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†

伏見 正則††

M系列に基づく擬似一様乱数の発生法である Tausworthe の方法と Lewis & Payne の方法との間に成り立つ相反関係 (reciprocity) を示す．その結果を使って，Lewis & Payne の方法における初期値設定の部分を高速化する方法，および相互相関がない複数の乱数列を発生する方法を提案する．

1. はじめに

M系列を使った擬似一様乱数のソフトウェアによる発生法として，Tausworthe[3] によるものと Lewis & Payne[2] によるものがよく知られている．前者については，それによって発生される系列の理論的性質が比較的よくわかっているが，発生速度が一般には遅いという欠点があり，一方，後者については，発生速度は速いが，初期値設定に手間どり，また理論的性質がよくわかっていないという欠点があった．

本論文の目的は，これらの二つの方法の間に相反関係 (reciprocity) があり，したがって両者は本質的には同じものであることを示すことである．その応用として，Lewis & Payne の方法の初期値設定を高速化する方法，および相互相関がない複数の乱数列を発生する方法を提案する．

2. 準 備

以下の議論のために必要な定義およびよく知られている事実を述べる（①〜④については，たとえば文献1)を参照)．

① ガロア体 GF(2) 上の p 次の原始多項式

$$f(z)=1+c_1z+c_2z^2+\cdots+z^p$$

を特性多項式とする漸化式

$$a_t=c_1a_{t-1}+c_2a_{t-2}+\cdots+a_{t-p} \pmod 2 \quad (2.1)$$

を任意の初期条件 $(a_0, a_1, \cdots, a_{p-1})\neq(0, 0, \cdots, 0)$ の下に解いて得られる系列 $\{a_t\}$ のことをM系列と呼ぶ．M系列の特性多項式を明示する必要がある場合には $\{a_t(f)\}$ と書くことにする．M系列は周期列であり，周期 $T=2^p-1$ である．初期条件の選び方は 2^p-1 通りあるが，いずれの初期条件によって得られるM系列も，(f が同一である限り) 位相をずらせば完全に一致する．この意味で，一つの原始多項式には本質的に一つのM系列が対応する．以下の議論では，系列の1周期全体にわたる性質を議論するので，M系列の初期値が何であるかは問題にしない．

② p 次の原始多項式を特性多項式とする任意のM系列 $\{a_t\}$ について次式が成り立つ．

$$\sum_{t=0}^{T-1} a_ta_{t+s}=\begin{cases}2^{p-1}, & s=0 \pmod T\\ 2^{p-2}, & s\neq 0 \pmod T\end{cases} \quad (2.2)$$

③ 1以上で T 未満の整数のうちで T と互いに素なものの全体を R とする．

$$R=\{r \mid 1\leq r<T,\ \gcd(r, T)=1\} \quad (2.3)$$

R は T を法とする乗法に関して群をなす．集合

$$C_0=\{1, 2, 4, \cdots, 2^{p-1}\} \quad (2.4)$$

は，この群の正規部分群であり，その剰余類は (C^0 も含めて) $K\equiv\varphi(T)/p$ 個ある ($\varphi(T)=|R|$ は Euler の totient function)．それらを $(C_0), C_1, C_2, \cdots, C_{K-1}$ で表すことにする．

④ p 次の原始多項式は全部で K 個ある．$\{a_t\}$ がM系列であるとすると，これから r 番目ごとの要素を系統的にサンプリング* して得られる系列

$$\{a_{rt+c}\} \quad (r\in R, 0\leq c<T)$$

もM系列である．同一の剰余類に属する p 個の r に対応するM系列 $\{a_{rt+c}\}$ はすべて同一の原始多項式を特性多項式とする．また，相異なる原始多項式によって生成されるM系列は互いに本質的に異なる．そこで $\{a_t\}$ に対応する原始多項式 f を f_0 と表し，$C_1, C_2, \cdots, C_{K-1}$ に属する r に対応するM系列 $\{a_{rt+c}\}$ を生成する原始多項式を $f_1, f_2, \cdots, f_{K-1}$ と表すことにする．

⑤ M系列 $\{a_t(f)\}$ をもとにして，l ビット ($2\leq$

† A Reciprocity Theorem on the Random Number Generation Based on M-sequences and Its Applications by MASANORI FUSHIMI (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

* 以後，このようなサンプリングのしかたを r-系統サンプリングと呼ぶことにする．

$l \leq p$) の2進小数の系列を次のようにして構成する.

