
 研 究

スペクトラム拡散符号としてのゴールド符号の相関特性

柴田 正司* 角川 靖夫**

(昭和55年7月15日受理)

CORRELATION PROPERTIES OF GOLD CODES IN SPREAD SPECTRUM COMMUNICATIONS

By

Masashi SHIBATA and Yasuo KADOKAWA

The Gold code is a kind of nonmaximal linear sequences, and it has a large number of different codes.

The Gold code, however, is not always the best spectrum-spreading code in spread spectrum communications having many different users, since the code sometimes shows bad properties in the behavior of both autocorrelation and crosscorrelation in comparison with those of maximal linear sequences (m-sequences).

This paper describes several merits of the Gold code derived from the preferred pair of m-sequences, together with some discussion on both autocorrelation and crosscorrelation of the Gold codes.

It is clarified that the specified pair of Gold codes with 3-values as obtained from the preferred pair of m-sequences gives a smaller upper bound of crosscorrelation than the arbitrary pair of Gold codes which are generated by m-sequences at random, and it has also a good autocorrelation properties.

It is found by computer simulation that most of the specified pair of Gold codes have a smaller rms value of crosscorrelation than that of m-sequences.

1. 緒 言

スペクトラム拡散通信方式の原理は、情報で1次変調を行うほかに、更に独立した拡散符号で2次変調を行うことにある。この拡散符号に必要な特性としては、(1)相関による信号検出を良くするため自己相関関数の弁別指数†が大きい、(2)同時アクセス局間の干渉を少なくする

ため拡散符号相互の相互相関が小さい、(3)アドレスを多数選択できるため符号の種類が多い、等が必要である⁽¹⁾⁽²⁾⁽³⁾。自己相関特性の優れている拡散符号としてはM系列が知られており、相互相関関数がある特定な上界を持ち符号の種類が多い拡散符号としてはゴールド符号(Gold code)が代表的である。

M系列の特性については、例えば文献(4)(5)等でかなり詳細に報告されているが、相互相関関数がある特定な上界を持つM系列の組合せについての検討は少ない。ま

*警察庁研修生 **通信機器部通信系研究室

†自己相関関数の最大ピークとそれに次ぐピークの差。

た、ゴールド符号の特性については今までほとんど発表されておらず、拡散符号として使用するうえで、その自己相関関数及び相互相関関数の性質を知る必要がある。

ここでは、まず、相互相関関数がある特定な上界を持つM系列の組合せについて計算機で検討した結果と、ゴールド符号の自己相関関数及び相互相関関数について明らかになった2, 3の点を述べ、ゴールド符号を構成するM系列の種類及び次数を適当に選ぶならば、その自己相関関数及び相互相関関数の性質はM系列とほぼ等しいことを示す。

2. M系列の相互相関関数^{(4)~(11)}

ここでは、11次のM系列がとる相互相関関数の値について計算機で求めた結果を述べ、11次までの相互相関関数の計算結果から相互相関関数が特定な上界を持つM系列の組合せの関係を示す。

2.1 M系列の相互相関関数

周期 p を持つ異なる二つのM系列を $M = \{a(k)\}$, $N = \{b(k)\}$ とし、その位相を i とする。この時、 M と N の相互相関関数 $\phi_c(i)$ は次式で表される。

$$\phi_c(i) = [p - 2 \sum_{k=0}^{p-1} \varphi_A(k)] / p \quad \dots\dots(1)$$

ただし、

$$\varphi_A(k) = a(k+i) \oplus b(k) \pmod{2} \quad \dots\dots(2)$$

M系列の相互相関関数の値は、M系列の組合せ、及びM系列の次数 n により異なり、 $\tau(i) = p\phi_c(i)$ とした時、 n が10次までについては、文献(4)により次の特定な値を取る。

$$\tau(i) = m \cdot 2^r - 1 \quad \dots\dots(3)$$

$$\begin{cases} n = 3, 4 \text{ の時} & \gamma = 1 \\ n = 5 \sim 7 \text{ の時} & \gamma = 3 \\ n = 8 \sim 10 \text{ の時} & \gamma = 4 \\ \text{二つのM系列がイメージ*の時} & \gamma = 2 \end{cases}$$

ただし、 m は0又は適当な整数

11次については、今回計算機により求めた結果、 $\gamma = 5$ となった。(3)式の1例として、二つのM系列が{7,

*任意のM系列に対し逆向きのM系列のこと。

第1表 M系列の相互相関関数の値の種類(計算例)

n=5	t=3 {5.4.3.2}	t=5 {5.4.2.1}						
t=1 ^{*1} {5.2}	$\Delta 3$	$\Delta 3$						
n=6	t=5 {6.5.2.1}	t=11 {6.5.3.2}						
t=1 {6.1}	$\Delta 3$	5						
n=7	t=3 {7.3.2.1}	t=5 {7.4.3.2}	t=7 {7.6.5.4.2.1}	t=9 {7.5.4.3.2.1}	t=11 {7.6.4.2}	t=13 {7.1}	t=19 {7.6.3.1}	t=21 {7.6.5.2}
t=1 {7.3}	$\Delta 3$	$\Delta 3$	3	$\Delta 3$	3	3	7	7
n=8	t=7 {8.6.5.3}	t=11 {8.7.6.5.2.1}	t=13 {8.5.3.1}	t=19 {8.6.5.2}	t=23 {8.6.5.1}	t=37 {8.6.4.3.2.1}	t=43 {8.7.6.1}	
t=1 {8.4.3.2}	6	7	5	5	5	6	6	
n=9	t=3 {9.6.4.3}	t=5 {9.8.5.4}	t=9 {9.8.4.1}	t=11 {9.5.3.2}	t=13 {9.6.5.4.2.1}	t=15 {9.8.6.5}	t=17 {9.7.6.4.3.1}	
t=1 {9.4}	$\Delta 3$	$\Delta 3$	3	5	3	14	$\Delta 3$	
n=10	t=5 {10.8.3.2}	t=7 {10.9.8.7.6.5.4.3}	t=13 {10.6.5.3.2.1}	t=17 {10.9.8.6.3.2}				
t=1 {10.3}	$\Delta 3$	13	3	$\Delta 3$				
n=11	t=3 {11.8.5.2}	t=5 {11.7.3.2}	t=7 {11.5.3.2}					
t=1 {11.2}	$\Delta 3$	$\Delta 3$	9					

