M 系列による TLP 乱数の二、三の性質

柏 木 潤*

On Some Properties of TLP Random Numbers Generated by M-Sequence

Hiroshi KASHIWAGI*

Some properties of random numbers generated by Tausworthe-Lewis-Payne (TLP) method are described.

It is shown that the generated random number w_i has the same period as that of n -th order M-sequence, unless the starting matrix W_0 which consists of $w_0, w_1, \dots, w_{n-1}$, is zero matrix. In order for w_i to be uniform in the sense that W_0 appears only once in a period, it is necessary that W_0 has independent columns, which is guaranteed if the delay between rows r is such that $(r, N)=1$, where $N=2^n-1$, the period of the M-sequence.

The autocorrelation function $\phi_{ww}(k)$ of w_i is shown to be obtained from sampling, every d digits, the autocorrelation function $\phi_{xx}(k)$ of the binary L -tuples from the original M-sequence. Namely,

$$\phi_{ww}(k) = \phi_{xx}(kd)$$

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

Keyword: M-sequence, pseudo-random sequence, random number, generation of random number, uniform random number

1. ま え が き

一様乱数や正規乱数は、制御系のシミュレーションなどには欠くことのできないものであり、ほとんどの計算機のライブラリーには、乱数発生サブルーチンが組み込まれている。現在、乱数の発生法は、いわゆる混合同法を用いたものが主流であるが、Marsaglia²⁾によって多次元分布に結晶構造的規則性があることが指摘されて以来、合同法以外の方法による乱数発生法として、M系列を用いる方法が注目されつつある。

M系列を用いる乱数発生は、Tausworthe¹⁾が n 次M系列の相続く L ビット ($L \leq n$) を2進数と考える

と、これが一様乱数となることを示して以来、幾つかの研究^{3), 4)}がなされているが、Lewis と Payne⁵⁾は、Tauswortheの方法を計算機内での発生が高速になるように改良した。この方法は、著者等の頭文字をとってTLP法とも呼ばれている。

本論文は、このTLP法で発生された乱数の周期性、一様性、相関特性などの幾つかの性質を明らかにしようとするものである。

2. TLP 法による乱数発生

TLP法によって乱数を発生する方法を簡単に説明するとつぎのようになる⁵⁾。演算は特に断わらない限りGF(2)のうで行われるものとする。今、GF(2)上の n 次原始三項式の一つを選んで、 $f(x)$ とする。

$$f(x) = x^n + x^q + 1 \quad (1)$$

発生するM系列を a_i ($=0$ または 1) とすると、(1)に対応する漸化式は、

$$a_i = a_{i-n} + a_{i-n+q} \quad (2)$$

となる。 $\{a_i\}$ の周期 $N=2^n-1$ と互いに素な整数 r を選んで、一様乱数列 $\{w_i\}$ をつぎのようにして作る。

$$w_i = 0 \cdot a_i a_{i+r} a_{i+2r} \cdots a_{i+(L-1)r} \quad (\text{base } 2) \quad (3)$$

ここに L は $L \leq n$ となるある整数で通常は使用する計算機の語長にとることが多い。 w_i の各ビットが(2)式を満たすから、 w_i のビットごとの演算を行うとつぎの式が成り立つ。

$$w_i = w_{i-n} + w_{i-n+q} \quad (4)$$

したがって、 w_{i-n} と w_{i-n+q} のビットごとの排他的論理和を取ることによって w_i が直ちに得られる。(4)式が使えるように出発時の初期値を決めておけば、計算機内の語と語との排他的論理和によって逐次一様乱数が発生できる。(2)式によって a_i を L 回発生させて、 $r=1$ に対する w_i を発生するのがTauswortheの方法であるから、それに比べて(4)式の方法は、かなり高速になっている訳である。

さて、このようにして発生される一様乱数列 $\{w_i\}$

* 熊本大学工学部 熊本市黒髪 2-39-1

* Faculty of Engineering, Kumamoto University, Kumamoto

(Received February 1, 1982)

(Revised April 8, 1982)

の一般的性質を調べるため, 特性多項式がつぎのように表わされる場合につき, 以下に考察する.

$$f(x) = \sum_{j=0}^n f_j x^j \quad (f_0 = f_n = 1) \quad (5)$$

ただし, $f_i = 0$ または 1 であり, (5)式に対する漸化式は

$$\sum_{j=0}^n f_j a_{i+j} = 0 \quad (6)$$

と表わされる.

w_i の各ビットの並びを一つのベクトルと考えて, つぎのように並べてみる.

