Invited paper

Applications of Hadamard matrices

Haralambos Evangelaras, Christos Koukouvinos, and Jennifer Seberry

Abstract — We present a number of applications of Hadamard matrices to signal processing, optical multiplexing, error correction coding, and design and analysis of statistics.

Keywords — Hadamard matrices, orthogonal sequences, CDMA spreading codes, Walsh functions, optical multiplexing.

1. Hadamard matrices and definitions

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

$$[\,1\,],\quad \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix},\quad \begin{bmatrix} - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \\ 1 & 1 & - & 1 \\ 1 & 1 & 1 & - \end{bmatrix}$$

where we write $-$ for -1. These were first studied by J. J. Sylvester [17] who observed that if H is an Hadamard matrix then

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

is also an Hadamard matrix. Indeed, using the matrix of order 2 we have

Lemma 1 (Sylvester [17]): *There is an Hadamard matrix of order 2^t for all integers t.*

We call matrices of order 2^t constructed by Sylvester's construction *Sylvester-Hadamard matrices*. They are naturally associated with discrete orthogonal functions called *Walsh functions*. Using Sylvester's method the first few Hadamard matrices obtained are:

$$\begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix} \quad \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ \hline 1 & 1 & - & - \\ 1 & - & - & 1 \end{array}\right] \quad \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & - & 1 & 1 & - & - & 1 \\ \hline 1 & 1 & 1 & 1 & - & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & - & - & - & - & 1 & 1 \\ 1 & - & - & 1 & - & 1 & 1 & - \end{array}\right]$$

For these matrices we count, row by row, the number of times the sign changes so $1--1$ changes sign twice. This gives:

for the matrix of order 2 : 0,1
for the matrix of order 4 : 0,3,1,2,
for the matrix of order 8 : 0,7,3,4,1,6,2,5

Indeed we shall see that the set of the number of sign changes in a Sylvester-Hadamard matrix of order n is $\{0,1,\ldots,n-1\}$ corresponding to the number of zero crossings of the Walsh functions.

In 1893 Jacques Hadamard [4] gave examples for a few small orders and conjectured they exist for every order divisible by 4. An example for order 12 is:

$$\begin{bmatrix}
1 & 1 & 1 & - & 1 & 1 & - & 1 & 1 & - & 1 & 1 \\
1 & 1 & 1 & 1 & - & 1 & 1 & - & 1 & 1 & - & 1 \\
1 & 1 & 1 & 1 & 1 & - & 1 & 1 & - & 1 & 1 & - \\
1 & - & - & 1 & 1 & 1 & - & 1 & 1 & 1 & - & - \\
- & 1 & - & 1 & 1 & 1 & 1 & - & 1 & - & 1 & - \\
- & - & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - & 1 \\
1 & - & - & 1 & - & - & 1 & 1 & 1 & - & 1 & 1 \\
- & 1 & - & - & 1 & - & 1 & 1 & 1 & 1 & - & 1 \\
- & - & 1 & - & - & 1 & 1 & 1 & 1 & 1 & 1 & - \\
1 & - & - & - & 1 & 1 & 1 & - & - & 1 & 1 & 1 \\
- & 1 & - & 1 & - & 1 & - & 1 & - & 1 & 1 & 1 \\
- & - & 1 & 1 & 1 & - & - & - & 1 & 1 & 1 & 1
\end{bmatrix}$$

We now look at some basic properties of Hadamard matrices:

Lemma 2: *Let H be an Hadamard matrix of order h. Then:*

(i) $HH^T = hI_h$;

(ii) $|\det H| = h^{\frac{1}{2}h}$;

(iii) $HH^T = H^T H$;

(iv) Hadamard matrices may be changed into other Hadamard matrices by permuting rows and columns and by multiplying rows and columns by -1. We call matrices which can be obtained from one another by these methods 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 $+1$ – matrices of this latter form are called normalized;

(vi) if H 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), further n minus ones in any row (column) overlap with n minus ones in each other row (column);

(vii) the order of an Hadamard matrix is 1,2, or $4n$, n positive integer.

