M 配列の二、三の性質†

森 内 勉*・柏 木 潤**

On Some Properties of M-Arrays

Tsutomu MORIUCHI* and Hiroshi KASHIWAGI**

Some basic properties of M-arrays are described. M-array is a two dimensional array in which an M-sequence is arranged under a certain rule.

Based on the fact that an M-sequence is represented by the trace of a finite field, the row sequences or the column sequences in the M-array are explicitly expressed by use of the trace.

Using this expression, the authors show theoretically some of the basic properties of M-array, such as

- (1) the column sequences of M-array are either M-sequences of small degree or zero sequences,
- (2) the row sequences of M-array are non-maximum length sequences of the same degree but all different,
- (3) for even degree M-sequence, M-array is symmetrical with respect to a zero column when only one zero column exists, and so on.

Key Words: M-sequence, M-array, trace on finite field, pseudo-random array

1. ま え が き

M 配列は M 系列をある規則のもとに 2 次元に配列したものであり、M 系列とよく似た 2 次元での擬似不規則な性質をもっているため¹⁾、その性質を利用して 2 次元面の位置検出²⁾や、M 系列間の遅延測定³⁾などに使用されている。しかし M 配列を構成している行と列の系列の性質などの M 配列の一般的性質につい

ては、まだよく知られていないところがあり M 配列の使用にあたって調べておく必要がある。Weng⁴⁾ は M 系列を M 配列として 2 次元に分解して M 配列の列系列について調べている。本論文は M 系列を有限体上のトレースによって表現して、M 配列の行と列の系列を明確に定義し、その行と列系列に着目することによって M 配列のいくつかの性質を明らかにしたものである。

2. M 配列の構成

系列 $\{m_k\}$, $k=0, 1, 2, \dots$, $m_k=0$ または 1 を周期 N の M 系列とすると、 n を適当な正整数として $N=2^n-1$ と表わせる。そこでつぎの式を満足する正整数 v, e, n_1, n_2 を考える。

$$N=2^v-1 (ve=n, 2 \leq v < n)$$

$$n_1=2^v-1, n_2=N/n_1, \text{GCD}(n_1, n_2)=1 \quad (1)$$

ここで $\text{GCD}(a, b)=c$ とは、 a と b の最大公約数が c であることを示す記号とする。M 系列 $\{m_k\}$ を 2 次元に配列した M 配列とは M 系列の擬似不規則性を 2 次元に拡張した性質をもつ配列をいい、たとえば 4 次の M 系列を用いると、 $n_1=3, n_2=5$ をとってつぎのような 3×5 の行列 M として表わされるものである。

$$M = \begin{bmatrix} m_0 & m_6 & m_{12} & m_3 & m_9 \\ m_{10} & m_1 & m_7 & m_{13} & m_4 \\ m_5 & m_{11} & m_2 & m_8 & m_{14} \end{bmatrix}$$

そこで一般的に $n_1 \times n_2$ の M 配列を b と記し、 i 行 j 列の要素を $b_{i,j}$ とするとつぎのように表わされる。

$$b_{i,j}=m_k, 0 \leq k \leq N-1 \quad (2)$$

ここで

$$i=k(\text{mod } n_1), j=k(\text{mod } n_2) \quad (3)$$

とする。 $\text{GCD}(n_1, n_2)=1$ なのでユークリッドアルゴリズムによって次式を満たす整数 μ と ν がある。

$$\mu n_1 + \nu n_2 = 1 \pmod{N} \quad (4)$$

ただし μ, ν はそれぞれ $0 < \mu < n_2, 0 < \nu < n_1$ の値をもつ整数である。(4)式の両辺に k を乗じて(3)式を

* 第 23 回計測自動制御学会学術講演会で発表 (昭 59・7)

* 八代工業高等専門学校, 八代市平山新町 2627

* Yatsushiro Technical College, Yatsushiro

** 熊本大学工学部 熊本市黒髪 2-39-1

** Faculty of Engineering, Kumamoto University, Kumamoto

(Received December 8, 1984)

(Revised August 14, 1985)

用いると次式のようになる。

$$js_e + is_r = k \pmod{N} \quad (5)$$

ここで $s_e = \mu n_1$, $s_r = \nu n_2$ とおいた。M 系列 $\{m_k\}$ の上で任意の要素 m_k と $m_{k+\tau}$ とは τ ビットの間隔があるが、(5)式よりつぎのことが容易に導かれる。M 配列 $\mathbf{b}$ の i 行 j 列の要素 $b_{i,j}$ のつぎの行の要素 $b_{i+1,j}$ には $m_k + s_r$ が配列されている。このように列の系列の要素間には $\{m_k\}$ の上で s_r ビットの間隔がある。ここではこのビット間隔を行間遅延と呼ぶこととする。同様に行の系列の要素間には $\{m_k\}$ の上で s_e ビットの間隔がある。これを列間遅延と呼ぶこととする。さらに左下方向の系列の要素間には $\{m_k\}$ の上で $s_r - s_e$ のビット間隔がある。