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

W_0

すなわち, 第 1 行は a_0 から始まる M 系列であり, 各行はそれより r ずつ遅れた M 系列である. この r は, Lewis と Payne⁹⁾ は列間遅れと呼んでいるが, ここでは上記のような並べ方をした関係上, 行間遅れと呼ぶことにする.

今, $w_0, w_1, \dots, w_{n-1}$ までのベクトルからなる $L \times n$ 行列を, $W_0, w_1, w_2, \dots, w_n$ までを W_1 などと表わすと,

$$C \triangleq \left[\begin{array}{cccc|c} 0 & 0 & \cdots & 0 & f_0 \\ 1 & & & & f_1 \\ & 1 & & 0 & f_2 \\ & & \ddots & & \vdots \\ 0 & & & 1 & f_{n-1} \end{array} \right] \quad (7)$$

として,

$$\begin{cases} W_1 = W_0 C \\ W_2 = W_1 C = W_0 C^2 \\ \vdots \\ W_i = W_0 C^i \\ \vdots \\ W_N = W_0 C^N = W_0 \end{cases} \quad (8)$$

という関係にある. また

$$C_0 = (f_0, f_1, f_2, \dots, f_{n-1})' \quad ({}' \text{ は転置を表わす}) \quad (9)$$

として,

$$\begin{cases} w_n = W_0 C_0 \\ w_{n+1} = W_1 C_0 = W_0 C C_0 \\ \vdots \\ w_{n+i} = W_0 C^i C_0 \\ \vdots \\ w_{n+N} = W_0 C^N C_0 = w_n \end{cases} \quad (10)$$

と表わされる.

3. 行列 C の性質

今, 乱数 w_{n+i} のあるビットのみ, たとえば第 1 ビットを a_i とすると,

$$a_i = (1, 0, 0, \dots, 0) w_{n+i} = (1, 0, 0, \dots, 0) W_0 C^i C_0$$

である. a_i は M 系列そのものであるから, 漸化式 (6) より,

$$(1, 0, 0, \dots, 0) W_0 \left(\sum_{j=0}^n f_j C^{i+j} \right) C_0 = 0 \quad (11)$$

となる. したがって, $W_0 = 0$ でない限り

$$\sum_{j=0}^n f_j C^{i+j} = 0 \quad (12)$$

となる. すなわち, 行列 C^i は M 系列が満たす漸化式と同じ漸化式を満たすことがわかる. したがって, C^i の周期も M 系列の周期と同じであり

$$C^N = I \quad (13)$$

である. ただし, I は $n \times n$ の単位行列である.

(12) 式から, M 系列の shift and add property に相当するつぎの式が導かれる. すなわち, 任意の i, j に対して

$$C^i + C^j = C^k \quad (14)$$

を満たす整数 k が mod N で一意的に存在する.

4. 初期行列 W_0 と乱数 w_i の周期

$L \times n$ の初期行列 W_0 について, つぎの性質がある. (性質 1)

$W_0 = 0$ でない限り, $W_0 C^i = 0$ にならない.

なぜなら, $W_0 \neq 0$ となるある W_0 に対して $W_0 C^i = 0$ となるなら,

$$0 = W_0 C^{i+1} = W_0 C^{i+2} = \dots = W_0 C^N = W_0$$

となって矛盾が生ずるからである.

(性質 2)

$W_0 = 0$ のとき, そしてそのときのみ, $i \neq j$ に対して $W_0 C^i = W_0 C^j$ となる.

$W_0 = 0$ なら $W_0 C^i = W_0 C^j$ は明らかであり, 逆に $i \neq j$ に対して $W_0 C^i = W_0 C^j$ となるなら, (14) 式より

$$0 = W_0 (C^i - C^j) = W_0 C^k$$

したがって, 性質 1 より $W_0 = 0$ となる.

したがって, 性質 2 から, $W_0 = 0$ でない限り, 任意の $i \neq j$ ($< N$) に対して $W_i \neq W_j$ となり, 乱数列 $\{w_i\}$ の周期は M 系列の周期 N に一致することがわかる. 文献 5), 6) には, $\{w_i\}$ の周期が M 系列の周期と一致するための必要条件として W_0 の各行が線形独立であることを挙げているが, これは単に十分条件であって必要条件ではないことがわかる.

