Published in Vehicular Technology Conference, 2004. VTC 2004-Spring. 2004 IEEE 59th
Volume 3, 17-19 May 2004 Page(s):1490 - 1493 Vol.3
Digital Object Identifier 10.1109/VETECS.2004.1390501

# Complex Orthogonal Sequences from Amicable Hadamard Matrices

L.C.Tran, J. Seberry, B. J. Wysocki and T. A. Wysocki, T. Xia, and Ying Zhao
Faculty of Informatics
University of Wollongong
Australia, NSW 2522
Wysocki@uow.edu.au

*Abstract*—**The paper deals with the novel technique of designing complex spreading sequences with only four phases (0.25π, 0.75 π, 1.25 π, 1.75 π). The interesting feature of those new sequences is the fact that not only the complex sequences are orthogonal but the real parts and imaginary parts are independently orthogonal. This can be utilized for spreading of complex constellation signals where the independent spreading using bipolar sequences (real part for in-phase component and imaginary part for quadrature component) can be applied. The paper introduces the theoretical background, and some example constructions of the amicable Hadamard matrices and the corresponding complex spreading sequences. The sequences are later modified using a diagonal method to achieve better correlation properties.**

***Spread spectrum, orthogonal sequences, complex spreading sequences, correlation functions***

## I. INTRODUCTION

Orthogonal bipolar spreading sequences are generally used for channel separation in direct sequence code division multiple access (DS CDMA) systems, e.g. [1]. The most commonly used sets of bipolar sequences are Walsh-Hadamard sequences [2], as they are easy to generate and simple to implement. It is well known, e.g. [3-5], that if the sequences have good aperiodic cross-correlation properties, the transmission performance can be improved for those CDMA systems where different propagation delays exist. However, the aperiodic cross-correlation between two Walsh-Hadamard sequences can rise considerably in magnitude if there is a non-zero delay shift between them [6]. Unfortunately, this is very often the case for up-link (mobile to base station) transmission, due to the differences in the corresponding propagation delays. As a result, significant multi-access interference (MAI) [3] occurs which needs to be combated either by complicated multi-user detection algorithms [5], or reduction in bandwidth utilization.

Another possible solution to this problem can be use of orthogonal complex valued polyphase spreading sequences, like those proposed in [6], which for some values of their parameters can exhibit a reasonable compromise between autocorrelation and cross-correlation functions. However, in most cases the choice of the parameters is not simple, and application of polyphase spreading sequences requires the use of analogue phase modulators that is rather a prohibitive factor.

In the paper we propose a novel technique to design complex spreading sequences with only four phases (0.25π, 0.75 π, 1.25 π, 1.75 π). The sequences are designed from bipolar amicable Hadamard matrices [1], which means that their real and imaginary parts are independently orthogonal. Therefore, the implementation of spreading is very simple, as it involves normal bipolar spreading for both in-phase and quadrature signal components.

The paper is organized as follows, the next section introduces some basic theory behind amicable Hadamard matrices as well as gives some simple examples of possible constructions. In Section 3, we show the technique for improving the correlation properties of the designed complex spreading sequences. An example design of the set of spreading sequences of length 32 is given in Section 4 together with the correlation characteristics of the set, while Section 5 concludes the paper.

## II. AMICABLE HADAMARD MATRICES

Suppose $\mathbf{I}+\mathbf{S}$ and $\mathbf{N}$ are amicable Hadamard matrices of order $n$ satisfying

$$(\mathbf{I}+\mathbf{S})\mathbf{N}^T = \mathbf{N}(\mathbf{I}+\mathbf{S})^T \quad \mathbf{S}^T = -\mathbf{S} \quad \mathbf{N}^T = \mathbf{N} \tag{1}$$

then $\begin{bmatrix} \mathbf{I}+\mathbf{S} & \mathbf{N} \\ -\mathbf{N} & \mathbf{I}+\mathbf{S} \end{bmatrix}$ and $\begin{bmatrix} \mathbf{N} & \mathbf{N} \\ \mathbf{N} & -\mathbf{N} \end{bmatrix}$ are amicable Hadamard matrices of order $2n$.

**Example 1**

Let $\mathbf{S} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $\mathbf{N} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ then $\mathbf{I}+\mathbf{S}$ and $\mathbf{N}$ are amicable Hadamard matrices of order 2. Hence amicable Hadamard matrices of this type exist for all orders $2^t$.