*1 GF(2) の上の n 次の原始多項式のうち、非零の係数の数が最小となる多項式の根を α とした。すなわち、{5, 2} は $\alpha^1(t=1)$ の最小多項式で、{5, 4, 3, 2} は $\alpha^3(t=3)$ の最小多項式となる。詳細は、文献(8)p.526を参照。

*2 Δ は、二つのM系列がプリファードペアの条件 (4), (6), (7)式) を満たすものを示す。

第2表 プリファードペアとなる原始多項式の根のべき乗 t の値。ただし、 n は原始多項式の次数で、 $p=2^{n-1}$

n	5	6	7	9	10	11
p	31	63	127	511	1023	2047
t	9	17	17	33	65	65
t'	5	5	9	17	17	33

3]*, [7, 6, 3, 1] の時, $\tau(i)$ は, 23, 15, 7, -1, -9, -17, -41 の7値を取り, r は3で m はそれぞれ, 3, 2, 1, 0, -1, -2, -5である。

第1表に, 今回計算した5~11次のM系列のうち, 幾つかの相互相関関数の値の種類を示す。

2.2 相互相関関数が特定な上界を持つM系列の組合せ

M系列の相互相関関数は前述したように, 次数 n に対応した離散的な値をとるが, 二つのM系列を次のように選択すると, その相互相関関数は次数 n により定まる特定な上界を持つことが知られている⁽¹²⁾。

まず, 第1のM系列の原始多項式を f_1 とし, その原始元^{*1}を α とする。次に, 次数 n に対し t を,

$$t = \begin{cases} 2^{(n+1)/2} + 1 & n : \text{奇数} \\ 2^{(n+2)/2} + 1 & n : \text{偶数, } n \not\equiv \text{mod } 4 \end{cases} \dots\dots(4)$$

とし, α^t を根に持つ原始多項式 f_t のM系列を第2のM系列とする。

二つのM系列をこのように選択すると, この二つのM系列の相互相関関数 $\phi(i)$ は次の上界を持ち, このように選択された二つのM系列は, プリファードペア (preferred pair) と呼ばれている。

$$|\phi(i)| \leq t/p \dots\dots(5)$$

$n=5\sim 11$ の時, (4)式の t , 及び原始多項式の根の位数^{*2}の性質^{*3}により, この t に等しい根のべき乗 t' は第2表のとおりになる。例えば, $n=5$ の時 $t=9, t'=5$ であるので, 第1表から $t=1$ のM系列 [5, 2] と $t'=5$ のM系列 [5, 4, 2, 1] を選ぶと, 両者の相互相関関数 $\phi(i)$ は(5)式から次の上界を持つ。

* [7, 3] は, M系列のシフトレジスタの7段目と3段目を半加算器で加え, 7段目のシフトレジスタに帰還することを意味し, M系列 $a(k) = a(k-7) \oplus a(k-3) (k=7, 8, \dots)$ を示す。

*1 拡大体 $GF(2^n)$ から零元を除いたすべての元は, $GF(2^n)$ のある元のべき乗で表すことができ, この元を原始元と言う。詳細は, 例えば文献(8)~(10)等を参考にされたい。

*2 ガロア体の任意の元を α とすると, $\alpha^e = 1$ となる正の整数があり, このうち最小の整数 e を位数 (order) という。

*3 例えば, $n=6$ の時 $t=2^{(6+2)/2} + 1 = 17$ であり, $17 \times 2^2 - 63 = 5$ なので α^{17} と α^5 の位数は同じ。

第3表 プリファードペアなM系列の相互相関関数の値及び頻度 (n : 奇数, $p=2^{n-1}$)

相互相関関数の値	頻度
$-1/p$	$2^{n-1} - 1$
$(2^{(n+1)/2} - 1)/p$	$2^{n-2} + 2^{(n-3)}/2$
$-(2^{(n+1)/2} + 1)/p$	$2^{n-2} - 2^{(n-3)}/2$

第4表 プリファードペアなM系列の相互相関関数の値及び頻度 (n : 偶数, $n \not\equiv \text{mod } 4, p=2^{n-1}$)

相互相関関数の値	頻度
$-1/p$	$3 \cdot 2^{n-2} - 1$
$(2^{(n+2)/2} - 1)/p$	$2^{n-3} + 2^{(n-4)}/2$
$-(2^{(n+2)/2} + 1)/p$	$2^{n-3} - 2^{(n-4)}/2$

$$|\phi(i)| \leq (2^{(n+1)/2} + 1)/p = 9/31$$

また, 次数 n が奇数で, 第2のM系列を構成する原始多項式 f_t の根のべき乗 t が,

$$\left. \begin{aligned} n &: \text{奇数} \\ (n, t) &= 1^* \\ t &= 2^t + 1 \end{aligned} \right\} \dots\dots(6)$$

ならば, 原始多項式 f_1, f_t で構成する二つのM系列の相互相関関数の値, 及びその値の頻度は第3表の値を取ることが証明されている⁽¹³⁾。

しかし, 次数が偶数の時の相互相関関数の値, 及びその値の頻度を求める関数関係はこれまで不明であった。そこで, 今回6, 8, 10次について計算機で求めた結果, 第2のM系列の原始多項式 f_t の根のべき乗 t をこのように選択すると, その二つのM系列の相互相関関数の値, 及びその値の頻度は第4表のとおりであることが明らかになった。

$$\left. \begin{aligned} n &: \text{偶数 } (n \not\equiv \text{mod } 4) \\ t &: \text{正の整数} \\ t &= 2^t + 1 \end{aligned} \right\} \dots\dots(7)$$

