

2005

On some applications of Hadamard matrices

Jennifer Seberry

University of Wollongong, jennie@uow.edu.au

Beata J. Wysocki

University of Wollongong, bjw@uow.edu.au

Tadeusz A. Wysocki

University of Wollongong, wysocki@uow.edu.au

Publication Details

This article was originally published as Seberry, J, Wysocki, Bj and Wysocki, TA, On some applications of Hadamard matrices, *Metrika*, 62, (2005) 221-239. Copyright Springer-Verlag.

On some applications of Hadamard matrices

Abstract

Modern communications systems are heavily reliant on statistical techniques to recover information in the presence of noise and interference. One of the mathematical structures used to achieve this goal is Hadamard matrices. They are used in many different ways and some examples are given. This paper concentrates on code division multiple access systems where Hadamard matrices are used for user separation. Two older techniques from design and analysis of experiments which rely on similar processes are also included. We give a short bibliography (from the thousands produced by a google search) of applications of Hadamard matrices appearing since the paper of Hedayat and Wallis in 1978 and some applications in telecommunications.

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as Seberry, J, Wysocki, Bj and Wysocki, TA, On some applications of Hadamard matrices, *Metrika*, 62, (2005) 221-239. Copyright Springer-Verlag.

On some applications of Hadamard matrices

Abstract Modern communications systems are heavily reliant on statistical techniques to recover information in the presence of noise and interference. One of the mathematical structures used to achieve this goal is Hadamard matrices. They are used in many different ways and some examples are given. This paper concentrates on code division multiple access systems where Hadamard matrices are used for user separation. Two older techniques from design and analysis of experiments which rely on similar processes are also included. We give a short bibliography (from the thousands produced by a google search) of applications of Hadamard matrices appearing since the paper of Hedayat and Wallis in 1978 and some applications in telecommunications.

1 Introduction

Hadamard matrices seem such simple matrix structures: they are square, have entries $+1$ or -1 and have orthogonal row vectors and orthogonal column vectors. Yet they have been actively studied for over 138 years and still have more secrets to be discovered. In this paper we concentrate on engineering and statistical applications especially those in communications systems, digital image processing and orthogonal spreading sequences for direct sequences spread spectrum code division multiple access.

2 Basic definitions and properties

A square matrix with elements ± 1 and size h , whose distinct row vectors are mutually orthogonal, is referred to as an *Hadamard matrix of order h* . The smallest examples are:

$$(1), \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ - & 1 & - & 1 \\ 1 & 1 & - & - \\ - & 1 & 1 & - \end{pmatrix}$$

where $-$ denotes -1 . Such matrices were first studied by Sylvester (1867) who observed that if H is an Hadamard matrix, then

$$\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

is also an Hadamard matrix. Indeed, using the matrix of order 1, we have:

Lemma 2.1 (Sylvester (1867)) : There is an Hadamard matrix of order 2^t for all non-negative t .

The matrices of order 2^t constructed using Sylvester's construction are usually referred to as Sylvester-Hadamard matrices. The Sylvester-Hadamard matrices are associated with discrete orthogonal functions called Walsh functions which will be discussed later in the paper.

Hadamard (1893) gave examples for a few small orders. An example of order 12 is as follows:

$$H_{12} = \begin{pmatrix} 1 & 1 & 1 & - & 1 & 1 & - & 1 & 1 & - & 1 & 1 \\ 1 & 1 & 1 & 1 & - & 1 & 1 & - & 1 & 1 & 1 & - \\ 1 & 1 & 1 & 1 & 1 & - & 1 & 1 & - & 1 & 1 & - \\ \hline 1 & - & - & 1 & 1 & 1 & - & 1 & 1 & 1 & - & - \\ - & 1 & - & 1 & 1 & 1 & 1 & - & 1 & - & - & 1 \\ - & - & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - & 1 \\ \hline 1 & - & - & 1 & - & - & 1 & 1 & 1 & 1 & - & 1 \\ - & 1 & - & - & 1 & - & 1 & 1 & 1 & 1 & - & 1 \\ - & - & 1 & - & - & 1 & 1 & 1 & 1 & 1 & 1 & - \\ \hline 1 & - & - & - & 1 & 1 & 1 & - & 1 & - & 1 & 1 \\ - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & 1 & 1 \\ - & - & 1 & 1 & 1 & - & - & - & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Some systematic constructions of Hadamard matrices different to Sylvester's construction will be given in the next section. The following two Lemmas give some basic properties of Hadamard matrices.

Lemma 2.2 Let H_h be an Hadamard matrix of order h . Then:

- (i) $H_h H_h^t = h I_h$, where I_h is the identity matrix of order h ;
- (ii) $|\det H_h| = h^{\frac{1}{2}h}$;
- (iii) $H_h H_h^t = H_h^t H_h$;
- (iv) Hadamard matrices may be changed into other Hadamard matrices by permuting rows and columns and by multiplying rows and columns by -1 . Matrices which can be obtained from one another by these methods are referred to as H -equivalent (not all Hadamard matrices of the same order are H -equivalent);

- (v) every Hadamard matrix is H -equivalent to an Hadamard matrix which has every element of its first row and column equal to $+1$ — matrices of this latter form are called normalized;
- (vi) if H_{4n} is a normalized Hadamard matrix of order $4n$, then every row (column), except the first, has $2n$ minus ones and $2n$ plus ones in each row (column);
- (vii) the order of an Hadamard matrix is 1, 2, or $4n$, where n is a positive integer. The first unsolved case is order 668. The previous smallest unsolved case, 428, was found in 2004 by Kharaghani and Tayfeh-Rezaie Kharaghani and Tayfeh-Rezaie (2004).

Lemma 2.3 (Sylvester) Let H_1 and H_2 be Hadamard matrices of orders h_1 and h_2 , then the Kronecker product of H_1 and H_2 is an Hadamard matrix of order $h_1 h_2$.

Hadamard in (1893) considered matrices with entries on the unit circle, and proved that these matrices, $X = [x_{ij}]_{n \times n}$, satisfied the following inequality:

$$|\det X|^2 \leq \prod_{i=1}^n \sum_{j=1}^n |x_{ij}|^2. \quad (1)$$

If they satisfied the equality of (1) then they satisfied $XX^t = I_n$ and had maximal determinant $n^{\frac{n}{2}}$. However, Hadamard's name has become associated only with the matrices having their entries equal to ± 1 .

