Vol. 26 No. 1 情報処理学会論文誌 Jan. 1985

多数項の原始多項式に基づくM系列乱数の高速発生法†

斎藤隆文†† 伏見正則†† 今井 徹††

M系列により擬似一様乱数列を生成する場合，高速化のため，通常は原始3項式を用いるが，このM系列乱数は多数項数の原始多項式に基づく乱数より劣る，という報告もある．そこで，本論文では，5項以上の原始多項式に基づく乱数を，原始3項式に基づくものと同じ速度で発生する方法を提案する．その原理は，適当な既約でない3項式を用い，初期値をうまく選べば，この3項式の因数である，より低次で項数の多い原始多項式に基づくM系列を生成できる，という事実である．任意の原始多項式に対応する，次数がさほど高くない非既約3項式を求めることはできないが，ある特定のものに限れば，M系列の系統サンプリングの性質を使うことにより，実用的な方法が得られる．本方法では，同じ次数の原始3項式に基づく方法と比較して，3倍のメモリを必要とし，初期設定にもより多くの手間がかかるが，初期設定後は原始多項式の項数にかかわらず乱数1個あたり排他的論理和1回だけで発生できる．M系列乱数に関する理論的性質の多くは，本方法の乱数にもあてはまる．例として，521次，279項の原始多項式に基づくM系列を用いて，16次元均等分布が保証された一様乱数を生成する方法を示す．

1. はじめに

1965年に Tausworthe[10] がガロア体 GF(2) 上の原始多項式

$$f(D)=1+c_1D+c_2D^2+\cdots+c_pD^p,\ c_p=1 \quad (1.1)$$

を特性多項式とする線形漸化式

$$a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_pa_{n-p} \pmod 2 \quad (1.2)$$

によって生成される系列（いわゆるM系列）を用いて擬似一様乱数列を作り出す方法を提案してから，これに関連した研究が数多く行われてきた．これらの研究によって得られた理論的な結果は，漸化式の項数——すなわち(1.1)式の項数——によらずに成り立つものも多いが，従来提案されている実用的な発生アルゴリズムは，発生速度が（項数－2）に比例するために，発生速度を重要視する結果，項数が最小（すなわち3項）の原始多項式を用いるものが圧倒的に多い．一方，乱数の使用目的によっては，3項式は必ずしも適当ではなく，もっと項数の多い原始多項式を使うほうがよいのではないか，という指摘もある[8]．そこで本論文では，多数項の原始多項式に基づく乱数を，3項の原始多項式に基づくものと同じ速度で発生する方法を提案する．ただし速度の代償として，同じ次数の3項式を用いる場合の3倍のメモリを必要とする．また，本方法は，5項以上の任意の原始多項式に対して適用できるのではなく，特定のものに限られることをお断りしておく．

2. 既約でない多項式を用いたM系列の発生法

本方法の基本的な原理は，「既約でない3項式を用いてM系列を発生させる」ことである．一般に，p次の原始多項式(1.1)に基づくM系列 $\{a_n\}$ を発生させる場合，漸化式 (1.2) を用いて直前の p 個の値 $a_{n-1}, a_{n-2}, \cdots, a_{n-p}$ だけから a_n を求めるのが通常の方法である．いま，s次 $(s>p)$ の既約でない多項式

$$F(D)=1+C_1D+C_2D^2+\cdots+C_sD^s, \quad C_s=1 \quad (2.1)$$

が，原始多項式 $f(D)$ で割り切れる場合，すなわち

$$F(D)=Q(D)\cdot f(D) \quad (Q(D)\text{は多項式}) \quad (2.2)$$

である場合，M系列 $\{a_n\}$ は

$$a_n=C_1a_{n-1}+C_2a_{n-2}+\cdots+C_sa_{n-s} \pmod 2 \quad (2.3)$$

を満たすから，(1.2)式のかわりに(2.3)式を用いて発生させてもよい．そこで，$F(D)$ として3項式を選べば，(2.3)式も3項間の関係となり，$f(D)$ の項数にかかわらず，M系列 $\{a_n\}$ を1個あたり排他的論理和 (exclusive or) 1回だけで発生させることができる．ただし，記憶領域はsビットが必要である．また，この場合，初期値として独立に選べるのはp項だけで，残りの $s-p$ 項は(1.2)式を満足するように定めないと，一般にはM系列にはならないので，注意を要する．

