11

Hadamard Matrices, Sequences, and Block Designs

Jennifer Seberry and Mieko Yamada

1	INTRODUCTION	431
2	HADAMARD MATRICES	437
3	THE STRONGEST HADAMARD CONSTRUCTION THEOREMS	443
4	ORTHOGONAL DESIGNS AND ASYMPTOTIC EXISTENCE	458
5	SEQUENCES	466
6	AMICABLE HADAMARD MATRICES AND AOD	487
7	CONSTRUCTIONS FOR SKEW HADAMARD MATRICES	492
8	M-STRUCTURES	498
9	WILLIAMSON AND WILLIAMSON-TYPE MATRICES	511
10	SBIBD AND THE EXCESS OF HADAMARD MATRICES	523
11	COMPLEX HADAMARD MATRICES	529
	APPENDIX	535
	REFERENCES	554

1 INTRODUCTION

One hundred years ago, in 1893, Jacques Hadamard [31] found square matrices of orders 12 and 20, with entries ± 1, which had all their rows (and columns) pairwise 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 so had maximal determinant among matrices with entries ± 1. Hadamard actually asked the question of finding the maximal determinant of matrices with entries on the unit disc, but his name has become associated with the question concerning real matrices.

Contemporary Design Theory: A Collection of Surveys, Edited by Jeffrey H. Dinitz and Douglas R. Stinson
ISBN 0-471-53141-3

Hadamard was not the first to study these matrices, for J. J. Sylvester in 1857, in his seminal paper, "Thoughts on inverse orthogonal matrices, simultaneous sign-successions and tesselated pavements in two or more colors with application to Newton's rule, ornamental tile work and the theory of numbers" [97], had found such matrices for all orders that are powers of two. Nevertheless, Hadamard showed that matrices with entries ± 1 and maximal determinant could exist only for orders 1, 2, and $4t$. The Hadamard conjecture states that "there exists an *Hadamard matrix*, or square matrix with every entry ± 1 and row (column) vectors pairwise orthogonal for these orders." This survey indicates the progress that has been made in the past 100 years.

Hadamard's inequality applies to matrices with entries from the unit circle. Matrices with entries ± 1, $\pm i$, and pairwise orthogonal rows (and columns) are called *complex Hadamard matrices* (note the scalar product is $a \cdot b = \sum a_i b_i^*$ for complex numbers). These matrices were first studied by R. J. Turyn [104]. We believe complex Hadamard matrices exist for every order $n \equiv 0 \pmod 2$. The truth of this conjecture would imply the truth of the Hadamard conjecture.

We begin by mentioning a few practical applications of Hadamard matrices. We note that it was M. Hall, Jr., L. Baumert, and S. Golomb [4] working with the U.S. Jet Propulsion Laboratories (JPL) who sparked the interest in Hadamard matrices in the past 30 years. In the 1960s the 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 black-and-white television pictures from the first landing on the moon were extremely poor quality. How many of us remember that the recent flyby of Neptune was by a space probe launched in the seventies? We take the high-quality color pictures of Jupiter, Saturn, Uranus, Neptune, and their moons for granted.

In brief, these high-quality color pictures are made by using three black-and-white pictures taken, in turn, through red, green, and blue filters. Each picture is then considered as a 1000×1000 matrix of black-and-white pixels. Each pixel is graded on a scale of 1 to 16, according to its greyness. So white is 1, and black is 16. These grades are then used to choose a codeword in an eight error correction code based on the Hadamard matrix of order 32. The codeword is transmitted to Earth, error corrected, the three black-and-white pictures are reconstructed, and then a computer is used to obtain the colored pictures.

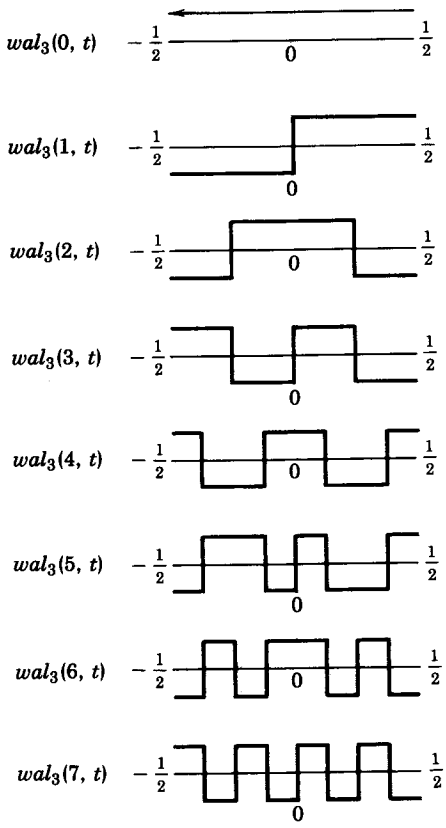
Hadamard matrices were used for these codewords for two reasons. First, error correction codes based on Hadamard matrices have maximal error correction capability for a given length of codeword. Second, the Hadamard matrices of powers of two are analogous to the Walsh functions, and thus all the computer processing can be accomplished using additions (which are very fast and easy to implement in computer hardware) rather than multiplications (which are far slower).

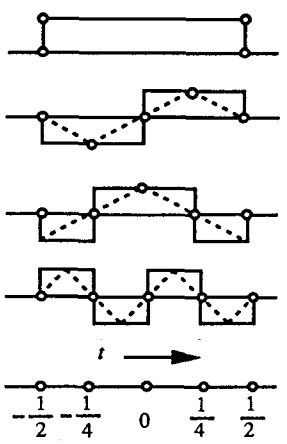
Sylvester's original construction for Hadamard matrices is equivalent to finding Walsh functions [48] which are the discrete analogue of Fourier Series.

Example 1.1. Let H be a Sylvester-Hadamard matrix (see Section 2) of order $8 = 2^3$.

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

The Walsh function wal_3 generated by H is the following:





$wal_2(0,t)$ — 1

$wal_2(1,t)$ — $\sqrt{2}\sin 2\pi t$

$wal_2(2,t)$ — $\sqrt{2}\cos 2\pi t$

$wal_2(3,t)$ — $\sqrt{2}\sin 4\pi t$

Walsh functions Trigonometrical functions

Figure 1.1. Walsh functions and trigonometrical functions.

The Walsh function wal_n is constructed in a similar way from the Sylvester-Hadamard matrix of order 2^n. The points of intersections of Walsh functions are identical with those of trigonometrical functions. See Figure 1.1.

As Figure 1.1 shows, by mapping $w(i,t) = wal_n(i,t)$ into the interval $[-\frac{1}{2},0]$, and then by extending the graph 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,

$$\sum_n a_n sal_n(i,t) + b_n cal_n(i,t) = \sum_n c_n wal_n(i,t),$$

where $sal_n(i,t)$ and $cal_n(i,t)$ are, respectively, even and odd components of the Walsh function $wal_n(i,t)$. The hardest curve to model with Fourier series is the step function $wal_2(0,t)$, and errors lead to the Gibbes phenomenon. 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 each form to the other.

Many problems require Fourier transforms to be taken, but Fourier transforms require many multiplications that 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 used extensively to transform power sequency spectrum density, band compression of television signals or facsimile signals or image processing.

Walsh functions are easy to extend to higher dimensions (and higher dimensional Hadamard matrices) to model surfaces in three and higher dimensions—

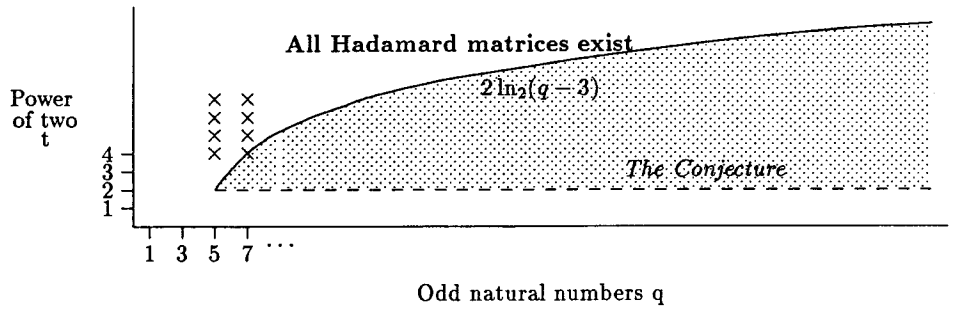


Figure 1.2. Hadamard matrices of order $2^t q$.

Fourier series are more difficult to extend. Walsh-Hadamard transforms in higher dimensions are also effected using only additions (and subtractions).

We now give an overview of construction methods for Hadamard matrices. Constructions for Hadamard matrices can be roughly classified into three types:

1. Multiplication theorems;
2. "Plug-in" methods;
3. Direct constructions.

In 1976, Jennifer Seberry Wallis, in her paper, "On the existence of Hadamard matrices" [121], showed that "given any odd natural number q, there exists a $t \approx 2\log_2(q-3)$ so that there is an Hadamard matrix of order $2^t q$ (and hence for all orders $2^s q$, $s \geq t$)." This is represented graphically in Figure 1.2.

In fact, as we show in our Appendix, Hadamard matrices are known to exist of order $2^2 q$ for most $q < 3000$ (we have results up to 40000 that are similar). In many other cases, Hadamard matrices of order $2^3 q$ or $2^4 q$ exist. A quick look at the Appendix shows most of the very difficult cases are for q (prime) $\equiv 3 \pmod 4$.

Hadamard's original construction for Hadamard matrices is a "multiplication theorem" as it uses the fact that the Kronecker product of Hadamard matrices of orders $2^a m$ and $2^b n$ is an Hadamard matrix of order $2^{a+b} mn$. Our graph shows that we would like to reduce this power of two. In his book, *Hadamard Matrices and Their Applications*, Agayan [1] shows how to multiply these Hadamard matrices to get an Hadamard matrix of order $2^{a+b-1} mn$ (which lowers the curve in our graph except for q prime).

Paley's 1933 "direct" construction [66], which gives Hadamard matrices of order $\Pi_{i,j}(p_i + 1)(2(q_j + 1))$, p_i (prime power) $\equiv 3 \pmod 4$, q_j (prime power) $\equiv 1 \pmod 4$, is extremely productive of Hadamard matrices, but we note again the proliferation of powers of two as more products are taken.

Many people do not realize that in the same issue of the *Journal of Mathematics and Physics* as Paley's paper appeared, J. A. Todd showed the equivalence of Hadamard matrices of order $4t$ and $(4t-1, 2t-1, t-1)$-SBIBD (see

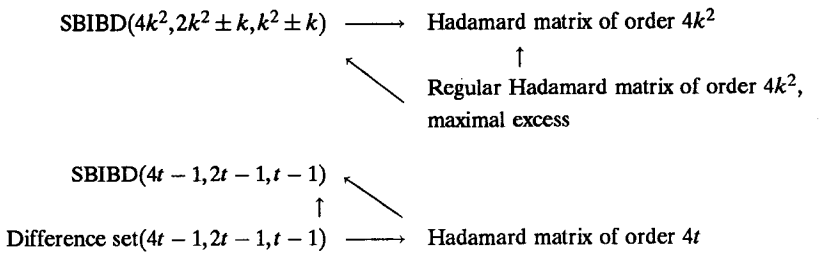


Figure 1.3. Relationship between SBIBD and Hadamard matrices.

Figure 1.3). This family of SBIBD, its complementary family $(4t-1, 2t, t)$-SBIBD, and the family $(4s^2, 2s^2 \pm s, s^2 \pm s)$-SBIBD are called *Hadamard designs*. The latter family satisfies the constraint $v = 4(k-\lambda)$, for $v = 4s^2$, $k = 2s^s \pm s$, and $\lambda = s^2 \pm s$, which appears in some constructions (e.g., Shrikhande [91]). Hadamard designs have the maximum number of one's in their incidence matrices among all incidence matrices of (v, k, λ)-SBIBD (see Tsuzuku [103]).

