Hadamard matrices, orthogonal designs and construction algorithms

S. Georgiou
National Technical University of Athens, Greece

C. Koukouvinos
National Technical University of Athens, Greece

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Hadamard matrices, orthogonal designs and construction algorithms

Abstract

We discuss algorithms for the construction of Hadamard matrices. We include discussion of construction using Williamson matrices, Legendre pairs and the discret Fourier transform and the two circulants construction. Next we move to algorithms to determine the equivalence of Hadamard matrices using the profile and projections of Hadamard matrices. A summary is then given which considers inequivalence of Hadamard matrices of orders up to 44. The final two sections give algorithms for constructing orthogonal designs, short amicable and amicable sets for use in the Kharaghani array.

Disciplines

Physical Sciences and Mathematics

Publication Details

Hadamard matrices, orthogonal designs and construction algorithms

S. Georgiou, C. Koukouvinos
Department of Mathematics
National Technical University of Athens
Zografou 15773, Athens, Greece
and
Jennifer Seberry
School of IT and Computer Science
University of Wollongong
Wollongong, NSW 2522, Australia

Contents

Abstract

     We discuss algorithms for the construction of Hadamard matrices. We include discussion of construction using Williamson matrices, Legendre pairs and the discret Fourier transform and the two circulants construction.

     Next we move to algorithms to determine the equivalence of Hadamard matrices using the profile and projections of Hadamard matrices. A summary is then given which considers inequivalence of Hadamard matrices of orders up to 44.

     The final two sections give algorithms for constructing orthogonal designs, short amicable and amicable sets for use in the Kharaghani array.

1   Algorithms for constructing Hadamard matrices

1.1   Hadamard matrices constructed from Williamson matrices

An Hadamard matrix H of order n has elements ± 1 and satisfies $HH^{\mathrm{T}} = nI_n$. These matrices are used extensively in coding and communications (see Seberry and Yamada [90]). The order of an Hadamard matrix is 1, 2 or $n \equiv (0 \bmod 4)$. The first unsolved case is order 428. We use Williamson's construction as the basis of our algorithm to construct a distributed computer search for new Hadamard matrices. We briefly describe the theory of Williamson's construction below. Previous computer searches for Hadamard matrices using Williamson's condition

are described in Section 1.1.1. The implementation of the search algorithm is presented in Section 1.1.2, and the results of the search are described in Section 1.1.3.

Theorem 1 (Williamson [104]) *Suppose there exist four* $(1, -1)$ *matrices* A, B, C, D *of order* n *which satisfy*

$$XY^{\mathrm{T}} = YX^{\mathrm{T}}, X, Y \in \{A, B, C, D\}$$

Further, suppose

$$AA^{\mathrm{T}} + BB^{\mathrm{T}} + CC^{\mathrm{T}} + DD^{\mathrm{T}} = 4nI_n \tag{1}$$

Then

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix} \tag{2}$$

is an Hadamard matrix of order $4n$ *constructed from a Williamson array.*

Let the matrix T given below be called the shift matrix:

$$T = \begin{bmatrix} 0\ 1\ 0 & \cdots & 0 \\ 0\ 0\ 1 & \cdots & 0 \\ \cdots & \cdots & . \\ 0\ 0\ 0 & \cdots & 1 \\ 1\ 0\ 0 & \cdots & 0 \end{bmatrix} \tag{3}$$

and note

$$T^n = I, \ (T^i)^{\mathrm{T}} = T^{n-i} \tag{4}$$

If n is odd, T is the matrix representation of the nth root of unity ω, $\omega^n = 1$.
Let

$$\begin{cases} A = \sum_{i=0}^{n-1} a_i T^i, & a_i = \pm 1, a_{n-i} = a_i \\ B = \sum_{i=0}^{n-1} b_i T^i, & b_i = \pm 1, b_{n-i} = b_i \\ C = \sum_{i=0}^{n-1} c_i T^i, & c_i = \pm 1, c_{n-i} = c_i \\ D = \sum_{i=0}^{n-1} d_i T^i, & d_i = \pm 1, d_{n-i} = d_i \end{cases} \tag{5}$$

Then matrices A, B, C, D may be represented as polynomials. The requirement that $x_{n-i} = x_i, x \in \{a, b, c, d\}$ forces the matrices A, B, C, D to be symmetric.

Since A, B, C, D are symmetric, (1) becomes:

$$A^2 + B^2 + C^2 + D^2 = 4nI_n$$

and the relation $XY^{\mathrm{T}} = YX^{\mathrm{T}}$ becomes $XY = YX$ which is true for polynomials.

Definition 1 *Williamson matrices are* $(1, -1)$ *symmetric circulant matrices. As a consequence of being symmetric and circulant they commute in pairs.*

We use the following theorem of Williamson's as the motivator for our search algorithm:

Theorem 2 (Williamson [104]) *If there exist solutions to the equations*

$$\mu_i = 1 + 2\sum_{j=1}^{s} t_{ij}(\omega^j + \omega^{n-j}), i = 1, 2, 3, 4 \tag{6}$$

where $s = \frac{1}{2}(n-1)$, ω is a nth root of unity, exactly one of $t_{1j}, t_{2j}, t_{3j}, t_{4j}$ is nonzero and equals ± 1 for each $1 \leq j \leq s$, and

$$\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2 = 4n$$

then there exist solutions to the equations:

$$\begin{cases} A = \sum_{i=0}^{n-1} a_i T^i, & a_0 = 1, a_i = a_{n-i} = \pm 1 \\ B = \sum_{i=0}^{n-1} b_i T^i, & b_0 = 1, b_i = b_{n-i} = \pm 1 \\ C = \sum_{i=0}^{n-1} c_i T^i, & c_0 = 1, c_i = c_{n-i} = \pm 1 \\ D = \sum_{i=0}^{n-1} d_i T^i, & d_0 = 1, d_i = d_{n-i} = \pm 1 \end{cases} \tag{7}$$

That is, there exists an Hadamard matrix of order $4n$.

In matrix form, $\omega^j + \omega^{n-j}$ is represented as $T^j + T^{n-j}$. Since these are symmetric, we write

$$\omega_j = \omega^j + \omega^{n-j}$$

Remark 1 The solutions for (6) are independent of the particular root ω, so if n as defined by (1) is prime, we can choose ω so that the first μ having any ω_j assigned has ω_1. Since the equations are true for all roots of unity ω, they are also true for $\omega = 1$.

Theorem 3 (Williamson [104]) *Let n be odd, and matrices A, B, C, D satisfy (1) and (5), suppose $a_0 = b_0 = c_0 = d_0$, then exactly three of $a_j, b_j, c_j, d_j, 1 \leq j \leq n-1$, have the same sign.*

1.1.1 Results from previous searches

In many cases complete searches have been conducted for Hadamard matrices of Williamson type. Searches have also been conducted for special classes of Williamson type Hadamard matrices. Furthermore, an infinite class of such matrices is known and will also be discussed briefly.

- Baumert and Hall [6] report results of a complete search for orders $4t$, t odd and $3 \leq t \leq 23$. Some incomplete results for higher orders are also given.

- Sawade [86] reports results of a complete search for orders $4t$, $t = 25, 27$. The results for $t = 25$ were later demonstrated to be incomplete by Djokovic [13].

- Djokovic [11] reports results of a complete search for orders $4t$, $t = 29, 31$. Only a single non-equivalent solution was found for $t = 29$ and is equivalent to an earlier result due to Baumert [4].

- Koukouvinos and Kounias [64, 65] report results of a complete search for order $4t$, $t = 33$ and 39. These results were later demonstrated to be incomplete by Djokovic [12].

- Djokovic [12] reports results of a complete search for orders $4t$, $t = 33, 35, 39$.

- Djokovic [13] reports results of a complete search for orders $4t$, $t = 25, 37$. This extends results obtained by Sawade [86] for $t = 25$ and, for $t = 37$, by Williamson [104] and later Yamada [105] for a special class of matrices.

- Horton, Koukouvinos, and Seberry [53] report results of a complete search for orders $4t$, t odd and $25 \leq t \leq 37$. No new results were found, confirming existence results.

An infinite family of Hadamard matrices of Williamson type has been proved to exist under certain conditions [98, 103]:

Theorem 4 *If q is a prime power, $q \equiv 1 \pmod 4$, $q + 1 = 2t$, then there exists a Williamson matrix of order $4t$; we have $C = D$, and A and B differ only on the main diagonal.*

This theorem gives examples of Hadamard matrices of Williamson type for orders $4t$, $t = 31, 37, 41, 45, 49, 51, 55, \ldots$, for example.

Yamada [105] has searched for Hadamard matrices of Williamson type, with certain restrictions. These matrices are referred to as *Williamson type j matrices*. The Williamson equation for such matrices, of order $4n$ is:

$$4n = \left(1 - 2\sum_{s \in A} c_s \omega_s\right)^2 + \left(1 - 2\sum_{s \in A} c_s \omega_{sj}\right)^2 + \left(1 - 2\sum_{s \in B} d_s \omega_s\right)^2 + \left(1 - 2\sum_{s \in B} d_s \omega_{sj}\right)^2 \tag{8}$$

where $c_s, d_s = \pm 1$, $\omega_s = \omega^s + \omega^{-s}$, $\omega^n = 1$, $j^2 \equiv -1 \pmod n$, A, B, jA, jB is a partition of $\{1, 2, \ldots, \frac{n-1}{2}\}$. Such a j exists if and only if all prime divisors of n are $\equiv 1 \pmod 4$. This led to some new results for $n = 29, 37, 41$.

1.1.2 Search method

The search method to find Williamson matrices described in this section was given in [53].

Introduction The basic search method is to examine all possible combinations of $\omega_j, 1 \leq j \leq \frac{1}{2}(n-1)$ for each $\mu_i, i = 1, 2, 3, 4$, testing each set of μ so generated to see if it satisfies Williamson's condition and can be used to form an Hadamard matrix of order $4n$. This search method is documented in more detail in the following sections.

As a result of the large size of the search space, a distributed client/server approach was taken to the problem: the server breaks work up into smaller portions which are then processed by the clients; any results discovered are reported to the server by the client. Very little work is done by the server itself.

Using a distributed approach, we are able to perform large amounts of work in a fraction of the time required for a single computer to perform the same amount of work.

At various times during the performance of the searches, Macintosh computers and computers running some variety of UNIX have been available for use. To make best use of the available resources, and to eliminate any need to install software beyond that of the client program itself, all communication was performed using low-level networking APIs, sockets [93] on UNIX and Open Transport [1] on the Macintosh, rather than using a package such as PVM [18] or MPI [42] that in some cases can facilitate the construction of distributed programs.

Searches for Hadamard matrices of all orders up to and including order 148 have been performed using Williamson's method implemented by a client/server system. Towards the end of an initial search of order 148, 37 computers were involved, 20 270MHz Ultra 5 computers

from Sun Microsystems, and 17 333MHz iMacs from Apple Computer. No computers not available on the local area network were employed in the initial search. However, a subsequent search performed to verify results utilized 35 350MHz Pentium-II computers at the University of Newcastle in addition to 30 local Ultra 5 computers.

The details of the implementation of Williamson's method within the framework of a client/ server system are discussed in the following sections.

Decompose $4n$ into sum-of-squares representation The first step in performing a search is to decompose $4n$ into all possible sums-of-squares representations. Observing the form of (6), we see that when $\omega = 1$ each μ_i satisfies:

$$\begin{aligned} |\mu_i| &\equiv 1 \bmod 4, \mu_i > 0; \text{ or} \\ |\mu_i| &\equiv 3 \bmod 4, \mu_i < 0. \end{aligned} \tag{9}$$

For example, the possible decompositions for 148 are:

$$\begin{array}{cccc} 1, & 1, & 5, & 11 \\ 1, & 7, & 7, & 7 \\ 3, & 3, & 3, & 11 \\ 3, & 3, & 7, & 9 \\ 5, & 5, & 7, & 7 \end{array}$$

In the sections to follow, we write ω_{sub} to indicate some $\omega_k = \omega^k + \omega^{n-k}$ for $1 \leq k \leq \frac{1}{2}(n-1)$ when it is necessary to distinguish from an nth root of unity, ω.

Decide on the number of ω_{sub} assigned to each μ The next step is to assign a number of ω_{sub} to each μ. Using (9), we see that if $|\mu_i| \equiv 1 \bmod 4$, then of the ω_{sub} contributing to μ_i, the number being added to μ_i will always be $\frac{|\mu_i|-1}{4}$ greater than the number of ω_{sub} that are subtracted. A similar condition can be derived for $|\mu_i| \equiv 3 \bmod 4$. These ω_{sub} are termed "fixed"; others are "floating" and always occur in pairs, one added and the other subtracted. These conditions are enforced to help limit the size of the space to be searched.