このように，任意の原始多項式 $f(D)$ に対して，

† High-Speed M-Sequence Random Number Generation Based on the Primitive Polynomials with Many Terms by TAKAFUMI SAITO, MASANORI FUSHIMI and TORU IMAI (Department of Mathematical Engineering and Instrumentation Physics, Faculty of Engineering, University of Tokyo).

†† 東京大学工学部計数工学科

(2.2)式を満たす3項式 $F(D)$ さえ見つかれば，$f(D)$ に基づくM系列乱数を高速に発生させることが，原理的には可能である．しかし現実問題として任意の $f(D)$ からこのような $F(D)$ を見つけることは，一般にきわめて困難である．また，かりに見つかったとしても，記憶領域および初期設定速度の問題から，$F(D)$ の次数があまり高いと実用にならない．

そこで，以下の章では，逆にある種の3項式 $F(D)$ に対して，これを割り切る多数項の原始多項式 $f(D)$ が存在することを示す．さらに，これを用いた乱数発生法について説明する．

3. M系列の系統サンプリング

本方法の基礎になっているのは，M系列の系統サンプリング (decimation) に関する次の性質である[5),7)]．

$\{a_n\}$ を p 次の原始多項式(1.1)によって生成されるM系列とし，σ を $\{a_n\}$ の周期 $T=2^p-1$ と互いに素な正整数とすると，$\{b_n\}=\{a_{n\sigma}\}$ もまた p 次の原始多項式（それを $g(D)$ と書くことにする）によって生成されるM系列である．$g(D)=f(D)$ が成り立つ——すなわち $\{b_n\}$ が $\{a_n\}$ の位相をずらせたものに一致する——ための必要十分条件は，σ が2のべき乗に等しいことである．

いま一般に τ を

$$\sigma\cdot\tau=1 \pmod T,\quad 1\leq\tau<T \tag{3.1}$$

を満たす整数とすると，$\{a_n\}=\{b_{n\tau}\}$ が成り立つ．ここで，われわれは $\sigma=3$ ととることにする（**図1**）．3が $T=2^p-1$ と互いに素になるのは，p が奇数の場合に限られる．そこで今後は，

$$p=2m+1 \tag{3.2}$$

とおくことにする．このとき，(3.1)を満たす τ は，

$$\tau=\frac{2T+1}{3}=4^m+4^{m-1}+\cdots+4+1 \tag{3.3}$$

となる．

次に $g(D)$ として3項式を選ぶ：

$$g(D)=D^p+D^q+1 \quad (p>q) \tag{3.4}$$

このとき，上記の性質により，$f(D)$ は $g(D)$ と異なり，一般に多数の項をもつ原始多項式となり，したがって $\{a_n\}$ は多数項をもつ p 次の漸化式によって生成されるM系列となる．しかしながら，

$$\begin{aligned}&a_n+a_{n-3p}+a_{n-3q}\\&=b_{n\tau}+b_{(n-3p)\tau}+b_{(n-3q)\tau}\\&=b_{n\tau}+b_{n\tau-3p\tau}+b_{n\tau-3q\tau}\\&=b_{n\tau}+b_{n\tau-p}+b_{n\tau-q}=0 \pmod 2\end{aligned} \tag{3.5}$$