3. M 配列の行と列系列

周期 $N(=2^n-1)$ をもつ M 系列 $\{m_k\}$ をつぎのように書くこととする。

$$m(z) = \sum_{k=0}^{N-1} m_k z^k \quad (6)$$

またガロア体 $GF(2^n)$ 上の元 ξ の $GF(2)$ へのトレースを $T_n(\xi)$ と書くと、つぎのように定義される。

$$T_n(\xi) = \xi + \xi^2 + \dots + \xi^{2^{n-1}} \quad (7)$$

なお $T_n(\xi) \in GF(2)$ となる。そして $\{m_k\}$ の特性多項式として $GF(2)$ 上 n 次の原始多項式を選択して、その根を α とすれば M 系列 $\{m_k\}$ は (7) 式を用いて

$$m_k = T_n(\lambda \alpha^k), \lambda \in GF(2^n), \neq 0 \quad (8)$$

と書ける⁷⁾。ここで元 λ は初期値 $m_0, m_1, \dots, m_{n-1}$ によって定まる元で M 系列の位相を決定する。もし特性 M 系列の位相にとるならば $m_k = m_{2^k}$ の条件を (8) 式へ代入して $\lambda = 1$ となる。(8) 式を (6) 式へ代入し

$$m(z) = \sum_{k=0}^{N-1} T_n(\lambda \alpha^k) z^k \quad (9)$$

となる。また $\{m_k\}$ より任意の正整数 τ ビット遅れた M 系列 $\{m_{k-\tau}\}$ は

$$\sum_{k=0}^{N-1} T_n(\lambda \alpha^{k-\tau}) z^k = z^\tau m(z) \quad (10)$$

と表わされる。ここで $\{m_k\}$ が周期 N をもつので $z^N = 1$ として取り扱う。

M 配列 $\mathbf{b}$ は、 $\mathbf{b}$ の行方向を x , 列方向を y で記して $z = xy (x^{n_1} = y^{n_2} = 1)$ として扱う) とおき、(2), (3) 式を用いて (9) 式の $m(z)$ を 2 変数に分解するとつぎのような関数 $b(x, y)$ によって表わされる。

$$b(x, y) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} T_n(\lambda \alpha^k) x^i y^j \quad (11)$$

そして元 α^k は (5) 式よりつぎのように書ける。

$$\alpha^k = \gamma^j \beta^i \quad (12)$$

ここで $\gamma = \alpha^{s_e}$, $\beta = \alpha^{s_r}$ とおいた。よって (12) 式を (11) 式へ代入して

$$b(x, y) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} T_n(\lambda \gamma^j \beta^i) x^i y^j \quad (13)$$

と書ける。M 配列 $\mathbf{b}$ の行, 列系列をつぎのように定義する。任意の i 行の行系列を $r_i(y)$ と表わして、(13) 式から次式のようになる。

$$r_i(y) = \sum_{j=0}^{n_2-1} T_n(\lambda \beta^j \gamma^i) y^j, 0 \leq i \leq n_1-1 \quad (14)$$

同様に任意の j 列の列系列を $c_j(x)$ と表わして、次式のようになる。

$$c_j(x) = \sum_{i=0}^{n_1-1} T_n(\lambda \gamma^i \beta^j) x^i, 0 \leq j \leq n_2-1 \quad (15)$$

4. M 配列の性質

[性質 1]

列系列 $c_j(x) (0 \leq j \leq n_2-1)$ は周期 $n_1 (= 2^v-1)$ をもつ同じ M 系列か、もしくは長さ n_2 の 0 系列 (すべての要素が 0 の系列) となる。

(証明)

$n = ve$ であるから、(15) 式のトレース $T_n(\lambda \gamma^i \beta^j)$ は、(7) 式を用いればつぎのように $GF(2^v)$ から $GF(2)$ へのトレースによって表現される⁴⁾。

$$T_n(\lambda r^j \beta^i) = T_v \{ [(\lambda \gamma^j) + (\lambda \gamma^j)^{2^v} + \dots + (\lambda \gamma^j)^{2^{(e-1)v}}] \beta^i \} \quad (16)$$