3 Some useful constructions of Hadamard matrices

Hadamard matrices have a very wide variety of applications in modern communications and statistics. A construction technique of crucial importance in one application may be less significant in another application. There is a close relationship between Hadamard matrices constructed using Sylvester's technique (see Lemma 1) and Walsh functions that are often used in engineering applications, including communication systems and digital image processing. Apart from Sylvester's construction there are several other systematic ways of constructing such matrices. Good lists of those techniques can be found in Geramita and Seberry (1979), Hedayat et al. (1999) and the listing of the matrices can be found on the home pages maintained by Seberry (2004), and Sloane (2004).

In this section, we want to introduce some of those techniques that lead to large families of H -inequivalent matrices since H -inequivalent matrices, and even H -equivalent matrices, can have quite different computational properties in some of the applications discussed and affect system performance. We present here two such construction techniques: Golay-Hadamard matrices, and Williamson-Hadamard matrices. More construction techniques can be found in Geramita and Seberry (1979). In addition, we will give a technique leading to the construction of pairs of amicable Hadamard matrices from circulant matrices. These amicable Hadamard matrices can be used to design complex four-phase orthogonal matrices having both real and imaginary components independently orthogonal. Hadamard matrices can be used also to design error correcting block codes which can correct large numbers of errors in communications. For definitions not given here the

interested reader is referred to Seberry and Yamada (1992) or Koukouvinos and Kounias (1989).

3.1 Construction of Hadamard matrices using Golay sequences

In Seberry et al. (2002), we have studied the use of Golay complementary sequences to construct Hadamard matrices for use in direct sequence spread spectrum (DS SS) code division multiple access (CDMA) communication systems. For a pair of Golay complementary sequences S_1 and S_2 , the sum of their aperiodic autocorrelation functions equals to zero, except for the zero shift Fan and Darnell (1966):

$$c_{S_1}(\tau) + c_{S_2}(\tau) = 0, \quad \tau \neq 0 \quad (2)$$

where $c_{S_1}(\tau)$ and $c_{S_2}(\tau)$ denote the aperiodic autocorrelation functions Fan and Darnell (1966).

It can be proven Seberry and Yamada (1992), Wallis et al. (1972) that if matrices A and B are the circulant matrices created from a pair of Golay complementary sequences S_1 and S_2 then the matrix

$$G = \begin{pmatrix} A & B \\ B^t & -A^t \end{pmatrix} \quad (3)$$

is an Hadamard matrix. We write in more detail about circulant matrices and how to construct Hadamard matrices using a circulant core in Section 3.3.

Golay complementary sequences have been defined as bipolar sequences, and one can generate bipolar Golay sequences of all lengths N , such that

$$N = 2^a 10^b 26^c \quad (4)$$

where a, b, c are non-negative integers. More recent research by a number of authors have relaxed the condition of bipolarity. Another technique, which can be employed to construct Hadamard matrices from bipolar complementary sequences, is based on the Goethals-Seidel array (1970). In (1989), Koukouvinos and Kounias, expanding on the work of Turyn (1974), used two Golay complementary sequences, U and V , of length ℓ_1 and two Golay complementary sequences, X, Y , of length ℓ_2 to note that

$$\begin{aligned} A &= [U, X] \\ B &= [U, -X] \\ C &= [V, Y] \\ D &= [V, -Y] \end{aligned}$$

are four complementary sequences of length $\ell_1 + \ell_2$, and that there is a Golay-Hadamard matrix of order

$$N = 4(\ell_1 + \ell_2)$$

constructed from Goethals-Seidel array. This technique produces many more Golay-Hadamard matrices than the construction given by Eq. (3), Craigen et al. (2001).

3.2 Williamson-Hadamard construction

Theorem 3.1 [Williamson (1944)] Suppose there exist four symmetric $(1, -1)$ matrices A, B, C, D of order n which satisfy

$$XY^t = YX^t, \quad X, Y \in \{A, B, C, D\}.$$

Further, suppose

$$AA^t + BB^t + CC^t + DD^t = 4nI_n. \quad (5)$$

Then, using A, B, C, D in the Williamson array H given by

$$H = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix} \quad (6)$$

gives an Hadamard matrix of order $4n$.

Williamson (1944) developed number theoretic techniques which allow computer searches for these matrices to be made far more efficiently but still in non polynomial time. An extensive list of sequences to generate circulant matrices to fill the Williamson array, to get Hadamard matrices of orders 12 to 252, can be found in Seberry et al. (2003).

3.3 Amicable Hadamard matrices

We now briefly discuss the construction of pairs of amicable Hadamard matrices as these matrices can be used to design complex four-phase orthogonal matrices having both real and imaginary components independently orthogonal.

Two square matrices M and N of order n are said to be amicable if $MN^t = NM^t$. Suppose $I + S$ and N are amicable Hadamard matrices of order n satisfying

$$(I + S)N^t = N(I + S)^t, \quad S^t = -S, \quad N^t = N \quad (7)$$

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

Example 3.1 Let $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $N = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, then $I + S$ and N are amicable Hadamard matrices of order 2. Hence amicable Hadamard matrices of this type exist for all orders 2^t .

An Hadamard matrix, A , of order n are said to be constructed using a circulant core if it uses a suitably use a bordered matrix $C = c(i, j)$ of order $n - 1$, satisfying $CC^t = nI - J$, $CJ = J$, where $c(i, j) = c(1, j - i + 1)$ where $j - i + 1$ is reduced (mod $n - 1$). For example

$$C = \begin{pmatrix} 1 & 1 & - \\ - & 1 & 1 \\ 1 & - & 1 \end{pmatrix}$$

is a circulant core and

$$A = \left(\begin{array}{c|ccc} 1 & 1 & 1 & 1 \\ - & 1 & 1 & - \\ - & - & 1 & 1 \\ - & 1 & - & 1 \end{array} \right)$$

is an Hadamard matrix constructed using a circulant core.

An Hadamard matrix, B , of order n is said to be constructed *using a back circulant core* if it uses a suitably bordered matrix $D = d(i, j)$ of order $n - 1$ satisfying $DD^t = nI - J$, $DJ = J$, where $d(i, j) = d(1, j + i - 1)$ where $j + i - 1$ is reduced ($\text{mod } n - 1$). For example

$$D = \left(\begin{array}{ccc} 1 & 1 & - \\ 1 & - & 1 \\ - & 1 & 1 \end{array} \right)$$

is a back circulant core and

$$B = \left(\begin{array}{c|ccc} - & 1 & 1 & 1 \\ 1 & 1 & 1 & - \\ 1 & 1 & - & 1 \\ 1 & - & 1 & 1 \end{array} \right)$$

is an Hadamard matrix constructed using a back circulant core.

