異なる M 系列間の相互相関値の上限†

森 内 勉*・柏 木 潤**

On Upper Bound of Crosscorrelation Values between Different M-Sequences

Tsutomu MORIUCHI* and Hiroshi KASHIWAGI**

The upper bound of crosscorrelation of M-sequences which have the same period but different characteristic polynomials is shown theoretically.

An M-sequence generated by an n -th degree characteristic polynomial which is a primitive polynomial over GF(2) is constructed, in case of the period $N=2^n-1$ is nonprime, by the combinations of s nonmaximum length sequences with length q generated by an n -th degree irreducible polynomial of exponent q , where $q=N/s$ and s is a positive integer and $q>s$. Therefore the primitive polynomials can be classified into the same class, if the nonmaximum length sequences are the same under the sampling of every s bits from the original M-sequences.

Using this classification, it is shown that the crosscorrelation between the M-sequences in the same class is larger than that of other M-sequences. The crosscorrelation function is obtained by the weights of the nonmaximum length sequences. And the maximum crosscorrelation value appears at the delay time of an integral multiple of q , when the two M-sequences are relatively phased so as for the initial points characteristic M-sequences to coincide, and then the crosscorrelation function is calculated with the delay taken from that phase.

The upper bounds of the crosscorrelation function of different M-sequences in case of $s=5$ and 7 are obtained.

Key Words: M-sequence, polynomial over GF(2), crosscorrelation

† 第 22 回計測自動制御学会学術講演会で発表 (昭 58・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 January 23, 1984)

(Revised June 18, 1984)

1. ま え が き

通信や計測制御で使用される符号系列に必要な性質の一つとして、異なる符号間では低い相互相関をもつということがあげられる。そのような符号として M 系列を用いる場合、等周期の特性多項式の異なる M 系列同士の相互相関を調べておく必要がある。ある特定の M 系列の組合せについては、低い相互相関をもつことが知られているが¹⁾、多数の等周期の異なる M 系列について、相互相関の大きい M 系列の組合せから小さい組合せへと分類して、相互相関を一般的に求める方法はいまだ知られていなかった。そこで著者らは M 系列の周期 $N=2^n-1$ (n は正整数) が素数でなければ、M 系列は N の約数 $q=N/s$ ($q>s$, s は N の素因数とする) を周期とする非極大系列を s 個組合せて構成されることに着目し、同じ非極大系列をもつか否かによって M 系列を分類し、分類された同じクラスの M 系列同士の相互相関はその他の M 系列同士より顕著に現れることを示した²⁾。相互相関は M 系列を構成している非極大系列の周期 q が長いほど大きくなるので、周期 N を素因数分解して s が小さいほうから順に M 系列をクラスに分類しておけば、相互相関の大きいほうから順に調べることができる。最小の s は 3 であり、その場合の相互相関値については理論的に求めた²⁾。 $s=3$ のつぎに相互相関の大きい組合せは 5、ならびに 7 である。これらについても明確に相互相関値を求めておく必要がある。周期 N の素因数として $s=3, 5, 7$ を含む M 系列の特性多項式の次数 n は、256 次までに約 80% ある。したがってかなりの異なる周期をもつ M 系列の相互相関を調べることができる。

本論文は $s=5$ と 7 の場合の M 系列の分類において、同じクラスの M 系列同士の相互相関値の上限値を示したものである。 $s=3$ の場合と相互相関値を求める基本的考え方は同じであるが、相互相関値を求める過程で、同じクラスの M 系列が共有する非極大系列の重み

分布の相違や、相互相関系列を構成する非極大系列の組合せが異なるため、理論式の導出方法に工夫を加えたものである。

2. 同じクラスの異なるM系列の相互相関²⁾

2元M系列 $\{g_k\}$, $k=0, 1, 2, \dots$, $g_k \in GF(2)$ において、同じクラスの異なるM系列 $\{g_{ak}\}$, $\{g_{bk}\}$ (a, b は N と互いに素な正整数) にはつぎの関係がある。

$$b = a + qc \pmod{N} \quad (2.1)$$

ここで $q = N/s$ で、 c は $0 < c \leq s-1$ の正整数とする。また $a=1$ としても一般性を失わないので、特に指定しないかぎり今後 $a=1$ として扱う。M系列 $\{g_k\}$ と $\{g_{bk}\}$ との間の相互相関系列 $C_{ab}(X, l)$ を次式で定義する。

$$C_{ab}(X, l) = \sum_{k=0}^{N-1} c_{k,l} X^k, \quad c_{k,l} \in GF(2) \quad (2.2.1)$$