In 1944, J. Williamson [128], who coined the name *Hadamard matrices*, first constructed what have come to be called *Williamson matrices*, or with a small set of conditions, *Williamson type matrices*. These matrices are used to replace the variables of a formally orthogonal matrix. We say Williamson type matrices are "plugged in" to the second matrix. Other matrices that can be "plugged in" to arrays of variables are called *suitable matrices*. Generally the arrays into which suitable matrices are plugged are *orthogonal designs*, which have formally orthogonal rows (and columns) but may have variations such as Goethals-Seidel arrays, Wallis-Whiteman arrays, Spence arrays, generalized quarternion arrays, Agayan families, Kharaghani's methods, and regular s-sets of regular matrices that give new matrices. This is an extremely prolific method of construction. We will discuss methods that give matrices to "plug in" and matrices to "plug into."

As a general rule, if we want to check if an Hadamard matrix of a specific order $4pq$ exists, we would first check if there are Williamson type matrices of order p, q, pq; then we would check if there is an OD$(4t; t, t, t, t)$ for $t = q, p, pq$. This failing, we would check the "direct" constructions. Finally, we would use a "multiplication theorem." When we talk of "strength" of a construction, this reflects a personal preference.

Before we proceed to more detail, we will consider diagrammatically some of the linkages between conjectures that will arise in this survey: The conjecture implied is "the necessary conditions are sufficient for the existence of (say) Hadamard matrices" (see Figure 1.4). (A *weighing matrix* W has entries $0, \pm 1$, is square, and satisfies $WW^T = kI$.)

The hierarchy of conjectures for weighing matrices and ODs is more straightforward. Settling the OD conjecture in Table 1.1 would settle the weighing matrix conjecture to its left. This survey emphasizes those constructions, selected by us, which we believe show the most promise toward solving the Hadamard conjecture and which were found in the last 15 years.

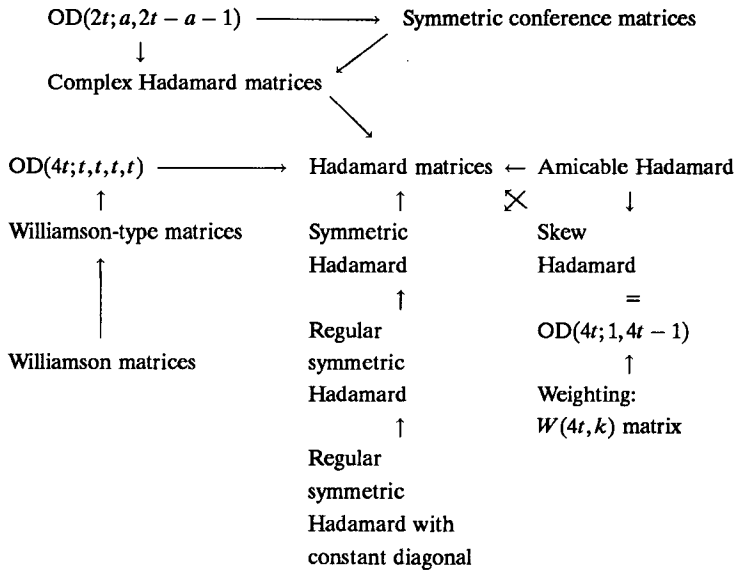


Figure 1.4. Conjecture: "The necessary conditions are sufficient for the existence of (say) Hadamard matrices."

TABLE 1.1 Weighing Matrix and OD Conjectures

	Matrices	OD's
Strongest	Skew-weighing	$\mathrm{OD}(n;1,k)$
	Weighing $W(n;k)$, n odd	
	Weighing $W(2n,k)$, n odd	$\mathrm{OD}(2n;a,b)$, n odd
	Weighing $W(4n,k)$, n odd	$\mathrm{OD}(4n;a,b,c,d)$, n odd
Weakest	$W(2^s n,k)$, n odd, $s \geq 3$	$\mathrm{OD}(2^s n;u_1,u_2,\ldots,u_s)$, n odd

2 HADAMARD MATRICES

A square matrix with elements ± 1 and order 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 [97] 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 2.1 (Sylvester [97]). *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*. We have seen that these matrices are naturally associated with the discrete orthogonal functions called *Walsh functions*. Using Sylvester's method, the first few Hadamard matrices obtained are

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

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

For these matrices, we count, row by row, the number of times the sign changes; for example, $1 - -1$ 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 will see that the set of the numbers of sign changes in the rows of a Sylvester-Hadamard matrix of order n is $\{0, 1, \ldots, n-1\}$, corresponding to the number times the Walsh functions cross the x-axis.

In 1893, Jacques Hadamard [31] gave examples of Hadamard matrices for a few small orders and conjectured that they exist for every order divisible by 4. Some examples for order 12 are

$$\left[\begin{array}{cc|cccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
- & 1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - \\
- & - & 1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 \\
- & 1 & - & 1 & 1 & - & 1 & 1 & 1 & - & - & - \\
- & - & 1 & - & 1 & 1 & - & 1 & 1 & 1 & - & - \\
- & - & - & 1 & - & 1 & 1 & - & 1 & 1 & 1 & - \\
- & - & - & - & 1 & - & 1 & 1 & - & 1 & 1 & 1 \\
- & 1 & - & - & - & 1 & - & 1 & 1 & - & 1 & 1 \\
- & 1 & 1 & - & - & - & 1 & - & 1 & 1 & - & 1 \\
- & 1 & 1 & 1 & - & - & - & 1 & - & 1 & 1 & - \\
- & - & 1 & 1 & 1 & - & - & - & 1 & - & 1 & 1 \\
- & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & 1
\end{array}\right],$$

$$\left[\begin{array}{cc|ccccc|cc|ccccc}
1 & 1 & 1 & 1 & 1 & 1 & - & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - & 1 \\
1 & 1 & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - \\
1 & - & 1 & 1 & 1 & - & 1 & - & 1 & - & 1 & - \\
1 & - & - & 1 & 1 & 1 & 1 & - & - & 1 & - & 1 \\
1 & 1 & - & - & 1 & 1 & 1 & 1 & - & - & 1 & - \\
\hline
- & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - \\
1 & - & 1 & - & - & 1 & - & - & - & 1 & 1 & - \\
1 & 1 & - & 1 & - & - & - & - & - & - & 1 & 1 \\
1 & - & 1 & - & 1 & - & - & 1 & - & - & - & 1 \\
1 & - & - & 1 & - & 1 & - & 1 & 1 & - & - & - \\
1 & 1 & - & - & 1 & - & - & - & 1 & 1 & - & -
\end{array}\right],$$

$$\left[\begin{array}{ccc|ccc|ccc|ccc}
1 & 1 & 1 & - & 1 & 1 & - & 1 & 1 & - & 1 & 1 \\
1 & 1 & 1 & 1 & - & 1 & 1 & - & 1 & 1 & - & 1 \\
1 & 1 & 1 & 1 & 1 & - & 1 & 1 & - & 1 & 1 & - \\
\hline
1 & - & - & 1 & 1 & 1 & - & 1 & 1 & 1 & - & - \\
- & 1 & - & 1 & 1 & 1 & 1 & - & 1 & - & 1 & - \\
- & - & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - & 1 \\
\hline
1 & - & - & 1 & - & - & 1 & 1 & 1 & - & 1 & 1 \\
- & 1 & - & - & 1 & - & 1 & 1 & 1 & 1 & - & 1 \\
- & - & 1 & - & - & 1 & 1 & 1 & 1 & 1 & 1 & - \\
\hline
1 & - & - & - & 1 & 1 & 1 & - & - & 1 & 1 & 1 \\
- & 1 & - & 1 & - & 1 & - & 1 & - & 1 & 1 & 1 \\
- & - & 1 & 1 & 1 & - & - & - & 1 & 1 & 1 & 1
\end{array}\right],$$

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

We have given these matrices in full because, unfortunately, an earlier survey contains errors.

Two Hadamard matrices are said to be *Hadamard equivalent* (or just *equivalent*) if one can be obtained from the other by a sequence of operations of the following two types:

1. Permute rows (or columns).
2. Multiply any row (or column) by -1.

Although the Hadamard matrices of order 12 presented above appear to be different, it is possible to show that they are equivalent.

In fact, we know that there are 5 inequivalent matrices of order 16 [32], 3 of order 20 [33], 60 of order 24 [37, 47], 486 of order 28 [44], over 15 of order 32 (N. Ito, personal communication, 1989), and over 109 of order 36 [11].

An Hadamard matrix of order 20 is given in Figure 2.1. This figure is more easily described by calling the rows 0 to 19 and saying that the zeroth row is all ones, the first row has ones in positions

$$\{1,2,5,6,7,8,10,12,17,18\},$$

the second row has ones in positions

$$\{2,3,6,7,8,9,11,13,18,19\},$$

the third row has ones in positions

$$\{4,5,8,9,10,11,13,15,1,2\},$$

and so on.

This example illustrates the use of difference sets with the parameters $(4t-1, 2t-1, t-1)$ in the construction of Hadamard matrices. $\{1,2,5,6,7,8,10,12,17,18\}$ is a difference set with parameters $(19,9,4)$. For more information on difference sets, see the survey by Jungnickel in this volume [40].

Hadamard matrices can also be constructed using supplementary difference sets. The existence of supplementary difference sets in the abelian group $Z_3 \times Z_3$ and can be used to construct another Hadamard matrix of order 20 given in Figure 2.2.

We now recall some basic properties of Hadamard matrices:

Lemma 2.2. *Let H be an Hadamard matrix of order h. Then the following hold*:

1. $HH^T = hI_h$.
2. $|\det H| = h^{(1/2)h}$.
3. $HH^T = H^T H$.

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	−
−	−	−	−	−	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	−	−
−	−	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

Figure 2.1. An Hadamard matrix of order 20.

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
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	−	−	−	−	−	−

Figure 2.2. A second Hadamard matrix of order 20.

4. *Every Hadamard matrix is equivalent to an Hadamard matrix that has every element of its first row and column* $+1$ *(matrices of this latter form are called normalized).*
5. $h = 1, 2,$ *or* $4n$, n *an integer.*

6. *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).*

Definition 2.1. An Hadamard matrix H is said to be *regular* if the sum of all the elements in each row or column is a constant k. Hence $HJ = JH = kJ$, where J is the matrix of all ones.

Definition 2.2. 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

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

Example 2.1. Let

$$M = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{and} \quad N = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}.$$

Then

$$M \times N = \begin{bmatrix} N & N \\ N & -N \end{bmatrix} = \left[\begin{array}{cccc|cccc} -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \\ \hline -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \end{array}\right].$$

Lemma 2.3 (Hadamard [31]). *Let H_1 and H_2 be Hadamard matrices of orders h_1 and h_2. Then $H = H_1 \times H_2$ is an Hadamard matrix of order $h_1 h_2$.*

We now prove a stronger result than Hadamard's, first proved by Agayan and Sarukhanyan, and then strengthened by Seberry and Yamada [87] and

Agayan-Sarukhanyan [1]. These theorems have the advantage of reducing the power of two in the resulting Hadamard matrix.

Lemma 2.4 (The Multiplication Theorem of Agayan-Sarukhanyan [1]). *Let H_1 and H_2 be Hadamard matrices of orders $4h$ and $4k$. Then there is an Hadamard matrix of order $8hk$.*

Proof. Write the two Hadamard matrices as

$$H_1 = \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \quad \text{and} \quad H_2 = \begin{bmatrix} K & L \\ M & N \end{bmatrix}.$$

We note that since $H_1 H_1^T = 4hI$ and $H_2 H_2^T = 4kI$, we have

$$PP^T + QQ^T = RR^T + SS^T = 2hI, \qquad PR^T + QS^T = O = RP^T + SQ^T;$$

$$KK^T + LL^T = MM^T + NN^T = 2kI, \qquad KM^T + LN^T = O = MK^T + NL^T.$$

The required Hadamard matrix of order $8hk$ is

$$\begin{bmatrix} \frac{1}{2}(P+Q)\times K + \frac{1}{2}(P-Q)\times M & \frac{1}{2}(P+Q)\times L + \frac{1}{2}(P-Q)\times N \\ \frac{1}{2}(R+S)\times K + \frac{1}{2}(R-S)\times M & \frac{1}{2}(R+S)\times L + \frac{1}{2}(R-S)\times N \end{bmatrix}$$

which can be verified by simple algebraic manipulation. □

Example 2.2. There are Hadamard matrices of orders 12 and 20. Sylvester's lemma guarantees the existence of an Hadamard matrix of order 240, while the Agayan-Sarukhanyan guarantees the existence of one of order 120.

