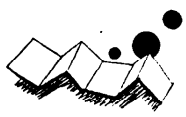
解　説



M系列と正規乱数発生への応用†

柏　木　　濶††

1. まえがき

一様乱数や正規乱数は，不規則変数を扱うシミュレーション実験や数値実験などには欠くことのできないものであり，その発生法に関しては従来数多くの研究がなされている．そして現在ほとんどの計算機のライブラリには，いわゆる合同法を用いた乱数発生のサブルーチンが用意されている．しかし，一方では，合同法によって発生された一様乱数は，多次元空間のある限られた空間に偏在するという「結晶構造」的な規則性があることも指摘されていて[1]，多次元分布が問題となるような使用法の場合は注意が必要となる[2),3)]．乱数発生には，この合同法のほか Tausworthe[4)]の提唱した M 系列を用いた乱数発生法も知られていて，この方法で発生した乱数の質の良さが種々議論されている．

筆者は，ここ数年，M 系列の計測制御への応用，とくに M 系列を用いた正規雑音の発生に関して興味をもってきたが，この方法は単にハードウェアで発生するのに適するだけでなく，計算機内でソフト的に発生するのにも適していて，発生された乱数の統計的性質（振幅分布のひずみ，とがりなど）の理論的予測が可能であり，かなり質の良い正規乱数が発生できることが次第に明らかにされてきている．

本稿は，まず M 系列について一般的解説をし，その後，M 系列を用いて正規乱数を発生する方法につき，内外の研究をもとにして解説を試みたものである．

2. M 系列とその発生法

M 系列とは，Maximum length sequence の最初の M をとった M-sequence の和訳であって，最大長系列または最大周期列といわれる．M 系列を指す用語にはこのほか次のようなものがある．

Maximum length linear shift register sequence
shift register sequence
pseudo-random shift register sequence
pseudo-random sequence
pseudo-random binary signal (PRBS)
linear recurring sequence
chain code
pseudo-noise sequence (PN sequence)

これらの名前は，M 系列がシフトレジスタによって簡単に発生できること，その性質が擬似不規則な性質をもっていることなどに由来する．またこれらの用語の中には M 系列以外の擬似不規則信号を含むものもあるが，多くの場合 M 系列を指すことが多い．一般に p-レベルの M 系列が考えられるが，ここでは最もふつうに用いられる 2-レベルの M 系列に限って記述することにする．

図-1 に示されるような n 段のシフトレジスタの各段に，h_i(=0または1）なる係数をかけ，フィードバックをかけた回路を考える．シフトレジスタの各段の内容 a_i は，0または1とし，図中 ⊕ は，排他的論理和 (Exclusive OR) を表わす．初期状態として各段がすべて0でない限り，ある状態から出発すると，フィードバック回路によって次々に a_i が発生される．係数 h_i のとり方によって，系列 a_i の周期は長くなったり短くなったりするが，h_i を適当に選ぶと，n 段のシフトレジスタを用いて発生することのできる最大の周期の系列が得られる．その周期は 2^n-1 とな

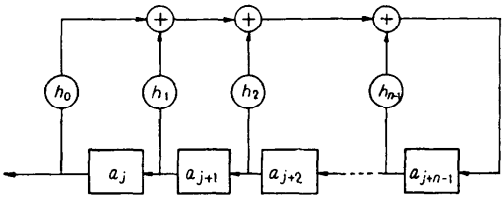


図-1　M系列発生器

† M-sequence and its Application to Gaussian Random Number Generation by Hiroshi KASHIWAGI (Faculty of Engineering, Kumamoto University).