ここで $c_{k,l} = g_{k-l} + g_{bk} \pmod{2}$, l は遅れ定数, $0 \leq l \leq N-1$ である。このように相互相関系列を定義すると、M系列 $\{g_k\}$ と $\{g_{bk}\}$ の一周期にわたる相互相関関数 $\Phi_{ab}(l)$ は、

$$\Phi_{ab}(l) = \sum_{k=0}^{N-1} (-1)^{c_{k,l}} \quad (2.2.2)$$

となる。またガロア体 $GF(2^n)$ の元 x の $GF(2)$ へのトレースを $T_n(x)$ と記し、つぎのように定義する。

$$T_n(x) = x + x^2 + \dots + x^{2^{n-1}}, \quad x \in GF(2^n)$$

ここで $T_n(x) \in GF(2)$ となる。M系列 $\{g_k\}$ を特性M系列 ($\{g_k\} = \{g_{2k}\}$) を満足し、特定の初期値によって発生されたM系列) の初期値にとれば、トレースを用いて、

$$g_k = T_n(\alpha^{-k}) \quad (2.3.1)$$

と書ける⁴⁾。ここで α はM系列 $\{g_k\}$ を発生する特性多項式の根とする。またもとのM系列 $\{g_k\}$ を s 個ごとにサンプルして得られる系列 (周期 q の非極大系列となる) を $\{f_{j,i}\}$, $0 \leq i \leq q-1$, $0 \leq j \leq s-1$ とすると、 $f_{j,i} = g_{is+j}$ であるから、(2.3.1)式で $k = is+j$ とおいて、

$$f_{j,i} = T_n(\beta^{-i} \alpha^{-j}), \quad \beta = \alpha^s \quad (2.3.2)$$

となる。系列 $\{f_{j,i}\}$ の特性多項式は根 β をもち、 j が異なると異なる系列である。よって逆にもとのM系列 $\{g_k\}$ は、 s 個の異なる系列 $\{f_{j,i}\}$ で構成することもできる。(2.1)と(2.3)式を(2.2.1)式へ代入して、

$$C_{ab}(X, l) = \sum_{j=0}^{s-1} \left[\sum_{i=0}^{q-1} T_n \{ \beta^{-i} \alpha^{-j} (\alpha^i + \alpha^{-qcj}) \} x^i \right] X^j, \quad x = X^s \quad (2.4)$$

となる。(2.4)式のトレースの項は各 j , $0 \leq j \leq s-1$ についてつぎのように書ける。

$$\alpha^{l-j} + \alpha^{-(qcj+j)} = \alpha^{-\lambda}, \quad \lambda = *, 0, 1, \dots, N-1 \quad (2.5.1)$$

ここで $\alpha^* = 0$ とし、右辺が0となるのは遅れ l が $l = -qcj \pmod{N}$ となる場合である。また、

$$st + \zeta = \lambda, \quad t = *, 0, 1, \dots, q-1, \quad \zeta = *, 0, 1, \dots, s-1 \quad (2.5.2)$$

とおく。ここで $\lambda = *$ のとき $t = \zeta = *$ とする。よって(2.4)式のトレースの項は(2.5.1)式と(2.5.2)式から、

$$T_n \{ \beta^{-i} \alpha^{-j} (\alpha^i + \alpha^{-qcj}) \} = T_n \{ \beta^{-(i+t)} \alpha^{-\zeta} \} \quad (2.5.3)$$

となる。ここで $\beta^* = 0$ とする。よって(2.5.3)式は、 $\zeta = *$ のとき0であり、 $\zeta \neq *$ のときは(2.3.2)式と同じ非極大系列の要素 $f_{\zeta, i+t}$ を表わしている。 ζ は(2.5.1)式と(2.5.2)式よりわかるように j に依存するので、 $f_{\zeta, i+t}$ を $f_{\zeta(j), i+t}$ と記すこととすると(2.4)式は、

$$C_{ab}(X, l) = \sum_{j=0}^{s-1} \left(\sum_{i=0}^{q-1} f_{\zeta(j), i+t} x^i \right) X^j \quad (2.6)$$

となる。系列 $\{f_{\zeta(j), i+t}\}$ は $\zeta = *$ のとき、すべての要素が0の長さ q の0系列となり、 $\zeta \neq *$ のときは s 個の異なる非極大系列 $\{f_{j,i}\}$ のいずれかと同じ系列である。また系列 $\{f_{\zeta(j), i+t}\}$ は系列 $\{f_{\zeta(j), i}\}$ と位相が t だけずれたものであるが同じ重み (一周期の系列での要素1の個数) をもつので、(2.6)式の $f_{\zeta(j), i+t}$ を $f_{\zeta(j), i}$ に置き換えて、(2.2.2)式の相互相関関数 $\Phi_{ab}(l)$ は次式のように書ける。

$$\begin{aligned} \Phi_{ab}(l) &= \sum_{j=0}^{s-1} \left(\sum_{i=0}^{q-1} (-1)^{f_{\zeta(j), i}} \right) \\ &= \sum_{j=0}^{s-1} (q - 2W_{\zeta(j)}) \end{aligned} \quad (2.7)$$