All possible permutations of the number of floating ω_{sub} are assigned to each μ over the course of the search of a particular sum-of-squares representation, subject to certain restrictions that are useful for reducing the size of the space to be searched:

1. The number of ω_{sub} assigned to μ_i must be greater than or equal to the number of ω_{sub} assigned to μ_j where $j < i$ and μ_i and μ_j correspond to the same value in the sum-of-squares decomposition. We may apply this condition because for the purposes of testing the set of μ to see if Williamson's condition is satisfied, μ_i and μ_j are interchangeable, and it is desirable to perform the test only once rather than twice. This may be extended further if more than two μ have the same value in the sum-of-squares decomposition.

2. If n is prime, then we may always place ω_1 in the first μ to which any ω_{sub} are assigned. This corresponds to solving the set of μ for some nth root of unity, ω^j, such that ω_1 is present in the first μ to which any ω_{sub} are assigned. Furthermore, if there are ω_{sub} both added and subtracted from this μ, we may either subtract or add ω_1; we do not need to check both. If this condition is in force, then condition 1 is not applied in the case of the μ to which ω_1 is assigned, but remains applicable for other μ corresponding to the same

6

value from the sum-of-squares decomposition. Enforcing this condition can greatly reduce the size of the space to be searched: for example, applying this condition for searching for Hadamard matrices of size 148 reduces the size of the space to be searched to 37% of its size were this condition not to be enforced (reducing from about 32,387,862,644,280 to 12,062,406,963,464)

For each permutation of floating ω_{sub} that is generated, we must assign specific identities to each ω_{sub} and evaluate Williamson's condition.

Assign specific identities to each ω_{sub} We must now assign specific identities to each ω_{sub} so that Williamson's condition may be tested.

Let the number of ω_{sub} added to μ_i be represented by c_{2i-1} and the number of ω_{sub} subtracted from μ_i by c_{2i}. S_{2i-1} is the set of ω_{sub} added to μ_i and S_{2i} is the set of ω_{sub} subtracted from μ_i. That is, there are eight sets S, two for each μ. Some of these sets S may be empty.

$$\mu_i = 1 + 2 \sum_{\forall j \in S_{2i-1}} \omega_j - 2 \sum_{\forall j \in S_{2i}} \omega_j$$

Dividing ω_{sub} into two groups, one added to a μ and the other subtracted, helps to simplify the procedure for iterating over all possible combinations of ω_{sub} .

The sets S_i are formed by choosing c_i elements from the set of ω_{sub} not already allocated to an $S_j, j < i$. Recalling that $s = \frac{1}{2}(n-1)$, $S_{\text{T},0}$ is defined as:

$$S_{\text{T},0} = \{\omega_1, \omega_2, \omega_3, \ldots, \omega_s\}.$$

$S_{\text{T},i}$ is defined as:

$$S_{\text{T},i} = S_{\text{T},i-1} - S_{i-1}, i = 1, \ldots, 8. \tag{10}$$

For convenience, we say that:

$$S_0 = \emptyset$$

Williamson's condition may be tested once $S_1, \ldots, S_8$ have been generated. All possible combinations of c_i elements from $S_{\text{T},i}$ are examined; once the combinations are exhausted, the next combination for S_{i-1} is generated. The process is illustrated by the small segment of pseudocode shown in Figure 1.

So it should be easy to see that the number of tests of Williamson's condition for a particular set of $c_1, \ldots, c_8$ can be calculated as follows:

$$\text{Evaluations} = \prod_{i=1}^{8} \binom{|S_{\text{T},i}|}{c_i} \tag{11}$$

Usually, however, the total number of evaluations performed will be less than this, for two reasons:

1. If condition 2 from Section 1.1.2 is applied, we choose one fewer ω_{sub} for the set S in which ω_1 is to appear.

2. If μ_i and $\mu_j, i < j$ correspond to the same value in the sum-of-squares decomposition of $4n$ and have the same number of ω_{sub} assigned, then we may require that if ω_x is the ω_{sub} of smallest subscript assigned to μ_i and ω_y has the smallest subscript assigned to

7

```
j := 1;
do
    for k from j to 8
        populate S_{T,k} from S_{T,k−1} and S_{k−1} using (10);
        generate combination S_k by choosing c_k elements from S_{T,k};
    ┌─────────────────────────────────────────────────────────────────────┐
    │ Test Williamson Condition using S_1, . . . , S_8 to generate μ_1, . . . , μ_4; │
    └─────────────────────────────────────────────────────────────────────┘
    j := 8;
    g := false;
    while ((j > 0) and (g == false))
        generate new combination S_j using c_j elements from S_{T,j}
        if successful
            g := true;
            j := j + 1;
        else
            j := j − 1;
while (j > 0);
```

Figure 1: Segment of pseudocode illustrating generation of combinations for testing Williamson's condition.

μ_j, that $x < y$. Otherwise, work will be repeated when μ_i replicates a sequence that had previously occurred in μ_j. Enforcing this condition ensures that no repetition takes place and reduces the size of the search space slightly. The reduction is unfortunately not as substantial as that for applying condition 2 from Section 1.1.2.

Dividing up the work for distribution   The obvious manner in which to reduce the amount of work performed by the clients to a reasonable level was to make the server perform part of the work described in Section 1.1.2. The server performs no evaluations itself, but would choose sets $S_1, \ldots, S_i$, for some $i < 8$. The client would evaluate all the possibilities for the choice of the remaining sets $S_{i+1}, \ldots, S_8$.

The server decides what value i should take by estimating the amount of work involved in a subproblem using a modification of Equation (11). Two constants $S_{\min}$ and $S_{\max}$ must be specified to the server: a subproblem is of acceptable size if its size lies between the two limits. Unfortunately, this does not yield subproblems with an even division of work: there are some very large and very small subproblems. Very small subproblems can be solved quickly, and result in a large number of reports of completed problems and requests for new problems being handled by the server over a short period of time. This can cause congestion and is not desirable.

The solution that was ultimately adopted was for the server to allocate multiple small subproblems to a client looking for work. The server also maintains a queue of pre-allocated subproblems ready for assignment to clients, so that client requests can be satisfied as rapidly as possible.

8

1.1.3 Search results

Lemma 1 *Let the Williamson decomposition into four squares be $s_1^2 + s_2^2 + s_3^2 + s_4^2 = 4n$. Further, let the row sums of the four Williamson matrices A, B, C, D be m_1, m_2, m_3, m_4. Let*

$$
M = \frac{1}{2}
\begin{bmatrix}
-1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 \\
1 & 1 & -1 & 1 \\
1 & 1 & 1 & -1
\end{bmatrix}
, \;
\underset{\sim}{s} =
\begin{bmatrix}
s_1 \\
s_2 \\
s_3 \\
s_4
\end{bmatrix}
, \;
\underset{\sim}{m} =
\begin{bmatrix}
m_1 \\
m_2 \\
m_3 \\
m_4
\end{bmatrix}
$$

Then

$$
s_1^2 + s_2^2 + s_3^2 + s_4^2 = 4n \Leftrightarrow m_1^2 + m_2^2 + m_3^2 + m_4^2 = 4n
$$

and

$$
M \underset{\sim}{s} = \underset{\sim}{m} \Leftrightarrow M \underset{\sim}{m} = \underset{\sim}{s}
$$

Proof. (6) gives, using the root $\omega = 1$, a decomposition with

$$
s_i = \mu_i = 1 + 4 \sum_{j=1}^{s} t_{ij}, \; i = 1, 2, 3, 4.
$$

By Williamson's assumption condition,

$$
s_1^2 + s_2^2 + s_3^2 + s_4^2 = 4n.
$$

On the other hand,

$$
\begin{aligned}
m_1 &= \sum_{j=1}^{n} a_j \\
&= 1 - 2 \sum_{j=1}^{\frac{n-1}{2}} t_{1j} + 2 \sum_{j=1}^{\frac{n-1}{2}} t_{2j} + 2 \sum_{j=1}^{\frac{n-1}{2}} t_{3j} + 2 \sum_{j=1}^{\frac{n-1}{2}} t_{4j} \\
&= 1 - \frac{1}{2}(s_1 - 1) + \frac{1}{2}(s_2 - 1) + \frac{1}{2}(s_3 - 1) + \frac{1}{2}(s_4 - 1) \\
&= \frac{1}{2}(-s_1 + s_2 + s_3 + s_4)
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
m_2 &= \frac{1}{2}(s_1 - s_2 + s_3 + s_4) \\
m_3 &= \frac{1}{2}(s_1 + s_2 - s_3 + s_4) \\
m_4 &= \frac{1}{2}(s_1 + s_2 + s_3 - s_4)
\end{aligned}
$$

and $M\underset{\sim}{s} = \underset{\sim}{m}$. Inverting we have, as $M^{-1} = M$, $M\underset{\sim}{m} = \underset{\sim}{s}$. It is easy to check that

$$
m_1^2 + m_2^2 + m_3^2 + m_4^2 = s_1^2 + s_2^2 + s_3^2 + s_4^2 = 4n.
$$

9

Unfortunately, no new matrices were found as a result of the searches run so far. However, we are able to provide independent verification of results from previous searches. This is considered of utility since some previous searches, such as that conducted by Sawade [86], for example, failed to reveal all solutions that are now known for the order searched, in that case, order 100. In particular, we provide verification of results reported by Djokovic [12, 13] for orders 100, 140 and 148. Results for order 100 are also verified by Christos Koukouvinos.

For reference purposes, tables of Hadamard matrices derived from Williamson matrices using circulant symmetric $(1, -1)$ matrices in the Williamson array for orders 100 through 180 are presented in Appendix 1 of [53]. A complete search of order 156 is claimed by Djokovic [12]. Results for orders 164, 172 and 180 are incomplete.

1.2 Hadamard matrices from Williamson matrices for non prime orders

An efficient algorithm to find Williamson matrices of order $n = p \cdot q$, i.e. n is not a prime has been described in [64]. This algorithm computes the solutions in groups of order p and q. In fact with the aim of this algorithm we can find all the inequivalent solutions which satisfy the Williamson equation in groups of orders p and q respectively. Then we can merge these solutions in order to find the solution in the group of order n. Of course this algorithm can also be used when n is prime power but it is not too efficient in this case. More details for this algorithm can be found in [64].

1.2.1 The method

In this section we give the necessary tools needed for our algorithm. We want to construct the $(1, -1)$ circulant matrices:

$$A = (a_0, a_1, \ldots, a_{m-1}), \quad B = (b_0, b_1, \ldots, b_{m-1}),$$
$$C = (c_0, c_1, \ldots, c_{m-1}), \quad D = (d_0, d_1, \ldots, d_{m-1}),$$

such that

$$A^2 + B^2 + C^2 + D^2 = 4mI_m. \tag{12}$$

The symmetry requirement gives $v_i = v_{m-i}$, $i = 1, 2, \ldots, \frac{1}{2}(m-1)$, $v_i \in \{a_i, b_i, c_i, d_i\}$. Let $G_q^T = (I_p, I_p, \ldots, I_p)$ be a $p \times p \cdot q$ matrix, i.e., the unit matrix I_p of order p is repeated q times.

The following theorems have been proved in [64] and are essential tools for our algorithm.

Theorem 5 *If*

1. $m = p \cdot q$, $p, q > 1$.

2. $V = (v_0, v_1, \ldots, v_{m-1})$ is circulant of order m, then

(a) $G_q^T \cdot V = U \cdot G_q^T$, where $U = (u_0, u_1, \ldots, u_{p-1})$ is circulant of order p with

$$u_j = \sum_{i \equiv j \pmod{p}, i < m} v_i, \quad j = 0, 1, \ldots, p-1,$$

(b) U is symmetric if V is symmetric.

Now multiplying on the left A, B, C, D by G_q^T we obtain:

$$G_q^T A = X_p G_q^T, \;\; G_q^T B = Y_p G_q^T, \;\; G_q^T C = Z_p G_q^T, \;\; G_q^T D = W_p G_q^T$$

where

$$
\begin{aligned}
X_p &= (x_0, x_1, \ldots, x_{p-1}), & \text{with } x_j &= \sum_i a_i, \\
Y_p &= (y_0, y_1, \ldots, y_{p-1}), & \text{with } y_j &= \sum_i b_i, \\
Z_p &= (z_0, z_1, \ldots, z_{p-1}), & \text{with } z_j &= \sum_i c_i, \\
W_p &= (w_0, w_1, \ldots, w_{p-1}), & \text{with } w_j &= \sum_i d_i
\end{aligned}
\tag{13}
$$

and the summations are over all $i \equiv j (mod\, p), \; i < m$.