T型系列 $\{x_t(f;\sigma)\}$:

$$x_t = 0.a_{\sigma t}a_{\sigma t+1}a_{\sigma t+2}\cdots a_{\sigma t+l-1},\quad \sigma \in R$$

LP型系列 $\{y_t(f;\tau)\}$:

$$y_t = 0.a_t a_{t+\tau}a_{t+2\tau}\cdots a_{t+(l-1)\tau},\quad \tau \in R$$

ここに, Rは(2.3)で定義した集合である.

T型系列がよい乱数列であるための一つの必要条件として Tausworthe[3] は

$$\sigma \geq l \qquad (2.5)$$

という条件を課しているが, 以下で相反性を議論する間はこの条件をはずしておく. また, Lewis & Payne の方法による乱数発生時の速度が速い理由の一つは, fとして3項式を選ぶためであるが, 当面はこの条件もはずしておく. なお, Lewis & Payne のプログラムでは $\tau = 100p$ と選んでいるが, それでは必ずしも $\tau \in R$ とはならず, よい乱数列が得られるとは限らないことを注意しておく.

3. 相反定理

定理　任意の p と l $(2 \leq l \leq p)$ に対して次の命題が成り立つ.

T型系列 (LP 型系列) の中で, 位相をずらせても重なり合わないという意味で本質的に異なるものの個数は $\varphi^2(T)/p$ 個である. 一方の型の任意の系列に対して, これと本質的に同じ他方の型の系列が一つ存在する. 対応関係は次のとおりである.

$$\{x_t(f_0;\sigma)\} \simeq \{y_t(f_i;\sigma^{-1})\} \text{ if } \sigma \in C_i$$

$$\{y_t(f_0;\tau)\} \simeq \{x_t(f_j;\tau^{-1})\} \text{ if } \tau \in C_j$$

ここに, σ^{-1}, τ^{-1} は, T を法とする乗算に関する σ, τ の逆元* を表し, 記号$\simeq$は両辺の系列が位相を適当にずらせば一致することを表す.

(証明)　まず本質的に相異なる LP 型系列の個数は $\varphi^2(T)/p$ であることを示す. p次の原始多項式fの選び方は $\varphi(T)/p$ 通りで, τ の選び方は $|R| = \varphi(T)$ 通りであるから, f または τ の少なくとも一方が異なる LP 型系列同士は相異なることを示せばよい. 相異なる二つの原始多項式 f および f' から作られる LP 型系列 $\{y_t(f;\tau)\}$ と $\{y'_t(f';\tau')\}$ が本質的に異なることは, これらの系列の第1ビットのみに注目すれば明らかである. つぎに, $f = f'$ としても, $\tau \neq \tau'$ ならば前記の二つの系列は相異なることを示そう. もしもこれらが同じであるとすると, 定数 $c(0 \leq c < T)$ が存在して, すべての t について

$$0.a_t a_{t+\tau}\cdots = 0.a_{t+c}a_{t+c+\tau'}\cdots$$

が成り立つ. 両辺の第1ビットに注目すれば, この式は $c=0$ のときにしか成り立ちえない. $c=0$ とすると, 第2ビットに注目することによって $\tau = \tau'$ でなければならないことが導かれ, $\tau \neq \tau'$ という前提条件に反する. これで, 定理の前半の証明は終わる.

つぎに任意の T 型系列 $\{x_t(f_0;\sigma)\}$, $\sigma \in C_i$, を考える. この系列の第 $(k+1)$ ビット $(0 \leq k \leq l-1)$ を取り出して得られる数列 $\{a_{\sigma t+k}(f_0)\}$ に注目する. これは $\{a_t(f_0)\}$ の σ-系統サンプリングになっているから,

$$\{a_{\sigma t+k}(f_0)\} \simeq \{a_{\sigma(t+k\sigma^{-1})}(f_0)\} \simeq \{a_{t+k\sigma^{-1}}(f_i)\}$$

である. これから, 定理の記述中の第1の対応関係式が得られる. 第2式についても同様で, 次の関係に注意すればただちに導かれる.

$$\{a_{t+k\tau}(f_0)\} \simeq \{a_{\tau^{-1}[\tau(t+k\tau)]}(f_0)\} \simeq \{a_{\tau^{-1}(t+k\tau)}(f_j)\} \simeq \{a_{\tau^{-1}t+k}(f_j)\}\quad \text{(証終)}$$

なお, 定理の中の二つの関係式は, もっと一般的な形に拡張することもできる. いま, $\{a_t(f_0)\}$ をもとにして次の形の系列 $\{z_t(f_0;\sigma,\tau)\}$ を構成する.

$$z_t(f_0;\sigma,\tau) = 0.a_{\sigma t}a_{\sigma t+\tau}a_{\sigma t+2\tau}\cdots a_{\sigma t+(l-1)\tau}$$

ここに σ, τ はともに(2.3)で定義した集合Rの要素であるとする. このとき, 次の命題が成り立つ.