ここで $W_{\zeta(j)}$ は系列 $\{f_{\zeta(j), i}\}$ の重みとする。なお前述の s 個の非極大系列 $\{f_{j,i}\}$ の重みを W_j と記すと、 $\zeta = *$ のときは0系列であるから $W_{\zeta(j)} = 0$ となり、 $\zeta \neq *$ のとき $W_{\zeta(j)}$ は W_j のいずれかと一致する。

よって同じクラスの異なるM系列同士の相互相関値を求めるには、まず非極大系列 $\{f_{j,i}\}$ の重み W_j を調べ、つぎに(2.6)式の相互相関系列中の系列 $\{f_{\zeta(j), i}\}$, $0 \leq j \leq s-1$, が非極大系列 $\{f_{j,i}\}$ と0系列のどのような組合せになっているかを(2.5)式によって求め、それらの結果を(2.7)式へ代入して求めればよい。したがって遅れ l が、 $l = -qcj \pmod{N}$ のときは、相互相関系列の s 個の系列 $\{f_{\zeta(j), i}\}$ のうち1個が0系列となって、(2.7)式の相互相関値は正方向へ大きく偏ることとなる。このような遅れ l の位置で相互相関値の上限値が現れる。

2.1 $s=5, 7$ の場合における非極大系列の重み分布

M系列を特性M系列の位相にとると、 $s=5$ の場合は $s=3$ の場合²⁾と同様に5を法とする j の剰余類が $C_0 = \{0\}$ と $C_1 = \{1, 2, 3, 4\}$ の2組しか存在しないため $\{f_{j,i}\}$ 系列は2種類の異なる重み W_0 と $W_j, 1 \leq j \leq 4$ をもつ。 W_0 と W_j は以下ようになる。なお N の素因数として $s=5$ をもつのは $4|n$ のときであり、 $8\chi n$ のときは $5|2^{n/2}+1$ となり、 $8|n$ のときは $5|2^{n/2}-1$ となる。したがって、 $8\chi n$ のとき

$$W_0 = \frac{2^{n-1} - 2^{n/2+1}}{5}, \quad W_j = \frac{2^{n-1} + 2^{n/2-1}}{5} \quad (2.8)$$

$8|n$ のとき

$$W_0 = \frac{2^{n-1} + 2^{n/2+1}}{5}, \quad W_j = \frac{2^{n-1} - 2^{n/2-1}}{5} \quad (2.9)$$

となる。 $a|b$ は a が b の約数であることを示す記号とする。また $a\chi b$ は a が b の約数でないことを示す記号とする。

つぎに $s=7$ の場合について考えてみよう。7を法とする正整数の剰余類はつぎの3組となる。

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 2, 4\} \\ C_3 &= \{3, 6, 5\} \end{aligned} \quad (2.10)$$

よって7個の異なる非極大系列において、3種類の異なる重み、すなわち $W_0, W_1 (=W_2, W_4), W_3 (=W_5, W_6)$ をもつ。すなわち特性M系列 $\{g_k\}$ を、要素 g_0 より始めて7個ごとにサンプルして得られる系列 $\{f_{0,i}\}$, g_1 より始めて得られる系列 $\{f_{1,i}\}$, および g_3 より始めて得られる系列 $\{f_{3,i}\}$ の3組の異なる系列の重みである。非極大系列 $\{f_{j,i}\}$ の重みの順序 W_j を基準にすると、異なる原始元 α^η (η は $\eta \neq 2^m, m=0, 1, 2, \dots, n-1$ の N と互いに素な正整数) を根とする原始多項式により発生されたM系列より得られる非極大系列の重みは7を法として、 $\eta \in C_1$ のときは $C_1\eta \in C_1, C_3\eta \in C_3$ となるので、重みの順序は $W_0, W_1, W_1, W_3, W_1, W_3, W_3$ となる。 $\eta \in C_3$ のときは $C_1\eta \in C_3, C_3\eta \in C_1$ となるので、重みの順序は $W_0, W_3, W_3, W_1, W_3, W_1, W_1$ となって W_1 と W_3 の位置が入れかわる。ここでこれらの異なる重み W_0, W_1, W_3 を一般的に求める方法について述べよう。第1の方法として、もとのM系列 $\{g_k\}$ を発生し、そのサンプル系列 $\{f_{j,i}\}$ から実験的に重みを求めることである (W_0, W_1, W_3 はもとのM系列 $\{g_k\}$ を7個ごとにサンプルして得られた系列 $\{f_{0,i}\}, \{f_{1,i}\}, \{f_{3,i}\}$ の重みである)。第2の方法は、非極大系列 $\{f_{j,i}\}$ の特性多項式を用いて直接系列 $\{f_{j,i}\}$ を発生し重みを求めることである。第2の方法について説明する。(2.3.2)式からわかるように

