Published in Mobile Future, 2004 and the Symposium on Trends in Communications. SympoTIC '04. Joint IST Workshop on 24-26 Oct. 2004 Page(s):82 - 85

Orthogonal Spreading Sequences Constructed Using Hall's Difference Set

Jennifer Seberry, Le Chung Tran, Yejing Wang, Beata J Wysocki, Tadeusz A.Wysocki, Ying Zhao
Faculty of Informatics, University of Wollongong
NSW2522, Australia
Wysocki@uow.edu.au

Abstract: In the paper we propose a new set of orthogonal spreading sequences based on the Hadamard matrix of order 32 constructed using the Hall difference set. The proposed sequences are characterised by low peaks in the aperiodic cross-correlation functions and have also good aperiodic auto-correlation properties.

1. Introduction

Orthogonal bipolar sequences are of a great practical interest for the current and future direct sequence (DS) code-division multiple-access (CDMA) systems where the orthogonality principle can be used for channels separation, 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. They are constructed using the Sylvester construction, so they only exist for the sequence lengths being integer powers of 2. In general, one can construct Hadamard matrices for most orders $N \equiv 0 \pmod 4$. The first unsolved case is order 428. Apart from the well-known Sylvester's construction of Hadamard matrices, there are several other systematic ways of constructing such matrices. Good lists of those techniques can be found in [3] and the listing of the matrices can be found on the home pages maintained by Seberry [4], and Sloane [5].

It is well known, e.g. [6], 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. In [7], Wysocki and Wysocki have shown that spreading sequences derived from different H-equivalent matrices [3] of Sylvester's construction have different aperiodic correlation properties, and that by choosing the appropriate H-equivalent matrix, one can significantly reduce the peaks whole set of sequences. The lowest value of peaks in the aperiodic cross-correlation functions for the sequences derived from a Hadamard matrix H-equivalent to the Sylvester-Hadamard matrix of order $N = 32$ published in [7] is 0.4063. This result is much lower than 0.9688 for sequences derived from the Sylvester-Hadamard matrix of order $N = 32$ in its well-known canonical form. On the other hand, the value of 0.4063 is still much greater than the Levenshtein bound [8] of 0.1410 for the set of 32 sequences of order 32. Of course, the bound is derived for sets of bipolar sequences without imposed condition of orthogonality for their perfect alignment.

In the paper, we propose to derive spreading sequences of order 32 from the Hall difference set (31,15,7) [9], usually referred to as $\mathbf{H}_{32\text{-}03}$ [4]. We have found through computer search that the lowest value of peaks in the aperiodic cross-correlation functions for the sequences derived from a Hadamard matrix H-equivalent to the matrix $\mathbf{H}_{32\text{-}03}$ is 0.3750. It is still significantly higher than the Levenshtein bound but is a significant improvement compared to the best result obtained from H-equivalent Sylvester-Hadamard matrices.

The paper is organised as follows. In section 2, we introduce the Hall difference set construction and apply it to produce a $\mathbf{H}_{32\text{-}03}$ Hadamard matrix in its canonical form. In section 3, we describe the method used to search for the H-equivalent matrices and give the example result leading to the spreading sequence set with the value of peaks in the aperiodic cross-correlation functions equal to 0.3750. The paper is concluded in section 4.

2. Hadamard matrices constructed using the Hall difference set

Let α be a primitive root of 31 ($\alpha = 2$ or 3 or 5) [9]. To construct the matrix $\mathbf{H}_{32\text{-}03}$ we first create a set:

$$A = \{\alpha^{6j}, \alpha^{6j+3}, \alpha^{6j+5}\} \quad j = 0,1,2,3,4 \qquad (1)$$

which in the considered case is a set of 15 integers:

$$A = \{a_1, \ldots, a_{15}\} \qquad (2)$$

Then we create a circulant matrix $\mathbf{B}$ of order 31, with first row elements $b_{1,k}$ defined as:

$$b_{1,k} = \begin{cases} 1, & if \quad k \in A \\ -1, & otherwise \end{cases} \qquad (3)$$