If we multiply both members of (12), on the left by G_q^T and on the right by G_q we obtain in the symmetric case:

$$X_p^2 + Y_p^2 + Z_p^2 + W_p^2 = 4m I_p. \tag{14}$$

Of course we do not know A, B, C, D so we do not know X_p, Y_p, Z_p, W_p. However it is easier to find X_p, Y_p, Z_p, W_p satisfying (14) than A, B, C, D because p is much smaller than m. Now to construct X_p, Y_p, Z_p, W_p note that:

Theorem 6 *If*

1. *A, B, C, D are circulant and symmetric $(1, -1)$-matrices satisfying (12) with row (and hence column) sums a, b, c, d,*

2. *X_p, Y_p, Z_p, W_p are as defined in (13),*

then

1.

$$
\begin{aligned}
&\sum_{j=0}^{p-1} x_j = a, \;\; \sum_{j=0}^{p-1} y_j = b, \;\; \sum_{j=0}^{p-1} z_j = c, \;\; \sum_{j=0}^{p-1} w_j = d, \\
&a^2 + b^2 + c^2 + d^2 = 4m, \;\; -q \leq x_j, y_j, z_j, w_j \leq q, \;\; x_j, y_j, z_j, w_j \;\; \text{odd}, \\
&x_j = x_{p-j}, \;\; y_j = y_{p-j}, \;\; z_j = z_{p-j}, \;\; w_j = w_{p-j}, \;\; j = 1, 2, \ldots, \tfrac{1}{2}(p-1),
\end{aligned}
\tag{15}
$$

2. *If moreover $a_0 + b_0 + c_0 + d_0 = 0, \; \pm 4$, then*

$$
(x_0 + y_0 + z_0 + w_0) - (a_0 + b_0 + c_0 + d_0) =
\begin{cases}
0 (mod\, 8), & \text{if } q \equiv 1 (mod\, 4), \\
4 (mod\, 8), & \text{if } q \equiv 3 (mod\, 4),
\end{cases}
\tag{16}
$$

$$x_j + y_j + z_j + w_j \equiv 2 (mod\, 4), \quad j = 1, 2, \ldots, \tfrac{1}{2}(p-1).$$

1.2.2 The algorithm

For a given decomposition $4m = a^2 + b^2 + c^2 + d^2$, with $m = p \cdot q, \; p < q$, the algorithm consists of four stages:

I)   1. Form all sequences $X_p = \{x_0, x_1, \ldots, x_{p-1}\}$ satisfying:

$(i) \sum_{i=0}^{p-1} x_i = a,\ (ii)\ -q \le x_i \le q\ (iii)\ x_i$ odd,

$(iv)\ x_i = x_{p-i},\ \ i = 1, 2, \ldots, \frac{1}{2}(p-1).$

     2. Repeat the construction for Y_p, Z_p, W_p replacing a with b, c, d respectively.

     3. Examine which quadruples X_p, Y_p, Z_p, W_p satisfy $X_p^2 + Y_p^2 + Z_p^2 + W_p^2 = 4mI_p$.

II)   1. Repeat stage **I** interchanging p and q.

     2. Find all inequivalent solutions by applying the transformation $j \to j \cdot s (mod\ q)$ to each solution X_q, Y_q, Z_q, W_q, where $(s, m) = 1$ for every $s < q$.

III)   1. If there are h_1 solutions X_p, Y_p, Z_p, W_p, and h_2 inequivalent solutions $\hat{X}_q, \hat{Y}_q, \hat{Z}_q, \hat{W}_q$, form the $h_1 \cdot h2$ combined solutions $X_p, Y_p, Z_p, W_p, \hat{X}_q, \hat{Y}_q, \hat{Z}_q, \hat{W}_q$.

     2. Find $A = (a_0, a_1, \ldots, a_{m-1})$ from:

$$a_i = a_{m-i}, \ \ i = 1, 2, \ldots, \frac{1}{2}(m-1),$$

$$\sum_{i \equiv j (mod\ p), i < m} a_i = x_j, \ \ j = 0, 1, 2, \ldots, \frac{1}{2}(p-1),$$

$$\sum_{i \equiv j (mod\ q), i < m} a_i = \hat{x}_j, \ \ j = 0, 1, 2, \ldots, \frac{1}{2}(q-1),$$

where $X_p = (x_0, x_1, \ldots, x_{p-1}),\ \ \hat{X}_q = (\hat{x}_0, \hat{x}_1, \ldots, \hat{x}_{q-1}).$

     3. Find B, C, D similarly.

IV) Examine which quadruples A, B, C, D satisfy $A^2 + B^2 + C^2 + D^2 = 4mI_m$.

Now repeat stages, **I, II, III, IV** for every decomposition of $4m$ as the sum of four odd squares.

    If $p = q$ then the algorithm is:

1)   1. Perform steps 1, 2 ,3 of stage **I** of the previous algorithm.

     2. Find all inequivalent solutions by applying the transformation $j \to j \cdot s (mod\ p)$ to each solution X_p, Y_p, Z_p, W_p, where $(s, m) = 1$ for every $s < p$.

2)   1. Find $A = (a_0, a_1, \ldots, a_{m-1})$ from:

$$a_i = a_{m-i}, i = 1, 2, \ldots, \frac{1}{2}(m-1), \qquad \sum_{i \equiv j (mod\ p), i < m} a_i = x_j, j = 0, 1, 2, \ldots, \frac{1}{2}(p-1),$$

where $X_p = (x_0, x_1, \ldots, x_{p-1}).$

     2. Find B, C, D similarly.

3) Examine which quadruples A, B, C, D satisfy $A^2 + B^2 + C^2 + D^2 = 4mI_m$.

Now repeat stages, **1, 2, 3,** for every decomposition of $4m$ as the sum of four odd squares.

    This algorithm was used in [64, 65] for a complete search for orders $4t$, $t = 33, 39$. The same algorithm was used later by Djokovic [12] for orders $4t$, $t = 33, 35, 39$. He noted one more solution for $t = 33$ and $t = 39$ which was missing in [64, 65]. He also claimed the non existence results for $t = 35$.

1.3 Hadamard matrices from generalized Legendre pairs using the discrete Fourier transform

1.3.1 Definitions and notations

Let U be a sequence of ℓ real numbers $u_0, u_1, ..., u_{\ell-1}$. The *periodic autocorrelation function, PAF*, $P_U(j)$ of such a sequence is defined, reducing $i + j$ modulo ℓ, by:

$$P_U(j) = \sum_{i=0}^{\ell-1} u_i u_{i+j}, \quad j = 0, 1, ..., \ell - 1.$$

Two sequences U and V of identical length ℓ are said to be *compatible* if the sum of their periodic autocorrelations is a constant, say a, except for the 0-th term. That is,

$$P_U(j) + P_V(j) = a, \quad j \neq 0. \tag{17}$$

(Such pairs are said to have *constant periodic autocorrelation* even though it is the sum of the autocorrelations that is a constant.) If U and V are both ±1 sequences, compatible and $a = -2$, then they are called *a generalized Legendre pair (or GL–pair)*.

In this section we are interested for compatible ±1 sequences which are a GL–pair, and may be used as below to construct Hadamard matrices of order $2\ell + 2$. The Legendre or Jacobi symbol is written $(a|n)$ if n is prime or composite, respectively. When referring to the elements of a $-1, 0, 1$ sequence we often write '$-$' instead of -1 and '$+$' instead of 1.

The *discrete Fourier transform (DFT)* of a sequence U is given by

$$DFT_U(k) = \mu_k = \sum_{i=0}^{\ell-1} u_i \omega^{ik}, \quad k = 0, 1, ..., \ell - 1$$

where ω is a primitive ℓ-th root of unity $e^{\frac{2\pi i}{\ell}}$. If we take the squared magnitude of each term in the DFT of U, the resulting sequence is called the *power spectral density (PSD)* of U. Because we use them so often, the k-th terms in the PSDs of U and V will be denoted by $|\mu_k|^2$ and $|\nu_k|^2$, respectively.

Example 1 The PSD of the sequence 1 2 2 -2 0 0 0 is

$$49.000 \quad 19.988 \quad 13.220 \quad 7.792 \quad 7.792 \quad 13.220 \quad 19.988$$

If a sequence u is transformed by the operation of cyclically taking every d-th element, where $\gcd(d, \ell) = 1$, the sequence U is said to be *decimated* by d. That is, if $V = U$ decimated by d, then $v_i = u_{di \mod \ell}$.

Example 2

$$1111000 \text{ decimated by } 2 = 1100110$$
$$1111000 \text{ decimated by } 3 = 1101010$$

The set of all possible decimations of a sequence is called a *decimation class*. Since d is required to be relatively prime to ℓ, a sequence of length ℓ has $\phi(\ell)$ decimations, though sometimes they are not all distinct. We note that decimation by -1 is the same as reversing a sequence. Hence, by assuming that each sequence also represents its reverse, the maximum size of any decimation class is $\phi(\ell)/2$. Finally, we define compatibility between decimation classes. Two decimation classes are said to be compatible if and only if some sequence belonging to one class is compatible with some sequence in the other class.

1.3.2 Some preliminary results

We make use of the following well-known theorem [84, Chapter 12], [97, Chapter 10].

Theorem 7 (Wiener–Khinchin Theorem) *The PSD of a sequence is equal to the DFT of its periodic autocorrelation function*

$$|\mu_k|^2 = \sum_{j=0}^{\ell-1} P_U(j)\omega^{jk}. \tag{18}$$

The periodic autocorrelation function is equal to the inverse DFT of the sequence's PSD

$$P_U(j) = \frac{1}{\ell} \sum_{k=0}^{\ell-1} |\mu_k|^2 \omega^{-jk}. \tag{19}$$

The next main theorem was proved in [17].

Theorem 8 *Two sequences are compatible if and only if their PSDs sum to a constant (i.e. $|\mu_k|^2 + |\nu_k|^2 = c$ iff $P_U(j) + P_V(j) = a$).*

Example 3 Two compatible sequences and their PSDs are shown below.

Sequences	PSD (terms 1 to 3)		
1 2 2 -2 0 0 0	19.988	13.220	7.792
2 1 -1 2 -1 0 0	5.012	11.780	17.208
	25.000	25.000	25.000	(hence c = 25)

In fact, the constant c depends only on the set of numbers comprising the sequences U and V. It is easily shown that

$$c = \frac{\ell \sum_{i=0}^{\ell-1} u_i^2 - (\sum_{i=0}^{\ell-1} u_i)^2}{\ell - 1} + \frac{\ell \sum_{i=0}^{\ell-1} v_i^2 - (\sum_{i=0}^{\ell-1} v_i)^2}{\ell - 1}. \tag{20}$$

Hence, all permutations of the sequences yield the same constant. Theorem 8 is a generalization of results that have appeared in the literature in other forms, see for example Kounias, Koukouvinos, Nikolaou and Kakos [75].

The following useful relationships are easily proved by direct application of the definitions of decimation, autocorrelation and DFT.

- If a sequence is decimated by d, then its autocorrelation is likewise decimated by d, and its DFT and PSD are decimated by $d^{-1} \bmod \ell$.

- It follows immediately that compatible sequences remain compatible if they are decimated by the same amount.

Remark 2 If U, V are $\pm 1, 0$–sequences then the above constant c is $c = w - a$, where w is the total number of non–zero entries and a is the constant from the periodic autocorrelation function of U and V.

1.3.3 Legendre sequences and modified Legendre sequences

For the remainder of this section we consider only GL–pairs. The following is well known (see for example [101]) and is included for completeness only. Let p be an odd prime. The $-1, 0, 1$ sequence U of length p is called a *Legendre sequence* L if its elements $x_i = l_i$ satisfy

$$l_i = (i|p).$$

In other words, $l_0 = 0$ and for $i \neq 0$, $l_i = 1$ if i is a square modulo p and $l_i = -1$, otherwise. We call $(-1, L)$, $(0, L)$, or $(1, L)$ a *modified Legendre sequence*. The values of the modified Legendre sequence are exactly the same as those of the unmodified one except for l_0 which is set to -1, 0, or $+1$, respectively. $((0, L)$ is of course the original Legendre sequence but sometimes it is convenient to refer to it as an modified Legendre sequence.) Two sequences (e_1, L), (e_2, L) with $e_1, e_2 \in \{-1, 0, 1\}$ are called *modified Legendre sequences* and they are defined in the obvious manner.