非極大系列 $\{f_{j,i}\}$ の特性多項式は根 β をもつ。根 β をもつ $GF(2)$ 上 n 次の既約多項式 $r(x)$ を系列 $\{f_{j,i}\}$ の特性多項式としよう。そこで(2.3.2)式を用いて系列 $\{f_{j,i}\}$ をつぎのような発生関数で表わすこととする。

$$f_j(x) = \sum_{i=0}^{q-1} f_{j,i} x^i = \sum_{i=0}^{q-1} T_n(\beta^{-i} \alpha^{-j}) x^i \quad (2.11.1)$$

ここで $j=0$ のとき、 $f_0(x)$ は $f_0(x)=f_0(x)^2$ の性質をもつ (特性M系列と同じく系列 $\{f_{j,i}\}$ の特性系列 $\{f_{0,i}\}$ を意味する)。このような $f_0(x)$ は特性多項式 $r(x)$ を用いてつぎのように表わせる⁴⁾。

$$f_0(x) = (1+x^q) \left(\frac{x r'(x)}{r(x)} + u \right) \quad (2.11.2)$$

ここで $r'(x)$ は $r(x)$ の導関数であり、 u は $r(x)$ の次数 n が偶数のときは0、奇数のときは1をとる。上式より $f_0(x)$ がわかればそのほかの $f_j(x), 1 \leq j \leq 6$ は(2.11.1)式より、

$$f_j(x) = f_0(x) \cdot \alpha^{-j}(x) \quad (2.11.3)$$

となる。ここで $\alpha^{-j}(x)$ は元 $\alpha^{-j} \in GF(2^n)$ を x の関数として表わしたものである。よって発生関数 $f_0(x), f_1(x), f_3(x)$ によって系列 $\{f_{0,i}\}, \{f_{1,i}\}, \{f_{3,i}\}$ を発生して重みを求めるとよい。しかしさらに容易な方法がある。(2.11.2)式 $f_0(x)$ によって系列 $\{f_{0,i}\}$ の重み W_0 が求まれば、 W_1 と W_3 はつぎのように求めることができる。(2.11)式で表わされる非極大系列 $\{f_{j,i}\}$ の発生関数 $f_j(x)$ と長さ q の0系列は、符号長 q 、情報点数 n の (q, n) 符号である。これらの符号は異なる重み W_0, W_1, W_3 と重み0をもっている。その双対符号 $(q, q-n)$ の最小重みは3であることから、ある重みをもつ符号の数とその重みとの積和がその符号と双対符号とで等しいことを表わすMacWilliamsの定理⁴⁾を用いて次式が成立する。

$$\begin{aligned} 1 + qy^{W_0} + 3qy^{W_1} + 3qy^{W_3} \\ = 2^{n-q} \{(1+y)^q + A'_3(1+y)^{q-3}(1-y)^3 + \dots\} \end{aligned}$$

ここで $q=N/7, A'_3$ は $(q, q-n)$ 符号の重み3をもつ符号数を示す。よって上式で W_0 が既知であるならば、 W_1, W_3 は上式より次式のように表わされる。

$$\begin{aligned} W_1 &= \frac{(2^{n-1} - W_0) + \sqrt{2^n W_0 - 7W_0^2 - 2^{n-2}(q-5)}}{6} \\ W_3 &= \frac{(2^{n-1} - W_0) - \sqrt{2^n W_0 - 7W_0^2 - 2^{n-2}(q-5)}}{6} \end{aligned} \quad (2.12)$$

Table 1 に $s=5$ の場合の非極大系列 $\{f_{j,i}\}$ の異なる重み W_0, W_1 を(2.8), (2.9)式で求めた一例を示し、**Table 2** に $s=7$ の場合の非極大系列の異なる重み W_0, W_1, W_3 を前述の第1および第2の方法によ

Table 1 Weight distribution in case of $s=5$

degree (n)	weight, W_j	
	$j=0$	$j=1, 2, 3, 4$
8	32	24
12	384	416
16	6656	6528
20	104448	104960
24	1679360	1677312