Definition 1: If $M = (m_{ij})$ is a $m \times p$ matrix and $N = (n_{ij})$ is an $n \times q$ matrix, then the *Kronecker product* $M \times N$ is the $mn \times pq$ matrix given by

$$M \times N = \begin{bmatrix} m_{11}N & m_{21}N & \cdots & m_{1p}N \\ m_{12}N & m_{22}N & \cdots & m_{2p}N \\ \vdots & & & \\ m_{m1}N & m_{m2}N & \cdots & m_{mp}N \end{bmatrix}$$

Example:

$$\text{Let } M = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ and}$$

$$N = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \text{ then}$$

$$M \times N = \begin{bmatrix} N & N \\ N & -N \end{bmatrix} =$$

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

Lemma 3 (Sylvester-Hadamard): *Let H_1 and H_2 be Hadamard matrices of orders h_1 and h_2. Then by the properties of Kronecker products $H = H_1 \times H_2$ is an Hadamard matrix of order $h_1 h_2$.*

2. Historical background

More than one hundred years ago, in 1893, Jacques Hadamard [4] found square matrices of orders 12 and 20, with entries ± 1, which had all their rows (and columns) orthogonal. These matrices, $X = (x_{ij})$, satisfied the equality of the following inequality

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

and had maximal determinant. Hadamard actually asked the question of matrices with entries on the unit disc but his name has become associated with the real matrices.
Hadamard was not the first to study these matrices for J. J. Sylvester in 1867 in his seminal paper "Thoughts on inverse orthogonal matrices, simultaneous sign-successions and tesselated pavements in two or more colours with application to Newton's rule, ornamental tile work and the theory of numbers" [17] had found such matrices for all orders which are powers of two. Nevertheless, Hadamard showed matrices with elements ± 1 and maximal determinant could exist for all orders 1, 2, and $4t$ and so the Hadamard conjecture "that there exists an *Hadamard matrix*, or square matrix with every element ± 1 and all row (column) vectors orthogonal" came from here. This survey discusses some of the applications of hadamard matrices.

2.1. Hadamard codes

Definition 2: The rows of an Hadamard matrix H of order $4n$ give a $(4n,\ 8n,\ n-1)$ block error correction code as each of the rows has distance at least $2n$ from each of the other rows. The block code is:

$$\begin{bmatrix} H \\ -H \end{bmatrix}$$

In the 1960's the U.S. Jet Propulsion Laboratories (JPL) was working toward building the Mariner and Voyager space probes to visit Mars and the other planets of the solar system. Those of us who saw early black and white pictures of the back of the moon remember that whole lines were missing. The first black and white television pictures from the first landing on the moon were extremely poor quality. How many of us now take the glorious high quality colour pictures of Jupiter, Saturn, Uranus, Neptune and their moons for granted.
In brief, these high quality colour pictures are taken by using three black and white pictures taken in turn through red, green and blue filters. Each picture is then considered as a thousand by a thousand matrix of black and white pixels. Each picture is graded on a scale of, say, one to sixteen, according to its greyness. So white is one and black is sixteen. These grades are then used to choose a codeword in, say, an eight error correction code based on, say, the Hadamard matrix of order 32. The codeword is transmitted to Earth, error corrected, the three black and white pictures reconstructed and then a computer used to reconstruct the coloured pictures.
Hadamard matrices were used for these codewords for two reasons, first, error correction codes based on Hadamard matrices have maximal error correction capability for a given length of codeword and, second, the Hadamard matrices of powers of two are analogous to the Walsh functions, thus all the computer processing can be accomplished using additions (which are very fast and easy to implement in computer hardware) rather than multiplications (which are far slower).

