M 系列によって発生される不規則信号の統計的独立性†

泉 照 之*

On the Statistical Independency of Random Signal Based on M-Sequences

Teruyuki Izumi*

The M-sequence, which is generated by connecting a feedback loop on an n -stage shift register with mod. 2 adders, is frequently used for a binary random signal. But the random signal $x(t)$ obtained from the M-sequences with a weight adder is not statistically independent because its randomness is not complete.

In this paper, a statistical dependency d of the $x(t)$ is defined by

$$d = \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} \{F(x_1, \dots, x_m) - F_1(x_1) \dots F_m(x_m)\}^2 dx_1 \dots dx_m,$$

where $F_i(x_i)$ is a cumulative distribution function of the random variable $x_i = x(t_i)$, $F(x_1, \dots, x_m)$ is a jointly cumulative distribution function of $x_1, \dots, x_m$. The statistical independency of the random signal based on the M-sequences is estimated by this definition. As a result, it is shown that d depends on the feedback loop and also on the weight arrangement of the weight adder even if the feedback loop is the same, and that d decreases if the weight elements are arranged according to the linearly dependent structure of the feedback loop.

1. はじめに

n 段シフトレジスタに mod. 2 加算器で適当に帰還回路を接続すれば、M 系列と呼ばれる 2 値の擬似乱数が発生できる。これは、発生速度が容易に変えられるだけでなく、安定性や再現性が良いため、従来の物理的雑音源に代ってよく用いられるようになった。

一般に、ある不規則信号列を合成して新しい分布の不規則信号を得る場合、元の不規則信号列間の統計的

独立性が前提になる場合が多い。ところが、M 系列信号は帰還回路接続に伴う漸化式に基づいて発生されるので周期性があり、しかもその周期内において完全に独立な 2 値乱数とはいえない。したがって、 $m > n$ なる要素数 m で M 系列を荷重加算して不規則信号を発生させる場合、その分布は解析的に求めにくく¹⁾、分布の低次積率の計算さえ煩雑である^{2), 3)}。一方、 $m \leq n$ の場合、不規則信号の分布やその積率は解析的に得られ、所望の分布を得るための荷重も比較的求めやすい。しかし、その場合でも得られる不規則信号間の統計的独立性は保障されない。このことは、一様分布の不規則信号から中心極限定理に基づいて正規分布を作る場合⁴⁾や、非線形演算によってベキ分布を作る⁵⁾場合などのように、M 系列を荷重加算して発生した不規則信号から、さらに新しい分布を合成するときに問題となる。そのため、漸化式の影響が小さくなるように、反対称 M 系列など修正された M 系列信号が用いられている¹⁰⁾。これに対して、M 系列を発生させる漸化式に適合した荷重を配列することによって、不規則信号間の統計的独立性が高められることも予想できる。

本論文は、M 系列を荷重加算して発生される不規則信号間の統計的独立性を調べ、それを高める条件を見い出すことを目的とする。まず、統計的従属度を定義し、従属度と高次相関の関係を導く。つぎに、M 系列において統計的独立性が満たされる条件を理論的に示す。この条件に従って同一荷重要素で加算されて得られた不規則信号間の高次相関を求め、M 系列を発生させる漸化式が従属度に及ぼす影響を調べる。さらに、荷重要素が異なる場合の従属度が荷重配列にも依存することを示し、一様分布の不規則信号を発生する荷重要素集合を例にとり、従属度を小さくする荷重配列について述べる。

2. 統計的従属度の定義と高次相関との関係

確率変数 X_i の分布関数を $F_i(x_i)$ 、密度関数を $f_i(x_i)$ とし、 m 変数 $X_1, \dots, X_m$ の結合分布関数を $F(x_1,$

† 第 24 回応用物理学関係連合講演会で発表 (昭 52・3)

* 九州工業技術試験所 鳥栖市宿町

* National Industrial Research Institute of Kyushu, Tosu

(Received September 16, 1977)

$\dots, x_m)$, 結合密度関数を $f(x_1, \dots, x_m)$ とすれば, $X_1, \dots, X_m$ は, つぎの同等な式が0のときに独立となる.

$$\begin{aligned} F_e(x_1, \dots, x_m) &\triangleq F(x_1, \dots, x_m) - F_1(x_1) \dots F_m(x_m) \\ f_e(x_1, \dots, x_m) &\triangleq f(x_1, \dots, x_m) - f_1(x_1) \dots f_m(x_m) \end{aligned} \quad (1)$$

