異なる特性多項式をもつ M 系列の相互相関†

森 内 勉*・柏 木 潤**

Cross-Correlation of M-Sequences Having Different Characteristic Polynomials

Tsutomu MORIUCHI* and Hiroshi KASHIWAGI**

The cross-correlation of m-sequences which have the same period but different characteristic polynomials is shown theoretically.

When the order N of a primitive element α in $GF(2^n)$ is nonprime, it is represented by $N=sq$ (s, q , integer). Therefore an irreducible polynomial of degree n of exponent q with a root α^s must exist. If each root of the two different primitive polynomials is denoted as α^a, α^b , the primitive polynomials can be classified into a set of primitive polynomials in such a way that sa, sb modulo N belong to the same coset. This means that the two m-sequences are classified into the same class if they become the same sequence under the sampling of s bits.

By the use of characteristic m-sequences it is shown that the cross-correlation between the different m-sequences generated by primitive polynomials of the same class becomes large when the delay is an integral multiple of q . This is due to the fact that the cross-correlation sequence contains the non-maximum length sequences generated by its irreducible polynomial.

The cross-correlation values in case of $s=3$ are analyzed and obtained explicitly. The cross-correlation values actually obtained agree well with the theoretical ones.

Keyword: M-sequence, polynomial over $GF(2)$, cross-correlation

1. ま え が き

スペクトル拡散通信方式などで使用される変調符号は、明確な自己相関をもつと同時に、ほかの符号とは

低い相互相関をもつ必要がある。その符号として M 系列符号がよく知られているが、等周期の特性多項式の異なる M 系列同士の相互相関についてはあまり知られていない。ここでは周期 $N=2^n-1$ が素数でない場合の相互相関についていくつかの性質を明らかにしたので、その結果について述べる。

すなわち、 $GF(2^n)$ 上の位数 N が素数でない原始元を根とする原始多項式を特性多項式として発生される M 系列は、 N の約数 $q=N/s$ (s は正整数) を指標とする n 次既約多項式 (原始的でない) で発生される周期 q の非極大系列を s 個組合せて構成されている⁵⁾ ことに注目し、同じ非極大系列をもつか否かによって、原始多項式を分類することができることを示す。分類された同じクラスの中の異なる原始多項式によって発生される M 系列は、同じ非極大系列を含むため相互相関はほかの M 系列より顕著に現れる。またそれらの相互相関系列は非極大系列によって構成されていて、相互相関値は周期 q の非極大系列中の要素 1 の個数 (重み) によって求められることを示す。そして特性 M 系列を用いて相互相関関数を求めると、 q の整数倍の遅れにおいて相互相関の最大値が現れることを示す。

M 系列の相互相関について Gold^{3) 4)} は、原始多項式の奇数次数について相互相関値が 3 値となる特定の M 系列の組合せを示し、さらに符号の最小重みの立場より、低い相互相関をもつ M 系列の組合せを、奇数と、4 の倍数を除く偶数次数について示している。後者は最適な相互相関特性をもつクラスの M 系列を探索する場合有効である。本論は、周期が素数でない場合について、Gold とは逆に、相互相関の値が最も大きい組合せを調べることによって、異なる特性多項式をもつ M 系列の相互相関値の上限を調べた。

2. 原始多項式の分類

$GF(2^n)$ 上の原始元を α とすると、その位数 N は、 2^n-1 であるが、 N が素数でなければ因数分解されて $N=sq$ と表わせる。ここで $q>s$, $s>1$ とする。よ

† 第 21 回計測自動制御学会学術講演会で発表 (昭 57・7)

* 八代工業高等専門学校 八代市平山新町 2627

** 熊本大学工学部 熊本市黒髪 2-39-1

* Yatsushiro Technical College, Yatsushiro

** Faculty of Engineering, Kumamoto University, Kumamoto

(Received March 4, 1983)

(Revised July 6, 1983)

って位数 q の元 α^i を根にもつ最小多項式 $r(x)$ が存在して、その次数 m は $q|2^m-1$ を満足する最小値となる。 q を N に近くとるか、あるいは N の素因数の中の小さいほうより s を選べば $r(x)$ の次数は n となる。

ところで N の素因数 s と原始多項式の次数 n との関連は、 s が小さいところではつぎのようになる。偶数次数 $(2|n)$ のときは $2^2-1|2^n-1$ より、 N の素因数として 3 をもつ。 $3|n$ のときは $2^3-1|2^n-1$ より 7 をもつ。 さらに $4|n$ のときは $2^2+1|2^n-1$ より素因数 5 を含んでいる。 ここで $a|b$ は、 a が b の約数であることを示す記号とする。

