

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 デイ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 $\alpha = \{a_i\}$; 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
$$\sum_{j=0}^m h_j a_{i-j} = 0$$
 を満たす系列 $\{a_i\}$ のことである。なお $h(x)$ は M 系列 α の 特性多項式 と呼ばれる。

(例 1) $p^n = 2$, $h(x) = 1 + x + x^2$, 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 α

が得られる。 $a = \text{---} 111101011001000 \text{---}$

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

(3) n タプル p 元 M 系列 $A = \{ A_i \}$; p 元 M 系列 a をそれぞれ, s_0, s_1, \dots, s_{n-1} デイジット (但し $s_i = -\infty$ も許す) シフトした n 個の p 元 M 系列 ${}_{s_0} a, {}_{s_1} a, \dots, {}_{s_{n-1}} a$ 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 $A = ({}_{s_0} a, {}_{s_1} a, \dots, {}_{s_{n-1}} a)^t = \{ ({}_{s_0} a_i, {}_{s_1} a_i, \dots, {}_{s_{n-1}} a_i)^t \} = \{ A_i \}$ のことである。但し, t は転置を表わす。なお, 各元 A_i は $GF(p^m)$ 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 $A = ({}_0 a, {}_{-\infty} a, {}_3 a)^t$ は, 次の様に与えられる。

$$A = \begin{pmatrix} {}_0 a \\ {}_{-\infty} a \\ {}_3 a \end{pmatrix} = \dots \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \dots \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \dots$$

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 $GF(p^m)$ 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 の一周期分のデイジット数) で表わせは,

$h(x)A(x) = 0 \pmod{x^N-1}$ 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、 $a_i \in \{0, 1, \dots, (p-1)\}$

(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 ディスクリット・フーリエ変換対 η, W ;

$\eta = [\eta_0, \eta_1, \dots, \eta_{p^n-1}]^T$, $W = [w_0, w_1, \dots, w_{p^n-1}]^T$ (但し、 $v_j \in \{0, 1, \dots, (p-1)\}$, $\sum_{j=0}^{n-1} v_j p^j = k$ として、 $\eta_k = \eta((v_0, v_1, \dots, v_{n-1})^T)$ とする。 w_k についても同様。) とすれば、次式が成立する。

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

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。

$$F_0 = 1$$

$$d = e^{j2\pi/p} ; \quad F_n = \begin{pmatrix} F_{n-1} & F_{n-1} & F_{n-1} & \dots & F_{n-1} \\ F_{n-1} & dF_{n-1} & d^2F_{n-1} & \dots & d^{p-1}F_{n-1} \\ F_{n-1} & d^2F_{n-1} & d^4F_{n-1} & \dots & d^{2(p-1)}F_{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ F_{n-1} & d^{p-1}F_{n-1} & d^{2(p-1)}F_{n-1} & \dots & d^{(p-1)(p-1)}F_{n-1} \end{pmatrix} \quad (2)$$

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 $\gamma(A)$ は、2 元 M 系列 α (の数値列 $Z(\alpha)$) の n 次結合系列として、次の様に表現できる。

$$\gamma(A) = W_0 + W_1 Z(\alpha_0 \alpha) + W_2 Z(\alpha_1 \alpha) + W_3 Z(\alpha_0 \alpha) Z(\alpha_1 \alpha) + \dots + W_{2^n-1} Z(\alpha_0 \alpha) Z(\alpha_1 \alpha) \dots Z(\alpha_{n-1} \alpha) \quad (3)$$

但し、 $W = [W_0, W_1, \dots, W_{2^n-1}]^t$ は、 $\gamma = [\gamma_0, \gamma_1, \dots, \gamma_{2^n-1}]^t$ 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 $(\alpha_0, \alpha_1)^t$ を考える。写像 γ とし

$$\begin{pmatrix} W_0 \\ W_1 \\ W_2 \\ W_3 \end{pmatrix} = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} -3 \\ -1 \\ 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -2 \\ -1 \end{pmatrix} \quad \begin{aligned} \gamma_0 &= \gamma((0,0)^t) = -3, \\ \gamma_1 &= \gamma((1,0)^t) = -1, \quad \gamma_2 = \gamma((0,1)^t) \\ &= 3, \quad \gamma_3 = \gamma((1,1)^t) = 1 \end{aligned}$$