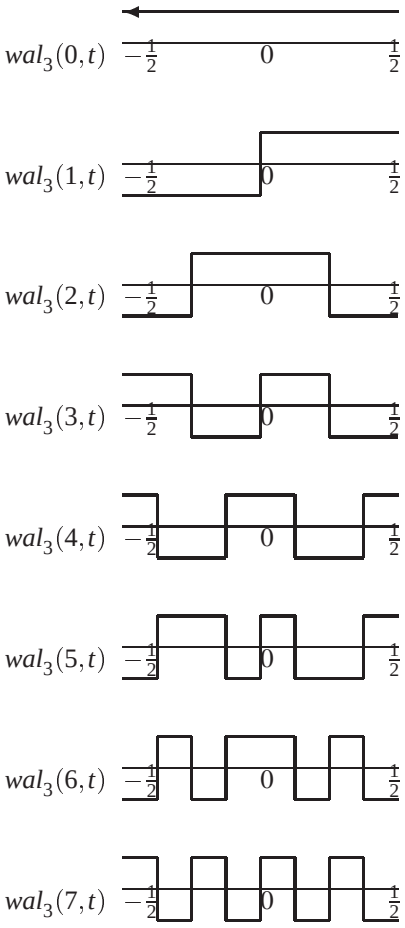
3. Walsh functions

Sylvester's original construction for Hadamard matrices is equivalent to finding Walsh functions which are the discrete analogue of Fourier series.

Example: Let H be a Sylvester-Hadamard matrix of order 8 and sequency order:

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

The Walsh function generated by H is the following:



The points of intersections of Walsh functions are identical with that of trigonometrical functions. By mapping $w(i,t) = wal_n(i,t)$ into the interval $[-\frac{1}{2},0]$, then by mapping axial symmetrically into $[0,\frac{1}{2}]$, we get $w(2i,t)$ which is an even function. By operating similarly we get $w(2i-1,t)$, an odd function.

Just as any curve can be written as an infinite Fourier series

$$\sum_n a_n \sin nt + b_n \cos nt$$

the curve can be written in terms of Walsh functions

$$\sum_n a_n\, sal(i,t) + b_n\, cal(i,t) = \sum_n c_n\, wal(i,t).$$

The hardest curve to model with Fourier series is the step function $wal_2(0,t)$ and errors lead to the Gibbes phenomenom. Similarly, the hardest curve to model with Walsh functions is the basic $\sin 2\pi t$ or $\cos 2\pi t$ curve. Still, we see that we can transform from one to another.

Many problems require Fourier transforms to be taken, but Fourier transforms require many multiplications which are slow and expensive to execute. On the other hand, the fast Walsh-Hadamard transform uses only additions and subtractions (addition of the complement) and so is extensively used to transform power sequency spectrum density, band compression of television signals or facsimile signals or image processing.

4. Desired characteristics of CDMA spreading codes

Hadamard matrices have a significant role to play in the search for desirable CDMA spreading codes.

For bipolar spreading codes $\{s_n^{(i)}\}$ and $\{s_n^{(l)}\}$ of length N, the normalized discrete aperiodic correlation function is defined as [9]:

$$c_{i,l}(\tau) = \begin{cases} \frac{1}{N}\sum_{n=0}^{N-1-\tau} s_n^{(i)} s_{n+\tau}^{(l)}, & 0 \le \tau \le N-1 \\ \frac{1}{N}\sum_{n=0}^{N-1+\tau} s_{n-\tau}^{(i)} s_n^{(l)}, & 1-N \le \tau < 0 \\ 0, & |\tau| \ge N \end{cases}.$$

When $\{s_n^{(i)}\}$ equals $\{s_n^{(l)}\}$, the above equation defines the normalized discrete aperiodic auto-correlation function.

In order to evaluate the performance of a whole set of M spreading codes, the average mean sqaure value of cross-correlation for all codes in the set, denoted by R_{CC}, was introduced by Oppermann and Vucetic [12] as a measure of the set cross-correlation performance:

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

A similar measure, denoted by R_{AC} was introduced there for comparing the auto-correlation performance:

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

The R_{AC} allows for comparison of the auto-correlation properties of the set of spreading codes on the same basis as their cross-correlation properties.

It is higly desirable to have both R_{CC} and R_{AC} as low as possible, as the higher value of R_{CC} results in stronger mult-access interferance (MAI), and an increase in the value of R_{AC} impedes code acquisition process. Unfortunately, decreasing the value of R_{CC} causes increase in the value of R_{AC}, and vice versa.