であるから，$\{a_n\}$ は $3p$ 次の3項漸化式

$$a_n=a_{n-3p}+a_{n-3q} \pmod 2 \tag{3.6}$$

によっても生成できることになる．このことは，$3p$ 次の既約でない3項式

$$F(D)=g(D^3)=D^{3p}+D^{3q}+1 \tag{3.7}$$

に対して，これを割り切るような多数項の原始多項式 $f(D)$ が存在することにほかならない．

なお，$f(D)$ の項数は，われわれの経験では $p/2$ 程度になることが多かった．p がある程度以上大きいとき，おそらく $f(D)$ は3項式にならないであろうと予想されるが，残念ながら，われわれはその証明を得ていない．したがって，乱数を使用する際は，$f(D)$ の項数を確認しておくことが望ましい（5章参照）．

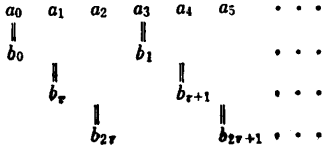

図1 $\{a_n\}$ と $\{b_n\}$ との関係
Fig. 1 The relationship between two M-sequences $\{a_n\}$ and $\{b_n\}\equiv\{a_{3n}\}$.

4. M系列に基づく一様乱数列の生成

4.1 乱数列の発生法

$\{a_n\}$ を用いて l ビットの2進整数乱数列 $\{X_n\}$ を構成する．ここでは簡単のために l が2のべき乗に等しいと仮定する（そうでない場合には，l より大きい最小の2のべき乗で以下の l を置き換えて乱数列を構成し，その上位あるいは下位 l ビットを取り出せばよい）．

X_n の構成のしかたは，Tausworthe 流に

$$X_n=a_{nl}a_{nl+1}\cdots a_{nl+l-1} \quad (2\text{進表現}) \tag{4.1}$$

とする．系列 $\{X_n\}$ の任意の（しかし固定した）位置に現れるビットの系列 $\{a_{nl+i};\ n=0,1,2,\cdots\}$ は，$\{a_n\}$ の要素を2のべき乗番目ごとに系統的にサンプリングしたものになっている．したがってそれは，前記の性質により，$\{a_n\}$ の位相をずらしたものになっているので，漸化式(3.6)によって生成できる．$\{X_n\}$ の任意の位置のビット列が(3.6)式によって生成できるのであるから，系列 $\{X_n\}$ は漸化式

$$X_n=X_{n-3p}\oplus X_{n-3q} \tag{4.2}$$

によって生成できる．ここに記号⊕はビットごとの排他的論理和をとる演算を表す．

4.2 初期値の設定法の原理

漸化式(4.2)を用いて $\{X_n\}$ を生成するためには，初

期値 X_n $(0\leq n\leq 3p-1)$ を与える必要がある．この初期値を構成するM系列の要素は a_n $(0\leq n\leq 3lp-1)$ であるから，このうちの $0\leq n\leq 3p-1$ に相当する部分を与えれば，残りは漸化式(3.6)を用いて生成される．ところが，2章でも述べたように，a_n $(0\leq n\leq 3p-1)$ のうち，独立に与えることができるのは p 項だけである．ここでは，

$$\{a_n;\ 0\leq n\leq 3p-1\}$$
$$=\{b_n;\ 0\leq n\leq p-1\}\cup\{b_{\tau+n};\ 0\leq n\leq p-1\}$$
$$\cup\{b_{2\tau+n};\ 0\leq n\leq p-1\} \qquad (4.3)$$

が成り立つ（図1参照）ことを用いる．右辺の三つの集合のうち，$\{b_{2\tau+n};\ 0\leq n\leq p-1\}$ を任意に与えれば，残りの $\{b_{\tau+n}\}$ および $\{b_n\}$ は一意に定まる．これらは次の手順により求めることができる．

1° D^τ を $g(D)$ で割って得られる剰余多項式を求める．これは，付録1に示す方法を用いれば $O(p^2)$ の手間で求められるが，$g(D)$ だけから求めることもできるので，あらかじめ計算して表にしておいてもよい（記憶領域は p ビット）．