Example 4 Let $p = 7$. The modified Legendre sequences $(0, L)$ and $(1, L)$ are given by

$$
\begin{aligned}
(0, L) &= 0 + + - + - - \\
(1, L) &= + + + - + - -
\end{aligned}
$$

The following two lemmas (see [17]) say that GL-pairs exist for lengths ℓ, where:

(i) ℓ is a prime (see for example [17]).

(ii) $2\ell + 1$ is a prime power (these arise from Szekeres difference sets, see for example [17] or [37]).

Lemma 2 *Let p be an odd prime then $(1, -L)$, $(1, L)$ is a GL–pair.*

This lemma shows the existence of a GL–pair for every odd prime p. We also note that

Lemma 3 *Let $p = 2\ell + 1$ be a prime power then there is a GL–pair.*

Theorem 9 *Suppose there is a GL-pair of length ℓ. Then there exists an Hadamard matrix of order $2\ell + 2$.*

Proof. The sequences are used to make two circulant matrices A and B of order ℓ. Then the following matrix is the required Hadamard matrix.

15

$$\begin{bmatrix} \begin{array}{cc|cccc} - & - & + & \cdots & + & + & \cdots & + \\ - & + & + & \cdots & + & - & \cdots & - \\ \hline + & + & & & & & & \\ \vdots & \vdots & & A & & & B & \\ + & + & & & & & & \\ + & - & & & & & & \\ \vdots & \vdots & & B^T & & & -A^T & \\ + & - & & & & & & \end{array} \end{bmatrix}$$

Corollary 1 *Suppose that there are* $2 - \{\ell; \frac{\ell+1}{2}, \frac{\ell+1}{2}; \frac{\ell+1}{2}\}$ *SDS. Then there exists an Hadamard matrix of order* $2\ell + 2$.

GL-pairs also exist for lengths ℓ, where:

(i) $\ell = 2^k - 1$, $k \geq 2$ (two Galois sequences are a GL-pair, see for example [85]).

(ii) $\ell = 49, 57$ (these have been found by a non-exhaustive computer search that uses generalized cyclotomy and master-switch techniques, see [37, 44]).

(iii) $\ell = 3, 5, \ldots, 45$ (these have been found and classified by exhaustive computer searches, see [17]).

(iv) $\ell = 47, 49$ and 51 (these have been found and classified by partial computer searches, see [17]).

(v) $\ell = 143$ (also verified the results for $\ell = 3, 5, 7, 11, 13, 15, 17, 19, 23, 25, 31, 35, 37, 41, 43, 53, 59, 61, 63$ see [22]).

GL-pairs do not exist for even lengths. It is indicated in [17] that the following lengths $\ell \leq 200$ are unresolved: $55, 77, 85, 87, 91, 93, 115, 117, 121, 123, 129, 133, 145, 147, 159, 161, 169, 171, 175, 177, 185, 187$ and 195.

We note here that a GL-pair for length $\ell = 143$ is constructed easily since $143 = 11 \cdot 13$ is a product of twin primes as indicated in Corollary 2.

1.3.4   The PSD test

We suppose that the set of numbers comprising sequences U and V are fixed and that only permutations of these sequences will be considered. Now every term in a PSD is non–negative. Hence if the sequences U and V are compatible, then no term in their PSDs can exceed the constant c in Theorem 8. That is,

$$|\mu_k|^2 + |\nu_k|^2 = c \implies |\mu_k|^2 \leq c.$$

Equivalently, if any term of a sequence's PSD exceeds c, then the sequence cannot be a member of a compatible pair and so maybe discarded from our search. This test can be generalized in a straightforward manner to any family of sequences over any alphabet that have constant periodic autocorrelation function. (Since, the nonperiodic autocorrelation function being constant implies that the periodic autocorrelation function is constant, the above test is also applicable for such candidate sequences.)

16

1.3.5 Empirical performance of the PSD test for binary sequences

Exhaustive searches over the space of all binary 0, 1–sequences were performed for various lengths and weights (number of ones) to see what fraction of sequences actually pass the PSD test. The lengths ℓ and weights w were chosen to correspond to supplementary difference sets used in the constructions of D–optimal designs [75] and Hadamard matrices (as described above) while c, the threshold for the PSD test, was determined by (20). The results are shown Table 1 of [17]. (The last three rows in this table are derived from a count of decimation classes rather than sequences, but the percentage reduction is approximately the same either way.) It is evident that very substantial reductions in the number of candidate sequences can be realized through the use of the PSD test.

The exhaustive search algorithm was divided into three steps. In the first step, all decimation classes of length ℓ and weight $w = \frac{\ell+1}{2}$ are exhaustively generated, and each one that passes the PSD test is saved in a list. In the second step, the list is sorted by offset. In this manner, pairs of classes with equal and opposite offsets can be quickly found, and the third step is to compute the autocorrelation functions of such pairs to confirm whether they are compatible or not.

The results from these three steps for $\ell = 15$ are illustrated in Table 2 of [17].
The results from the exhaustive searches for $\ell \leq 45$ are shown in Table 3 of [17].

1.4 Hadamard matrices from generalized Legendre pairs using supplementary difference sets

1.4.1 Some preliminary results

We say that two sets of residues modulo ℓ, say P and Q, are $2 - \{\ell;\ k_1,\ k_2;\ \lambda\}$ *supplementary difference sets* mod ℓ (abbreviated as *sds*) if $|P| = k_1$, $|Q| = k_2$, and for each non-zero residue $k(mod\ell)$ the congruences $i - j \equiv k;\quad i,j \in P$, $i - j \equiv k;\quad i,j \in Q$, have in total exactly λ solutions.

If P, Q are $2 - \{\ell;\ k_1,\ k_2;\ \lambda\}$ *sds*, then we construct the first row of the corresponding $(-1, 1)$ circulant incidence matrices $A = (a_{ij})$ and $B = (b_{ij})$, $\quad i,j = 0, 1, \ldots, \ell - 1$, as follows:

$$a_{0j} = -1,\quad if\quad j \in P\quad and\quad a_{0j} = 1,\quad otherwise,$$

and

$$b_{0j} = -1,\quad if\quad j \in Q\quad and\quad b_{0j} = 1,\quad otherwise$$

We know (see [7] or [101]) that:

Theorem 10 *(i) If P, Q are supplementary difference sets $2 - \{\ell;\ k_1,\ k_2;\ \lambda\}$ and A, B the corresponding $(-1, 1)$ incidence matrices, then*

$$AA^T + BB^T = 4(k_1 + k_2 - \lambda)I_\ell + 2(\ell - 2(k_1 + k_2 - \lambda))J_\ell \tag{21}$$

(ii) Given two $\ell \times \ell$ circulant matrices A, B satisfying (21), then the corresponding sets P, Q are supplementary difference sets $2 - \{\ell;\ k_1,\ k_2;\ \lambda\}$, where k_1, k_2 is the number of -1's in each row of A, B respectively.

We note that two compatible sequences may contain elements from any alphabet. If the elements of two compatible sequences are $-1, 1$ then they are described as $2 - \{\ell; k_1, k_2; \lambda\}$ sds as the previous theorem say. In this section we are interested in the particular case of $2 - \{\ell; \frac{\ell+1}{2}, \frac{\ell+1}{2}; \frac{\ell+1}{2}\}$ since these give, compatible ± 1 sequences which are a GL-pair, and may be used to construct Hadamard matrices of order $2\ell + 2$.

In this particular case, relation (21) becomes

$$AA^T + BB^T = (2\ell + 2)I_\ell - 2J_\ell \tag{22}$$

Multiplying on the left by e^T and on the right by e both sides of (22) we obtain:

$$(\ell - 2k_1)^2 + (\ell - 2k_2)^2 = 2 \tag{23}$$

where e is the $\ell \times 1$ vector of one's. Since $k_1 = k_2 = (\ell + 1)/2$, we conclude that, the sum of the elements in each row and column of the circulant matrices A and B must be minus one. Since multiplication by -1 of the first row of A and/or B leaves relation (22) invariant, we deduce that the first element in the first rows of A and B will be $+1$ and from the remaining elements half will have positive sign and half negative one. Thus, a necessary condition for the existence of the $(-1, 1)$ circulant matrices A and B satisfying (22), or for the existence of the corresponding sds is that, ℓ should be odd.

Now we consider the first rows of A and B as two sequences of length ℓ. Using (19) it is easy to see that relation (22) is equivalent to

$$P_A(0) + P_B(0) = 2\ell \tag{24}$$

$$P_A(s) + P_B(s) = -2, \quad for \quad s = 1, 2, \ldots, \ell - 1 \tag{25}$$

If a sequence A of length ℓ is transformed by the operation of cyclically taking every d-th element, where $(d, \ell) = 1$, the sequence A is said to be *decimated* by d. That is, if $A^{'} = A$ decimated by d, then $a_i^{'} = a_{di}$, reducing di modulo ℓ. The set of all possible decimations of a sequence is called a *decimation class*. Since d is required to be relatively prime to ℓ, a sequence of length ℓ has $\phi(\ell)$ decimations, though sometimes they are not all distinct. We note that decimation by -1 is the same as reversing a sequence. Hence, by assuming that each sequences also represents its reverse, the maximum size of any decimation class is $\phi(\ell)/2$. Any pair of sequences that can be transformed into another pair by exchanging the sequences, cyclically shifting or reversing either of the sequences, or decimating both by the same amount are considered equivalent. The corresponding sds are also considered equivalent. This notice of equivalent sds was also considered in [75].

Since in our case the parameters k_1 and k_2 of the sds are equal, we investigate multipliers of $2 - \{\ell; \frac{\ell+1}{2}, \frac{\ell+1}{2}; \frac{\ell+1}{2}\}$ sds. This efficient technique has already applied for some other families of sds in [19, 74]. In these cases the authors construct the set P and search for all possible w's prime to the ℓ, i.e. $(w, \ell) = 1$ such that $Q = wP \ (mod\ell)$, and P, Q constitute a sds, if such w's exist. They found many multipliers of the sds and constructed D-optimal designs for some orders.

In particular, Koukouvinos, Seberry, Whiteman, and Xia [74] used cyclotomy to prove the following theorem, where C_i are the cyclotomic classes in $GF(v)$ constructed by using a generator g of $GF(v) \setminus \{0\}$.

Theorem 11 (see [74]) *Let g be a generator of the cyclic group $GF(v) \setminus \{0\}$. Suppose*

(i) $v = 2q^2 + 2q + 1$ is a prime power,

(ii) A and B are $2 - \{v; q^2, q^2; \lambda\}$ sds such that $2q+1$ is a multiplier ie $B = (2q+1)A$, and $2q + 1 \in C_i$,

(iii) A and B are unions of cyclotomic classes.

Then every $\alpha \in C_i$ or $\alpha \in C_i^{-1}$ is also a multiplier i.e. $B = \alpha A$.

1.4.2   Twin prime power construction

For a comprehensive introduction to cyclotomy see [37] and [94].
Stanton and Sprott [92], Storer [94], and Whiteman [102], showed constructions of difference sets over $GF(p) \times GF(p+2)$, with p, $p+2$ both prime powers. Gysin and Seberry [45] constructed

$$\frac{p+1}{2} - \{p(p+2); \frac{p^2 - 1}{2}, 2, \ldots, 2; \frac{(p-1)^2}{4}\}$$

sds over $GF(p) \times GF(p+2)$, where p, $p+2$ are two prime powers, $p > 2$. In fact if x, y generate $GF(p)^*$, $GF(p+2)^*$ respectively, they defined the following cyclotomic classes

$$C_i = \{(x^s, y^{s+i}) : s = 0, \ldots, f-1\}$$

$$E_k = \{(x^{\frac{p-1}{2}s+k}, 0) : s = 0, 1\}$$

where $i = 0, 1$, $k = 0, \ldots, \frac{p-1}{2} - 1$, and $f = \frac{p^2-1}{2} = lcm(p-1, p+1)$.
   Furthermore they defined $E = \{(x^s, 0) : s = 0, \ldots, p-2\}$, $D = \{(0, y^s) : s = 0, \ldots, p\}$. Then using the classes C_0, E, and D they reproved the following theorem, which was originally proved by Stanton and Sprott [92], and Whiteman [102]. This is also included in [5].

Theorem 12 (Stanton-Sprott-Whiteman restated) *Let C_0, E be defined as above, then $\{C_0 \cup E \cup \{0\}\}$ is a*

$$\{p(p+2); \frac{p^2-1}{2} + p; \frac{(p+1)^2}{4} - 1\}$$

difference set over $GF(p) \times GF(p+2)$.

Gysin and Seberry [45] also noted the following corollary.