Table 2 Weight distribution in case of $s=7$

degree (n)	weight, W_j		
	$j=0$	$j=1, 2, 4$	$j=3, 5, 6$
9	28	36	40
12	296	280	304
15	2416	2320	2336
18	18848	18784	18624
21	149440	149632	150080
24	1196672	1198848	1198464

て求めた一例を示す。ここで $s=7$ の場合、M 系列によって重み W_1 と W_3 が入れかわることについては前に述べた。

ほかに非極大系列の重み W_j について、たとえば $s=7$ の場合、McElice らが Davenport-Hasse の理論を用いて理論的に求めている⁵⁾し、McWilliams らは計算機を用いて種々の s について重み分布を求めている⁶⁾。

2.2 $s=5$ の場合における、遅れが q の整数倍での相互相関値

$q=N/5$, $l=-qce$, $0 \leq e \leq 4$ として (2.4) 式に代入すると次式のようになる。ただしトレースの項のみを示すことにする。

$$T_n\{\beta^{-i}\alpha^{-j}\gamma^{-qce}(1+\alpha^{-qc(j-e)})\} \quad (2.13)$$

ここで $\beta=\alpha^5$ とする。そこで $\gamma=\alpha^{q/3}$ ($2|n$ であるため q は因数として 3 を含んでいる) とすると、

$$T_n\{\beta^{-i}\alpha^{-j}\gamma^{-3ce}(1+\gamma^{-3c(j-e)})\} \quad (2.14)$$

となる。もちろん $j=e$ のときはトレースの値が 0 となる。 $j \neq e$ のときはつぎのようになる。

$$c(j-e) \equiv 2^e, \quad e=0, 1, 2, 3 \pmod{5} \quad (2.15)$$

となるので、(2.14) 式に代入すれば、

$$T_n\{\beta^{-i}\alpha^{-j}\gamma^{-3ce}(1+\gamma^{-3c2^e})\} \quad (2.16)$$

となる。ここで γ の位数は 15 であるから、 $GF(2)$ 上で指標 15 の既約多項式は 2 個存在し、 X^4+X+1 と X^4+X^3+1 である。よってこの二つの既約多項式に分

けて (2.16) 式を解くことにする。

(1) $1+\gamma+\gamma^4=0$ のとき

$$T_n\{\beta^{-i}\alpha^{-j}\gamma^{-3ce-2^e+2}\} \quad (2.17)$$

$$= T_n\{\beta^{-i}\alpha^{-(3q'ce+4 \cdot 2^e q' + j)}\} \quad (2.18)$$

ここで $q'=q/3$ とする。(2.18) 式の α のべきのみに注目して (2.5) 式の ζ を決定しよう。

$$\begin{aligned} 3q'ce+4 \cdot 2^e q' + j &= 5t + \zeta \\ \zeta &\equiv 3q'ce+4 \cdot 2^e q' + j \pmod{5} \end{aligned} \quad (2.19)$$

ここで $q' \pmod{5}$ を求めてみよう。 $s=5$ のとき $n=4n'$ ($n'=1, 2, \dots$) と表わせるので、 $q'=(2^{4n'}-1)/(2^4-1)$ となる。したがって $q' \equiv n' \pmod{5}$ となる。よって (2.19) 式は次式となる。

$$\zeta \equiv 3n'ce+4 \cdot 2^e n' + j \pmod{5} \quad (2.20)$$

(2) $1+\gamma^3+\gamma^4=0$ のとき

$$\begin{aligned} T_n\{\beta^{-i}\alpha^{-j}\gamma^{-3ce+2^e}\} \\ = T_n\{\beta^{-i}\alpha^{-(3q'ce-2^e q' + j)}\} \end{aligned} \quad (2.21)$$

(2.18) 式と (2.21) 式の α のべきを 5 を法として比較すると等しくなるので、 ζ は γ を根としてもつ既約多項式に依存しないで求めることができる。ここで逆に (2.20) 式の 2^e に $c(j-e)$ を代入すると次式となる。

$e=0$ のとき

$$\zeta \equiv j(cn+1) \pmod{5}$$

$e \neq 0$ のとき

$$\zeta \equiv cen+j(cn+1) \pmod{5} \quad (2.22)$$

ただし $j=e$ は上記計算より省く。よって $l=-qce$ の遅れに対しては (2.22) 式によって、各 j に対して ζ を容易に算出することができるので、非極大系列 $\{f_{i(j)}, i\}$ の組合せを知ることができる。それと (2.8), (2.9) 式で表わされる $\{f_{i,j}\}$ の重み W_j から (2.7) 式によって相互相関値は得られる。

