数理解析研究所講究録
第259巻 1976年 14-24

14

nタプルM系列の諸性質

日本電気(株) 中央研究所　中村勝洋

[1] まえがき

一様な擬似乱数列としての性質を有し，種々の工学的応用を持つM系列(Maximum-length linear shift register sequence)自体の諸性質については，すでに多くの文献(1)～(6)に詳しく記されている。このM系列(一般にp元M系列とする)から，さらに多元(多値)の一様乱数列や，他の分布を持つ乱数列などを求めたい場合，普通、次の様な方法が考えられる。つまり、一つのM系列を相続くn個ディジット毎に区切ってできるn次元ベクトルの系列や，数学的な拡張として得られるp^n元M系列，あるいはまた，互いにシフトした関係にあるn個のM系列を適当に結合(n次結合)させてできる系列などを利用する方法である。

しかしながら，p^n元M系列を除いては，これらの系列に関する解析は、あまり十分にはなされておらず，その一般的な性質や，これらの系列間の関係については，あまりよく知ら

れていないように思われる。

本稿は，これらの系列を統一的に取扱うために，まず'n-タプルM系列'なるものを定義し，その自己相関性を中心とした一般的な諸性質について論ずることを目的とする。n-タプルM系列（n-tuple M sequences）とは，要するに，互いにシフトした関係にあるn個のM系列を並置して得られるn次元ベクトル（n-タプル）の系列のことで，上記各系列はすべてこのn-タプルM系列の中に包摂されてしまう。

本稿によって得られた一般的な諸結果により，M系列をもとにして得られる種々の乱数列の構造が明らかになったと考えられる。

[2] nタプルM系列と，M系列のn次結合系列

まず いくつかの記号，語句を定義しておこう。

(1) p^n元M系列 $a=\{a_i\}$ ； 有限体$GF(p^n)$（pは素数）の上のM系列の事。即ち，$a_i \in GF(p^n)$であって，$h(x)=\sum_{j=0}^{m} h_j x^j$を$GF(p^n)$上のある$m$次の原始多項式としたとき，$GF(p^n)$上の関係式 $\sum_{j=0}^{m} h_j a_{i-j}=0$ を満す系列$\{a_i\}$のことである。なお$h(x)$はM系列aの特性多項式と呼ばれる。

(例1) $p^n=2$，$h(x)=1+x+x^4$，初期ビット$a_0=a_1=a_2=a_3=1$とすれば，次の様な一周期15ビットの2元M系列a

が得られる。　$a = \cdots 1111010110010000 \cdots$

(2) <u>シフトした系列 $_sa = \{_sa_i\}$</u> ; a を s ディジット時間軸方向へシフトして得られる系列。即ち $_sa = \{_sa_i\} = \{a_{i-s}\}$。ただし，$_{-\infty}a$ は，すべて0の系列と定義する。

(3) <u>n タプル p 元M系列 $A = \{A_i\}$</u> ; p 元M系列 a をそれぞれ，$s_0, s_1, \cdots, s_{n-1}$ ディジット（但し $s_i = -\infty$ も許す）シフトした n 個の p 元M系列 $_{s_0}a, _{s_1}a, \cdots, _{s_{n-1}}a$ を，並置して得られる $GF(p)$ 上の n 次元ベクトル（n-タプル）の系列 $A = (_{s_0}a, _{s_1}a, \cdots, _{s_{n-1}}a)^t = \{(_{s_0}a_i, _{s_1}a_i, \cdots, _{s_{n-1}}a_i)^t\} = \{A_i\}$ のことである。但し，t は転置を表わす。なお，各元 A_i は $GF(p^n)$ の元とみなせることに注意。

（例2）　M系列 a を（例1）で与えた系列としたとき，3-タプル2元M系列 $A = (_0a, _{-\infty}a, _3a)^t$ は，次の様に与えられる。

$$A = \begin{pmatrix} {}_0a \\ {}_{-\infty}a \\ {}_3a \end{pmatrix} = \cdots \begin{pmatrix}1\\0\\0\end{pmatrix}\begin{pmatrix}1\\0\\0\end{pmatrix}\begin{pmatrix}1\\0\\0\end{pmatrix}\begin{pmatrix}1\\0\\1\end{pmatrix}\begin{pmatrix}0\\0\\1\end{pmatrix}\begin{pmatrix}1\\0\\1\end{pmatrix}\begin{pmatrix}0\\0\\1\end{pmatrix}\cdots\begin{pmatrix}0\\0\\0\end{pmatrix}\begin{pmatrix}0\\0\\1\end{pmatrix}\cdots\cdots\cdots$$