Theorem 3.2 *An 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 Paley (1933);
2. $p = q(q + 2)$, where q and $q + 2$ are both prime Stanton and Sprott (1958), Whiteman (1962);
3. $p = 2^t - 1$, where t is a positive integer Singer (1938);
4. $p = 4x^2 + 27$, where p is prime and x a positive integer Hall (1967).

Theorem 3.3 [(Wallis et al., 1972, p300)] *An Hadamard matrix of order n constructed using a circulant core A and an Hadamard matrix of order n constructed using a back circulant core B are amicable. That is $AB^t = BA^t$.*

Proof We note that if X is a circulant core and Y is a back circulant core, both of order $n - 1$, then $XY^t = YX^t$. Let J be the matrix of all 1s. Suppose $XJ = YJ = Y$. (This can certainly be done for if, say $XJ = -J$, we would merely replace X by its negative.) Further suppose $XX^t = YY^t = nJ - J$, (which is a property of being the core of an Hadamard matrix) then

$$A = \left(\begin{array}{c|ccc} 1 & 1 & \dots & 1 \\ - & & & \\ \vdots & & X & \\ - & & & \end{array} \right) \text{ and } B = \left(\begin{array}{c|ccc} - & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & Y & \\ 1 & & & \end{array} \right)$$

can easily be checked to satisfy $AB^t = BA^t$ and so are amicable Hadamard matrices.

This means there are amicable Hadamard matrices of order $2^t \prod (p+1)$ for any integer t and p given in Theorem 3.2. Using the amicability property, the following theorem follows directly:

Theorem 3.4 *If matrices A and B are amicable Hadamard matrices of order n , then a matrix $X = A + jB$, $j^2 = -1$, is a complex orthogonal matrix, i.e. $XX^H = 2nI_n$, where $(\cdot)^H$ is the Hermitian conjugate.*

This leads to the easy design of complex four-phase orthogonal matrices having both real and imaginary components independently orthogonal.

4 Applications of Hadamard matrices in telecommunications and signal processing

Hadamard matrices have found many applications in modern telecommunications and digital signal processing Yarlagaadda and Hershey (1997). In this section, we will briefly discuss some of those applications in error-control coding Peterson (1961), and to define Walsh functions Walsh (1923) that can be used for signal modelling Harmuth (1960) and transformation of information in image compression and image encoding Jain (1989). We will also consider the use of Hadamard matrices to design spreading sequences for application in code division multiple access (CDMA) direct sequence (DS) spread spectrum (SS) systems Lam and Tantaratana (1994).

4.1 Error-control codes derived from Hadamard matrices

Error correcting capabilities of codes derived from Hadamard matrices were first pointed out by Plotkin in 1951 Plotkin (1960). This has been later studied by Bose and Shrikhande (1959), who have shown the connection between Hadamard matrices and symmetrical block code designs and later extended by Harmuth in (1960).

Theorem 4.1 *[Peterson (1961)] If there exists an $n \times n$ Hadamard matrix, then there exists a binary code with $2n$ code vectors, and minimum distance $n/2$. (This is not necessarily a linear code.)*

The block code designed from an Hadamard matrix H has the following structure:

$$\begin{pmatrix} H \\ -H \end{pmatrix}.$$

Because the minimum distance for such a code is equal to $n/2$, codes derived from Hadamard matrices have maximal error correcting capability for a given length of a codeword. These codes were used in the 1960's in the Mariner and Voyager space probes to encode information transmitted back to the Earth while the probes visited Mars and the outer planets of the solar system. Due to the enormous distance between those planets and the Earth, not only does it take the signal a considerable amount of time to come to the Earth but the signal is also very weak. Only

because of the powerful error-correction capabilities of those codes, was it possible to decode properly the glorious high quality pictures of Jupiter, Saturn, Uranus, Neptune and their moons. As a matter of fact, application of Hadamard matrices to design powerful error-correcting codes was one of the factors in an increased interest in finding new constructions of Hadamard matrices, e.g. Ang et al. (2003), Baumert and Hall (1965), Turyn (1972).

4.2 Walsh functions

There are a couple of formal definitions of Walsh functions introduced in the literature (e.g. Szabatin (1982), Yarlagadda and Hershey (1997)). Here, we give their definition on the interval $[0, 1]$.

$$\begin{aligned} Wal(0, t) = x_0(t) &= 1, \quad 0 \leq t \leq 1 \\ Wal(1, t) = x_1(t) &= \begin{cases} 1, & 0 \leq t < 0.5 \\ -1, & 0.5 \leq t \leq 1 \end{cases} \\ Wal(2, t) = x_2(t) &= \begin{cases} 1, & 0 \leq t < 0.25 \text{ and } 0.75 \leq t \leq 1 \\ -1, & 0.25 \leq t < 0.75 \end{cases} \\ Wal(3, t) = x_3(t) &= \begin{cases} 1, & 0 \leq t < 0.25 \text{ and } 0.5 \leq t < 0.75 \\ -1, & 0.25 \leq t < 0.5 \text{ and } 0.75 \leq t \leq 1 \end{cases} \end{aligned} \quad (8)$$

and recursively for $m = 1, 2, \dots$ and $k = 1, \dots, 2^{m-1}$ we have:

$$Wal(2^{m-1} + k - 1, t) = x_m^k(t) \quad (9)$$

$$\begin{aligned} x_{m+1}^{2k-1}(t) &= \begin{cases} x_m^k(2t), & 0 \leq t < 0.5 \\ (-1)^{k+1} x_m^k(2t - 1), & 0.5 \leq t \leq 1 \end{cases} \\ x_{m+1}^k(t) &= \begin{cases} x_m^k(2t), & 0 \leq t < 0.5 \\ (-1)^k x_m^k(2t - 1), & 0.5 \leq t \leq 1 \end{cases} \end{aligned} \quad (10)$$