†† 熊本大学工学部

る．この系列を最大長系列または最大周期列 (Maximum length sequence) という．

図-1 において，a_i も h_i も共に 0 または 1 の二値であり，それらの間の演算は，加算が mod 2，乗算が通常の乗算であるから，このような回路で発生される系列を扱うには，a_i や h_i がガロア体 $GF(2)$*に属すると考えると都合がよい．

図-1 の回路で発生される系列は，式でかくと

$$a_{i+n}=\sum_{j=0}^{n-1} h_j a_{i+j} \qquad (1)$$

となる．(1)式は，$h_n=1$ として次のようにもかける．

$$\sum_{j=0}^{n} h_j a_{i+j}=0 \qquad (2)$$

(1)式または (2) 式は，系列を発生させる線形漸化式または線形再帰式 (linear recurrence equation) と呼ばれる．ここで $a_{i+j}=x^j a_i$ となるような一種の遅延演算子 x を導入すると，(2)式は

$$\left(\sum_{j=0}^{n} h_j x^j\right) a_i=0 \qquad (3)$$

となる．ここで

$$h(x)=\sum_{j=0}^{n} h_j x^j \quad (h_0\neq 0,\ h_n=1) \qquad (4)$$

なる多項式は，特性多項式と呼ばれ，発生する系列の性質を決める重要な多項式である．(4)式のような係数が $GF(2)$ に属するような x の多項式は，$GF(2)$ の上の多項式 (a polynomial over $GF(2)$) といわれ，多項式同志の演算は $GF(2)$ の上で行われる．

さて発生される系列 a_i が M 系列であるためには，特性多項式 $h(x)$ は，どのような多項式であればよいだろうか．その答は，原始多項式 (primitive polynomial) とよばれる多項式でなければならない．

$GF(2)$ 上の n 次多項式 $h(x)$ が原始多項式であるとは，次の条件が満たされることである[5),6)]．

(1) $h(x)$ は，n 次の既約多項式である．すなわち，$h(x)$ 自分自身と 1 以外のものは，$h(x)$ を割りきらない．

(2) $h(x)$ は，x^k-1 という多項式を

(a) $0<k<2^n-1$ のとき，割りきらない．

(b) $k=2^n-1$ のときにのみ割りきる．

この 2 つの条件のうち，(2)の方が本質的に重要であって，(2)が満たされれば (1) は自動的に満たされることも示されている[6)]．したがって，原始多項式を求めるには，$GF(2)$ 上の割算を行うことが重要である[7)]．

なお $g(x)=x^n h(x^{-1})$ という多項式は，相反多項式と呼ばれ，$h(x)$ が原始多項式なら $g(x)$ も原始多項式である．$g(x)$ を用いて発生した M 系列は，$h(x)$ による M 系列を時間的に逆向きに並べたものであり，その統計的性質は同じである．図-1 のシフトレジスタをそのまま逆向きにまわしても，$g(x)$ によって発生された系列が得られる．

実際に M 系列を発生する際に，いちいちこの条件をテストするのは大変であるので，次に述べる既発表の原始多項式を利用すると便利である．Peterson[5)]は 16 次まではすべての原始多項式を，17 次以上 34 次までは項数の少ないものを求めている．それより高い次数のものは，Watson[8)]が 100 次まで各次数 1 個の原始多項式を求めており，Zierler and Brillhart[9)]は 1,000 次までの 3 項の原始多項式を求めている．筆者等[10)]は，128 次までの 5 項の原始多項式を求めている．

3. M 系列の性質

M 系列の性質を列挙すると次のようになる[2),7)]．

P 1 一周期内にある 0 の数は 1 の数より常に 1 個少ない．周期 2^n-1 のうち，n のいかんにかかわらず，0 の数 $2^{n-1}-1$ 個，1 の数 2^{n-1} 個であるから，一周期内にある 0 の数と 1 の数はほぼ等しいと考えてよい．

P 2 周期 2^n-1 の M 系列は，その一周期内に，すべてが 0 である場合を除く長さ n のすべてのパターンが 1 回だけ現われる．

P 3 長さ 1 の連は，全体の連の数の半数あり，連の長さが 1 増すごとに数は半減する．長さ $n-1$ の 0 の連と，長さ n の 1 の連は各 1 個ずつあるが，長さが $n-1$ より短い連は，0 の連と 1 の連と同数ある．