Corollary 2 *Let C_0, D be defined as above, then $\{C_0 \cup D\}$ is a*

$$\{p(p+2); \frac{(p+1)^2}{2}; \frac{(p+1)^2}{4}\}$$

difference set over $GF(p) \times GF(p+2)$.

Example 5 Let $p = 3$, $p + 2 = 5$, $(x, y) = (2, 2) = 2$. Now

$$
\begin{aligned}
C_0 &= \{1, 2, 4, 8\} \\
D &= \{3, 6, 12, 9\} \\
E = E_0 = E_1 &= \{5, 10\}
\end{aligned}
$$

in this case
$$\{C_0 \cup D\} = \{1, 2, 4, 8, 3, 6, 12, 9\},$$
is a $\{15; 8; 4\}$ difference set over $GF(3) \times GF(5) \simeq Z_{15}$.

Example 6 Let $p = 5$, $p + 2 = 7$, $(x, y) = (2, 3) = 17$. Now

$$
\begin{aligned}
C_0 &= \{1, 17, 9, 13, 11, 12, 29, 3, 16, 27, 4, 33\} \\
D &= \{15, 10, 30, 20, 25, 5\} \\
E &= \{21, 7, 14, 28\} \\
E_0 &= \{21, 14\} \\
E_1 &= \{7, 28\},
\end{aligned}
$$

In this case

$$\{C_0 \cup D\} = \{1, 17, 9, 13, 11, 12, 29, 3, 16, 27, 4, 33, 15, 10, 30, 20, 25, 5\},$$

is a $\{35; 18; 9\}$ difference set over $GF(5) \times GF(7) \simeq Z_{35}$.

We observe that the parameters of the difference sets constructed in corollary 2, are $\{\ell, \frac{\ell+1}{2}, \frac{\ell+1}{4}\}$. Hence, the above corollary motivate us to find $2 - \{\ell; \frac{\ell+1}{2}, \frac{\ell+1}{2}; \frac{\ell+1}{2}\}$ sds. Thus we have:

Theorem 13 *There exist* $2 - \{\ell; \frac{\ell+1}{2}, \frac{\ell+1}{2}; \frac{\ell+1}{2}\}$ *sds, where* $\ell = p(p + 2)$ *and* p, $p + 2$ *are two prime powers,* $p > 2$.

Proof. Let D_1 be the $\{\ell, \frac{\ell+1}{2}, \frac{\ell+1}{4}\}$ difference set constructed in corollary 2. Then D_1 and $D_2 = D_1$ constitute a $2 - \{\ell; \frac{\ell+1}{2}, \frac{\ell+1}{2}; \frac{\ell+1}{2}\}$ sds. $\square$

Thus we conclude that:

Corollary 3 *Let* $\ell = p(p + 2)$, *with* $p, p + 2$ *both prime powers. Then there exist GL-pairs of length* ℓ.

1.4.3 The algorithm

For the construction of $2 - \{\ell; \frac{\ell+1}{2}, \frac{\ell+1}{2}; \frac{\ell+1}{2}\}$ sds, we use the following algorithm, which is given in [22]. A modified version of this algorithm has been applied in [19]. This algorithm uses the idea of multipliers and is much faster than the algorithms that have been used in [7] and [43]. This algorithm provides the sds that can be constructed using multipliers and performs an exhaustive search for the multipliers of these sds. Not only the complexity of the algorithm is reduced but also using some powerful but elementary results from group theory the construction used in this algorithm give us a theoretical result on the multipliers of the corresponding sds. Modifications of the algorithm can be used for searching sds with same parameters $k_1 = k_2$ and their multipliers.

For a given ℓ odd

(i) Find positive integers k_1, k_2, λ satisfying:
   $k_1 = k_2 = \lambda = \frac{\ell+1}{2}$.

(ii) For an integer t, $1 \le t < \ell$, $(t,\ell) = 1$, form all sets $\{a, at, \ldots, at^{m-1}\}$ with $at^m \equiv a \, mod(\ell)$ for all $a = 0, 1, \ldots, \ell - 1$. Sort the sets by the smallest element and call them a_i, $i = 0, 1, \ldots, m$.

(iii) Find all possible multipliers using Lemmas 4 and 5. Try only one element from the groups a_i and a_i^{-1}, and do not try multipliers w, unless $(w, \ell) = 1$.

(iv) Form one set P with k_1 elements as union of sets found in step (ii).

(v) For each multiplier w found in step (iii), set $Q = wP$.

(vi) Examine if P, Q are supplementary difference sets $2 - \{\ell; k_1, k_2; \lambda\}$.

(vii) If the answer in (vi) is positive then save the set P and multiplier w.

(viii) If the multiplier that used was not the last, then go to step (v) and try the next multiplier.

(ix) Repeat steps (iv)-(viii) until all possible combinations of unions of sets P are examined.

(x) If the last possible union of sets P is reached, then go to step (ii) and use the next integer t to form the sets a_i.

(xi) Repeat steps (ii)-(x) until all values of t, $1 < t < \ell$, $(t, \ell) = 1$ are examined.

Next Lemmas which are essential in our search for multipliers of sds were proved in [22].

Lemma 4 *Let a_i, $i = 0, 1, \ldots, m$ be the subsets constructed in step (ii) of our algorithm and $P = a_{i_1} \cup a_{i_2} \cup \ldots \cup a_{i_n}$, $Q = w_1 P$, $w_1 \in a_j$, $j \in \{1, \ldots, m\}$ be $2 - \{v; k, k; \lambda\}$ supplementary difference set (we say that w_1 is a multiplier for the difference set). Then*

(i) Every $w \in a_j$ is a multiplier for the supplementary difference set. That is $\forall w \in a_j$, P, $R = wP$ constitute a $2 - \{v; k, k; \lambda\}$ supplementary difference set.

(ii) Every $w \in a_j^{-1}$ is also a multiplier.

Lemma 5 *If $(w, \ell) > 1$ then w cannot be a multiplier.*

The above algorithm can perform an exhaustive search for multipliers but only a partial search for the corresponding sds. If the sds can be constructed using multipliers then they will be easily found otherwise the sds can not be constructed using multipliers but they may exist.

1.5 Hadamard matrices constructed from two circulant matrices

Let $A = \{A_j : A_j = \{a_{j1}, a_{j2}, ..., a_{jn}\}, \ j = 1, \ldots, \ell\}$, be a set of ℓ sequences of length n. The *non-periodic autocorrelation function (NPAF)* $N_A(s)$ of the above sequences is defined as

$$N_A(s) = \sum_{j=1}^{\ell} \sum_{i=1}^{n-s} a_{ji} a_{j,i+s}, \quad s = 0, 1, ..., n - 1. \tag{26}$$

If $A_j(z) = a_{j1} + a_{j2}z + \ldots + a_{jn}z^{n-1}$ is the associated polynomial of the sequence A_j, then

$$A(z)A(z^{-1}) = \sum_{j=1}^{\ell} \sum_{i=1}^{n} \sum_{k=1}^{n} a_{ji} a_{jk} z^{i-k} = N_A(0) + \sum_{j=1}^{\ell} \sum_{s=1}^{n-1} N_A(s)(z^s + z^{-s}). \tag{27}$$

It is clear that $P_A(s) = N_A(s) + N_A(n - s), \quad s = 1, \ldots, n - 1$. Therefore, if $N_A(s) = 0$ for all $s = 1, \ldots, n - 1$, then $P_A(s) = 0$ for all $s = 1, \ldots, n - 1$. But, $P_A(s)$ may equal zero for all $s = 1, \ldots, n - 1$, even though the $N_A(s)$ are not.

Definition 2 (Golay sequences) Two sequences $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ of length n, with elements ± 1, are defined as *Golay sequences* of length n, if the following equations

$$N_A(s) + N_B(s) = 0 \ \ s \quad s = 1, 2, \ldots, n - 1.$$

hold, where $N_A(s)$ is the nonperiodic autocorrelation function.

Example 7 The following binary sequences, with elements ± 1, are Golay sequences of length $n = 2, 10$ and 26 respectively.

(a) $n = 2, \ A = \{1, 1\}, \ \ B = \{1, -1\}$

(b) $n = 10$
$A = \{1, -1, -1, 1, -1, 1, -1, -1, -1, 1\}$
$B = \{1, -1, -1, -1, -1, -1, -1, 1, 1, -1\}$.

(c) $n = 26$

$$
\begin{aligned}
A = \{ \ & 1, 1, 1, -1, -1, 1, 1, 1, -1, 1, -1, -1, -1, -1, -1, \\
& 1, -1, 1, 1, -1, -1, 1, -1, -1, -1, -1 \ \} \\
B = \{ \ & -1, -1, -1, 1, 1, -1, -1, -1, 1, -1, 1, 1, -1, 1, -1, \\
& 1, -1, 1, 1, -1, -1, 1, -1, -1, -1, -1 \ \}.
\end{aligned}
$$

Lemma 6 *If A and B are $n \times n$ circulant ± 1 matrices with first rows two Golay sequences $\{a_1, a_2, \ldots, a_n\}$, $\{b_1, b_2, \ldots, b_n\}$ of length n respectively, then*

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

Lemma 7 *Let $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ are two Golay sequences of order n. Suppose that k_1 of the elements a_i are positive $(+1)$ and k_2 of the elements b_i are also positive $(+1)$. Then*

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

and n is even.

This condition is necessary but not sufficient for the existence of Golay sequences of order n.

Theorem 14 *If $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ are Golay sequences of length n and, $C = \{c_1, c_2, \ldots, c_m\}$ and $D = \{d_1, d_2, \ldots, d_m\}$ are Golay sequences of length m, then the sequences:*

$$X = A \times \left(\frac{C+D}{2}\right) + B \times \left(\frac{C-D}{2}\right)$$

$$Y = A \times \left(\frac{C^* - D^*}{2}\right) - B \times \left(\frac{C^* + D^*}{2}\right)$$

are Golay sequences of length nm.

So, as we know that Golay sequences of length $n = 2, 10, 26$ exist, then with the previous theorem we obtain that they exist in lengths $n = 2^a 10^b 26^c$, where a, b, c are non-negative integers. These results obtained by Golay [41] and Turyn [99], and these are the only known values of n that Golay sequences exist, These are the *Golay numbers*. It has been proved by Eliahou, Kervaire and Saffari [15] that Golay sequences do not exist for values $n = 34, 50, 58, 68$ and for every n that is divided by a prime number $p \equiv 3 \ (mod \ 4)$. The existence of Golay sequences of length n, if n, $n < 200 : n = 74, 82, 106, 116, 122, 130, 136, 146, 148, 164, 170, 178, 194$, is an open problem.
The following theorem is analogous to Theorem 10 and can be used for the construction of Hadamard matrices, see [101] or [106].

Theorem 15 *If A, B are $v \times v$ (v even) circulant matrices with entries ± 1, satisfying:*

$$AA^T + BB^T = 2vI_v \tag{28}$$

Then the matrix

$$H = \left[\begin{array}{cc} A & B \\ -B^T & A^T \end{array} \right]$$

is a Hadamard matrix of order $2v$.

Corollary 4 *If there are two $(1, -1)$ sequences of length n with zero PAF or NPAF then there exists a Hadamard matrix of order $2n$.*

Theorem 16 *There exist two sequences $(1, -1)$ with zero PAF for all lengths $n = 2^e \cdot 10^f \cdot 26^h \cdot 34$ for all non negative integers e, f, h.*

Proof. There are Golay sequences X, Y of length $2^e \cdot 10^f \cdot 26^h$. The following sequences A and B of length 34 have zero PAF, and are given in [21].

$$A = \{a, a, a, \bar{a}, \bar{a}, \bar{a}, \bar{b}, \bar{a}, \bar{b}, b, \bar{b}, b, a, \bar{b}, \bar{b}, b, b, a, b, \bar{b}, a, b, \bar{b}, b, b, a, a, \bar{a}, b, \bar{b}, a, b, b, a\}$$

$$B = \{b, \bar{a}, \bar{a}, b, a, \bar{a}, \bar{b}, b, b, \bar{a}, \bar{a}, a, \bar{a}, b, a, \bar{a}, b, \bar{a}, \bar{a}, a, a, b, \bar{a}, a, \bar{a}, a, \bar{b}, a, \bar{b}, \bar{b}, \bar{b}, b, b, b\}$$

In these sequences we replace variables a, b by the sequences X, Y respectively to obtain the desired result. $\square$

23

2   On inequivalent Hadamard matrices

2.1   Basic definitions and preliminaries

A Hadamard matrix is said to be *normalized* if it has its first row and column all 1's. Thus we can normalize the Hadamard matrix by multiplying rows and columns by -1 where needed. In these matrices, n is necessarily 2 or a multiple of 4. Two Hadamard matrices H_1 and H_2 are called equivalent (or Hadamard equivalent, or H-equivalent) if one can be obtained from the other by a sequence of row negations, row permutations, column negations and columns permutations.