0-7803-8556-X/04/$20.00 © 2004 IEEE

The matrix $\mathbf{H}_{32\text{-}03}$ is created from the matrix $\mathbf{B}$ by adding the first row and the first column containing all '1s', i.e.:

$$\mathbf{H}_{32-03} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & b_{1,1} & b_{1,2} & \cdots & b_{1,31} \\ 1 & b_{1,31} & b_{1,1} & \cdots & b_{1,30} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & b_{1,2} & b_{1,3} & \cdots & b_{1,1} \end{bmatrix} \quad (4)$$

The matrix $\mathbf{H}_{32\text{-}03}$ is therefore equal to [4]:

$$\mathbf{H}_{32-03} = \left[\begin{array}{l}
\texttt{++++++++++++++++++++++++++++++++} \\
\texttt{+-++++-+-+---+--+++-----++--+-++} \\
\texttt{++-++++-+-+---+--+++-----++--+-+} \\
\texttt{+++-++++-+-+---+--+++-----++--+-} \\
\texttt{+-++-++++-+-+---+--+++-----++--+} \\
\texttt{++-++-++++-+-+---+--+++-----++--} \\
\texttt{+-+-++-++++-+-+---+--+++-----++-} \\
\texttt{+--+-++-++++-+-+---+--+++-----++} \\
\texttt{++--+-++-++++-+-+---+--+++-----+} \\
\texttt{+++--+-++-++++-+-+---+--+++-----} \\
\texttt{+-++--+-++-++++-+-+---+--+++----} \\
\texttt{+--++--+-++-++++-+-+---+--+++---} \\
\texttt{+---++--+-++-++++-+-+---+--+++--} \\
\texttt{+----++--+-++-++++-+-+---+--+++-} \\
\texttt{+-----++--+-++-++++-+-+---+--+++} \\
\texttt{++-----++--+-++-++++-+-+---+--++} \\
\texttt{+++-----++--+-++-++++-+-+---+--+} \\
\texttt{++++-----++--+-++-++++-+-+---+--} \\
\texttt{+-+++-----++--+-++-++++-+-+---+-} \\
\texttt{+--+++-----++--+-++-++++-+-+---+} \\
\texttt{++--+++-----++--+-++-++++-+-+---} \\
\texttt{+-+--+++-----++--+-++-++++-+-+--} \\
\texttt{+--+--+++-----++--+-++-++++-+-+-} \\
\texttt{+---+--+++-----++--+-++-++++-+-+} \\
\texttt{++---+--+++-----++--+-++-++++-+-} \\
\texttt{+-+---+--+++-----++--+-++-++++-+} \\
\texttt{++-+---+--+++-----++--+-++-++++-} \\
\texttt{+-+-+---+--+++-----++--+-++-++++} \\
\texttt{++-+-+---+--+++-----++--+-++-+++} \\
\texttt{+++-+-+---+--+++-----++--+-++-++} \\
\texttt{++++-+-+---+--+++-----++--+-++-+} \\
\texttt{+++++-+-+---+--+++-----++--+-++-}
\end{array}\right]$$

2. Search for best H-equivalent matrices

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:

$$\mathbf{W}_N = \mathbf{H}_N \mathbf{D}_N \quad (5)$$

Of course, the matrix $\mathbf{W}_N$ is also orthogonal [7].

In [7], 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:

$$|d_{l,m}| = \begin{cases} 0 & \text{for} \quad l \neq m \\ k & \text{for} \quad l = m \end{cases}; \quad l, m = 1, \ldots, N, \quad (6)$$

with k being any non-zero real constant. That way, the matrix $\mathbf{D}_N$ satisfies the condition:

$$\mathbf{D}_N \mathbf{D}_N = \mathbf{D}_N \mathbf{D}_N^T = k^2 \mathbf{I}_N \quad (7)$$

where $\mathbf{I}_N$ is the $N \times N$ identity matrix.

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

$$d_{l,m} = \begin{cases} 0 & \texttt{for} \quad l \neq m \\ \exp(j\phi_l) & \texttt{for} \quad l = m \end{cases}; \quad (8)$$
$$l, m = 1, \ldots, N$$

The parameters ϕ_l, $l = 1, \ldots, N$, are phase coefficients, which are real numbers with values from $[0, 2\pi)$. From the implementation point of view, the best class of sequences is the one of binary sequences, i.e. when $\phi_l = 0$ or π.