P 4 M 系列を $\{a_i\}$ とするとき，それを k だけシフトした系列 $\{a_{i+k}\}$ をつくり，$\{a_i+a_{i+k}\}$ なる系列をつくると，それはもとの系列を j (一意的に定まる) だけシフトしたものになる．すなわち，$a_{i+j}=a_i+a_{i+k}$ (mod 2)．この性質は，shift and add property と呼ばれ，j と k の関係は，個々の特性多項式に依存する．一般に，すべてがゼロでない $s_1, s_2, \cdots s_n$ $(\in GF(2))$ に対して

$$s_1 a_{k-1}+s_2 a_{k-2}+\cdots+s_n a_{k-n}=a_{k+v}$$

なる v が一意的に存在する．

---

* 0 と 1 の 2 つの要素から成る有限集合で，要素間の加減乗除の演算が 2 を法とする算法で定義されるとき，この集合をガロア体 $GF(2)$ という．

P 5 : $\{a_i\}$ の 0 を +1 に, 1 を −1 に対応させた系列 $\{m_i\}$ を考えると, m_i の自己相関関数は次のように与えられる. $N=2^n-1$ とする.

$$\left.\begin{aligned}\phi_{mm}(k)&=\frac{1}{N}\sum_{i=0}^{N-1}m_i m_{i+k}\\&=\begin{cases}1, & k=0,\ N,\ 2N,\ \cdots\\ -\dfrac{1}{N}, & k\neq 0,\ N,\ 2N,\ \cdots\end{cases}\end{aligned}\right\}\qquad(5)$$

M 系列 $\{m_i\}$ を時刻 $i\Delta t<t\leq(i+1)\Delta t$ の間は m_i に保持した M 系列信号 $m(t)$ を考えると, $m(t)$ の自己相関関数は図-2 のようになる. Δt を充分小さくとり, N を充分大きくとれば, 図-2 はほとんどディラックの δ 関数とみなされ, したがって $m(t)$ はほとんど白色信号と近似してよいことが分かる. この性質が M 系列信号を雑音の模擬としてシミュレーションなどに用いるゆえんである. また乱数発生もこの性質に依存している.

P 6 M 系列 $\{a_i\}$ を p 個ごとにサンプルした系列は, p が N と互いに素である限り, 同じ周期の M 系列になる. ただしその特性多項式は一般には異なったものになる.

4. 一様乱数発生への応用

M 系列は, 前章で述べたように, ある一定の規則によって発生される確定的系列でありながら, その性質はランダムな系列によく似ている. この意味で M 系列は擬似不規則 (pseudo-random) な系列といわれる.

この系列を用いて, 一様乱数が発生できることは, 性質 P 2 によって容易に分かる. すなわち, シフトレジスタの内容を 2 進数 x_k (k はシフトパルス周期を単位とする時間を表わす) とみると, x_k は 1 から 2^n-1 までのすべての整数を一周期内に一回ずつとる. そこで $Z_k=x_k/(2^n-1)$ なる数をとると, Z_k は近似的に $(0,1]$ の間で一様分布する数となる. ただ, このままでは, Z_k と Z_{k+1} の内容がオーバラップするため, 相関をもつので, Z_k に白色性も要求するときは, Z_k の次の乱数は Z_{k+n} をとるようにする.

2 進数とみる系列の長さ L を, シフトレジスタの長さ n より小さくとった場合はどうなるか. Tausworthe[4]は, この問題を扱った. すなわち $q\geq L$, $(q,2^n-1)=1$ として,