補題1[7]　p 元M系列 a をもとにして構成される n-タプルM系列 A の全集合は，a の特性多項式を $h(x)$（m 次）とすれば，$h(x)$ をチェック多項式とする，拡大体 $GF(p^n)$ 上の巡回符号である。それ故，A の一周期分を多項式 $A(x) = \sum_{i=0}^{N-1} A_i x^i$　（$N = p^m - 1$ は，A の一周期分のディジット数）で表わせば，

$h(x)A(x)=0 \pmod{x^N-1}$ が成立する。

なお，$GF(p^n)$ 上の原始多項式は，$GF(p)$ 上の原始多項式の因数として求められることから，p^n 元M系列は，n タプル p 元M系列の特別な場合であることが，この補題1より分る。これについては，またあとで述べる。

次に、n-タプルM系列の自己相関などの性質を調べるための準備として，シンボル列としてのM系列，あるいは n-タプルM系列を数値列に変換して考える。

(4) p 元M系列 $a=\{a_i\}$ の数値列 $Z(a)=\{Z(a_i)\}$ ； Z を，$GF(p)$ より複素単位円周上への写像，即ち $Z(a_i)=e^{j2\pi a_i/p}$ として得られる数値列。但し，$a_i \in \{0,1,\cdots,(p-1)\}$

(5) n タプル p 元M系列 $A=\{A_i\}$ の数値列 $\eta(A)=\{\eta(A_i)\}$ ；$GF(p^n)$ より複素数体へのある任意の写像 η によって定まる数値列。上の Z は η の特別な場合である。

(6) n 次元ディスクリート・フーリエ変換対 η, W ；

$\eta=[\eta_0,\eta_1,\cdots,\eta_{p^n-1}]^t$, $W=[W_0,W_1,\cdots,W_{p^n-1}]^t$ （但し，$v_i \in \{0,1,\cdots,(p-1)\}$, $\sum_{i=0}^{n-1} v_i p^i = k$ として，$\eta_k=\eta((v_0,v_1,\cdots,v_{n-1})^t)$ とする。W_k についても同様。）とすれば，次式が成立する。

$$\eta=F_n\cdot W \quad , \quad W=p^{-n}F_n^*\eta \qquad (1)$$

但し，F_n^* は，F_n の複素共役な行列を意味し，F_n は，$p^n\times p^n$ の正方行列で，次の漸化式によって定義される。

$$F_0 = 1$$

$$\alpha = e^{j2\pi/p} \quad ; \quad F_n = \begin{bmatrix} F_{n-1} & F_{n-1} & F_{n-1} & \cdots\cdots & F_{n-1} \\ F_{n-1} & \alpha F_{n-1} & \alpha^2 F_{n-1} & \cdots\cdots & \alpha^{p-1} F_{n-1} \\ F_{n-1} & \alpha^2 F_{n-1} & \alpha^4 F_{n-1} & \cdots\cdots & \alpha^{2(p-1)} F_{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ F_{n-1} & \alpha^{p-1} F_{n-1} & \alpha^{2(p-1)} F_{n-1} & & \alpha^{(p-1)(p-1)} F_{n-1} \end{bmatrix} \qquad (2)$$

なお，特に $p=2$ の場合には，(2)式の F_n は，いわゆるクロネッカ積型のアダマール行列となっていることに注意。

また(1)式より次の補題が容易に導ける。

補題2 n タプル2元M系列 A の数値列 $\eta(A)$ は，2元M系列 a（の数値列 $z(a)$）の n 次結合系列として，次の様に表現できる。

$$\eta(A) = W_0 + W_1 z(s_0 a) + W_2 z(s_1 a) + W_3 z(s_0 a) z(s_1 a) + \cdots\cdots + W_{2^n-1} z(s_0 a) z(s_1 a) \cdots z(s_{n-1} a) \qquad (3)$$

但し，$W = [W_0, W_1, \cdots, W_{2^n-1}]^t$ は，$\eta = [\eta_0, \eta_1, \cdots \eta_{2^n-1}]^t$ の n 次元アダマール変換対である。

