AN ANALYSIS OF A MODULATED ORTHOGONAL SEQUENCE

Seong Ill Park, Iickho Song*, Kwang Soon Kim*, Naoki Suehiro†, and Jooshik Lee**

*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

† Institute of Applied Physics
University of Tsukuba
Tsukuba-shi, Ibaraki, 305, Japan

ABSTRACT

In this paper, a new generation and an information construction methods for a modulated orthogonal sequence are suggested: the sequence is generated by only integer sums and modular techniques. The autocorrelation and cross-correlation characteristics of the sequence are investigated via a new procedure. A modified sequence also having the orthogonality and satisfying the mathematical lower bound of the cross-correlation is proposed, and the symbol error probability of the sequence is investigated.

1. INTRODUCTION

For direct sequence code division multiple access (DS/CDMA) systems, some sequences are suggested: among the examples are the m−sequences or Gold's sequences [1]-[6]. These sequences, however, have some co-channel interference. The co-channel interference in these systems lowers to some degree the performance of the systems. For example, the variance of inter-user interference is $\frac{K-1}{3N}$, where K is the number of users and N is the spreading ratio [7].

In [8], an orthogonal sequence is proposed. When the period is N, the autocorrelation function of the sequence is 0 except for every Nth term. Therefore, systems using this sequence do not suffer from inter-user interference. This sequence, however, has some disadvantages. One is that it is highly time-consuming to generate the sequence and to reconstruct the information symbols. As an example of the generation complexity, consider a DS/CDMA system, where length 1024 sequences are used. To generate sequences of this length, we need 37×37 discrete Fourier transform (DFT) matrix for every 37 information symbols. (Here 37 is the smallest prime number whose square is greater than or equal to 1024.) Another is that, since length N^2 sequences are generated from N information symbols, receivers have to wait N^2 time units to get N informations. Still another disadvantage of the sequence is that one dummy symbol has to be included for the sequence generation.

In this paper, we suggest an information reconstruction method of the sequence proposed in [8]. We then suggest a modified orthogonal sequence and analyze the system performance with the modified sequence under nonselective fading environment. In Section 2, we briefly introduce an orthogonal sequence which is suggested in [8]. Methods of information reconstruction are described in Section 3. In Section 4, a modified sequence which overcomes the disadvantages of the sequence in [8] is suggested. System performance with the modified sequence is investigated in Section 5.

2. AN ORTHOGONAL SEQUENCE

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

$$F_N = \frac{1}{\sqrt{N}}\left[W_N^{-ij}\right] \text{ and } F_{N,m} = \frac{1}{\sqrt{N}}\left[W_N^{-ijm}\right], \qquad (1)$$

where $i, j = 0, 1, ..., N-1$, m is an integer, and $W_N = \exp\left(2\pi\sqrt{-1}/N\right)$.

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

$$D(\{x_l\}) = diag\,\{x_l\}. \qquad (2)$$

Definition 3. Let the quotient and residual functions Q and R be defined as

$$Q(\alpha, \beta) = q,\ R(\alpha, \beta) = r, \qquad (3)$$

where $\alpha = q\beta + r$, $0 \le r < \beta$, and $q \ge 0$.

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

0-7803-4428-6/98 $10.00

Information symbols are divided into N blocks, diagonalized, and multiplied by a DFT matrix. Then the N^2 elements of the output matrix $G = [g_{pq}]$ constitute orthogonal sequences s_l, $l = 0,1,... N^2 - 1$ [8]. These procedures can be expressed as

$$G = F_{N,m}^{-1} D(\{b_i\}), \tag{4}$$

and

$$s_{pN+q} = g_{pq}, \; p,q = 0,1,2,...,N-1. \tag{5}$$

When N is a prime number, we can generate $N-1$ orthogonal sequences: that is, $N-1$ users can use the same channel simultaneously in CDMA systems. The method of generating the sequences, however, is too time-consuming and complex, since $N \times N$ complex matrix multiplications are required for every N information symbols. Since user capacity increases as N, it is desirable to use large values of N: the complexity, however, increases as N^2. In addition, it is desirable that one information symbol generates N code symbols *individually*, as opposed to the method in (4), where N information symbols *collectively* generate N^2 code symbols.