$$y_k=0.a_{kq-1}a_{kq-2}\cdots a_{kq-L}\ (\text{base }2)\qquad(6)$$

なる数を考えると, y_k は 0 と 1 の間の数であるが,

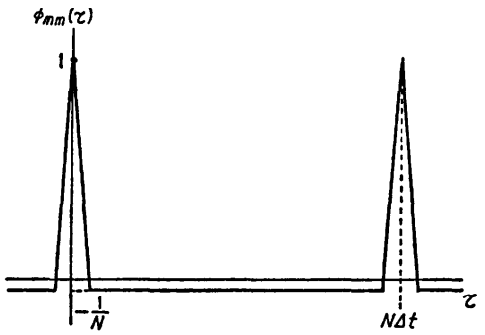


図-2 M系列信号の自己相関関数

これを $(-1,1)$ の間に分布する数に変更するため,

$$w_k=1-2y_k-2^{-L}\qquad(7)$$

なる数を考えると, w_k の平均値 μ は,

$$\mu=-2^{-n}\left(\frac{1-2^{-L}}{1-2^{-n}}\right)\simeq 0\qquad(8)$$

であり, 分散 σ^2 は,

$$\sigma^2=\frac{1}{3}+2^{-n}\left[\frac{1}{3}\left(\frac{1-2^{-2L}}{1-2^{-n}}\right)-\frac{(1-2^{-L})^2}{1-2^{-n}}-2^{-n}\left(\frac{1-2^{-L}}{1-2^{-n}}\right)^2\right]\simeq\frac{1}{3}\qquad(9)$$

となり, w_k は平均値, 分散に関する限り $(-1,1)$ の間で一様分布する乱数と一致することを示した. また, w_k の自己相関関数を計算して, 原点以外では近似的にゼロになることを示し, w_k が白色性も有することも示した. 一周期内の一部分をみても, w_k は一様分布性, 白色性を有することも示している. M 系列を用いて発生される一様乱数列のことを Tausworthe 系列と呼ぶこともある.

Lewis and Payne[2]は, これに対して, 3 項の原始多項式を用いて計算機内での乱数発生に適した方法を示した. いま計算機の一語が L ビット 2 進数から成るとすると, 原始多項式 $h(x)=x^n+x^q+1$ を用いて, M 系列 $\{a_i\}$ から次のような数列 W_k をつくる.

$$\left.\begin{aligned}W_0&=0.a_0a_da_{2d}\cdots a_{Ld-1}\\W_1&=0.a_1a_{d+1}a_{2d+1}\cdots a_{Ld}\\W_2&=0.a_2a_{d+2}\cdots\\&\vdots\\W_i&=0.a_ia_{d+i}\cdots\end{aligned}\right\}(\text{base }2)\qquad(10)$$

すなわち, 数列 W_0, W_1, …の第 1 ビット (第 1 コラム) 目に順に a_i を配列し, 第 2 ビット目には適当に選ばれた数 d だけ第 1 ビット目より遅れた a_i を配置する. d はコラム間遅れと呼んでいる. 第 3 ビット目以下も同様である. このような数列 W_k は, M 系

列の再帰式 $a_k=a_{k-n+q}\oplus a_{k-n}$ に従って，$W_k=W_{k-n+q}\oplus W_{k-n}$ という再帰式に従うことが分かる．したがって，計算機内では，W_{k-n+q} と W_{k-n} とをビットごとに排他的論理和をとることによって，次々に W_k が作られるから大変便利がよい．W_k の周期も出発時における $W_0\sim W_{n-1}$ を適当にとれば，a_i の周期 2^n-1 に一致することも示されている．Lewis and Payne[2]は，$h(x)=x^{98}+x^{27}+1$ を用いて発生した W_k について，連の検定を含み種々の統計的検定を行い，5% 有意水準でほぼ満足すべき一様乱数が得られたと述べているが，津田[3]は同じ原始多項式を用いて検定した結果，連の性質がよくないことを示している．筆者等[11]は，後述する正規乱数発生の経験および重みをつけた M 系列の 2 次元分布に関する研究から，連の性質が悪いのは原始多項式が 3 項から成るためではないかと考え，5 項の原始多項式を用いて同様の検定をした結果，系列相関および連のいずれの検定においても，3 項の場合に比べて良好な結果を得ている．5 項の場合，排他的論理和をとる回数が 3 回必要になるけれども，3 項に比べて質のよい一様乱数が得られる点が有利である．

