sim w_{n-1}$ の初期値の設定であるが、Lewis & Payne の提案による all 1 を基準とする初期化は、部分的性質が極めて悪いことは明らかである。また L の行間遅れを大きくとることも一般に容易でない (もっとも文献による方法を用いれば計算は簡単である)。そこで、希望の位相矢より出発して高速に w_i を発生するには、 w_i の性質を利用して次のようにすればよい。

$f(x)$ を a_i の特性多項式として、 α をその原始根とすると、 $a_0, a_r, a_{2r}, \dots$ の特性多項式 $g(x)$ は、 α^r に対する最小多項式であり、 $g(x)$ により発生される M 系列上で w_0, w_1 の位相差 d は、次の式を満たす。⁵⁾

$$r \cdot d = 1 \pmod{N}$$



そこで、16 ビットの計算機であれば $r = 2^{n-4}$ ととれば、 $d = 2^4$ となり、 $w_0, w_1, \dots$ は w_0 より出発した M 系列を 16 ビット毎に続けて取り出したものになる。しかも、 r は 1 を含む四分割余類に属しているから、 $g(x)$ は $f(x)$ と同じもの

であり, $f(x)$ に 5 項式を用いれば $g(x)$ も 5 項式であり, r が一般の場合のように, どのような $g(x)$ になるか一抹の不安を抱く必要が全くない。

プログラムを ^{Fig. 4} に示す。SUBROUTINE INITP(IX) は, $w_0 \sim w_{n-1}$ までの初期化を行なうものである。IRP(I, J) は, $x^{(I-1)/8} \bmod f(x)$ という剰余多項式をビットパターンにしたものである。IVS(I, J) は, $I=1, 2, 3, 4$ について $1/3, 1/5, 1/7, 1/11$ (いおれも C.M. より) 真の初期 nタッフルをビットパターンに直したものである。ただし計算機は 16 ビットマシンを想定している。SUBROUTINE UNIFP(X) は, INITP(IX) で初期化を行なった後に呼ぶことによって, 一様乱数 ($0 \sim 1$) X が発生される。

初期パラメータ IX をランダムに 128 通り選んで, このプログラムで発生した一様乱数について, 一様性, 組合せ, 連の検定を行なった結果を Fig. 5 に示す。組合せ, 連の検定結果が必ずしも良くないが一様性については満足すべき結果が得られている。これら以外の検定項目 (gap テストなど) についても実施したいと考えている。

なお, 研究集会で 3 項式もあてたものではないのではないかという議論があったが, やはり 3 項式はあまり良くないという例を次に示したい。一様乱数は一様乱数としての性質を

```

SUBROUTINE INITP(IX)
COMMON /RAND/IW(89),ICNT
DIMENSION IRP(8,6),IVS(4,6),IV(6),LPW(16),NBP(16)
DATA IRP/256,402,477,158,258,195,381,429,
*0,20929,-26015,-21257,1886,11950,-11830,29212,
*0,10102,32193,-17959,16032,2453,-26394,11586,
*0,-305,25927,22799,-24544,-26479,8815,29014,
*0,-13912,1429,-26064,8354,12430,-25569,-29078,
*0,24585,7190,-1536,-22006,-28296,-7279,-26625/
DATA IVS/91,100,219,49,22396,-11311,7078,23508,
*9731,-30556,-21074,-14154,6918,-4805,28990,-32514,
*-2089,17461,27249,10938,-3337,20604,-14682,-13093/
DATA LPW/-32768,16384,8192,4096,2048,1024,
*512,256,128,64,32,16,8,4,2,1/
DATA NBP/0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0/
IP=MOD(IX,8)+1
IQ=MOD(ISL(IX,-3),4)+1
DO 100 L=1,6
100 IV(L)=IVS(IQ,L)
DO 110 K=1,89
IW(K)=0
DO 120 M=1,16
LPR=0
DO 130 L=1,6
130 LPR=IEOR(LPR,IAND(IV(L),IRP(IP,L)))
LPR=IEOR(LPR,ISL(LPR,-8))
LPR=IEOR(LPR,ISL(LPR,-4))
IW(K)=IW(K)+NBP(IAND(LPR,15)+1)*LPW(M)
KPR=IEOR(IAND(IV(1),384),IAND(IV(2),4096))
KPR=IEOR(KPR,IAND(IV(3),256))
KPR=IEOR(KPR,ISL(KPR,-8))
KPR=IEOR(KPR,ISL(KPR,-4))
DO 140 L=1,5
IV(L)=ISL(IV(L),1)
IF(IV(L+1).LT.0) IV(L)=IV(L)+1
140 CONTINUE
IV(6)=ISL(IV(6),1)+NBP(IAND(KPR,15)+1)
120 CONTINUE
110 CONTINUE
ICNT=0
DO 150 I=1,IX
ICNT=MOD(ICNT,89)+1
K1=MOD(ICNT,89)+1
K2=MOD(ICNT+11,89)+1
K3=MOD(ICNT+31,89)+1
150 IW(ICNT)=IEOR(IEOR(IW(ICNT),IW(K1)),IEOR(IW(K2),IW(K3)))
ICNT=0
RETURN
END