系　もし $\sigma \in C_i$, $\tau \in C_j$ であるならば,

$$\{z_t(f_0;\sigma,\tau\} \simeq \{x_t(f_j;\sigma\tau^{-1}) \simeq \{y_t(f_i;\sigma^{-1}\tau)\}$$

である.

証明は, 定理の証明と同様であるから省略する. この関係式は, σ または τ のいずれか一方を1に等しくすると, 定理のなかの関係式に帰着する. なお, 系のなかの $\{x_t\}$ と $\{y_t\}$ の関係は, 次のように解釈することもできる. $\{x_t(f_j;\sigma')\}$ において, $\sigma' \in C_m$ であるとする. C_j の任意の要素 τ に対して $\tau C_m = C_i$ となる番号 i が (τ の選び方によらず) 一意に定まる. その i に対して

$$\{x_t(f_j;\sigma')\} \simeq \{y_t(f_i;\sigma'^{-1})\}$$

が成り立つ.

4. 応　用

4.1 LP 型系列の初期値設定の高速化

Lewis & Payne の原論文では, 初期値 $y_t(0 \leq t \leq$

* σ, τ は2章の③で定義した群 R の要素であるから, 逆元は存在し, Rのなかでは一意である.

$p-1$) の設定のために必要となる $a_\tau, a_{2\tau}, \cdots, a_{(l-1)\tau}$ 等を求める際に，原則的には漸化式(2.1)を繰り返し使用するという方法を採っているので，所要時間の制約を考えると τ はあまり大きくはできない．一方，系列の自己相関関数

$$R_{yy}(s)=\frac{1}{T}\sum_{t=0}^{T-1}(y_t-\bar{y})(y_{t+s}-\bar{y})$$

($\bar{y}$ は $\{y_t\}$ の1周期分の平均値) の値は，$|s|$ の値ができるだけ大きいところまでほぼ0に等しいことが望ましく，そのためには τ の値を大きくする必要がある*．そこで彼らは，なんらの理論的根拠なしに，$\tau=100p$ と選んだのであるが，これでは不十分なこともある．しかし，相反定理を用いると，τ の値をずっと大きくとって，しかも Lewis & Payne の方法よりもずっと速く初期値を設定する方法が得られる．

まず，乱数のビット数 l が2のべき乗である場合について述べる．$l=2^d$ とし，$\tau=2^p/l\in C_0$ と選ぶ．そうすると，$\tau^{-1}=l$ であるから，相反定理により

$$\{y_t(f_0;\tau)\}\simeq\{x_t(f_0;l)\}$$

となり，M系列 $\{a_t(f_0)\}$ の最初の lp 個 ($0\le t\le lp-1$) の要素を ($\sigma=l$ として) T型に並べれば，LP 型系列の初期値の設定が完了することになる．この初期値設定のために漸化式(2.1)を用いてM系列の要素を計算する回数は $(lp-p)$ 回であり，Lewis & Payne の方法で必要な回数 $(l-1)\tau$ 回に比べてはるかに少ない．(一般に $\tau\gg p$ である．) なお，初期値 $y_t(0\le t\le p-1)$ の設定には，M系列の lp 個の要素が必要であり，したがって漸化式を少なくとも $(lp-p)$ 回は用いる必要があるから，われわれの方法は最小の手間で初期値の設定ができるという意味で最適である**．

l が2のべき乗でない場合には (前記の意味での最適性はないが)，次のようにするのが実際的であろう．l より大きい最小の2のべき乗数を 2^d とする．$\sigma=2^d$ として，M系列 $\{a_t(f_0)\}$ の要素をT型に並べる (これは，2^d ビットの乱数列の初期値を前記の方法で設定し，その先頭の l ビットだけを使用し，下位のビットを切り捨てることに相当する)．

なお，初期値の設定が完了した後の乱数発生の段階では，Lewis & Payne の提案どおり，漸化式

$$y_t=c_1y_{t-1}\oplus c_2y_{t-2}\oplus\cdots\oplus y_{t-p},\quad t\ge p \qquad (4.1)$$

を用いるのがよい．ここに⊕はビットごとの繰り上りなしの足し算を表す．(4.1)式による計算は，右辺の項数が少ないほど速く，したがって原始多項式 $f_0(z)=1+c_1z+c_2z^2+\cdots+z^p$ として3項式を選ぶのが (速度に関する限りでは) 最適である．