さて、位数 N の原始元を根とする n 次の原始多項式の個数を P とし、位数 q の元を根とする n 次の既約多項式の個数を R とすれば、オイラ関数 ϕ を用いて、 $P=\phi(N)/n$, $R=\phi(q)/n$ であるから、次式で関係づけられる。

$$P=\rho \cdot R, \begin{cases} s^2|N \text{ のとき, } \rho=s \\ s^2 \nmid N \text{ のとき, } \rho=s-1 \end{cases} \quad (2.1)$$

ここに $a|b$ は、 a が b の約数でないことを示す記号とする。 よって、 P 個の原始多項式を ρ 個 1 クラスとして、 R 個の既約多項式でもって分類される。

そこで P 個の原始多項式の分類について考えてみる。 まず、ある原始多項式の根は原始元 α のベキで表わされるから、その一つの根はベキの最小値を C_0 として α^{C_0} と書ける。異なる原始多項式の根を同様に α^{C_i} としておいて、 N を法として sC_0, sC_i が同じ剰余類に属するような原始多項式の集合を一つのクラスとして分類することを考えよう。このことは、異なる原始多項式から発生されるM系列をおのおの s 個ごとにサンプルしたとき、同じ系列 (M系列でない) になるような原始多項式を一つのクラスとして分類することに相当する。

sC_0, sC_i が同じ剰余類に属するから、

$$\min(sC_i 2^k) = \min(sC_0 2^k), \text{ mod } N \quad (2.2)$$

$$= \min\{(sC_0 + Ni)2^k\} \quad (2.3)$$

となる。ここで、 $0 \leq k \leq n-1$, $0 < i \leq s-1$ とする。

そこで、両辺を s で割ると次式のようになる。

$$\min(C_i 2^k) = C_i = \min\{(C_0 + qi)2^k\}, \text{ mod } N \quad (2.4)$$

ゆえに C_i は (2.4) 式と、 $GCD(C_i, N)=1$ を満たさなければならない。このとき s 個または s

−1 個の $\alpha^{C_0}, \alpha^{C_i}, \alpha^{C_{s-1}}$ は同じクラスの異なる原始多項式の各根となる。したがって、同一クラスの原始多項式を求める手順はつぎのようになる。

(1) 基準となる剰余類首を N と互いに素な C_0 とし、(2.4) 式を用いて $C_i (0 < i \leq s-1)$ を算出する。ただし $GCD(C_i, N) \neq 1$ を省く。

(2) 原始元 α を根とする原始多項式を与えておいて、各元 α^{C_i} を根とする原始多項式を算出する^{10), 12)}。

この手順により $n=4, 6, 8, 10, s=3$ の場合について分類したものを **Table 1** に示す。表中では、多項式 $P(X)=1+X^i+X^j+X^k+\dots$ を、0 を除くベキの組 $(i, j, k, \dots)$ で表わしている。なお、クラスの共有する指標 q の既約多項式は α^{sC_0} を根とするので、手順 (2) によって求められる。また、前述のような同じクラスの二つの異なる原始多項式の根には指標 q の既約

Table 1 A classified example of primitive polynomials and an irreducible polynomial which they have in common in the same class