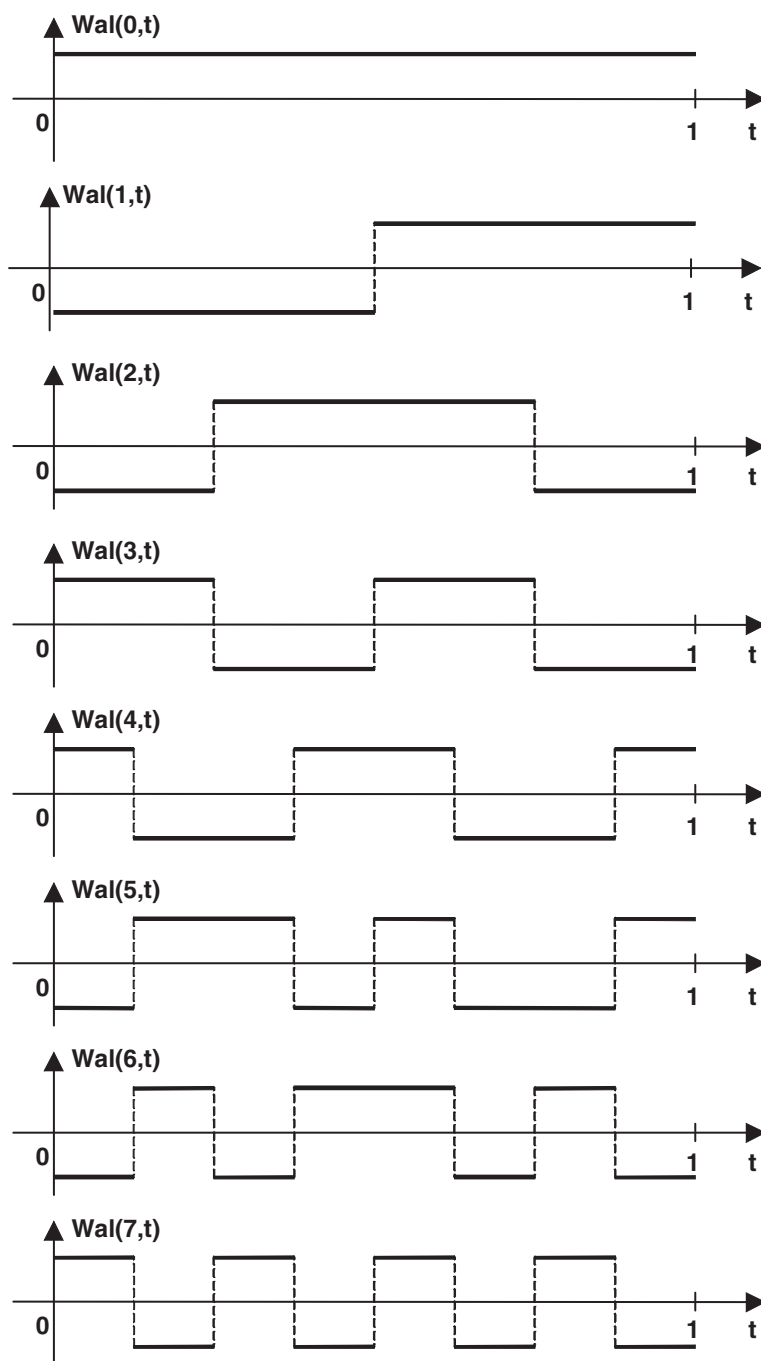
These recursive formulae can be used to define Walsh functions for any value of m and k , and the plots of first eight Walsh functions are presented in Figure 1. The Walsh functions can also be defined using the Sylvester-Hadamard matrices. Using such a matrix of order 2^m , H_{2^m} , we can define the functions $Wal(0, t)$ to $Wal(2^m - 1, t)$ in the following way. If we divide the interval $[0, 1]$ into 2^m intervals:

$$\left[0, \frac{1}{2^m}\right), \left[\frac{1}{2^m}, \frac{2}{2^m}\right), \dots, \left[\frac{2^m - 1}{2^m}, 1\right),$$

then the Walsh function defined by the i^{th} row of a matrix H_{2^m} takes the value of '1' in the interval $[k/2^m, (k+1)/2^m]$ if :

$$H_{2^m}(i, k + 1) = 1 \quad (11)$$

otherwise it takes the value of '-1'.

**Fig. 1** The First 8 Walsh functions

The following example illustrates the usefulness of the described method to generate Walsh functions. The matrix H_8 is obtained as:

$$H_8 = \begin{pmatrix} H_4 & H_4 \\ H_4 & -H_4 \end{pmatrix} = \left(\begin{array}{cc|cc} H_2 & H_2 & H_2 & H_2 \\ H_2 & -H_2 & H_2 & -H_2 \\ \hline H_2 & H_2 & -H_2 & -H_2 \\ H_2 & -H_2 & -H_2 & H_2 \end{array} \right)$$

$$= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 \end{pmatrix}.$$

It is easy to see by comparing the rows of H_8 with Fig.1 that the mapping between H_8 and the Walsh functions is as follows:

$$H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 \end{pmatrix} \begin{matrix} Wal(0, t) \\ Wal(7, t) \\ Wal(3, t) \\ Wal(4, t) \\ Wal(1, t) \\ Wal(6, t) \\ Wal(2, t) \\ Wal(5, t) \end{matrix}$$

In general, the i^{th} row of the matrix H_{2^m} defines the k^{th} Walsh function $Wal(k, t)$ where k is the number of sign changes in the elements of that row.

The Walsh functions constitute a complete set of orthogonal functions Walsh (1923), which means that every function defined on the interval $[0, 1]$ and having finite norm can be expanded into the generalized Fourier series [26] using Walsh functions.