Both R_{CC} and R_{AC} are very useful for large code sets and large number of active users, when the constellation of interferers (i.e. relative delays among the active users and the spreading codes 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 and in the aperiodic auto-correlation function for $\tau \neq 0$. Hence, one needs to consider two additional measures to compare the spreading sequence sets.
Maximum value of the aperiodic cross-correlation functions C_{max}:

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

Maximum value of the off-peak aperiodic auto-correlation functions A_{max}

$$a_{max}(\tau) = \max_{k=1,\cdots,M} |c_{k,k}(\tau)|;$$

$$A_{max} = \max_{\tau\neq 0}\{a_{max}(\tau)\}.$$

The known relationships between C_{max} and A_{max} are due to Welch [18] and Levenshtein [10].
The Welch bound states that for any set of M bipolar sequences of length N

$$max\{C_{max}, A_{max}\} \geq \sqrt{\frac{M-1}{2NM-M-1}}.$$

A tighter Levenshtein bound is expressed by:

$$max\{C_{max}, A_{max}\} \geq \sqrt{\frac{(2N^2+1)M-3N^2}{3N^2(MN-1)}}.$$

It must be noted here that both Welch and Levenshtein bounds are derived for sets of bipolar sequences where the condition of orthogonality for perfect synchronization is not imposed. Hence, one can expect that by introducing the orthogonality condition, the lower bound for the aperiodic cross-correlation and aperiodic out-of-phase auto-correlation magnitudes must be significantly lifted.

4.1. Constructions for Hadamard matrices for CDMA

There are many constructions for Hadamard matrices and recent work of Seberry, B. Wysocki and T. Wysocki [15] have found that different constructions give different auto-correlation and cross correlation coefficients when tested for CDMA coding.

5. Boolean functions

Hadamard matrices are intimately related with two families of symmetric balanced incomplete block designs. These families of designs are also connected with *boolean functions* used in the construction of *S*-boxes for cryptographic algorithms. The family SBIBD$(4t-1, 2t-1, t-1)$ is related to linear boolean functions and the SBIBD$(4s^2, 2s^2 \pm s, s^2 \pm s)$ to those functions which are "furthest" from linear functions the *bent functions*.

6. The existence and construction of a complete set of orthogonal $F(4t; 2t, 2t)$-squares

This material is from Walter T. Federer [2].

6.1. Introduction and definitions

Hedayat [5] and Hedayat and Seiden [6] have defined an F-square as follows:

Definition 3: Let $A = [a_{ij}]$ be an $n \times n$ matrix and let $\Sigma = (c_1, c_2, ..., c_m)$ be the ordered set of m distinct elements or symbols of A. In addition, suppose that for each $k = 1, 2, \cdots, m$, c_k appears exactly λ_k times $(\lambda_k \geq 1)$ in each row and in each column of A. Then A will be called a *frequency square* or, more concisely, an *F-square* on Σ of order n and frequency vector $(\lambda_1, \lambda_2, \cdots, \lambda_m)$ and will be denoted by $F(n; \lambda_1, \lambda_2, \cdots, \lambda_m)$. Note that $(\lambda_1 + \lambda_2 + \cdots + \lambda_m) = n$ and that when $\lambda_k = 1$ and $m = n$, a latin square results.
As with latin squares, one may consider orthogonality of a pair or a set of F-squares of the same order. The above cited authors give the following two definitions covering these cases:

Definition 4: Given an F-square $F_1(n; \lambda_1, \lambda_2, \cdots, \lambda_k)$ on a set $\Sigma = (a_1, a_2, \ldots, a_k)$ and an F-square $F_2(n; u_1, u_2, ..., u_t)$ on a set $\Omega = (b_1, b_2, ..., b_t)$, we say F_2 is an *orthogonal mate* for F_1 (and write $F_2 \perp F_1$) if upon supposition of F_2 on F_1, a_i appears $\lambda_i u_j$ times with b_j.

Definition 5: Let S_i be an n_i-set, $i = 1, 2, \cdots, t$, and let F_i be an F-square of order n on the set S_i with frequency vector $\lambda_i = (\lambda_{i1}, \lambda_{i2}, \cdots, \lambda_{ih})$. Then $F_1, F_2, ..., F_t$ is a set of t *mutually (pairwise) orthogonal F-squares* if $F_i \perp F_j$, $i \neq j$; $i, j = 1, 2, \cdots, t$. If every $n_i = n$ and every $\lambda_{i\ell} = 1$, $\ell = 1, 2, \cdots, n$, a set of t mutually orthogonal latin squares results and is denoted as $OL(n, t)$.