The discussion of Hadamard equivalence is quite difficult, principally because of the lack of a good canonical form. The exact results which have been discovered are as follows : Hadamard matrices of orders less than 16 are unique up to equivalence. There are precisely five equivalence classes at order 16, and three equivalence classes at order 20, see [46, 47]. There are precisely 60 equivalence classes at order 24, see [54, 59]. There are precisely 487 equivalence classes at order 28, see [60, 61]. The classification of Hadamard matrices of orders $n \geq 32$ is still remains an open and difficult problem since an algorithmic approach of an exhaustive search is an NP hard problem.

Given two Hadamard matrices of the same order, it can be quite difficult to decide whether or not they are equivalent.

The next two subsections discuss the use of the "profile" and "projections" of Hadamard matrices to determine inequivalence.

The following criterion (profile) was given in [8].

2.2   The profile criterion

Cooper, Milas and Wallis in [8] suggested the profile criterion to investigate the equivalence of Hadamard matrices. Later Lin, Wallis and Zhu in [78, 80, 81] proposed some modifications of this criterion. Suppose H is a Hadamard matrix of order $4n$ with typical entries h_{ij}. We write $P_{ijk\ell}$ for the absolute value of the generalized inner product of rows i, j, k and ℓ :

$$P_{ijk\ell} = |\sum_{x=1}^{4n} h_{ix} h_{jx} h_{kx} h_{\ell x}|$$

This criterion does not work in the case of Hadamard matrices of order $n = 20$ because it gives the same profile for all three equivalent classes of Hadamard matrices of this order.

Proposition 1 (see [8]) $P_{ijk\ell} \equiv 4n \ (mod \ 8)$.

We shall write $\pi(m)$ for the number of sets $\{i, j, k, \ell\}$ of four distinct rows such that $P_{ijk\ell} = m$. The definition and the above give that $\pi(m) = 0$ unless $m \geq 0$ and $m \equiv 4n \ (mod \ 8)$. We call $\pi(m)$ *the profile* (or 4-profile) of H.

The (unique) matrices of order $4, 8$ and 12 have profiles

$$\pi(4) = 1$$
$$\pi(0) = 56, \quad \pi(8) = 14$$
$$\pi(4) = 495, \quad \pi(12) = 0$$

respectively.

The five inequivalent classes of order 16 gave four distinct profiles.

$$
\begin{aligned}
class\ H_0 : \quad &\pi(0) = 1680, \quad \pi(8) = 0, \quad\ \ \ \pi(16) = 140 \\
class\ H_1 : \quad &\pi(0) = 1488, \quad \pi(8) = 256, \quad \pi(16) = 76 \\
class\ H_2 : \quad &\pi(0) = 1392, \quad \pi(8) = 484, \quad \pi(16) = 44 \\
class\ H_3 : \quad &\pi(0) = 1344, \quad \pi(8) = 448, \quad \pi(16) = 28 \\
class\ H_4 : \quad &\pi(0) = 1344, \quad \pi(8) = 448, \quad \pi(16) = 28
\end{aligned}
$$

The matrices of class H_4 are the transposes of the matrices of class H_3.

The three classes of order 20 all gave the same profile:

$$
\pi(4) = 4560, \ \pi(12) = 285, \pi(20) = 0.
$$

Similarly we can define a more general profile criterion based on more than 4 rows. For some modifications of the profile such as extended profile and generalized profile we refer the reader to [80]. We now give a modified version of the profile that was given in [8]. We observe that all the conditions which hold for the rows of a Hadamard matrix also hold for its columns.

We write $Q(m)$ for the absolute value of the generalized inner product of m columns, say $c_1, c_2, \ldots, c_m$ and we call this m-column profile.

$$
Q(m) = |\sum_{x=1}^{4n} h_{xa_1} h_{xa_2} \cdots h_{xa_m}|
$$

We shall write $q(s)$ for the number of sets $\{a_1, a_2, \ldots, a_m\}$ of m distinct rows such that $Q(m) = s$. The definition and the above give that $q(s) = 0$ unless $s \geq 0$. We call $q(s)$ the m-column profile (or m-cprofile) of H.

This criterion as well does not work in the case of Hadamard matrices of order $n = 16, 20$ because it also gives the same m-cprofile for the last two classes in order 16 and the same m-cprofile for all three equivalent classes of Hadamard matrices of order $n = 20$ for all $1 \leq m \leq n-1$.

Two more useful criterions to determine inequivalence of Hadamard matrices which are called "K-matrices" and "K-boxes" are also developed in [57, 58]. To save space we do not discuss these criteria here.

2.3   The projection and Hamming distance distribution algorithms

In this section we describe two new criteria, to test inequivalence in Hadamard matrices of order n, based on their projection properties and their Hamming distances.

Let H be a $n \times n$ Hadamard matrix. A $n \times k$ submatrix of H which consist of n rows and k columns is called a *projection* of H into k columns. In some statistical applications the rows of H refer to the runs of a factorial experiment and the columns refer to the factors, see [77] or [10].

The projection properties of the 2_R^{q-p} fractional factorials are well known and have been used effectively in a number of published examples of experimental investigations. Here in, we use inequivalent projections of Hadamard matrices to check inequivalent Hadamard matrices. Using this criterion we are able to find all inequivalent projections in k factors as well as to classify Hadamard matrices of that order. As an example we apply this criterion to orders 16 and 20.

The idea of the first criterion is that if two Hadamard matrices of order n are inequivalent then these matrices should have at least one different projection for some $k \leq n$ and vice versa (if there exist a $k \leq n$ such that the two Hadamard matrices give some different, inequivalent projections then these Hadamard matrices are inequivalent). So if we find all projections of a Hadamard matrix of order n we have a bonus. We can decide the equivalence of Hadamard matrices and moreover use the projections for statistical analysis of experiments.

Now we give in brief the description of our algorithm that can be used to determine all inequivalent projections for n and k.

First we give the definition of inequivalent projections of a Hadamard matrix of order n.

Two projections in k factors of Hadamard matrices of order n are *equivalent* if one can be obtained from the other by one or more of the following transformations

(a) Sign changes in the columns (multiply one or more columns by -1).

(b) Permutations of the columns

(c) Rearrangements of the rows.

The next algorithm gives us all the inequivalent projections of Hadamard matrices and through them the inequivalent Hadamard matrices.

The inequivalent projections algorithm:

(i) Set $k = 2$.

(ii) Normalize the Hadamard matrices given by multiplying, whenever this is necessary, any rows or columns by -1. Then remove the first column (with all 1's);

(iii) Find all projections for each Hadamard matrix of a given order n and k factors by taking all possible k columns of the remaining $n \times (n-1)$ matrix. These are $\binom{n-1}{k}$ projections in total.

(iv) From the projections found in step (iii) find the inequivalent ones.

(v) Check if the set of all projections of the first Hadamard matrix is different (inequivalent) from the set of all projections of the second Hadamard matrix.

(vi) If the answer in step (v) is true then stop and say that these two Hadamard matrices are inequivalent, otherwise increase k by 1.

(vii) If now $k \leq n - 1$ then go to step (iii) and continue, otherwise stop and say that these Hadamard matrices are equivalent.

Lemma 8 *When we project a Hadamard matrix of order $4m$ into $k = 2$ columns we always obtain $\binom{4m-1}{2}$ identical projections. Each of these is m times over the full 2^2 design.*

Proof. A Hadamard matrix has its columns orthogonal to each other. Therefore, in any two columns each of the pairs $(1, 1)$, $(1, -1)$, $(-1, 1)$, $(-1, -1)$ appear exactly m times. $\square$

Using the above lemma we can slightly improve this algorithm by not checking the projections in $k = 2$ columns, and starting the algorithm with $k = 3$.

Lemma 9 *Let h_k be a projection, in k factors, of a Hadamard matrix of order n. Then h_k cannot contain a full 2^k design if $k > log_2(n)$.*

Proof. A full 2^k experimental design has 2^k rows. A Hadamard matrix of order n has n rows. So if $2^k > n$ there cannot be a full 2^k design in a k column projection of this Hadamard matrix. We have that
$$2^k > n \implies k \cdot log_2(2) > log_2(n) \implies k > log_2(n).$$
Now if k is not an integer we take the next integer number. Thus, if k is not an integer we have that $k \geq [log_2(n)] + 1$. □

Corollary 5 *For a Hadamard matrix of order n we have that if $2^m < n \leq 2^{m+1}$ then $k \geq m+1$.*

Proof. We know that *log* function is continuous and increasing function. Since $log_2(2^m) = m$, we have that if $2^m < n \leq 2^{m+1}$ then $m < log_2(n) \leq m + 1$ and so $k \geq m + 1$. □

Theorem 17 *Let H_1, H_2 be two inequivalent Hadamard matrices of order n. The first Hadamard matrix H_1 will give at least one projection different (inequivalent) from all the projections of H_2 for some $k > log_2(n)$.*

Proof. The result follows from lemma 9. □

Example 8 We give some orders of Hadamard matrices and the bound for k.

- For $n = 2^m$ we obtain $k \geq m$.

- For $n = 12$ we obtain $k \geq 4$.

- For $n = 20$ we obtain $k \geq 5$.

- For $n = 24$ we obtain $k \geq 5$.

- For $n = 28$ we obtain $k \geq 5$.

Theorem 18 *If two Hadamard are equivalent then their projections for all $k = 2, 3, \ldots, n - 1$ are equivalent as well.*

Proof. Suppose that H_1 and H_2 are two equivalent Hadamard matrices of order n. Then, for a given k, both of them have $\binom{n-1}{k}$ projections in total. The equivalence of the Hadamard matrices indicates that each projection of the first Hadamard matrix is equivalent with one projection of the second Hadamard matrix and vice versa. □

We will now discuss the complexity of the first new algorithm. First, we observe that the total number of all possible projections of a Hadamard matrix of order n in k factors is $\binom{n-1}{k}$. We note that the finding the inequivalent projections by applying the definition of inequivalent projections is computationally-intensive. This is an NP hard problem when n and k increase. The sign changes in the columns (multiply one or more columns by -1) required 2^k possible multiplications. The permutations of the columns and rearrangements of the rows need $k!$

possible permutations. That is in total we have $2^k \cdot k! \cdot \binom{n-1}{k}$ cases to check and that's a large complexity when k increases. So, if we are not interested in finding all inequivalent projections of Hadamard matrices we can apply the following algorithm which uses all projections and the Hamming distance distribution. The *Hamming distance distribution* is defined to be

$$W(x) = a_0 + a_1 x^1 + \ldots + a_k x^k$$

where a_m is the number describing how many pairs of runs of the projection have distance m.

Example 9 Consider the projections for $k = 3$ and $n = 8$. We first normalize the Hadamard matrix of order 8 so it's first column is all 1s. We then remove the first column so we have the 8×7 matrix

$$
\begin{array}{rrrrrrr}
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1 \\
1 & -1 & -1 & -1 & 1 & 1 & -1 \\
1 & -1 & 1 & -1 & -1 & -1 & 1 \\
-1 & 1 & 1 & -1 & 1 & -1 & -1 \\
-1 & 1 & -1 & -1 & -1 & 1 & 1 \\
-1 & -1 & 1 & 1 & -1 & 1 & -1 \\
-1 & -1 & -1 & 1 & 1 & -1 & 1 \\
\end{array}
$$

Since $k = 3$ the projections are all possible 3-sets of columns. We will just illustrate with the sets of columns (factors) 1, 2, 3 and 1, 2, 4.

$$
\begin{array}{rrr}
1 & 1 & 1 \\
1 & 1 & -1 \\
1 & -1 & -1 \\
1 & -1 & 1 \\
-1 & 1 & 1 \\
-1 & 1 & -1 \\
-1 & -1 & 1 \\
-1 & -1 & -1 \\
\end{array}
\quad \text{and} \quad
\begin{array}{rrr}
1 & 1 & 1 \\
1 & 1 & 1 \\
1 & -1 & -1 \\
1 & -1 & -1 \\
-1 & 1 & -1 \\
-1 & 1 & -1 \\
-1 & -1 & 1 \\
-1 & -1 & 1 \\
\end{array}
$$

We now consider the distance between all pairs of rows (runs) of these 8×3 matrices. The first set has distance 3 (4 times), 2 (12 times) and 1 (12 times) so its Hamming distance distribution is

$$W(x) = 0 + 12x + 12x^2 + 4x^3,$$

while the second sets has 0 (4 times) and 2 (24 times) so its Hamming distance distribution is

$$W(x) = 4 + 24x^2.$$

$\square$

Lemma 10 *Two equivalent projections have the same Hamming distance distribution.*

Proof. Let $P_a = \{a_1, a_2, \ldots, a_k\}, P_b = \{b_1, b_2, \ldots, b_k\}$ be two runs in a given projection in k factors. The result follows from the fact that the Hamming distance of these two runs is not affected if we apply some sign changes to factors or exchange the runs or factors. $\square$

28

The modified algorithm (Hamming distance distribution algorithm) is much faster than the previous algorithm as it only gives us an answer to the question "are the two Hadamard matrices are equivalent or not". It does not not give us all inequivalent projections of the Hadamard matrices.