4.3 Direct sequence spread spectrum CDMA systems

Bipolar spreading sequences derived from Sylvester-Hadamard matrices by simply considering each row of the matrix as a spreading sequence can be used for channel separation in direct sequence code division multiple access (DS CDMA) systems, e.g. Steele (1999). Because of the connection between Sylvester-Hadamard matrices and the Walsh functions described in the previous section, these sequences are often referred to as Walsh-Hadamard sequences in literature dealing with communication systems. Because of the simplicity of Sylvester's construction, they are easy to generate. The spread spectrum signals are of course orthogonal Harmuth (1960) in the case of perfect synchronization, which means that signals spread using different sequences can be perfectly resolved at the receiver. However, the aperiodic

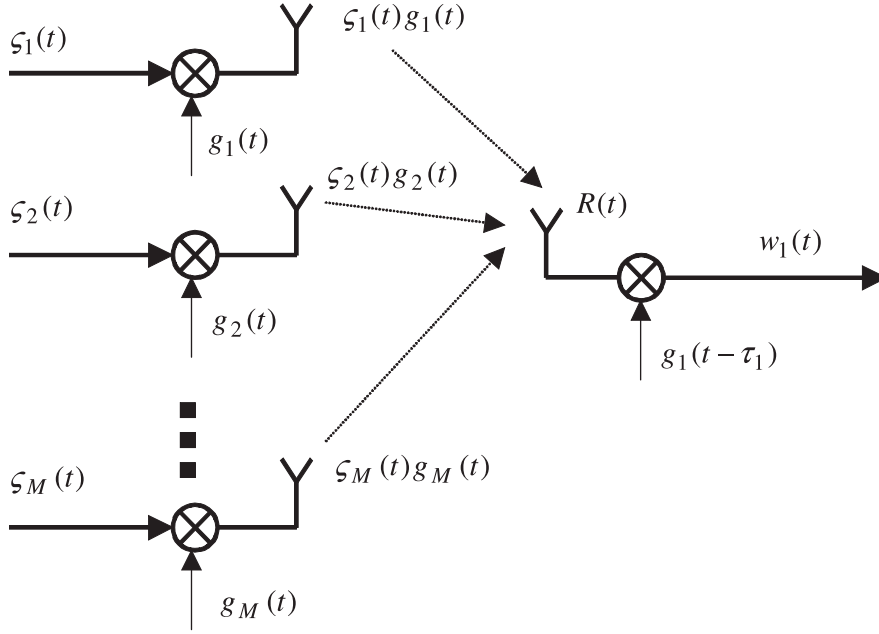


Fig. 2 Block diagram of a basic DS CDMA system

cross-correlation between two Walsh-Hadamard sequences can rise considerably in magnitude if there is a non-zero delay shift between them. Unfortunately, this is very often the case for up-link (mobile to base station) transmission, due to the differences in the corresponding propagation delays.

A block diagram of a conventional Direct Sequence Code Division Multiple Access (DS CDMA) system Lam and Tantaratana (1994) is shown in Figure 2. The first block represents the data modulation of a carrier $c(t)$. Usually, this is of the form $c(t) = A \cos(\omega_0 t)$ and the modulation is either binary phase shift keying (BPSK) or quaternary phase shift keying QPSK, however, there is no restriction placed either on the waveform or the modulation type.

In the case of an angular modulation, the modulation signal of user 1, $\zeta_1(t)$, is expressed as

$$\zeta_1(t) = A \cos[\omega_0 t + \phi_1(t) + \phi_0]$$

where A is the amplitude of the modulated signal, $\omega_0 = 2\pi/T_0$ is the angular carrier frequency, T_0 is a period of the carrier, $\phi_1(t)$ represents the information carrying phase function and ϕ_0 is an initial value of the phase.

Next, the signal $\zeta_1(t)$ is multiplied by the spreading signal $g_1(t)$ of the user 1 being the physical realization of the spreading sequence $\{s_n^{(1)}\}$. The resulting signal $g_1(t)\zeta_1(t)$ is then transmitted over the radio channel. Simultaneously, all other users 2 through M multiply their signals by their own spreading signals. The signal $R(t)$ intercepted in the receiver antenna, neglecting the different path losses and channel noise, is given by:

$$R(t) = g_1(t - \tau_1)\zeta_1(t - \tau_1) + g_2(t - \tau_2)\zeta_2(t - \tau_2) + \cdots + g_M(t - \tau_M)\zeta_M(t - \tau_M)$$

where $\tau_i, i = 1, 2, \dots, M$, denotes delays corresponding to different transmission paths associated with the user i .

Assuming the receiver is configured to receive message from user 1, the de-spread signal $w_1(t)$ is given by

$$w_1(t) = g_1^2(t - \tau_1)\zeta_1(t - \tau_1) + \cdots + g_1(t - \tau_1)g_M(t - \tau_M)\zeta_M(t - \tau_M)$$

where $g_1^2(t - \tau_1)\zeta_1(t - \tau_1)$ is the desired signal and the other terms are the interfering signals responsible for the multi-access interference (MAI).

For general polyphase sequences $\{s_n^{(i)}\}$ and $\{s_n^{(\ell)}\}$ of length N , the discrete aperiodic correlation function is defined as (see Fan and Darnell (1966)):

$$c_{i,k}(\tau) = \begin{cases} \frac{1}{N} \sum_{n=0}^{N-1-\tau} s_n^{(i)} [s_{n+\tau}^{(\ell)}]^*, & 0 \leq \tau \leq N-1 \\ \frac{1}{N} \sum_{n=0}^{N-1+\tau} s_{n-\tau}^{(i)} [s_n^{(\ell)}]^*, & 1-N \leq \tau < 0 \\ 0, & |\tau| \geq N \end{cases} \quad (12)$$

where $[*]$ denotes a complex conjugate operation. When $\{s_n^{(i)}\} = \{s_n^{(\ell)}\}$, Eq.(12) defines the discrete aperiodic auto-correlation function.

Another important parameter used to assess the synchronization amicability of the spreading sequence $\{s_n^{(i)}\}$ is a merit factor, or a figure of merit Golay (1982), 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:

$$F = \frac{c_i^{(0)}}{2 \sum_{\tau=1}^{N-1} |c_i(\tau)|^2} \quad (13)$$

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 (1977) 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 SNR_i , can be expressed in the form:

$$SNR_i = \left(\frac{N_0}{2E_b} + \frac{1}{6N^3} \sum_{k=1, k \neq i}^K \rho_{k,i} \right)^{-0.5} \quad (14)$$

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

$$\rho_{k,i} = 2\mu_{k,i}(0) + \text{Re}\{\mu_{k,i}(1)\} \quad (15)$$

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

$$\mu_{k,i} = N^2 \sum_{n=1-N}^{N-1} c_{k,i}(n)[c_{k,i}(n+\tau)]^*. \quad (16)$$

However, following the derivation in Karkkainen (1992), $\rho_{k,i}$ for polyphase sequences may be well approximated as:

$$\rho_{k,i} \approx 2N^2 \sum_{n=1-N}^{N-1} |c_{k,i}(n)|^2 \quad (17)$$

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 (1997) as a measure of the set cross-correlation performance:

$$R_{CC} = \frac{1}{M(M-1)} \sum_{i=1}^M \sum_{k=1, k \neq i}^M \sum_{\tau=1-N}^{N-1} |c_{k,i}(\tau)|^2 \quad (18)$$

A similar measure, denoted by R_{AC} was introduced in Oppermann and Vucetic (1997) for comparing the auto-correlation performance:

$$R_{AC} = \frac{1}{M} \sum_{i=1}^M \sum_{\tau=1-N, \tau \neq 0}^{N-1} |c_{i,i}(\tau)|^2 \quad (19)$$

The measure defined by (19) allows for comparison of the auto-correlation properties of the set of spreading sequences on the same basis as the cross-correlation properties. It can be used instead of the figures of merit, which have to be calculated for the individual sequences.