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性 d として, 次式を定義する.

$$d \triangleq \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} \{F_e(x_1, \dots, x_m)\}^2 dx_1 \dots dx_m \quad (2)$$

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

$$d = \frac{1}{(2\pi)^m} \int_{-\infty}^{\infty} \dots$$

$$\Phi_e(u_1, \dots, u_m) = \sum_{k=2}^{\infty} j^k \sum'_{k=k_1+\dots+k_m} \frac{E\{X_1^{k_1} \dots X_m^{k_m}\} - E\{X_1^{k_1}\} \dots E\{X_m^{k_m}\}}{k_1! \dots k_m!} u_1^{k_1} \dots u_m^{k_m} \quad (6)$$

となる. ここで, Σ' は条件 $k=k_1+\dots+k_m$ のもとで非負整数 k_i のすべての組合せについての総和を示す. $m=2$ の場合, $(E\{X_1^{k_1} X_2^{k_2}\} - E\{X_1^{k_1}\} E\{X_2^{k_2}\})/k_1! k_2! = C^{k_1, k_2}$ を (k_1, k_2) 次相関とすれば, X_1 と X_2 の d は(3)式より

$$\begin{aligned} d &= \frac{1}{4\pi^2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \left[\sum_{k=1}^{\infty} (-1)^k \right. \\ &\quad \cdot \sum_{i=1}^{2k-1} C^{2k-i, i} u_1^{2k-i-1} u_2^{i-1} \Big]^2 \\ &\quad + \left[\sum_{k=1}^{\infty} (-1)^k \sum_{i=1}^{2k} C^{2k+1-i, i} u_1^{2k-i} u_2^{i-1} \right]^2 \Big] du_1 du_2 \end{aligned} \quad (7)$$

と表わされる. この式より, すべての k_1, k_2 において $C^{k_1, k_2} = 0$ ならば, $d=0$, すなわち, X_1 と X_2 は統計的に独立となることがわかる.

3. M系列の統計的独立性

3.1 M系列信号の性質⁶⁾

Fig. 1 の実線部は, n 段シフトレジスタの中で $\alpha_i = 1$ なる A_i の出力を mod. 2 加算して, 初段に帰還しているのを示す. このとき, 帰還回路接続パターン $\alpha (\alpha = \alpha_0, \alpha_1, \dots, \alpha_n; \alpha_i = 0 \text{ or } 1, \alpha_0 = \alpha_n = 1)$ を係数とした特性多項式

$$g(D) = \alpha_0 D^0 \oplus \alpha_1 D^1 \oplus \dots \oplus \alpha_n D^n \quad \oplus: \text{mod. 2 和} \quad (8)$$

が, ガロア体 $GF(2)$ 上での原始既約多項式ならば, Fig. 1 の $a_i(t)$ は周期 $N (=2^n - 1)T$ のM系列信号

$$\int_{-\infty}^{\infty} \left| \frac{\Phi_e(u_1, \dots, u_m)}{(-ju_1) \dots (-ju_m)} \right|^2 du_1 \dots du_m \quad (3)$$

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

$$\begin{aligned} \Phi_e(u_1, \dots, u_m) &= \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} e^{j(u_1 x_1 + \dots + u_m x_m)} \\ &\quad \times f_e(x_1, \dots, x_m) dx_1 \dots dx_m \end{aligned} \quad (4)$$

つぎに, (4)式の Φ_e を確率変数の高次積率で表わし, (3)式の d に具体性をもたせる. (4)式に(1)式の f_e を代入して, 積分記号の代りに期待値演算子 E を用いると, Φ_e はつぎようになる.

$$\begin{aligned} \Phi_e(u_1, \dots, u_m) &= E\{e^{j(u_1 X_1 + \dots + u_m X_m)}\} \\ &\quad - E\{e^{ju_1 X_1}\} \dots E\{e^{ju_m X_m}\} \end{aligned} \quad (5)$$

指数項を Taylor 展開すると, (5)式は

となる. ここで, D は遅延演算子を, T はその遅延時間を示す. いま, n 個の連なった $a_k(t), a_{k+1}(t), \dots, a_{k+n-1}(t)$ を列ベクトル $\mathbf{a}_k(t)$ とすれば, これは状態遷移行列 S を用いてつぎの漸化式で表わされる.

$$\mathbf{a}_k(t) = \mathbf{a}_1(t - (k-1)T) = S^{k-1} \mathbf{a}_1(t) \quad (9)$$

$$S = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_{n-1} \end{bmatrix} \quad (10)$$

ここで, S はシフトレジスタの性質と $g(D)=0$ とした特性方程式から求められる. また, I を単位行列とすれば, $\mathbf{a}_k(t)$ がM系列なので $S^N = S^0 = I$ となる.