5. 乱数 w_i の一様性

つぎに乱数 w_i が一周期にただ一度しか現れない、すなわち、 $w_1, w_2, \dots, w_N$ がすべて異なるための初期行列 W_0 の条件を出してみよう。

任意の $i \neq j$ ($< N$) に対して

$$w_i \neq w_j$$

であるためには、(10)式より

$$W_0 C^i C_0 \neq W_0 C^j C_0$$

であり、(14)式より

$$W_0 C^k C_0 \neq 0 \quad (15)$$

でなければならない。ところで、 $C^k C_0$ は、 $k=1, 2, \dots, N$ に対してゼロ以外のすべての値をとることがつぎのようにしていえる。すなわち、任意の $i \neq j$ に対して $C^i C_0 \neq C^j C_0$ であるから、 $C^k C_0$ は一周期内ではただ一度しか現れず、その総数は $2^n - 1$ である。一方 $C^k C_0$ は、0, 1 を要素とする n 元ベクトルであるから、ゼロを除くベクトルの数は $2^n - 1$ しかない。したがって、 $C^k C_0$ はゼロ以外のすべての値をとる。このような $C^k C_0$ に対して (15) 式が成り立つためには、 W_0 の各列は線形独立でなければならない。つまり、 W_0 の各列が線形独立であることは、 w_i が一周期内ですべて異なるという意味の一様性のためには必要条件であることがわかる。この条件は、Bright⁷⁾ 等も別の方法を用いて導いている。

W_0 の各列は L 元ベクトル ($L \leq n$) であるから、 n 個の L 元ベクトルが線形独立であるためには、 $L=n$ でなければならない。そして、そのとき、 W_0 の行間遅れ r が $2^n - 1$ と互いに素な定数である限り、各列は必ず線形独立となる。その理由は、一般的には、 W_0 の各行は n 次 M 系列の n -タプルであるから、そのビット間にはすべての n -タプルに対して成り立つような線形従属性がないからであるといえる。ただし、幾つかの n タプルに対して成り立つ線形従属性を見出すことは容易であるから (たとえば、(101...), (011...) の形の n タプルには、(1 ビット) + (2 ビット) = (3 ビット) という従属性がある)、そのような n タプルがたまたま W_0 の各行となるようなことはないことを示しておかなければならない。

今、 n 個の n タプル $(a_i, a_{i+1}, \dots, a_{i+n-1})$ ($i=0, r, \dots, (n-1)r$) につぎのような従属関係があるとする。

$$\begin{cases} h_0 a_0 + h_1 a_1 + \dots + h_{n-1} a_{n-1} = 0 \\ h_0 a_r + h_1 a_{r+1} + \dots + h_{n-1} a_{r+n-1} = 0 \quad (h_i = 0 \text{ or } 1) \\ \vdots \\ h_0 a_{(n-1)r} + h_1 a_{(n-1)r+1} + \dots + h_{n-1} a_{(n-1)r+n-1} = 0 \end{cases} \quad (16)$$

もし、 r が $2^n - 1$ と互いに素な整数なら、 $(a_i, a_{i+r},$

$\dots, a_{i+(n-1)r})$ は、やはり n 次の M 系列の n タプルであるから、 $1 \leq j < 2^n - 1$ なるすべての j に対して

$$k_0 a_i + k_1 a_{i+r} + \dots + k_{n-1} a_{i+(n-1)r} = a_j$$

となるように $k_i (=0 \text{ または } 1)$ を決めることができる。

したがって、(16) 式の各式に k_i をかけて加算すると、

$$h_0 a_j + h_1 a_{j+1} + \dots + h_{n-1} a_{j+n-1} = 0 \quad (j=1, 2, \dots, 2^n - 1) \quad (17)$$

となり、すべての j に対して $n-1$ 次の線形漸化式が成り立つことになり、 a_j が n 次の M 系列であることに反することになる。したがって、(16) 式のような n 次未満の同じ線形従属性をもつ n タプルが n 個以上存在することはないことがわかる。さらに一般的表現をすると、 $m > n$ なる任意の m に対して、周期と素な一定個数離れた n 個以上の m タプルについて成り立つ線形従属な関係があれば、その関係は任意の m タプルについて成り立つ関係であり、したがって M 系列の線形漸化式そのものである。

$L < n$ のときは、 W_0 の各列を独立にとることはできず、 $n-L$ 個の従属な列が現れる。そのときは、乱数 w_i は同じ値を 2^{n-L} 回 (ただしゼロは $2^{n-L}-1$ 回) づつとる一様乱数になることは容易に示すことができる。

