数理解析研究所講究録
第498巻 1983年 118-139

M系列による一様乱数の高次一様性の改善

九州工業技術試験所
泉 照之 (Teruyuki Izumi)

1. まえがき

一様分布の乱数は，モンテカルロ法による数値計算やシミュレーション実験などによく用いられている。従来の一様乱数は，多くの場合合同法に基づいて発生されていた。しかし，この方法による一様乱数は，多次元分布の一様性，すなわち，乱数列が統計的独立性に欠けることが最近明らかにされた。[1] それ以来，通信や制御の分野などでよく用いられている2値のM系列から一様乱数を発生させる方法が注目され始めた。n次のM系列は，n段シフトレジスタの最終段と適当な中間段の出力を排他的論理和することにより，簡単に発生される。一様乱数の発生は，M系列 $\{a_i,\ i=1,2,3,\cdots\cdots,\ a_i=0 \text{ or } 1\}$ からℓ個をサンプルした系列 $(b_1, b_2, \cdots, b_\ell)$ を1つのℓビットの整数とみなすことによってなされ，$(b_1, b_2, \cdots, b_\ell)$ の選び方によって，大きく2つの方法に分けられる。[1] 1つは，

$\{a_i\}$ から σ 個おきに相続く ℓ 個をとって来てならべる Tausworthe 系列で，他の1つは，$\{a_i\}$ から r 個ずつ離れた ℓ 個を逐次取り出してならべる Lewis-Payne系列である．後者は，高速に発生できるので，計算機でのソフトウェアによる方法，あるいは Arvillias-Maritsas が提案するハードウェアによる方法のどちらも有望視されている。また，Lewis-Payne 系列の変形である手塚-伏見による異なる系列間隔 $r_1, r_2, \cdots, r_{\ell-1}$ で $(b_1, b_2, \cdots, b_\ell)$ を作る方法もある。[2] n 次のM系列は，n 次の2値乱数であるので，これから得られる一様乱数の相続く $[n/\ell]$ 個までの系列は，σ，r，$r_1, r_2, \cdots, r_{\ell-1}$ を適当に選ぶことによって $[n/\ell]$ 次元の統計的独立性を満たすことができる．ここで，$[q]$ は q を越えない最大の整数を表わすガウスの記号である．

一方，一様乱数を使う場合，ある決められた次元数の独立性を満たせば十分な場合もあるが，一般には真の乱数に近づけるために，独立性を満たす次元数が大きい方がより望ましい。しかし，M系列の次数 n は大きくても 500程度が普通で，さらに，パーソナルコンピュータやハードウェアで一様乱数を発生させる場合，n は自ら制限される。したがって，定められた n と ℓ において，M系列から得られる一様乱数の $[n/\ell]$ 次以上の独立性を改善させる必要がある．

筆者は，1977年頃から一様乱数がM系列からサンプルした系列 $(b_1, b_2, \cdots, b_l)$ を荷重要素 $(2^0, 2^1, 2^2, \cdots, 2^{l-1})$ で荷重加算されたものであることに注目し，M系列を発生させる特性多項式に基づく線形従属関係を配慮して，荷重要素の配列順を適当にすれば，$l=n$ としたときの2次の統計的独立性が向上させられることを見い出した[3]。そこでは，統計的独立度の逆の概念である統計的従属度なるものを定義し，それと一様乱数列の高次相関値との関係を求め，そして，高次相関値が荷重配列順序に依存することを示し，統計的従属度が小さくなるような荷重配列順について検討している。

本稿は，前述の研究を発展させて，$l<n$ のもとで，$[n/l]$ 次以上の一様乱数の統計的独立性を調べ，M系列を発生させる特性多項式に基づく線形従属関係に応じて荷重要素を配列すれば，統計的独立性が，2次の場合と同様に改善されることを示す。さらに独立性の高い一様乱数を用いれば，それから得られる任意確率の2値乱数の独立性も向上することを示し，荷重配列順を工夫する効果を確かめる．

2. 統計的従属度の定義と高次相関との関係[3]

確率変数 X_i の分布関数を $F_i(x_i)$ とし，m 変数 $X_1, X_2, \cdots X_m$ の結合分布関数を $F(x_1, x_2, \cdots, x_m)$ とすれば，$X_1, X_2, \cdots, X_m$ は

次式が0のとき独立となる．

$$F_e(x_1, x_2, \cdots, x_m) \triangleq F(x_1, x_2, \cdots, x_m) - F_1(x_1) F_2(x_2) \cdots F_m(x_m) \qquad (1)$$

いま，独立でない場合を考え，統計的独立度の逆概念である統計的従属度として次式を定義する．

$$d_m = 2^{m-1} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \{F_e(x_1, x_2, \cdots, x_m)\}^2 \, dx_1 \, dx_2 \cdots dx_m \qquad (2)$$

ここで，右辺の係数 2^{m-1} は，異なる次元における従属度を比較するために導入している．確率変数の密度関数を $f_i(x_i)$，$f(x_1, x_2, \cdots, x_m)$ と表わすと，(1)式の $F_e(x_1, x_2, \cdots, x_m)$ が

$$f_e(x_1, x_2, \cdots, x_m) = f(x_1, x_2, \cdots, x_m) - f_1(x_1) f_2(x_2) \cdots f_m(x_m) \qquad (3)$$

の積分関数であり，かつ，$[-\infty, \infty]$ における f_e の積分値が0となるので，(2)式は，f_e の特性関数 Φ_e を用いて Parseval の等式より

$$d_m = \frac{2^{m-1}}{(2\pi)^m} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \left| \frac{\Phi_e(u_1, u_2, \cdots, u_m)}{(-ju_1)(-ju_2) \cdots (-ju_m)} \right|^2 du_1 \, du_2 \cdots du_m \qquad (4)$$