2° 次の関係式

$$(b_{\tau+p-q}+b_{\tau+p-q+1}D+\cdots+b_{\tau+p-1}D^{q-1})$$
$$+(b_\tau D^q+b_{\tau+1}D^{q+1}+\cdots+b_{\tau+p-q-1}D^{p-1})$$
$$=\{(b_{2\tau+p-q}+b_{2\tau+p-q+1}D+\cdots+b_{2\tau+p-1}D^{q-1})$$
$$+(b_{2\tau}D^q+b_{2\tau+1}D^{q+1}+\cdots+b_{2\tau+p-q-1}D^{p-1})\}D^\tau$$
$$(\mathrm{mod}\ g(D)) \qquad (4.4)$$

を用いて $\{b_{n+\tau};\ 0\leq n\leq p-1\}$ を求める．この計算は，p 項の多項式どうしの乗算であるから，$O(p^2)$ の手間でできる．

3° 同様に，関係式

$$(b_{p-q}+b_{p-q+1}D+\cdots+b_{p-1}D^{q-1})$$
$$+(b_0D^q+b_1D^{q+1}+\cdots+b_{p-q-1}D^{p-1})$$
$$=\{(b_{\tau+p-q}+b_{\tau+p-q+1}D+\cdots+b_{\tau+p-1}D^{q-1})$$
$$+(b_\tau D^q+b_{\tau+1}D^{q+1}+\cdots$$
$$+b_{\tau+p-q-1}D^{p-1})\}D^\tau\ (\mathrm{mod}\ g(D)) \qquad (4.5)$$

を用いて $\{b_n;\ 0\leq n\leq p-1\}$ を求める．これも $O(p^2)$ の手間で計算できる．

なお，(4.4)式および(4.5)式の導出法を，付録2に示す．

4.3 初期値設定の高速化

上記の $\{X_n\}$ の初期値設定は，$\{a_n\}$ を1項ずつ求めて X_n に埋め込んでいくという形式で，1ビットずつ処理してもよいが，論理演算を用いて並列に処理して高速化することもできる．一例として，$p=521$，$q=32$（すなわち $g(D)=D^{521}+D^{32}+1$），$l=32$ の場合の手順を示せば次のようになる（$1562=3p-1$，$1567=\lceil 3p/l\rceil l-1$ であることに注意）．

1° 4.2節の手順により $\{a_n;\ 0\leq n\leq 1562\}$ を求める．

2° 漸化式(3.6)を用いて $\{a_n;\ 1563\leq n\leq 1567\}$ を求める．

3° $\{a_n;\ 0\leq n\leq 1567\}$ を用いて $\{X_n;\ 0\leq n\leq 48\}$ を構成する．

4° 漸化式

$$X_n=M^{32}((L^5X_{n-49}+R^{27}X_{n-48})\oplus X_{n-3}) \qquad (4.6)$$

を用いて $\{X_n;\ 49\leq n\leq 1562\}$ を求める．

この手順中の $+$ は論理和，$\oplus$ は排他的論理和，L^5 は5ビット左論理シフト，R^{27} は27ビット右論理シフト，M^{32} は下位32ビットのみを取り出すマスク演算を表す（1語＝32ビットの計算機を用いるなら，マスク演算はもちろん不要である）．

5. 原始多項式 $f(D)$

上記のアルゴリズムでは，乱数列 $\{X_n\}$ を構成しているM系列 $\{a_n\}$ を生成する原始多項式 $f(D)$(1.1式)の具体的な形は不要である．しかし，$f(D)$ の項数が実際に何項になるのかを，念のために確かめておくのがよいであろう．そして，それは次の手順によって実行できる．

4.2節で述べた手続きにより，$\{b_{n+2\tau};\ 0\leq n\leq p-1\}$ を任意に与えて $\{a_n;\ 0\leq n\leq 2p-1\}$ を求めることができる．これらを，(1.2)式で $n=p, p+1,\cdots,2p-1$ とおいたものに代入すると，$f(D)$ の係数 $c_1, c_2,\cdots, c_p$ に関する GF(2) 上の連立1次方程式が得られる．これを解くことによって $f(D)$ の形が陽に求められ

表1 $g(D)=1+D^{32}+D^{521}$ から得られる原始多項式，$f(D)=1+c_1D+c_2D^2+\cdots+c_{521}D^{521}$ の係数 $(1, c_1, c_2,\cdots, c_{521})$

Table 1 The coefficients $(1, c_1, c_2,\cdots, c_{521})$ of the primitive polynomial $f(D)=1+c_1D+c_2D^2+\cdots+c_{521}D^{521}$. The M-sequence generated by the proposed method is based on this $f(D)$ if $g(D)=1+D^{32}+D^{521}$ is used as the original primitive trinomial.