```

Fig. 4 (a)

```

SUBROUTINE UNIFF(X)
COMMON /RAND/IW(89),ICNT
ICNT=MOD(ICNT,89)+1
K1=MOD(ICNT,89)+1
K2=MOD(ICNT+11,89)+1
K3=MOD(ICNT+31,89)+1
IW(ICNT)=IEOR(IEOR(IW(ICNT),IW(K1)),IEOR(IW(K2),IW(K3)))
X=FLOAT(IW(ICNT))/65536.0+0.5
RETURN
END

```

Fig. 4 (b)

	有意水準 5% 不合格	有意水準 1% 不合格
一様性	5 / 128	
組み合わせ	15 / 128	5 / 128
連 above/below	22 / 128	16 / 128
連 up/down	11 / 128	10 / 128

Fig. 5. 検定結果. ($5/128$ は 128 例中 5 例が不合格であることを示す).

持たなければならぬのは言うまでもないが、何個か加算したときに正規乱数にならなければならず、実際にそういう期待をもって一様乱数発生サブルーチンを使うユーザが多いことに注意しなければならない。この観点からすると、3項式を用いるのは都合が悪い。なぜなら、文献(2)にあるように、加算する範囲内にある3項の線形従属のペアが多いほど、

skewness が悪くなり，特性多項式として 3 項式を用いるとまさに 3 項の線形従属のペアの連続によって M 系列が発生されるから skewness が極めて悪くなるからである。例として，伏見ら¹⁾の提案による $f(x) = x^{521} + x^{32} + 1$ を TLP 法で発生した一様乱数を加算した乱数の正規性について検定した結果のうち，skewness についての結果を Fig. 6 に示す。加算個数が大きくなると不合格になる例が多いことが分る。ちなみに同じ検定を $f(x) = x^{521} + x^{358} + x^{195} + x^{32} + 1$ について行なった結果を Fig. 7 に示す。Fig. 6 に比べて不合格になる例が少ないことが分る。

[参考文献]

- (1) 柏木, 原田: M 系列の四分位相, 計測自動制御学会論文集, (SICE) 18 巻, 10 号, pp. 1004-1009, 1982.
- (2) 柏木, 坂田: M 系列を用いる擬似正規信号の発生, SICE 論文集, 12 巻, 3 号, pp. 293-299, 1976.
- (3) 柏木, 森内: GF(2) 上の多項式を法とする演算の高速化, SICE 論文集, 18 巻, 3 号, pp. 300-303, 1982.
- (4) 柏木, 内村: GF(2) 上の原始五項式を求める簡単な方法, SICE 論文集, 18 巻, 7 号, pp. 747-750, 1982.
- (5) 柏木: M 系列による TLP 乱数の二, 三の性質, SICE 論文集, 18 巻, 8 号, pp. 828-832, 1982.

(6) 泉, 柏木: 2値乱数源用高次M系列の初期値, SICE論文集,

第18巻, 第9号, pp. 929-935, 1982.

(7) 伏見, 手塚: 多次元分布が一様な擬似乱数列の生成法,

応用統計学, Vol. 10, NO. 3, pp. 151-163, 1982.

加算個数	有意水準5%不合格	有意水準1%不合格
6 4		
1 2 8	1/5	
2 5 6		
3 8 4	3/5	1/5
5 1 2	1/5	
7 6 8		
1 0 2 4	2/5	
1 5 3 6	2/5	1/5
2 0 4 8	2/5	1/5
3 0 7 2	1/5	
4 0 9 6	3/5	3/5

Fig. 6 $f(x) = x^{521} + x^{32} + 1$ のときのひずみ検定.

加算個数	有意水準5%不合格	有意水準1%不合格
6 4		
1 2 8		
2 5 6		
3 8 4		
5 1 2	1/5	1/5
7 6 8	2/5	
1 0 2 4	2/5	
1 5 3 6		
2 0 4 8		
3 0 7 2		
4 0 9 6		

Fig. 7 $f(x) = x^{521} + x^{358} + x^{195} + x^{32} + 1$
のときのひずみ検定

ただし 3/5 などは 5例中 3例が不合格であることを示す。