Degree	Primitive polynomials	Irreducible polynomial
4	(1, 4) (3, 4)	(1, 2, 3, 4)
6	(1, 6) (2, 3, 5, 6) (1, 4, 5, 6) (5, 6) (1, 2, 5, 6) (1, 3, 4, 6)	(1, 2, 4, 6) (2, 4, 5, 6)
8	(2, 3, 4, 8) (1, 6, 7, 8) (3, 5, 6, 8) (1, 5, 6, 8) (1, 2, 5, 6, 7, 8) (4, 5, 6, 7, 8) (1, 3, 5, 8) (2, 5, 6, 8) (2, 3, 7, 8) (2, 3, 5, 8) (1, 2, 3, 4, 6, 8) (1, 2, 3, 6, 7, 8) (3, 5, 7, 8) (2, 3, 6, 8) (1, 2, 7, 8) (4, 5, 6, 8)	(1, 2, 4, 5, 6, 8) (1, 3, 7, 8) (2, 3, 4, 5, 7, 8) (3, 4, 5, 6, 7, 8) (1, 5, 7, 8) (1, 3, 4, 5, 6, 8) (1, 2, 3, 4, 5, 8) (2, 3, 4, 7, 8)
10	(3, 10) (2, 3, 4, 8, 9, 10) (2, 3, 8, 10) (1, 2, 3, 4, 6, 7, 9, 10) (3, 4, 5, 6, 7, 8, 9, 10) (3, 4, 5, 6, 9, 10) (1, 2, 3, 5, 6, 10) (2, 3, 4, 5, 8, 10) (2, 3, 6, 8, 9, 10) (3, 7, 9, 10) (1, 3, 4, 5, 6, 7, 8, 10) (1, 2, 4, 5, 9, 10) (1, 3, 4, 10) (2, 4, 5, 7, 9, 10) (1, 5, 8, 10) (3, 4, 5, 8, 9, 10) (4, 5, 8, 10) (5, 8, 9, 10) (1, 4, 9, 10) (1, 2, 3, 4, 5, 6, 9, 10) (1, 5, 6, 8, 9, 10) (2, 3, 4, 5, 6, 7, 9, 10) (2, 5, 6, 7, 8, 10) (4, 5, 7, 8, 9, 10) (3, 4, 8, 10) (1, 6, 8, 10) (2, 4, 6, 8, 9, 10) (1, 2, 4, 8, 9, 10) (1, 2, 3, 7, 8, 10) (1, 4, 7, 8, 9, 10) (1, 4, 5, 6, 7, 8, 9, 10) (1, 6, 9, 10) (1, 4, 6, 7, 9, 10) (2, 3, 4, 5, 6, 8, 9, 10) (1, 2, 6, 8, 9, 10) (1, 2, 4, 6, 8, 10) (1, 2, 5, 6, 7, 10) (2, 5, 9, 10) (1, 2, 6, 7, 8, 10) (7, 10) (1, 2, 4, 6, 7, 10) (5, 7, 8, 10) (2, 5, 6, 10) (1, 2, 5, 10) (2, 3, 5, 10) (3, 4, 6, 8, 9, 10) (1, 2, 4, 5, 6, 7, 8, 10) (1, 3, 4, 6, 9, 10) (6, 7, 9, 10) (1, 3, 5, 6, 8, 10) (1, 2, 3, 5, 5, 6, 7, 10) (3, 4, 5, 6, 7, 10) (2, 4, 9, 10) (2, 6, 7, 10) (2, 3, 7, 8, 9, 10) (1, 2, 3, 6, 9, 10) (1, 3, 4, 6, 7, 8, 6, 10) (2, 7, 8, 10) (1, 3, 7, 10) (1, 2, 4, 7, 8, 10)	(1, 2, 3, 10) (1, 3, 5, 7, 8, 10) (1, 3, 5, 6, 7, 8, 9, 10) (4, 5, 8, 10) (1, 2, 5, 6, 8, 10) (4, 6, 9, 10) (6, 7, 8, 10) (1, 2, 3, 4, 8, 10) (3, 6, 7, 10) (1, 2, 7, 8, 9, 10) (1, 4, 6, 10) (4, 8, 9, 10) (1, 2, 3, 5, 7, 10) (2, 3, 5, 6, 7, 10) (1, 2, 4, 5, 6, 7, 9, 10) (1, 2, 3, 8, 9, 10) (1, 3, 4, 7, 8, 10) (3, 4, 5, 7, 8, 10) (2, 6, 7, 8, 9, 10) (7, 8, 9, 10) (4, 5, 9, 10) (3, 4, 7, 10) (1, 5, 6, 10) (2, 3, 6, 7, 9, 10) (2, 3, 4, 10) (1, 2, 3, 4, 5, 7, 9, 10) (3, 5, 7, 8, 9, 10) (1, 3, 4, 5, 6, 8, 9, 10) (2, 3, 5, 7, 9, 10) (2, 4, 5, 8, 9, 10)

多項式の根が含まれることを示すこともできる。

3. 異なる M 系列の相互相関

$GF(2)$ 上の元を係数とする M 系列発生関数を次式で与える。

$$G(X) = \sum_{k=0}^{N-1} g_k X^k, \text{ mod } 2 \quad (3.1)$$

いま M 系列 $\{g_k\}$ は, $\{g_k\} = \{g_{2k}\}$, $k=0, 1, 2, \dots$ の性質をもつ特性 M 系列とすると, (3.1) 式は $G(X) = \{G(X)\}^2 = G(X^2)$ と表わせるので, このような特性 M 系列は $GF(2^n)$ 上のすべての元 (0 を除く) の $GF(2)$ へのトレース (T_n と書く) により表現される。トレース T_n は次式で定義される。

$$T_n(x) = x + x^2 + x^4 + \dots + x^{2^{n-1}}$$

x を $GF(2^n)$ 上の任意の元とすると, $T_n(x)$ はそれに対応する $GF(2)$ 上の元となる。よって (3.1) 式は次式のように表わされる。

$$G(X) = \sum_{k=0}^{N-1} T_n(\alpha^{-k}) X^k \quad (3.2)$$

なお, トレースの性質上 $T_n(\alpha^{-k}) = \{T_n(\alpha^{-k})\}^2 = T_n(\alpha^{-2k})$ となるから, $G(X)$ は特性 M 系列を表わしていることがわかる。