This can also be strengthened.

Theorem 2.5 (Craigen-Seberry-Zhang [14]). *Suppose that there are Hadamard matrices of orders $4a, 4b, 4c, 4d$. Then there is an Hadamard matrix of order $16abcd$.*

So, for example, we can get an Hadamard matrix of order $16 \cdot 15 \cdot 15$ from this theorem.

3 THE STRONGEST HADAMARD CONSTRUCTION THEOREMS

For easy reference, we will now give the strongest construction theorems for Hadamard matrices. These theorems do not give all the known orders but give

the vast majority of those known. We leave the proofs until our later book as well as details of when these conditions can be satisfied.

Theorem 3.1 (Paley [66]). *Let $p \equiv 3 \pmod 4$ be a prime power. Then there is an Hadamard matrix of order $p+1$.*

Theorem 3.2 (Paley [66]). *Let $p \equiv 1 \pmod 4$ be a prime power. Then there is an Hadamard matrix of order $2(p+1)$.*

Theorem 3.3 (Goethals-Seidel [25]). *Suppose that there is an Hadamard matrix of order h. Then there is a regular symmetric Hadamard matrix with constant diagonal of order h^2.*

Since Hadamard matrices are of order $h \equiv 0 \pmod 4$ and Hadamard's inequality studies matrices on the unit disc, it is natural to consider matrices with complex entries.

Definition 3.1. A matrix C of order $2n$ with elements ± 1, $\pm i$ that satisfies $CC^* = 2nI$ will be called a *complex Hadamard matrix*.

The strongest theorem using complex Hadamard matrices is the following "multiplication theorem":

Theorem 3.4 (Turyn [104]). *Suppose that there is a complex Hadamard matrix of order $2n$ and an Hadamard matrix of order $4h$. Then there is an Hadamard matrix of order $8hn$.*

This means that the complex Hadamard conjecture is intricately woven with the Hadamard conjecture.

Definition 3.2. X and Y are said to be *amicable matrices* if

$$XY^T = YX^T. \tag{1}$$

Now we look more precisely at definitions of matrices to "plug in."

Definition 3.3. Four circulant symmetric ± 1 matrices A,B,C,D of order w that satisfy

$$AA^T + BB^T + CC^T + DD^T = 4wI_w$$

will be called *Williamson matrices*. Four ± 1 matrices A,B,C,D of order w that satisfy both

$$XY^T = YX^T \qquad \text{for} \quad X,Y \in \{A,B,C,D\}$$

(that is, A, B, C, D are pairwise amicable), and

$$AA^T + BB^T + CC^T + DD^T = 4wI_w, \tag{2}$$

will be called *Williamson-type matrices.*

Analogously, eight circulant ± 1 matrices $A_1, A_2, \ldots, A_8$ of order w which are symmetric and which satisfy

$$\sum_{i=1}^{8} A_i A_i^T = 8wI_w$$

will be called *8-Williamson matrices.* Eight ± 1 amicable matrices $A_1, A_2, \ldots, A_8$ of order w which satisfy both

$$\sum_{i=1}^{8} A_i A_i^T = 8wI_w \qquad \text{and} \qquad A_j A_i^T = A_i A_j^T, \quad i, j = 1, \ldots, 8,$$

will be called *8-Williamson-type matrices.*

The most common structure matrices are "plugged into" is the orthogonal design, defined as follows:

Definition 3.4. An *orthogonal design of order n and type* $(s_1, \ldots, s_u)$, s_i positive integers, is an $n \times n$ matrix X, with entries $\{0, \pm x_1, \ldots, \pm x_u\}$ (the x_i commuting indeterminates) satisfying

$$XX^T = \left(\sum_{i=1}^{u} s_i x_i^2 \right) I_n. \tag{3}$$

We write this as $\mathrm{OD}(n; s_1, s_2, \ldots, s_u)$.

Alternatively, each row of X has s_i entries of the type $\pm x_i$, and the distinct rows are orthogonal under the euclidean inner product. We may view X as a matrix with entries in the field of fractions of the integral domain $Z[x_1, \ldots, x_u]$ (Z the rational integers), and if we let $f = (\Sigma_{i=1}^{u} s_i x_i^2)$, then X is an invertible matrix with inverse $(1/f)X^T$. Thus, $XX^T = fI_n$, and so our alternative definition that the row vectors are orthogonal applies equally well to the column vectors of X.

An orthogonal design with no zeros and in which each of the entries is replaced by $+1$ or -1 is an Hadamard matrix. A special orthogonal design, the $\mathrm{OD}(4t; t, t, t, t)$, is especially useful in the construction of Hadamard matrices. An $\mathrm{OD}(12; 3, 3, 3, 3)$ was first found by L. Baumert and M. Hall, Jr. [6], and an $\mathrm{OD}(20; 5, 5, 5, 5)$ by Welch (see below). $\mathrm{OD}(4t; t, t, t, t)$ are sometimes called *Baumert-Hall arrays.*

Another set of matrices of a very different kind can be obtained by partitioning a matrix as follows: Let M be a matrix of order tm. Then M can be expressed as a t^2 block M-structure when M is an orthogonal matrix:

$$M = \begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1t} \\ M_{21} & M_{22} & \cdots & M_{2t} \\ \vdots & & & \vdots \\ M_{t1} & M_{t2} & \cdots & M_{tt} \end{bmatrix},$$

where M_{ij} is of order m $(i, j = 1,2,\ldots,t)$.

Some orthogonal designs of special interest are the following:

1. The Williamson array—the OD(4;1,1,1,1):

$$\begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$ the right representation of the quaternions;

$$\begin{bmatrix} A & B & C & D \\ -B & A & D & -C \\ -C & -D & A & B \\ -D & C & -B & A \end{bmatrix}$$ the left representation of the quaternions.

2. The OD(8;1,1,1,1,1,1,1,1):

$$\left[\begin{array}{cccc|cccc} A & B & C & D & E & F & G & H \\ -B & A & D & -C & F & -E & -H & G \\ -C & -D & A & B & G & H & -E & -F \\ -D & C & -B & A & H & -G & F & -E \\ \hline -E & -F & -G & -H & A & B & C & D \\ -F & E & -H & G & -B & A & -D & C \\ -G & H & E & -F & -C & D & A & -B \\ -H & -G & F & E & -D & -C & B & A \end{array}\right].$$

3. The Baumert-Hall array—the OD(12;3,3,3,3):

$$A(x,y,z,w) =$$

$$\begin{bmatrix}
y & x & x & x & -z & z & w & y & -w & w & z & -y \\
-x & y & x & -x & w & -w & z & -y & -z & z & -w & -y \\
-x & -x & y & x & w & -y & -y & w & z & z & w & -z \\
-x & x & -x & y & -w & -w & -z & w & -z & -y & -y & -z \\
-y & -y & -z & -w & z & x & x & x & -w & -w & z & -y \\
-w & -w & -z & y & -x & z & x & -x & y & y & -z & -w \\
w & -w & w & -y & -x & -x & z & x & y & -z & -y & -z \\
-w & -z & w & -z & -x & x & -x & z & -y & y & -y & w \\
-y & y & -z & -w & -z & -z & w & y & w & x & x & x \\
z & -z & -y & -w & -y & -y & -w & -z & -x & w & x & -x \\
-z & -z & y & z & -y & -w & y & -w & -x & -x & w & x \\
z & -w & -w & z & y & -y & y & z & -x & x & -x & w
\end{bmatrix};$$

or alternatively (using the Cooper-J.Wallis theorem [12]), the OD(12;3, 3,3,3) is

$$\left[\begin{array}{ccc|ccc|ccc|ccc}
a & b & c & -b & a & d & -c & -d & a & -d & c & -b \\
c & a & b & a & d & -b & -d & a & -c & c & -b & -d \\
b & c & a & d & -b & a & a & -c & -d & -b & -d & c \\
\hline
b & -a & -d & a & b & c & -d & -b & c & c & -a & d \\
-a & -d & b & c & a & b & -b & c & -d & -a & d & c \\
-d & b & -a & b & c & a & c & -d & -b & d & c & -a \\
\hline
c & d & -a & d & b & -c & a & b & c & -b & d & a \\
d & -a & c & b & -c & d & c & a & b & d & a & -b \\
-a & c & d & -c & d & b & b & c & a & a & -b & d \\
\hline
d & -c & b & -c & a & -d & b & -d & -a & a & b & c \\
-c & b & d & a & -d & -c & -d & -a & b & c & a & b \\
b & d & -c & -d & -c & a & -a & b & -d & b & c & a
\end{array}\right]$$

4. The Plotkin array—the OD(24;3,3,3,3,3,3,3,3):

Let $A(x,y,z,w)$ be as in array 3, and let

$$B = (x,y,z,w)$$

$$= \begin{bmatrix}
y & x & x & x & -w & w & z & y & -z & z & w & -y \\
-x & y & x & -x & -z & z & -w & -y & w & -w & z & -y \\
-x & -x & y & x & -y & -w & y & -w & -z & -z & w & z \\
-x & x & -x & y & w & w & -z & -w & -y & z & y & z \\
-w & -w & -z & -y & z & x & x & x & -y & -y & z & -w \\
y & y & -z & -w & -x & z & x & -x & -w & -w & -z & y \\
-w & w & -w & -y & -x & -x & z & x & z & y & y & z \\
z & -w & -w & z & -x & x & -x & z & y & -y & y & w \\
z & -z & y & -w & y & y & w & -z & w & x & x & x \\
y & -y & -z & -w & -z & -z & -w & -y & -x & w & x & -x \\
z & z & y & -z & w & -y & -y & w & -x & -x & w & x \\
-w & -z & w & -z & -y & y & -y & z & -x & x & -x & w
\end{bmatrix},$$

then $\begin{bmatrix} A(x_1,x_2,x_3,x_4) & B(x_5,x_6,x_7,x_8) \\ B(-x_5,x_6,x_7,x_8) & -A(-x_1,x_2,x_3,x_4) \end{bmatrix}$ is the required design.

5. The Welch array—the OD(20;5,5,5,5) constructed from 16-block circulant matrices is an M-structure:

$-D\ B\ -C\ -C\ -B$	$C\ A\ -D\ -D\ -A$	$-B\ -A\ C\ -C\ -A$	$A\ -B\ -D\ D\ -B$
$-B\ -D\ B\ -C\ -C$	$-A\ C\ A\ -D\ -D$	$-A\ -B\ -A\ C\ -C$	$-B\ A\ -B\ -D\ D$
$-C\ -B\ -D\ B\ -C$	$-D\ -A\ C\ A\ -D$	$-C\ -A\ -B\ -A\ C$	$D\ -B\ A\ -B\ -D$
$-C\ -C\ -B\ -D\ B$	$-D\ -D\ -A\ C\ A$	$C\ -C\ -A\ -B\ -A$	$-D\ D\ -B\ A\ -B$
$B\ -C\ -C\ -B\ -D$	$A\ -D\ -D\ -A\ C$	$-A\ C\ -C\ -A\ -B$	$-B\ -D\ D\ -B\ A$
$-C\ A\ D\ D\ -A$	$-D\ -B\ -C\ -C\ B$	$-A\ B\ -D\ D\ B$	$-B\ -A\ -C\ C\ -A$
$-A\ -C\ A\ D\ D$	$B\ -D\ -B\ -C\ -C$	$B\ -A\ B\ -D\ D$	$-A\ -B\ -A\ -C\ C$
$D\ -A\ -C\ A\ D$	$-C\ B\ -D\ -B\ -C$	$D\ B\ -A\ B\ -D$	$C\ -A\ -B\ -A\ -C$
$D\ D\ -A\ -C\ A$	$-C\ -C\ B\ -D\ -B$	$-D\ D\ B\ -A\ B$	$-C\ C\ -A\ -B\ -A$
$A\ D\ D\ -A\ -C$	$-B\ -C\ -C\ B\ -D$	$B\ -D\ D\ B\ -A$	$-A\ -C\ C\ -A\ -B$
$B\ -A\ -C\ C\ -A$	$A\ B\ -D\ D\ B$	$-D\ -B\ C\ C\ B$	$-C\ A\ -D\ -D\ -A$
$-A\ B\ -A\ -C\ C$	$B\ A\ B\ -D\ D$	$B\ -D\ -B\ C\ C$	$-A\ -C\ A\ -D\ -D$
$C\ -A\ B\ -A\ -C$	$D\ B\ A\ B\ -D$	$C\ B\ -D\ -B\ C$	$-D\ -A\ -C\ A\ -D$
$-C\ C\ -A\ B\ -A$	$-D\ D\ B\ A\ B$	$C\ C\ B\ -D\ -B$	$-D\ -D\ -A\ -C\ A$
$-A\ -C\ C\ -A\ B$	$B\ -D\ D\ B\ A$	$-B\ C\ C\ B\ -D$	$A\ -D\ -D\ -A\ -C$
$-A\ -B\ -D\ D\ -B$	$B\ -A\ C\ -C\ -A$	$C\ A\ D\ D\ -A$	$-D\ B\ C\ C\ -B$
$-B\ -A\ -B\ -D\ D$	$-A\ B\ -A\ C\ -C$	$-A\ C\ A\ D\ D$	$-B\ -D\ B\ C\ C$
$D\ -B\ -A\ -B\ -D$	$-C\ -A\ B\ -A\ C$	$D\ -A\ C\ A\ D$	$C\ -B\ -D\ B\ C$
$-D\ D\ -B\ -A\ -B$	$C\ -C\ -A\ B\ -A$	$D\ D\ -A\ C\ A$	$C\ C\ -B\ -D\ B$
$-B\ -D\ D\ -B\ -A$	$-A\ C\ -C\ -A\ B$	$A\ D\ D\ -A\ C$	$B\ C\ C\ -B\ -D$

