International Conference on
Information, Communications and Signal Processing
ICICS '97
Singapore, 9-12 September 1997

A New Method of Modulated Orthogonal Sequence Generation for MPSK Signal Constellation

Seong Ill Park, Kwang Soon Kim, Jeongsoon Park, So Ryoung Park, and Iickho Song

Department of Electrical Engineering
Korea Advanced Institute of Science and Technology (KAIST)
373-1 Guseong Dong, Yuseong Gu
Daejeon 305-701, Korea
Tel : +82-42-869-3445
Fax : +82-42-869-3410
e-mail : isong@sejong.kaist.ac.kr

Abstract

In this paper, a code sequence generation method of the modulated orthogonal sequence is suggested. By this method, a code is generated only with integer sums and modular techniques. The autocorrelation and cross-correlation characteristics of these sequences are investigated. The sequence generated by the suggested method has the orthogonality and satisfies the mathematical lower bound of the cross-correlation.

1 Introduction

For code division multiple access (CDMA) systems, some sequences are suggested: among the examples are the $m-$sequences [1] or Gold's sequences [2]. These sequences, however, have some co-channel interference of which the value exceeds $1/\sqrt{K}$, where K is the spreading ratio of the CDMA systems. The co-channel interference in these systems lowers to some degree the performance of the system.

In [3], an orthogonal sequence is proposed. When the period is K, the autocorrelation function of the code sequence is 0 except for the every Kth term, and the absolute value of the cross-correlation is $1/K$. This absolute value $1/K$ of the cross-correlation function is the mathematical lower bound for orthogonal sequences. Since this code sequence is made by the discrete Fourier transform (DFT) method, however, it is very complicated to generate this sequence.

In this paper, we suggest a generation method of the sequence proposed in [3] for M-ary phase shift keying (MPSK) information symbols. In Section 2, the generation method is described, which can be accomplished only by integer sum and modular techniques. For the multiple user access cases, two examples are shown in Subsection 2.2. The characteristics of the code sequences generated by the suggested method are investigated in Section 3. We also discuss the autocorrelation and cross-correlation properties of the suggested code sequence.

2 Generation of code sequences

2.1 The method

Let b_i, $i = 0, 1, 2, ..., N-1$, be the *information* symbols, N be the length of the information symbols, and $s_l, l = 0, 1, 2, ..., N^2 - 1$, be the *code* symbols. Without loss of generality, we can assume that $|s_l|^2 = 1$.

Assuming MPSK signal constellation in this paper, consider the information symbol value set

$$I = \{c_p | c_p = W_M^p,\ p = 0, 1, 2, ..., M-1\}, \quad (1)$$

the DFT symbol value set

$$F = \{w_q | w_q = W_N^q,\ q = 0, 1, 2, ..., N-1\}, \quad (2)$$

and the code symbol value set

$$C = \left\{d_k | d_k = W_L^k,\ k = 0, 1, 2, ..., L-1\right\}, \quad (3)$$

where $L = LCM[M, N]$ and

$$W_M = \exp\left[\frac{2\pi j}{M}\right] \quad (4)$$

with $j = \sqrt{-1}$. Note that I and C are the set of the values of the information symbols and that of the code symbols, respectively. That is, the value of b_i is an element in I and the value of s_l is an element in C.

Then we suggest the transmitting code sequence as follows

$$s_l = b_{P(l)} w_{R(mQ(l)P(l),N)}, \quad (5)$$

where $R(\alpha, \beta)$ is the remainder of α dividing β, $P(l) = R(l, N)$, $Q(l)$ is the quotient of l dividing N, and m is

$m = 1, M = 4, N = 3, L = 12$					
l	$Q(l)$	$P(l)$	$J(P(l), b)$	$R(mQ(l)P(l), N)$	$V(l)$
0	0	0	0	0	0
1	0	1	1	0	3
2	0	2	1	0	3
3	1	0	0	0	0
4	1	1	1	1	7
5	1	2	1	2	11
6	2	0	0	0	0
7	2	1	1	2	11
8	2	2	1	1	7

Table 1: Code index generation when $m = 1, M = 4, N = 3$ and $L = 12$. The information symbols are $\{W_4^0, W_4^1, W_4^1\}$.