1101100011 1111101010 1100000000 1101101110 1101011111
0110100100 1110110111 1111101000 1101000110 0001111111
1111100101 1101010111 0111101101 0011000000 1111111110
0011000110 1111110001 0110111011 1001100001 0010111011
1110010010 0000100000 0010000101 0100111011 1011110100
1100101110 0101110011 1110100010 0101110011 0100011110
0110010111 1111011101 0010110111 1011011100 0001110001
1100011011 0001100111 0011001010 1001110000 1000011101
0111100110 0000000000 1010110100 0101111010 1001111111
1110000001 1110111000 1010000010 0000011001 0000001010
1100010111 1101010001 11

る．なお，この連立1次方程式の解が $\{b_n; 0 \leq n \leq p-1\}$ の与え方によらないことは，M系列の一般論によって保証されている[7]．

一例として，前出の $g(D)=D^{521}+D^{32}+1$ について $f(D)$ を求めてみたところ，279項式となった．**表1** は $f(D)$ の係数を昇べきの順 $(1, c_1, c_2, \cdots, c_{p-1}, c_p)$ に並べたものである．

6. むすび

M系列の系統サンプリングの性質を利用して，多数項の原始多項式に基づく擬似一様乱数列を高速に発生する方法を提案した．最後に，本方法で生成した乱数列の性質に関して一言ふれておく．まず，これまでに知られているM系列乱数に関する理論的性質の多くは，特性多項式の項数に依存しないため，本方法にもあてはまる．とくに，4章で示した例（$p=521, l=32$ の場合）では，16次以下の任意の次元で均等分布することが，理論的に保証される[3),5)]．一方，特性多項式の違いからくるM系列の乱数としての性質の良し悪しについては，重要な問題だが，理論的な解析は困難であり，まだ十分には解明されていない．今後，研究すべき課題だと思われる．

参考文献

1) Arvillias, A. C. and Maritsas, D. G.: Partitioning the Period of a Class of m-Sequences and Application to Pseudorandom Number Generation, *J. ACM*, Vol. 25, No. 4, pp. 675-686 (1978).
2) Bright, H. and Enison, R.: Quasi-Random Number Sequences from a Long TLP Generator with Remarks on Application to Cryptography, *Comput. Surv.*, Vol. 11, No. 4, pp. 357-370 (1979).
3) Fushimi, M. and Tezuka, S.: The k-Distribution of the Generalized Feedback Shift Register Pseudorandom Numbers, *Comm. ACM*, Vol. 26, No. 7, pp. 516-523 (1983).
4) 伏見正則：一様乱数の発生法，情報処理，Vol. 24, No. 4, pp. 367-371 (1983).
5) 伏見正則：M系列に基づく乱数発生法に関する相反定理とその応用，情報処理学会論文誌，Vol. 24, No. 5, pp. 576-579 (1983).
6) 伏見正則，手塚 集：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. 1, pp. 151-163 (1981).
7) Golomb, S. W.: *Shift Register Sequences*, 224 pp., Holden-Day, San Francisco (1967).
8) 柏木 潤：M系列と正規乱数発生への応用，情報処理，Vol. 22, No. 1, pp. 31-37 (1981).
9) Lewis, T. G. and Payne, W. H.: Generalized Feedback Shift Register Pseudorandom Number Algorithms, *J. ACM*, Vol. 20, No. 3, pp. 456-468 (1973).
10) Tausworthe, R. C.: Random Numbers Generated by Linear Recurrence Modulo Two, *Mathematics of Computation*, Vol. 19, pp. 201-209 (1965).
11) Tootill, J. P. R., Robinson, W. D. and Adams, A. G.: The Runs Up-and-Down Performance of Tausworthe Pseudo-Random Number Generators, *J. ACM*, Vol. 18, No. 3, pp. 381-399 (1971).
12) Tootill, J. P. R., Robinson, W. D. and Eagle, D. J.: An Asymptotically Random Tausworthe Sequences, *J. ACM*, Vol. 20, No. 3, pp. 469-481 (1973).