元 β は α^{s_r} であるから (5) 式より β の位数は $n_1 (= 2^v-1)$ となり、 $GF(2^v)$ の原始元となる。(16) 式の [] 中の元は、 $GF(2^v)$ の元であるから原始元 β のべき表現によって次式のように表わされる。

$$(\lambda \gamma^j) + (\lambda \gamma^j)^{2^v} + \dots + (\lambda \gamma^j)^{2^{(e-1)v}} = \beta^{l_j} \quad (17)$$

ここに l_j は $*$, $0, 1, \dots, n_1-1$ のいずれかである。なお $\beta^* = 0$ とおいている。(17) 式を (16) 式へ代入し、

$$T_n(\lambda \gamma^j \beta^i) = T_v(\beta^{l_j} \beta^i) \quad (18)$$

となるので、(15) 式の列系列は次式のように書ける。

$$c_j(x) = \sum_{i=0}^{n_1-1} T_v(\beta^{l_j} \beta^i) x^i \quad (19)$$

ここで $l_j = *$ のときは $\beta^* = 0$ であるからトレースはすべての i に対して 0 となり、このような場合 $c_j(x)$ は長さ n_1 の 0 系列となる。また $l_j \neq *$ の場合、(8) 式から列系列 $c_j(x)$ の特性多項式は β を根としてもち、元 β は $GF(2^v)$ の原始元であることより、その

特性多項式は $GF(2)$ 上 v 次の原始多項式となつて、列系列 $c_i(x)$ は周期 n_1 の同じ M 系列となる。

(証明終)

この性質から n_2 個の列系列の中で、0 系列の個数は $n_2 - 2^{n-v}$ 個となることも容易に導かれる。

〔性質 2〕

$n_2 \nmid 2^m - 1, m < n$ の場合、行系列 $r_i(y) (0 \leq i \leq n_1 - 1)$ は周期 $n_2 (= N/n_1)$ の非極大系列で、同じ n 次の特性多項式を持つがすべて異なる系列である。

(証明)

(14) 式で表わされる行系列 $r_i(y)$ の特性多項式は γ を根として持っている。元 γ は α^{e_c} であり、(5) 式より $n_2 (= N/n_1)$ の位数をもつ。また $n_2 \nmid 2^m - 1, m < n$ から $\gamma^{2^i} \neq \gamma^{2^j} (i \neq j, 0 \leq i, j \leq n_1 - 1)$ となるので特性多項式は n 次の非原始既約多項式となり、 $r_i(y)$ は周期 n_2 の非極大系列となる。なお $a \mid b$ は、 a が b の約数であることを示し、 $a \nmid b$ は、 a が b の約数でないことを示す記号とする。元 γ は n 次既約多項式の根であるから、元 $1, \gamma, \dots, \gamma^{n-1}$ は $GF(2^n)$ 上ですべて異なつて基底となれるし、それらの逆元 $1, \gamma^{-1}, \dots, \gamma^{-(n-1)}$ も基底となる。よつて (14) 式の固定元 $\lambda \beta^i (0 \leq i \leq n_1 - 1)$ は基底を用いて次式のように表わされる。

$$\lambda \beta^i = a_0 + a_1 \gamma^{-1} + \dots + a_{n-1} \gamma^{-(n-1)} \quad (20)$$

ここで $a_0, a_1, \dots, a_{n-1} \in GF(2)$ とする。(20) 式を (14) 式へ代入し、トレースの線形性を用いると (14) 式の行系列 $r_i(y)$ はつぎのように書ける。

$$\begin{aligned} r_i(y) = & a_0 \sum_{j=0}^{n_2-1} T_n(\gamma^j) y^j + a_1 \sum_{j=0}^{n_2-1} T_n(\gamma^j) y^{j+1} + \dots \\ & + a_{n-1} \sum_{j=0}^{n_2-1} T_n(\gamma^j) y^{j+n-1} \end{aligned} \quad (21)$$

(20) 式において、ある $k (0 \leq k \leq n_1 - 1)$ で $\lambda \beta^k = 1$ が成立するならば $a_0 = 1, a_i \neq 0 (1 \leq i \leq n-1)$ となり、行系列 $r_k(y)$ は (21) 式の右辺第 1 項で表わされる。そのほかの行系列 $r_i(y) (0 \leq i \leq n_1 - 1, i \neq k)$ は、(21) 式で表わされるように $r_k(y)$ とそれより $\tau (1 \leq \tau \leq n-1)$ ビット遅れた系列 $y^\tau r_k(y)$ の線形結合で表わされる。そして元 β の位数は n_1 であり、 $\beta^i \neq \beta^j (i \neq j, 0 \leq i, j \leq n_1 - 1)$ であるから (21) 式の右辺の結合式はすべての i に対して異なることとなり、行系列 $r_i(y) (0 \leq i \leq n_1 - 1)$ は同じ特性多項式をもつがすべて異なる系列となる。