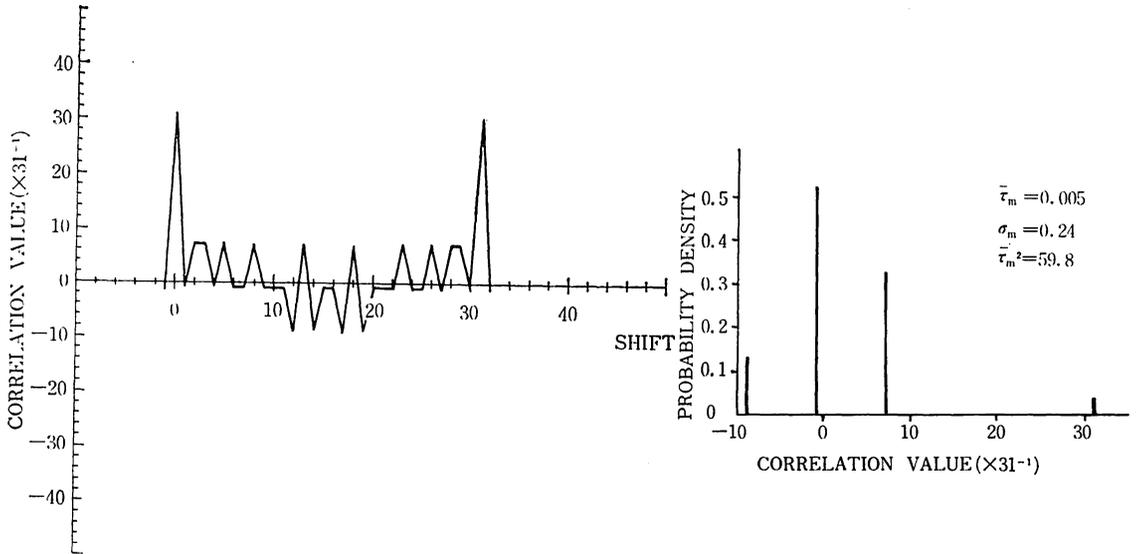
(6)式, (7)式を満たす二つのM系列は, 相互相関関数が前述(5)式と同じ上界を持つ良好な組合せなので, ここでは, このように選択した二つのM系列もプリファードペアと呼ぶことにする。

第1表で各次数の左側のM系列に対し Δ 印をしたM系列がプリファードペアである。

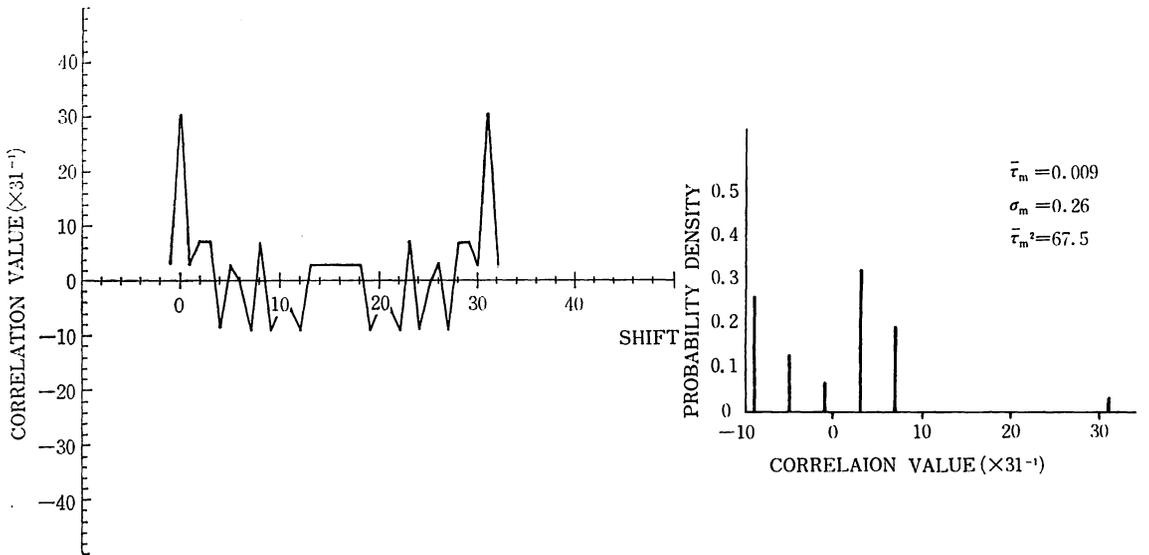
3. ゴールド符号の構成, 自己相関関数, 及び相互相関関数

ここでは, まず, ゴールド符号の構成及び種類を述

* $(n, t) = 1$ は n と t が互いに素であることを示す。



(1) 2つのM系列 [5, 2] [5, 4, 3, 2] (プリフェードペア) 相互の位相が0のゴールド符号の場合



(2) 2つのM系列 [5, 2] [5, 3] (イメージ) 相互の位相が0のゴールド符号の場合

第1図 ゴールド符号の自己相関関数

項式の根の位数が31の多項式は6種類*あることがわかり、その中の二つの多項式の積が非既約多項式 f_3 、すなわちゴールド符号となる。この場合、根の位数が31なので、ゴールド符号の周期は31である。

次に、ゴールド符号の種類は、この例の場合33種類であるが、これは非既約多項式 f_3 に対応した10次の帰還シフトレジスタの初期値の与え方により、次のよう

に分類できる。

- (i) 2種類——元の既約多項式 f_1 、又は f_2 のM系列から個々にとった10ビットを初期値とするゴールド符号
- (ii) 31種類——元のM系列相互の位相を1ビットずつ変えて加えた(mod 2)系列から取った10ビットを初期値とするゴールド符号