Hadamard matrices of order $n$ are said to be constructed using a circulant core if they use a matrix $C=c(i,j)$ of order n-1 where $c(i,j) = c(1, j-i+1) \pmod{n-1}$. For example

$$\mathbf{C} = \begin{bmatrix} 1 & 1 & -1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{bmatrix}$$

is a circulant core and

$$\mathbf{A} = \left[\begin{array}{c|ccc} 1 & 1 & 1 & 1 \\ \hline -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \end{array}\right]$$

is a Hadamard matrix constructed using a circulant core.

An Hadamard matrix of order $n$ is said to be constructed *using a back circulant core* if it used a matrix $\mathbf{D} = d(i,j)$ of order $n$ - 1 where $d(i,j) = d(1, j+i-1) \pmod{n-1}$.
For example

$$\mathbf{D} = \begin{bmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{bmatrix}$$

is a back circulant core and

$$\mathbf{B} = \left[\begin{array}{c|ccc} -1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \end{array}\right]$$

is a Hadamard matrix constructed using a back circulant core.

**Theorem 1** *A Hadamard matrix of order $p+1$ can be constructed with circulant core and with back circulant core when*

1. $p \equiv 3 \pmod 4$ *is prime* [8];
2. $p = q(q+2)$ *where $q$ and $q+2$ are both primes* [9],[10];
3. $p = 2^t - 1$ *where $t$ is a positive integer* [11];
4. $p = 4x^2 + 27$ *where $p$ is prime and $x$ a positive integer* [12].

**Theorem 2** *A Hadamard matrix of order n constructed using a circulant core* **A** *and a Hadamard matrix of order n constructed using a back circulant core* **B** *are amicable. That is* $\mathbf{AB}^T = \mathbf{BA}^T$.

This means there are amicable Hadamard matrices $2^t(p+1)$ for any integer $t$ and $p$ given in Theorem 1. From the amicability principle, the following theorem follows directly

**Theorem 3** *If matrices* **A** *and* **B** *are amicable Hadamard matrices, then a matrix* $\mathbf{X} = \mathbf{A} + j\mathbf{B}$; $j^2 = -1$, *is a complex orthogonal matrix, i.e.* $\mathbf{XX}^H = n\mathbf{I}$, *where* $(\cdot)^H$ *is the Hermitian transposition.*

## III. Modification Method

The sequence modification method is based on the fact that for a matrix $\mathbf{X}$ to be orthogonal, it must fulfil the condition $\mathbf{XX}^H = n\mathbf{I}$ . The modification is achieved by taking another orthogonal $n \times n$ matrix $\mathbf{D}_N$, and the new set of sequences is based on a matrix $\mathbf{W}_N$, given by:

$$\mathbf{W}_N = \mathbf{X}\mathbf{D}_N \tag{2}$$

Of course, the matrix $\mathbf{W}_N$ is also orthogonal. In [6], it has been shown that the correlation properties of the sequences defined by $\mathbf{W}_N$ can be significantly different to those of the original sequences.

A simple class of orthogonal matrices of any order are diagonal matrices with their elements $d_{i,j}$ fulfilling the condition:

$$|d_{l,m}| = \begin{cases} 0 & \text{for} \quad l \neq m \\ k & \text{for} \quad l = m \end{cases}; \quad l, m = 1, \ldots, n \tag{3}$$

To preserve the normalization of the sequences, the elements of $\mathbf{D}_N$, being in general complex numbers, must be of the form:

$$d_{l,m} = \begin{cases} 0 & \text{for} \quad l \neq m \\ \exp(j\phi_l) & \text{for} \quad l = m \end{cases}; \quad l, m = 1, \ldots, n \tag{4}$$

## IV. Sequence Comparison Criteria

In order to compare different sets of spreading sequences, we need a quantitative measure for the judgment. Therefore, we introduce here some useful criteria, which can be used for such a purpose. They are based on correlation functions of the set of sequences, since both the level of multiaccess interference and synchronization amiability depend on the cross-correlations between the sequences and the autocorrelation functions of the sequences, respectively. There are, however, several specific correlation functions that can be used to characterize a given set of the spreading sequences [3], [4], [5].

For general polyphase sequences $\{s_n^{(i)}\}$ and $\{s_n^{(l)}\}$ of length $N$, the discrete aperiodic correlation function is defined as [4]:

$$c_{i,k}(\tau)=\begin{cases}\dfrac{1}{N}\displaystyle\sum_{n=0}^{N-1-\tau} s_n^{(i)}[s_{n+\tau}^{(l)}]^*, & 0\le\tau\le N-1\\ \dfrac{1}{N}\displaystyle\sum_{n=0}^{N-1+\tau} s_{n-\tau}^{(i)}[s_n^{(l)}]^*, & 1-N\le\tau<0\\ 0, & |\tau|\ge N\end{cases} \quad (5)$$

where $[\bullet]^*$ denotes a complex conjugate operation. When $\{s_n^{(i)}\}=\{s_n^{(l)}\}$, Eqn. (5) defines the discrete aperiodic auto-correlation function.