と表わされる．ここで，Φ_e は次式のような m 変数関数のフーリエ変換である．

$$\Phi_e(u_1, u_2, \cdots, u_m) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} e^{j(u_1 x_1 + u_2 x_2 + \cdots + u_m x_m)}$$

$$\times f_e(x_1, x_2, \cdots, x_m) \, dx_1 \, dx_2 \cdots dx_m \qquad (5)$$

(4) 式の d_m を確率変数の高次積率を用いて具体的に表現するために，(5) 式に (3) 式を代入し，積分記号の代りに期待値演算子 $\langle\cdot\rangle$ を用いて

$$\Phi_e(u_1,u_2,\cdots,u_m)=\left\langle e^{j(u_1X_1+u_2X_2+\cdots+u_mX_m)}\right\rangle - \langle e^{ju_1X_1}\rangle\langle e^{ju_2X_2}\rangle\cdots\langle e^{ju_mX_m}\rangle$$

と表わし，さらに，これを Taylor展開して，つぎのように整理する．

$$\Phi_e(u_1,u_2,\cdots,u_m)=\sum_{k=2}^{\infty} j^k \sum_{k=k_1+\cdots+k_m}{}' C^{k_1,k_2,\cdots,k_m} u_1^{k_1}u_2^{k_2}\cdots u_m^{k_m} \qquad (6)$$

ここで，$C^{k_1,k_2,\cdots,k_m}$ は m 個の確率変数 $X_1, X_2, \cdots, X_m$ の $(k_1, k_2, \cdots, k_m)$ 次の相関値

$$C^{k_1,k_2,\cdots,k_m}=\frac{\langle X_1^{k_1}X_2^{k_2}\cdots X_m^{k_m}\rangle-\langle X_1^{k_1}\rangle\langle X_2^{k_2}\rangle\cdots\langle X_m^{k_m}\rangle}{k_1!k_2!\cdots k_m!} \qquad (7)$$

であり，$\sum'$ は条件 $k=k_1+k_2+\cdots+k_m$ のもとでの非負整数 k_j のすべての組合せについての総和を示す．結局 (4) 式は (7) 式を用いて，(6) 式よりつぎのように表わされる．

$$d_m=\frac{2^{m-1}}{(2\pi)^m}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left|\sum_{k=2}^{\infty} j^k \sum_{k=k_1+\cdots+k_m}{}' C^{k_1,k_2,\cdots,k_m} u_1^{k_1-1}u_2^{k_2-1}\cdots u_m^{k_m-1}\right|^2 \times du_1\,du_2\cdots du_m \qquad (8)$$

この式は，統計的従属度 d_m が高次相関値 $C^{k_1,k_2,\cdots,k_m}$ の複雑な

関数になっているが，高次相関値が小さければ，統計的従属度が小さくなり，確率変数の統計的独立度が高くなることを示す．

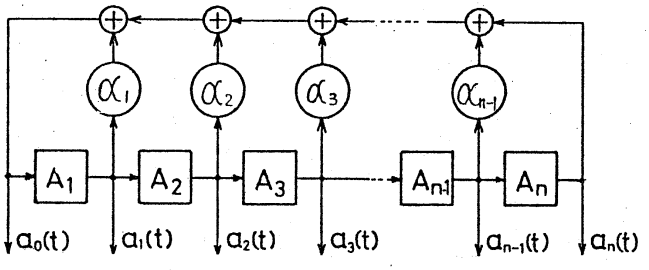
3．M系列による一様乱数

3.1 n次M系列の2値乱数性

図1は，n段シフトレジスタの中で $\alpha_i=1$ なるi段目のレジスタ A_i の出力を排他的論理和して初段に帰還する回路を示す．$\alpha_0=\alpha_1=1$ として，$\alpha_i\ (i=1,2,\cdots,n-1)$ を係数とする特性多項式

$$g(x)=\alpha_0 x^0 \oplus \alpha_1 x^1 \oplus \alpha_2 x^2 \oplus \cdots \oplus \alpha_n x^n \qquad (9)$$

が，ガロア体GF(2)上での原始既約多項式ならば，図1で示す回路は周期 $N=(2^n-1)T$ をもつn次のM系列信号を発生する．ここで，Tはシフトレジスタのクロックパルス周期を示す．いま，A_1 の入力信号 $a_0(t)$ よりkT だけ位相の遅れたM系列を $a_k(t)$ とすれば，n個の相連らなった $a_k(t), a_{k+1}(t)$



⊕ : mod.2 adder
$\alpha_i = \begin{cases} 0 : \text{open} \\ 1 : \text{closed} \end{cases}$
A : shift register

図1 M系列の発生法

$a_{k+2}(t), \cdots, a_{k+n-1}(t)$ を要素とする列ベクトル $a_k(t)$ は，状態遷移行列 S

$$S = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ & & & & & & \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & & \alpha_{n-1} \end{bmatrix} \tag{10}$$

を用いてつぎのような漸化式で表わされる．

$$a_k(t) = S^{k-1} a_1(t) \tag{11}$$

行列 S^{k-1} の第一行ベクトルを β_k とすれば，$a_k(t) = \beta_k(t)\, a_1(t)$ となる．β_k と β_l が GF(2) での n 次元ベクトル空間で線形独立ならば，$a_k(t)$ と $a_l(t)$ は無相関

$$\langle a_k\, a_l \rangle = \langle a_k \rangle \langle a_l \rangle \tag{12}$$

となる[8]．ここで，n 次M系列において，長さ $(n-1)$ の0の連に1つの0を付加して，長さ n の0の連があるものと仮定している．したがって，$\langle a_k \rangle$ は $\sum_{i=1}^{N} a_k(t+iT)/(N+1)$ を意味する．(11) 式の行列 S^{k-1} の階数は n なので，$\beta_k, \beta_{k+1}, \cdots, \beta_{k+n-1}$ は線形独立となり次式が成立する．

$$\langle a_k, a_{k+1}, \cdots, a_{k+n-1} \rangle = \langle a_k \rangle \langle a_{k+1} \rangle \cdots \langle a_{k+n-1} \rangle \tag{13}$$

a_i は0と1からなる2値の確率変数なので，(13)式は，(7)

式の高次相関値 $C^{k_1,k_2,\cdots,k_m}$ をあらゆる組合せの $k_1,k_2,\cdots,k_m$ において0に導く。したがって，n 次M系列の相続く n 個は統計的に独立な2値乱数であるとみなせる．