上記のゴールド符号の種類を第6表に示す。(17番と22番が(i)の場合で、その他が(ii)の場合である。

*位数31の既約多項式は、[5, 4, 3, 2] [5, 3, 2, 1] [5, 4, 2, 1] [5, 4, 3, 1] [5, 3] [5, 2]の6通り。詳細は例えば文献(8)p.529を参考にされたい。

3.2 ゴールド符号の自己相関関数

周期 p の相異なる二つのM系列の位相を i とする。この時、この二つのM系列で構成するゴールド符号 $G_a = \{g_a(k)\}$ の自己相関関数 $\phi'_A(i)$ は次式で表される。

$$\phi'_A(i) = [p - 2 \sum_{k=0}^{p-1} \phi'_A(k)] / p \quad \dots\dots(9)$$

ただし、

$$\phi'_A(k) = g_a(k+i) \oplus g_a(k) \pmod{2} \quad \dots\dots(10)$$

ゴールド符号の自己相関関数の例を第1図に示す。

以下に明らかになった点を述べる。

mod 2 の加法は線形関数なので⁽⁶⁾、(8)式を(10)式に代入すると、

$$\begin{aligned} \phi'_A(k) &= \{a(k+m+i) \oplus b(k+i) \\ &\quad \oplus [a(k+m) \oplus b(k)]\} \\ &= \{a(k+m+i) \oplus a(k+m)\} \\ &\quad \oplus \{b(k+i) \oplus b(k)\} \quad \dots\dots(11) \end{aligned}$$

(1) $i=0$ (in phase) の時

(11)式の右辺は、第1項、第2項とも零系列なので、

$$\phi'_A(0) = 1$$

(2) $i \neq 0$ (out of phase) の時

M系列のシフト加法性により、(11)式の右辺の第1項、第2項には、 $a(k+m+i) \oplus a(k+m) = a(k+j)$ 、 $b(k+i) \oplus b(k) = b(k+l)$ となる j, l が存在するので、

$$\begin{aligned} \phi'_A(k) &= a(k+j) \oplus b(k+l) \\ &= a(k+j-l) \oplus b(k) \end{aligned}$$

となり、これはゴールド符号を構成するM系列の相互相関関数の(2)式に等しい。 j と l の明確な関数関係は未知であり、その都度計算により求めなければならない*。また、 $(j-l)$ と i の関係は、M系列の組合せ及びM系列相互の位相 m により異なり、1対1の対応は成立しない。例えば、二つのM系列が [5, 2] [5, 4, 3, 2] の時、M系列の相互相関関数の値及び頻度は、7/31 が10回、-1/31 が15回、-9/31 が6回である。この二つのM系列で構成するゴールド符号の自己相関関数の値及び頻度は、第1図に示したようにM系列相互の位相 m が0の時、7/31 が10回、-1/31 が16回、-9/31 が4回である。また、位相 m が9の時、7/31 が10回、-1/31 が20回であり、位相 m により自己相関関数の値の頻度が異なる。

(3) 二つのM系列がプリファードペアの時

ゴールド符号を構成するM系列がプリファードペアならば、ゴールド符号の自己相関関数の値は前述したよう

に、必ず $-1/p$ 、 $(2^{(n+1)/2}-1)/p^*$ 、 $-(2^{(n+1)/2}+1)/p^*$ の3値のいずれかを取る。したがって、この時ゴールド符号の弁別指数 (index of discrimination : ID) は次のとおりになる。

$$2^n - 2^{(n+1)/2} \leq ID \leq 2^n + 2^{(n+1)/2} \quad \dots\dots(12)$$

3.3 ゴールド符号の相互相関関数

ゴールド符号の相互相関関数については、次の2通りの場合が考えられる。

(i) ゴールド符号を構成するM系列の組合せが同じ場合すなわち、二つのゴールド符号が、いずれも二つのM系列M, Nから構成される場合。

(ii) ゴールド符号を構成するM系列の組合せが異なる場合すなわち、二つのゴールド符号を構成するM系列が、一方は M_1, N_1 で、他方はこれと異なる M_2, N_2 の場合。

ここでは最も基本的な(i)の場合を検討するため、二つのゴールド符号 $G_a = \{g_a(k)\}$ 、 $G_b = \{g_b(k)\}$ を次のとおりとする。

$$g_a(k) = a(k+m) \oplus b(k) \quad \dots\dots(13)$$

$$g_b(k) = a(k+n) \oplus b(k) \quad (m \neq n) \quad \dots\dots(14)$$

この時、この二つのゴールド符号の相互相関関数 $\phi'_c(i)$ は次式で表される。

$$\phi'_c(i) = [p - 2 \sum_{k=0}^{p-1} \phi'_c(k)] / p \quad \dots\dots(15)$$

ただし、

$$\phi'_c(k) = g_a(k+i) \oplus g_b(k) \quad \dots\dots(16)$$

(13)式、(14)式を(16)式に代入すると

$$\begin{aligned} \phi'_c(k) &= \{a(k+m+i) \oplus b(k+i)\} \\ &\quad \oplus \{a(k+n) \oplus b(k)\} \\ &= \{a(k+m+i) \oplus a(k+n)\} \\ &\quad \oplus \{b(k+i) \oplus b(k)\} \quad \dots\dots(17) \end{aligned}$$