4.2 相互相関のない複数の乱数列の発生法

マイクロ・プロセッサを複数台使って並列計算を行う場合等のように，複数の乱数列が必要になる際には，各乱数列が良いものであるとともに，乱数列相互の間に相関がないことが要請されるのが普通である．各プロセッサ内で全然別の (合同法あるいはM系列による) 乱数列を発生させたり，あるいは同一の乱数列の初期値だけをでたらめに変えて使用したりするのでは，相互相関がないという性質を事前に理論的に保証することはできない．そこで，つぎのようにして，非常に周期の長い LP 型系列の位相が互いに大きくずれた部分を各プロセッサで使うこととなるように初期値を設定するのがよく，これによって相互相関のない乱数列を発生することができる．

m 台のプロセッサでそれぞれ l' ビットの乱数を発生するものとする．簡単のために $l'm=2^d$ の場合について述べるが，そうでない場合には，4.1節で述べたのと類似の措置を講ずればよい．$l=l'm$ として，4.1節の方法により，l ビットの LP 型系列の初期値を設定する．これを先頭から l' ビットずつ m 個の部分に切り分け (て小数点を適宜挿入し) たものを各プロセッサで発生する LP 型系列の初期値とする．すなわち，k 番 ($0\le k\le m-1$) のプロセッサで発生させる乱数列を $\{y_t^{(k)}\}$ と書くことにすると，

$$y_t^{(k)}=\sum_{i=1}^{l'}2^{-i}a_{(mt+k)l'+i-1},\quad 0\le t\le p-1$$

とする．

このようにして設定した初期値から作り出される LP 型系列のビット間の位相差 τ は，相反定理により $\tau=2^p/l$ であり，任意の2台のプロセッサで発生される乱数列 $\{y_t\}$ および $\{y'_t\}$ の相互相関関数

$$R_{yy'}(s)=\frac{1}{T}\sum_{t=0}^{T-1}(y_t-\bar{y})(y'_{t+s}-\bar{y}')$$

は，位相差 s が1以上で τ 未満ならばほぼ0に等しいことが(2.2)により容易に示される．原始多項式の次数 p は，各プロセッサで使用する乱数の個数が τ を超えないように大きく選んでおく必要がある．そのような原始多項式は，たとえば文献5),6) の表から容易に探すことができるが，一例として

$$f_0(z)=z^{521}+z^{32}+1$$

---

* $0<|s|<\tau$ なら $R_{yy}(s)\fallingdotseq 0$ であるが，$|s|=\tau$ では $|R_{yy}(s)|$ は大きな値になることが(2.2)から導かれる．

** 文献4) に述べられているような並列演算を用いると，もっと速くすることが可能である．

を選べば，実用上あらゆる場合に十分な大きさのτが得られる．

5. むすび

M系列に基づく擬似一様乱数の発生法である Tausworthe の方法と Lewis & Payne の方法の間に存在する相反関係を示した．それに基づいて，Lewis & Payne 流の乱数発生法の初期値設定の部分を高速化する方法，および相互相関のない複数の乱数列の発生法を提案した．相反性の応用としては，このほかに，一方の系列について知られている理論的性質をもとにして他方の系列の性質を明らかにすることが挙げられるが，これについては別途報告する予定である．

謝辞 相互相関のない複数の乱数列を発生する方法の必要性についてご教示くださった筑波大学の小柳義夫氏に感謝します．また，初稿に対していくつかの有益なコメントをして下さった査読者の方に深謝いたします．

参考文献

1) Golomb, S. W.: *Shift Register Sequences*, 224 pp., Holden-Day, San Francisco (1967).
2) Lewis, T. G. and Payne, W. H.: Generalized Feedback Shift Register Pseudorandom Number Algorithms, *J. ACM*, Vol. 20, No. 3, pp. 456-468 (1973).
3) Tausworthe, R. C.: Random Numbers Generated by Linear Recurrence Modulo Two, *Math. Comput.*, Vol. 19, pp. 201-209 (1965).
4) Tootill, J. P. R., Robinson, W. D. and Eagle, D. J.: An Asymptotically Random Tausworthe Sequence, *J. ACM*, Vol. 20, No. 3, pp. 469-481 (1973).
5) Zierler, N. and Brillhart, J.: On Primitive Trinomials (mod 2), *Inf. Control*, Vol. 13, No. 6, pp. 541-554 (1968).
6) Zierler, N. and Brillhart, J.: On Primitive Trinomials (mod 2) II, *Inf. Control*, Vol. 14, No. 6, pp. 556-569 (1969).