3.2 M系列による一様乱数列の独立性

$[0,1)$ の一様乱数は，M系列 $\{a_i(j);\ j=1,2,\cdots,2^n-1\}$ から選んだ l 個の要素 $b_{j,1}, b_{j,2},\cdots, b_{j,l}$ を2進小数とみなすことによって得られる．すなわち，時刻 j における一様乱数 u_j は，荷重要素 $w_i=1/2^i$ $(i=1,2,\cdots,l)$ を用いてつぎのように表わされる．

$$u_j=\sum_{i=1}^{l} b_{j,i}\,w_i \tag{14}$$

$u_{j+1}, u_{j+2},\cdots, u_{j+m}$ を確率変数 $X_1, X_2,\cdots, X_m$ とすれば，(7)式の高次相関値

$$C^{k_1,k_2,\cdots,k_m}=\sum_{k_1=k_{1,1}+\cdots+k_{1,l}}{}'\cdots\sum_{k_m=k_{m,1}+\cdots+k_{m,l}}{}' \frac{w_1^{\sum_{j=1}^{m}k_{j,1}}\ w_2^{\sum_{j=1}^{m}k_{j,2}}\cdots\ w_l^{\sum_{j=1}^{m}k_{j,l}}}{k_{1,1}!k_{1,2}!\cdots k_{1,l}!\,k_{2,1}!\cdots k_{2,l}!\cdots k_{m,1}!\cdots k_{m,l}!}$$

$$\times\{\langle b_{1,1}\,b_{1,2}\cdots b_{1,l}\,b_{2,1}\cdots b_{2,l}\cdots b_{m,1}\cdots b_{m,l}\rangle$$

$$-\langle b_{1,1}\,b_{1,2}\cdots b_{1,l}\rangle\langle b_{2,1}\cdots b_{2,l}\rangle\cdots\langle b_{m,1}\cdots b_{m,l}\rangle\} \tag{15}$$

となる．この式の $\{\ \}$ が0，すなわち，$b_{1,1}\,b_{1,2}\cdots b_{1,l}\,b_{2,1}b_{2,2}\cdots b_{2,l}\cdots\ b_{m,1}\,b_{m,2}\cdots b_{m,l}$ が統計的に独立ならば，$u_1, u_2,\cdots, u_m$ は m 次独立な一様乱数になる．

$\{b_{j,i},\ i=1,2,\cdots,\ell\}$ を選ぶ方法として，$\{a_i(j)\}$ から相続く ℓ 個をとる Tausworthe 系列

$$(b_{j,1}b_{j,2}\cdots b_{j\ell})=(a_1(\sigma j),\ a_2(\sigma j),\cdots,\ a_\ell(\sigma j)) \qquad (16)$$

と，r 個飛びに ℓ 個を採用する Lewis-Payne 系列

$$(b_{j,1}\ b_{j,2}\cdots b_{j,\ell})=(a_0(j),\ a_r(j),\ a_{2r}(j),\cdots,\ a_{r(\ell-1)}(j)) \qquad (17)$$

が有名である．前者は，$\sigma=\ell$ で σ と $N(=2^n-1)$ が素ならば，$[n/\ell]$ 次元の独立性が満たされることが (13)式より容易にわかる．(17)式において，r が N を法として $\sigma(=\ell)$ の逆元ならば，2つの系列は同値であることが，柏木[4]や伏見[5]の研究によって最近明らかにされた．したがって，Lewis-Payne 系列も $[n/\ell]$ 次元の独立性を満たすものが存在する．一方，手塚-伏見は，$[n/\ell]$ 次元の独立性を保障して，しかも，単位クロックパルス時間丁毎に一様乱数を発生させるように，図2のような回路構成で，つぎのような $b_{j,i}$ を作ることを提案した。[2]

$$(b_{j,1}\ b_{j,2}\cdots\ b_{j,\ell})=$$
$$(a_1(j),a_n(j),\cdots,a_{r_{n-1}}(j)) \qquad (18)$$

ここで，a_{r_1} は a_1 と $a_{i+\frac{n}{2}}$ との排他的論理和出力で，r_i が

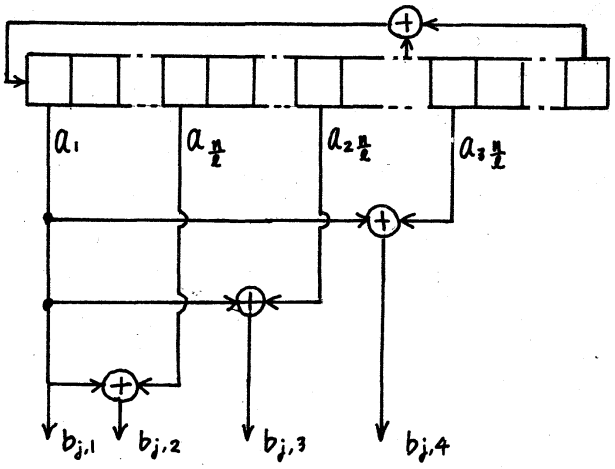


図2　手塚-伏見による一様乱数

その位相を示している.

このように，種々の方法でM系列から一様乱数が発生できるが，いずれにしても m が $[n/l]$ より大きい場合，(15)式の $\{\quad\}$ が0でない場合が必ず生じ，$[n/l]+1$ 次以上の独立性は満たされない.

4 独立性の改善

n 次M系列から l ビットの一様乱数を発生させる場合，$[n/l]$ より高次の独立性は満たされない。一様乱数を使う場合，ある決められた次数 m の独立性が満たされれば十分な場合もある．しかし，一般に真の一様乱数に近ずけるために，独立性が満たされる次数が大きい方が望ましい。また，n を大きくしても500程度が普通であり，さらにパーソナルコンピュータやハードウェアで一様乱数を発生させる場合，n は強い制限を受ける。そこで，ある一定の n，l において $[n/l]+1$ 次以上の独立性をできるだけ改善させる方法を検討する.