したがって、ゴールド符号の相互相関関数は、自己相関関数の場合と同様に、次のようになる。

(1) $i=0$ (in phase) の時

(17)式の右辺の第2項は零系列であり、第1項については $a(k+m) \oplus a(k+n) = a(k+j)$ となる j が存在し、

$$\sum_{k=0}^{p-1} \phi'_c(k) = (p+1)/2 \text{ なので}$$

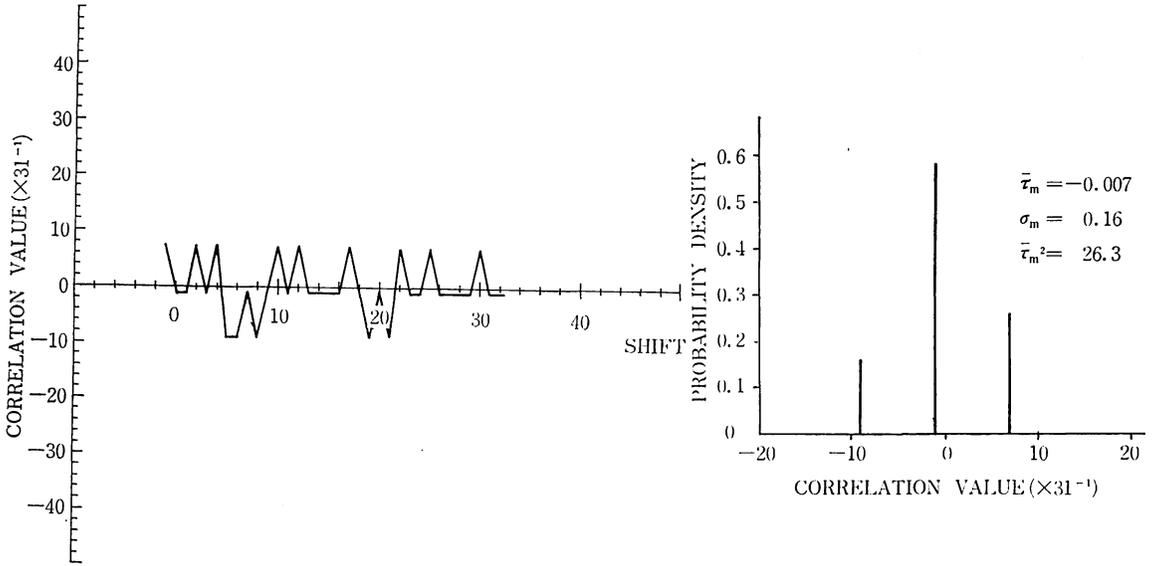
$$\phi'_c(0) = -1/p$$

(2) $i \neq 0$ (out of phase) の時

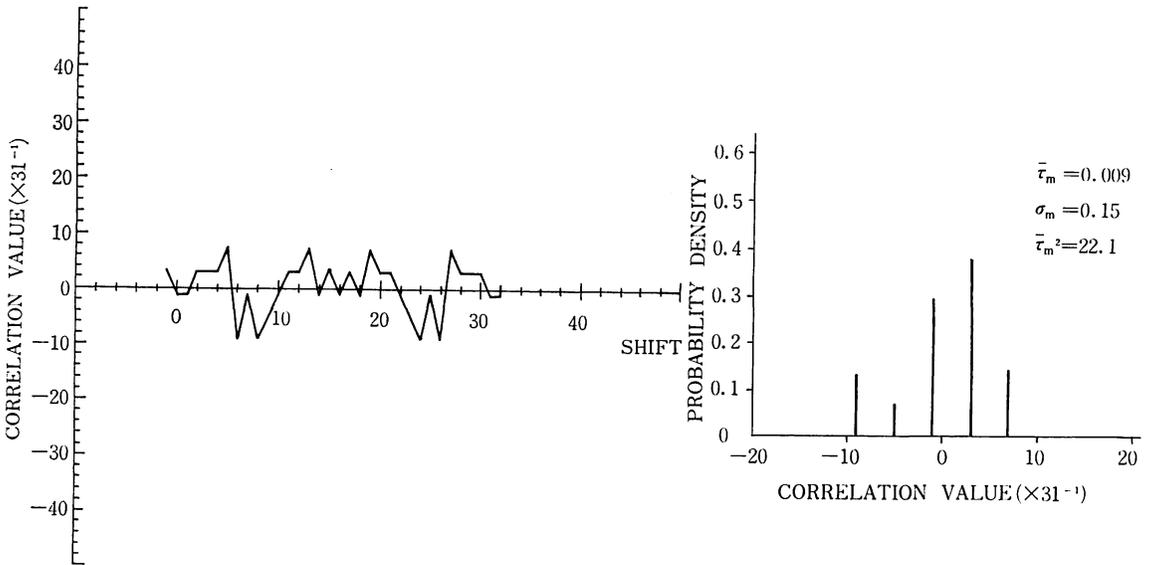
この時の相互相関関数 $\phi'_c(i)$ は、3.2の(2)で述べた説明により、ゴールド符号を構成するM系列の相互相関関数の値を取る。例えば、二つのM系列が [5, 2] [5, 4, 3, 2] でM系列相互の位相 m, n がそれぞれ、0, 1

* i が与えられた時、 $b(k+i) \oplus b(k) = b(k+j)$ を満たす j を求める計算方法は、例えば文献(6) p. 54 を参考にされたい。

* 次数 n が偶数の時は、それぞれ、 $(2^{(n+2)/2}-1)/p$ 、 $-(2^{(n+2)/2}+1)/p$ となる。以下同様。



(1) 2つのM系列 [5, 2] [5, 4, 3, 2] (プリファードペア) 相互の位相が0のゴールド符号と, 1のゴールド符号の場合



(2) 2つのM系列 [5, 2] [5, 3] (イメージ) 相互の位相が0のゴールド符号と, 1のゴールド符号の場合

第2図 ゴールド符号の相互相関関数

である二つのゴールド符号の相互相関関数の値及び頻度は, 第2図に示すように, $7/31$ が8回, $-1/31$ が18回, $-9/31$ が5回である。また, 位相 m , n がそれぞれ1, 11の場合は, $7/31$ が10回, $-1/31$ が15回, $-9/31$ が6回で, 他の位相の場合もすべてM系列 [5, 2] [5, 4, 3, 2]の相互相関関数の3値 $7/31$, $-1/31$, $-9/31$ を取る。なお, 第2図には, ゴールド符号を構成するM系列がイメージの場合も示してある。