いっぽう M 系列 $\{g_k\}$ を s 個ごとにサンプルして得られる非極大系列を $\{f_{j,i}\}$ とおくと, $\{f_{j,i}\} \equiv \{g_{is+j}\}$, $0 \leq i \leq q-1$, $0 \leq j \leq s-1$ であるから (3.1) 式は次式となる。

$$G(X) = \sum_{j=0}^{s-1} \left(\sum_{i=0}^{q-1} g_{is+j} X^i \right) X^j, x \equiv X^s \quad (3.3.1)$$

$$= \sum_{j=0}^{s-1} \left(\sum_{i=0}^{q-1} f_{j,i} X^i \right) X^j \quad (3.3.2)$$

また (3.3) 式は (3.2) 式を使って次式で表わせる。

$$G(X) = \sum_{j=0}^{s-1} \left\{ \sum_{i=0}^{q-1} T_n(\beta^{-i} \alpha^{-j}) X^i \right\} X^j, \beta \equiv \alpha^s \quad (3.4)$$

3.1 同じクラスの異なる M 系列の相互相関

ここで, 同じクラスに属する M 系列同士の相互相関を考えてみよう。相互相関をとるべき同じクラスの異なる原始多項式の根を α^a, α^b とするとき, おのおのの発生関数を $G_a(X), G_b(X)$ とおく。 $a=1$ としても一般性を失わないので, $G_a(X)$ は (3.1) 式から (3.4) 式で与えられる場合を考える。そこで (2.4) 式より $C_0 = 1$ として, 適当な整数 u, v と $0 < c \leq s-1$ を用いて,

$$b = (1+qc)2^u - Nv \quad (3.5)$$

と表わされる。もちろん, $GCD(b, N) = 1$ を満足する b を用いるものとする。そこで, 発生関数 $G_b(X)$ は (3.1) 式より次式で表わせる。

$$G_b(X) = \sum_{k=0}^{N-1} g_{bk} X^k, \text{ mod } 2 \quad (3.6.1)$$

$$= \sum_{k=0}^{N-1} T_n(\alpha^{-bk}) X^k \quad (3.6.2)$$

(3.3) 式より,

$$G_b(X) = \sum_{j=0}^{s-1} \left\{ \sum_{i=0}^{q-1} T_n(\beta^{-bi} \alpha^{-bj}) X^i \right\} X^j \quad (3.7.1)$$

となる。よって, (3.5) 式を (3.7.1) 式に代入して,

$$G_b(X) = \sum_{j=0}^{s-1} \left\{ \sum_{i=0}^{q-1} T_n(\beta^{-i} \alpha^{-j} \alpha^{-qcj}) X^i \right\} X^j \quad (3.7.2)$$

となる。 $G_a(X), G_b(X)$ の相互相関系列 $C_{ab}(X, l)$ は (l は遅れを表わす), つぎのように表わされる。

$$C_{ab}(X, l) = \sum_{k=0}^{N-1} c_k(l) X^k, \begin{cases} 0 \leq l \leq N-1 \\ \text{mod } 2 \end{cases} \quad (3.8.1)$$

$$= \sum_{k=0}^{N-1} (g_{k-l} + g_{bk}) X^k \quad (3.8.2)$$

$$= G_a(X) X^l + G_b(X) \quad (3.8.3)$$

となる。(3.2), (3.6.2) 式を (3.8.2) 式に代入して次式となる。

$$C_{ab}(X, l) = \sum_{k=0}^{N-1} T_n(\alpha^{-k+l} + \alpha^{-bk}) X^k \quad (3.9)$$

上式で $T_n(\) = T_n(\)^{2^p} (p=0, 1, 2, \dots)$ であることより, l の剰余類に属する遅れ $2^p l$ は等しい相互相関値をとる。そこで, (3.4), (3.7.2) 式を (3.9) 式に代入すると次式となる。

$$C_{ab}(X, l) = \sum_{j=0}^{s-1} \left[\sum_{i=0}^{q-1} T_n \{ \beta^{-i} \alpha^{-j} (\alpha^l + \alpha^{-qcj}) \} X^i \right] X^j \quad (3.10)$$