5. 正規乱数発生への応用

この章では M 系列の擬似不規則な性質を用いて正規乱数を作る方法について，歴史的背景と共に述べる．一般に不規則な信号がいくつかあって，各信号の統計的性質がほぼ似かよっているとき（すなわち，どれかがずば抜けて大きな分散をもつなどということがないとき），その和は中央極限定理によって正規信号に近づく．一つの不規則信号についていえば，低域のフィルタを通すほど，出力は正規信号に近づく．そこで，M 系列を不規則信号とみなし，それを低域フィルタに通して正規信号を得ようとする試みがなされた．Hampton[12]や Kramer[13]の低周波雑音発生器がそれである．Roberts and Davies[14]も M 系列を低域フィルタに通した信号の統計的性質を調べているが，フィルタの時定数が適当な範囲になければ正規にならない点を指摘している点が注目される．この点をより明確に示したのが Gilson[15]であり，フィルタの時定数の影響を実験的に調べ，フィルタの時定数が大きくなると，振幅分布のひずみが大きくなることを示した．またフィルタのカットオフ周波数を f_b とし，M 系列発生器のシフトパルス周波数を f_c とすると，$f_b/f_c\simeq 1/20$ にしたときが最も正規に近い信号が得られることを示した．現在 M 系列を低域フィルタ（またはディジタルフィルタ）に通した形の正規信号発生器が市販されているが，その f_b/f_c の値が約 1/20 であるのは，恐らくこの辺に根拠があるものと思われる．

さて正規信号は，その特徴として線形な系ならどのような系を通過しても依然として正規であるという特徴をもつ．しかるに以上述べた M 系列を単に低域フィルタに通す方法では，フィルタの時定数がある値のときは正規性を示すが，それをさらに低域フィルタに通せばひずみが大きくなって正規性でなくなってしまうという欠点をもつ．この欠点は，発生した信号の使い方によっては全く正規でない信号を用いたことに等価になるわけで，充分気をつけなければならない点である．White[16]は，この点を指摘しており，Douce and Healy[17]は，ひずみの原因が M 系列発生の線形漸化式の影響であることを指摘した．一方 Lindholm[18]は，長い M 系列から相つづく M 個の系列の組（これを M タップルとよぶ）をとり出したとき，M タップルを構成する要素 0, 1 の和がどのような統計的性質を有するかをモーメントを計算することによって調べた．（この系列の和をとる方法は，低域フィルタを通すことと原理的に等価である）．その結果，M タップルの要素の和の平均値と分散は系列の周期が同じなら特性多項式に関係なく一定であるが，三次以上のモーメントは特性多項式によって大きく異なってくることを示した．三次モーメントは分布のひずみを規定する量であるが，M タップルの長さ M を大きくしたとき三次モーメントが大きくなる特性多項式を用いると，低域フィルタを通したとき振幅分布のひずみが大きくなる．大まかな法則として特性多項式が 3 項より成るものは，分布のひずみが大きくなる傾向にあることを示した．

Row and Kerr[19]は，低域フィルタを極値探索法により設計しているが，得られた信号をさらに低域フィルタに通した場合，なお正規性を示すかどうかは疑問である．鈴木，朴，藤井[20]は，きわめて大きい位相差を有する M 系列を加えあわせて擬似正規信号を得る方法を報告している．Thomlinson and Galvin[21]は，M 系列を一次フィルタに通した信号について，3 次までのモーメントを求め，フィルタ時定数が大きくなるとひずみが大きくなる原因が，フィルタ時定数の時間内にある，M 系列の特性多項式で割りきれる 3 項多項式に大きく依存することを示した．

以上述べた方法は，大まかにいって M 系列をその

まま低域フィルタを通して正規信号を得ようとする方法をもとにした議論であった．これに対して筆者等[22]は Tausworthe 法によって発生された一様乱数を加算して正規信号を得るという，いわば中央極限定理に忠実な方法を報告した．以下少しくわしく述べることとする．M 系列の相続く M 個の値に，b_j なる重みをかけて和をとり，次式により X_i を作る．

$$X_i=\sum_{j=0}^{M-1} b_j m_{i+j} \tag{11}$$

重み b_j が 2^{M-j-1} のとき，すなわち，M タップルを2進数とみるとき，X_i は一様分布する乱数となる．そこで X_i と X_{i+1} がオーバラップ部がないように，X_i を M 個ごとにサンプルして X_i^* をつくると，X_i^* は ① 完全に独立ではないにしても互いに無相関であり，② 一様分布という同一の分布に従うため，中央極限定理が適用できるための条件を近似的に満たす．そこで X_i^* を次式によって L 個加算した信号 Y_i をつくると，Y_i は L が大きくなると標準正規分布 $N(0,1)$ に近づくことが期待される．

$$Y_i=\frac{\sqrt{L}}{\sigma}\left(\frac{1}{L}\sum_{j=0}^{L-1} X_{iL+j}^*-\mu\right) \tag{12}$$