$m = 2, M = 4, N = 3, L = 12$					
l	$Q(l)$	$P(l)$	$J(P(l), b)$	$R(mQ(l)P(l), N)$	$V(l)$
0	0	0	0	0	0
1	0	1	1	0	3
2	0	2	1	0	3
3	1	0	0	0	0
4	1	1	1	2	11
5	1	2	1	1	7
6	2	0	0	0	0
7	2	1	1	1	7
8	2	2	1	2	11

Table 2: Code index generation when $m = 2, M = 4, N = 3$ and $L = 12$. The information symbols are $\{W_4^0, W_4^1, W_4^1\}$.

the user index (a different number is given to each user). We have

$$\begin{aligned} s_l &= c_{J(P(l),b)} W_N^{R(mQ(l)P(l),N)} \\ &= W_M^{J(P(l),b)} W_N^{R(mQ(l)P(l),N)} \\ &= W_L^{R\left(J(P(l),b)\frac{L}{M}+R(mQ(l)P(l),N)\frac{L}{N},L\right)} \\ &= d_{R\left(J(P(l),b)\frac{L}{M}+R(mQ(l)P(l),N)\frac{L}{N},L\right)} \\ &= d_{V(l)}, \end{aligned} \quad (6)$$

where $J(i, b)$ is the index of the value of b_i, (i.e., if $b_i = c_k$, then $J(i, b) = k$, $k = 0, 1, ..., M-1$), and

$$V(l) = R\left(J(P(l), b)\frac{L}{M} + R(mQ(l)P(l), N)\frac{L}{N}, L\right). \quad (7)$$

An implication of (6) and (7) is that the code sequence can be obtained easily by calculating only the symbol indices.

2.2 An example

Before starting transmission, we can determine all parameters except for the information symbols. If the information is determined, therefore, we can generate the code sequences by only some summations. For example, assume that we use QPSK information symbol ($M = 4$), transmit 3 symbols by one code sequence ($N = 3$), and have 2 users with user indices $m = 1, 2$. The elements of the sets I, F, and C are shown in Figures 1-3. The code sequence generation is tabulated in Tables 1 and 2 when the information symbols are $\{W_4^0, W_4^1, W_4^1\}$. Specifically, the code sequence $\{s_l\}$ of the first user is

$$\left\{W_{12}^{V(l)}\right\}_{l=0}^{8} = \{W_{12}^0, W_{12}^3, W_{12}^3, W_{12}^0, W_{12}^7, W_{12}^{11}, W_{12}^0, W_{12}^{11}, W_{12}^7\}, \quad (8)$$

and that of the second user is

$$\left\{W_{12}^{V(l)}\right\}_{l=0}^{8} = \{W_{12}^0, W_{12}^3, W_{12}^3, W_{12}^0, W_{12}^{11}, W_{12}^7, W_{12}^0, W_{12}^7, W_{12}^{11}\}. \quad (9)$$

3 Characteristics of the code sequence

Using the Fourier transform multiplication method [3], we now investigate the autocorrelation and cross-correlation of the code sequence generated by the suggested method.

Definition 1. Let us define the $N \times N$ DFT matrix as

$$F_N = \frac{1}{\sqrt{N}}\left[W_N^{-ij}\right], \quad (10)$$

where $i, j = 0, 1, ..., N-1$.

Definition 2. The diagonalized matrix $D(x_l)$ of a sequence x_l, $l = 0, 1, ..., H$, is defined as

$$D(x_l) = \begin{bmatrix} x_0 & 0 & 0 & \cdots & 0 \\ 0 & x_1 & 0 & \cdots & 0 \\ 0 & 0 & x_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & x_H \end{bmatrix}. \quad (11)$$

Definition 3. The element-by-element multiplication of two matrices $A = [a_{ij}]$ and $B = [b_{ij}]$ of the same size is defined as

$$A * B = [a_{ij}\, b_{ij}]. \quad (12)$$

3.1 Autocorrelation

Using the method in [3], the autocorrelation AR of the code sequence can be evaluated as

$$AR = F_{N^2}^{-1}\left\{G\left(F_{N^2}S\right) * G\left(\overline{F_{N^2}S}\right)\right\}, \quad (13)$$

where $\overline{A}$ is the conjugate of A, and $G(A)$ is the column vector made by the diagonal elements of A.