If a complete set of orthogonal latin squares exists, then $t = n-1$ and the set is denoted as $OL(n, n-1)$. If a complete set of orthogonal F-squares of order n exists, the number will depend upon the values of the n_i in Definition 5. This leads to the following definition:

Definition 6: A complete set of orthogonal F-squares of order n is denoted as $CSOFS(\cdot,\cdot,\cdot)$, and the number of F-squares with i distinct elements is given by the terms in the summation $\sum_{i=2}^{n} N_i F(n; \lambda_1, \lambda_2, \cdots, \lambda_i)$ where $\sum h = 1^i \lambda_h = n$, $\sum i = 2^n N_i (i-1) = (n-1)^2$ and N_i is the number of the squares with i distinct elements.

The fact that $\sum i = 2^n N_i (i-1) = (n-1)^2$ in order to have a *CSOFS* follows directly from analysis of variance theory and from factorial theory in that the interaction of two n-level factors has $(n-1)^2$ degrees of freedom and from the fact that only interection degrees of freedom are available to construct F-squares. For each $F_i(n; \lambda_1, \lambda_2, \cdots, \lambda_i)$-square, there are $(i-1)$ degrees of freedom associated with the i distinct symbols of an F-square, there are N_i F-squares containing i symbols, and hence $(n-1)^2 = \sum_{i=2}^{n} N_i (i-1)$. Federer [2] showed that a *CSOFS* exists for $n = 4t$ and for $i = 2$ distinct symbols. The results have application in zero-one graph theory, in orthogonal arrays, in coding theory, and other areas. It illustrates now analysis of variance and factorial theory can be used to construct the CSOFS and thus provides a new tool for construction purposes.

6.2. Construction of a complete set of $F(4t; 2t, 2t)$-squares

The use of orthogonal contrasts in the analysis of variance for factorial experiments to construct latin squares was indicated by Federer et al [1], Mandeli [11] also used this procedure. It would appear that there is considerable potential in using the orthogonality of single degree of freedom contrasts from the interaction to construct F-squares and latin squares. The following theorem represents one such example:

Theorem 1: *There exists a complete set of* $(4t-1)^2$ *mutually orthogonal* $F(4t; 2t, 2t)$ *squares.*

Proof: A normalised Hadamard matrix is one in which there are all plus ones in the first row and in the first column. The remaining elements are plus and minus ones. Hadamard matrices of side $4t$ are known to exist for all $1 \le t \le 105$ and are presumed to exist for all $4t$. In the last $4t-1$ rows of a normalised $4t \times 4t$ Hadamard matrix, the number of plus ones is equal to the number of minus ones. The Kronecker product of two normalised Hadamard matrices, i.e. $H_{4t} \times H_{4t}$, is a normalised Hadamard matrix of side $16t^2$. Delete the first $4t$ rows of the resulting H_{16t^2} and delete the $4t+1$st, the $8t+1$st, ..., $16t^2-4t+1$st row of the H_{16t^2} matrix. $8t-1$ rows are thus deleted, leaving $(16t^2-8t+1) = (4t-1)^2$ rows having $2t$ plus ones and $2t$ minus ones. Let the plus one be symbol a_1 and the minus on be symbol a_2 in these remaining $(4t-1)^2$ rows. Thus, an $F(4t; 2t, 2t)$-square will be formed from each row resulting in $(4t-1)^2 F(4t; 2t, 2t)$-squares. The resulting F-squares will be mutually orthogonal from the properties of Hadamard matrices. Hence, the *CSOFS* is constructed in this manner. □

7. 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 jth object is placed in the left pan in the ith weighing,

$x_{ij} = -1$ if the jth object is placed in the right pan in the ith weighing,

Then the $n \times p$ matrix $X = (x_{ij})$ completely characterizes the weighing experiment.

Let us write $w_1, w_2, \cdots, w_p$ for the true weights of the p objects, and $y_1, y_2, \cdots, y_n$ for 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 weighing of i), denote the column vectors of w's and y's by W and Y respectively.