発生された一様乱数は，相続く m ($>[n/l]$) 個の独立性が問題となるので，まず，$([n/l]+1)$ 次，つぎに $([n/l]+2)$ 次というようにより低次における統計的従属度 d_m を低めることが必要である．そのために(15)式の高次相関値 $C^{f_{a_1}, f_{a_2}, \cdots, f_{a_m}}$ を小さくさせることを考える．(15)式において，m が $[n/l]+1$ 以上な

らば, $b_{1,1}\ b_{1,2}\cdots b_{1,\ell}\ b_{2,1}\ b_{2,2}\cdots b_{2\ell}\cdots b_{m,1}\ b_{m,2}\cdots b_{m,\ell}$ は線形従属な関係にあり, 全ての組合せにおいて0とならない。しかし, M系列を発生する (9)式の特性多項式に基づく線形従属構造に応じてつぎの手続で荷重要素を配列すれば, $C^{j_1,j_2,\cdots,j_m}$ が小さくなる。

i) 線形従属な組合せのレジスタには小さな値の荷重要素を配置し, 逆に線形独立な組合わせには大きな荷重を配置する.

ii) 線形従属に関係する回数の多いレジスタほど小さな荷重を配置する。

iii) 最大荷重要素 $\frac{1}{2}$ の影響は大きいので, それが配置されたレジスタと線形従属関係をもつレジスタには小さな荷重を配置する.

例えば, $\langle b_{1,j_1}\ b_{2j_2}\ b_{mj_3}\rangle \neq \langle b_{1j_1}\rangle\langle b_{2j_2}\rangle\langle b_{mj_3}\rangle$ のとき, $i=j_1$, j_2, j_3 に比較的小さな荷重 $1/2^{\ell}$, $1/2^{\ell-1}$, $1/2^{\ell-2}$ を配置すれば良い. また, j_1 に最大荷重がすでに配置されていれば, j_2, j_3 には出来るだけ小さな荷重を配置する. 次頁の表1は, 特性多項式 $g(x)=1+x^9+x^{11}$, $\ell=3$ における Tausworthe 系列と Lewis-Payne系列の荷重配列の変えたときの統計的従属度 d_m の実験結果である. 各々, W_{good} は, 3!通りある荷重ベクトルの中で統計的従属度 d_4 を最小にする荷重ベクトルで, W_{bad}

	荷重＼次数	1	2	3	4	5
Tausworthe	$w_{good}=(\frac{1}{8},\frac{1}{2},\frac{1}{4})$	0	0	0	0.0000775	0.0005395
	$w_{bad}=(\frac{1}{2},\frac{1}{8},\frac{1}{4})$	0	0	0	0.002558	0.00420
	$w_{normal}=(\frac{1}{2},\frac{1}{4},\frac{1}{8})$	0	0	0	0.0008528	0.001630
Lewis-Payne	$w_{good}=(\frac{1}{8},\frac{1}{4},\frac{1}{2})$	0	0	0	0.0000046	0.0000197
	$w_{bad}=(\frac{1}{2},\frac{1}{8},\frac{1}{4})$	0	0	0	0.0000502	0.0000829
	$w_{normal}=(\frac{1}{2},\frac{1}{4},\frac{1}{8})$	0	0	0	0.0000167	0.0000384

表1 荷重配列による統計的従属度の比較

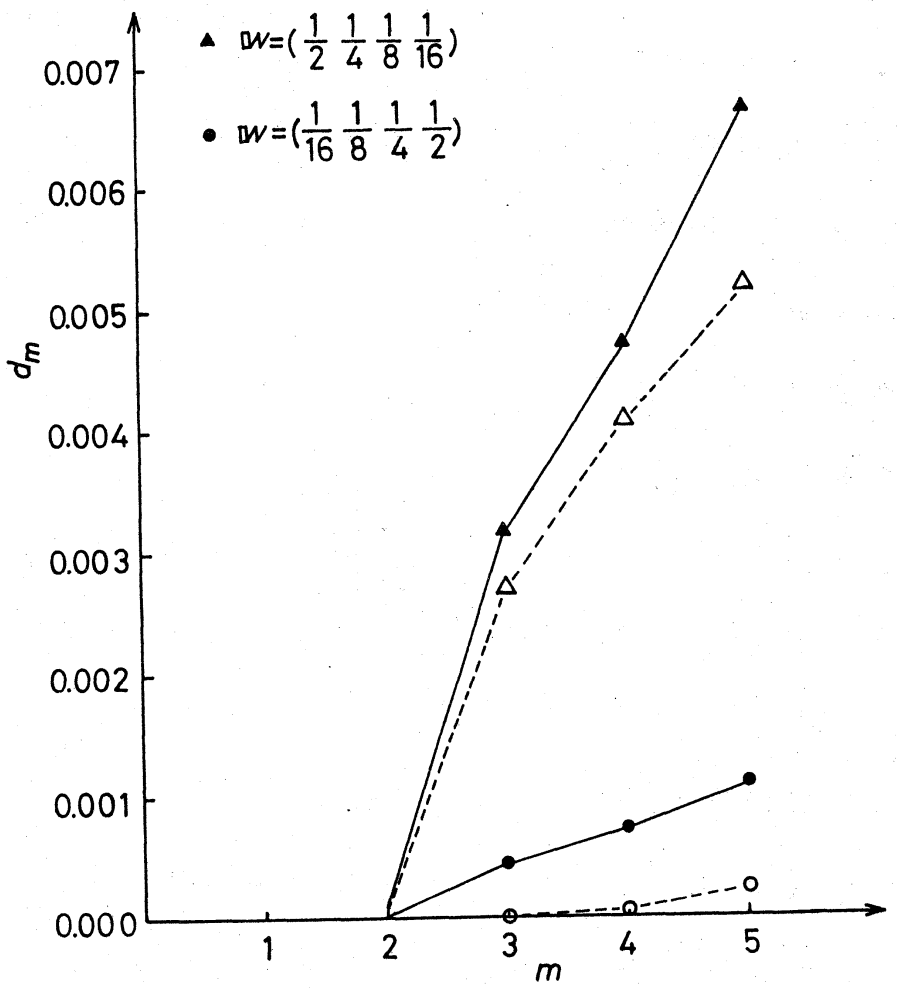


図3 図2による一様乱数の統計的従属度

は d_4 を最大にする荷重ベクトルである．W_{normal} は通常用いられる荷重ベクトルで，大きい順に並んでいる．Tausworthe 系列において，$m=4$ の $b_{j,i}$ をベクトル表現すると表2のようになる．これから $b_{4,3} = b_{1,1} \oplus b_{4,1}$ という線形従属関係があることがわかり，1番目と3番目に小さな荷重が，W_2 に最大荷重がある W_{good} の d_4 が極めて小さくなっていることが了解できる．また，d_4 が小さければ d_5 も小さくなる傾向にあることも表1より明らかであり，荷重配列を工夫することによって統計的独立性が高められることがわかる．