6. 乱数 w_i の自己相関関数

一般に GF(2) 上の n 次原始多項式 $f(x)$ により発生された M 系列を r 個ごとにサンプルした系列は、 x^r に対する最小多項式 $g(x)$ を特性多項式とする系列であり、 r が $2^n - 1$ と互いに素であるときは $g(x)$ も n 次の原始多項式になることが知られている¹¹⁾。したがって、TLP 法により発生した乱数 w_i は、 $g(x)$ を特性多項式とする M 系列の相続く L ビットを 2 進小数とみると等価である。では、 w_i と w_{i+1} とは $g(x)$ による M 系列上で位相がどのくらい離れているだろうか。これは実は任意の i に対して w_i と w_{i+1} の位相差は一定であることがつぎのようにしていえる。

w_i の第 1 ビットを、 a_i, w_{i+1} のそれを a_{i+1} とすれば、 a_i, a_{i+1} は $f(x)$ による M 系列上でとなり同志である。そこで、 a_i を r 個ごとにサンプルしてゆき、それが d 回繰り返されたときに a_{i+1} に一致する d の最小値を探せば、その d が w_i と w_{i+1} との間の $g(x)$ による M 系列上の位相差となる。すなわち、

$$a_{i+rd} = a_{i+1} \quad (\text{添字は mod } N)$$

したがって、

$$r \cdot d = 1 \pmod{N} \quad (18)$$

となる。

(3) 式において、 $r=1$ に対する乱数列を $\{x_i\}$ と

すると, その自己相関関数 $\phi_{xx}(k)$ はつぎのようにして求まる. まず, x_i の平均値をゼロにしておいたほうが都合がよいから, つぎの式によって $a_i (=0$ または $1)$ を m_i (1 または -1) に変換する.

$$m_i = 1 - 2a_i \quad (19)$$

m_i から (3) 式の方法で作られる乱数を次式のように x_i と置く.

$$x_i = \sum_{j=1}^L 2^{-j} m_{i+j} + \frac{1-2^{-L}}{N} \quad (20)$$

(20) 式の一周期にわたる平均はゼロである. x_i の正規化していない自己相関関数 $R_{xx}(k)$ は, 文献 12) において荷重を 2^{-j} ($j=1, 2, \dots, L$) と置けばよいからつぎのようになる.

$$R_{xx}(k) = \begin{cases} \frac{2^k \cdot 2^{-k} (1 - 2^{-2(L-k)}) - \frac{N+1}{N} (1 - 2^{-L})^2}{3}, & k < L \\ -\frac{N+1}{N} (1 - 2^{-L})^2, & k \geq L \end{cases} \quad (21)$$

したがって, 正規化した自己相関関数 $\phi_{xx}(k)$ は, つぎのようになる.

$$\phi_{xx}(k) = \begin{cases} \frac{2^{-k} (1 - 2^{-2(L-k)}) - \varepsilon}{1 - 2^{-2L} - \varepsilon}, & k < L \\ \frac{-\varepsilon}{1 - 2^{-2L} - \varepsilon}, & k \geq L \end{cases} \quad (22)-1$$

$$(22)-2$$

ただし, $\varepsilon = 3 \cdot 2^{-n} \frac{(1-2^{-L})^2}{1-2^{-n}}$ である.

したがって, 一般の r に対する乱数列 $\{w_i\}$ の自己相関関数を $\phi_{ww}(k)$ とすると, (18) 式と (22) 式より,

$$\phi_{ww}(k) = \phi_{xx}(kd) \quad (23)$$

となる. もし $k=1, 2, \dots, s$ に対する $\{w_i\}$ の自己相関関数の値を無視できるほど小さく選びたいのであれば, $d, 2d, \dots, sd$ なる遅れに対する $\phi_{xx}(\cdot)$ が (22)-2 式となるように d (したがって r) を選ばなければならない. すなわち,

$$d \geq L, \quad sd \leq 2^n - 1 - L \quad (24)$$

となる. 通常は, w_i の自己相関の値が小さい遅れ k の範囲は広いほうがよいから, s を大きく d を小さくすることになる. 一例として, $d \geq L$ の範囲で $d=2^l$ (l は整数) の形の最小の l を選べば, 行間遅れ r は, (18) 式より,

$$r = 2^{n-l} \quad (25)$$

となる (この形の r は, 任意の n に対して r と $2^n - 1$ とが互いに素になる). このときは, 遅れ k がほぼ 2^{n-l} まで自己相関関数の値が ε の order となる.

ただし, (25) 式の形の r は, 1 を含む円分剰余類に属するから, サンプルされた M 系列の特性多項式 $g(x)$ は, もとの M 系列の特性多項式 $f(x)$ と同じであり,

$f(x)$ が 3 項式であれば $g(x)$ も 3 項式となるから, 3 項式に特有な規則性¹³⁾が w_i に現れる可能性がある. したがって, 相関特性以外の乱数の性質にとってよい r や $f(x)$ の選び方に関しては別途調べる必要がある.