(証明終)

なお性質 1, 2 については Weng⁴⁾ も別の方法で導出している。

〔性質 3〕

M 系列 $\{m_k\}$ からの M 配列 $\mathbf{b}$ を $b(x, y)$ で表わし、正整数 $\tau (0 \leq \tau \leq N-1)$ ビット遅れた M 系列 $\{m_{k-\tau}\}$

からの同じ大きさの M 配列 $\tau \mathbf{b}$ を $\tau b(x, y)$ と表わしたとき、これらの M 配列間に次式が成立する。

$$\tau b(x, y) = x^{\tau_r} y^{\tau_c} b(x, y) \quad (22)$$

ここで $\tau_r = \tau \pmod{n_1}$, $\tau_c = \tau \pmod{n_2}$ とする。

(証明)

M 配列 $\tau b(x, y)$ は (11) 式の $T_n(\lambda \alpha^k)$ を $T_n(\lambda \alpha^{k-\tau})$ に置き換えてつぎのように表わされる。

$$\tau b(x, y) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} T_n(\lambda \alpha^{k-\tau}) x^i y^j \quad (23)$$

また (4) 式の両辺に $k - \tau$ を乗じると

$$(j - \tau_c) s_c + (i - \tau_r) s_r = k - \tau \pmod{N} \quad (24)$$

となる。(24) 式を (23) 式へ代入し (12) 式を用いるとつぎのように書ける。

$$\begin{aligned} \tau b(x, y) = & \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} T_n(\lambda \gamma^{j-\tau_c} \beta^{i-\tau_r}) x^i y^j \\ = & \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} T_n(\lambda \gamma^j \beta^i) x^{i+\tau_r} y^{j+\tau_c} \end{aligned} \quad (25)$$

(25) 式と (13) 式から (22) 式が得られる。(証明終)

M 配列 $\tau b(x, y)$ の列系列を $\tau c_i(x)$ とし、行系列を $\tau r_i(y)$ と記することとすると、(25) 式と (18), (19) 式を用いて M 配列 $b(x, y)$ の行または列系列との間に次式のような関係が成立することも容易に導かれる。

$$\tau c_i(x) = x^{\tau_r} c_d(x) \quad (d = (j - \tau_c) \pmod{n_2}) \quad (26)$$

$$\tau r_i(y) = y^{\tau_c} r_f(y) \quad (f = (i - \tau_r) \pmod{n_1}) \quad (27)$$

したがつて M 配列 $\tau \mathbf{b}$ は、 $\mathbf{b}$ のすべての行系列を右へ τ_c ビットシフトした後、さらに列系列を下方へ τ_r ビットシフトすることによって得られることを意味する。**Fig. 1** と **Fig. 2** に位相の異なる同じ M 系列からの M 配列を示す。ここで Fig. 1 の M 配列を $\mathbf{b}$ とし、Fig. 2 の M 配列を $\tau \mathbf{b}$ とする。なお $\tau = 127$, $\tau_r = 7$, $\tau_c = 8$ である。 $\tau \mathbf{b}$ の列系列 $\tau c_8(x)$ と $\mathbf{b}$ の列系列 $c_0(x)$ は共に 0 系列であり、 $\tau \mathbf{b}$ の行系列 $\tau r_7(y)$ は $\mathbf{b}$ の行系列 $r_0(y)$ を右へ 8 ビットシフトした系列と等しくなるが、これは (26), (27) 式から得られる結果と一致する。

〔性質 4〕

もとの M 系列 $\{m_k\}$ を列間遅延の s_c ごとにサンプリングして得られる系列によつてつぎのような $n_1 \times n_2$ の配列 $\mathbf{S}_c$ を作ることにする。

$$\mathbf{S}_c = \begin{bmatrix} m_0 & m_{s_c} & \dots & m_{(n_2-1)s_c} \\ m_1 & m_{s_c+1} & \dots & m_{(n_2-1)s_c+1} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n_1-1} & m_{s_c+n_1-1} & \dots & m_{(n_2-1)s_c+n_1-1} \end{bmatrix} \quad (28)$$

ここで上の配列 $\mathbf{S}_c$ における行系列を $\tau r_i(y)$ と記することとすると、M 配列 $\mathbf{b}$ の行系列 $r_i(y)$ との間に次式が成立する。

$$r_i(y) = y^i \tau r_i(y), \quad 0 \leq i \leq n_1 - 1 \quad (29)$$

Fig. 1 An example of M-array
Characteristic Poly. = $X^8 + X^4 + X^3 + X^2 + 1$
Initial Value = 00000100
 $\tau = 0$