$$\begin{bmatrix} {}_1b_1 \\ {}_1b_2 \\ {}_1b_3 \\ {}_2b_1 \\ {}_2b_2 \\ {}_2b_3 \\ {}_3b_1 \\ {}_3b_2 \\ {}_3b_3 \\ {}_4b_1 \\ {}_4b_2 \\ {}_4b_3 \end{bmatrix} = \begin{bmatrix} 10000000000 \\ 01000000000 \\ 00100000000 \\ 00010000000 \\ 00001000000 \\ 00000100000 \\ 00000010000 \\ 00000001000 \\ 00000000100 \\ 00000000010 \\ 00000000001 \\ 10000000010 \end{bmatrix}$$

表2. Tausworthe 系列の $b_{j,i}$
$g(x) = 1 + x^9 + x^{11}$
$l = 3$

前頁の図3は，$n=9$，$l=4$ における図2のような手塚－伏見による方法で発生した一様乱数の d_m を $m=5$ まで調べた結果である．▲印は大きい順に荷重要素を並べ，●印は小さい順に並べた時の結果を示す．図2の回路からわかるように，a_1 は $b_{j,1}$ $b_{j,2}$ $b_{j,3}$ $b_{j,4}$ の全てに関係しているので，1番目のレジスタは線形従属に関係する回数が最も多い．したがって，頁11の手続iiからわかるように●印の荷重ベクトルの方が d_m を小さくする．なお，○，△印の結果は，手塚－伏見の方法を改良した図7の回路における一様乱数の場合である．

5. 任意確率の2値乱数発生への応用

0と1からなるn次M系列は，3.1で述べたようにn次の独立性を満たすが，1の生じる確率pが0.5に限定されている．ところが2値乱数としては，pが0.5だけでなく0から1までの任意の値が要望されている．任意確率の2値乱数r_iは，n次M系列から得られるlビットの$[0, 2^l)$の一様乱数u_jをVなる値と比較し，$u_j \geq V$なら$r_j=1$，$u_j < V$なら$r_j=0$として発生されるのが普通である．このとき，r_jの1の生じる確率pは

$$p = 1 - \frac{V}{2^l} \tag{19}$$

となる。この2値乱数r_jのm-tuple $(r_{j+1}, r_{j+2}, \cdots, r_{j+m})$の乱数性は，一様乱数$u_j$のm次独立度に依存する．そこで，この章では，M系列による一様乱数から任意確率の2値乱数を発生させる際，一様乱数を得るときの荷重配列順が2値信号の乱数性に及ぼす影響を調べ，乱数性を高める方法について検討する．

5.1 2値乱数性の定義と統計的従属度の関係

2値乱数の相続くm-tuple $(r_{j+1}, r_{j+2}, \cdots, r_{j+m})$に注目し，これらを確率変数$X_1, X_2, \cdots, X_m$とすれば，その1-tuple当りのエントロピは

$$H_m(p) = -\frac{1}{m} \sum f(X_1, X_2, \cdots, X_m) \log_2 f(X_1, X_2, \cdots, X_m) \qquad (20)$$

となる．ここで，Σ は m-tuple のすべてについての和をとることを意味する．m-tuple が真の2値乱数，すなわち m 次独立なとき，1-tuple 当りのエントロピ $H(p)$ は

$$H(p) = -\{p \log p + (1-p) \log (1-p)\} \qquad (21)$$

となる．(20)式と(21)式の差の p に関する平均

$$E_m = \int_0^1 \{H_m(p) - H(p)\} dp \qquad (22)$$

を2値系列 r_i の乱数性の悪さと定義する．

(2)式で定義した統計的従属度 d_m と(22)式の E_m との関係を調べると図4，5のようになった．図4は $m=3$，図5は $m=4$ における種々の一様乱数のもとでの実験結果を示す．これらの図から d_m と E_m はほぼ直線関係にあり，一様乱数の独立性を増せば，それから得られる2値信号の乱数性が良くなることがわかる。

5.2 実験結果

筆者は，1978年にM系列によって発生される任意確率の2値乱数の統計的独立性について発表した[7]．これは，Tauswothe 系列による一様乱数から2値乱数を発生させる場合，荷重の配列順によって2値乱数性が向上することを示している．$p=0.5$ のときは，最大荷重 2^{l-1} のみの影響を受けるので，0と