3.2 M系列の周期内における統計的独立性

M系列は周期性をもつため, その統計的性質は1周期内で議論することになる. その場合でも, M系列の統計的独立性はつぎの問題点 A), B) を含んでいる.

Fig. 1 Random signal generator by weight-adding the state of shift register which is generating M-sequence (broken line is imaginary circuit)

A) $a_k(t)$ の 0 の回数は $2^{n-1}-1$ で 1 の回数より 1 回少なく, $a_k(t)$ の平均値は $2^{n-1}/N \approx 0.5$ である.

B) $a_k(t)$ は, 漸化式に基づく比較的少数 k_i 個の $a_{k_1}(t), a_{k_2}(t), \dots, a_{k_i}(t)$ の影響をうける.

A) は n の増加とともに解消されるので, 本論文の中心課題は B) を調べることである. しかし, この目的は A) のために通常の周期内平均操作で達成できない. そこで, 小さい n において B) のみを際立たせるために, 2 章の E の代りに新しい平均操作 $\langle a_k \rangle = \sum_{i=1}^N a_k(t+iT)/(N+1)$ を用いる. なお, この平均操作に基づく (6) 式による (3) 式の d は, (2) 式のそれと少し異なるが, n の増加につれて一致する.

(9) 式において, 行列 S^{k-1} の第 1 行ベクトルを β_k とすれば, $a_k(t) = \beta_k \alpha_i(t)$ となる. いま, 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 $\langle a_k a_l \rangle = \langle a_k \rangle \langle a_l \rangle$ となる⁷⁾. したがって, $\beta_k, \beta_{k+1}, \dots, \beta_{k+n-1}$ は行列 S^{k-1} の階数が n となるので, 線形独立となり, 次式が成立する.

$$\langle a_k^{r_1} a_{k+1}^{r_2} \dots a_{k+n-1}^{r_n} \rangle = \langle a_k^{r_1} \rangle \langle a_{k+1}^{r_2} \rangle \dots \langle a_{k+n-1}^{r_n} \rangle \quad (11)$$

ここで, r_i は 0 or 1 である. M 系列は 2 値であるた

め, (11) 式の無相関性だけで (6) 式の Φ_e は恒等的に 0 となる. したがって, (3) 式の d は 0 となり, a_k の n 要素は統計的に独立な 2 値乱数となる. もし, $\beta_{k_1}, \beta_{k_2}, \dots, \beta_{k_m}$ からなる (m, n) 行列の階数が m ならば, $a_{k_1}, a_{k_2}, \dots, a_{k_m}$ も統計的に独立となる. なお, 行列の階数はたかだか n なので, M 系列における $(n+1)$ 個以上からなる要素間の統計的独立性は満たされない.

4. M 系列を荷重加算して発生される不規則信号の統計的独立性

M 系列を発生しているシフトレジスタの状態 $a_i(t)$ を荷重ベクトル $w (=w_1, \dots, w_n; n' \leq n)$ で荷重加算すれば, 次式のような不規則信号 $x(t)$ が得られる.

$$x(t) = \sum_{i=1}^{n'} a_i(t) w_i \quad (12)$$

この $x(t)$ を $n_s T$ ごとにサンプルした m 個の確率変数 $X_{jn_s} = x(t - jn_s T)$ ($j=0, 1, \dots, m-1$) の統計的独立性に関する議論は, (3), (6) 式よりなされるが, m が大きいと簡単でない. したがって, ここでは大きな m の場合の基礎になる $m=2$ について調べる. そこで, X_0 と X_{n_s} の (K, L) 次相関 $C_{n_s}^{K,L}$ を (12) 式より計算すると, つぎのようになる.