ここに，μ，σ^2 はそれぞれ X_i^* の平均値，分散であり，次の式で与えられる．

$$\mu\simeq -2^{-n+M},\quad \sigma^2\simeq 2^{2M}/3 \tag{13}$$

乱数 Y_i の四次までのモーメントを求めると次のようになる．一次モーメント S_1 は，

$$S_1=\frac{1}{N}\sum_{i=0}^{N-1} Y_i=0 \tag{14}$$

二次モーメント S_2 は，

$$S_2=\frac{1}{N}\sum_{i=0}^{N-1} Y_i^2=1 \tag{15}$$

三次モーメント S_3 は，

$$S_3=\frac{1}{N}\sum_{i=0}^{N-1} Y_i^3\simeq\frac{3.9}{L\sqrt{L}}H \tag{16}$$

ここに

$$H=2^{-3(M-1)}\sum_{j=0}^{LM-3}{}^{*}\sum_{k=j+1}^{LM-2}{}^{*}\sum_{l=k+1}^{LM-1}{}^{*} b_j b_k b_l \tag{17}$$

であり，* のついた加算は，$0<j<k<l<LM$ の範囲で

$$a_{i+j}+a_{i+k}+a_{i+l}=0 \pmod 2 \tag{18}$$

が成立つような i，j，k についてのみ加算することを意味するものとする．すなわち，加算をとる範囲内で3項の線形従属の関係にある a_i の組が多いほど H は大きくなることを意味する．$S_1=0$，$S_2=1$ であるから，S_3 は振幅分布のひずみ S (skewness) と同じである．したがって H が大きいほど分布のひずみが大きい．加算の範囲 L が増加したとき，$L\sqrt{L}$ の増加に比して H の増加が大きくならないような特性多項式を用いると，L の増加と共にひずみ S はゼロに近づくことが (16)式から分かる．四次モーメント S_4 も同様に

$$S_4\simeq 3-\frac{1.2}{L}+\frac{13.5}{L^2}G \tag{19}$$

で与えられ，ここに

$$G=2^{-4(M-1)}\sum_{j=0}^{LM-4}{}^{*}\sum_{k=j+1}^{LM-3}{}^{*}\sum_{l=k+1}^{LM-2}{}^{*}\sum_{h=l+1}^{LM-1}{}^{*} b_j b_k b_l b_h \tag{20}$$

であり，* のついた加算は，$0<j<k<l<h\leq LM$ の範囲で

$$a_{i+j}+a_{i+k}+a_{i+l}+a_{i+h}=0 \pmod 2$$

を満たす j，k，l，h の組についてのみ加算することを意味する．加算する範囲内に4項の線形従属のペアが多いほど G は大きくなる．S_4 は，この場合，Y_i のとがり (kurtosis) K に等しいから，4項の線形従属のペアが多いほど，Y_i のとがりが大きくなる．そこで L の増加と共に G が大きくならないような特性多項式を用いれば，L が大きくなると $S_4\to 3$ となり正規分布に近づくことが分かる．

H や G という関数は，L，M，特性多項式などが分かれば計算機で簡単に求められるから，それを(16)，(19)式に代入すると，発生された乱数 Y_i のひずみ S ととがり K が分かる．そこで S と K を用いて Y_i の確率密度関数と正規分布のそれとの差の2乗積分 PI が求められこれを最小にするように M などのパラメータを決めることができる．筆者等[23]は，このような方法で，$n=17\sim34$ の M 系列に対して，3項，5項，7項よりなる特性多項式について，誤差2乗積分 PI を最小にする M タップルの長さ M を求めている．大まかにいって，3項の特性多項式の場合は慎重に M を定めなければならず，下手な選び方をするとひずみが大きい分布になってしまうが，5項，7項の場合は，PI が比較的小さく，M の選定もさほど厳しくない．極端な場合，5項の場合，$M=1$ が最適という場合があって，これは M 系列を単純加算（単に低域フィルタを通す）すればよいことを意味していて興味深い．要するに，正規乱数を得るには3項は避けて5項，7項の特性多項式を用いるのが望ましいといえる．最適に選ばれた M を用いて，種々の加算個数