Fig. 2 An example of M-array
Characteristic Poly. = $X^8 + X^4 + X^3 + X^2 + 1$
Initial Value = 00101101
 $\tau = 127$

(証明)

配列 S_c の行系列に着目すると、 i 行 ($0 \leq i \leq n_1 - 1$) の行系列 $r_i(y)$ は、もとの M 系列 $\{m_k\}$ を s_c ごとにサンプルして得られる系列 $\{m_{js_c+i}\}$ ($0 \leq j \leq n_2 - 1$) であり、(14) 式と同じ形式で表わすならば、次式となる。

$$\begin{aligned} r_i(y) &= \sum_{j=0}^{n_2-1} m_{js_c+i} y^j \\ &= \sum_{j=0}^{n_2-1} T_n(\lambda \alpha^{js_c+i}) y^j \\ &= \sum_{j=0}^{n_2-1} T_n(\lambda \alpha^i \gamma^j) y^j \end{aligned} \quad (30)$$

一方 (14) 式は、 $\beta^i = \alpha^i \gamma^{-i}$ であるからつぎのようになる。

$$\begin{aligned} r_i(y) &= \sum_{j=0}^{n_2-1} T_n(\lambda \alpha^i \gamma^{-i} \gamma^j) y^j \\ &= \sum_{j=0}^{n_2-1} T_n(\lambda \alpha^i \gamma^j) y^{j+i} \end{aligned} \quad (31)$$

(30) 式と (31) 式から (29) 式が得られる。 (証明終)

同じようにつぎの性質も容易に導かれる。

〔性質 5〕

もとの M 系列 $\{m_k\}$ を行間遅延の s_r ごとにサンプルして得られる系列によってつぎのような $n_1 \times n_2$ の配列 S_r を作ることにする。

$$S_r = \begin{bmatrix} m_0 & m_1 & \cdots & m_{n_2-1} \\ m_{s_r} & m_{s_r+1} & \cdots & m_{s_r+n_2-1} \\ \vdots & \vdots & \ddots & \vdots \\ m_{(n_1-1)s_r} & m_{(n_1-1)s_r+1} & \cdots & m_{(n_1-1)s_r+n_2-1} \end{bmatrix} \quad (32)$$

ここで上の配列 S_r における列系列を $r_c(x)$ と記すこととすると、M 配列 b の列系列 $c_j(x)$ との間に次式が成立する。

$$c_j(x) = x^j r_c(x), \quad 0 \leq j \leq n_2 - 1 \quad (33)$$

Fig. 3 は、Fig. 1 の M 配列のもとなる M 系列を s_c ごとにサンプルして得られた配列 S_c である。ここで $s_c (= \mu n_1) = 120$ である。Fig. 1 の行系列 $r_i(y)$ と、Fig. 3 の行系列 $r_c(y)$ との関係は (29) 式から得られる結果と一致していることがわかる。

〔性質 6〕

M 系列 $\{m_k\}$ の次数 n を偶数とすると、 $v = n/2$, $n_1 = 2^v - 1$, $n_2 = 2^v + 1$ をもつ M 配列において、ある一つの列系列は長さ n_1 の 0 系列になる (この列系列を $c_{j_0}(x)$ ($0 \leq j_0 \leq n_2 - 1$) と記すこととする)。そのほかの列系列は周期 n_1 の M 系列になる。そしてこれらの列系列を $c_{j_0+\sigma}(x)$ (σ は $1 \leq \sigma \leq n_2 - 1$ の整数) と記すこととすると次式が成立する。

$$c_{j_0+\sigma}(x) = c_{j_0-\sigma}(x) \quad (34)$$

ただし $j_0 \pm \sigma$ は n_2 を法とする。

(証明)

$v = n/2$, $n_1 = 2^v - 1$, $n_2 = 2^v + 1$ は (1) 式の条件を満足していて、(4) 式から $\mu = v = 2^{v-1}$ となるので列間、行間遅延はそれぞれ $s_c = 2^{v-1} - 1$, $s_r = 2^{v-1} + 1$ となる。(17) 式に $v = n/2$, $e = 2$ を代入すると次式となる。

$$\beta^{ij} = (\lambda \gamma^j) + (\lambda \gamma^j)^{2^v} \quad (35)$$

ここで右辺が 0 となる j の値 (j_0) を求めてみる。 $(\lambda \gamma^j) = (\lambda \gamma^j)^{2^v}$ より $(\lambda \gamma^j)^{2^v-1} = (\lambda \gamma^j)^{n_1} = 1$ となる。 λ は GF(2^n) 上の元であるから、原始元 α を用いて $\lambda = \alpha^{-\tau}$ ($0 \leq \tau \leq N-1$) と書けるので、 $\gamma^{jn_1} = \lambda^{-n_1} = \alpha^{\tau n_1} = \gamma^{\tau n_1}$ となり、 $j_0 = \tau \pmod{n_2}$ が一意に求まる。よって (19) 式から $c_{j_0}(x)$ のみが 0 系列となり、そのほかの j のとき