$$C_{n_s}^{K,L} \triangleq (\langle X_0^K X_{n_s}^L \rangle - \langle X_0^K \rangle \langle X_{n_s}^L \rangle) / (K! L!) = \sum_{K=k_1+\dots+k_{n'}} \sum_{L=l_1+\dots+l_{n'}} \frac{w_1^{k_1} w_2^{k_2} \dots w_{n'}^{k_{n'}} w_1^{l_1} w_2^{l_2} \dots w_{n'}^{l_{n'}}}{k_1! \dots k_{n'}! l_1! \dots l_{n'}!} \times \{ \langle a_1^{k_1} a_2^{k_2} \dots a_{n'}^{k_{n'}} a_{n_s+1}^{l_1} a_{n_s+2}^{l_2} \dots a_{n_s+n'}^{l_{n'}} \rangle - \langle a_1^{k_1} a_2^{k_2} \dots a_{n'}^{k_{n'}} \rangle \langle a_{n_s+1}^{l_1} a_{n_s+2}^{l_2} \dots a_{n_s+n'}^{l_{n'}} \rangle \} \quad (13)$$

これから, $n_s < n'$ ならば, 任意の自然数 K, L において $C_{n_s}^{K,L} \neq 0$ となることが直ちにわかる. 一方, もし $n_s \geq n'$ であつ $n_s + n' \leq n$ ならば, (11) 式より (13) 式の $\{ \}$ 内は 0 ゼロとなる. すなわち, すべての K, L において $C_{n_s}^{K,L} = 0$ となり, (7) 式より X_0 と X_{n_s} は統計的に独立となる. ところが一般に, n' は (12) 式の $x(t)$ を所望の密度関数にするために条件 $n' \leq n$ のもとで大きいほうが良い. また, n_s は高速の不規則信号を得るために条件 $n_s \geq n'$ のもとで小さいほうが望ましい. したがって, 実際には Fig. 1 のように $n' = n_s = n$ とする場合が多い. このとき, $X_0, X_{n_s}, X_{2n_s}, \dots$ の周期は, n と N が互いに素の場合に限り M 系列の周期 N に一致する. そこで, これらの条件のもとで得られる不規則信号 X_0 と X_n の独立性について議論する.

4.1 荷重要素が同じ場合

4.1.1 高次相関

最初にすべての荷重が 1 のとき, すなわち, (12) 式の $x(t)$ が 2 項分布になる場合を考える. このとき,

a_k は 0 or 1 なので $\langle X_0^K \rangle$ は次式のようになる.

$$\begin{aligned} \langle X_0^K \rangle &= K! \left\{ \gamma_1^K \sum_{i_1=1}^n \langle a_{i_1} \rangle + \gamma_2^K \sum_{i_1=1}^n \sum_{i_2=i_1+1}^n \langle a_{i_1} a_{i_2} \rangle + \dots \right. \\ &\quad \left. + \gamma_K^K \sum_{i_1=1}^n \sum_{i_2=i_1+1}^n \dots \sum_{i_K=i_{K-1}+1}^n \langle a_{i_1} a_{i_2} \dots a_{i_K} \rangle \right\} \end{aligned} \quad (14)$$

ここで, γ_k^K はつぎのような値をもつ定数である.

$$\left. \begin{aligned} \gamma_1^1 &= 1 \\ \gamma_1^2 &= 1/2!, \quad \gamma_2^2 = 1 \\ \gamma_1^3 &= 1/3!, \quad \gamma_2^3 = 2/2!, \quad \gamma_3^3 = 1 \\ \gamma_1^4 &= 1/4!, \quad \gamma_2^4 = 2/3! + 1/2!2!, \quad \gamma_3^4 = 3/2!, \quad \gamma_4^4 = 1 \end{aligned} \right\} \quad (15)$$

(14) 式を用いれば (13) 式の $C_{n_s}^{K,L}$ は

$$\begin{aligned} C_{n_s}^{K,L} &= \sum_{k=1}^K \sum_{l=1}^L \gamma_k^K \gamma_l^L \left[\sum_{i_1=1}^n \dots \sum_{i_k=i_{k-1}+1}^n \sum_{j_1=1}^n \dots \sum_{j_l=j_{l-1}+1}^n \right. \\ &\quad \times \{ \langle a_{i_1} a_{i_2} \dots a_{i_k} b_{j_1} b_{j_2} \dots b_{j_l} \rangle \\ &\quad \left. - \langle a_{i_1} a_{i_2} \dots a_{i_k} \rangle \langle b_{j_1} b_{j_2} \dots b_{j_l} \rangle \right] \end{aligned} \quad (16)$$