Then the readings can be represented by the linear model

$$Y = XW + e,$$

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

We assume X to be a non-singular matrix. Then the best linear unbiased estimator of W is

$$\hat{W} = (X^T X)^{-1} X^T Y$$

with covariance of $\hat{W}$

$$Cov(\hat{W}) = \sigma^2 (X^T X)^{-1}.$$

Hotelling showed that for any weighing design the variance of $\hat{w}_i$ 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 [8] proved that an optimal weighing design in our sense is actually optimal with respect to a very general class of criteria. It can be shown that X is optimal if and only if $X^T X = nI$. This means that a chemical balance weighing design X is optimal if it is an $n \times p$ matrix of ± 1 whose columns are orthogonal, that is an *Hadamard matrix*.

8. Hadamard matrices and optical multiplexing

The connection between Hadamard designs and multiplexing optics is now straightforward. In the optical case

the unknowns w_i represent intensities of individual spatial and/or spectral elements in a beam of radiation. In contrast to scanning instruments which measure the intensities one at a time, the multiplexing optical system measures (i.e. weighs) several intensities (or w_i's) simultaneously. The y_i's now represent the readings of the detector (instead of the reading of the balance). Finally, the weighing design itself, X, is represented by a mask. More precisely, one row of X, which specifies which objects are present in a single weighing, corresponds to the row of transmitting, absorbing or reflecting elements. We usually refer to such a row as a mask configuration.

The two types of weighing designs – chemical and spring balance designs – are realized by masks which contain either transmitting, absorbing and reflecting elements (for the chemical balance design) or simply open and close slots (for the spring balance design). Note that the former case requires two detectors, whereas in the latter case the reference detector can be omitted. In Hadamard transform spectrometry the separated light is sent to a mask. Various parts of the mask will be clear, allowing the light to pass through, reflective (sending light to a secondary detector), or opaque. Let us represent clear, reflective and opaque by $1,\ -1$ respectively. Then the configuration of the mask is represented by a sequence of elements $1,\ -1$.

Suppose k measurements are to be made, and suppose it is convenient to measure the intensity of light at n points of the spectrum. Then the experiment will involve k masks, which can be thought of as $n \times k$ matrix of entries 1, and -1. The efficiency of the experiment is the same as the efficiency of the matrix as a weighing design. The best systems of mask are thus derived from Hadamard matrices.

9. 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 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 insist that the first column of any Hadamard matrix contain only 1's. Then, by removing this column we obtain a $(N, N-1, p)$ screening design, with $p \geq 2$. Some screening designs of this form were introduced by Plackett and Burman [13] and they are termed as *Plackett-Burman* designs. These designs can be generated from the first row, that consists of $N-1$ elements, by cyclic arrangement. The second row is generated by removing all the entries of the first row one position to the right and placing the last element in the first position. The third row is generated from the second row with the same procedure, and the process stops when $N-1$ rows are generated. A row of -1's is then added as the last row, completing the design with N runs and $N-1$ columns. By adding a column of all 1's in a Plackett and Burman design with N runs we obtain a Hadamard matrix of order N. In fact, Plackett and Burman constructed Hadamard matrices of order N, for all $N \leq 100$ except $N = 92$ which was later given by Baumert, Colomb and Hall in 1962. For more details see [16]. As an example, the first rows that generate the Plackett and Burman designs with $N = 8,\ 12,\ 16,\ 20$ and 24 runs are given below.

```
 8  + + + − + − −
12  + + − + + + − − − + −
16  + + + + − + − + + − − + − − −
20  + + − − + + + + − + − + − − − − + + −
24  + + + + + − + − + + − − + + − − + − + − − − −
```

After the identification of the active factors, the original design is then projected into k dimensions for further analysis, that is, we select the columns that correspond to the active factors to form a new design with N runs and k columns which is called a *projection*.

Since the choice of k columns varies with the outcome of the analysis, it is desired to study the properties of all projection designs that may arise.

Projection designs that arise from Hadamard matrices are either regular or non-regular factorial plans. Regular fractional factorial designs, have simple aliasing structures and usually arise from Hadamard matrices of orders $N = 2^p$; non-regular fractional factorial designs have complex aliasing structures.

The aliasing structure of regular factorial designs can easily be computed. On the other hand, the alias structure of non-regular designs cannot easily be computed. For more details on fractional factorial designs and screening experiments we refer the interested reader to Wu and Hamada [20].

10. Supersaturated designs

Supersaturated designs are useful in situations in which the number of active factors is very small compared to the total number of factors being considered.