(例3) 2タプル2元M系列 $(s_0 a, s_1 a)^t$ を考える。写像 η として，

$$\begin{bmatrix} W_0 \\ W_1 \\ W_2 \\ W_3 \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} -3 \\ -1 \\ 3 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -2 \\ -1 \end{bmatrix}$$

て，$\eta_0 = \eta((0,0)^t) = -3$，$\eta_1 = \eta((1,0)^t) = -1$，$\eta_2 = \eta((0,1)^t) = 3$，$\eta_3 = \eta((1,1)^t) = 1$

とすれば，$W = [W_0, W_1, W_2, W_3]^t$ は，左上の計算式で与えられる。

よって，$\eta((s_0 a, s_1 a)^t) = 0 + 0 \cdot z(s_0 a) - 2 z(s_1 a) - 1 \cdot z(s_0 a) z(s_1 a) = -2 z(s_1 a) - z(s_0 a) z(s_1 a)$

なお，**補題2**は，M系列自体の性質を全く使っていないので，任意の n タプル2元系列に対して成立することに注意。

[3] n-タプルM系列の諸性質

性質1 n-タプルP元M系列 $A=(s_0a, s_1a, \cdots, s_{n-1}a)^t$ において，$s_0a, s_1a, \cdots, s_{n-1}a$ が互いに線型独立であれば，一周期分の $A=\{(s_0a_i, s_1a_i, \cdots, s_{n-1}a_i)\}_{i=0}^{N-1}$ （但し，$N=p^m-1$ ；m はM系列 a の特性多項式の次数）に含まれる $0=(0,0,\cdots,0)$ の個数は $p^{m-n}-1$ 個，0 でないnタプルの個数は，それぞれ p^{m-n} 個ずつである。

この性質からn-タプルM系列の一様性がわかる。さらに拡張して次の性質も導ける。

性質2 n タプルP元M系列 $A=\{A_i\}=(s_0a, s_1a, \cdots, s_{n-1}a)^t$ において，nl 個の系列 $\{s_{i-j}a\}$ $(i=0,1,\cdots,n-1\ ;\ j=0,1,\cdots,(l-1))$ が互いに線型独立であれば，相続く l 個のnタプル $(A_i, A_{i+1}, \cdots, A_{i+l-1})$ のパターンが，$(0,0,\cdots 0)$ となる頻度は，一周期内おいて，$p^{m-nl}-1$ であり，それ以外の各パターンとなる頻度は，p^{m-nl} である。

次にn-タプルM系列の自己相関に関する性質を導く。

(1) 定義： P元M系列 $a=\{a_i\}$ とnタプルM系列 $A=\{A_i\}$ の各自己相関関数 $\varphi_z(\tau)$, $\varphi_\eta(\tau)$ は，前節の写像 z, η を用いて，

$$\varphi_z(\tau)=\sum_{i=0}^{N-1} z(a_i)z^*(a_{i-\tau}) \Big/ N \qquad (4)$$

$$\varphi_\eta(\tau)=\sum_{i=0}^{N-1} \eta(A_i)\cdot\eta^*(A_{i-\tau}) \Big/ \left\{\sum_{i=0}^{N-1}(|\eta(A_i)|)^2\right\} \qquad (5)$$

と定義される。但し，N は a あるいは A の一周期の長さを，

＊は共役複素数を意味する。

(ロ) M系列に関する性質 ： 上記 $\varphi_\eta(\tau)$ の一般式を導く過程で用いるM系列の性質を補題として掲げる。

補題3 n 個のp元M系列 $s_0a, s_1a, \cdots, s_{n-1}a$ のGF(p)上の線型結合系列 $\sum_{j=0}^{n-1} u_j s_j a = \left\{\sum_{j=0}^{n-1} u_j s_j a_i\right\}$ $(u_j \in GF(p))$ は，a の特性多項式を $h(x)$ とし，$\sum_{j=0}^{n-1} u_j x^{\Delta_j} = x^t \pmod{h(x)}$ (6)

とすれば，p元M系列 ta に等しい。但し，(6)式$=0$のときは，$t=-\infty$ とする。

なお，(6)式を満すtを以後 $t(u_\ell, a)$ と記す。但し，$u_\ell = (u_0, u_1, \cdots u_{n-1})$ で，$\sum_{j=0}^{n-1} u_j p^j = \ell$ ，$\Delta = (s_0, s_1, \cdots, s_{n-1})$。