Table 1 Statistical dependency d and number of linearly dependent combination $N_{t^{k,l}}(N_{m^{k,l}})$ for coefficients of $g(D)$ of $n=7$

coefficient of $g(D)$		d	$N_{t^{k,l}}(N_{m^{k,l}})$				
			$k+l=3$		$k+l=4$		
			$\begin{pmatrix} k,l \\ 1,2 \end{pmatrix}$	$\begin{pmatrix} k,l \\ 2,1 \end{pmatrix}$	$\begin{pmatrix} k,l \\ 1,3 \end{pmatrix}$	$\begin{pmatrix} k,l \\ 2,2 \end{pmatrix}$	$\begin{pmatrix} k,l \\ 3,1 \end{pmatrix}$
α^1	10001001	0.00861	4(4)	3(3)	23(20)	43(42)	18(15)
α^2	10001111	0.00910	0	0	0	5(0)	5(0)
α^3	10011101	0.00515	0	4(4)	0	28(24)	20(20)
α^4	11110111	0.00866	0	0	4(0)	4(0)	3(0)
α^5	10111111	0.00468	1(1)	0	6(5)	11(6)	5(0)
α^6	11010101	0.00855	0	0	0	4(0)	5(0)
α^7	10000011	0.01430	6(6)	1(1)	31(30)	47(42)	6(5)
α^8	11001011	0.00451	0	0	3(0)	2(0)	0
α^9	11100101	0.00521	0	0	0	3(0)	2(0)

となる。ここで、 $b_j = a_{n+j}$ である。したがって、(16) 式の [] の計算は、単位行列 I から k 個、行列 S^n から l 個の行ベクトルを取って得られる $(k+l, n)$ 行列の階数を調べて、線形従属の組合せ数 $N_{t^{k,l}}$ を求めることに相当する。いま、 $N_{t^{k,l}}$ の中で、(16) 式の { } が { $0 - (1/2)^{k+l}$ } となる個数を $N_{m^{k,l}}$ とし、 $\{(1/2)^{k+l-1} - (1/2)^{k+l}\}$ になる個数を $(N_{t^{k,l}} - N_{m^{k,l}})$ とすれば、(16) 式は

$$C_n^{K,L} = \sum_{k=1}^K \sum_{l=1}^L \gamma_k^K \gamma_l^L \left[\frac{N_{t^{k,l}} - 2N_{m^{k,l}}}{2^{k+l}} \right] \quad (17)$$

となる。これから、 $k \leq K$, $l \leq L$ なるすべての k, l において、 $N_{t^{k,l}} = 0$ 、または $N_{t^{k,l}} = 2N_{m^{k,l}}$ ならば、 $C_n^{K,L} = 0$ となることがわかる。また、行列の性質より一般的につぎのことがいえる。

(1) $N > 2n$ ならば、 I と S^n は同一行ベクトルを含まないので、 $N_{t^{1,1}} = 0$ となり、普通の意味の相関はない。

(2) 線形従属な k 個のベクトルに別な k' 個のベクトルを加えた行列の階数は $k+k'$ 未満なので、 k, l の増加と共に $N_{t^{k,l}}$ は増える傾向にある。

(3) n 要素の行ベクトルからなる行列の階数はたかだか n なので、 $k+l > n$ のとき $N_{t^{k,l}} \neq 0$ である。すなわち、 n 段シフトレジスタからなる M 系列による X_0 と X_n は、必ず $(n+1)$ 次以上の相関をもつので、統計的に独立な信号になりえない。

さらに、 $g(D)$ の係数 α に関連してつぎのことがいえる。 α_0, α_n 以外に α_p のみが1となる3項の $g(D)$ による M 系列では、行列 S^n の第1行目が $(\alpha_0, \alpha_1, \dots, \alpha_p,$

Table 2 Coefficients of $g(D)$ which bring maximum and minimum values of statistical dependency for n

n	$\phi(N)/2n$	dependency d	coefficients $\alpha (= \alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n)$
8	8	$d_{\min} = 0.001588$	111100111
		$d_{\max} = 0.004143$	101011111
9	24	$d_{\min} = 0.000966$	1111101001
		$d_{\max} = 0.008080$	1011011011
10	30	$d_{\min} = 0.000324$	10100011001
		$d_{\max} = 0.007601$	10000001001
11	88	$d_{\min} = 0.000226$	101110111101
		$d_{\max} = 0.008861$	100000000101

$\dots, \alpha_{n-1}$) であるから $b_1 = a_1 \oplus a_p$ となり、 $K=2$, $L=1$ ですでに相関をもつ。一方、多くの項からなる $g(D)$ でも低次で相関をもつ場合があり、逆は真でない。