(3.10) 式で $\alpha^l + \alpha^{-qcj} = 0$ を満たすとき, $T_n\{ \ } = 0$ となる。したがって,

$$l = -qcj, \text{ mod } N \quad (3.11)$$

のとき, すなわち遅れ l が q の整数倍のとき, $C_{ab}(X, l)$ に 0 系列を含むことになる。相互相関値は相互相関系列 $C_{ab}(X, l)$ の係数の平均値であるから, このように 0 系列を含む場合は, 平均値がいっぽうに偏より顕著な相互相関が現れることになる。

また (3.10) 式の相互相関系列は $\{f_{j,i}\}$ 系列の組合せによって決まる。すなわち (3.10) 式の $T_n\{ \ }$ において,

$$\alpha^\lambda \equiv \alpha^{l-j} + \alpha^{-qcj-j} \quad (3.12)$$

$$\lambda = st - \zeta, \text{ mod } N, 0 \leq t \leq q-1, 0 \leq \zeta \leq s-1 \quad (3.13)$$

とおくと,

$$T_n \{ \beta^{-i} \alpha^{-j} (\alpha^l + \alpha^{-qcj}) \} = T_n(\beta^{-i+j} \alpha^{-\zeta}) \quad (3.14)$$

となる。相互相関系列 $C_{ab}(X, l)$ を構成する非極大系列の種類を決めるのは $\alpha^{-\zeta}$ であるから, (3.10) 式で

与えられる相互相関系列はM系列 $\{g_k\}$ を s 個ごとにサンプルして得られる非極大系列 $\{f_{j,i}\}$ から、重複をみとめて s 個選んだ系列 (それを $f_{(j)} \equiv \{f_{(j),i}\}$ と表わし, j を特に指定しない場合は $f_{(j)}$ と書く. 特にそれが0系列になる場合を $0_{(j)}$ と表わすことにする) の組合せとなり, 選び方は, 各 j について (3.14) 式によって決まる.

(3.8.1) 式より c_k を $\begin{pmatrix} 0 \rightarrow 1 \\ 1 \rightarrow -1 \end{pmatrix}$ に実数変換して $\hat{c}_k$ とおくと, 1周期にわたる相互相関関数は次式となる.

$$\Phi_{ab}(l) = \sum_{k=0}^{N-1} \hat{c}_k(l) \quad (3.15)$$

そこで, $\{f_{(j),i}\}$ の周期 q における重みを W_j とすると, (3.15) 式は次式となる.

$$\Phi_{ab}(l) = \sum_{j=0}^{s-1} (q - 2W_j) \quad (3.16)$$

よって, 相互相関値は非極大系列 $\{f_{j,i}\}$, $0 \leq i \leq s-1$ の重み分布と, 相互相関系列が $f_{j,i}$ のどのような組合せになっているのかを知ることにより, (3.16) 式によって与えられる.

3.2 非極大系列の重み分布

M系列 $\{g_k\}$ をつぎの特性M系列とする.

$$\{g_k\} = \{g_{2k}\}, \quad k=0, 1, 2, \dots \quad (3.17)$$

$\{g_k\}$ を s 個ごとにサンプルして得られる $\{f_{j,i}\}$ 系列は, s を法として, j の剰余類が,

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{2^0, 2^1, 2^2, \dots, 2^{s-2}\}, \quad 2^{s-1} \equiv 1 \end{aligned} \quad (3.18)$$

の2組しかないような s の場合を考えると次式のようになる.

$$\begin{aligned} g_k &\in \{f_{0,i}\}, \quad k \equiv 0 \pmod{s} \\ g_k &\in \{f_{j,i}\}, \quad k \not\equiv 0 \pmod{s} \end{aligned} \quad (3.19)$$

よって $k \not\equiv 0 \pmod{s}$ に対する g_k は, $N-q=q(s-1)$ 個あるから, g_k は j の異なる $s-1$ 個の $\{f_{j,i}\}$ 系列に均等に配分される. このように s を法として, 原始根が2の場合, $\{f_{j,i}\}$ 系列が2種類の異なる重みをもつ. すなわち $\{f_{j,i}\}$ 系列の重みを $w_{\{f_{j,i}\}} \equiv w_j$ とすると, w_0 と w_j , $0 < j \leq s-1$ の2種類である. ここで, $\{f_{j,i}\}$ 系列を発生する特性多項式を $r(x)$ と置いたとき,

$$f(x) = \frac{x^q - 1}{r(x)} \quad (3.20)$$

と表わせる. $f(x)$ を発生関数とする (q, n) コードは $\{f_{j,i}\}$ 系列であるから, その双対コード $(q, q-n)$ の最小重みは3である. いっぽう, MacWilliams の定理によって次式が成立する¹¹⁾.