The use of Hadamard matrices to construct supersaturated designs that can examine $k = N-2$ factors in $n = N/2$ runs, where N is the order of the normalized Hadamard matrix used. The first column of all 1's is not taken into consideration since it is fully aliased with the mean. Then, we choose a *branching column* out of the remaining $N-1$ columns and we split the N runs into two groups. Group I contains all the runs with the sign $+1$ in the branching column and Group II contains the remaining runs. Then by deleting the branching column either from Group I or Group II causes the remaining $N-2$ columns to form a super saturated design to examine $k = N-2$ factors in $N/2$ runs.

11. Edge designs

These designs allow a model-independent estimate of the set of relevant variables, thus providing more robustness than traditional designs. They use a construction known as skew-Hadamard matrices.

If the first row and first column of C is removed, a $(N-1)\times(N-1)$ matrix S is obtained to be used in the form

$$X = \begin{pmatrix} \mathbf{1} & S+I_{N-1} \\ \mathbf{1} & S-I_{N-1} \end{pmatrix}$$

in order to obtain the resulting edge design, where $\mathbf{1}^T = (1,1,\ldots,1)$ is a $1\times(N-1)$ vector with all entries equal to 1.

12. Idle column method

This uses Hadamard matrices of order $N = 8t$ to construct multi-level idle column arrays.

Let $H_{N/2}$ be a normalized Hadamard matrix of order $N/2$. We can denote this matrix by $H_{N/2} = (\mathbf{1}, \mathbf{C}_1, \ldots, \mathbf{C}_{N/2-1})$. Then it is well known that

$$\begin{aligned} H_N &= \begin{pmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{1}\ \mathbf{C}_1 \cdots \mathbf{C}_{N/2-1} & \mathbf{1} & \mathbf{C}_1 \cdots & \mathbf{C}_{N/2-1} \\ \mathbf{1}\ \mathbf{C}_1 \cdots \mathbf{C}_{N/2-1} & -\mathbf{1} & -\mathbf{C}_1 \cdots & -\mathbf{C}_{N/2-1} \end{pmatrix} \end{aligned}$$

is a Hadamard matrix of order N.

Remove the first column of H_N and by treating the column $(\mathbf{1}^T, -\mathbf{1}^T)^T$ as the idle column, the product of columns $(\mathbf{C}_i^T, \mathbf{C}_i^T)^T$ and $(\mathbf{C}_i^T, -\mathbf{C}_i^T)^T$ for $1 \le i \le \frac{N}{2} - 1$, equals to the idle column. Then, for the level combinations of the two columns in a pair, the recoding scheme

$$\begin{aligned} (-1,-1) &\longrightarrow -1 \\ (-1,1) &\longrightarrow 0 \\ (1,-1) &\longrightarrow 1 \\ (1,1) &\longrightarrow 0 \end{aligned}$$

is used to construct a three level column.

References

[1] W. T. Federer, A. Hedayat, E. T. Parker, B. L. Raktoe, E. Seiden, and R. J. Turyn, "Some techniques for constructing mutually orthogonal latin squares", MRC Technical Summary Report no. 1030, Mathematics Research Centre University of Wisconsin, June 1971. (A preliminary version of this report appeared in the proceedings of the Fifteenth Conference on the Design of Experiments in Army Research Development and Testing, ARO-D Report 70-2, July 1970, The Office of Chief of Research and Development, Durham, North Carolina).

[2] W. T. Federer, "On the existence and construction of a complete set of orthogonal $F(4t;2t,2t)$-squares", Paper no. BU-564-M in the Biometrics Unit Mimeo Series, Department of Plant Breeding and Biometry, Cornell University, Ithica, New York, 14853, 1975.

[3] A. V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*. New York-Basel: Marcel Dekker, 1979.

[4] J. Hadamard, "Resolution d'une question relative aux determinants", *Bull. Sci. Math.*, vol. 17, pp. 240–246, 1993.

[5] A. Hedayat, "On the theory of the existence, non-existence and the construction of mutually orthogonal F-squares and latin squares". Ph.D. dissertation, Cornell University, June 1969.