Table 1 は、 $n=7$ において M 系列を発生する各 α に対する $N_{t^{k,l}}$ を行列 I と S^n から具体的に求めたものである (() 内は $N_{m^{k,l}}$ を示す)。これから、 α^1 と α^7 は3項よりなる $g(D)$ なので $k+l=3$ 次から相関をもち、一方 α^8 の $N_{t^{k,l}}$ は比較的小さいことがわかる。

4.1.2 統計的従属度の実験結果と考察

荷重要素がすべて1の場合でも、 $g(D)$ によって X_0 と X_n の高次相関が違うので、その統計的従属度 d も (7) 式により当然異なる。**Table 1** の d は、計算機上で発生した $x(t)$ の分布関数から (2) 式によって計算したものである。最小の d は α^8 において得られ、これが d を小さくする $g(D)$ の係数ベクトルである。 α^7 の d は最大値を示しているが、このことは3次ですでに相関があるのでかなり予想できる。 $\phi(N)$ を Euler の関数とすれば、本質的に異なる M 系列を発生する $g(D)$ の個数は $\phi(N)/2n$ である。その中で d の最小値 $d_{\min}$ と最大値 $d_{\max}$ をもたらす α は、 $n=8, 9, 10, 11$ の場合 **Table 2** のようになった。3項からなる $g(D)$ は、 $n=10, 11$ の場合 $d_{\max}$ を生じさせ、 $n=9$ の場合23番目に大きな値をもった。なお、 $n=8$ の場合の $g(D)$ は5項以上で占められ、 $d_{\max}$ は比較的小さい。いずれにしても $d_{\max}$ を生じさせる α は、3次から相関をもつものばかりである。一方、 $d_{\min}$ を生じさせる α は比較的高次まで相関をもたない。したがって、(7) 式の d は $C^{k,l}$ の複雑な関数になっているが、小さな d 、すなわち独立に近い不規則信号は、高次まで相関のない $g(D)$ のもとで得られる傾向にあるといえる。

Table 3 $w_{\text{bad}}, w_{\text{normal}}, w_{\text{improved}}, w_{\text{good}}$ for coefficient vector $\alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8$

Coefficient vector	structure of linearly dependent combination	weight vector							d	
			w_1	w_2	w_3	w_4	w_5	w_6		w_7
α^1	$a_4 \quad b_1 \quad b_4$ $a_5 \quad b_2 \quad b_5$ $a_6 \quad b_3 \quad b_6$ $a_7 \quad b_4 \quad b_7$ $a_1 \quad a_5 \quad b_1$ $a_2 \quad a_6 \quad b_2$ $a_3 \quad a_7 \quad b_3$	w_{bad}	32	4	1	64	16	2	8	38.320
		w_{normal}	1	2	4	8	16	32	64	2.114
		w_{improved}	8	4	2	1	16	32	64	0.364
		w_{good}	32	16	8	1	2	4	64	0.338
α^5	$a_1 \quad b_4 \quad b_7$	w_{bad}	4	1	2	16	64	32	8	10.948
		w_{normal}	1	2	4	8	16	32	64	2.378
		w_{improved}	1	8	16	2	32	64	4	1.078
		w_{good}	16	8	1	4	32	2	64	0.381
α^6	$a_1 \quad a_4 \quad b_3 \quad b_4$ $a_2 \quad a_5 \quad b_4 \quad b_5$ $a_3 \quad a_6 \quad b_5 \quad b_6$ $a_4 \quad a_7 \quad b_6 \quad b_7$ $a_1 \quad a_2 \quad a_3 \quad b_3$ $a_2 \quad a_3 \quad a_4 \quad b_4$ $a_3 \quad a_4 \quad a_5 \quad b_5$ $a_4 \quad a_5 \quad a_6 \quad b_6$ $a_5 \quad a_6 \quad a_7 \quad b_7$	w_{bad}	16	32	64	8	2	1	4	8.535
		w_{normal}	1	2	4	8	16	32	64	8.400
		w_{improved}	64	32	4	1	2	8	16	0.451
		w_{good}	64	4	2	32	16	1	8	0.410
α^7	$a_2 \quad b_1 \quad b_2$ $a_3 \quad b_2 \quad b_3$ $a_4 \quad b_3 \quad b_4$ $a_5 \quad b_4 \quad b_5$ $a_6 \quad b_5 \quad b_6$ $a_7 \quad b_6 \quad b_7$ $a_1 \quad a_7 \quad b_1$	w_{bad}	32	64	8	1	2	4	16	38.276
		w_{normal}	1	2	4	8	16	32	64	30.797
		w_{improved}	8	4	16	2	32	1	64	0.333
		w_{good}	8	4	16	2	32	1	64	0.333
α^8	$a_1 \quad b_3 \quad b_5 \quad b_7$ $a_3 \quad b_1 \quad b_3 \quad b_5$ $a_4 \quad b_2 \quad b_4 \quad b_7$ $a_1 \quad a_6 \quad b_1 \quad b_4$ $a_2 \quad a_7 \quad b_2 \quad b_5$	w_{bad}	2	32	1	64	8	4	16	8.207
		w_{normal}	1	2	4	8	16	32	64	0.565
		w_{improved}	1	2	4	8	32	64	16	0.563
		w_{good}	8	4	1	16	64	2	32	0.418