The Hamming distance distribution algorithm:

(i) Set $k = 2$.

(ii) Normalize the Hadamard matrices given by multiplying, whenever this is necessary, any rows or columns by -1. Then remove the first column (with all 1's);

(iii) Find all projections for each Hadamard matrix of a given order n and k factors by taking all possible k columns of the remaining $n \times (n-1)$ matrix. There are $\binom{n-1}{k}$ projections in total.

(iv) In the projections found in step (iii) calculate the Hamming distance distributions for any two runs (rows) of the projection. There are $\binom{n-1}{2}$ Hamming distance distributions. Save the different Hamming distance distributions and how many times each of them appears.

(v) Check if the set of all different Hamming distance distributions of the first Hadamard matrix is the same with the set of all different Hamming distance distributions of the second Hadamard matrix.

(vi) If the answer in step (v) is false, then stop and say that these two Hadamard matrices are inequivalent, otherwise increase k by 1.

(vii) If now $k \leq n-1$ then go to step (iii) and continue, otherwise stop and say that these Hadamard matrices are equivalent.

Let us discuss the complexity of the Hamming distance distribution algorithm. First, we observe again that all possible projections in k factors of a Hadamard matrix of order n is $\binom{n-1}{k}$. We note that finding the Hamming distance distribution of all projections is not computationally-intensive. It needs only $n(n-1)$ calculations. A calculation of the Hamming distance of two runs in a projection takes k comparisons and thus we have in total $\binom{n-1}{k} n(n-1)k$ multiplications, summations and comparisons. This is not an NP hard problem when n and k increase but polynomial in n^{k+2}. It is much faster than the inequivalent projections algorithm.

2.4 Application of the new criterion to Hadamard matrices of small orders

In this section we apply our new algorithm to the cases of Hadamard matrices of small orders. As we can see from the next tables when the Hadamard matrices are equivalent we have to check the Hamming distance distributions for all projections into $k = 2, \ldots, n-1$ factors. If the Hadamard matrices are inequivalent there exist $k \in \{2, 3, \ldots, n-1\}$ such that the Hamming distance distributions for the projections in k factors are different for each Hadamard matrix.

To save space, we give here the table with Hamming distance distribution only for orders $4, 8, 12$. For larger orders the reader should consider [23].

2.4.1 Hadamard matrices of order $n = 4, 8, 12$

We know that there exists only one Hadamard matrix of these orders up to equivalence, see [9] for example. The results of the application of the Hamming distance distribution algorithm for these orders are given in Table 1. Since there is only one Hadamard matrix in each case the criterion needs to test Hamming distance distributions for all projections into $k = 2, \ldots, n-1$ factors. In Table 1 the word "times" is used to show the number of times that the given Hamming distance distribution occurs in the projections. For example there are $\binom{7}{3} = 35$ projections in a Hadamard matrix of order $n = 8$ in $k = 3$ factors and $\binom{8}{2} = 28$ Hamming weights in each Hamming distance distribution of each projection.

When we say that the Hamming distance distribution is $0, 12, 12, 4$ and times 28 that means that there are 0 pairs of runs in the projection with Hamming distance 0, 12 pairs of runs in the projection with Hamming distance 1, 12 pairs of runs in the projection with Hamming distance 2 and 4 pairs of runs in the projection with Hamming distance 3. This distribution occurs for 28 of the 35 projections.

When we say that the Hamming distance distribution is $4, 0, 24, 0$ and times 7 that means that there are 4 pairs of runs in the projection with Hamming distance 0, 0 pairs of runs in the projection with Hamming distance 1 and 24 pairs of runs in the projection with Hamming distance 2, 0 pairs of runs in the projection with Hamming distance 2. This distribution occurs for 7 of the 35 projections.

As you can see the total number of Hamming distance (the sum of all Hamming distances in the Hamming distance distribution) is $\binom{8}{2} = 28$ and the total number of times each distribution occurs (the sum of all different Hamming distance distributions) is $\binom{7}{3} = 35$.

2.4.2 Hadamard matrices of order $n = 16$

We know that there are exactly five inequivalent Hadamard matrices of this order, see [46]. The results of the application of the Hamming distance distribution algorithm for this order are given in [23]. Observe that for $k = 2$ the Hamming distance distributions of all projections of all five matrices are exactly the same. For $k = 3$ we have four different Hamming distance distributions (thus four inequivalent Hadamard matrices) and we have to go up to $k = 6$ to obtain all five of them.

2.4.3 Hadamard matrices of order $n = 20$

We know that there are exactly three inequivalent Hadamard matrices of this order, see [47]. The results of the application of the Hamming distance distribution algorithm for this order are given in [23]. Observe that for $k = 2, 3, 4$ the Hamming distance distributions of all projections of all three matrices are exactly the same. For $k = 5$ we have all three different Hamming distance distributions and thus we obtain all three of the inequivalent Hadamard matrices.

2.5 Inequivalent Hadamard matrices

2.5.1 Hadamard matrices of order $n = 24$

We know that there are exactly 60 inequivalent Hadamard matrices of this order, see [54, 59]. For Hadamard matrices of order 24 it is not convenient to give all different Hamming distance

H_{name}	n	k	Hamming distance	times
H_4	4	2	0,4,2	3
H_4	4	3	0,0,6	1
H_8	8	2	4,16,8	21
H_8	8	3	0,12,12,4	28
H_8	8	3	4,0,24,0	7
H_8	8	4	0,0,24,0,4	7
H_8	8	4	0,4,12,12,0	28
H_8	8	5	0,0,8,16,4,0	21
H_8	8	6	0,0,0,16,12,0,0	7
H_8	8	7	0,0,0,0,28,0,0,0	1
H_{12}	12	2	12,36,18	55
H_{12}	12	3	4,24,30,8	165
H_{12}	12	4	1,12,30,20,3	330
H_{12}	12	5	0,5,20,30,10,1	396
H_{12}	12	5	1,0,30,20,15,0	66
H_{12}	12	6	0,0,15,20,30,0,1	66
H_{12}	12	6	0,1,10,30,20,5,0	396
H_{12}	12	7	0,0,3,20,30,12,1,0	330
H_{12}	12	8	0,0,0,8,30,24,4,0,0	165
H_{12}	12	9	0,0,0,0,18,36,12,0,0,0	55
H_{12}	12	10	0,0,0,0,0,36,30,0,0,0,0	11
H_{12}	12	11	0,0,0,0,0,0,66,0,0,0,0,0	1

Table 1: Application of Hamming distance distribution algorithm for $n = 4, 8, 12$

distributions for all k. We shall only discuss the results our algorithm gives. The algorithm moves to $k = 3$ and finds 31 different Hamming distance distributions and thus 31 of the sixty inequivalent Hadamard matrices. Then for $k = 4$ we obtain 42 different Hamming distance distributions and thus 42 of the sixty inequivalent Hadamard matrices. Finally for $k = 5$ we obtain 60 different Hamming distance distributions and thus all 60 of the inequivalent Hadamard matrices. For more details in this order the reader should consider [23].

2.5.2 Hadamard matrices of order $n = 28$

In the case $n = 28$ there are 487 inequivalent Hadamard matrices, see [60, 61]. If we apply our algorithm to this case we obtain the following results. The algorithm moves to $k = 3$ and finds 17 different Hamming distance distributions and thus 17 of the 487 inequivalent Hadamard matrices. Then for $k = 4$ we obtain 216 different Hamming distance distributions and thus 216 of the 487 inequivalent Hadamard matrices. Finally for $k = 5$ we obtain 487 different Hamming distance distributions and thus all 487 of the inequivalent Hadamard matrices. For more details in this order the reader should consider [23].

2.5.3 Hadamard matrices of order 32

The classification of Hadamard matrices of orders $n \geq 32$ is still remains an open and difficult problem since an algorithmic approach using an exhaustive search is an NP hard problem. In particular, in this case, Lin, Wallis and Zhu [79] found 66104 inequivalent Hadamard matrices of order 32. Extensive results appear in [82] and [83]. Thus the lower bound for inequivalent Hadamard matrices of order 32 is 66104.

2.5.4 Hadamard matrices of order 36

There are at least 762 inequivalent Hadamard matrices of order 36. In fact this number is obtained as follows: Seberry's home page http://www.uow. edu.au/∼jennie gives 192 inequivalent Hadamard matrices of order 36. These are supplied by E. Spence (180 matrices) see [91], Z. Janko, (1 matrix of Bush-type) see [55] and V. D. Tonchev (11 matrices) see [95]. Using an efficient algorithm Georgiou and Koukouvinos [24] found that 190 of their transposes, are inequivalent to these. This was also confirmed in [16]. Georgiou and Koukouvinos in [24] improved further this bound to 762 by constructing 380 new Hadamard matrices of order 36.

2.5.5 Hadamard matrices of order 40

Lam, Lam and Tonchev [76] showed that the lower bound for inequivalent Hadamard matrices of order 40 is 3.66×10^{11}.

2.5.6 Hadamard matrices of order 44

Recently Topalova [96] classified the Hadamard matrices of order 44 with an automorphism of order 7, and found 384 inequivalent Hadamard matrices of this order. Georgiou and Koukouvinos in [25] further improved this lower bound to 2507 by constructing 2123 new Hadamard matrices.

3 Algorithms for constructing orthogonal designs

3.1 Basic definitions and preliminaries

An *orthogonal design* of order n and type $(s_1, s_2, \ldots, s_u)$ $(s_i > 0)$, denoted $OD(n; s_1, s_2, \ldots, s_u)$, on the commuting variables $x_1, x_2, \ldots, x_u$ is an $n \times n$ matrix A with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ such that

$$AA^T = (\sum_{i=1}^{u} s_i x_i^2) I_n.$$

Alternatively, the rows of A are formally orthogonal and each row has precisely s_i entries of the type $\pm x_i$. In [33], where this was first defined, it was mentioned that

$$A^T A = (\sum_{i=1}^{u} s_i x_i^2) I_n$$

and so our alternative description of A applies equally well to the columns of A. It was also shown in [33] that $u \leq \rho(n)$, where $\rho(n)$ (Radon's function) is defined by $\rho(n) = 8c + 2^d$, when $n = 2^a b$, b odd, $a = 4c + d$, $0 \leq d < 4$.

Some small orthogonal designs are given in the following example, see [88].

Example 10 Some small orthogonal designs.

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

$$
OD(2;1,1) \quad OD(4;1,1,1,1) \qquad OD(4;1,1,2) \qquad OD(4;1,1)
$$

$OD(4;1,1,1,1)$ is the Williamson array. $\qquad\square$

A weighing matrix $W = W(n,k)$ is a square matrix with entries $0, \pm 1$ having k non-zero entries per row and column and inner product of distinct rows zero. Hence W satisfies $WW^T = kI_n$, and W is equivalent to an orthogonal design $OD(n;k)$. The number k is called the *weight* of W.