Fig. 3 An array formed by sampling sequences from an M-sequence
 Characteristic Poly. = $X^8 + X^4 + X^3 + X^2 + 1$
 Initial Value = 00000100
 Sampling Period of Row Seq. $s_c = 120$

は $\beta^{j_0} \neq 0$ となるため、 $c_j(x)$ は周期 n_1 の M 系列となる。0 系列 $c_{j_0}(x)$ を基準にすると、そのほかの列系列は $c_{j_0+\sigma}(x)$ (ただし $j_0+\sigma$ は n_2 を法とする) と表わせるので、(35) 式に $j = j_0 + \sigma$ と $\lambda = \beta^{-\tau}\gamma^{-\sigma} = \beta^{-\tau}\gamma^{-j_0}$ を代入するとつぎようになる。

$$\beta^{j_0+\sigma} = \beta^{-\tau}\gamma^{\sigma} + \beta^{-\tau}\gamma^{-\sigma} \quad (36)$$

(36) 式右辺は、 $\sigma = -\sigma$ においても同じ式になるから (34) 式が得られる。 (証明終)

したがって性質 6 の条件を満足する偶数次数の M 系列を用いて作られた M 配列は、0 系列を中心として左右対称に配列されていることとなる。Fig. 1 は 8 次の特性 M 系列からの M 配列 $\mathbf{b}$ であり、Fig. 2 は遅れ $\tau = 127$ をもつ M 配列 $\mathbf{c}\mathbf{b}$ である。これらの M 配列は性質 6 を満足している。また $\mathbf{b}$ と $\mathbf{c}\mathbf{b}$ の列系列の中で、0 系列はそれぞれ $c_0(x)$ と $c_{c_0}(x)$ である。このことは、 $\mathbf{b}$ では (35) 式の λ が 1 ($\tau = 0$ を意味する) なので $j_0 = 0$ となり、 $\mathbf{c}\mathbf{b}$ では $\tau = 127$ なので $j_0 = 127 \pmod{17} = 8$ となることより明らかである。

M 配列は性質 4 (または性質 5) を持つので、著者が文献 6) に示したように等次数の M 系列群から、それらを s_c (または s_r) ごとにサンプルして得られた系列が同じ系列 (同じ特性多項式から発生された系列を意味する) になるような M 系列の集合を一つのクラスに分類しておけば、同一クラスに属する M 系列から作られた同じ大きさの M 配列は、同じ行 (または列) 系列で構成されることになる。このようなサンプリング周期 s_c のもとで同一クラスに属する n 次 M 系列の二つを一般に $\{m_k\}$, $\{\hat{m}_k\}$ とし、それらの特性多項式の根をそれぞれ α , α^p (p は $1 < p \leq N-1$ の N と互いに素な整数で、 N を法として 1 と同じ円分

剰余類に属さないものとする) と記すこととするとつぎのような関係が成立する^{5), 6)}。

$$p = 1 + n_2\eta, \quad 1 \leq \eta \leq n_1 - 1 \quad (37)$$

ここで p は η の値により $n_1 - 1$ 個の異なる値をとるが、その中で N と互いに素なものだけ選ぶこととし、 p を $p(\eta)$ と表わせば、同じクラスに属する異なる各 M 系列の特性多項式の根は、元 α , $\alpha^{p(1)}$, $\alpha^{p(2)}$, ..., のいずれかであることを意味している。このような M 系列の分類をサンプリング周期 s_c のもとでの分類と呼ぶこととし、同様にしてサンプリング周期 s_r のもとでの分類も考えることができる。