補題4[2]

$$\varphi_z(\tau) = \begin{cases} 1 & (\tau = 0 \pmod N) \\ -1/N & (\tau \neq 0 \pmod N) \end{cases} \quad (7)$$

また，任意のτに対し，

$$\sum_{i=0}^{N-1} z(-\infty a_i) z^*(-\infty a_{i+\tau})/N = 1 \quad (8)$$

$$\sum_{i=0}^{N-1} z(-\infty a_i) z^*(a_{i+\tau})/N = \sum_{i=0}^{N-1} z(a_i) z^*(-\infty a_{i+\tau})/N = -1/N \quad (9)$$

(ハ) $\varphi_\eta(\tau)$ の一般式の導出 ： 補題2より，次式が成立つ。

$$\eta(A_i) = \sum_{u_0=0}^{p-1}\sum_{u_1=0}^{p-1}\cdots\sum_{u_{n-1}=0}^{p-1} \left\{z(s_0 a_i)\right\}^{u_0}\left\{z(s_1 a_i)\right\}^{u_1}\cdots\left\{z(s_{n-1} a_i)\right\}^{u_{n-1}} W(u_0, u_1, \cdots u_{n-1})$$

$$= \sum_{u_0=0}^{p-1}\sum_{u_1=0}^{p-1}\cdots\sum_{u_{n-1}=0}^{p-1} z\left\{\sum_{j=0}^{n-1} u_j \cdot s_j a_i\right\} W(u_0, u_1, \cdots u_{n-1}) \quad (10)$$

但し，$\sum$ は，mod pでの，従ってGF(p)上での総和を意味する。従って，補題3より $\eta(A_i) = \sum_{\ell=0}^{p^n-1} z(t(u_\ell, \Delta) a_i) W_\ell$ (11)

これを定義式(5)へ代入し，補題4と，関係式 $\sum_{\ell=0}^{p^n-1} W_\ell = \eta_0$ を用いて更に変形すれば，$\varphi_\eta(\tau)$ の一般式が次の通り導ける。

性質3[7] (自己相関) p を素数とする。n タプル P 元 M 系列 $(s_0a, s_1a, \cdots, s_{n-1}a)^t$ の自己相関関数 $\varphi_\eta(\tau)$ ((5)式) は，次の様に表せる。

$$\varphi_\eta(\tau) = \left[(N+1)\left\{\sum_{(l_i,l_j)\in L_\tau}\sum_{l_i}\sum_{l_j} W_{l_i} W_{l_j}^* + C_\infty\right\} - (|\eta_0|)^2\right] \Big/ T \qquad (12)$$

但し，

$$T = (N+1)\left\{\sum_{(l_i,l_j)\in L_0}\sum_{l_i}\sum_{l_j} W_{l_i} W_{l_j}^* + C_\infty\right\} - (|\eta_0|)^2 \qquad (13)$$

また，L_τ および C_∞ は，次の様に定義されたものである。まず $W_l \neq 0$ を満す l のうち，$t(u_l, s) \neq -\infty$ を満すものを $l_1, l_2, \cdots, l_r$ とし，$t(u_l, s) = -\infty$ を満すものを $l_{r+1}, l_{r+2}, \cdots l_{r+w}$ とする。このとき

$$\begin{cases} L_\tau = \{(l_i, l_j)\ ;\ \tau = t(u_{l_i}, s) - t(u_{l_j}, s) \pmod N\} \quad (1 \leqq i, j \leqq r) \\ C_\infty = \sum_{i=r+1}^{r+w}\sum_{j=r+1}^{r+w} W_{l_i} W_{l_j}^* \end{cases} \qquad (14)$$

なお，一般式 $\sum_{l=0}^{p^n-1}(|W_l|)^2 = p^{-n}\sum_{l=0}^{p^n-1}(|\eta_l|)^2$ に着目すれば，次の補題が導ける。

補題5 n 個の M 系列 $\{s_j a\}_{j=0}^{n-1}$ が，互いに線型独立ならば，(13)式は，

$$T = p^{-n}(N+1)\sum_{l=0}^{p^n-1}(|\eta_l|)^2 - (|\eta_0|)^2 \qquad (15)$$

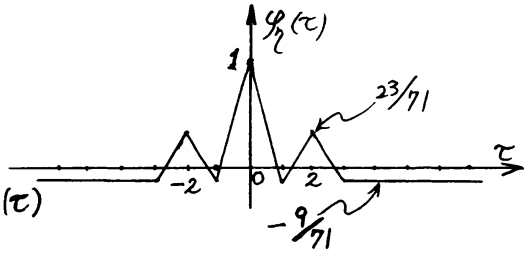
と表わすこともできる。また，このとき $C_\infty = (|W_0|)^2$ となる。