6. The Ono-Sawade-Yamamoto array—the OD(36;9,9,9,9) constructed from 16 type one matrices is an M-structure and is given on the facing page.

a	a	a	b	c	d	-b	-d	-c	b	-a	a	b	c	-d	b	d	-c	c	-a	a	-b	c	d	b	-d	c	d	-a	a	b	-c	d	-b	d	c
a	a	a	d	b	c	-c	-b	-d	a	b	-a	-d	b	c	-c	b	d	a	c	-a	d	-b	c	c	b	-d	a	d	-a	d	b	-c	c	-b	d
a	a	a	c	d	b	-d	-c	-b	-a	a	b	c	-d	b	d	-c	b	-a	a	c	c	d	-b	-d	c	b	-a	a	d	-c	d	b	d	c	-b
-b	-d	-c	a	a	a	b	c	d	b	d	-c	b	-a	a	b	c	-d	b	-d	c	c	-a	a	-b	c	d	-b	d	c	d	-a	a	b	-c	d
-c	-b	-d	a	a	a	d	b	c	-c	b	d	a	b	-a	-d	b	c	c	b	-d	a	c	-a	d	-b	c	c	-b	d	a	d	-a	d	b	-c
-d	-c	-b	a	a	a	c	d	b	d	-c	b	-a	a	b	c	-d	b	-d	c	b	-a	a	c	c	d	-b	d	c	-b	-a	a	d	-c	d	b
b	c	d	-b	-d	-c	a	a	a	b	c	-d	b	d	-c	b	-a	a	-b	c	d	b	-d	c	c	-a	a	b	-c	d	-b	d	c	d	-a	a
d	b	c	-c	-b	-d	a	a	a	-d	b	c	-c	b	d	a	b	-a	d	-b	c	c	b	-d	a	c	-a	d	b	-c	c	-b	d	a	d	-a
c	d	b	-d	-c	-b	a	a	a	c	-d	b	d	-c	b	-a	a	b	c	d	-b	-d	c	b	-a	a	c	-c	d	b	d	c	-b	-a	a	d
-b	a	-a	-b	c	-d	-b	d	-c	a	a	a	b	-c	-d	-b	d	c	-d	-a	a	b	c	-d	-b	-d	-c	c	a	-a	b	c	d	-b	-d	c
-a	-b	a	-d	-b	c	-c	-b	d	a	a	a	-d	b	-c	c	-b	d	a	-d	-a	-d	b	c	-c	-b	-d	-a	c	a	d	b	c	c	-b	-d
a	-a	-b	c	-d	-b	d	-c	-b	a	a	a	-c	-d	b	d	c	-b	-a	a	-d	c	-d	b	-d	-c	-b		-a	c	c	d	b	-d	c	-b
-b	d	-c	-b	a	-a	-b	c	-d	-b	d	c	a	a	a	b	-c	-d	-b	-d	-c	-d	-a	a	b	c	-d	-b	-d	c	c	a	-a	b	c	d
-c	-b	d	-a	-b	a	-d	-b	c	c	-b	d	a	a	a	-d	b	-c	-c	-b	-d	a	-d	-a	-d	b	c	c	-b	-d	-a	c	a	d	b	c
d	-c	-b	a	-a	-b	c	-d	-b	d	c	-b	a	a	a	-c	-d	b	-d	-c	-b	-a	a	-d	c	-d	b	-d	c	-b	a	-a	c	c	d	b
-b	c	-d	-b	d	-c	-b	a	-a	b	-c	-d	-b	d	c	a	a	a	b	c	-d	-b	-d	-c	-d	-a	a	b	c	d	-b	-d	c	c	a	-a
-d	-b	c	-c	-b	d	-a	-b	a	-d	b	-c	c	-b	d	a	a	a	-d	b	c	-c	-b	-d	a	-d	-a	d	b	c	c	-b	-d	-a	c	a
c	-d	-b	d	-c	-b	a	-a	-b	-c	-d	b	d	c	-b	a	a	a	c	-d	b	-d	-c	-b	-a	a	-d	c	d	b	-d	c	-b	a	-a	c
-c	a	-a	-b	-c	d	b	-d	-c	d	a	-a	b	c	d	-b	d	-c	a	a	a	-b	c	-d	b	d	-c	-b	-a	a	-b	c	d	-b	-d	-c
-a	-c	a	d	-b	-c	-c	b	-d	-a	d	a	d	b	c	-c	-b	d	a	a	a	-d	-b	c	-c	b	d	a	-b	-a	d	-b	c	-c	-b	-d
a	-a	-c	-c	d	-b	-d	-c	b	a	-a	d	c	d	b	d	-c	-b	a	a	a	c	-d	-b	d	-c	b	-a	a	-b	c	d	-b	-d	-c	-b
b	-d	-c	-c	a	-a	-b	-c	d	-b	d	-c	d	a	-a	b	c	d	b	d	-c	a	a	a	-b	c	-d	-b	-d	-c	-b	-a	a	-b	c	d
-c	b	-d	-a	-c	a	d	-b	-c	-c	-b	d	-a	d	a	d	b	c	-c	b	d	a	a	a	-d	-b	c	-c	-b	-d	a	-b	-a	d	-b	c
-d	-c	b	a	-a	-c	-c	d	-b	d	-c	-b	a	-a	d	c	d	b	d	-c	b	a	a	a	c	-d	-b	-d	-c	-b	-a	a	-b	c	d	-b
-b	-c	d	b	-d	-c	-c	a	-a	b	c	d	-b	d	-c	d	a	-a	-b	c	-d	b	d	-c	a	a	a	-b	c	d	-b	-d	-c	-b	-a	a
d	-b	-c	-c	b	-d	-a	-c	a	d	b	c	-c	-b	d	-a	d	a	-d	-b	c	-c	b	d	a	a	a	d	-b	c	-c	-b	-d	a	-b	-a
-c	d	-b	-d	-c	b	a	-a	-c	c	d	b	d	-c	-b	a	-a	d	c	-d	-b	d	-c	b	a	a	a	c	d	-b	-d	-c	-b	-a	a	-b
-d	a	-a	b	-c	-d	-b	-d	c	-c	-a	a	b	-c	d	-b	-d	-c	b	a	-a	b	c	d	b	-d	-c	a	a	a	-b	-c	d	b	-d	c
-a	-d	a	-d	b	-c	c	-b	-d	a	-c	-a	d	b	-c	-c	-b	-d	-a	b	a	d	b	c	-c	b	-d	a	a	a	d	-b	-c	c	b	-d
a	-a	-d	-c	-d	b	-d	c	-b	-a	a	-c	-c	d	b	-d	-c	-b	a	-a	b	c	d	b	-d	-c	b	a	a	a	-c	d	-b	-d	c	b
-b	-d	c	-d	a	-a	b	-c	-d	-b	-d	-c	-c	-a	a	b	-c	d	b	-d	-c	b	a	-a	b	c	d	b	-d	c	a	a	a	-b	-c	d
c	-b	-d	-a	-d	a	-d	b	-c	-c	-b	-d	a	-c	-a	d	b	-c	-c	b	-d	-a	b	a	d	b	c	c	b	-d	a	a	a	d	-b	-c
-d	c	-b	a	-a	-d	-c	-d	b	-d	-c	-b	-a	a	-c	-c	d	b	-d	c	b	a	-a	b	c	d	b	-d	c	b	a	a	a	-c	d	-b
b	-c	-d	-b	-d	c	-d	a	-a	b	-c	d	-b	-d	-c	-c	-a	a	b	c	d	b	-d	-c	b	a	-a	-b	-c	d	b	-d	c	a	a	a
-d	b	-c	c	-b	-d	-a	-d	a	d	b	-c	-c	-b	-d	a	-c	-a	d	b	c	-c	b	-d	-a	b	a	d	-b	-c	c	b	-d	a	a	a
-c	-d	b	-d	c	-b	a	-a	-d	-c	d	b	-d	-c	-b	-a	a	-c	c	d	b	-d	-c	b	a	-a	b	-c	d	-b	-d	c	b	a	a	a

7. The Goethals-Seidel array [27] (see also J. Wallis-Whiteman [113]):

$$\begin{bmatrix} A & BR & CR & DR \\ -BR & A & -D^TR & C^TR \\ -CR & D^TR & A & -B^TR \\ -DR & -C^TR & B^TR & A \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} A & BR & CR & DR \\ -BR & A & D^TR & -C^TR \\ -CR & -D^TR & A & B^TR \\ -DR & C^TR & -B^TR & A \end{bmatrix},$$

where A,B,C,D are circulant (type one) matrices satisfying (2) and R is the back diagonal (equivalent type two) (0,1) matrix.

Definition 3.5. *Suitable matrices* of order w for an OD$(n;s_1,s_2,\ldots,s_u)$ are u pairwise amicable (i.e., pairwise satisfy (1)) matrices, A_i, $i = 1,\ldots,u$, that have entries $+1$ or -1 and that satisfy

$$\sum_{i=1}^{u} s_i A_i A_i^T = (\Sigma s_i) w I_w. \tag{4}$$

They are used in the following theorem:

Theorem 3.5 (Geramita-Seberry). *Suppose that there exists an* OD$(\Sigma s_i;s_1,\ldots,s_u)$ *and* u *suitable matrices of order* m. *Then there is an Hadamard matrix of order* $(\Sigma s_i)m$.

If we generalize the definition of suitable matrices so that entries $0,+1,-1$ are allowed, then *weighing matrices* rather than Hadamard matrices could be constructed.

An overview of matrices to "plug in" and "plug into" is given in Table 3.1.

The most prolific method for constructing matrices to "plug into" uses T-matrices or T-sequences:

Definition 3.6 (T-matrices). A set of 4 *T-matrices*, T_i, $i = 1,\ldots,4$ of order t are four circulant or type one matrices that have entries 0, $+1$ or -1 and that satisfy

1. $T_i * T_j = 0$, $i \neq j$ ($*$ denotes the Hadamard product);
2. $\sum_{i=1}^{4} T_i$ is a $(1,-1)$ matrix;
3. $\sum_{i=1}^{4} T_i T_i^T = tI_t$; and for r/v
4. $t = t_1^2 + t_2^2 + t_3^2 + t_4^2$, where t_i is the row [column] sum of T_i.