$5|q'$ ($5|n'$) となる、たとえば $n=20, 40$ などの場合は (2.19) 式よりわかるように $\zeta=j$ となり、(2.7), (2.8), (2.9) 式より容易に相互相関値を求めることができる。よって次式のようになる。

$8 \nmid n$ のとき

$$\Phi_{ab}(0) = N - \frac{1}{5}(2^{n+2} + 2^{(n/2)+2}) \quad (2.23)$$

$$\Phi_{ab}(q\sigma) = N - \frac{1}{5}(2^{n+2} - 2^{(n/4)+2} + 3 \cdot 2^{(n/2)}) \quad (2.24)$$

$$\sigma=1, 2, 3, 4$$

$8|n$ のとき

$$\Phi_{ab}(0) = N - \frac{1}{5}(2^{n+2} - 2^{(n/2)+2}) \quad (2.25)$$

$$\Phi_{ab}(q\sigma) = N - \frac{1}{5}(2^{n+2} + 2^{(n/2)+2} - 3 \cdot 2^{(n/2)}) \quad (2.26)$$

$$\sigma=1, 2, 3, 4$$

なお $5|q'$ のときには, $8|n$ のとき (2.25) 式で表わされる相互相関値が $\text{Max.}\Phi_{ab}(l)$ となる. このときの非極大系列 f_i (非極大系列 $\{f_{i(j),i}\}$ は j を特に指定しないとき f_i と記す. また特に 0 系列となる場合は 0 と記す) の組合せは $\{0, f_1, f_1, f_1, f_1\}$ である. また $8|n$ のときの相互相関値の最大は $\{0, f_0, f_0, f_0, f_0\}$ の組合せで起こり (2.7), (2.8) 式より次式となる.

$8|n$ のとき

$$\text{Max.}\Phi_{ab}(l) = N - \frac{1}{5}(2^{n+2} - 2^{(n/2)+4}) \quad (2.27)$$

もちろん $5|q'$ のときの最大相互相関値は, $8|n$ では (2.24) 式, $8|n$ では (2.25) 式となる. **Table 3** に $s=5$ の場合における q の整数倍での遅れに対する相互相関値を示す. これは (2.22) 式より ζ を求め, Table 1 の重みを用いて (2.7) 式により相互相関値を求めた結果である. 表中 2 列目は相互相関をとるべき同じクラスの M 系列の組合せであるが, それらの M 系列を発生する $GF(2)$ 上 n 次の原始多項式の根の組合せで示している. たとえば $C_0 - C_i$ (i は $1 \leq i \leq 4$ の正整数) とは, $GF(2^n)$ 上のある原始元を α^{C_0} とすると,

$$C_i = \min_k \{(C_0 + qi)2^k\} \pmod{N} \quad (2.28)$$

Table 3 Cross-correlation value between C_0 and C_i in case of $s=5$

degree (N: length)	$C_0 - C_i$	C. C. V., $\Phi(l)$ delay, $l = (N/5)\sigma$		MAX., $\Phi(l)/N$
		$\sigma=0$	$\sigma=1, 2, 3, 4$	
8 (255)	$C_0 - C_1$	63	47	0.2471
	$C_0 - C_2$	63	47	
	$C_0 - C_3$	-1	63	
12 (4095)	$C_0 - C_2$	1023	767	0.2498
	$C_0 - C_3$	767	831	
	$C_0 - C_4$	767	831	
16 (65535)	$C_0 - C_1$	13311	13055	0.2031
	$C_0 - C_3$	13311	13055	
	$C_0 - C_4$	12287	13311	
20 (1048575)	$C_0 - C_1$	208895	209919	0.2002
	$C_0 - C_2$	208895	209919	
	$C_0 - C_3$	208895	209919	
	$C_0 - C_4$	208895	209919	
24 (16777215)	$C_0 - C_1$	3342335	3358719	0.2002
	$C_0 - C_2$	3358719	3354623	
	$C_0 - C_4$	3358719	3354623

Fig. 1 Cross-correlation of Ma and Mb
Ma: primitive poly. = $X^8 + X^4 + X^3 + X^2 + 1$
initial value = 00010110
Mb: primitive poly. = $X^8 + X^6 + X^3 + X + 1$
initial value = 01101100

となる元, α^{C_0} と α^{C_i} を意味する. ただし $GCD(C_i, N)=1$ とする. a と b の最大公約数が c であることを $GCD(a, b)=c$ と記すこととする. すなわち α^{C_0} と α^{C_i} を根とする同じクラスの異なる二つの原始多項式より発生された M 系列同士の相互相関を意味している.

Fig. 1 に同じクラスの 8 次の原始多項式より発生された M 系列同士の相互相関関数の一例を示す. 図中の相関値は周期 N で規準化している. q の整数倍での遅れに対する相互相関値は Table 3 の理論的考察と一致している.