To find the best possible modifying diagonal matrix $\mathbf{D}_N$ we can do an exhaustive search of all possible bipolar sequences of length N, and choose the one, which leads to the best performance of the modified set of sequences. However, this approach is very computationally intensive, and even for a modest values of N, e.g. $N = 20$, it is rather impractical. Hence, other search methods, like a random search, must be considered, e.g. Monte Carlo algorithm.

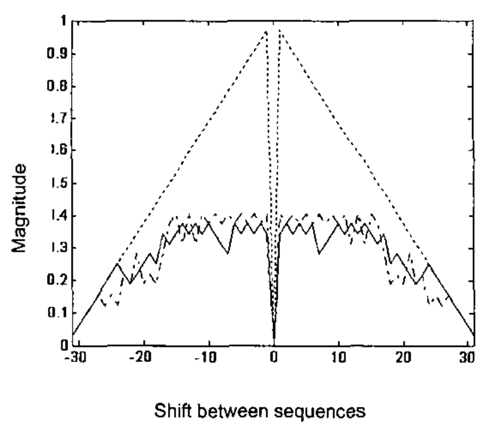

Figure 1: Peaks in the magnitude of aperiodic cross-correlation functions between any two pairs of the sequences derived from: matrix $\mathbf{W}_{32\text{-}03}$ – solid line, Walsh-Hadamard sequences – dotted line, modified Walsh-Hadamard sequences [7] – dashed line.

In the considered case, we have performed 10,000 random drawings of binary sequences of length 32, and used them as diagonals of the modifying matrix $\mathbf{D}_{32}$. The matrix $\mathbf{W}_{32\text{-}03}$, H-equivalent to $\mathbf{H}_{32\text{-}03}$, giving the lowest maximum peaks in any pair of aperiodic cross-correlation functions is obtained when the diagonal of the matrix $\mathbf{D}_{32}$ is

[-+-+-++++---+--+++-+++++++++++++]

The matrix $\mathbf{W}_{32\text{-}03}$ is then:

$$
W_{32-03} = \begin{bmatrix}
\text{-+-+-++++---+--+++-+++++++++++} \\
\text{---+-+-+--++--+-++-------++--+-++} \\
\text{-+++-++-++-+-+---+-+-----++--+-+} \\
\text{-+---+++--+--+++---++-----++--+-} \\
\text{---+++++++-++++-+-++++-----++--+} \\
\text{-+++--+++-+---+--++-+++------++--} \\
\text{-----+-++--+++--------+++-----++-} \\
\text{--+++++-+-----++--++--+++-----++} \\
\text{-++---++----++--+-+-+--+++-----+} \\
\text{-+--++-+++--+-++-++--+--+++-----} \\
\text{---++-+-+-+-+---+-----+--+++----} \\
\text{--++---+---++--+-+++----+--+++---} \\
\text{--+--+--++------++---+---+--+++--} \\
\text{--+-+++---+-++-+++++-+---+--+++-} \\
\text{--+-+-++-+-++-++++--+-+---+--+++} \\
\text{-++-+--++++-----++-+-+-+---+--++} \\
\text{-+--+---+-++++-+-+-++-+-+---+--+} \\
\text{-+-++------+--+++--+++-+-+---+--} \\
\text{---+-----+---+--+++++++-+-+---+-} \\
\text{--++-+---++-++++-+--++++-+-+---+} \\
\text{-++--++--++++-+-+--+-++++-+-+---} \\
\text{----++++-+++-----++++-++++-+-+--} \\
\text{--+++-++++++-+-+----++-++++-+-+-} \\
\text{--+----++-++-++++-++-++-++++-+-+} \\
\text{-++-++--+--+-++-+++-+-++-++++-+-} \\
\text{----+-+-------++--+---+-++-++++-+} \\
\text{-++++--+-+--+++----+--+-++-++++-} \\
\text{--------+++-+-+---+++--+-++-++++} \\
\text{-+++++----+++-----+-++--+-++-+++} \\
\text{-+----+--+-+---+--+--++--+-++-++} \\
\text{-+-+++-+-++--+-++-+---++--+-++-+} \\
\text{-+-+--+-+++++++++++-----++--+-++-}
\end{bmatrix}
$$