(5)

T-matrices are known (see Cohen, Rubie, Koukouvinos, Kounias, Seberry, Yamada [10] for a recent survey) (71 occurs in [58]) for many orders including the following:

TABLE 3.1 The Relationship Between Matrices to "Plug in" and Matrices to "Plug into"

	Matrices to "Plug in"	Matrices to "Plug into"
Hardest to find	Williamson Williamson-type	OD(4t;t,t,t,t)
	8-Williamson 8-Williamson-type	OD(8t;t,t,t,t,t,t,t,t)
Easiest to find	Suitable matrices	OD($2^t n$;$u_1,u_2,\ldots,u_3$)
	4 circulant suitable matrices	Goethals-Seidel
	4 type one suitable matrices	J. Wallis-Whiteman
	Near suitable	"Bordered arrays"
	Regular s-sets M-structures Kharaghani matrices	Latin squares

1,...,72,74,...,78,80,...,82,84,...,88,90,...,96,98,...,102,104,...,106,108,110, ...,112,114,...,126,128,...,130,132,...,136,138,140,...,148,150,152,...,156, 158,...,162,164,...,166,168,...,172,174,...,178,180,182,184,...,190,192,194, ...,196, 198, 200,...,210,.... T-matrices of order t give Hadamard matrices of order $4t$.

Definition 3.7 (T-sequences). A set of four sequences $A = \{\{a_{11},\ldots,a_{1n}\}, \{a_{21},\ldots,a_{2n}\},\{a_{31},\ldots,a_{3n}\},\{a_{41},\ldots,a_{4n}\}\}$ of length n, with entries $0,1,-1$ so that exactly one of $\{a_{1j},a_{2j},a_{3j},a_{4j}\}$ is ± 1 (three are zero) for $j = 1,\ldots,n$ and with zero nonperiodic autocorrelation function, that is, $N_A(j) = 0$ for $j = 1,\ldots,n-1$, where

$$N_A(j) = \sum_{i=1}^{n-j}(a_{1i},a_{1,i+j} + a_{2i}a_{2,i+j} + a_{3i}a_{3,i+j} + a_{4i}a_{4,i+j}),$$

are called *T-sequences*.

T-matrices are a slightly weaker structure than T-sequences, being defined on finite abelian groups rather than the infinite cyclic group. They are known for a few important small orders, for example, 61 and 67 [36, 75] for which no T-sequences are yet known. Sequences are discussed extensively in Section 5. They are also known for even orders t for which no T-sequences of length t are known [53].

The following result, in a slightly different form, was also discovered by R. J. Turyn. It is the single, most useful method for constructing OD($4n;n,n,n,n$), that is, matrices to "plug into."

Theorem 3.6 (Cooper–J. Wallis [12]). *Suppose there exist circulant T-matrices (T-sequences)* $X_i, i = 1,\ldots,4$, *of order* n. *Let* a,b,c,d *be commuting variables. Then*

$$A = aX_1 + bX_2 + cX_3 + dX_4,$$
$$B = -bX_1 + aX_2 + dX_3 - cX_4,$$
$$C = -cX_1 - dX_2 + aX_3 + bX_4,$$
$$D = -dX_1 + cX_2 - bX_3 + aX_4,$$

can be used in the Goethal-Seidel (or J. Wallis-Whiteman) array to obtain an OD$(4n;n,n,n,n)$ *and an Hadamard matrix of order* $4n$.

Corollary 3.7. *If there are T-matrices of order* t, *then there is an* OD$(4t;t,t,t,t)$.

The results on T-matrices and T-sequences as applied to Hadamard matrices are given in Section 5.

The appropriate theorem for the construction of Hadamard matrices (it is implied by Williamson, Baumert-Hall, Welch, Cooper–J. Wallis, Turyn) is

Theorem 3.8. *Suppose that there exists an* OD$(4t;t,t,t,t)$ *and four suitable matrices* A,B,C,D *of order* w *that satisfy*

$$AA^T + BB^T + CC^T + DD^T = 4wI_w.$$

Then there is an Hadamard matrix of order $4wt$.

Williamson matrices (which are discussed further in a later section) are suitable matrices for OD$(4t;t,t,t,t)$, and as such, Williamson matrices are plugged into the OD.

Corollary 3.9. *If there are circulant T-matrices of order* t *and there are Williamson matrices of order* w, *there is an Hadamard matrix of order* $4tw$. *Alternatively, if there are an* OD$(4t;t,t,t,t)$ *and Williamson matrices of order* w, *there is an Hadamard matrix of order* $4tw$.

We modify a construction of Turyn to obtain the first theorem which capitalized on M-structures. The OD$(4s;u_1,\ldots,u_n)$ of the next theorem is an M-structure of which the Welch and Ono-Sawade-Yamamoto arrays are powerful examples.

Theorem 3.10 (Seberry-Yamada-Turyn [87, 108]). *Suppose that there are T-matrices of order* t. *Further suppose that there is an* OD$(4s;u_1,\ldots,u_n)$ *constructed of* 16 *circulant (or type one)* $s \times s$ *blocks on the variables* $x_1,\ldots,x_n$.

Then there is an OD$(4st;tu_1,\ldots,tu_n)$. *In particular, if there is an* OD$(4s;s,s,s,s)$ *constructed of* 16 *circulant (or type one)* $s \times s$ *blocks, then there is an* OD$(4st;st,st,st,st)$.

Proof. We write the OD as (N_{ij}), $i,j = 1,2,3,4$, where each N_{ij} is circulant (or type one). Hence, we are considering the OD purely as an M-structure. Since we have an OD,

$$N_{i1}N_{j1}^T + N_{i2}N_{j2}^T + N_{i3}N_{j3}^T + N_{i4}N_{j4}^T = \begin{cases} \sum_{k=1}^4 u_k x_k^2 I_s, & i = j; \\ 0, & i \neq j. \end{cases}$$

Suppose that the T-matrices are T_1,T_2,T_3,T_4. Then form the matrices

$$A = T_1 \times N_{11} + T_2 \times N_{21} + T_3 \times N_{31} + T_4 \times N_{41},$$
$$B = T_1 \times N_{12} + T_2 \times N_{22} + T_3 \times N_{32} + T_4 \times N_{42},$$
$$C = T_1 \times N_{13} + T_2 \times N_{23} + T_3 \times N_{33} + T_4 \times N_{43},$$
$$D = T_1 \times N_{14} + T_2 \times N_{24} + T_3 \times N_{34} + T_4 \times N_{44}.$$

Now

$$AA^T + BB^T + CC^T + DD^T = t\sum_{k=1}^4 u_k x_k^2 I_{st},$$

and since A,B,C,D are type one, they can be used in the J. Wallis-Whiteman generalization of the Goethals-Seidel array to obtain the result. □

Use the Welch and Ono-Sawade-Yamamoto arrays to see

Corollary 3.11. *Suppose that the T-matrices are of order* t. *Then there are orthogonal designs* OD$(20t;5t,5t,5t,5t)$ *and* OD$(36t;9t,9t,9t,9t)$.

Note that to prove the Hadamard conjecture "there is an Hadamard matrix of order $4t$ for all $t > 0$," it would be sufficient to prove:

Conjecture 3.12. *There exists an* OD$(4t;t,t,t,t)$ *for every positive integer* t.

The most encompassing theorem presently known, in that it gives a result for every odd q, is proved using a "plug in" technique:

Theorem 3.13 (Seberry [121]). *Let* q *be any odd natural number. Then there exists an integer* $t \leq [2\log_2(q-3)] + 1$ *so that there is an Hadamard matrix of order* $2^t q$. *(The best known bounds are* $t \leq [\log_2(q-3)(q-7) - 1]$ *for* q *(prime)* $\equiv 3 \pmod 4$ *and* $t \leq [\log_2(q-1)(q-5)] + 1$ *for* p *(prime)* $\equiv 1 \pmod 4$.*)*

The proof of this theorem allows a number of cases of interest and stronger results in some cases where q is not prime.

Corollary 3.14 (Seberry [121]). *Let q be any odd natural number. Then there exists a regular symmetric Hadamard matrix with constant diagonal of order $2^{2t}q^2$, $t \leq [2\log_2(q-3)] + 1$.*

Corollary 3.15 (Seberry, unpublished).

1. *Let p and $p+2$ be twin prime powers. Then there exists a $t \leq [\log_2(p+3)(p-1)(p^2+2p-7)] - 2$ so that there is an Hadamard matrix of order $2^t p(p+2)$.*
2. *Let $p+1$ be the order of a symmetric Hadamard matrix. Then there exists a $t \leq [\log_2(p-3)(p-7)] - 2$ so that there is an Hadamard matrix of order $2^t p$.*

Corollary 3.16 [81]. *Let pq be an odd natural number. Suppose that all $\mathrm{OD}(2^s p; 2^r a, 2^r b, 2^r c)$ exist, $s \geq s_0$, $2^{s-r}p = a+b+c$. Then there exists an Hadamard matrix of order $2^t \cdot p \cdot q$, $s \leq t \leq [2\log_2((q-3)/p)] + r + 1$. (The best-known bounds are $s \leq t \leq [\log_2((q-3)(q-7)/p)] - 1 + r$ for q (prime) $\equiv 3 \pmod 4$ and $st \leq [\log_2((q-1)(q-5)/p)] + r + 1$ for q (prime) $\equiv 1 \pmod 4$).)*

Example 3.1. Often we can find better results than indicated by Theorem 3.13. Let $q = 3 \cdot 491$. We know there is an Hadamard matrix of order 12. Now, using the proof of Theorem 3.13, rather than the enunciation, we can find an Hadamard matrix of order $2^{15} \cdot 491$. So there is an Hadamard matrix of order $2^{16} \cdot 3 \cdot 19$ using the multiplication theorem. On the other hand, the proof of the corollory gives an Hadamard matrix of order $2^{13} \cdot 3 \cdot 491$ using the $\mathrm{OD}(2^{12} \cdot 3; 22, 3, 2^{12} \cdot 3 - 25)$.

Other similar results are known. The Appendix gives an indication of the smallest t for each odd natural number q for which an Hadamard matrix is known. A list of the construction methods used is given in Section A.3 of the Appendix.

Theorem 3.13 changes ideas for evaluating construction methods: We consider a method to be more powerful if it lowers the power of two for the resultant odd number. Thus, Agayan's theorem, which gives Hadamard matrices of order $8mn$ from Hadamard matrices of order $4m$ and $4n$, is more powerful than that of Hadamard, which gives a matrix of order $16mn$.

We now see another way to lower the power in a multiplication method. First, we introduce some notation.

Let $M = (M_{ij})$ and $N = (N_{gh})$ be orthogonal matrices or t^2 block M-structures of orders tm and tn, respectively, where M_{ij} is of order m $(i,j = 1,2, \ldots,t)$ and N_{gh} is of order n $(g,h = 1,2,\ldots,t)$.

We now define the operation $\bigcirc$ as the following:

$$M \bigcirc N = \begin{bmatrix} L_{11} & L_{12} & \cdots & L_{1t} \\ L_{21} & L_{22} & \cdots & L_{2t} \\ \vdots & & & \vdots \\ L_{t1} & L_{t2} & \cdots & L_{tt} \end{bmatrix},$$

where L_{ij} is of order of mn, and

$$L_{ij} = M_{i1} \times N_{1j} + M_{i2} \times N_{2j} + \cdots + M_{it} \times N_{tj},$$

$i, j = 1,2,\ldots,t$. We call this the *strong Kronecker* multiplication of two matrices. We note that the strong Kronecker product preserves orthogonality but not necessarily with entries in a useful form (i.e. equal to $0, \pm 1$).

Theorem 3.17. *Let A be an* OD$(tm; p_1,\ldots,p_u)$ *with entries $x_1,\ldots,x_u$, and let B be an* OD$(tn; q_1,\ldots,q_s)$ *with entries $y_1,\ldots,y_s$, then*

$$(A \bigcirc B)(A \bigcirc B)^T = \left(\sum_{j=1}^{u} p_j x_j^2\right)\left(\sum_{j=1}^{s} q_j y_j^2\right) I_{tmn}.$$

($A \bigcirc B$ is not an orthogonal design but an orthogonal matrix.) If A is a $W(tm,p)$ and B is a weighing matrix $W(tn,q)$, then $A \bigcirc B = C$ satisfies $CC^T = pqI_{tmn}$.