2.3 $s=7$ の場合における, 遅れが q の整数倍での相互相関値

$q=N/7$, $l=-qce$, $0 \leq e \leq 6$ として (2.4) 式に代入し, トレースの項のみを示すと (2.13) 式となる. ただし $\beta=\alpha^7$ とする. そこで $\delta=\alpha^q$ とすると,

$$T_n \{ \beta^{-i} \alpha^{-j} \delta^{-ce} (1 + \delta^{-c(j-e)}) \} \quad (2.29)$$

となる. よって $c(j-e)$ をつぎの二つの場合に分けて (2.29) 式を解いてみよう.

(1) $c(j-e) \equiv 2^e$, $\tau=0, 1, 2 \pmod{7}$ のとき,

$$T_n \{ \beta^{-i} \alpha^{-j} \delta^{-ce} (1 + \delta^{-1})^{2^e} \} \quad (2.30)$$

となる.

(2) $c(j-e) \equiv 3 \cdot 2^e$, $\tau=0, 1, 2 \pmod{7}$ のとき

$$T_n \{ \beta^{-i} \alpha^{-j} \delta^{-ce} (1 + \delta^{-3})^{2^e} \} \quad (2.31)$$

となる. ここで δ の位数は 7 であり, よって $GF(2)$ 上で指標 7 の既約多項式は 2 個存在し, $X^3 + X + 1$ と $X^3 + X^2 + 1$ である. よってこの二つの既約多項式に分けて (2.30), (2.31) 式を解くことにする.

(A) $1 + \delta + \delta^3 = 0$ のとき

(2.30) 式より,

$$\begin{aligned} T_n \{ \beta^{-i} \alpha^{-j} \delta^{-ce} (1 + \delta^3)^{2^e+1} \} \\ = T_n \{ \beta^{-i} \alpha^{-j} \delta^{-ce+2^e+1} \} \end{aligned} \quad (2.32)$$

となる. また (2.31) 式より,

$$T_n \{ \beta^{-i} \alpha^{-j} \delta^{-ce-2^e+1} \} \quad (2.33)$$

となる.

(B) $1+\delta^2+\delta^3=0$ のとき

(2.30)式より,

$$\begin{aligned} T_n \{ \beta^{-i} \alpha^{-j} \delta^{-ce} (1+\delta^3)^{2^c+1} \} \\ = T_n \{ \beta^{-i} \alpha^{-j} \delta^{-ce+2^c+2} \} \end{aligned} \quad (2.34)$$

となる。また(2.31)式より,

$$T_n \{ \beta^{-i} \alpha^{-j} \delta^{-ce-2^c} \} \quad (2.35)$$

となる。

そこで α のべきにのみ注目して ζ を求めてみると,

(A) の場合は(2.32)式より,

$$\begin{aligned} \zeta &\equiv qce - 2 \cdot 2^c q + j \pmod{7} \\ &\equiv cen' + 5 \cdot 2^c n' + j \pmod{7} \end{aligned} \quad (2.36)$$

となる。ここで $q \equiv n' = n/3 \pmod{7}$ とおいた。 $c(j-e) \equiv 2^c \pmod{7}$ なので(2.36)式は,

$$\zeta \equiv 3cen' + j(5cn' + 1) \pmod{7} \quad (2.37)$$

となる。 $c(j-e) \equiv 3 \cdot 2^c \pmod{7}$ のときは, (2.33)式より,

$$\begin{aligned} \zeta &\equiv cen' + 2 \cdot 2^c n' + j \pmod{7} \\ &\equiv 5cen' + j(3cn' + 1) \pmod{7} \end{aligned} \quad (2.38)$$

となる。(B)の場合, $c(j-e) \equiv 2^c \pmod{7}$ のとき, (2.34)式から ζ を求めると(2.38)式と等しくなり, $c(j-e) \equiv 3 \cdot 2^c \pmod{7}$ のとき, (2.35)式から ζ を求めると(2.37)式と等しくなる。なお $7|q$ ($7|n'$)となる。たとえば $n=21, 42$ など)のときは(2.37), (2.38)式より $\zeta=j$ となり容易に非極大系列の組合せを知ることができる。一般的には(2.37), (2.38)式を用いて, 各 j に対する ζ を求めることによって非極大系列の組合せを知らなければならない。よって Table 2 にあるような非極大系列の重みが与えられると, (2.7)式により相互相関値を求めることができる。Table 4 に q の整数倍の遅れに対する相互相関値を示す。これは(2.37), (2.38)式より各 j に対する ζ を求め, Table 2 の重みと(2.7)式を用いて求めた結果である。Fig. 2 に同じクラスの9次の原始多項式より発生されるM系列同士の相互相関関数の一例を示す。 q の整数倍の遅れ