3. RECONSTRUCTION OF INFORMATION

3.1. Conventional method

A procedure of information reconstruction is as follows [8]. Let us assume the received sequences for multiple access are

$$\{r_l\} = \left\{ \sum_{k=1}^{K} s_l^{(k)} \right\}, \tag{6}$$

where K is the number of users and $s_l^{(k)}$ is the $(l+1)$th symbol of the kth user. Then the received symbols $\{r_l\}$ will pass through the matched filter with coefficients

$$p_l = W_N^{-l_q l_r m(k)}, \; 0 \le l \le N^2 - 1, \tag{7}$$

where $m(k)$ is the index of the kth user, and $l_q = Q(l,N)$ and $l_r = R(l,N)$. The matched filter output is therefore [9]

$$\begin{aligned} y_l &= \sum_{i=0}^{N^2-1} r_i p_{R(i+l,N^2)} \\ &= \begin{cases} N \sum_{i=0}^{N-1} \sum_{k=1}^{K} b_i^{(k)} W_N^{-l_q i m(k)} & \text{if } l_r = 0, \\ 0 & \text{otherwise,} \end{cases} \end{aligned} \tag{8}$$

where $b_i^{(k)}$ is the $(i+1)$th information symbol of the kth user.

Let us now define the matched filter output matrix as [9]

$$Y = \begin{bmatrix} y_0 & y_1 & \cdots & y_{N-1} \\ y_N & y_{N+1} & \cdots & y_{2N-1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{(N-1)N} & y_{(N-1)N+1} & \cdots & y_{N^2-1} \end{bmatrix}. \tag{9}$$

Then the FFT processor outputs are given by

$$R = F_{N,m(k)}^{-1} Y, \tag{10}$$

and the column vector T_k made of the first column of R is

$$T_k = N^2 \left[\sum_{i=0}^{K} b_0^{(i)} \; b_1^{(k)} \; b_2^{(k)} \; \cdots \; b_{N-1}^{(k)} \right]^T. \tag{11}$$

As we can see in (11), information symbols of the kth user are reconstructed without inter-user interference except for the first information symbol.

3.2. A new method

The procedure described in 3.1 is too complex and needs $N \times N$ complex matrix multiplications. Here, based on the new generation method in [9], we suggest a simpler method to reconstruct information symbols. The $(p+1)$th element t_p of T_k is

$$\begin{aligned} t_p &= \sum_{q=0}^{N-1} W_N^{pqm(k)} y_{qN} \\ &= \sum_{l=0}^{N^2-1} r_l \sum_{q=0}^{N-1} W_N^{f(l,q)}, \end{aligned} \tag{12}$$

where $f(l,q) = \left[pq - Q(R(l+qN, N^2), N) \;\; R(R(l+qN, N^2), N) \right] m(k)$.

We calculate the exponent of W_N in (12). Since

$$R(l+qN, N^2) = \begin{cases} l+qN \\ \quad \text{if } 0 \le l+qN \le N^2-1, \\ l+qN-N^2 \\ \quad \text{if } N^2 \le l+qN \le 2N^2-N-1, \end{cases} \tag{13}$$

$$Q(R(l+qN, N^2), N) = \begin{cases} l_q + q \\ \quad \text{if } 0 \le l+qN \le N^2-1, \\ l_q + q - N \\ \quad \text{if } N^2 \le l+qN \le 2N^2-N-1, \end{cases}$$

and

$$R(R(l+qN, N^2), N) = l_r, \tag{14}$$

the exponent term of W_N in (12) is

$$f(l,q) = \begin{cases} (pq - l_q l_r - q l_r)\, m(k) \\ \quad \text{if } 0 \le l+qN \le N^2-1 \\ (pq - l_q l_r - q l_r + N l_r)\, m(k) \\ \quad \text{if } N^2 \le l+qN \le 2N^2-N-1 \end{cases} \tag{15}$$

Substituting (15) into (12), we have

$$\begin{aligned} t_p &= \sum_{l=0}^{N^2-1} r_l \sum_{q=0}^{N-1} W_N^{(pq - l_q l_r - q l_r) m(k)} \\ &= N \sum_{l=0}^{N-1} r_{lN+p} W_N^{-lpm(k)}. \end{aligned} \tag{16}$$

or

$$b_p^{(k)} = N \sum_{l=0}^{N-1} r_{lN+p} W_N^{-lpm(k)}. \quad (17)$$

That is, we can reconstruct the information symbols more easily by using (17).