(昭和57年11月18日受付)
(昭和58年2月14日採録)

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†

伏見 正則††

M系列に基づく擬似一様乱数の発生法である Tausworthe の方法と Lewis & Payne の方法との間に成り立つ相反関係 (reciprocity) を示す．その結果を使って，Lewis & Payne の方法における初期値設定の部分を高速化する方法，および相互相関がない複数の乱数列を発生する方法を提案する．

1. はじめに

M系列を使った擬似一様乱数のソフトウェアによる発生法として，Tausworthe[3] によるものと Lewis & Payne[2] によるものがよく知られている．前者については，それによって発生される系列の理論的性質が比較的よくわかっているが，発生速度が一般には遅いという欠点があり，一方，後者については，発生速度は速いが，初期値設定に手間どり，また理論的性質がよくわかっていないという欠点があった．

本論文の目的は，これらの二つの方法の間に相反関係 (reciprocity) があり，したがって両者は本質的には同じものであることを示すことである．その応用として，Lewis & Payne の方法の初期値設定を高速化する方法，および相互相関がない複数の乱数列を発生する方法を提案する．

2. 準 備

以下の議論のために必要な定義およびよく知られている事実を述べる（①〜④については，たとえば文献1)を参照)．

① ガロア体 GF(2) 上の p 次の原始多項式

$$f(z)=1+c_1z+c_2z^2+\cdots+z^p$$

を特性多項式とする漸化式

$$a_t=c_1a_{t-1}+c_2a_{t-2}+\cdots+a_{t-p} \pmod 2 \quad (2.1)$$

を任意の初期条件 $(a_0, a_1, \cdots, a_{p-1})\neq(0, 0, \cdots, 0)$ の下に解いて得られる系列 $\{a_t\}$ のことをM系列と呼ぶ．M系列の特性多項式を明示する必要がある場合には $\{a_t(f)\}$ と書くことにする．M系列は周期列であり，周期 $T=2^p-1$ である．初期条件の選び方は 2^p-1 通りあるが，いずれの初期条件によって得られるM系列も，(f が同一である限り) 位相をずらせば完全に一致する．この意味で，一つの原始多項式には本質的に一つのM系列が対応する．以下の議論では，系列の1周期全体にわたる性質を議論するので，M系列の初期値が何であるかは問題にしない．

② p 次の原始多項式を特性多項式とする任意のM系列 $\{a_t\}$ について次式が成り立つ．

$$\sum_{t=0}^{T-1} a_ta_{t+s}=\begin{cases}2^{p-1}, & s=0 \pmod T\\ 2^{p-2}, & s\neq 0 \pmod T\end{cases} \quad (2.2)$$

③ 1以上で T 未満の整数のうちで T と互いに素なものの全体を R とする．

$$R=\{r \mid 1\leq r<T,\ \gcd(r, T)=1\} \quad (2.3)$$

R は T を法とする乗法に関して群をなす．集合

$$C_0=\{1, 2, 4, \cdots, 2^{p-1}\} \quad (2.4)$$

は，この群の正規部分群であり，その剰余類は (C^0 も含めて) $K\equiv\varphi(T)/p$ 個ある ($\varphi(T)=|R|$ は Euler の totient function)．それらを $(C_0), C_1, C_2, \cdots, C_{K-1}$ で表すことにする．

④ p 次の原始多項式は全部で K 個ある．$\{a_t\}$ がM系列であるとすると，これから r 番目ごとの要素を系統的にサンプリング* して得られる系列

$$\{a_{rt+c}\} \quad (r\in R, 0\leq c<T)$$

もM系列である．同一の剰余類に属する p 個の r に対応するM系列 $\{a_{rt+c}\}$ はすべて同一の原始多項式を特性多項式とする．また，相異なる原始多項式によって生成されるM系列は互いに本質的に異なる．そこで $\{a_t\}$ に対応する原始多項式 f を f_0 と表し，$C_1, C_2, \cdots, C_{K-1}$ に属する r に対応するM系列 $\{a_{rt+c}\}$ を生成する原始多項式を $f_1, f_2, \cdots, f_{K-1}$ と表すことにする．

⑤ M系列 $\{a_t(f)\}$ をもとにして，l ビット ($2\leq$

† A Reciprocity Theorem on the Random Number Generation Based on M-sequences and Its Applications by MASANORI FUSHIMI (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

* 以後，このようなサンプリングのしかたを r-系統サンプリングと呼ぶことにする．

$l \leq p$) の2進小数の系列を次のようにして構成する.