Hereafter, let $H = H_{ij}$ and $N = (N_{ij})$ of order $4h$ and $4n$, respectively, be 16 block M-structures. So

$$H = \begin{bmatrix} H_{11} & H_{12} & H_{13} & H_{14} \\ H_{21} & H_{22} & H_{23} & H_{24} \\ H_{31} & H_{32} & H_{33} & H_{34} \\ H_{41} & H_{42} & H_{43} & H_{44} \end{bmatrix},$$

where

$$\sum_{j=1}^{4} H_{ij} H_{ij}^T = 4hI_h = \sum_{j=1}^{4} H_{ji} H_{ji}^T,$$

for $i = 1,2,3,4$, and

$$\sum_{j=1}^{4} H_{ij} H_{kj}^T = 0 = \sum_{j=1}^{4} H_{ji}^T H_{jk},$$

for $i \neq k$, $i,k = 1,2,3,4$, and similarly for N.

For ease of writing, we define $X_i = \frac{1}{2}(H_{i1} + H_{i2})$, $Y_i = \frac{1}{2}(H_{i1} - H_{i2})$, $Z_i = \frac{1}{2}(H_{i3} + H_{i4})$, and $W_i = \frac{1}{2}(H_{i3} - H_{i4})$, where $i = 1,2,3,4$. Then both $X_i \pm Y_i$ and $Z_i \pm W_i$ are $(1,-1)$ matrices with $X_i \wedge Y_i = 0$ and $Z_i \wedge W_i = 0$, where $\wedge$ is the Hadamard product.

Let

$$S = \begin{bmatrix} X_1 & -Y_1 & Z_1 & -W_1 \\ X_2 & -Y_2 & Z_2 & -W_2 \\ X_3 & -Y_3 & Z_3 & -W_3 \\ X_4 & -Y_4 & Z_4 & -W_4 \end{bmatrix}.$$

Obviously, S is a $(0,1,-1)$ matrix.

Write

$$R = \begin{bmatrix} Y_1 & X_1 & W_1 & Z_1 \\ Y_2 & X_2 & W_2 & Z_2 \\ Y_3 & X_3 & W_3 & Z_3 \\ Y_4 & X_4 & W_4 & Z_4 \end{bmatrix},$$

also a $(0,1,-1)$ matrix.

We note $S \pm R$ is a $(1,-1)$ matrix, $R \wedge S = 0$, and by the previous theorem,

$$SS^T = RR^T = 2hI_{4h}.$$

Lemma 3.18. *If there exists an Hadamard matrix of order $4h$, there exists an* OD$(4h; 2h, 2h)$.

Proof. Form S and R as above. Now $H = S + R$. Note that $HH^T = SS^T + RR^T + SR^T + RS^T = 4hI_{4h}$ and $SS^T = RR^T = 2hI_{4h}$. Hence, $SR^T + RS^T = 0$. Let x and y be commuting variables; then $E = xS + yR$ is the required orthogonal design. □

In fact, exploiting the strong Kronecker product, Seberry and Zhang show

Lemma 3.19. *If there exist Hadamard matrices of order $4h$ and $4n$, there exists a $W(4hn, 2hn)$. If there exists an Hadamard matrix of order $4h$, there exists a $W(4h, 2h)$ $(h > 1)$.*

Theorem 3.20. *Suppose that $4h$ and $4n$ are the orders of Hadamard matrices; then there exist two disjoint amicable $W(4hn, 2hn)$ whose sum and difference are $(1,-1)$ matrices. Suppose that there exists an Hadamard matrix of order $4h$; then there exists disjoint amicable $W(4h, 2h)$ whose sum and difference are $(1,-1)$ matrices.*

We now proceed to use the idea of *orthogonal pairs* or ± 1 matrices, S and P of order n, satisfying

1. $SS^T + PP^T = 2nI_n$,
2. $SP^T = PS^T = 0$,

first introduced by R. Craigen [13] who showed

Lemma 3.21 (Craigen). *If there exist Hadamard matrices of order* $4p$ *and* $4q$, *then there exist two* $(1,-1)$ *matrices,* S *and* P *of order* $4pq$, *satisfying*

1. $SS^T + PP^T = 8pqI_{4pq}$,
2. $SP^T = PS^T = 0$.

Proof. By Theorem 3.20, there exist two $W(4pq,2pq)$, X and Y, satisfying $X \wedge Y = 0$; $X \pm Y$ is a $(1,-1)$ matrix, and $XY^T = YX^T$. Let $S = X + Y, P = X - Y$. Then both S and P are $(1,-1)$ matrices of order $4pq$. Note that

$$SS^T + PP^T = 2(XX^T + YY^T) = 8pqI_{4pq}$$

and

$$SP^T = XX^T - YY^T = 0.$$

Similarly, $PS^T = 0$. So S and P are the required matrices. □

These results can be combined to give

Theorem 3.22 (Craigen-Seberry-Zhang [14]). *If there exist Hadamard matrices of order* $4m, 4n, 4p, 4q$, *then there exists an Hadamard matrix of order* $16mnpq$.

Proof. Let U,V be amicable $W(4mn,2mn)$ constructed in Theorem 3.20. By Lemma 3.21, there exist two $(1,-1)$ matrices S and P of order $4pq$ satisfying conditions 1 and 2 in Lemma 3.21.

Let $H = U \times S + V \times P$. Then H is a $(1,-1)$ matrix, and

$$HH^T = UU^T \times SS^T + VV^T \times PP^T = 2mnI_{4mn}(SS^T + PP^T)$$

$$= 2mnI_{4mn} \times 8pqI_{4pq} = 16mnpqI_{16mnpq}.$$

Thus H is the required Hadamard matrix. □

The theorem gives an improvement and extension for the result of Agayan [1] that if there exist Hadamard matrices of order $4m$ and $4n$, then there exists an Hadamard matrix of order $8mn$, since using Agayan's theorem repeatedly on four Hadamard matrices of order $4m, 4n, 4p, 4q$ gives an Hadamard matrix of order $32mnpq$.

$$\begin{bmatrix} x & y \\ y & -x \end{bmatrix} \qquad \begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix} \qquad \begin{bmatrix} a & b & b & d \\ -b & a & d & -b \\ -b & -d & a & b \\ -d & b & -b & a \end{bmatrix} \qquad \begin{bmatrix} a & 0 & -c & 0 \\ 0 & a & 0 & c \\ c & 0 & a & 0 \\ 0 & -c & 0 & a \end{bmatrix}$$

(a) (b) (c) (d)

OD(2;1,1); OD(4;1,1,1,1); OD(4;1,1,2); OD(4;1,1).

Figure 4.1. Orthogonal designs.

Other similar results exist.

4 ORTHOGONAL DESIGNS AND ASYMPTOTIC EXISTENCE

The primary result regarding the asymptotic existence of Hadamard matrices is the theorem of Seberry Wallis (Theorem 4.11 of this section). In this section we outline the proof of this theorem. We begin this section with a discussion of orthogonal designs. These are key ingredients in the proof of the main theorem.

4.1. Orthogonal Designs

An orthogonal design is a generalization of an Hadamard matrix (see Definition 3.8). First we collect a few preliminary results and give some examples.

Example 4.1. Some small orthogonal designs are shown in Figure 4.1. Notice that Figure 4.1(b) is the Williamson array.

The following lemma gives some properties of orthogonal designs.

Lemma 4.1. *Let D be an orthogonal design* $\mathrm{OD}(n; u_1, u_2, \ldots, u_t)$ *on the commuting variables* $x_1, x_2, \ldots, x_t$. *Then D can be written as*

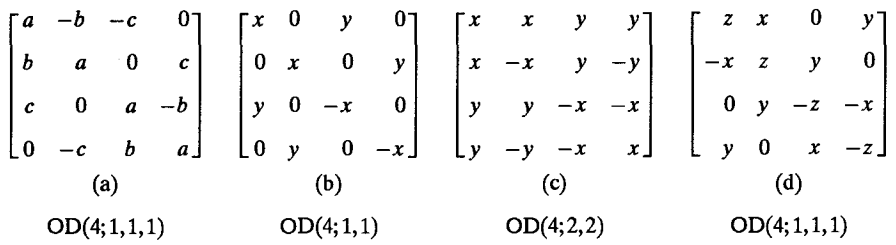
$$D = x_1A_1 + x_2A_2 + \cdots + x_tA_t,$$

where, for each $i, j \in \{1, \ldots, t\}$,

1. A_i *is an* $n \times n$ *matrix with entries* $0, \pm 1$;
2. $A_iA_i^T = u_iI_n$;
3. $A_iA_j^T + A_jA_i^T = 0$, $i \neq j$.

We need one further basic result:

Lemma 4.2. *Let D be an orthogonal design* $\mathrm{OD}(n; u_1, u_2, \ldots, u_t)$, *on the t commuting variables* $x_1, x_2, \ldots, x_t$. *Then the following orthogonal designs exist*:



(a) OD(4;1,1,1) (b) OD(4;1,1) (c) OD(4;2,2) (d) OD(4;1,1,1)

Figure 4.2. Orthogonal designs.

1. OD$(n;u_1,u_2,\ldots,u_i+u_j,\ldots,u_t)$ *on* $t-1$ *variables (i.e.,* u_i+u_j *replaces* u_i, u_j, $i\neq j$);
2. OD$(n;u_1,\ldots,u_{i-1},u_{i+1},\ldots,u_t)$ *on* $t-1$ *variables*;
3. OD$(2n;\ u_1,u_2,\ldots,u_t)$ *on* t *variables*;
4. OD$(2n;2u_1,2u_2,\ldots,2u_t)$ *on* t *variables*;
5. OD$(2n;u_1,u_1,u_2,\ldots,u_t)$ *on* $t+1$ *variables*;
6. OD$(2n;u_1,u_1,2u_2,\ldots,2u_t)$ *on* $t+1$ *variables*.

The techniques of this lemma are exhibited in the following example:

Example 4.2. Let D_1 and D_2 be the designs of Figure 4.2(b) and (a), respectively. Applying Lemma 4.2 to these designs gives examples as follows: D_1 is an OD(4;1,1,1,1); letting $b=c$ as in case 1 of Lemma 4.2 gives the OD(4;1, 1,2) design in Figure 4.2(c); letting $d=0$ as in case 2 gives the OD(4;1,1,1) design in Figure 4.2(a). D_2 is a (2;1,1) design; replacing variables by 2×2 matrices as in cases 3, 4, and 5 gives the designs OD(4;1,1), OD(4;2,2), OD(4;1,1,1), in Figure 4.2(b), (c), and (d), respectively.

Lemma 4.2 now lets us show

Lemma 4.3. *Suppose that for all choices of nonnegative integers* a,b,c *with* $a+b+c=n$, *an orthogonal design* OD$(n;a,b,c)$ *exists. Then for all choices of nonnegative integers* x,y,z *with* $x+y+z=2n$, *an orthogonal design* OD$(2n;x,y,z)$ *exists.*

Proof. Notice first that we make the convention that an OD$(n;a,b)$ may also be considered as an OD$(n;a,b,0)$, and so on.

Let x,y,z be nonnegative integers such that $x+y+z=2n$, and assume that $0\leq x\leq y\leq z$, so that $y\leq n$. Four cases arise:

1. Both x and y are even, so we may write $x=2a, y=2b$, and $a+b<n$. By hypothesis, an OD$(n;a,b,c)$ exists, where $c=n-a-b$. Hence, by case 6 of Lemma 4.2, an OD$(2n;a,a,2b,2c)$ exists and, by case 1, an OD$(2n;2a,2b,2c)$ also exists. This is the design we want.