The plot of the peaks in the aperiodic cross-correlation functions between any two pairs of the sequences derived from the matrix $\mathbf{W}_{32\text{-}03}$ is given in Figure 1. For the comparison, we present there also the peaks in the aperiodic cross-correlation functions between any two pairs of the sequences derived from the matrix $\mathbf{H}_{32\text{-}03}$ and for the sequences presented in [7] that are derived from an H-equivalent Sylvester-Hadamard matrix, known also as the modified-Walsh-Hadamard sequences.

The set of sequences derived from the matrix $\mathbf{W}_{32\text{-}03}$ is characterized by the following aperiodic correlation characteristics:

$$C_{\max} = 0.3750$$

$$R_{CC} = 0.9682$$

$$R_{AC} = 0.9844$$

where $C_{\max}$ denotes the maximum peak value in the magnitude of aperiodic cross-correlation functions between any pair of the sequences in the set, R_{CC} is the mean square aperiodic cross-correlation for the set of sequences [6], and R_{AC} is the mean square aperiodic auto-correlation for the set of sequences [6].

Synchronisation amenability of the derived sequences can be assessed by examining the maximum off-peak values in the magnitudes of aperiodic autocorrelation functions for the whole sequence set. From Figure 2, it is visible that the sequences derived from the matrix $\mathbf{W}_{32\text{-}03}$ have a very distinctive peak for the perfect alignment and that there are no other significant peaks for any non-zero shift.

3. Conclusions

In the paper we presented correlation properties of the sequences derived from the Hadamard matrix of order 32 ($\mathbf{H}_{32\text{-}03}$) constructed using Hall difference set. After searching the H-equivalent matrices, we found that there exist some matrices H-equivalent to $\mathbf{H}_{32\text{-}03}$ that sequences derived using those matrices have peaks in the magnitudes of their cross-correlation functions equal to 0.3750. This is lower value than that for the modified Walsh-Hadamard sequences, for which those peaks are equal to 0.4063 [7]. Because of this, and the fact that the auto-correlation functions of this new sequence set have very distinctive peaks for the perfect alignment, the proposed sequences can be useful for DS CDMA applications.

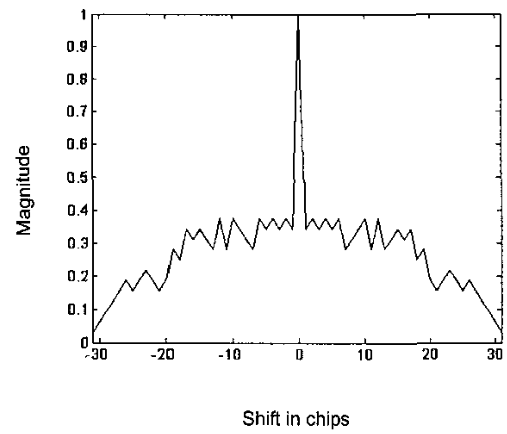

Figure 2: Maximum values for the magnitude of aperiodic auto-correlation functions for the sequences derived from matrix $\mathbf{W}_{32\text{-}03}$.

Unfortunately, the Hadamard matrices constructed using Hall difference set exist only for such orders N where $(N - 1)$ is a prime number. Therefore, $N = 32$ seems to be the only order with a possible practical application.

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] A.V.Geramita, and J.Seberry: "Orthogonal designs, quadratic forms and Hadamard matrices," *Lecture Notes in Pure and Applied Mathematics,*

vol.43, Marcel Dekker, New York and Basel, 1979.

[4] J.Seberry: *Library of Hadamard Matrices*, http://www.uow.edu.au/~jennie/hadamard.html

[5] N.J.A.Sloane: *A Library of Hadamard Matrices*, http://www.research.att.com/~njas/hadamard/

[6] 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.

[7] 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.

[8] V.I.Levenshtein: "A new lower bound on aperiodic crosscorrelation of binary codes," *4th International Symp. On Communication Theory and Applications, ISCTA '97*, Ambleside, U.K., 13-18 July 1997, pp. 147-149.

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