For DS CDMA applications we want both parameters R_{CC} and R_{AC} to be as low as possible Oppermann and Vucetic (1997). Because these parameters characterize the whole sets of spreading sequences, it is convenient to use them as the optimization criteria in the design of new sequence sets.

The measures defined by Eqs (18) and (19) 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 analyzing the maximum value of peaks in the aperiodic cross-correlation functions over the whole set of sequences. Hence, an additional measure to compare the spreading sequence sets needs to be considered Seberry et al. (2003):

- The maximum value of the aperiodic cross-correlation functions C_{max}

$$c_{max}(\tau) = \max_{\substack{i=1, \dots, M \\ k=1, \dots, M \\ i \neq k}} |c_{i,k}(\tau)|; \quad \tau = (-N+1), \dots, (N-1) \quad (20)$$

$$C_{max} = \max_{\tau} \{c_{max}(\tau)\}$$

In (2002), Wysocki and Wysocki have shown that by applying the property (iv) of Lemma 2, one can alter aperiodic correlation functions for the whole set of the spreading sequences. For example, the sequences derived from the normalized Sylvester-Hadamard matrix of order 32 have the following correlation parameters:

$$\begin{aligned} C_{max} &= 0.9688 \\ R_{AC} &= 6.5938 \\ R_{CC} &= 0.7873. \end{aligned}$$

On the other hand, the sequences derived from an H -equivalent matrix obtained by multiplying the Sylvester-Hadamard matrix of order 32 by a diagonal matrix with the main diagonal

$$diag = [11 - -1 - 1 - -1 - - - 1111 - -111111111111]$$

are characterized by the following set of the parameters:

$$\begin{aligned} C_{max} &= 0.4063 \\ R_{AC} &= 0.8925 \\ R_{CC} &= 0.9738. \end{aligned}$$

The significant reduction in the value of C_{max} translates to the improvement in the bit error rate for the asynchronous CDMA system utilizing such spreading sequences.

The interesting research question is whether one can further reduce the value of C_{max} by choosing a different diagonal matrix or by permuting the columns of the Hadamard matrix. Theoretically, the minimum value of C_{max} can be computed using the Levenshtein bound Levenshtein (1997), which for the case of bipolar sequences of length 32 equals 0.1410. The bound is, however, obtained without assuming orthogonality of sequences for their perfect alignment, and as such can be considered only as a remote target. To find the absolute answer to the question of a minimum value of C_{max} for the given starting set of sequences, one needs to perform an exhaustive search of all possible diagonal matrices and all possible permutation of columns. Unfortunately, even for the modest matrix order of 32 this is not a trivial task that can be completed, at the current level of computing technology, in a reasonable time. To date, the value of $C_{max} = 0.4063$ is the lowest value obtained for sequences derived from the Sylvester-Hadamard matrix of order 32.

In our successive works Seberry et al. (2002), Seberry et al. (2003), Ang et al. (2003), Seberry et al. (2004), we considered application of Hadamard matrices constructed using different techniques to design spreading sequences for DS CDMA applications. It is interesting to note that the value of C_{max} depends on the construction method used to obtain the non-modified Hadamard matrix. For example, in case of sequences derived from the Hadamard matrix constructed using Hall's difference set Hall (1956) that value can be as low as 0.3750 Seberry et al. (2004).

5 Some other applications of Hadamard matrices

5.1 Screening Properties of Hadamard Matrices

An array on two symbols with N rows and k columns is a (N, k, p) screening design if for each choice of p columns, each of the 2^p row vectors appears at least once. Screening designs are useful for situations where a large number of factors (q) is examined but only a few (k) of these are expected to be important. Screening designs that arise from Hadamard matrices have traditionally been used for identifying main effects only, because of their complex aliasing structures. Without loss of generality we can assume that the first column of a Hadamard matrix contains only 1's. Then by removing this column we obtain $(N, N-1, p)$ screening design, with $p \geq 2$. Some screening designs of this form were introduced by Plackett and Burman (1946) and they are usually referred to as Plackett-Burman designs.

Further interesting papers on the construction of supersaturated screening designs are given by Lin (1993a), Tang and Wu (1997) and Wu (1993).

5.2 Hadamard matrices and optimal weighing designs

Suppose we are given p objects to be weighed in n weighings with a chemical balance (two-pan balance) having no bias. Let:

$x_{ij} = 1$ if the j^{th} object is placed in the left pan in the i^{th} weighing,

$x_{ij} = -1$ if the j^{th} object is placed in the right pan in the i^{th} weighing. Then the $n \times p$ matrix $X = (x_{ij})$ completely characterizes the weighing experiment.

Let us denote the true weights of the p objects by w_1, w_2, \dots, w_p , and by y_1, y_2, \dots, y_n the results of n weighings (so that the readings indicate that the weight of the left pan exceeds that of the right pan by y_i in the i^{th} weighing). Then, denoting the column vectors of w 's and y 's by W and Y , respectively, the readings can be represented by a linear model:

$$Y = XW + e \quad (21)$$

where e is the column vector of e_1, e_2, \dots, e_n and e_i is the error between observed and expected readings. We assume that e is a random vector with a zero mean and a covariance matrix $\sigma^2 I$. This is a reasonable assumption in the case where objects to be weighed have small mass compared to the mass, and hence the inertia, of the balance itself.

Hotelling (1944) showed that for any weighing design the variance \hat{w}_i cannot be less than σ^2/n . Therefore, we shall call a weighing design X optimal, if it estimates each of the weights with this minimum variance σ^2/n . Kiefer's work Kiefer (1975) shows that a chemical balance weighing design X is optimal if it is an $n \times p$ matrix of ± 1 whose columns are orthogonal, and are taken from an Hadamard matrix.