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、 $\gamma((\alpha_0, \alpha_1)^t) = 0 + 0 \cdot Z(\alpha_0 \alpha) - 2Z(\alpha_1 \alpha) - 1 \cdot Z(\alpha_0 \alpha) Z(\alpha_1 \alpha) = -2Z(\alpha_1 \alpha) - Z(\alpha_0 \alpha) Z(\alpha_1 \alpha)$

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 $A = (a_0, a_1, \dots, a_{n-1})^t$ において, a_0, a_1, \dots, a_{n-1} が互いに線型独立であれば, 一周期の $A = \{(a_{0i}, a_{1i}, \dots, a_{n-1i})\}_{i=0}^{N-1}$ (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 $O = (0, 0, \dots, 0)$ の個数は $p^{m-n} - 1$ 個, O 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 $A = \{A_i\} = (a_0, a_1, \dots, a_{n-1})^t$ において, $n\ell$ 個の系列 $\{a_{i-j} a\}$ ($i=0, 1, \dots, n-1$; $j=0, 1, \dots, \ell-1$) が互いに線型独立であれば, 相続く ℓ 個の n -タプル $(A_i, A_{i+1}, \dots, A_{i+\ell-1})$ のパターンが, $(0, 0, \dots, 0)$ となる頻度は, 一周期内において, $p^{m-n\ell} - 1$ であり, それ以外の^各パターンとなる頻度は, $p^{m-n\ell}$ 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,

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

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

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 a_0, a_1, \dots, a_{n-1} の $GF(p)$ 上の線型結合系列 $\sum_{j=0}^{n-1} u_j a_j = \left\{ \sum_{j=0}^{n-1} u_j a_j \right\}$ ($u_j \in GF(p)$) は, Q の特性多項式を $h(x)$ とし, $\sum_{j=0}^{n-1} u_j x^{Aj} = x^t \pmod{h(x)}$ (6) とすれば, p 元 M 系列 tQ に等しい。但し, (6) 式 $= 0$ のときは, $t = -\infty$ とする。

なお, (6) 式を満たす t を以後 $t(u_\ell, A)$ と記す。但し, $u_\ell = (u_0, u_1, \dots, u_{n-1})$ で, $\sum_{j=0}^{n-1} u_j p^j = \ell$, $A = (a_0, a_1, \dots, a_{n-1})$ 。

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

$$\begin{aligned} \eta(A_i) &= \sum_{u_0=0}^{p-1} \sum_{u_1=0}^{p-1} \dots \sum_{u_{n-1}=0}^{p-1} \left\{ z(a_0) \right\}^{u_0} \left\{ z(a_1) \right\}^{u_1} \dots \left\{ z(a_{n-1}) \right\}^{u_{n-1}} W(u_0, u_1, \dots, u_{n-1}) \\ &= \sum_{u_0=0}^{p-1} \sum_{u_1=0}^{p-1} \dots \sum_{u_{n-1}=0}^{p-1} z \left\{ \sum_{j=0}^{n-1} u_j a_j \right\} W(u_0, u_1, \dots, u_{n-1}) \end{aligned} \quad (10)$$

但し, \sum は, \pmod{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 $\eta(A_i) = \sum_{\ell=0}^{p^n-1} z(t(u_\ell, A) a_i) W_\ell$ (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) ρ を素数とする。 n タプル P 元 M 系列 $(a_0, a_1, a_2, \dots, a_{n-1}, a)^t$ の自己相関関数 $\mathcal{G}_\eta(\tau)$ (5式) は、次の様に表せる。
$$\mathcal{G}_\eta(\tau) = \frac{[(N+1) \sum_{(l_i, l_j) \in L_\tau} \sum_{(l_i, l_j) \in L_\tau} W_{l_i} W_{l_j}^* + C_\infty] - (|\eta_0|^2)^2}{T} \quad (12)$$

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

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 $W_{l_i} \neq 0$ を満たす l のうち、 $t(u_l, \mathcal{A}) \neq -\infty$ を満たすものを l_1, l_2, \dots, l_r とし、 $t(u_l, \mathcal{A}) = -\infty$ を満たすものを $l_{r+1}, l_{r+2}, \dots, l_{r+w}$ とする。このとき