性質 1 によれば M 配列の列系列は 0 系列か、もしくは周期 n_1 の同じ M 系列であった。0 系列をのぞくある列系列を基準にして、そのほかの列系列との位相差を列系列位相と呼ぶこととしよう。そこで基準系列を 1 列目の列系列 $c_1(x)$ にとることとし (もし 1 列目が 0 系列のときはそのほかの列系列を基準にするものとする)、任意の列系列 $c_j(x)$ ($0 \leq j \leq n_2 - 1$, $j \neq 1$) との列系列位相を L_j ($0 \leq L_j \leq n_1 - 1$) と表わせば、(17), (19) 式からつぎのように書ける。

$$L_j = l_j - l_1 \pmod{n_1} \quad (38)$$

すなわち $c_j(x) = c_1(x)x^{-L_j}$ と表わされる。一般的にすべての j について L_j を知るには、(17) 式によってすべての j について l_j を求めておかなければならないが、もし特性 M 系列を用いて作られた M 配列では、 n_2 を法とする各円分剰余類首に相当する j の値についての l_j を求めておけばよい。なぜならば (17) 式において $\lambda = 1$ であり、ある剰余類首 s ($0 \leq s \leq n_2 - 1$) と同じ剰余類に属する j は、 $j = 2^s s \pmod{n_2}$, $0 \leq s \leq n_1 - 1$ と表わせるので $l_j = 2^s l_s \pmod{n_1}$ となるからである。なお $l_s = *$ のときは $l_j = *$ として扱うこととする。たとえば Fig. 1 の M 配列において n_2 は 17 であり、異なる剰余類首 s はそれぞれ 0, 1, 3 である。 $\gamma = \alpha^{120}$, $\beta = \alpha^{136}$ を (17) 式に代入して各 s について l_s を求めると、 $l_0 = *$, $l_1 = 3$, $l_3 = 1$ となる。よって各列系列位相は $L_j = 2^s l_s - l_1 \pmod{15}$ と表わせるが、これは図から明からである。

【性質 7】

異なる M 系列 $\{m_k\}$ と $\{\hat{m}_k\}$ はサンプリング周期 s_c のもとで同じクラスに属するものとし、共に特性 M 系列の位相にとるものとする。M 系列 $\{m_k\}$ からの M 配列における列系列位相を L_j ($0 \leq j \leq n_2 - 1$) とし、M 系列 $\{\hat{m}_k\}$ からの M 配列における列系列位相を $\hat{L}_j$ と記すこととすると、 L_j と $\hat{L}_j$ との間に次式が成立する。

$$\hat{L}_j = p(\eta)^{-1} L_j \pmod{n_1} \quad (39)$$

ここで $p(\eta)^{-1}$ は n_1 を法とする $p(\eta)$ の逆元とする。

(証明)

M 系列 $\{m_k\}$ からの M 配列, 列系列をそれぞれ (13), (15) 式で示される $b(x, y)$, $c_j(x)$ とする。ただし特性 M 系列であるから $\lambda=1$ とする。M 系列 $\{\hat{m}_k\}$ はサンプリング周期 s_c のもとで $\{m_k\}$ と同じクラスに属するため, その特性多項式は (37) 式で示される元 $\alpha^{p(\eta)}$ を根としてもつ。よって (9) 式 ($\lambda=1$ とする) の k を $p(\eta)k$ に置き換えて $\{\hat{m}_k\}$ はつぎのように表わせる。

$$\hat{m}(z) = \sum_{k=0}^{N-1} T_n(\alpha^{p(\eta)k}) z^k \quad (40)$$

$\alpha^{p(\eta)} = \gamma \beta^{p(\eta)}$ を (40) 式に代入し, $\{\hat{m}_k\}$ からの M 配列 $\hat{b}(x, y)$ はつぎのように書ける。

$$\hat{b}(x, y) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} T_n(\gamma^j \beta^{p(\eta)i}) x^i y^j \quad (41)$$

そして列系列を $\hat{c}_j(x)$ と記すと, (17), (18), (41) 式を用いてつぎのように表わされる。

$$\begin{aligned} \hat{c}_j(x) &= \sum_{i=0}^{n_1-1} T_n(\gamma^j \beta^{p(\eta)i}) x^i \\ &= \sum_{j=0}^{n_1-1} T_n(\beta^{p(\eta)j}) x^j \end{aligned} \quad (42)$$

(42) 式から, $\hat{c}_1(x)$ と $\hat{c}_j(x)$ との列系列位相 $\hat{L}_j$ は, $\hat{L}_j = p(\eta)^{-1}(j - l_1) \pmod{n_1}$ と書けるので, これと (38) 式から (39) 式が得られる。 (証明終)

性質 2 による M 配列の行系列は, 同じ特性多項式によって発生される周期 n_2 のすべて異なる非極大系列であるため, 列系列位相と同じような意味での位相差は定義できない。しかしサンプリング周期 s_c のもとで同じクラスに属する各 M 系列を用いて作られたそれぞれの M 配列の行系列は, 同じ系列によって構成されていることに着目し, その中のある M 配列の行系列がほかの M 配列でどの行位置に配列されているかということを行系列位相と考えることとしよう。