T型系列 $\{x_t(f;\sigma)\}$:

$$x_t = 0.a_{\sigma t}a_{\sigma t+1}a_{\sigma t+2}\cdots a_{\sigma t+l-1},\quad \sigma \in R$$

LP型系列 $\{y_t(f;\tau)\}$:

$$y_t = 0.a_t a_{t+\tau}a_{t+2\tau}\cdots a_{t+(l-1)\tau},\quad \tau \in R$$

ここに, Rは(2.3)で定義した集合である.

T型系列がよい乱数列であるための一つの必要条件として Tausworthe[3] は

$$\sigma \geq l \qquad (2.5)$$

という条件を課しているが, 以下で相反性を議論する間はこの条件をはずしておく. また, Lewis & Payne の方法による乱数発生時の速度が速い理由の一つは, fとして3項式を選ぶためであるが, 当面はこの条件もはずしておく. なお, Lewis & Payne のプログラムでは $\tau = 100p$ と選んでいるが, それでは必ずしも $\tau \in R$ とはならず, よい乱数列が得られるとは限らないことを注意しておく.

3. 相反定理

定理　任意の p と l $(2 \leq l \leq p)$ に対して次の命題が成り立つ.

T型系列 (LP 型系列) の中で, 位相をずらせても重なり合わないという意味で本質的に異なるものの個数は $\varphi^2(T)/p$ 個である. 一方の型の任意の系列に対して, これと本質的に同じ他方の型の系列が一つ存在する. 対応関係は次のとおりである.

$$\{x_t(f_0;\sigma)\} \simeq \{y_t(f_i;\sigma^{-1})\} \text{ if } \sigma \in C_i$$

$$\{y_t(f_0;\tau)\} \simeq \{x_t(f_j;\tau^{-1})\} \text{ if } \tau \in C_j$$

ここに, σ^{-1}, τ^{-1} は, T を法とする乗算に関する σ, τ の逆元* を表し, 記号$\simeq$は両辺の系列が位相を適当にずらせば一致することを表す.

(証明)　まず本質的に相異なる LP 型系列の個数は $\varphi^2(T)/p$ であることを示す. p次の原始多項式fの選び方は $\varphi(T)/p$ 通りで, τ の選び方は $|R| = \varphi(T)$ 通りであるから, f または τ の少なくとも一方が異なる LP 型系列同士は相異なることを示せばよい. 相異なる二つの原始多項式 f および f' から作られる LP 型系列 $\{y_t(f;\tau)\}$ と $\{y'_t(f';\tau')\}$ が本質的に異なることは, これらの系列の第1ビットのみに注目すれば明らかである. つぎに, $f = f'$ としても, $\tau \neq \tau'$ ならば前記の二つの系列は相異なることを示そう. もしもこれらが同じであるとすると, 定数 $c(0 \leq c < T)$ が存在して, すべての t について

$$0.a_t a_{t+\tau}\cdots = 0.a_{t+c}a_{t+c+\tau'}\cdots$$

が成り立つ. 両辺の第1ビットに注目すれば, この式は $c=0$ のときにしか成り立ちえない. $c=0$ とすると, 第2ビットに注目することによって $\tau = \tau'$ でなければならないことが導かれ, $\tau \neq \tau'$ という前提条件に反する. これで, 定理の前半の証明は終わる.

つぎに任意の T 型系列 $\{x_t(f_0;\sigma)\}$, $\sigma \in C_i$, を考える. この系列の第 $(k+1)$ ビット $(0 \leq k \leq l-1)$ を取り出して得られる数列 $\{a_{\sigma t+k}(f_0)\}$ に注目する. これは $\{a_t(f_0)\}$ の σ-系統サンプリングになっているから,

$$\{a_{\sigma t+k}(f_0)\} \simeq \{a_{\sigma(t+k\sigma^{-1})}(f_0)\} \simeq \{a_{t+k\sigma^{-1}}(f_i)\}$$

である. これから, 定理の記述中の第1の対応関係式が得られる. 第2式についても同様で, 次の関係に注意すればただちに導かれる.

$$\{a_{t+k\tau}(f_0)\} \simeq \{a_{\tau^{-1}[\tau(t+k\tau)]}(f_0)\} \simeq \{a_{\tau^{-1}(t+k\tau)}(f_j)\} \simeq \{a_{\tau^{-1}t+k}(f_j)\}\quad \text{(証終)}$$

なお, 定理の中の二つの関係式は, もっと一般的な形に拡張することもできる. いま, $\{a_t(f_0)\}$ をもとにして次の形の系列 $\{z_t(f_0;\sigma,\tau)\}$ を構成する.

$$z_t(f_0;\sigma,\tau) = 0.a_{\sigma t}a_{\sigma t+\tau}a_{\sigma t+2\tau}\cdots a_{\sigma t+(l-1)\tau}$$

ここに σ, τ はともに(2.3)で定義した集合Rの要素であるとする. このとき, 次の命題が成り立つ.