6 Conclusions

Hadamard matrices have a very wide variety of applications in modern communications and statistics. A construction technique of crucial importance in one

application may be less significant in another application. Even H -equivalent Hadamard matrices possess different properties that can lead to different system performance. We give a short bibliography of applications of Hadamard matrices, chosen from the 44 thousand produced by a web search search, to indicate some further applications that have appeared in the literature since Hedayat and Wallis (1978).

7 Bibliography on Hadamard matrices and their applications

- AGAI Agaian S S (1985) Hadamard matrices and their applications, Lecture Notes in Mathematics, vol.1168, Springer-Verlag, Springer-Verlag, Berlin-Heidelberg-New York.
- ARAY Araya M, Harada M and Kharaghani H (2004) Some Hadamard matrices of order 32 and their binary codes, *Journal of Combinatorial Designs*, 12 (2): 142–146.
- BOUS Boussakta S and Holt J G A (1989) Fast algorithm for calculation of both Walsh-Hadamard and Fourier transforms (FWFTs), *Electron. Lett.*, 25 (20): 1352–1353.
- EVAN Evangelaras H, Koukouvinos C and Seberry J (2003) Applications of Hadamard matrices, *J Telecommunications and IT*, 2:2–10.
- FAND Fan P and Darnell M (1966) *Sequence design for communications applications*, John Wiley & Sons, New York.
- GEAD Geadah Y A and Corinthios M J (1977) Natural, dyadic and sequency order algorithms and processors for the Walsh-Hadamard transforms, *IEEE Trans. Comput.*, C-26: 435–442.
- GERA Gerakoulis D P and Ghassemzadeh S S , System and method for generating orthogonal codes, U.S. patent 6,700,864 (Application to wireless communications).
- HAMMa Hammer J and Seberry J (1979) Higher dimensional orthogonal designs and Hadamard matrices II, *Congressus Numerantium*, 27: 23–29. Proceedings of the Ninth Manitoba Conference on Numerical Mathematics.
- HAMMb Hammer J and Seberry J (1981) Higher dimensional orthogonal designs and applications, *IEEE Transactions on Information Theory*, 27(6): 772–779.
- HARA Harada M and Tonchev V D (1995/96) Singly-even self-dual codes and Hadamard matrices, In: Cohen G, Giusti M and Mora T (eds.), *AAECC-11, Hadamard matrices*, In: *Lecture Notes in Comput. Sci.*, vol.948, Springer-Verlag, Berlin-Heidelberg-New York.
- HARW Harwit M and Sloane N J A (1979) *Hadamard transform optics*, Academic Press, Sydney.
- KITA Kitajima H and Shimono T (1983) Residual correlation of the Hadamard transforms of stationary Markov-1 signals, *IEEE Trans. Communications*, 31 (1): 119–121.
- LEEK Lee M H and Kaveh M (1986) Fast Hadamard transform based on a simple matrix factorization, *IEEE Trans. Acoust., Speech, Signal Processing*, ASSP-34 (6): 1666–1667.
- MASC Maschietti A (1992) Hyperovals and Hadamard designs, *J. Geom.*, 44: 107–116.

- MAVR Mavron V and Tonchev V D (2000) On symmetric nets and generalized Hadamard matrices from affine designs, *J. Geometry* 67: 180–187.
- SAMA Samadi S, Suzukake Y and Iwakura H (1998) On automatic derivation of fast Hadamard transform using genetic programming, In: *Proc. 1998 IEEE Asia-Pacific Conference on Circuits and Systems, Thailand*, pp.327–330.
- SEBE Seberry Wallis J (1972) Hadamard matrices, In: Wallis W D, Street A P and Seberry Wallis J, *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, Springer-Verlag, Berlin-Heidelberg-New York.
- YUYI Yu, F T S; Yin, S and Ruffin, B P, (1993) Application of Hadamard transform to fiber-optic smart-skin sensing, *Microwave and Optical Technology Letters*, 6 (11): 632–634.

References

- Ang, R., Seberry, J., Wysocki, B.J., Wysocki, T.A.: Application of nega-cyclic matrices to generate spreading sequences. *ISCTA'2003, Ambleside, U.K.*, (2003)
- Baumert, L.D.: Hadamard matrices of orders 116 and 232. *Bull. Amer Math. Soc.* **72**, 237 (1966)
- Baumert, L.D., Hall, Jr. M.: Hadamard matrices of the Williamson type. *Math. Comput.*, **19** 442–447 (1965)
- Bose, R.C., Shrikhande, S.S.: A note on result in the theory of code construction. *Inf. And Control* **2**, 183–194 (1959)
- Craigen, R., Holzman, W., Kharaghani, H.: Complex golay sequences structure and applications. Report, Univ of Lethbridge, 2001
- Fan, P., Darnell, M.: Sequence design for communications applications. John Wiley & Sons, New York, 1966
- Geramita, A.V., Seberry, J.: Orthogonal designs, quadratic forms and Hadamard matrices. *Lecture Notes in Pure and Applied Mathematics*, vol.43, Marcel Dekker, New York and Basel, 1979
- Goethals, J.-M., Seidel, J.J. A skew-Hadamard matrix of order 36. *J. Austral. Math. Soc.* **22**, 597–614 (1970)
- Golay, M.J.E.: The merit factor of long low autocorrelation binary sequences. *IEEE Trans. on Info. Theory*, vol. **IT-28** 543–549, (1982)
- Hadamard, J.: Resolution d'une question relative aux determinants. *Bull. Sci. Math.* **17**, 240–246 (1893)
- Hall, Jr. M.: A survey of difference sets. *Proc. Amer. Math. Soc.* **7**, 975–986 (1956)
- Hall, Jr. M.: *Combinatorial theory*. Blaidell, Waltham, Mass, 1967
- Harmuth, H.F.: Orthogonal codes. *Proc. of IEE*, 107, Part C, Monograph **369E**, 242–248 (1960)
- Harmuth, H.F.: *Transmission of information by orthogonal functions*. Springer-Verlag, Berlin, 1960
- Hedayat, A.S., Sloane, N.J.A., Stufken, J.: *Orthogonal arrays theory and applications*. Springer-Verlag, New York, 1999
- Hedayat, A., Wallis, W.D.: Hadamard matrices and their applications. *Ann. Stat.* **6**, 1184–1238 (1978)
- Hotelling, H.: Some improvements in weighing and other experimental techniques. *Ann. Math. Stat.* **15**, 297–306 (1944)
- Jain, A.K.: *Fundamentals of digital image processing*. Prentice-Hall, Englewood Cliffs, 1989
- Karckainen, K.H.: Mean-square cross-correlation as a performance measure for spreading code families. *IEEE 2nd Int. Symp. on Spread Spectrum Techniques and Applications (ISSSTA'92)*, 147–150 (1992)
- Kharaghani, H., Tayfeh-Rezaie: A Hadamard matrix of order 428. <http://www.cs.uleth.ca/hadi/h428.pdf>, 2004
- Kiefer, J.: Construction and optimality of generalized Youden designs. In: *Srivastava JN (ed), Statistical design and linear models*, North-Holland, Amsterdam, 1975, pp 333–353
- Koukouvinos, C., Kounias, S.: An infinite class of Hadamard matrices. *J Austral Math Soc A* **46**, 384–394 (1989)