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

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

補題 5 n 個の M 系列 $\{a_j\}_{j=0}^{n-1}$ が、互いに線型独立ならば、(3)式は、
$$T = p^{-n} (N+1) \sum_{l=0}^{p-1} (|\eta_l|^2)^2 - (|\eta_0|^2)^2 \quad (15)$$

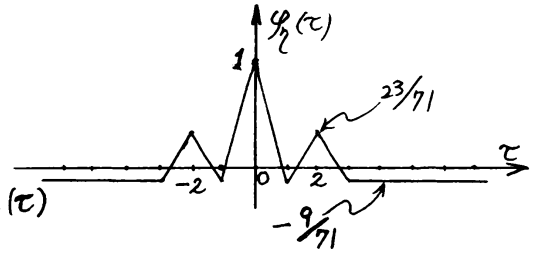
と表わすこともできる。また、このとき $C_\infty = (|W_0|^2)^2$ となる。

(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 $(0, a, 9a)$ 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。 $0 \cdot x^0 + 1 \cdot x^9 = x^9$, $1 \cdot x^0 + 1 \cdot x^9 = x^9 \pmod{h(x) = 1+x+x^4}$ であるので $t(u_2, \mathcal{A}) = 9$, $t(u_3, \mathcal{A}) = 7$. 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 $\varphi_\eta(\tau) = \frac{[(15+1)\{(-2)(-1)+0\} - (-3)^2]}{[(15+1)\{(-2)^2+(-1)^2\} - (-3)^2]} = 23/71$ 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 $h_\gamma(x) = \sum_{i=0}^{n-1} h_i x^i$ (γ 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 $(a_0 a, a_1 a, \dots, a_{n-1} a)$ であり, a_j ($j = 0, 1, \dots, n-1$) の間に $\frac{1}{n}$ 次の関係式が成立する.

$$a_j - a_0 = \sum_{i=1}^j C_i \cdot (p^{nm} - 1) / (p^n - 1) \quad (j = 1, 2, \dots, (n-1)) \quad (16)$$

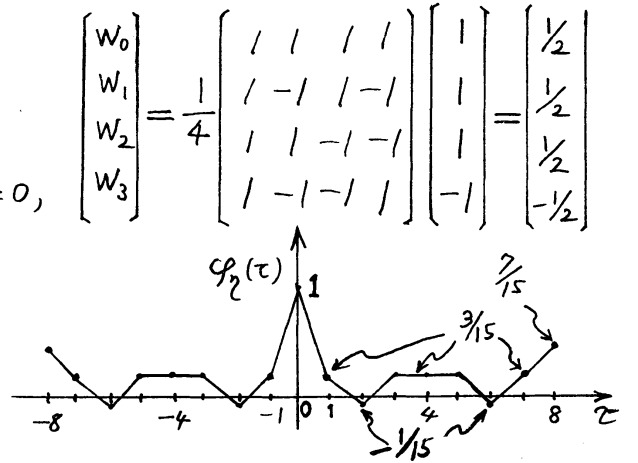
但し C_i は, 次式によって一意に定まる数である.

$$\begin{cases} \delta = \beta^{-(p^{nm}-1)/(p^n-1)} & (17) \end{cases}$$

$$\begin{cases} \delta^{C_{n-i}} = h_{n-i} \cdot \delta^{-\sum_{j=1}^{i-1} C_{n-j}} + \gamma & (i = 1, 2, \dots, (n-1)) \quad (18) \end{cases}$$

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

$\gamma_3 = \gamma((11)^t) = -1$ として,
 W は右の様に求められる。
 また, $t(u_0, \Omega) = -\infty, t(u_1, \Omega) = 0,$
 $t(u_2, \Omega) = 7, t(u_3, \Omega) = 9$
 $C_\infty = (\frac{1}{2})^2 = \frac{1}{4}$. これら
 をもとにして (12), (13) 式より,
 $\varphi_2(\tau)$ 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 マル 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, "擬疑似ランダム系列 (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 マル M 系列について" 電子通信学会オートマトンと言語研究 AL.72-29 1972年6月