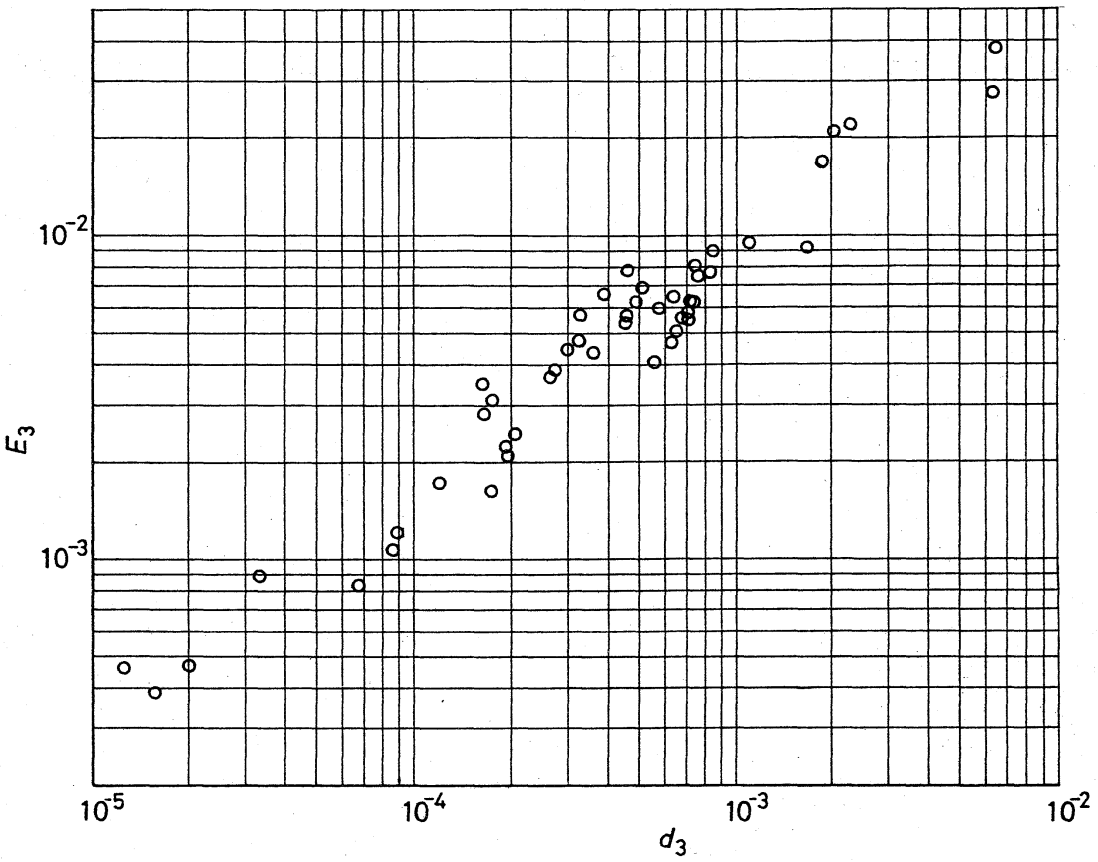


図 4　d_3 と E_3 の実験結果

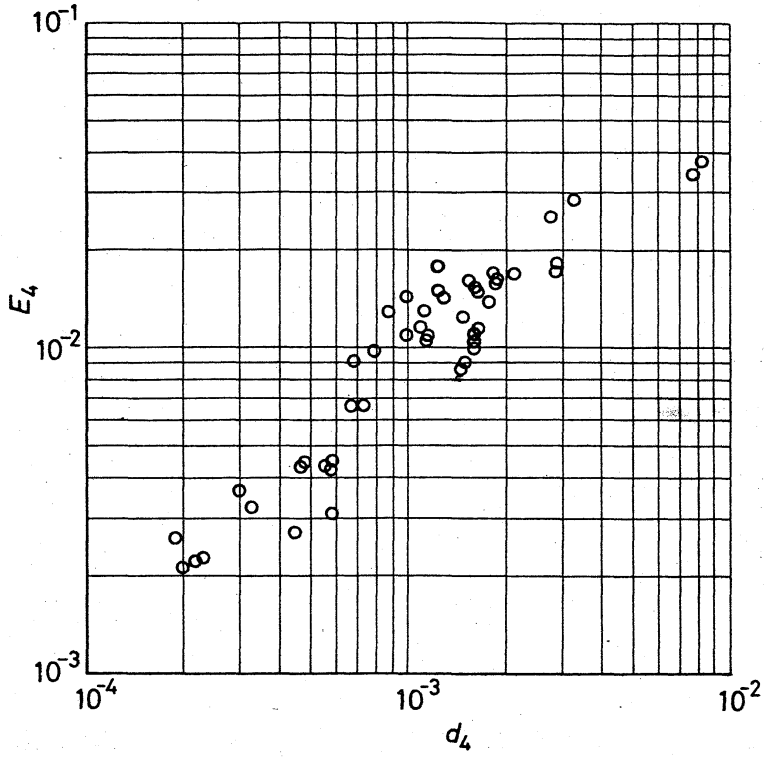


図 5

d_4 と E_4 の実験結果

M系列の周期Nが互いに素であれば，いかなる荷重配列でもn次の独立性を満たし，Pが$\frac{1}{4}, \frac{2}{4}, \frac{3}{4}$のときは，2つの大きな荷重$2^{l-1}, 2^{l-2}$の影響を受けるので，$w_1 = 2^{l-1}$, $w_{\frac{l}{2}} = 2^{l-2}$ならば，$n/2$次の独立性が満たされる．以下同様に，大きな荷重要素を1個毎に配置すれば，$P = \frac{1}{2^{\frac{l}{2}}}, \frac{2}{2^{\frac{l}{2}}}, \frac{3}{2^{\frac{l}{2}}}, \cdots \frac{2^{\frac{l}{2}-1}}{2^{\frac{l}{2}}}$において2次の独立性が満たされる．伏見は，以上のような主旨のことを体系化している[6]が，それでもまだ荷重配列の自由度があり，4章で示した手続きを用いれば，任意のPにおいて2値乱数性が向上する．図6はその結果を示す．•印は，伏見が体系化した荷重配列による一様乱数から得られた結果である．この荷重配列を