- Lam, A.W., Tantaratana, S.: Theory and applications of spread spectrum systems. IEEE/EAB Self-Study Course, IEEE Inc., Piscataway, 1994
- Levenshtein, V.I.: A new lower bound on aperiodic crosscorrelation of binary codes, 4th International Symp. On Communication Theory and Applications, Ambleside, U.K., 13-18 July 1997, ISCTA'97: 147-149, (1997)
- Lin, D.K.J.: A new class of supersaturated designs. *Technometrics* **35**, 28-31 (1993)
- Oppermann, I., Vucetic, b.S.: Complex spreading sequences with a wide range of correlation properties. *IEEE Trans. on Commun.*, **COM-45** 365-375, 1997
- Paley, R.E.A.C.: On orthogonal matrices. *J. Math. Phys.* **12**, 311-320 (1933)
- Peterson, W.W.: Error correcting codes. The M.I.T. Press, Massachusetts Institute of Technology & J.Wiley & Sons, New York, 1961
- Plackett, R.L., Burman, J.P.: The design of optimum multifactorial experiments. *Biometrika* **33**, 365-375 (1946)
- Plotkin, M.: Binary codes with specified minimum distance, IRE Transactions, IT-6: 445-450 (1960) Also Research Division Report, 51-20, University of Pennsylvania, 1951
- Proakis, J.G.: Digital communications, 3rd ed. McGraw Hill, New York, 1995
- Pursley, M.B.: Performance evaluation for phase-coded spread-Spectrum multiple-access communication - part I system analysis. *IEEE Trans. on Commun.*, **COM-25** 795-799 (1977)
- Seberry, J.: Library of hadamard matrices. <http://www.uow.edu.au/jennie/hadamard.html>, 2004
- Seberry, J., Yamada, M.: Hadamard matrices, sequences, and block designs. In: Dinitz JH, Stinson DR (eds) Contemporary design theory: a collection of surveys, John Wiley & Sons, Inc., 1992, pp 431-437
- Seberry, J.R., Wysocki, B.J., Wysocki, T.A.: On a use of Golay sequences for asynchronous DS CDMA applications. In: Wysocki TA, Darnell M, Honary B (eds) Advanced digital signal processing for communication systems, Kluwer Academic Publishers, Boston/Dordrecht/London, 2002, pp 182-196
- Seberry, J., Wysocki, B.J., Wysocki, T.A.: Williamson-Hadamard spreading sequences for DS-CDMA applications. *J. Wireless Commun. Mobile Comput.* **3**(5), 597-607 (2003)
- Seberry, J., Wysocki, B.J., Wysocki, T.A., Tran, L.C., Wang, Y., Xia, T., Zhao, Y.: Complex orthogonal sequences from amicable Hadamard matrices, IEEE VTC'2004-Spring, Milan, Italy, 17-19 May 2004 - CD ROM, 2004
- Seberry, J., Tran, L.C., Wang, Y., Wysocki, B.J., Wysocki, T.A., Zhao, Y.: Orthogonal spreading sequences constructed using Hall's difference set, IEEE SYMPOTIC'04, Bratislava 23-26 October, 2004 - CD, 2004
- Singer, J.: A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.* **43**, 377-385 (1938)
- Sloane, N.J.A.: A library of Hadamard matrices, <http://www.research.att.com/njas/hadamard/>, 2004
- Stanton, R.G., Sprott, D.A.: A family of difference sets. *Can. J. Math.* **10**, 73-77 (1958)
- Steele, R.: Introduction to digital cellular radio. In: Steele R, Hanzo L (eds), Mobile radio communications, 2nd ed., IEEE Press, New York, 1999
- Sylvester, J.J.: Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *Phil. Mag.* **34** 461-475 (1867)
- Szabatin, J.: Fundamentals of signal theory (in Polish). WKL, Warsaw, 1982
- Tang B, Wu, C.F.J.: A method for constructing supersaturated designs and Es^2 optimality. *Can. J. Statistics* **25**, 191-201 (1997)
- Turyn, R.J.: An infinite class of Williamson matrices. *J. Combin. Theory Ser. A*, **12** 319-321 (1972)
- Turyn, R.J.: Hadamard matrices, Baumert-Hall units, four symbol sequences, pulse compression, and surface wave encodings. *J. Combin. Theory Ser. A* **16**, 313-333 (1974)
- Wallis, W.D., Street, A.P., Seberry Wallis, J.: Combinatorics room squares, sum-free sets, Hadamard matrices. *Lecture Notes in Mathematics*, vol **292**, Springer Verlag, Berlin-Heidelberg-New York, 1972
- Walsh, J.L.: A closed set of normal orthogonal functions. *American J. of Mathematics*, **55**, 5-24 (1923)
- Whiteman, A.L.: A family of difference sets. *Illinois J. Math.*, **6**, 107-121 (1962)
- Williamson, J.: Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.* **11**, 65-81 (1944)

-
- Wu, C.F.J.: Construction of supersaturated designs through partially aliases interactions. *Biometrika* **80**, 661–669 (1993)
- Wu, C.F.J., Hamada, M.: Experiments, planning, analysis, and parameter design optimization. Wiley, New York, 2000
- Wysocki, B.J., Wysocki, T.A.: Modified Walsh-Hadamard sequences for DS CDMA wireless systems. *Int. J. Adapt. Control Signal Process.*, **16** 589–602 (2002)
- Yarlagadda, R.K., Hershey, J.E.: Hadamard matrix analysis and synthesis: with applications to communications and signal/image processing. Kluwer, 1997