なお, r が非常に大きい場合, 現実に行間遅れをそのようにとることは不可能に思えるかも知れない. たとえば, $n=98$ の場合, $d=2^7$ とれば, $r=2^{91}$ となる. 実際に 2^{91} 回シフトレジスタを回して行間遅れを作ることは不可能である. しかし, このような場合は, 筆者等¹⁴⁾の開発した GF(2) 上の高速演算法, または, 被除多項式が 1 項であるから Van Luyk¹⁵⁾の方法を用いて, x^r を $f(x)$ で割った剰余をあらかじめ求めておけばよい. この剰余によって, 第 i 行の M 系列から r 個遅れた第 $i+1$ 行の M 系列を容易に求めることができる. 各行間の遅れ r が一定なら, この剰余はあらかじめ 1 回求めておけば十分である.

7. あとがき

M 系列を用いて発生される一様乱数のうち, TLP 法と呼ばれる方法による乱数について, その周期性, 一様性, 相関特性などの性質を明らかにした.

はじめに, 行列 C が M 系列と同じ漸化式を満たすことを示し, 出発行列 W_0 が恒等的にゼロでない限り, 任意の W_0 に対して, 乱数 w_i の周期は, M 系列の周期と一致することを示した. つぎに, 乱数 w_i が一周期内ですべて異なるという一様性のためには, 出発行列 W_0 の各列は線形独立でなければならず, 行間遅れ r が M 系列の周期と互いに素な定数である限り, $n \times n$ 行列 W_0 の各列は線形独立であることを示した.

また, 乱数 w_i の自己相関関数は, もとの M 系列の L タップルを 2 進数とみる乱数の自己相関関数を d 個 ($r \cdot d \equiv 1, \pmod{N}$) ごとにサンプルしたものであることを示し, 具体的に式で示した. これらの考察から, 自己相関の値がほとんどゼロとなる遅れの範囲を大きくとるための行間遅れ r の選び方について示唆を与えた.

参考文献

- 1) R. C. Tausworthe: Random Numbers Generated by Linear Recurrence Modulo two, Math. Comp., **19**, 201/209 (1965)
- 2) G. Marsaglia: Random Numbers Fall Mainly in the Planes, Proc. Nat. Acad. Sci., **61**, 25/28 (1968)
- 3) J. P. R. Toftill, W. D. Robinson and A. G. Adams: The Runs Up and Down Performance of Tausworthe Pseudo-Random Number Generators, J. Assoc. Comp. Mach., **18**, 381/399 (1971)

- 4) J. P. R. Tootill, W. D. Robinson and D. J. Eagle: An Asymptotically Random Tausworthe Sequence, J. Assoc. Comp. Mach., **20**, 469/481 (1973)
- 5) T. G. Lewis and W. H. Payne: Generalized Feedback Shift Register Pseudo-random Number Algorithms, J. Assoc. Comp. Mach., **20**, 456/468 (1973)
- 6) 津田: モンテカルロ法とシミュレーション, 培風館 (1977)
- 7) H. S. Bright and R. L. Enison: Quasi-Random Number Sequences from a Long-period TLP Generator with Remarks on Application to Cryptography, ACM Computing Surveys, **11**-4, 357/370 (1979)
- 8) 津田: レーマー型合同法によらない乱数について, bit, **12**-9, 1180/1191 (1980)
- 9) 伏見: 擬似乱数の発生法について, 情報処理, **21**-9, 968 /974 (1980)
- 10) 柏木: M系列再発見, 計測と制御, **20**-2, 236/245 (1981)
- 11) S. W. Golomb: Shift Register Sequences, Holden-Day (1967)
- 12) H. Kashiwagi: A Method of System Identification Using Weighted m-sequence Signal, Proc. 1974 JACC held in Austin, Texas, 285/292 (1974)
- 13) J. H. Lindholm: An Analysis of the Pseudo-Randomness Properties of Subsequences of Long m-sequences, IEEE Trans. on Information Theory, **IT-14**-4, 569/576 (1968)
- 14) 柏木, 森内: GF(2) 上の多項式を法とする演算の高速化, 計測自動制御学会論文集, **18**-3, 300/303 (1982)
- 15) A. N. Van Luyk: Shift Register Connections for Delayed Version of m-sequences, Electron. Lett., **14**-22, 713/715 (1978)