4. A MODIFIED SEQUENCE

The orthogonal sequence considered in Section 2 has two disadvantages. One is, as we can see in (11), that the first information symbol cannot be reconstructed correctly. The other is that, since N information symbols collectively make a length N^2 sequence, we have to wait N^2 time units to get N information symbols. This also means that we have to have N^2 buffers. It is thus desirable to get one information symbol each from a length N subsequence of the length N^2 sequence.

The sequence we suggest is

$$s_l^{(k)} = b^{(k)} W_N^{lm(k)},\ k, l = 0, 1, 2, ..., N-1, \quad (18)$$

where $b^{(k)}$ represents an information symbol of the $(k+1)$th user. As stated previously, if N is a prime number, then we can generate $N-1$ different sequences by using different $m(k)$'s. Then the received symbols for multiple access is

$$r_l = \sum_{k=0}^{K-1} b^{(k)} W_N^{lm(k)}. \quad (19)$$

To reconstruct the information symbol of the $(i+1)$th user, we use

$$\begin{aligned} t &= \sum_{l=0}^{N-1} r_l W_N^{-lm(i)} \\ &= N b^{(i)}. \end{aligned} \quad (20)$$

As we can see in (20), we get one information symbol each from N sequential symbols without any inter-user interference. The autocorrelation and cross-correlation of the modified sequence are easily derived [9] as

$$AR = \frac{1}{\sqrt{N}} [1\ 0\ 0\ \cdots\ 0]^T \quad (21)$$

and

$$R_c = \frac{1}{\sqrt{N}} b^{(x)} \overline{b^{(y)}} \sum_{l=0}^{N-1} \delta\left(l + m(x) - m(y)\right), \quad (22)$$

where $b^{(x)}$ and $b^{(y)}$ represent the xth and yth user information symbols, respectively. We can see the modified sequence has orthogonality and satisfies the cross-correlation bound from (21) and (22).

5. PERFORMANCE ANALYSIS

The transmitted symbols by (18) are

$$s_l^{(k)} = b^{(k)} W_N^{lm(k)},\ l = 0, 1, ..., N-1, \quad (23)$$

and the transmitted signals are

$$\begin{aligned} s_l^{(k)}(t) &= Re\left[A \exp\left\{j\left(2\pi f_c t + \phi_l^{(k)}\right)\right\}\right], \\ &\quad (l-1)T_c \le t < lT_c, \end{aligned} \quad (24)$$

where $A = \sqrt{\frac{2E}{T_c}}$, E is the energy of the transmitted signal, T_c is the time interval for one transmitted signal, f_c is the carrier frequency, and $\phi_l^{(k)}$ is the phase containing the information.

We assume synchronization and nonselective fading channel with additive white Gaussian noise of variance $\sigma^2 = N_o/2$.

Then the received signals are

$$r_l(t) = \sum_{k=0}^{K-1} \rho^{(k)} s_l^{(k)}(t) + n_l(t), \quad (25)$$

where $\rho^{(k)}$ is a Rayleigh random variable of fading and $n_l(t)$ is zero mean Gaussian noise with variance $\sigma^2 = N_o/2$. The real part of the received signal is obtained as

$$\begin{aligned} r_l^r &= \int_{(l-1)T_c}^{lT_c} \left\{\sum_{k=0}^{K-1} \rho^{(k)} s_l^{(k)}(t) + n_l(t)\right\} A\cos(2\pi f_c t)\, dt \\ &= E \sum_{k=0}^{K-1} \rho^{(k)} \cos\phi_l^{(k)} + n_l^r, \end{aligned} \quad (26)$$

where

$$n_l^r = A \int_{(l-1)T_c}^{lT_c} n_l(t) \cos(2\pi f_c t)\, dt. \quad (27)$$

Similarly, the imaginary part is

$$r_l^i = E \sum_{k=0}^{K-1} \rho^{(k)} \cos\phi_l^{(k)} + n_l^i, \quad (28)$$

where $n_l^i = -A \int_{(l-1)T_c}^{lT_c} n_l(t) \sin(2\pi f_c t)\, dt$.

Then the complex received symbol is

$$\begin{aligned} r_l &= r_l^r + j r_l^i \\ &= E \sum_{k=0}^{K-1} \rho^{(k)} s_l^{(k)} + n_l, \end{aligned} \quad (29)$$

where $n_l = n_l^r + j n_l^i$.