(例4) 2元 M 系列 a を (例 1) で与えた系列とし，2-タプル2元 M 系列 (a, ga) を考える。写像 η としては，(例3) で与えた η を選べば，W_2 と W_3 のみが非零である。$0\cdot x^0 + 1\cdot x^9 = x^9$，$1\cdot x^0 + 1\cdot x^9 = x^7 \pmod{h(x) = 1+x+x^4}$ であるので $t(u_2, s) = 9$，$t(u_3, s) = 7$. 従って，$L_{-2} = \{(3, 2)\}$，

$L_2=\{(2,3)\}$, $L_0=\{(2,2),(3,3)\}$

$C_\infty=0$ である。よって，

(12),(13)式より，自己相関関数 $\varphi_\eta(\tau)$ は，① $\tau=0 \pmod{15}$ のとき，$\varphi_\eta(\tau)=1$ ② $\tau=\pm 2 \pmod{15}$ のとき $\varphi_\eta(\tau)=\left[(15+1)\{(-2)(-1)+0\}-(-3)^2\right]/\left[(15+1)\{(-2)^2+(-1)^2\}-(-3)^2\right]=23/71$ ③ $\tau\neq 0,\pm 2 \pmod{15}$ のとき $\varphi_\eta(\tau)=-(-3)^2/71=-9/71$



次に，特殊な n-タプル M 系列について考察する。

性質4[7]（p^n元 M 系列） p^n元 M 系列 $b=\{b_i\}$ の特性多項式を $h_\beta(x)$，その次数を m，根を β とし，β の GF(p) 上の**最小多項式**を特性多項式とする p 元 M 系列を a とする。b の各元 b_i $(\in GF(p^n))$ を，GF(p) 上のある適当な n 次の既約多項式 $h_\gamma(x)=\sum_{i=0}^{n-1}h_i x^i$（$\gamma$ はその根）を法として，n 次元ベクトルで表わした系列は，n タプル M 系列 $(s_0a, s_1a, \cdots, s_{n-1}a)$ であり，s_j $(j=0,1,\cdots,n-1)$ の間には次の関係式が成立する。

$$s_j-s_0=\sum_{i=1}^{m}c_i\cdot(p^{nm}-1)/(p^n-1) \quad (j=1,2,\cdots(n-1)) \tag{16}$$

但し c_i は，次式によって一意に定まる数である。

$$\begin{cases} \delta=\beta^{-(p^{nm}-1)/(p^n-1)} & (17) \\ \delta^{c_{n-i}}=h_{n-i}\cdot\delta^{-\sum_{j=1}^{i-1}c_{n-j}}+\gamma \quad (i=1,2,\cdots,(n-1)) & (18) \end{cases}$$

（例 5）$h_\beta(x)=x^2+\gamma x+\gamma$ を特性多項式とする 8 元 M 系列を b とする（但し，γ は $h_\gamma(x)=x^3+x+1$ の根）。b および，b と等価な 3 タプル 2 元 M 系列を次に示す。（一周期 $N=(2^3)^2-1=63$）

b :	$0\gamma^6\gamma^6\gamma\gamma^6\gamma^2\gamma^3 \mid \gamma^6$	$0\gamma^5\gamma^5 \mid \gamma^5\gamma\gamma^2\gamma^6\gamma^5$	$0\gamma^4\gamma^4\gamma^6\gamma^4 \mid \gamma\gamma^5\gamma^4$ ------
3	0 1 1 0 1 0 1 1 1	0 1 1 1 1 0 0 1 1	0 0 0 1 0 1 0 1 0 ------
Mタプル系列:	0 0 0 1 0 0 1 0 0	0 1 1 0 1 1 0 0 1	0 1 1 0 1 0 1 1 1 ------
	0 1 1 0 1 1 0 0 1	0 1 1 0 1 0 1 1 1	0 1 1 1 1 0 0 1 1 ------

今の場合，$\delta=\beta^{-9}$，また $\delta^{c_2}=0+\gamma=\delta^6$ より $c_2=6$，$\delta^{c_1}=1\cdot\delta^{-6}+\delta^6=\delta^2$ より $c_1=2$。従って $s_0=0$ とすれば，$s_1=18$，$s_2\overset{(\mathrm{mod}\,63)}{=}9$ となり上の図と一致する。