4.2 荷重要素が異なる場合

所望の分布をもつ不規則信号を得るためには、異なる荷重要素からなる荷重ベクトルが用いられる。ここでは、一様分布を発生させる荷重ベクトルを例にとり、 d を小さくする荷重要素の配列方法について述べる。荷重要素の集合を $W = \{2^{i-1}, i=1, 2, \dots, n\}$ とすれば、(12)式の $x(t)$ は、要素の配列順序に関係なく M 系列の周期内で離散的な一様分布になる。しかし、 X_0 と X_n の d は(7), (13)式からわかるように荷重配列によって当然異なる。 $n!$ 通りある荷重ベクトルの中で(2)式の d を最小にする荷重ベクトルを w_{good} 、最大にするものを w_{bad} とすると、それらは $n=7$ の $\alpha^1, \alpha^5, \alpha^6, \alpha^7, \alpha^8$ において Table 3 のようになった。各 α における w_{bad} の d を比較すると、 α^8 が一番小さく、 $\alpha^6, \alpha^5, \alpha^7, \alpha^1$ の順に大きくなっている。このことと Table 1の結果より、 w_{bad} の d は、高次まで相関のない $g(D)$ を使用すれば、比較的小さくすることが

わかる。

ところで、ここで知りたい w_{good} の発見は、限なく調べる方法によると n の増加と共に困難となる。そこで、 d を比較的小さくする荷重ベクトル w_{improved} の簡便な求め方について述べる。一般に、 $n'=n_s=n$ とした(13)式の低次相関が小さいとき、 d は小さくなる傾向にある。よって、 I と S^n の線形従属構造に応じて得られるつぎの手続きが有効と考えられる。

(i) 線形従属の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 2^{n-1} 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。

Table 3に示すように、 α^5 の3次における線形従属の組合せは $a_1b_4b_7$ である ($\langle a_1b_4b_7 \rangle$ キ $\langle a_1 \rangle \langle b_4 \rangle \langle b_7 \rangle$)。そこで、 α^5 の w_{improved} は、手続き(i)よりレジスタ A_1, A_4, A_7 に小さな荷重が配置されたものになる。この w_{improved} による d は1.078で、 w_{good} における0.381に及ばないが、通常用いられる荷重ベクトル w_{normal} における2.378に比べて小さい。 α^6, α^8 の場合、すべての i の A_i が線形従属に関係しているので、手続き(ii)より w_{improved} を決めた。 α^1, α^7 の場合、線形従属に関係する回数はすべて3回

であるので、手続き(iii)によって w_{improved} を決める必要がある。すなわち、 α^1 の場合には $w_i w_{j+1}^2 (j=i+2 \bmod 7)$ を小さくするように、 $A_7 (j=6)$ に最大荷重64 ($=w_{j+1}$)を配置すれば $A_4 (i=4)$ に最小荷重1 ($=w_i$)を配置し、さらに $w_6=32$ ならば $w_3=2$ のようにすればよい。 α^7 の w_{improved} は、 $w_i w_{j+1}^2 (j=i \bmod 7)$ が小さくなるようにすれば、偶然 w_{good} に一致した。

以上、5個の $g(D)$ のもとで得られた w_{improved} の d は w_{normal} のそれに比べて小さくなり、上で述べた三つの手続きの効果が確められた。特に、3項からなる $g(D)$ における w_{improved} は、比較的求めやすく、かつ、その効果が顕著に表われた。