(3) M系列がプリファードペアの時

二つのゴールド符号がプリファードペアなM系列から構成されると, その相互相関関数は, $-1/p$, $(2^{(n+1)/2}-1)/p$, $-(2^{(n+1)/2}+1)/p$ のいずれかの値を取る。しかし, 相互相関関数の値の頻度を求める明確な関数関係は未知であるので, その都度計算する必要がある。

3.4 ゴールド符号の相互相関関係の平均値及び自乗平均値

ゴールド符号を使用する場合, 相互相関関数の値が小さく, かつその頻度が多いほど望ましい。このため, 相

互相関関数の値と頻度の特性を示す平均値、及び自乗平均値を検討することが必要となる。ゴールド符号を構成するM系列がプリファードペアならば、相互相関関数は第3表、第4表の3値を取ることで、その頻度をX, Y, Zと置くことにより、相互相関関数の平均値、及び自乗平均値が求まる。

(1) 次数nが奇数の時

ゴールド符号が取る相互相関関数の3値、 $-1/p$, $(2^{(n+1)/2}-1)/p$, $-(2^{(n+1)/2}+1)/p$ の頻度をそれぞれZ, X, Yとすると、相互相関関数の平均値 $\bar{\tau}_m$ は、次式で表される。

$$\begin{aligned} \bar{\tau}_m &= \{-1 \cdot Z + X \cdot (2^{(n+1)/2} - 1) \\ &\quad - Y \cdot (2^{(n+1)/2} + 1)\} / p^2 \\ &= \{-p + (X - Y) \cdot 2^{(n+1)/2}\} / p^2 \quad \dots\dots(18) \end{aligned}$$

したがって、頻度X, Yの関係が次式の時、 $|\bar{\tau}_m|$ は最小になる。

$$X - Y = (2^n - 1) / 2^{(n+1)/2} \quad \dots\dots(19)$$

また、自乗平均値 $\bar{\tau}_m^2$ は、次式のとおりになるので、変数Kが小さいほど $\bar{\tau}_m^2$ は小さい。

$$\begin{aligned} \bar{\tau}_m^2 &= \{Z + X \cdot (2^{(n+1)/2} - 1)^2 \\ &\quad + Y \cdot (2^{(n+1)/2} + 1)^2\} / p^3 \\ &= \{p + K \cdot 2^{(n+3)/2}\} / p^3 \quad \dots\dots(20) \end{aligned}$$

ただし、

$$K = X \cdot (2^{(n-1)/2} - 1) + Y \cdot (2^{(n-1)/2} + 1) \quad \dots\dots(21)$$

特に、X, Yが第3表の頻度に等しい時は、

$$\bar{\tau}_m = 1/p^2, \quad \bar{\tau}_m^2 = (p^2 + p - 1) / p^3$$

となる。

(2) 次数nが偶数の時

この場合は、第4表の3値を取ることで、 $-1/p$, $(2^{(n+2)/2}-1)/p$, $-(2^{(n+2)/2}+1)/p$ の頻度をそれぞれZ, X, Yとすると、相互相関関数の平均値、自乗平均値は次のとおりになる。

$$\begin{aligned} \bar{\tau}_m &= \{-1 \cdot Z + X \cdot (2^{(n+2)/2} - 1) \\ &\quad - Y \cdot (2^{(n+2)/2} + 1)\} / p^2 \\ &= \{-p + (X - Y) \cdot 2^{(n+2)/2}\} / p^2 \quad \dots\dots(22) \end{aligned}$$

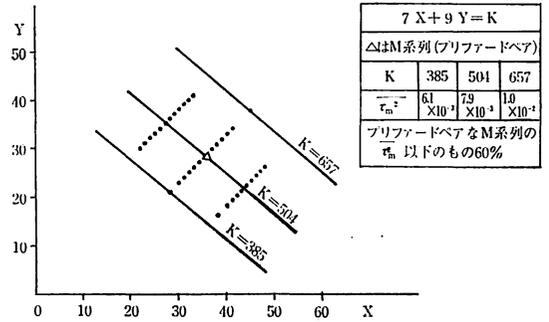
$$\begin{aligned} \bar{\tau}_m^2 &= \{Z + X \cdot (2^{(n+2)/2} - 1)^2 \\ &\quad + Y \cdot (2^{(n+2)/2} + 1)^2\} / p^3 \\ &= \{p + K \cdot 2^{(n+4)/2}\} / p^3 \quad \dots\dots(23) \end{aligned}$$

ただし、

$$K = X \cdot (2^{n/2} - 1) + Y \cdot (2^{n/2} + 1) \quad \dots\dots(24)$$

(3) ゴールド符号の相互相関関数の自乗平均値

すでに述べたように、ゴールド符号の相互相関関数の値の頻度はその都度計算により求めなければならない。多元接続を行う場合、拡散符号に必要な特性とし、使用されるすべての符号との相関ができるだけ小さなものほどよく、これは、拡散符号間の相互相関関数の自乗平均



第3図 ゴールド符号の相互相関関数の値の頻度の分布

M系列は [7, 3], [7, 3, 2, 1] で、X, YはM系列相互の位相が0のゴールド符号と位相が0以外のゴールド符号との相互相関関数の値15/127, -17/127の頻度。