付録1 $D^\tau \pmod{g(D)}$ の求め方

τ は(3.3)式で与えられているので，

$$D^\tau = D^{4^m+4^{m-1}+\cdots+4+1} \tag{A.1}$$

である．いま，$D^{4^k+4^{k-1}+\cdots+4+1}$ を $g(D)$ で割って得られる剰余多項式を $h_k(D)$ と書くことにすると，容易に確かめられるように，

$$\begin{aligned} h_{k+1}(D) &= \{h_k(D)\}^4 D \\ &= [\{h_k(D)\}^2 (\bmod\ g(D))]^2 D \ (\bmod\ g(D)) \end{aligned} \tag{A.2}$$

という漸化式が成り立つ．これを使って，$h_0(D)=D$ から出発して $h_m(D)=D^\tau (\bmod\ g(D))$ を求めることができる．なお，GF(2) 上では一般に，

$$\begin{aligned} &(\beta_0+\beta_1 D+\beta_2 D^2+\cdots+\beta_{p-1}D^{p-1})^2 \\ &\quad = \beta_0+\beta_1 D^2+\beta_2 D^4+\cdots+\beta_{p-1}D^{2(p-1)} \end{aligned} \tag{A.3}$$

であるから，(A.2)式中の2乗の計算はきわめて単純である．この算法によって $h_m(D)$ を求める手間は $O(p^2)$，所要メモリは $2p$ ビットである．

付録2 (4.4)式および(4.5)式の導出法

一般に

$$R_i(D)=\sum_{k=0}^{q-1} b_{i+p-q+k}D^k+\sum_{k=q}^{p-1} b_{i-q+k}D^k \tag{A.4}$$

とおくと，

$$\begin{aligned} R_{i-1}(D) &= b_{i-1+p-q}+\sum_{k=1}^{q-1} b_{i-1+p-q+k}D^k \\ &\quad + b_{i-1}D^q+\sum_{k=q+1}^{p-1} b_{i-1-q+k}D^k \end{aligned} \tag{A.5}$$

である．ここで，関係式

$$D^p+D^q=1 \ (\bmod\ g(D)) \tag{A.6}$$

$$b_{i-1}+b_{i-1+p-q}=b_{i-1+p} \pmod 2 \qquad \text{(A. 7)}$$

より

$$b_{i-1+p-q}+b_{i-1}D^q=b_{i-1+p}D^q+b_{i-1+p-q}D^p \qquad \text{(A. 8)}$$

が成り立つから，(A. 5)式は

$$R_{i-1}(D)=\sum_{k=1}^{q} b_{i-1+p-q+k}D^k+\sum_{k=q+1}^{p} b_{i-1-q+k}D^k$$

$$=\left(\sum_{k=0}^{q-1} b_{i+p-q+k}D^k+\sum_{k=q}^{p-1} b_{i-q+k}D^k\right)D$$

$$=R_i(D)\cdot D \qquad \text{(A. 9)}$$

となる．これを j 回くり返せば，

$$R_{i-j}(D)=R_i(D)\cdot D^j \qquad \text{(A. 10)}$$

が得られる．(4. 4)式および(4. 5)式は，(A. 10)式にそれぞれ $(i, j)=(2\tau, \tau), (\tau, \tau)$ を代入することにより得られる．

(昭和59年5月21日受付)
(昭和59年7月19日採録)