$$\sum_{i=0}^q A_i y^i = 2^{n-q} \sum_{i=0}^q A'_i (y+1)^{q-i} (1-y)^i \quad (3.21)$$

A_i は重み i をもつコード数, A'_i は A_i の双対コードのコード数を表わす. ただし $A_0 = A'_0 = 1$. 今の場合, 左辺は重みが2種類 (w_0, w_1) しかなくまた右辺は最小重み3であるから, (3.21) 式は次式となる.

$$\begin{aligned} 1 + qy w_0 + (s-1)qy w_1 \\ = 2^{n-q} \{(1+y)^q + A'_3(1+y)^{q-3}(1-y)^3 + \dots\} \end{aligned} \quad (3.22)$$

上式より w_0, w_1 について解くと次式のようになる. n は偶数として,

$$\begin{aligned} s \mid 2^{n/2} + 1 \text{ のとき,} \\ w_0 = \frac{2^{n-1} - (s-1)2^{(n/2)-1}}{s}, \quad w_j = \frac{2^{n-1} + 2^{(n/2)-1}}{s} \end{aligned} \quad (3.23)$$

$$\begin{aligned} s \mid 2^{n/2} - 1 \text{ のとき,} \\ w_0 = \frac{2^{n-1} + (s-1)2^{(n/2)-1}}{s}, \quad w_j = \frac{2^{n-1} - 2^{(n/2)-1}}{s} \end{aligned} \quad (3.24)$$

3.3 $s=3$ の場合における, 遅れが q の整数倍での相互相関値

$\alpha^q \equiv r$ として, (3.10) 式の $T_n\{\}$ について求めるおつぎのようになる. $l = -qce$, $e=0, 1, 2$ と書けることを用いて, $\beta \equiv \alpha^3$ として,

$$\begin{aligned} T_n\{\beta^{-i}\alpha^{-j}(\alpha^l + \alpha^{-qcej})\} &= T_n\{\beta^{-i}\alpha^{-j}(\alpha^{-qce} + \alpha^{-qcej})\} \\ &= T_n\{\beta^{-i}\alpha^{-j}(r^{-ce} + r^{-cej})\} \end{aligned} \quad (3.25)$$

となる. r の位数は3であるから, この場合の原始多項式の次数は偶数をとる. $GF(2^n)$ 上において, 指標3の既約多項式は1個存在し, $1+X+X^2$ である. したがって, $1+r+r^2=0$, $1+r^{-1}+r^{-2}=0$ を満足している.

(1) $3 \nmid q$ のときの相互相関値

ν を適当な整数として, $3\nu+qc=1$ と書けるから,

$$r^{-c} = \beta^{\nu} \alpha^{-1} \quad (3.26)$$

となり, c は1または2であるから, (3.26) 式より,

$$\begin{aligned} 1 + r^{-c} &= r^{-2c} = \beta^{2\nu} \alpha^{-2} \\ 1 + r^{-2c} &= r^{-c} = \beta^{\nu} \alpha^{-1} \end{aligned} \quad (3.27)$$

となる. よって各 $e=0, 1, 2$ について, (3.27) 式を (3.25) 式に代入すると, 非極大系列の組合せがわかり, (3.14) 式で与えられる γ を用いて $f_{(j)}$ と $0_{(j)}$ で表わすことができる. たとえば $e=0$ ($l=0$) はつぎのようになる.

$$\begin{aligned} j=0 \text{ のとき, } T_n\{\beta^{-i}(1+1)\} &\equiv 0_{(0)} \\ j=1 \text{ のとき, } T_n\{\beta^{-i}\alpha^{-1}(1+\gamma^{-c})\} \\ &= T_n\{\beta^{-i}\beta^{2\nu-1}\} \equiv f_{0(1)} \\ j=2 \text{ のとき, } T_n\{\beta^{-i}\alpha^{-2}(1+\gamma^{-2c})\} \\ &= T_n\{\beta^{-i}\beta^{\nu-1}\} \equiv f_{0(2)} \end{aligned}$$

$e=1, 2$ の場合も同様にして求められ、結局、非極大系列の組合せは、

$$\begin{aligned} l=0(e=0) \text{ のとき, } \{f_{0(0)}, f_{0(1)}, f_{0(2)}\} \\ l=-qc(e=1) \text{ のとき, } \{f_{2(0)}, 0_{(1)}, f_{2(2)}\} \\ l=-2qc(e=2) \text{ のとき, } \{f_{1(0)}, f_{1(1)}, 0_{(2)}\} \end{aligned} \quad (3.28)$$