値ができるだけ小さな符号を選ぶことになる。n=7の時の127種類のゴールド符号の相互相関関数について求めたKの値、及びX, Yの分布を第3図に示す。使用したM系列は、プリファードペアな [7, 3] [7, 3, 2, 1] で、M系列相互の位相が0のゴールド符号と、位相を0以外に変えて得られる126種類のゴールド符号との相互相関関数の値の頻度を示してある。この図から、Kの値は385から657の間にあるので、 $\bar{\tau}_m^2$ の最小値は 6.1×10^{-3} である。また、 $|\bar{\tau}_m|$ は(19)式により $(X - Y) = 8$ の時最小となるので、 $|\bar{\tau}_m|$ 及び $\bar{\tau}_m^2$ を小さくするには、頻度がX=28, Y=21に近いゴールド符号を使用するとよい。この例では、M系列より $\bar{\tau}_m^2$ の小さいものが約60%ある。ゴールド符号を構成するM系列の組合せを変えても、Kの値及びX, Yの分布はほぼ同じである。

4. M系列とゴールド符号の比較

ここでは、プリファードペアなM系列で構成するゴールド符号と、M系列の自己相関関数、相互相関関数及び符号の種類を比較し、次数nが11次以上ならば、両者の自己相関関数及び相互相関関数はほぼ等しいことを示す。なお、M系列の特性については、例えば文献(5)等で詳細に述べられているが、以下に述べる説明の理解を容易にするため、それらのまとめを第7表に示す。

4.1 自己相関関数の比較

M系列の自己相関関数は、第7表に示すように、同期時には相関値1のピークを持ち、非同同期時には一律に $-1/p$ の相関値を持つ。

一方、ゴールド符号の場合には3.2で述べたように、同期時には相関値1のピークを持つが、非同同期時には $-1/p$, $(2^{(n+1)/2}-1)/p$, $-(2^{(n+1)/2}+1)/p$ のいずれかの相関値を持つ。

第7表 M系列の性質⁽⁴⁾⁽⁵⁾⁽⁶⁾

項目	性質	例
1. 周期性	$\circ p=2^n-1$ の周期をもつ。	$\circ n=7$ の時、周期 p は 127。
2. 均一性	$\circ 1$ 周期内での“1”の出現回数は“0”の出現回数より1回多い。	$\circ n=7$ の時、“1”は 64 回、“0”は 63 回出現。
3. 連なり性	$\circ 1$ 周期内における連なり数 $k(\leq n-2)$ の出現回数は、 $2^{n-k}-1$ であり、“1”と“0”の連なりの出現回数は等しい。 \circ 連なり数の分類数は、 2^{n-1} である。 \circ 連なり数 k の出現率は 2^{-k} で、連なり数 $(n-1)$ の“0”が 1 回、連なり数 n の“1”が 1 回ある。	$\circ p=127$ の時、1 周期内で“1”が 5 個連続している所が $2^{7-5}-1=2$ 回あり“0”も 2 回ある。 $\circ p=127$ の時、“1”及び“0”の連なりは、全部で $2^{7-1}=64$ に区分される。 \circ 連なり数 5 の出現率は 2^{-5} 。又、“1”が 7 個連続している所が 1 回、“0”が 6 個連続している所が 1 回ある。
4. 尽状態性	\circ M系列を作る n 段シフトレジスタは、周期 p の間に、 $1\sim p$ までの全ての状態を 1 回ずつ取る。	$\circ n=7$ の時、シフトレジスタは、1 から 127 までの全ての状態を 1 回ずつ取る。
5. シフト加法性	\circ M系列と、その位相を任意(但し、零及び周期の倍数を除く)ずらした系列との和の系列は、元のM系列の位相を一定数ずらしたM系列に等しい。	\circ M系列を $\{a_k\}$ とすると、 $a_k \oplus a_{k+l} = a_{k+m}$ ($l \neq 0, l \neq np, n$: 整数) となる整数 m が存在する。 l と m の間の関係は未知だが、 l に対し m は計算により求まる。又、 l と m の間には、1 対 1 の対応関係が成立ち、 $l=1\sim p$ の時、 m も $1\sim p$ の全ての値を取る。
6. 自己相関特性	\circ 自己相関関数 $\phi_A(i)$ は、位相に i より、 $\phi_A(i) = \begin{cases} 1 & i=0 \\ -1/p & i \neq 0, np \end{cases}$	
7. 相互相関特性	\circ 相互相関関数 $\phi_c(i)$ は、M系列の次数及び組合せにより決まる特定値のみを取る。 \circ M系列の相互相関関数の平均値 τ_m は、 $\tau_m = \frac{1}{p^2}$ であり、標準偏差 $\tau\sigma$ は、 $\tau\sigma = (p^3 + p^2 - p - 1)^{1/2} / p^3$ となる(文献(4))。	$\circ p \cdot \phi_c(i) = \tau(i)$ とすると、 n が 10 次までについては文献(4)から $\tau(i) = 2^k \cdot m - 1$ m : 0 または適当な整数 で表され、 3 ~ 4 次の時 $k=1$ 5 ~ 7 次の時 $k=3$ 8 ~ 10 次の時 $k=4$ となり、2 つのM系列がイメージの時 $k=2$ となる。11 次については今回計算した結果 $k=5$ となった。

したがって、ゴールド符号の自己相関関数の値は、M系列に比較し、非同期時に最大 $(2^{(n+1)/2})/p$ 劣化する。しかし、この劣化は、例えば $n=11$ の時 0.031 なので、 $n \geq 11$ ならば、ほぼ零とみなすことができる。

なお、自己相関関数の弁別指数 ID は、M系列の場合、 $ID_M = 2^n$ であり、ゴールド符号の場合、 $2^n - 2^{(n+1)/2} \leq ID_G \leq 2^n + 2^{(n+1)/2}$ であるので、両者の差は $|ID_M - ID_G| \leq 2^{(n+1)/2}$ となる。