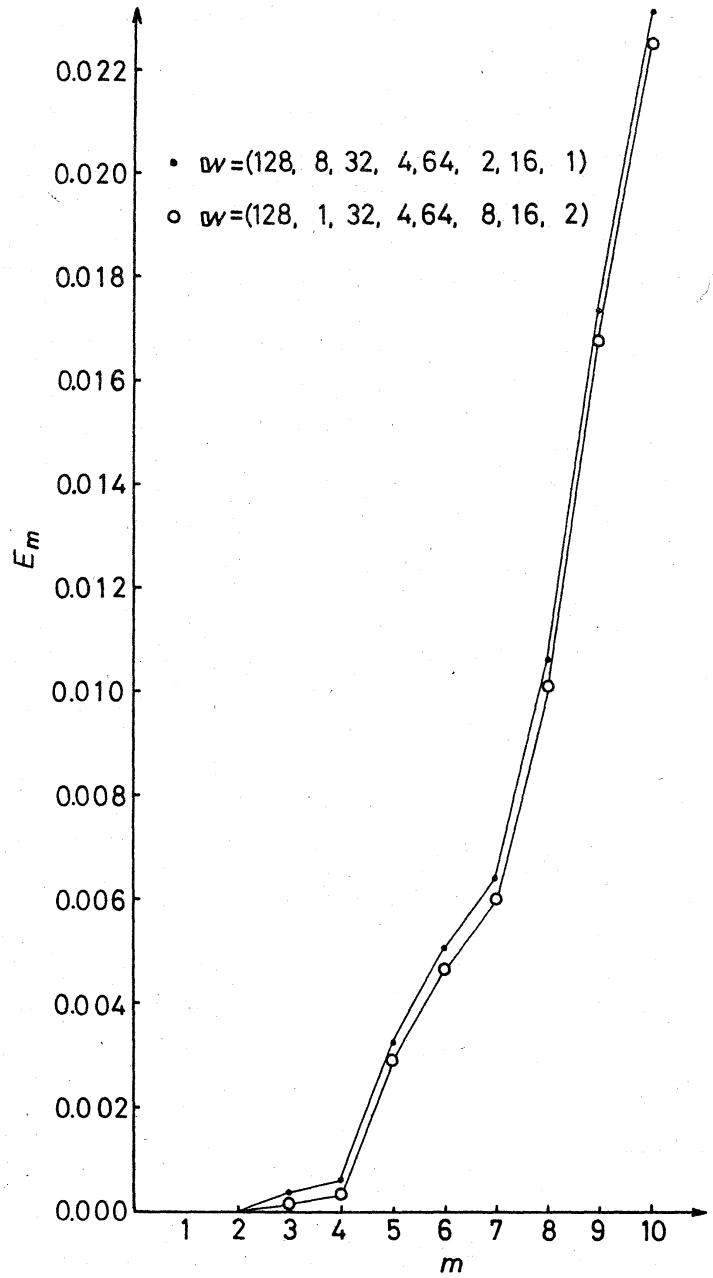


図6　2値乱数性の改善 ($n=15, l=8$ Tausworthe)

基礎にして，小さい荷重 8, 4, 2, 1 を特性多項式 $g(x)=1+x+x^{15}$ の線形従属構造に応じて配列すれば，○印のような結果が得られた．わずかであるが $m=10$ までの全ての m において，E_m が減少しており，2値乱数性が向上している．なお，E_m を求める dp は $1/2^6$ としている．

図7は，図2で示した手塚－伏見が提案した一様乱数発生法において，(18)式の $b_{j,i}$ の線形従属関係を複雑にするために改良したものである．$b_{j,1}=a_1$，$b_{j,2}=a_1+a_{s_b+1}$ で図2と同じであるが，$b_{j,3}=a_2+a_{2s_b+1}$，$b_{j,4}=a_3+a_{3s_b+1}$ となっている．（一般に $b_{j,i}=a_{(i-1)s_a}+a_{(i-1)s_b+1}$）図7は，このように改良した $b_{j,i}$ で一様乱数 u_i を発生し，確率設定用の電圧をAD

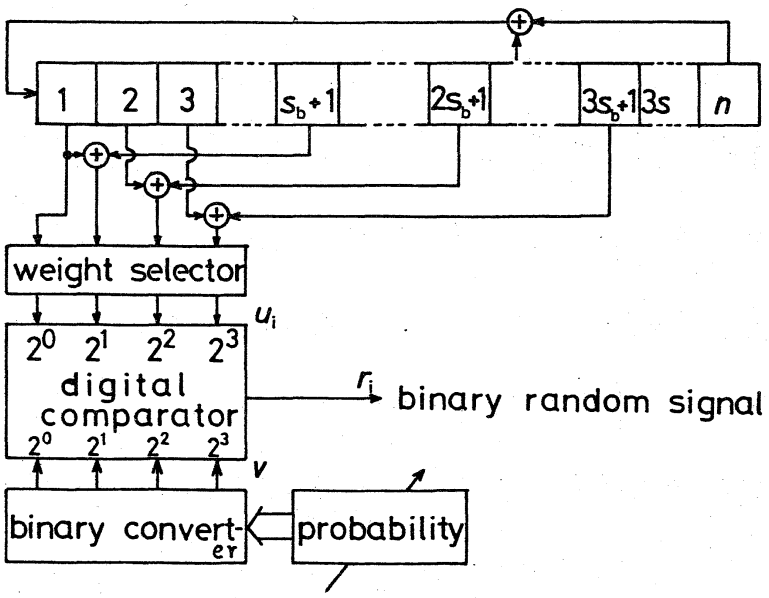


図7　図2を改良した一様乱数から，任意確率の2値乱数発生

変換した値 v と u_i をディジタルコンパレータで比較し，高速に2値乱数を発生させる回路である．

図8は，$n=16$，$l=4$，$S_b=4$，$W=(1,2,4,8)$ のもとで，S_a を0から5まで変えたときの E_m の変化を調べた結果である．$S_a=0$ は図2に相当し，この場合●印のようになった．図2を改良した図7の場合は，$S_a=1$ に相当し，(○印)，E_m が大幅に減少していることがわかる．これによって，$b_{j,i}$ の線形従属関係を配慮すれば，2値乱数性が改善されることがわかる．なお，■印は，$S_a=4$ の場合で，E_m が極めて大きく，$S_a=S_b$ という条件は避けなければいけない．