Now the despreaded symbol for the first user is

$$\begin{aligned} t &= \sum_{l=0}^{N-1} r_l W_N^{-lm(0)} \\ &= NE\rho^{(0)} b^{(0)} + n, \end{aligned} \quad (30)$$

where $n = \sum_{l=0}^{N-1} n_l W_N^{-lm(0)}$ is a complex Gaussian random variable with variance $N\sigma^2$.

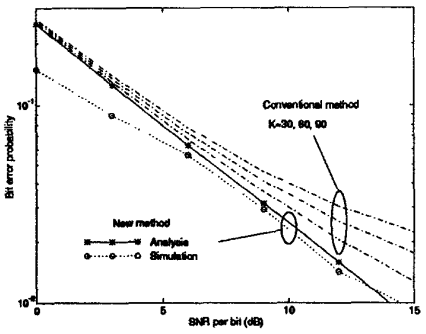

Figure 1: The bit error probabilities of conventional and suggested sequences: Parameters are $N = 511$, $K = 30, 60, 90$, and $M = 2$.

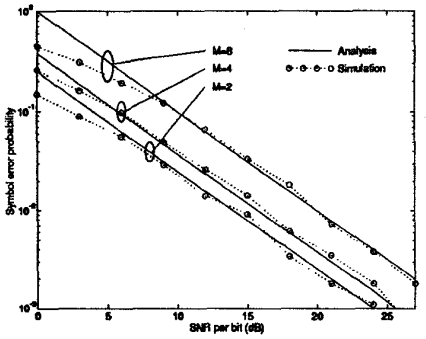

Figure 2: The symbol error probabilities of the suggested sequences: Parameters are $N = 511$, $K = 510$, and $M = 2, 4, 8$. Analysis and simulation results are shown.

From (30), we can obtain the symbol error probability of the suggested sequence. Since the only restriction on information symbols is that they should have the same amplitude, we can assume they are equally spaced on the unit circle in the complex plane. When SNR per bit $\bar{\gamma}_b >> 1$, the symbol error probability is well approximated as [10]

$$P_M \approx \frac{M-1}{M \log_2 M \sin^2(\pi/M) 2\bar{\gamma}_b}. \quad (31)$$

To compare the performance between the conventional and suggested sequences, we show the bit error probabilities in Figure 1: the parameters are $N = 511$, $K = 30, 60, 90$, and $M = 2$. Both analysis and simulation results of the suggested sequence are shown. We can clearly see that the bit error probabilities of the suggested sequence are not affected by the number K of users. Since (31) is an approximation more useful at high SNR, we see more difference between the analysis and simulation results at lower SNR.

In Figure 2, analysis and simulation results of the suggested sequence are shown when $N = 511$, $K = 510$, and $M = 2, 4, 8$. It is easily seen that the system performance is stable even when the number of users is large.

6. CONCLUDING REMARK

We have suggested simpler method of reconstructing information symbols for an orthogonal sequence. A modified sequence is also suggested. The sequence inherently rejects interference and can be easily implemented. Symbol error probabilities from the analysis and simulation results are shown. The performance of the suggested sequence is shown to be not affected by the number of users.

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.

7. REFERENCES

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

[2] R. Gold, "Maximal recursive sequences with 3-valued cross-correlation functions," *IEEE Trans. Inform. Theory*, vol. 14, pp. 154-156, Nov. 1968.

[3] 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

[4] T. Helleseth and T. Klove, "The Number of Cross-Join Pairs in Maximum Length Linear Sequences," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1731-1733, Nov. 1991.

[5] T. Chang, I. Song, H.M. Kim, and S.H. Cho, "Cross-Joins in de Bruijn Sequences and Maximum Length Linear Sequences," *IEICE Trans. Fundamentals*, vol. E76A, pp. 1494-1501, Sep. 1993.

[6] T. W. Cusick and H. Dobbertin, "Some New Three-Valued Crosscorrelation Functions for Binary m-Sequences," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1238-1240, July 1996.

[7] M. B. Pursley, "Performance evaluation for phase-coded spread spectrum multiple access communications-Part I: System analysis," *IEEE Trans. Comm.*, vol. 25, pp. 795-799, Aug. 1977.

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

[9] S. I. Park, *Optimum Modulation and Demodulation Techniques and Channel Coding Schemes for Spread Spectrum Multiple Access Systems*, Ph. D. Dissertation, Dept. Electr. Eng., Korea Advanced Institute of Science and Technology, Daejeon, 1998 (in preparation).

[10] John G. Proakis, *Digital Communications*, 1989, McGraw-Hill.