Fig. 2 Cross-correlation of Ma and Mb

Ma: primitive poly. = $X^9 + X^4 + 1$

initial value = 100000000

Mb: primitive poly. = $X^9 + X^6 + X^5 + X^3 + X^2 + X + 1$

initial value = 111110101

Table 4 Cross-correlation value between C_0 and C_i in case of $s=7$

degree (N: length)	$C_0 - C_i$	C. C. V., $\phi(l)$ delay, $l=(N/7)\sigma$			MAX., $\phi(l)/N$
		$\sigma=0$	$\sigma=1, 2, 4$	$\sigma=3, 5, 6$	
9 (511)	$C_0 - C_1$	79	95	47	0.2016
	$C_0 - C_3$	103	47	87	
	$C_0 - C_4$	31	95	63	
	$C_0 - C_5$	79	47	95	
	$C_0 - C_6$	103	47	87	
12 (4095)	$C_0 - C_1$	639	639	511	0.1795
	$C_0 - C_2$	447	639	575	
	$C_0 - C_3$	735	575	543	
	$C_0 - C_4$	639	639	511	
	$C_0 - C_6$	447	575	639	
15 (32767)	$C_0 - C_1$	4735	4479	4863	0.1504
	$C_0 - C_2$	4927	4479	4799	
	$C_0 - C_3$	4927	4799	4479	
	$C_0 - C_4$	4255	4799	4703	
	$C_0 - C_6$	4255	4799	4703	
18 (262143)	$C_0 - C_2$	38655	37119	37375	0.1475
	$C_0 - C_3$	37311	38015	36927	
	$C_0 - C_4$	36735	37119	38015	
	$C_0 - C_5$	37311	38015	36927	
	$C_0 - C_6$	36735	38015	37119	
21 (2097151)	$C_0 - C_1$	298879	299263	300159	0.1431
	$C_0 - C_2$	298879	299263	300159	
	$C_0 - C_3$	298879	300159	299263	
	$C_0 - C_4$	298879	299263	300159	
	$C_0 - C_5$	298879	300159	299263	
24 (16777215)	$C_0 - C_1$	2391039	2394111	2401279	0.1434
	$C_0 - C_2$	2406399	2394111	2396159	
	$C_0 - C_3$	2391039	2401279	2394111	
	$C_0 - C_4$	2406399	2394111	2396159	
	$C_0 - C_5$	2395647	2401279	2392575	

に対する相互相関値は Table 4 の理論的考察と一致している。

3. あとがき

周期が素数でない異なる特性多項式をもつM系列の

相互関数が原始多項式を分類することによって理論的に求められることを示した。

分類された同一クラスの異なる原始多項式より発生されたM系列同士の相互相関は、その相互相関系列を構成する非極大系列の組合せと、その重み分布を知ることによって理論的に求められることを示した。

M系列の周期 N の素因数 $s=3$ の場合について相互相関値の理論値とその上限値を発表してあるが²⁾、 $s=5, 7$ についても同様の方法により、遅れが q の整数倍の相互相関値は理論的に求めることができることを示し、相互相関値の上限値を求めた。 s が11以上の素数についても、同様の方法で相互相関の上限値を理論的に求めることが可能であるが、 s が大きくなると(2.6)式の f_{min} を求めることが煩雑になること、および256次までのM系列について最小の素因数 s が11以上になる場合は約2割しかないことを考えると、 $s=7$ まで求めておけば実用上十分と考えられる。

参 考 文 献

- 1) 森内, 柏木: 異なる特性多項式をもつM系列の相互相関, 第22回 SICE 学術講演会予稿集, 311/312 (1983)
- 2) 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)
- 3) F. Surböck and H. Weinrichter: Interlacing Properties of Shift-Register Sequences with Generator Polynomials Irreducible over $GF(p)$, IEEE Trans. on Information Theory, **IT-24-3**, 386/389 (1978)
- 4) F. J. Mac Williams and N. J. A. Sloane: The Theory of Error Correcting Codes, North Holland (1978)
- 5) R. J. McEliece and H. Rumsey: Euler Products, Cyclotomy, and Coding, J. Number Theory, **4**, 302/311 (1972)
- 6) J. Mac Williams and J. Seery: The Weight Distribution of Some Minimal Cyclic Codes, IEEE Trans. on Information Theory, **IT-27-6**, 796/806 (1981)
- 7) D. V. Sarwate and M. B. Pursley: Crosscorrelation Properties of Pseudorandom and Related Sequences, Proc. IEEE, **68-5**, 593/619 (1980)