Now, it is easy to see that

$$F_{N^2}S = \frac{1}{N}\begin{bmatrix} W_{N^2}^0 & W_{N^2}^0 & \cdots & W_{N^2}^0 \\ W_{N^2}^0 & W_{N^2}^{-1} & \cdots & W_{N^2}^{-(N^2-1)} \\ W_{N^2}^0 & W_{N^2}^{-2} & \cdots & W_{N^2}^{-2(N^2-1)} \\ \vdots & \vdots & \ddots & \vdots \\ W_{N^2}^0 & W_{N^2}^{-(N^2-1)} & \cdots & W_{N^2}^{-(N^2-1)(N^2-1)} \end{bmatrix} \cdot \begin{bmatrix} s_0 & 0 & 0 & \cdots & 0 \\ 0 & s_1 & 0 & \cdots & 0 \\ 0 & 0 & s_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & s_{N^2-1} \end{bmatrix} \tag{14}$$

and

$$G(F_{N^2}S) = \frac{1}{N}\begin{bmatrix} W_{N^2}^0 s_0 \\ W_{N^2}^{-1} s_1 \\ W_{N^2}^{-4} s_2 \\ \vdots \\ W_{N^2}^{-(N^2-1)(N^2-1)} s_{N^2-1} \end{bmatrix} = \frac{1}{N}\left[W_{N^2}^{-l^2} s_l\right]. \tag{15}$$

Then

$$G(F_{N^2}S) * G(\overline{F_{N^2}S}) = \frac{1}{N^2}\left[W_{N^2}^{-l^2} s_l \, W_{N^2}^{l^2} \overline{s_l}\right] = \frac{1}{N^2}\left[|s_l|^2\right]. \tag{16}$$

Using (13) and (16), the autocorrelation can be obtained as

$$F_{N^2}^{-1}\left\{G(F_{N^2}S) * G(\overline{F_{N^2}S})\right\} = \frac{1}{N^3}\begin{bmatrix} \sum_{l=0}^{N^2-1} W_{N^2}^0 |s_l|^2 \\ \sum_{l=0}^{N^2-1} W_{N^2}^{l} |s_l|^2 \\ \sum_{l=0}^{N^2-1} W_{N^2}^{2l} |s_l|^2 \\ \vdots \\ \sum_{l=0}^{N^2-1} W_{N^2}^{(N^2-1)l} |s_l|^2 \end{bmatrix} = \frac{1}{N}\begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{17}$$

since $\sum_{l=0}^{N^2-1} W_{N^2}^{kl} = N^2\delta(k)$.

Eq. (17) implies that the code sequence generated by the suggested method possesses the same autocorrelation and orthogonality as the code sequence defined in [3].

3.2 Cross-correlation

In this section, we will investigate the cross-correlation property of the code sequence. Let x_l and y_l be the code sequences of two users. Then the cross-correlation CR can be obtained as

$$CR = F_{N^2}^{-1}\left\{G(F_{N^2}A) * G(\overline{F_{N^2}B})\right\}, \tag{18}$$

where $A = D(x_l)$ and $B = D(y_l)$. Following the steps similar to those used in (14)-(17), we have from (18)

$$\begin{aligned} CR &= \frac{1}{N^2}F_{N^2}^{-1}\left[W_{N^2}^{-l^2} x_l W_{N^2}^{l^2} \overline{y_l}\right] \\ &= \frac{1}{N^2}F_{N^2}^{-1}\left[x_l \overline{y_l}\right] \\ &= \frac{1}{N^3}\left[\sum_{l=0}^{N^2-1} W_{N^2}^{kl} x_l \overline{y_l}\right]. \end{aligned} \tag{19}$$