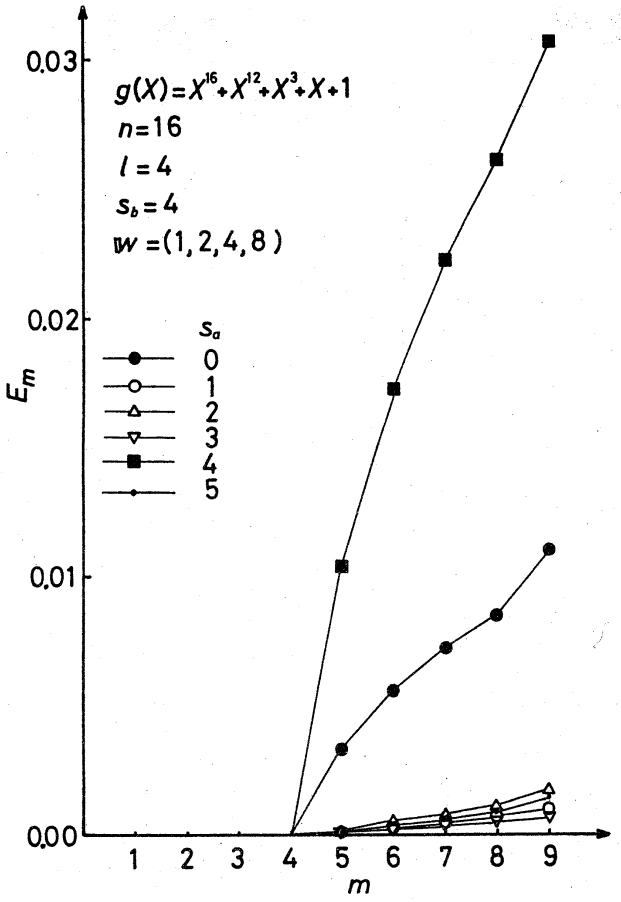


図8　S_a による2値乱数性の比較

図9は，図7で得られた2値乱数の E_m と，Tausworthe 系列から得られた2値乱数の E_m とを比較したものである．$g(x)=1+x^4+x^{15}$，$l=s=4$ のもとで，4! 通りの荷重で Tausworthe 系列を得，これから任意確率の2値乱数の E_m を

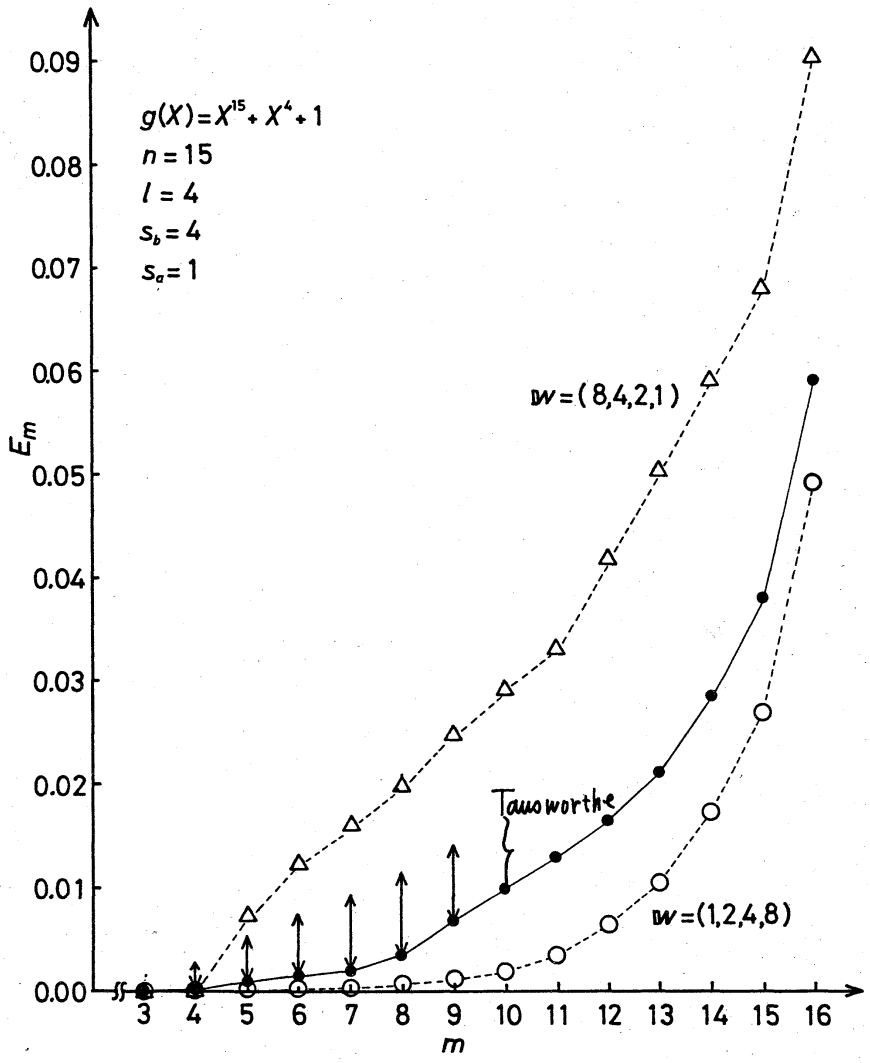


図9　図7の回路による2値乱数とTausworthe のそれとの比較.

求めると，矢印の範囲に収まった．●印は，E_m が最小であると思われる荷重ベクトルで $m=16$ まで調べた結果を示している．これに対して，○印は，図7の回路で発生された2値乱数の E_m であり，Tausworthe 系列のいかなる荷重ベクトルによる場合よりも E_m が小さい．したがって，手塚－伏見の方法を改良した図7は，簡単な回路で，高速にしかも独立性

の良い2値乱数が発生できる．なお，図7の方法において，荷重配列を大きい順にするとEmは△印のようになるので，線形従属構造に応じた荷重配列をしなければならない．

6．あとがき

n次M系列からlビットの一様乱数を得る場合，[n/l]+1次以上の独立性は完全には満たされない．しかし，M系列の特性多項式に基づく線形従属構造に応じて荷重を配列すれば，[n/l]+1次以上の独立性が改善されることを示した．この方法を任意確率の2値乱数発生に応用した結果，かなり高次まで乱数性の良い2値系列が得られ，一様乱数の高次一様性を改善させた効果が確認できた．

参考文献

(1) 津田：モンテカルロ法とシミュレーション，培風館

(2) 手塚，伏見：M系列を用いた擬似乱数発生法，情報処理学会第21回全国大会，昭55年

(3) 泉：M系列によって発生される不規則信号の統計的独立性，計測自動制御学会論文集，vol. 15，no. 1，47～52 (1979)

(4) 柏木：M系列によるTLP乱数の二，三の性質，計測

自動制御学会論文集, vol. 18, no. 8, 828~832 (1982)

(5) 伏見：一様乱数の発生法, 情報処理, vol. 24, no 4, 367~371 (1983)

(6) 伏見："きわめてランダム"な擬似乱数列の発生法, 日本オペレーション学会春季研究発表会, IC-12, 昭57

(7) 泉：M系列によって発生される任意確率の2値乱数の統計的独立性について, 1085, P. 1398~1399, 昭53

(8) H.A. Barker and T. Pradisthayon : High-Order Autocorrelation Functions of Pseudorandom Signals Based on m-Sequences, Proc. IEE, 117-9 1857~1863 (1970)