4.2 相互相関関数の比較

M系列がプリファードペアの時、その相互相関関数の値及び頻度は、第3表、第4表で与えられる。

また、ゴールド符号を構成するM系列もプリファードペアなので、その相互相関関数も第3表、第4表の値を

取る。ただし、この場合、頻度は未知である。

したがって、次数 n が 11 次以上であれば、両者の相互相関関数の値は、ほぼ零とみなすことができる。

なお、相互相関関数の値と頻度の特性を示す自乗平均値は、M系列の場合、M系列の組合せに無関係に一定であるが、ゴールド符号の場合、第3図に示したように一定でなく、M系列より自乗平均値の小さいもののがかなりある。

4.3 符号の種類比較

次数 n のM系列の種類は、それを生成する原始多項式の数であり、これはオイラー (Euler) 関数* で表され

*オイラー関数については、例えば文献(11)等を参考にされたい。

第8表 [7, 3] と他の7次のM系列との $\tau(i)$ の値及びその頻度 (Δ 印はプリファードペアの条件を満たすことを示す)

M系列の種類	$\tau(i)$ の種類	$\tau(i)$ (頻度)
[7, 1] [7, 6] Δ [7, 3, 2, 1] Δ [7, 4, 3, 2] [7, 5, 2, 1] [7, 5, 3, 1] [7, 6, 4, 1] [7, 6, 4, 2] Δ [7, 5, 4, 3, 2, 1] [7, 6, 5, 3, 2, 1]	3	15(36) -1(63) -17(28)
[7, 5, 4, 3] [7, 6, 3, 1] [7, 6, 5, 2] [7, 6, 5, 4] [7, 6, 5, 4, 3, 2] [7, 6, 5, 4, 2, 1]	7	23(7) 15(14) 7(28) -1(35) -9(28) -17(14) -41(1)
[7, 4] (IMAGE)	11	19(7) 15(14) 11(14) 7(7) 3(21) -1(14) -5(7) -9(21) -13(8) -17(7) -21(7)

る。

例えば、 $n=7$ の時、M系列は18種類あるが、このうち9種類はイメージの系列である。更に、(6)式、(7)式の関係を満たすM系列はプリファードペアとなり第3表、第4表の値を取るが、(6)式、(7)式以外にもこの値を取るM系列の組合せがある。すなわち、(6)式、(7)式はM系列が第3表、第4表の値を取る十分条件ではあるが、必要条件ではない。[7, 3]に対する相互相関関数の値及び頻度の計算結果は第8表のとおりで、(6)式から導かれるM系列は3種類であるのに対し、第3表を満たすM系列は10種類ある。他の8種類のM系列についても同様であるので、7次のM系列全体で(6)式から導かれるプリファードペアなM系列は27種類であるが、第3表を満たすM系列の組合せは90種類ある。

一方、周期 $p=(2^n-1)$ のゴールド符号の種類は、3.1で述べたように相異なる二つのM系列1組に対し 2^n+1 種類あり、 $n=7$ の時129通りである。したがって、(6)式を満たすプリファードペアなM系列で構成するゴールド符号は $129 \times 27 = 3483$ 種類であるのに対し、相互相関関数が第3表の3値を取るゴールド符号は $129 \times 90 = 11610$ 種類ある。

5. 結 言

M系列の相互相関関数がある特定な上界を持つ関係を調べ、相互相関関数が3値を取る条件のうち、次数が偶数の場合について明らかにした。

更に、ゴールドの符号自己相関関数及び相互相関関数

の特性についても明らかにし、M系列との比較を行った。

M系列は、スペクトラム拡散通信の拡散符号としてすでに使用されているが、これらの結果から、符号の種類がM系列より多いゴールド符号も、M系列の種類と次数を適当に選び構成するならば、M系列とはほぼ同程度の特性で使用できる。

謝 辞

本研究の機会を与えていただいた宮島通信機器部長と、この論文をまとめるにあたり有益な助言をいただいた情報処理部音声研究室吉谷研究官、並びに、有益な討論と助言をいただいた通信系研究室の横山主任研究官、塚田研究官、水野技官に深く感謝いたします。

参 考 文 献

- (1) 角川靖夫, 横山光雄, 水野光彦, 塚田藤夫, 柴田正司; “スペクトラム拡散技術を用いた地上通信方式について”, 第57回電波研研究発表会予稿, pp. 13—27, July 1979.
- (2) 松尾良雄; “スプレッドスペクトラム通信”, 電子科学, pp. 89, Nov, 1978.
- (3) Dixon, R. C., 立野敏, 片岡志津雄, 飯田清 (共訳), スペクトラム拡散通信方式, ジャテック, 1979.
- (4) 吉谷清澄; “M系列の相互相関について”, 電波研季報, 17, No. 90, pp. 244—248, May 1971.
- (5) 吉谷清澄; PN系列——特にM系列について”, 電波研季報, 17, No. 90, pp. 249—263, May 1971.
- (6) G. Hoffmann de Visme 著, 伊理正夫, 伊理由美共訳, 2値系列, 共立出版, 1977.
- (7) Peterson, W. W., Weldon, E. J, Error-Correcting Codes, 2nd Edition, MIT Press, 1972.
- (8) 宮川洋, 岩垂好裕, 今井秀樹, 符号理論, 昭晃堂, 1976.
- (9) 嵩忠雄, 都倉信樹, 岩垂好裕, 稲垣康善, 符号理論, コロナ社, 1975.
- (10) 松坂和夫, 代数系入門, 岩波書店, 1976.
- (11) Golomb, S. W., Shift Register Sequences, Holden-Day Inc., 1967.
- (12) Gold, R.; “Optimal Binary for Spread Spectrum Multiplexing”, IEEE Trans., Inf., Theory, IT-13, pp. 619—621, Oct. 1967.
- (13) Gold, R.; “Maximal Recursive Sequences with 3-valued Recursive Cross-Correlation Functions”, IEEE Trans., Inf., Theory, IT-14, pp. 154—156, Jan. 1968.

- (14) Orr, J.A. ; "Effects Fading on A Multi-User SS system Using DS Modulation", Doctor Thesis of University of Illinois, 1969.