The kth element of this column vector can be obtained as

$$\begin{aligned} &\frac{1}{N^3}\sum_{l=0}^{N^2-1} W_{N^2}^{kl} x_l \overline{y_l} \\ = &\frac{1}{N^3}\sum_{l=0}^{N^2-1} W_{N^2}^{k(NQ(l)+P(l))} c_{J(P(l),x)} \overline{c_{J(P(l),y)}} W_N^{(m_x-m_y)Q(l)P(l)} \\ = &\frac{1}{N^3}\sum_{P(l)=0}^{N-1} c_{J(P(l),x)} \overline{c_{J(P(l),y)}} W_{N^2}^{kP(l)} \sum_{Q(l)=0}^{N-1} W_N^{Q(l)\{k+P(l)(m_x-m_y)\}}, \end{aligned} \tag{20}$$

where the subscripts x and y in m_x and m_y are used to denote the first and second users, respectively. Now the second summation of the right-hand side of (20) is

$$\sum_{Q(l)=0}^{N-1} W_N^{Q(l)\{k+P(l)(m_x-m_y)\}} = \begin{cases} N, & \text{if } R(k+P(l)(m_x-m_y), N) = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{21}$$

Using (19), (20), and (21), we have

$$CR = \frac{1}{N^2}\left[\sum_{P(l)=0}^{N-1} c_{J(P(l),x)} \overline{c_{J(P(l),y)}} W_{N^2}^{kP(l)} \delta(R(k+P(l)(m_x-m_y), N))\right]. \tag{22}$$

If we denote by ϕ the value of $P(l)$ satisfying $R(k + P(l)(m_x - m_y), N) = 0$, then the absolute value squared of the kth element is

$$\frac{1}{N^4} c_{J(\phi,x)} \overline{c_{J(\phi,y)}} W_{N^2}^{k\phi} \overline{c_{J(\phi,x)}} c_{J(\phi,y)} W_{N^2}^{-k\phi} = \frac{1}{N^4} \left|c_{J(\phi,x)}\right|^2 \left|c_{J(\phi,y)}\right|^2 . \quad (23)$$

From (22) and (23), we can observe that the absolute value of the cross-correlation of two sequences with different user indices has the constant absolute value of $1/N^2 = 1/K$, since the elements in the set I have unity magnitude.

4 Concluding remark

We have suggested an easy method of making an orthogonal sequence. This method consists only of integer sums and modular techniques. The sequences generated by the suggested method possesses the orthogonality after modulated by information symbols. The cross-correlation of the sequence has the constant absolute value which satisfies the mathematical lower bound.

Acknowledgements

This research was supported by Korea Science and Engineering Foundation (KOSEF) under Grant 961-0923-134-2 for which the authors would like to express their thanks.

References

[1] S. W. Golomb, *Shift-Register Sequences*, San Francisco, CA: Holden-Day, 1967.

[2] D. V. Sarwate and W. B. Pursley, "Cross-correlation properties of pseudo-random and related sequences," *Proc. IEEE,* vol. 68, pp. 593-619, May 1980

[3] N. Suehiro and M. Hatori, "Modulatable orthogonal sequences and their application to SSMA systems," *IEEE Trans. Inform. Theory,* vol. IT-34, pp. 93-100, January 1988.

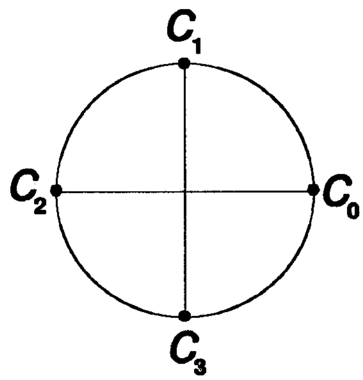

Figure 1: The elements of I when $M = 4$.

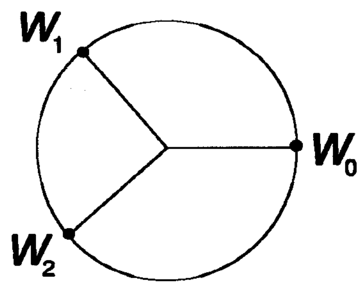

Figure 2: The elements of F when $N = 3$.

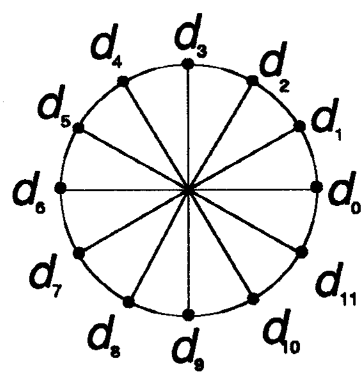

Figure 3: The elements of C when $L = 12$.