系　もし $\sigma \in C_i$, $\tau \in C_j$ であるならば,

$$\{z_t(f_0;\sigma,\tau\} \simeq \{x_t(f_j;\sigma\tau^{-1}) \simeq \{y_t(f_i;\sigma^{-1}\tau)\}$$

である.

証明は, 定理の証明と同様であるから省略する. この関係式は, σ または τ のいずれか一方を1に等しくすると, 定理のなかの関係式に帰着する. なお, 系のなかの $\{x_t\}$ と $\{y_t\}$ の関係は, 次のように解釈することもできる. $\{x_t(f_j;\sigma')\}$ において, $\sigma' \in C_m$ であるとする. C_j の任意の要素 τ に対して $\tau C_m = C_i$ となる番号 i が (τ の選び方によらず) 一意に定まる. その i に対して

$$\{x_t(f_j;\sigma')\} \simeq \{y_t(f_i;\sigma'^{-1})\}$$

が成り立つ.

4. 応　用

4.1 LP 型系列の初期値設定の高速化

Lewis & Payne の原論文では, 初期値 $y_t(0 \leq t \leq$

* σ, τ は2章の③で定義した群 R の要素であるから, 逆元は存在し, Rのなかでは一意である.

$p-1$) の設定のために必要となる $a_\tau, a_{2\tau}, \cdots, a_{(l-1)\tau}$ 等を求める際に，原則的には漸化式(2.1)を繰り返し使用するという方法を採っているので，所要時間の制約を考えると τ はあまり大きくはできない．一方，系列の自己相関関数

$$R_{yy}(s)=\frac{1}{T}\sum_{t=0}^{T-1}(y_t-\bar{y})(y_{t+s}-\bar{y})$$

($\bar{y}$ は $\{y_t\}$ の1周期分の平均値) の値は，$|s|$ の値ができるだけ大きいところまでほぼ0に等しいことが望ましく，そのためには τ の値を大きくする必要がある*．そこで彼らは，なんらの理論的根拠なしに，$\tau=100p$ と選んだのであるが，これでは不十分なこともある．しかし，相反定理を用いると，τ の値をずっと大きくとって，しかも Lewis & Payne の方法よりもずっと速く初期値を設定する方法が得られる．

まず，乱数のビット数 l が2のべき乗である場合について述べる．$l=2^d$ とし，$\tau=2^p/l\in C_0$ と選ぶ．そうすると，$\tau^{-1}=l$ であるから，相反定理により

$$\{y_t(f_0;\tau)\}\simeq\{x_t(f_0;l)\}$$

となり，M系列 $\{a_t(f_0)\}$ の最初の lp 個 ($0\le t\le lp-1$) の要素を ($\sigma=l$ として) T型に並べれば，LP 型系列の初期値の設定が完了することになる．この初期値設定のために漸化式(2.1)を用いてM系列の要素を計算する回数は $(lp-p)$ 回であり，Lewis & Payne の方法で必要な回数 $(l-1)\tau$ 回に比べてはるかに少ない．(一般に $\tau\gg p$ である．) なお，初期値 $y_t(0\le t\le p-1)$ の設定には，M系列の lp 個の要素が必要であり，したがって漸化式を少なくとも $(lp-p)$ 回は用いる必要があるから，われわれの方法は最小の手間で初期値の設定ができるという意味で最適である**．

l が2のべき乗でない場合には (前記の意味での最適性はないが)，次のようにするのが実際的であろう．l より大きい最小の2のべき乗数を 2^d とする．$\sigma=2^d$ として，M系列 $\{a_t(f_0)\}$ の要素をT型に並べる (これは，2^d ビットの乱数列の初期値を前記の方法で設定し，その先頭の l ビットだけを使用し，下位のビットを切り捨てることに相当する)．

なお，初期値の設定が完了した後の乱数発生の段階では，Lewis & Payne の提案どおり，漸化式

$$y_t=c_1y_{t-1}\oplus c_2y_{t-2}\oplus\cdots\oplus y_{t-p},\quad t\ge p \qquad (4.1)$$

を用いるのがよい．ここに⊕はビットごとの繰り上りなしの足し算を表す．(4.1)式による計算は，右辺の項数が少ないほど速く，したがって原始多項式 $f_0(z)=1+c_1z+c_2z^2+\cdots+z^p$ として3項式を選ぶのが (速度に関する限りでは) 最適である．