Another important parameter used to assess the synchronization amiability of the spreading sequence $\{s_n^{(i)}\}$ is a merit factor, or a figure of merit [4], which specifies the ratio of the energy of autocorrelation function main-lobes to the energy of the auto-correlation function side-lobes in the form:

$$F=\frac{c_i(0)}{2\sum_{\tau=1}^{N-1}|c_i(\tau)|^2} \quad (6)$$

In DS CDMA systems, we want to have the maximum values of aperiodic cross-correlation functions and the maximum values of out-of-phase aperiodic autocorrelation functions as small as possible, while the merit factor as great as possible for all of the sequences used.

The bit error rate (BER) in a multiple access environment depends on the modulation technique used, demodulation algorithm, and the signal-to-noise power ratio (SNR) available at the receiver. Pursley [3] showed that in case of a BPSK asynchronous DS CDMA system, it is possible to express the average SNR at the receiver output of a correlator receiver of the $i$th user as a function of the average interference parameter (AIP) for the other $K$ users of the system, and the power of white Gaussian noise present in the channel. The SNR for $i$th user, denoted as $\mathrm{SNR}_i$, can be expressed in the form:

$$\mathrm{SNR}_i=\left(\frac{N_0}{2E_b}+\frac{1}{6N^3}\sum_{\substack{k=1\\k\neq i}}^{K}\rho_{k,i}\right)^{-0.5} \quad (7)$$

where $E_b$ is the bit energy, $N_0$ is the one-sided Gaussian noise power spectral density, and $\rho_{k,i}$ is the AIP, defined for a pair of sequences as

$$\rho_{k,i}=2\mu_{k,i}(0)+\mathrm{Re}\{\mu_{k,i}(1)\} \quad (8)$$

The cross-correlation parameters $\mu_{k,i}(\tau)$ are defined by:

$$\mu_{k,i}=N^2\sum_{n=1-N}^{N-1}c_{k,i}(n)[c_{k,i}(n+\tau)]^* \quad (9)$$

However, following the derivation in [13], $\rho_{k,i}$ for polyphase sequences may be well approximated as:

$$\rho_{k,i}\approx 2N^2\sum_{n=1-N}^{N-1}|c_{k,i}(n)|^2 \quad (10)$$

In order to evaluate the performance of a whole set of $M$ spreading sequences, the average mean-square value of cross-correlation for all sequences in the set, denoted by $R_{CC}$, was introduced by Oppermann and Vucetic [4] as a measure of the set cross-correlation performance:

$$R_{CC}=\frac{1}{M(M-1)}\sum_{i=1}^{M}\sum_{\substack{k=1\\k\neq i}}^{M}\sum_{\tau=1-N}^{N-1}|c_{i,k}(\tau)|^2 \quad (11)$$

A similar measure, denoted by $R_{AC}$ was introduced in [4] for comparing the auto-correlation performance:

$$R_{AC}=\frac{1}{M}\sum_{i=1}^{M}\sum_{\substack{\tau=1-N\\\tau\neq 0}}^{N-1}|c_{i,i}(\tau)|^2 \quad (12)$$

The measure defined by (12) allows for comparison of the auto-correlation properties of the set of spreading sequences on the same basis as the cross-correlation properties.

The measures defined by (11) and (12) are very useful for large sets of sequences and large number of active users, when the constellation of interferers (i.e. relative delays among the active users and the spreading sequences used) changes randomly for every transmitted information symbol. However, for a more static situation, when the constellation of interferers stays constant for the duration of many information symbols, it is also important to consider the worst-case scenarios. This can be accounted for by analysing the maximum value of peaks in the aperiodic cross-correlation functions over the whole set of sequences and in the aperiodic autocorrelation function for $\tau\neq 0$. Hence, we introduce here two additional measures to compare the spreading sequence sets:

- Maximum value of the aperiodic cross-correlation functions $C_{\max}$

$$c_{\max}(\tau)=\max_{\substack{i=1,\ldots,M\\k=1,\ldots,M\\i\neq k}}\left|c_{i,k}(\tau)\right|,\qquad \tau=(-N+1),\ldots,(N-1)$$
$$C_{\max}=\max_{\tau}\{c_{\max}(\tau)\} \quad (13)$$