【性質 8】

異なる M 系列 $\{m_k\}$ と $\{\hat{m}_k\}$ はサンプリング周期 s_c のもとで同じクラスに属するものとし, 共に特性 M 系列の位相にとるものとする。 $\{m_k\}$ と $\{\hat{m}_k\}$ から得られたそれぞれの M 配列の行系列を $r_i(y)$, $\hat{r}_i(y)$ ($0 \leq i \leq n_1 - 1$) とした場合, $\hat{r}_i(y) = r_w(y)$ ($0 \leq w \leq n_1 - 1$) とするような行系列位相 w はつぎのように表わせる。

$$w = p(\eta)i \pmod{n_1} \quad (43)$$

(証明)

M 系列 $\{\hat{m}_k\}$ から得られる M 配列 $\hat{b}(x, y)$ の行系列 $\hat{r}_i(y)$ は, (41) 式からつぎのように書ける。

Fig. 4 An example of M-array

Characteristic Poly. = $X^8 + X^5 + X^3 + X + 1$

Initial Value = 00010111

$\tau=0$, $\eta=3$, $p(\eta)=7 \pmod{15}$, $p(\eta)^{-1}=13$

$$\hat{r}_i(y) = \sum_{j=0}^{n_2-1} T_n(\beta^{p(\eta)i} \gamma^j) y^j \quad (44)$$

また M 系列 $\{m_k\}$ から得られた M 配列 $b(x, y)$ の行系列 $r_i(y)$ は, (14) 式で与えられる (ただし $\lambda=1$ とする)。(14) 式と (44) 式より, $\hat{r}_i(y) = r_w(y)$, $w = p(\eta)i \pmod{n_1}$ となる。 (証明終)

Fig. 1 と Fig. 4 は, サンプリング周期 $s_c=120$ のもとで同じクラスに属する 8 次の M 系列 (共に特性 M 系列の位相にとられている) を用いて得られた 15×17 の M 配列である。Fig. 1 の M 系列の特性多項式 $X^8 + X^4 + X^3 + X^2 + 1$ が α を根にもつならば, Fig. 4 の M 系列の特性多項式 $X^8 + X^5 + X^3 + X + 1$ は α^{52} ((37) 式の $p(3)$ に相当する) を根としてもつ。性質 7 より Fig. 1 の列系列位相 L_j と Fig. 4 の列系列位相 $\hat{L}_j$ は $\hat{L}_j = p(\eta)^{-1} L_j = 13 L_j \pmod{15}$, $0 \leq j \leq 16$ の関係があるが, これは Fig. 1, Fig. 4 の L_j と $\hat{L}_j$ より明らかである。また性質 8 より Fig. 4 の行系列 $\hat{r}_i(y)$ ($0 \leq i \leq 15$) は Fig. 1 の行系列 $r_w(y)$ ($0 \leq w \leq 15$) と $w = p(\eta)i = 7i \pmod{15}$ の関係があるが, これも Fig. 1, Fig. 4 の i と w より明らかである。

5. あとがき

M 系列を有限体上のトレースによって表現し, M 配列の行と列の系列を定義した。その行と列系列に着目して M 配列のいくつかの一般的性質について理論的に示した。そして M 配列がこれらの性質をもつことを数値計算によって確認した。これらの結果は M 配列を種々の方面に応用するとき, きわめて有効かと思われる。

参 考 文 献

- 1) F. J. MacWilliams and N. J. A. Sloane. Pseudo-Random Sequences and Arrays, Proc. IEEE, **64**-12 (1976)
- 2) 今井, 片山: M 平面を用いた 2 次元面の位置検出装置, 電子通信学会論文誌, **59-A**-3, 260/262 (1976)
- 3) 柏木, 内村: M 配列を用いる遅延の測定, 第 20 回 SICE 学術講演会予稿集, 175/176 (1981)
- 4) L. J. Weng: Decomposition of M-Sequences and Its Applications, IEEE Trans. on Information Theory, **IT-17**-4, 457/463 (1971)
- 5) 森内, 柏木: M 配列の二, 三の性質, 第 23 回 SICE 学術講演会予稿集, 605/606 (1984)
- 6) 森内, 柏木: 異なる特性多項式をもつ M 系列の相互相関, 計測自動制御学会論文集, **19**-10, 60/65 (1983)
- 7) F. J. MacWilliams and N. J. A. Sloane: The Theory of Error Correcting Codes, North Holland (1978)