この章では X_0 と X_n 間の d を小さくする α や荷重配列について述べたが、任意の j の X_{jn} と $X_{(j+1)n}$ でも同じことになる。したがって、(6)式からわかるように $m=2$ におけるこれらの結果は、 $3 \leq m \ll N/m$ において d を小さくするための重要な必要条件であると

いえる。なお、簡単ではないが行列 $I, S^n, S^{2n}, \dots, S^{(m-1)n}$ の線形従属構造に注目して荷重配列を決めれば、いっそう d は小さくなる。

5. 統計的従属性 d の評価

統計的従属性の測度として、(2)式で定義した d 以外に、エントロピー⁹⁾や(1)式の f_e の2乗積分 d' などが考えられる。しかし、これらは密度関数に基づいているので、現実に応用できない場合が多い。たとえば、 d' は、(3)式における被積分関数の分母 u_i がない式となるので、大きな u における Φ_e の影響を強く受ける。したがって、4.2 で述べた離散的な一様分布における d' は

$$d' = (2^n - 1)/2^{2n} \quad (18)$$

となり、 n に依存するのみである。すなわち、いかなる α や荷重配列でも、また、完全相関の場合でもすべて同一になる。これに対して、分布関数をもとにして定義された d は、荷重配列などに強く依存し、完全相関のとき最大の値 $N^2/90$ となり、統計的従属性の測度になりうる。このことを確認するためにつぎの実験を行った。[0, 1] に属する二つの一様乱数 X_1, X_2 を比較し、大きいほうを Y とすれば、確率変数 Y の分布関数 $F(y)$ は、 X_1 と X_2 が独立なときベキ分布 y^2 ($0 \leq y \leq 1$) となることが知られている。そこで、4.2 で述べた一様乱数 X_0 と X_n を [0, 1] に規格化し、それらによる d とベキ分布⁵⁾の誤差 $\varepsilon = \int_0^1 (F(y) - y^2)^2$

Fig. 2 Error ε of 2-th power distribution vs. statistical dependency d Plotted with log-log scales

dy との関係調べると、Fig. 2 のようになった。これは、 ε が全領域で d に比例していないが、 d の単調増加関数とみなされる。すなわち、 d が小さいほど $F(y)$ は y^2 に近づくので、 d は統計的従属性を示す測度に適している。

6. おわりに

統計的独立性の逆概念である統計的従属性を分布関数に基づいて定義し、それが現実の不規則信号間の従属性の測度になりうることを確かめた。この測度を用いて、 M 系列を荷重加算して得られる不規則信号の周期内における従属性を調べた。その結果、従属性を低くする M 系列が存在し、それは、線形従属の組合せ数の少ない特性多項式で得られる傾向があった。さらに、荷重要素が異なる場合、従属性が荷重要素の配列によっても異なることを示した。そして、線形従属の組合せ数の多い3項からなる特性多項式でも、その線形従属構造に応じて荷重を配列すれば、統計的従属性の小さい不規則信号が得られることを述べた。

最後に、有益なご助言を賜った熊本大学 柏木潤教授に深く感謝します。

参考文献

- 1) A. C. Davies: Properties of Waveforms Obtained by Nonrecursive Digital Filtering of Pseudorandom Binary Sequences, IEEE Trans. on Computers, C-20-3, 270/281 (1971)
- 2) 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)
- 3) T. J. Healy: Forms of Probability-Density Functions Obtainable from Summed m -Sequences, Electronics Letters, 5-24, 624/625 (1969)
- 4) 柏木, 坂田: m 系列を用いる擬似正規信号の発生, 計測自動制御学会論文集, 12-3, 293/299 (1976)
- 5) 泉: M 系列によるベキ分布の不規則信号発生器, 第16回 SICE 学術講演会予稿集, 653/654 (1977)
- 6) 佐藤, 井戸川: m 系列の二, 三の性質とその応用, 計測自動制御学会論文集, 2-2, 121/131 (1966)
- 7) H. A. Barker and T. Pradisthayon: High-Order Autocorrelation Functions of Pseudorandom Signals Based on m -Sequences, Proc. IEE, 117-9, 1857/1863 (1970)
- 8) W. W. Peterson: Error-Correcting Codes, MIT Press (1961)
- 9) 河原田: 高速二進乱数の発生とその特性評価, 計測自動制御学会論文集, 3-2, 129/134 (1967)
- 10) 柏木, 坂田, 三平: 反対称 m 系列を用いる擬似正規信号の発生, 計測自動制御学会論文集, 13-6, 575/579 (1977)