性質5[7] n を N と互いに素な数として，$n\cdot n^{-1}=1\ (\mathrm{mod}\,N)$ とする。また周期 $N=p^m-1$ の p 元M系列 a の特性多項式を $h(x)$ とし，$h(\alpha)=0$ としたとき，α^n の $GF(p)$ 上の最小多項式を特性多項式とする p 元M系列を $a^{(n)}$ で表わす。この時，M系列 a を相続く n ディジット毎に区切ってできる n 次元ベクトルの系列は，n タプル p 元M系列 $(_0a^{(n)}_{,-n^{-1}}a^{(n)}_{,-2n^{-1}}a^{(n)},\cdots\cdots,{}_{-(n-1)n^{-1}}a^{(n)})^t$ と同じ系列である。

(例6) 例1で与えられたM系列 a を相続く2ビット毎に区切って得られる系列は，$-2^{-1}=7\ (\mathrm{mod}\,15)$ で，$a^{(2)}$ と a が互いにシフトした関係にあることから，2タプル2元M系列 $(_0a,{}_7a)^t$ と同じ系列であることが分る。これは左上図でも確められる。

a	1 1 1 1 0 1 0 1 1 0 0 1 0 0 0 -----
$\binom{{}_0a^{(2)}}{{}_7a^{(2)}}$	1 1 0 0 1 0 0 0 1 1 1 1 0 1 0 ------
	1 1 1 1 0 1 0 1 1 0 0 1 0 0 0 ------
b	1 1 0 0 0 0 0 0 1 0 0 1 0 0 0 ------

次に，この2ビット毎の論理積をとって得られる系列 b（左上図）の自己相関関数 $\varphi_\eta(\tau)$ を求める。まず $\eta_0=\eta_1=\eta_2=1$，

$\eta_3 = \eta((11)^t) = -1$ として，

Wは右の様に求められる。

$$\begin{bmatrix} W_0 \\ W_1 \\ W_2 \\ W_3 \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 1/2 \\ 1/2 \\ 1/2 \\ -1/2 \end{bmatrix}$$

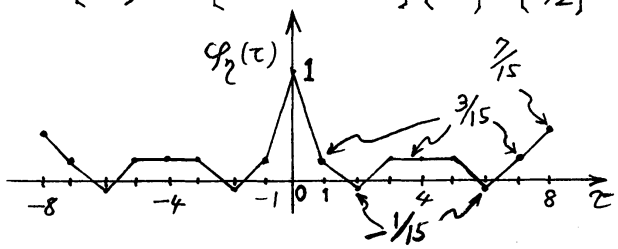
また，$t(u_0, \mathcal{A}) = -\infty$, $t(u_1, \mathcal{A}) = 0$,

$t(u_2, \mathcal{A}) = 7$, $t(u_3, \mathcal{A}) = 9$

$c_\infty = \left(\frac{1}{2}\right)^2 = 1/4$。これら

をもとにして (12), (13) 式より，

$\varphi_\eta(\tau)$ は，右図のように，求められる。



[4] むすび　M系列をもとにして構成される乱数列の中で，かなり一般的な系列と思われるnタプルM系列なるものを定義し，その自己相関性などを中心とした諸性質を明らかにした。本稿の諸結果をもとにして，その様な乱数列の解析・合成が，容易になったと考えられる。残った問題として，混合合同法などによる乱数列との長短の比較などがある。

おわりに，日頃御指導，御討論頂く関係各位に感謝する。

文献 (1) Golomb ;「Shift Register Sequences」Holden-Day 1967.

(2) N. Zierler, "Linear Recurring Sequences", SIAM. J. Vol. 7 Mar. 1959.

(3) W.W. Peterson et al. ;「Error Correcting Codes」2nd edition The MIT Press 1972.

(4) 佐藤，中村，"擬似ランダム系列 (4), (5)" bit 1975年2月号，3月号.

(5) Golomb et al. ;「Digital Communication with Space Application」Prentice-Hall 1964

(6) R.C. Tausworthe ;"Random Numbers Generated by Linear Recurrence Modulo Two" Math. Comp. 19, 1965.

(7) 中村，"nタプルM系列について" 電子通信学会オートマトンと言語研資 AL-72-29 1972年6月