[6] A. Hedayat and E. Seiden, "F-square and orthogonal F-square design: A generalization of Latin square and orthogonal Latin squares design", *Ann. Math. Stat.*, vol. 41, pp. 2035–2044, 1970.

[7] C. Koukouvinos and J. Seberry, "New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function – a review", *J. Stat. Plan. Infer.*, vol. 81, pp. 153–182, 1999.

[8] J. Kiefer, "Construction and optimality of generalized Youden designs", in: *Statistical Design and Linear Models*, J. N. Srivastava, Ed. Amsterdam: North-Holland, 1975, pp. 333–353.

[9] A. W. Lam and S. Tantaratana, "Theory and applications of spread-spectrum systems", IEEE/EAB Self-Study Course, IEEE Inc., Piscataway, 1994.

[10] V. I. Levenshtein, "A new lower bound on aperiodic crosscorrelation of binary codes", in *4th Int. Symp. Commun. Theory & Appl., ISCTA'97*, 1997, pp. 147–149.

[11] J. P. Mandeli, "Complete sets of orthogonal F-squares". M.Sc. thesis, Cornell University, Aug. 1975.

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

[13] R. L. Plackett and J. P. Burman, "The design of optimum multifactorial experiments", *Biometrika*, vol. 33, pp. 305–325, 1946.

[14] J. Seberry and R. Craigen, "Orthogonal designs", in *Handbook of Combinatorial Designs,* C. J. Colbourn and J. H. Dinitz, Eds. CRC Press, 1996, pp. 400–406.

[15] J. Seberry, B. J. Wysocki, and T. A. Wysocki, "Golay sequences for DS CDMA applications", in *Sixth Int. Symp. DSP Commun. Syst. DSPCS'02*, Manly, TITR, Wollongong, Jan. 2002, pp. 103–108.

[16] J. Seberry and M. Yamada, "Hadamard matrices, sequences and designs", in *Contemporary Design Theory – a Collection of Surveys*, D. J. Stinson and J. Dinitz, Eds. Wiley, 1992, pp. 431–560.

[17] J. J. Sylvester, "Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers", *Phil. Mag.*, vol. 34, pp. 461–475, 1967.

[18] L. R. Welch, "Lower bounds on the maximum cross-correlation of signals", *IEEE Trans. Inform. Theory*, vol. 20, pp. 397–399, 1974.

[19] J. Seberry Wallis, "Part IV of combinatorics: Room squares, sum-free sets and Hadamard matrices", *Lecture Notes in Mathematics*, W. D. Wallis, A. Penfold Street, and J. Seberry Wallis, Eds. Berlin-Heidelberg-New York: Springer, 1972, vol. 292.

[20] C. F. J. Wu and M. Hamada, *Experiments, Planning, Analysis, and Parameter Design Optimization*. New York: Wiley, 2000.

Haralambos Evangelaras received the B.Sc. degree in mathematics from the University of Athens, Athens, Greece, in 1998. He is currently a Ph.D. student at the National Technical University of Athens in the area of statistics.

Department of Mathematics
National Technical University of Athens
Zografou 15773
Athens, Greece

Christos Koukouvinos received the B.Sc. degree in mathematics and the Ph.D. in statistics, both from the University

of Thessaloniki, Thessaloniki, Greece, in 1983 and 1988, respectively. In 1996, he received the Hall medal (a research award) from the ICA. He is a fellow of the ICA and since 2001 an elected member of the Council of the ICA. He is in the Editorial Board for the *Australasian Journal of Combinatorics*, and the *Journal of Modern Applied Statistical Methods*. He is currently a Professor at the National Technical University of Athens. His research interests include statistics, combinatorics, matrix theory, coding theory and computational mathematics.

Department of Mathematics
National Technical University of Athens
Zografou 15773, Athens, Greece

Jennifer Seberry received her B.Sc.(Hons), M.Sc. in mathematics from the University of NSW and her M.Sc. and Ph.D. in mathematics from La Trobe University, Victoria, Australia. For the past twent years she has also been working in cryptography and computer security. In 1987 she founded the Centre for Computer Security Research. She is presently Professor of Computer Science at the University of Wollongong. She has over 300 publication and has successfully supervised 22 Ph.D. theses.

School of IT and Computer Science
University of Wollongong
Wollongong, NSW, 2522
Australia