2. Next, let x be even and y odd, so we may take $x = 2a, y = 2a + l$. Now $a + y = 3a + l$, and $z = 2n - 4a - l$. Since $y \leq z$, we have $3a + l \leq n$. Thus, an $\mathrm{OD}(n; y, a, n - a - y)$ exists, and as before, this means that an $\mathrm{OD}(2n; y, y, 2a, 2n - 2a - 2y)$ also exists. Setting $x_1 = x_4$, we get an $\mathrm{OD}(2n; y, 2a, 2n - 2a - y)$. Since $2a = x$ and $2n - 2a - y = z$, the last design is the required one.
3. If x is odd and y is even, we can take $x = 2a + 1, y = 2b$ and $z = 2t + 1$. Since $x + y + z = 2n$, we have $a + b + t + 1 = n$. Now, by assumption, $a < t$, so $x + b = 2a + b + 1 < n$. Hence, we have the following orthogonal designs: $\mathrm{OD}(n; x, b, n - x - b)$, $\mathrm{OD}(2n; x, x, 2b, 2n - 2x - 2b)$, and $\mathrm{OD}(2n; x, 2b, 2n - x - 2b)$. Since $y = 2b$ and $z = 2n - x - y$, we have the required design.
4. Finally, if x and y are both odd, we let $y = x + 2b$, where $b \geq 0$. Since $x + b \leq n$, we have orthogonal designs

$$\mathrm{OD}(n; x, b, n - x - b), \qquad \mathrm{OD}(2n; x, x, 2b, 2n - 2x - 2b),$$

and finally, $\mathrm{OD}(2n; x, x + 2b, 2n - 2x - 2b)$, as required. □

Corollary 4.4. *If x, y, z are nonnegative integers such that $x + y + z = 2^m$, then an orthogonal design $\mathrm{OD}(2^m; x, y, z)$ exists.*

Proof. From the the array in Figure 4.1(a) and Lemma 4.2, the statement is true for $m = 2$. It then follows from Lemma 4.3 for all $m > 2$. □

Corollary 4.5. *If x, y, are nonnegative integers such that $x + y = 2^m$, then an orthogonal design $\mathrm{OD}(2^m; x, y)$ exists.*

Proof. Apply case 1 of Lemma 4.2 to the $\mathrm{OD}(2^m; x, y, z)$ obtained from the previous corollary. □

4.2. An Existence Theorem for Hadamard Designs

We need one further result from number theory.

Theorem 4.6. *Let x and y be positive integers such that $(x, y) = 1$. Then every integer $N \geq (x - 1)(y - 1)$ can be written as a linear combination $N = ax + by$, where a and b are nonnegative integers.*

Corollary 4.7. *Let z be an odd integer. Then there exist nonnegative integers a and b such that*

$$a(z + 1) + b(z - 3) = n = 2^t$$

for some t.

Proof. If $z \geq 9$, let

$$d = (z+1, z-3) = \begin{cases} 2 & \text{if } z \equiv 1 \pmod 4, \\ 4 & \text{if } z \equiv 3 \pmod 4. \end{cases}$$

Let

$$N = \left(\frac{z+1}{d} - 1\right)\left(\frac{z-3}{d} - 1\right),$$

and choose m so that $2^{m-1} < N \leq 2^m$. By Theorem 4.6 there exist nonnegative integers a and b such that

$$\frac{a(z+1)}{d} + \frac{b(z-3)}{d} = 2^m,$$

and thus

$$a(z+1) + b(z-3) = 2^{m+s},$$

where

$$s = \begin{cases} 1 & \text{if } z \equiv 1 \pmod 4, \\ 2 & \text{if } z \equiv 3 \pmod 4, \end{cases}$$

and $t = m + s$. It is easy to verify that this result also holds for odd $3 \leq z \leq 9$. □

Lemma 4.8. *Let p be a prime, $p \geq 11$. Then there exists a positive integer t such that an Hadamard matrix of size $2^s p$ exists for every $s > t$.*

Proof. Let $x = p + 1$ and $y = p - 3$. By Corollary 4.7 there exist nonnegative integers a and b such that $ax + by = 2^t = n$ for some t. By Corollary 4.4 there exists an OD$(n; a, b, n-a-b)$ orthogonal design D on the variables x_1, x_2, x_3.

The proof now divides into two cases.

Case 1 $p \equiv 3 \pmod 4$. We replace each variable in D by a $p \times p$ $(1,-1)$ matrix: x_1 by J_p, x_2 by $J_p - 2I_p$, and x_3 by the back-circulant matrix N formed from the quadratic residues. This gives a $(1,-1)$ matrix E which is an Hadamard matrix of size $np = 2^t p$, and the Lemma follows for $p \equiv 3 \pmod 4$.

Case 2 $p \equiv 1 \pmod 4$. There exists an OD$(2n; 2a, 2b, n-a-b, n-a-b)$ orthogonal design F on the variables x_1, x_2, x_3, x_4 by identity 4 of Lemma 4.2. We replace each variable in F by a $p \times p$ $(1,-1)$ matrix: x_1 by J_p, x_2 by $J_p - 2I_p$, x_3, and x_4, respectively, by the circulant matrices $X = Q + I$ and $Y =$

$Q-I$ formed from the quadratic residue matrix Q. This gives an $np \times np$ $(1,-1)$ matrix G which is an Hadamard matrix of size $2np = 2^{t+1}p$, and the lemma also follows for $p \equiv 1 \pmod 4$.

This completes the proof for all primes, except 2, 3, 5, and 7. □

Lemma 4.9. *There exist Hadamard matrices of sizes 2^t for all $t \geq 1$, and $2^t p$ for all $t \geq 2$ and $p = 3,5,7$.*

Proof. There exists an Hadamard matrix of size 2^t for $t \geq 1$.

By Sylvester's multiplication theorem, if there exist Hadamard matrices of sizes 12, 20, and 28, then there exist Hadamard matrices of sizes $2^t p$ for all $t \geq 2$ and $p = 3,5,7$.

Hadamard matrices of these orders are obtained by the Paley construction. □

Theorem 4.10. *Let q be any positive integer. Then there exists $t = t(q)$ such that an Hadamard matrix of size $2^s q$ exists for every $s \geq t$.*

Proof. We apply Lemma 4.8 and/or Lemma 4.9 to each prime factor of q. Since a Kronecker product of Hadamard matrices is an Hadamard matrix, the result follows. □

Theorem 4.11 (Seberry Wallis [121]). *Let q be any positive integer, then there exists an Hadamard matrix of order $2^s q$ for every $s \geq [2\log_2(q-3)]$.*

Proof. By the proof of Corollary 4.7, we can choose t so that

$$2^t \geq \left(\frac{z+1}{d} - 1\right)\left(\frac{z-3}{d} - 1\right),$$

where z is an odd prime and $d = (z+1, z-3)$.

If $z \equiv 1 \pmod 4$, then $d = 2$ and we must have

$$2^t \geq \frac{(z-1)(z-5)}{4}.$$

Since

$$(z-3)^2 > (z-1)(z-5),$$

it is sufficient to ensure that

$$2^{t+2} > (z-3)^2;$$

that is,

$$t + 2 > 2\log_2(z-3).$$

Since t is an integer, we may choose

$$t = [2\log_2(z-3)] - 1.$$

Similarly, if $z \equiv 3 \pmod 4$, then $d = 4$, and we may choose

$$t = [2\log_2(z-5)] - 3.$$

As in the proof of Lemma 4.8, these choices of t ensure the existence of an Hadamard matrix of size $2^t z$.

If $z = pq$ where p and q are primes, $p \equiv 1 \pmod 4$, $q \equiv 1 \pmod 4$, then there exists an Hadamard matrix of size $2^r pq$, where

$$r = [2\log_2(p-3)] + [2\log_2(q-3)] < [2\log_2(pq-3)].$$

Analogously, if $z = \prod_i p_i$ for p_i prime and $p_i \equiv 1 \pmod 4$, then

$$r = \sum_i 2\log_2(p_i - 3) < 2\log_2\left(\prod_i (p_i - 3)\right)$$

Since an integer z that is a product of primes congruent to 1 (mod 4) gives the greatest lower bound on the value of t for which we know an Hadamard matrix of size $2^t z$ exists, we have proved the theorem. □

We note that better bounds (i.e., smaller r) can be obtained if not all primes in the decomposition of z are congruent to 1 (mod 4). We use the equivalence of Hadamard matrices and Hadamard designs to obtain the following corollary:

Corollary 4.12. *Let λ be any positive integer; then there exists an $s \geq 0$ so that an SBIBD$(2^{s+2}\lambda - 1, 2^{s+1}\lambda - 1, 2^s\lambda - 1)$ exists.*

In fact, as was indicated in Theorem 3.13, the value of s in Theorem 4.11 is slightly smaller if the proof is applied carefully.

4.3. Orthogonal Designs in Order 24

In this section, we discuss the particular case of orthogonal designs of order 24. In so doing, we demonstrate how the power of s in Theorem 4.11 can be reduced in specific cases.

The following is an OD(12;1,2,3,6) on the variables A,B,C,D:

$$\left[\begin{array}{ccc|ccc|ccc|ccc}
A & B & -B & C & B & B & C & -B & D & B & D & -C \\
-B & A & B & B & B & C & -B & D & C & D & -C & B \\
B & -B & A & B & C & B & D & C & -B & -C & B & D \\
\hline
-C & -B & -B & A & B & -B & -B & C & -D & C & D & -B \\
-B & -B & -C & -B & A & B & C & -D & -B & D & -B & C \\
-B & -C & -B & B & -B & A & -D & -B & C & -B & C & D \\
\hline
-C & B & -D & B & -C & D & A & B & -B & -C & -B & -B \\
B & -D & -C & -C & D & B & -B & A & B & -B & -B & -C \\
-D & -C & B & D & B & -C & B & -B & A & -B & -C & -B \\
\hline
-B & -D & C & -C & -D & B & C & B & B & A & B & -B \\
-D & C & -B & -D & B & -C & B & B & C & -B & A & B \\
C & -B & -D & B & -C & -D & B & C & B & B & -B & A
\end{array}\right]$$

Hence, there exists (equating variables) an OD(12;4,8).

Now, by identity 6 of Lemma 4.2, there are OD(24;2,4,3,3,12), OD(24;4,4,16), OD(24;8,8,8), and OD(24;1,1,4,6,12), giving

$$\begin{aligned}
&\mathrm{OD}(24;2,4,18);\\
&\mathrm{OD}(24;3,a,21-a), \qquad a = 3,4,5,6,7;\\
&\mathrm{OD}(24;4,a,20-a), \qquad a = 4,5,6,7,8;\\
&\mathrm{OD}(24;8,8,8).
\end{aligned}$$

Robinson [72] has found OD(24;1,1,1,1,1,5,5,9) and OD(24;1,1,1,1,1,2,8,9) from which, by equating variables, all other OD(24;$x,y,24-x-y$) may be obtained.

Consider the following matrices, M_1 and M_2: (we use the convention that $\overline{x} = -x$):

$$M_1 = \begin{array}{c|c|c|c|c|c}
e & d\bar{h}f\bar{g} & gfhh & f\bar{g}\bar{h}h & \bar{g}\overline{fhh} & gfhh \\
\hline
\bar{d}h\bar{f}\bar{g} & \bar{e} & fghh & \bar{g}fh\bar{h} & \bar{g}fh\bar{h} & g\overline{fh}h \\
\hline
\bar{g}\bar{f}hh & \bar{f}\bar{g}\bar{h}h & g & dhef & \bar{h}hgg & hh\bar{f}f \\
\hline
\bar{f}ghh & g\overline{fhh} & \overline{d\bar{h}\bar{e}f} & \bar{g} & h\bar{h}ff & hhg\bar{g} \\
\hline
gfh\bar{h} & g\overline{fhh} & h\bar{h}\bar{g}g & \bar{h}h\bar{f}f & f & dhge \\
\hline
\bar{g}\bar{f}hh & \bar{g}fhh & \overline{hhff} & \overline{hh\bar{g}\bar{g}} & \overline{d\bar{h}\bar{g}e} & \bar{f}
\end{array}$$

$$M_2 = \begin{array}{|c|c|c|c|c|c|}
\hline
e & d\bar{f}h\bar{f} & hhgg & h\bar{h}\bar{g}g & \bar{h}\bar{g}\bar{h}\bar{g} & hghg \\
\hline
\bar{d}f\bar{h}f & \bar{e} & hhgg & \bar{h}hg\bar{g} & h\bar{g}\bar{h}g & h\bar{g}\bar{h}g \\
\hline
\bar{h}\bar{h}\bar{g}g & \bar{h}\bar{h}\bar{g}g & g & dgeh & \bar{g}ghh & hh\bar{f}f \\
\hline
\bar{h}hgg & h\bar{h}\bar{g}\bar{g} & \bar{d}\bar{g}eh & \bar{g} & h\bar{h}ff & gghh \\
\hline
hgh\bar{g} & \bar{h}ghg & g\bar{g}\bar{h}h & \bar{h}h\bar{f}f & g & dghe \\
\hline
\bar{h}\bar{g}\bar{h}g & \bar{h}ghg & \bar{h}\bar{h}ff & \bar{g}\bar{g}\bar{h}\bar{h} & \bar{d}ghe & \bar{g} \\
\hline
\end{array}$$

Let N_1 and N_2 be the matrices obtained from M_1 and M_2 by replacing the diagonal entries, y, of M_i by

$$\begin{array}{cccc} a & b & c & y \\ \bar{b} & a & y & \bar{c} \\ \bar{c} & \bar{y} & a & b \\ \bar{y} & c & \bar{b} & a \end{array}$$

and the off-diagonal block entries p,q,r,s of M_i by

$$\begin{array}{cccc} p & q & r & s \\ q & \bar{p} & s & \bar{r} \\ r & s & \bar{p} & q \\ s & \bar{r} & q & p. \end{array}$$

Then N_1 and N_2 give orthogonal designs of order 24 and types (1,1,1,1,1,5, 5,9) and (1,1,1,1,1,2,8,9), respectively.