## V. EXAMPLE DESIGN

Using a circulant and a back circulant matrices of order 31 we construct two amicable matrices **A** and **B** of order 32. The **A** and **B** are then used to construct the complex orthogonal matrix $\mathbf{X} = \frac{\sqrt{2}}{2}(\mathbf{A} + j\mathbf{B})$, where the coefficient $\sqrt{2}/2$ is used to keep the magnitude of every element of **X** equal to 1. Later we applied the modification method described in the previous section to improve the correlation properties of **X**. However, in order to have both real and imaginary parts of the new matrix $\mathbf{W}_{32}$ having bipolar, only, the elements on the diagonal of $\mathbf{D}_N$ must take values of '1' or '-1'. The resulting set of spreading sequences is characterised by low peaks in the aperiodic cross-correlation functions for any pair of the sequences. The maximum values of those peaks are plotted in Fig. 1 versus the relative shift between the sequences. From the plot, it is also visible that the designed sequences are orthogonal as there is zero cross-correlation for the zero shift. It is also visible that even after the modification the real and imaginary parts of $\mathbf{W}_{32}$ are orthogonal.

## VI. CONCLUSIONS

In the paper we present the novel technique to construct complex four-phase orthogonal spreading sequences. Since the construction is based on amicable orthogonal Hadamard matrices, the real and imaginary parts of the sequences are independently orthogonal.

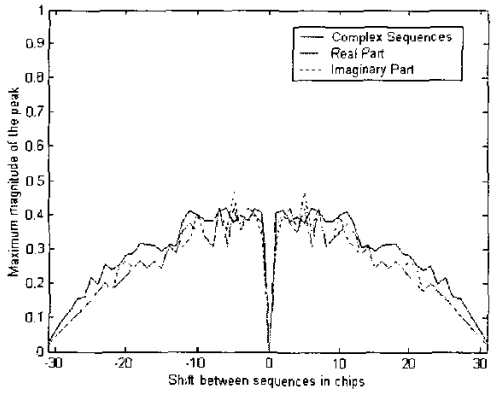


**Figure 1**: Maximum values of the magnitude of aperiodic cross-correlation peaks for the designed sequence set.

## REFERENCES


[1] R.Steele: "Introduction to Digital Cellular Radio," in R.Steele and L.Hanzo (eds), "*Mobile Radio Communications*, " 2nd ed., IEEE Press, New York, 1999

[2] H.F. Harmuth: "*Transmission of Information by Orthogonal Functions*," Springer-Verlag, Berlin, 1970.

[3] M.B.Pursley: "Performance Evaluation for Phase-Coded Spread-Spectrum Multiple-Access Communication – Part I: System Analysis," *IEEE Trans. on Commun.*, vol. COM-25, pp. 795-799, 1977.

[4] I.Oppermann and B.S.Vucetic: "Complex spreading sequences with a wide range of correlation properties," *IEEE Trans. on Commun.*, vol. COM-45, pp.365-375, 1997.

[5] I.Oppermann: "Orthogonal Complex-Valued Spreading Sequences with a Wide Range of Correlation Properties," *IEEE Trans. on Commun.*, vol. COM-45, pp.1379-1380, 1997.

[6] B.J.Wysocki, T.Wysocki: "Modified Walsh-Hadamard Sequences for DS CDMA Wireless Systems," *Int. J. Adapt. Control Signal Process.*, vol.16, 2002, pp.589-602.

[7] L.D.Baumert: "Cyclic Difference Sets," *Lecture Notes in Mathematics*, vol.182, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[8] R.E.A.C.Paley: "On orthogonal matrices," *J. Math. Phys.*, 12 (1933), pp.311-320.

[9] R.G.Stanton, D.A.Sprott: "A family of difference sets, " *Can. J. Math.*, 10 (1958), pp.73-77

[10] A.L.Whiteman: "A family of difference sets," *Illinois J. Math..*, 6 (1962), 107-121.

[11] J.Singer: "Atheorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.*, 43 (1938), pp.377-385.

[12] Marshall Hall Jr: "A survey of difference sets," *Proc. Amer. Math. Soc.*, 7 (1956), pp.975-986.

[13] K.H.Kärkkäinen: "Mean-square cross-correlation as a performance measure for spreading code families," *IEEE 2nd Int. Symp. on Spread Spectrum Techniques and Applications (ISSSTA '92)*, pp.147-150.