となる。

3.2 節より、 s が 3 の場合、 w_0 と w_1 という異なる 2 種類の重み分布があり、 $4 \nmid n$ のときは (3.23) 式で、 $4 \mid n$ のときは (3.24) 式で表わされる。よって、(3.23)、(3.24) 式と (3.28) 式を (3.16) 式に代入して相互相関値は、

$$\begin{aligned} 4 \nmid n \text{ のとき, } \\ \Phi_{ab}(0) = q + 2/3(2^{(n/2)+1} - 1) \\ \Phi_{ab}(qi) = q - 2/3(2^{(n/2)+1} - 1) \end{aligned} \quad (3.29.1)$$

$$\begin{aligned} 4 \mid n \text{ のとき, } \\ \Phi_{ab}(0) = q - 2/3(2^{(n/2)+1} + 1) \\ \Phi_{ab}(qi) = q + 2/3(2^{(n/2)-1} - 1) \end{aligned} \quad (3.29.2)$$

となる。例として n が 8 次の場合をとると $N=255=3 \times 5 \times 17$ であるから、 $s=3$ 、 $q=85$ ととれる。この場合、同じクラスの異なる特性多項式をもつ M 系列の相互相関の 1 例を Fig. 1 に示す。なお図中の相関値は周期 N で規準化されている。遅れ qi 、 $i=0, 1, 2$ の相互相関値は理論値と一致している。

(2) $3 \mid q$ のときの相互相関値

$$\begin{aligned} 3 \nmid q+qc=3 \text{ より, } \\ \gamma^{-c} = \beta^{q-1} \end{aligned} \quad (3.30)$$

となり、よって式 (3.30) より、

$$\begin{aligned} 1+r^{-c} &= r^{-2c} = \beta^{2(q-1)} \\ 1+r^{-2c} &= r^{-c} = \beta^{q-1} \end{aligned} \quad (3.31)$$

となる。(1) 項と同様に、非極大系列の組合せは、

$$l=0 \text{ のとき, } \{0_{(0)}, f_{1(1)}, f_{2(2)}\}$$

$$l=-qc \text{ のとき, } \{f_{0(0)}, 0_{(1)}, f_{2(2)}\} \quad (3.32)$$

$$l=-2qc \text{ のとき, } \{f_{0(0)}, f_{1(1)}, 0_{(2)}\}$$

となる。したがって相互相関値は、

$$\begin{aligned} 4 \nmid n \text{ のとき, } \\ \Phi_{ab}(0) = q - 2/3(2^{n/2} + 1) \\ \Phi_{ab}(qi) = q + 2/3(2^{(n/2)-1} - 1) \end{aligned} \quad (3.33.1)$$

$$\begin{aligned} 4 \mid n \text{ のとき, } \\ \Phi_{ab}(0) = q + 2/3(2^{n/2} - 1) \\ \Phi_{ab}(qi) = q - 2/3(2^{(n/2)-1} + 1) \end{aligned} \quad (3.33.2)$$

となる。例として n が 6 次の場合をとると $N=63=3 \times 3 \times 7$ 、 $s=3$ 、 $q=21$ ととれる。この場合、同じクラスの特性多項式の異なる M 系列の相互相関の 1 例を Fig. 2 に示す。遅れ qi 、 $i=0, 1, 2$ の相互相関値は理論値と一致している。

つぎに遅れ l が q の整数倍以外での相互相関値について考えてみよう。 l が q の整数倍以外では (3.14) 式より相互相関系列に 0 系列を含まないことがわかる。よって、異なる相関値をもつ非極大系列の組合せとしてつぎのものが考えられる。ただし非極大系列の f_i 、 $i=1, 2$ は重みが等しいので f_1 と書くことにする。またそれらの組合せのときの相互相関値を右側に書くことにする。

$$\begin{aligned} \{f_0, f_0, f_0\} \text{ のとき, } & 4 \nmid n \text{ で, } \Phi(l) = 2^{(n/2)+1} - 1 \\ & 4 \mid n \text{ で, } \Phi(l) = -2^{(n/2)+1} - 1 \\ \{f_0, f_0, f_1\} \text{ のとき, } & 4 \nmid n \text{ で, } \Phi(l) = 2^{n/2} - 1 \\ & 4 \mid n \text{ で, } \Phi(l) = -2^{n/2} - 1 \\ \{f_0, f_1, f_1\} \text{ のとき, } & 4 \nmid n \text{ で, } \Phi(l) = -1 \\ & 4 \mid n \text{ で, } \Phi(l) = -1 \\ \{f_1, f_1, f_1\} \text{ のとき, } & 4 \nmid n \text{ で, } \Phi(l) = -2^{n/2} - 1 \\ & 4 \mid n \text{ で, } \Phi(l) = 2^{n/2} - 1 \end{aligned}$$