Hence, we have

Lemma 4.13 (P. Robinson [72]). *All three-tuples* (x,y,z), $x+y+z=24$, *are the types of orthogonal designs in order* 24. *That is, all* $\mathrm{OD}(24;x,y,24-x-y)$ *exist.*

Proceeding as in Theorem 4.10 we obtain

Theorem 4.14. *Let* q *be a positive integer. Then there exists a* $t=t(q)$ *so that there is an Hadamard matrix of order* $2^s\cdot 3\cdot q$ *for all* $s\geq t$.

Remark. A few other results of the kind in this section are known for orders $4\cdot p\cdot q$ and $3<p\leq 11$. The importance of this result lies in the fact that the power s will be smaller than the power t obtained from Theorem 3.13 (see [81]).

5 SEQUENCES

A special orthogonal design, the OD$(4t;t,t,t,t)$, is especially useful in constructing Hadamard matrices. An OD(12;3,3,3,3) was first found by Baumert-Hall [6] and an OD(20;5,5,5,5) by Welch. These were given in Section 3. OD$(4t;t,t,t,t)$ are sometimes called *Baumert-Hall arrays*. This chapter concentrates on the powerful construction techniques for these OD$(4t;t,t,t,t)$ using disjoint orthogonal matrices and sequences with zero autocorrelation.

Since we are concerned with orthogonal designs, we will consider sequences of commuting variables. Let $X = \{\{a_{11},\ldots,a_{1n}\},\{a_{21},\ldots,a_{2n}\}\ldots\{a_{m1},\ldots,a_{mn}\}\}$ be m sequences of commuting variables of length n. The *nonperiodic autocorrelation function of the family of sequences* X (denoted N_X) is a function defined by

$$N_X(j) = \sum_{i=1}^{n-j}(a_{1,i}a_{1,i+j} + a_{2,i}a_{2,i+j} + \cdots + a_{m,i}a_{m,i+j}).$$

Early work of Golay [28, 29] was concerned with two $(1,-1)$ sequences with zero nonperiodic autocorrelation function, but Welti [123], Tseng [101], and Tseng and Liu [102] approached the subject from the point of view of two orthonormal vectors, each corresponding to one of two orthogonal waveforms. Later work, including Turyn's [108, 107], used four or more sequences.

Note that if the following collection of m matrices of order n is formed,

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & a_{11} & & a_{1,n-1} \\ & & \ddots & \\ 0 & & & a_{11} \end{bmatrix}, \begin{bmatrix} a_{21} & a_{22} & \cdots & a_{2n} \\ & a_{21} & & a_{2,n-1} \\ & & \ddots & \\ 0 & & & a_{21} \end{bmatrix}, \ldots,$$

$$\begin{bmatrix} a_{m1} & a_{m2} & \cdots & a_{mn} \\ & a_{m1} & & a_{m,n-1} \\ & & \ddots & \\ 0 & & & a_{m1} \end{bmatrix},$$

then $N_X(j)$ is simply the sum of the inner products of rows 1 and $j+1$ of these matrices.

The *periodic autocorrelation function of the family of sequences* X (denoted P_X) is a function defined by

$$P_X(j) = \sum_{i=1}^{n}(a_{1,i}a_{1,i+j} + a_{2,i}a_{2,i+j} + \cdots + a_{m,i}a_{m,i+j}),$$

where we assume the second subscript is actually chosen from the complete set of residues (mod n).

We can interpret the function P_X in the following way: Form the m circulant matrices that have first rows, respectively,

$$[a_{11}a_{12}\ldots a_{1n}],[a_{21}a_{22}\ldots a_{2n}],\ldots,[a_{m1}a_{m2}\ldots a_{mn}];$$

then $P_X(j)$ is the sum of the inner products of rows 1 and $j+1$ of these matrices. In these matrices, all a_{ij} are chosen from the set $\{0,1,-1\}$.

We say the *weight* of a set of sequences X is the number of nonzero entries in X. If X is as above with $N_X(j)=0$, $j=1,2,\ldots,n-1$, then we will call X *m-complementary sequences* of length n. If

$$X=\{A_1,A_2,\ldots,A_m\}$$

are m-complementary sequences of length n and weight $2k$ such that

$$Y=\left\{\frac{(A_1+A_2)}{2},\frac{(A_1-A_2)}{2},\ldots,\frac{(A_{2i-1}+A_{2i})}{2},\frac{(A_{2i-1}-A_{2i})}{2},\ldots\right\}$$

are also m-complementary sequences (of weight k), then X will be said to be *m-complementary disjointable sequences* of length n. X will be said to be *m-complementary disjoint sequences* of length n if all $\binom{m}{2}$ pairs of sequences are disjoint.

For example $\{1\ 1\ 0\ 1\}$, $\{0\ 0\ 1\ 0\ -1\}$, $\{0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ -1\}$, $\{0\ 0\ 0\ 0\ 0\ 0\ 1\ -1\}$ are disjoint as they have zero nonperiodic autocorrelation function and precisely one $a_{ij}\neq 0$ for each j.

One more piece of notation is in order. If g_r denotes a sequence of integers of length r, then by xg_r we mean the sequence of integers of length r obtained from g_r by multiplying each member of g_r by x.

Proposition 5.1. *Let X be a family of m sequences of commuting variables. Then*

$$P_X(j)=N_X(j)+N_X(n-j),\qquad j=1,\ldots,n-1.$$

Corollary 5.2. *If $N_X(j)=0$ for all $j=1,\ldots,n-1$, then $P_X(j)=0$ for all $j=1,\ldots,n-1$.*

Note: $P_X(j)$ may equal 0 for all $j=1,\ldots,n-1$, even though the $N_X(j)$ do not.

If $X=\{\{a_1,\ldots,a_n\},\{b_1,\ldots,b_n\}\}$ are two sequences where $a_i,b_j\in\{1,-1\}$ and $N_X(j)=0$ for $j=1,\ldots,n-1$, then the sequences in X are called *Golay complementary sequences of length n*. For example, writing $-$ for minus 1, we

have

$n = 2$ 11 and 1−

$n = 10$ 1−−1−1−−−1 and 1−−−−−−11−

$n = 26$ 111−−111−1−−−−−1−11−−1−−−− and

−−−11−−−1−11−1−1−11−−1−−−−.

We note that if X is as above, if A is the circulant matrix with first row $\{a_1,\ldots,a_n\}$, and, if B the circulant matrix with first row $\{b_1,\ldots,b_n\}$, then

$$AA^T + BB^T = \sum_{i=1}^{n}(a_i^2 + b_i^2)I_n = 2nI_n.$$

Consequently, such matrices may be used to obtain Hadamard matrices constructed from two circulants.

We would like to use Golay sequences to construct other orthogonal designs, but first we consider some of their properties.

Lemma 5.3. *Let $X = \{\{a_1,\ldots,a_n\},\{b_1,\ldots,b_n\}\}$ be Golay complementary sequences of length n. Suppose that k_1 of the a_i are positive and k_2 of the b_i are positive. Then*

$$n = (k_1 + k_2 - n)^2 + (k_1 - k_2)^2,$$

and n is even.

Proof. Since $P_X(j) = 0$ for all j, we may consider the two sequences as $2 - \{n;k_1,k_2;\lambda\}$ supplementary difference sets with $\lambda = k_1 + k_2 - \frac{1}{2}n$. But the parameters (counting differences two ways) satisfy $\lambda(n-1) = k_1(k_1-1) + k_2(k_2-1)$. On substituting λ in this equation we obtain the result of the enunciation. □

Geramita and Seberry [23, pp. 133–137], Andres [2] and James [38] have studied the smaller values of n,k_1,k_2 of the lemma, showing the only lengths ≤ 68 for which Golay sequences exist are 2, 4, 8, 10, 16, 20, 26, 32, 40, 52, and 64. Malcolm Griffin [30] has shown no Golay sequences can exist for lengths $n = 2\cdot 9^t$. The value $n = 18$, which was previously excluded by a complete search, is now theoretically excluded by Griffin's theorem and independently by a result of Kruskal [62] and C. H. Yang [133, 134]. Andres [2] and James [38] have found greatly improved computer algorithms for studying these sequences.

Recent theoretical work of Koukouvinos, Kounias, and Sotirakoglou [50] and Eliahou, Kervaire, and Saffari [20] shows that Golay sequences do not exist for $n = 2p$ where p has any prime factor $\equiv 3 \pmod 4$. This means the unresolved cases < 200 are $n = 74, 82, 106, 116, 122, 130, 136, 146, 148, 164, 170, 178, 194$.

Constraints can be found on the elements of a Golay sequence. One useful result (see Geramita and Seberry [23]) is

Lemma 5.4. *For Golay sequences* $X = \{\{x_i\},\{y_i\}\}$ *of length* n,

$$x_{n-i+1} = e_i x_i \Leftrightarrow y_{n-i+1} = -e_i y_i,$$

where $e_i = \pm 1$. *That is,*

$$x_{n-i+1}x_i = -y_{n-i+1}y_i.$$

Example 5.1. The sequences of length 10 are

$$1--1-1---1 \text{ and}$$
$$1------11-.$$

Clearly, $e_1 = 1$, $e_2 = 1$, $e_3 = 1$, $e_4 = -1$, and $e_5 = -1$.

Proof (of Lemma 5.4*).* We use the fact that if x,y,z are $\pm 1, (x+y)z \equiv x+y \pmod 4$ and $x+y \equiv xy+1 \pmod 4$.

Let $i = 1$. Clearly, the result holds. We proceed by induction. Suppose that the result is true for every $i \leq k-1$. Now consider $N(k) = N(n-k) = 0$, and we have

$$\begin{aligned}
0 &= x_1x_{n+1-k} + x_2x_{n+2-k} + \cdots + x_kx_n + y_1y_{n+1-k} + y_2y_{n+2-k} + \cdots + y_ky_n \\
&= x_1e_kx_k + x_2e_{k-1}x_{k-1} + \cdots + x_ke_1x_1 + y_1y_{n+1-k} - y_2e_{k-1}y_{k-1} \\
&\quad - \cdots - y_ke_1y_1 \\
&\equiv e_1 + e_2 + \cdots + e_k + y_1y_{n+1-k} - e_{k-1} - \cdots - e_2 - y_ke_1y_1 \pmod 4 \\
&\equiv e_1 + e_k + y_1y_{n+1-k} - y_ke_1y_1 \pmod 4 \\
&\equiv e_k + y_ky_{n+1-k} \pmod 4 \\
&\equiv 0 \pmod 4.
\end{aligned}$$

So $y_{n+1-k} = -e_ky_k$. □

5.1. Summary of Golay Properties

Two sequences $\{x_1,\ldots,x_n\}$ and $\{y_1,\ldots,y_n\}$ are called *Golay complementary sequences* of length n if all their entries are ± 1 and

$$\sum_{i=1}^{n-j}(x_ix_{i+j} + y_iy_{i+j}) = 0 \qquad \text{for every} \quad j \neq 0, \quad j = 1,\ldots,n-1,$$