について実際に発生された乱数について，正規分布への適合度を，χ^2，ひずみ，とがりの3種の検定*によって検定した結果，ほとんどの場合1% 有意水準で正規とみてよい乱数が得られている．

このように同じ周期の M 系列でも特性多項式によって，その性質が大きく異なるから，M 系列を用いる場合，特性多項式を明示することが望ましい．上に引用した文献の中には特性多項式に言及していない文献が多いが，今後注意すべき事項と思われる．特性多項式を明記していない文献では，推定する以外に方法はないが，初期の文献では最も発生が簡単な3項の多項式を用いていると考えてよいようである．

以上述べた方法は，M 系列そのものを用いて乱数を発生する方法であるが，M 系列から派生する系列を用いる方法も考えられている．たとえば，異なる次数の M 系列の和をとって，それを平均する方法[15]，M 系列に非線形な操作，たとえばビット間の論理積をとった系列を作り，それを平均する方法[24]，M 系列を 1 ビットごとに符号を反転して得られる反対称 M 系列を用いる方法[25]などである．また，通信の分野で暗号に関連して，より複雑な系列を作る努力もいくつかなされている．(「複雑な」というのは，容易には解読されないという意味で，ふつうの M 系列ではシフトレジスタの2倍の長さの系列が分かれば，漸化式を解くことによって，それ以後の系列はすべて分かってしまう)．例として，M 系列発生器をいくつか並べておき，1つの発生器のいくつかの段の出力を組合せて，次の発生器の入力にして，いわゆる多重構造にして，複雑さ(complexity)を増した系列を作る方法[26]などがある．このような派生系列は沢山考えられていて，正規乱数発生への応用が種々考えられているが，発生の簡便さ，乱数の質の良さなどから見て，M 系列そのものを用いる方法よりどれがすぐれているかという点は，まだ分かっていないのが現状である．今後の研究が期待されるところである．

6. あ と が き

M 系列と呼ばれる擬似不規則系列について，一般的な概説をし，次にそれを用いて一様乱数，正規乱数を発生させる方法について解説を試みた．

筆者はもともと，制御系のシミュレーション実験などに用いる質の良い正規雑音，発生の容易な正規雑音が欲しいという立場から，正規信号の発生にたずさわってきた．そのような関係で，実際にハードウェアで正規雑音を発生させる方法の記述も含まざるを得なかったが，計算機内で正規乱数を発生させたいと考える情報処理関係の技術者・研究者にも充分参考になるように記述したつもりである．本稿が乱数発生に関心のある方々にとって，少しでもお役に立てば幸いである．

* 発生した乱数に対して，どの程度の正規性を要求するかは，その乱数の使用によってまちまちである．場合によっては，χ^2 検定だけでよい場合もあろうし，ひずみ，とがりよりさらに高次のモーメントに対する検定も必要かもしれない．しかし，ごく普通の使い方を考えれば，ひずみ，とがりの検定まで要求するのは，かなり厳しい要求であって，振幅分布をみただけでは正規性とみえるものでも，はねられる場合が数多くある．したがって，この3種の検定に合格していれば，かなり質の良い正規乱数と考えてよい．