したがって、異なる相互相関値は、遅れが q の整数倍での相互相関値も入ると 6 値以下となる。また、相互

Fig. 1 Cross-correlation of Ma and Mb

Ma: primitive poly. $= x^8 + x^4 + x^3 + x^2 + 1$
initial value $= 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0$
Mb: primitive poly. $= x^8 + x^7 + x^6 + x + 1$
initial value $= 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1$

Fig. 2 Cross-correlation of Ma and Mb

Ma: primitive poly. $= x^8 + x + 1$
initial value $= 0 \ 1 \ 1 \ 1 \ 1 \ 1$
Mb: primitive poly. $= x^8 + x^5 + x^3 + x^2 + 1$
initial value $= 0 \ 0 \ 0 \ 1 \ 0 \ 0$

相関値の最大値は、上記の組合せにおいては起こらず、遅れが q の整数倍においてのみ起こることがわかる。

ゆえに、相互相関値の絶対値を $|\Phi(l)|$ とすると、つぎのように表わされる。

$3 \nmid q$ のとき、

$$4 \nmid n \text{ で, } 1 \leq |\Phi(l)| \leq \Phi_{ab}(0)$$

$$4 \mid n \text{ で, } 1 \leq |\Phi(l)| \leq \Phi_{ab}(qi), \quad i=1, 2$$

$3 \mid q$ のとき、

$$4 \nmid n \text{ で, } 1 \leq |\Phi(l)| \leq \Phi_{ab}(qi), \quad i=1, 2$$

$$4 \mid n \text{ で, } 1 \leq |\Phi(l)| \leq \Phi_{ab}(0)$$

4. あとがき

周期が素数でない異なる特性多項式をもつM系列の相互相関が、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。

すなわち $GF(2^n)$ 上で原始元の位数 N が素数でないとき、 N の約数 $q(=N/s)$ の指標をもつ既約多項式が存在するので、異なる原始多項式の一つの根を α^a, α^b とすると、 N を法として sa, sb が同じ剰余類に属するような原始多項式の集合を一つのクラスとして分類できる。これは異なる原始多項式から発生されるM系列をおのおの s 個ごとにサンプルしたとき、同じ系列になるような原始多項式を一つのクラスとして分類することを意味する。このように分類された同一クラスの異なる原始多項式により発生された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、その重み分布によって理論的に求められることを示した。特に $s=3$ の場合について、相互相関値の理論値を求め、遅れが q の整数倍の相互相

関値が最大になることを示した。 $s=3$ 以外も同様の方法により理論的に求められると思われる。

参考文献

- 1) 柏木, 森内: 異なる特性多項式をもつM系列の相互相関, 第21回 SICE 前刷, 431/432 (1982)
- 2) 森内, 柏木: 異なる特性多項式をもつM系列の相互相関, (第2報), 第1回 SICE 九州支部前刷, 147/148, (1982)
- 3) R. Gold: Maximal Recursive Sequences with 3 Valued Recursive Cross-Correlation Functions, IEEE Trans. on IT, **IT-14**, 154/156 (1968)
- 4) R. Gold: Optimal Binary Sequences for Spread Spectrum Multiplexing, IEEE Trans. on IT, **IT-13**, 619/621 (1967)
- 5) F. Surbock and H. Weinrichter: Interlacing Properties of Shift-Register Sequences with Generator Polynomials Irreducible over $GF(p)$, IEEE Trans. on IT, **IT-24-3**, 386/389 (1978)
- 6) S. W. Golomb: Shift Register Sequences, Holden-Day, San Francisco, (1967)
- 7) H. Weinrichter and F. Surbock: Phase Normalised m-Sequences with the Inphase Decimation Property $\{m(k)\} = \{m(2k)\}$, Electronics Letters, **12-22**, 590/591 (1976)
- 8) R. Gold: Characteristic Linear Sequences and Their Coset Functions, J. SIAM Appl. Math., **14-5**, (1966)
- 9) N. Zierler: Linear Recurring Sequences, J. Soc. Indust. Appl. Math., **7-1**, 31/48 (1959)
- 10) H. Kashiwagi and T. Moriuchi: A Fast Method for Arithmetic Modulo a Polynomial Over $GF(2)$ and Its Applications, IFAC, Preprints, **II-9**, II-124/II-129 (1981)
- 11) F. J. MacWilliams and N. J. A. Sloane: The Theory of Error Correcting Codes, North Holland (1978)
- 12) W. W. Peterson: Error-Correcting Codes, MIT Press (1961)