4.2 相互相関のない複数の乱数列の発生法

マイクロ・プロセッサを複数台使って並列計算を行う場合等のように，複数の乱数列が必要になる際には，各乱数列が良いものであるとともに，乱数列相互の間に相関がないことが要請されるのが普通である．各プロセッサ内で全然別の (合同法あるいはM系列による) 乱数列を発生させたり，あるいは同一の乱数列の初期値だけをでたらめに変えて使用したりするのでは，相互相関がないという性質を事前に理論的に保証することはできない．そこで，つぎのようにして，非常に周期の長い LP 型系列の位相が互いに大きくずれた部分を各プロセッサで使うこととなるように初期値を設定するのがよく，これによって相互相関のない乱数列を発生することができる．

m 台のプロセッサでそれぞれ l' ビットの乱数を発生するものとする．簡単のために $l'm=2^d$ の場合について述べるが，そうでない場合には，4.1節で述べたのと類似の措置を講ずればよい．$l=l'm$ として，4.1節の方法により，l ビットの LP 型系列の初期値を設定する．これを先頭から l' ビットずつ m 個の部分に切り分け (て小数点を適宜挿入し) たものを各プロセッサで発生する LP 型系列の初期値とする．すなわち，k 番 ($0\le k\le m-1$) のプロセッサで発生させる乱数列を $\{y_t^{(k)}\}$ と書くことにすると，

$$y_t^{(k)}=\sum_{i=1}^{l'}2^{-i}a_{(mt+k)l'+i-1},\quad 0\le t\le p-1$$

とする．

このようにして設定した初期値から作り出される LP 型系列のビット間の位相差 τ は，相反定理により $\tau=2^p/l$ であり，任意の2台のプロセッサで発生される乱数列 $\{y_t\}$ および $\{y'_t\}$ の相互相関関数

$$R_{yy'}(s)=\frac{1}{T}\sum_{t=0}^{T-1}(y_t-\bar{y})(y'_{t+s}-\bar{y}')$$

は，位相差 s が1以上で τ 未満ならばほぼ0に等しいことが(2.2)により容易に示される．原始多項式の次数 p は，各プロセッサで使用する乱数の個数が τ を超えないように大きく選んでおく必要がある．そのような原始多項式は，たとえば文献5),6) の表から容易に探すことができるが，一例として

$$f_0(z)=z^{521}+z^{32}+1$$

---

* $0<|s|<\tau$ なら $R_{yy}(s)\fallingdotseq 0$ であるが，$|s|=\tau$ では $|R_{yy}(s)|$ は大きな値になることが(2.2)から導かれる．

** 文献4) に述べられているような並列演算を用いると，もっと速くすることが可能である．

を選べば，実用上あらゆる場合に十分な大きさのτが得られる．

5. むすび

M系列に基づく擬似一様乱数の発生法である Tausworthe の方法と Lewis & Payne の方法の間に存在する相反関係を示した．それに基づいて，Lewis & Payne 流の乱数発生法の初期値設定の部分を高速化する方法，および相互相関のない複数の乱数列の発生法を提案した．相反性の応用としては，このほかに，一方の系列について知られている理論的性質をもとにして他方の系列の性質を明らかにすることが挙げられるが，これについては別途報告する予定である．

謝辞 相互相関のない複数の乱数列を発生する方法の必要性についてご教示くださった筑波大学の小柳義夫氏に感謝します．また，初稿に対していくつかの有益なコメントをして下さった査読者の方に深謝いたします．

参考文献

1) Golomb, S. W.: *Shift Register Sequences*, 224 pp., Holden-Day, San Francisco (1967).
2) Lewis, T. G. and Payne, W. H.: Generalized Feedback Shift Register Pseudorandom Number Algorithms, *J. ACM*, Vol. 20, No. 3, pp. 456-468 (1973).
3) Tausworthe, R. C.: Random Numbers Generated by Linear Recurrence Modulo Two, *Math. Comput.*, Vol. 19, pp. 201-209 (1965).
4) Tootill, J. P. R., Robinson, W. D. and Eagle, D. J.: An Asymptotically Random Tausworthe Sequence, *J. ACM*, Vol. 20, No. 3, pp. 469-481 (1973).
5) Zierler, N. and Brillhart, J.: On Primitive Trinomials (mod 2), *Inf. Control*, Vol. 13, No. 6, pp. 541-554 (1968).
6) Zierler, N. and Brillhart, J.: On Primitive Trinomials (mod 2) II, *Inf. Control*, Vol. 14, No. 6, pp. 556-569 (1969).

(昭和57年11月18日受付)
(昭和58年2月14日採録)