参 考 文 献

1) Marsaglia, G.: Random numbers fall mainly on the planes, Proc. Nat. Acad. Sci., Vol. 61, No. 1, pp. 25-28 (1968).
2) Lewis, T.G. and Payne, W.H.: Generalized feedback shift register pseudorandom number algorithm, J. ACM, Vol. 20, No. 3, pp. 436-468 (1973).
3) 津田孝夫：モンテカルロ法とシミュレーション，p. 22, 培風館，東京 (1977).
4) Tausworthe, R.C.: Random numbers generated by linear recurrence modulo 2, Math. Comp. Vol. 19, pp. 201-209 (1965).
5) Peterson, W.W.: Error correcting codes, MIT Press (1961).
6) 佐藤，中村：擬似ランダム系列 (4), bit, Vol. 7, No. 2, pp. 114-124 (1975).
7) 柏木，森内，管：$GF(2)$上の多項式を法とする演算の高速化，第 22 回自動制御連合前刷，pp. 147-148 (1979).
8) Watson, E.J.: Primitive polynomials (mod 2), Math. Comp. Vol. 16, pp. 368-369 (1962).
9) Zierler, N. and Brillhart, J.: On primitive trinomials (mod 2), Inf. & Control, Vol. 13, pp. 541-554 (1968).
10) 柏木，坂田，管：$GF(2)$上の高次原始多項式，第 19 回計測自動制御学会 (SICE) 講演会前刷，pp. 5-6 (1980).
11) 柏木，坂田，白神：m 系列を用いる擬似乱数の発生，第 19 回 SICE 前刷，pp. 407-408 (1980).
12) Hampton, R.: Experiments using pseudo-random noise, Simulation, Vol. 4, pp. 246-254 (1965).
13) Kramer, C.: A low-frequency pseudo-random noise generator, Electron. Eng. Vol. 37, pp. 465-467 (1965).
14) Roberts, P.D. and Davies, R.H.: Statistical properties of smoothed maximum length linear

binary sequences, Proc. IEE, Vol. 113, pp. 190-196 (1966).
15) Gilson, R. P.: Some results of amplitude distribution experiments on shift register generated pseudorandom noise, IEEE Trans. Vol. EC-15, pp. 926-927 (1966).
16) White, R. C. Jr.: Experiments with digital computer simulation of pseudo-random noise generators, IEEE Trans. Vol. EC-16, pp. 355-357 (1967).
17) Douce, J. L. and Healy, T. J.: Evaluation of the amplitude distribution of quasi-Gaussian signals obtained from pseudorandom noise, IEEE Trans. Vol. C-14, pp. 749-752 (1969).
18) Lindholm, J. H.: An analysis of the pseudo-randomness properties of subsequences of long m-sequences, IEEE Trans. Inf. Theory, Vol. IT-14, pp. 569-576 (1968).
19) Row, I.H. and Kerr, I.M.: A broad spectrum pseudorandom Gaussian noise generator, IEEE Trans. Autom. Control, Vol. AC-15, pp. 529-535 (1970).
20) 鈴木, 朴, 藤井: ハイブリッド式擬似正規白色信号発生器の試作, システムと制御, Vol. 16, No. 4, pp. 569-574 (1972).
21) Thomlinson, G. H. and Galvin, P.: Analysis of skewing in amplitude distributions of filtered m-sequences, Proc. IEE, Vol. 21, No. 12, pp. 1475-1479 (1974).
22) 柏木, 坂田: m 系列を用いる擬似正規信号の発生, SICE 論文集, Vol. 12, No. 3, pp. 293-299 (1976).
23) Kashiwagi, H. and Sakata, M.: A simple method for generating a pseudo-Gaussian signal using a weighted m-sequence, Proc. 7th IFAC Congress held in Helsinki, Finland, pp. 627-633 (1978).
24) 柏木, 坂田, 白神: m 系列の非線形操作による擬似正規信号の発生, 第 18 回 SICE 前刷, pp. 245-246 (1979).
25) 柏木, 坂田, 三竿: 反対称m系列を用いる擬似正規信号の発生, SICE 論文集, Vol. 13, No. 6, pp. 575-579 (1977).
26) Groth, E. J.: Generation of binary sequences with controllable complexity, IEEE Trans. Inf. Theory, Vol. IT-17, pp. 288-296 (1971).
27) 磯部 孝編: 相関函数およびスペクトル, p. 170, 東大出版会, 東京 (1968).
28) 津田孝夫: レーマー型合同法によらない乱数について, bit, Vol. 12, No. 9, pp. 1180-1191 (1980).
29) 伏見正則: 擬似乱数の発生法について, 情報処理, Vol. 21, No. 9, pp. 968-974 (1980).

(昭和 55 年 10 月 6 日受付)