We make extensive use of the book of Geramita and Seberry [37]. We quote the following theorems, giving their reference from the aforementioned book, that we use:

Lemma 11 [37, Lemma 4.11, The Doubling Lemma] *If there exists an orthogonal design* $OD(n; s_1, s_2, \ldots, s_u)$ *then there exists an orthogonal design* $OD(2n; s_1, s_1, es_2, \ldots, es_u)$ *where* $e = 1$ *or* 2. $\qquad\square$

Lemma 12 [37, Lemma 4.4, The Equating and Killing Lemma] *If A is an orthogonal design* $OD(n; s_1, s_2, \ldots, s_u)$ *on the commuting variables* $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ *then there is an orthogonal design* $OD(n; s_1, s_2, \ldots, s_i + s_j, \ldots, s_u)$ *and* $OD(n; s_1, s_2, \ldots, s_{j-1}, s_{j+1}, \ldots, s_u)$ *on the $u-1$ commuting variables* $\{0, \pm x_1, \pm x_2, \ldots, \pm x_{j-1}, \pm x_{j+1}, \ldots, \pm x_u\}$. $\qquad\square$

Theorem 19 [37, Theorems 2.19 and 2.20] *Suppose $n \equiv 0 (mod\ 4)$. Then the existence of a $W(n, n-1)$ implies the existence of a skew-symmetric $W(n, n-1)$. The existence of a skew-symmetric $W(n,k)$ is equivalent to the existence of an $OD(n; 1, k)$.* $\qquad\square$

Theorem 20 [37, Proposition 3.54 and Theorem 2.20] *An orthogonal design $OD(n; 1, k)$ can only exist in order $n \equiv 4(mod\ 8)$ if k is the sum of three squares. An orthogonal design $OD(n; 1, n-2)$ can only exist in order $n \equiv 4(mod\ 8)$ if $n-2$ is the sum of two squares.* $\qquad\square$

Theorem 21 [37, Theorem 4.49] *Suppose there exist four circulant matrices A, B, C, D of order n satisfying*

$$
AA^T + BB^T + CC^T + DD^T = fI_n
$$

Let R be the back diagonal matrix. Then

$$
GS = \begin{pmatrix}
A & BR & CR & DR \\
-BR & A & D^T R & -C^T R \\
-CR & -D^T R & A & B^T R \\
-DR & C^T R & -B^T R & A
\end{pmatrix}
$$

is a $W(4n, f)$ when A, B, C, D are $(0, 1, -1)$ matrices, and an orthogonal design $OD(4n; s_1, s_2, \ldots, s_u)$ on $x_1, x_2, \ldots, x_u$ when A, B, C, D have entries from $\{0, \pm x_1, \ldots, \pm x_u\}$ and $f = \sum_{j=1}^{u}(s_j x_j^2)$. $\qquad\square$

Corollary 6 *If there are four sequences A, B, C, D of length n with entries from $\{0, \pm x_1, \pm x_2, \pm x_3, \pm x_4\}$ with zero periodic or non-periodic autocorrelation function, then these sequences can be used as the first rows of circulant matrices which can be used in the Goethals-Seidel array to form an $OD(4n; s_1, s_2, s_3, s_4)$. We note that if there are sequences of length n with zero non-periodic autocorrelation function, then there are sequences of length $n + m$ for all $m \geq 0$.* □

3.2   Construction algorithms

In this section we are interested in the construction of orthogonal designs using four circulant matrices in the Goethals-Seidel array. Specifically, for positive integers $s_1, s_2, \ldots, s_u$ and odd n, the method searches for four circulant matrices A_1, A_2, A_3, A_4 or order n with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$, $u \leq 4$, such that

$$A_1 A_1^T + A_2 A_2^T + A_3 A_3^T + A_4 A_4^T = \left(\sum_{i=1}^{u} s_i x_i^2 \right) I_n. \tag{29}$$

In the remainder of this section, when four circulant (or group circulant) matrices of order n, with entries from the set $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$, satisfy equation (29) will be said that these matrices satisfy the *additive property*.

3.2.1   The matrix based algorithm

Suppose the row and column sum of A_i is

$$r_i = p_{1i} x_1 + p_{2i} x_2 + p_{3i} x_3 + p_{4i} x_4, \quad i = 1, 2, 3, 4$$

Let e^T be the $1 \times n$ vector of 1's, then $e^T A_i = r_i e^T$. Multiplying on the left of (29) by e^T and the right of (29) by e we have

$$\sum_{i=1}^{4} (e^T A_i)(e^T A_i)^T = n \sum_{i=1}^{4} s_i x_i^2$$

or

$$\sum_{i=1}^{4} (r_i e^T)(r_i e^T)^T = n \sum_{i=1}^{4} r_i^2 = n \sum_{i=1}^{4} s_i x_i^2$$

Thus we have

$$
\begin{aligned}
s_1 x_1^2 + s_2 x_2^2 + s_3 x_3^2 + s_4 x_4^2 = \quad & x_1^2 \sum_{i=1}^{4} p_{1i}^2 + x_2^2 \sum_{i=1}^{4} p_{2i}^2 + x_3^2 \sum_{i=1}^{4} p_{3i}^2 \\
& + x_4^2 \sum_{i=1}^{4} p_{4i}^2 + 2 x_1 x_2 \sum_{i=1}^{4} p_{1i} p_{2i} \\
& + 2 x_1 x_3 \sum_{i=1}^{4} p_{1i} p_{3i} + 2 x_1 x_4 \sum_{i=1}^{4} p_{1i} p_{4i} \\
& + 2 x_2 x_3 \sum_{i=1}^{4} p_{2i} p_{3i} + 2 x_2 x_4 \sum_{i=1}^{4} p_{2i} p_{4i} \\
& + 2 x_3 x_4 \sum_{i=1}^{4} p_{3i} p_{4i}
\end{aligned}
$$

Hence we have four integer vectors $p_1^T = (p_{11}, p_{12}, p_{13}, p_{14})$, $p_2^T = (p_{21}, p_{22}, p_{23}, p_{24})$, $p_3^T = (p_{31}, p_{32}, p_{33}, p_{34})$, $p_4^T = (p_{41}, p_{42}, p_{43}, p_{44})$, which are pairwise orthogonal. Also $|p_1^T|^2 = s_1$, $|p_2^T|^2 = s_2$, $|p_3^T|^2 = s_3$, $|p_4^T|^2 = s_4$.

Form these vectors into an orthogonal integer matrix P with $P^T = (p_1, p_2, p_3, p_4)$. Then $PP^T = diag\,(s_1, s_2, s_3, s_4)$ and $det\,P = \sqrt{s_1 s_2 s_3 s_4}$. But P is integer so $s_1 s_2 s_3 s_4$ is a square. Thus we have

Lemma 13 *The Goethals-Seidel construction for an orthogonal design $OD\,(4n; s_1, s_2, s_3, s_4)$ can only be used if*

(i) there is an integer matrix P satisfying $PP^T = diag\,(s_1, s_2, s_3, s_4)$ and hence

(ii) $s_1 s_2 s_3 s_4$ is a square. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Since the row sum of A_j is $\sum_{i=1}^{4} p_{ij} x_i$ for $1 \leq j \leq 4$, the 4×4 matrix $P = (p_{ij})$ is called the *sum matrix* of A_1, A_2, A_3, A_4.

In this section we are interested in the construction of orthogonal designs using four circulant matrices in the Gorthals-Seidel array. Specifically, for positive integers $s_1, s_2, \ldots, s_u$ and odd n, the method searches for four circulant matrices A_1, A_2, A_3, A_4 or order n with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ that satisfy equation (29).

Definition 3 *If A_1, A_2, A_3, A_4 are $n \times n$ circulant matrices with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ and the first row of A_j has m_{ij} entries of the kind $\pm x_i$, then the $u \times 4$ matrix $M = (m_{ij})$ is called the* entry matrix *of (A_1, A_2, A_3, A_4).* $\qquad\qquad$ □

The elements of the entry matrices satisfy the following conditions.

$$\sum_{j=1}^{4} m_{ij} = s_i \quad \text{for} \quad 1 \leq i \leq u$$
$$\sum_{i=1}^{u} m_{ij} \leq n \quad \text{for} \quad 1 \leq j \leq 4$$

(30)

Thus the rows of the entry matrices refer to the variables x_i and the columns to the circulant matrices A_1, A_2, A_3, A_4 which are constructed from four sequences of length n as described in Corollary 6.

Definition 4 Suppose that the row sum of A_j is $\sum_{i=1}^{u} p_{ij} x_i$ for $1 \leq j \leq 4$. Then the $u \times 4$ integral matrix $P = (p_{ij})$ is called the *sum matrix* of (A_1, A_2, A_3, A_4). The *fill matrix* of (A_1, A_2, A_3, A_4) is $M - abs(P)$, where $abs(P)$ denotes the matrix having as elements the absolute values of elements of P. The content of A_i is determined by the i-th columns of the sum and fill matrices. □

The following theorem may be used to find the sum matrix of a solution of (29).

Theorem 22 (Eades Sum Matrix Theorem) The sum matrix P of a solution of (29) satisfies $PP^T = diag(s_1, s_2, \ldots, s_u)$. □

The algorithm

Step 1. Find all sum matrices P of the desirable orthogonal design using theorem 22.

Step 2. Select the first sum matrix.

Step 3. For the selected sum matrix P find all entry matrices M and the corresponding fill matrices (Q=M-abs(P)) using equations given by (30).

Step 4. Select the first entry matrix M and the corresponding fill matrix Q.

Step 5. Using P, M and Q write down the elements of sequences A_j, $j = 1, 2, 3, 4$.

Step 6. Construct all possible sequences A_j with entries we found in Step 5 and their corresponding PAF.

Step 7a. Combine the lists find in Step 6 and check if a combination gives zero PAF and if so save these sequences into PAF solution file.

Step 7b. If a zero PAF solution exist then search if some permutation of these sequences have zero NPAF and if so save these sequences into NPAF solution file.

Step 8. If there are more entry matrices then select the next entry matrix M and the corresponding fill matrix Q and go to Step 5.

Step 9. If there are more sum matrices then select the next sum matrix P and go to Step 3.

For more details about the construction of orthogonal designs which uses entry matrices, see [37].

3.2.2   The extension algorithm

This algorithm extents already known orthogonal designs on t variables into new orthogonal designs on $t + 1$ variables. The algorithm is given briefly in the next steps.

Step 1. Input the sequences of the known orthogonal design $OD(4n; s_1, \ldots, s_t)$ on t variables $(a_1, a_2, \ldots, a_t)$, you wish to extent.

Step 2. In these sequences replace all zeros with variables x_i (a deferent variable on each zero).

Step 3. Using the new sequences and the equation

$$P_{A_1}(s) + P_{A_2}(s) + P_{A_3}(s) + P_{A_4}(s) = 0, \quad s = 1, 2, \ldots, \frac{(n-1)}{2}$$

create a system of equations.

Step 4. Solve this system ofequations and find all possible values x_i, where $x_i \in \{-1, 0, 1\}$, that satisfy equations given in Step 3.

Step 5. For all solutions, diferent from the zero solution, (of weight $k \neq 0$) replace ± 1 by $\pm a_{t+1}$ respectively and obtain the $OD(4n; s_1, \ldots, s_t, k)$ on $t + 1$ variables $(a_1, a_2, \ldots, a_t, a_{t+1})$.

Then next example illustrates how this algorithm works.

Example 11 Start with the four sequences of length 9 and type $(5, 9)$ with $NPAF = 0$ (Step 1).

$$
\begin{array}{ccccccccc}
b & 0 & -b & 0 & 0 & 0 & 0 & 0 & 0 \\
b & a & -b & 0 & 0 & 0 & 0 & 0 & 0 \\
b & a & 0 & a & -b & 0 & 0 & 0 & 0 \\
b & a & b & -a & b & 0 & 0 & 0 & 0
\end{array}
$$

Now fill each zero position with one of the 22 variables $x_1, x_2, \ldots, x_{22}$ (Step 2). Thus we obtain

$$
\begin{array}{ccccccccc}
b & x_1 & -b & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\
b & a & -b & x_8 & x_9 & x_{10} & x_{11} & x_{12} & x_{13} \\
b & a & x_{14} & a & -b & x_{15} & x_{16} & x_{17} & x_{18} \\
b & a & b & -a & b & x_{19} & x_{20} & x_{21} & x_{22}
\end{array}
$$

Using relations

$$P_{A_1}(s) + P_{A_2}(s) + P_{A_3}(s) + P_{A_4}(s) = 0, \quad s = 1, 2, \ldots, \frac{(n-1)}{2}$$

we construct the following twelve equations (Step 3):

$$2x_{14} = 0$$
$$x_7 - x_2 + x_{13} - x_8 + x_{18} - x_{15} + x_{22} + x_{19} = 0$$
$$x_3x_2 + x_4x_3 + x_5x_4 + x_6x_5 + x_7x_6 + x_9x_8 + x_{10}x_9 + x_{11}x_{10} + x_{12}x_{11} + x_{13}x_{12} + x_{16}x_{15}$$
$$+ x_{17}x_{16} + x_{18}x_{17} + x_{20}x_{19} + x_{21}x_{20} + x_{22}x_{21} = 0$$
$$x_{13} + x_8 + x_{18} + x_{15} + x_{22} - x_{19} = 0$$
$$x_6 - x_3 + x_{12} - x_9 + x_{17} - x_{16} + x_{21} + x_{20} = 0$$
$$x_1x_7 + x_2x_1 + x_4x_2 + x_5x_3 + x_6x_4 + x_7x_5 + x_{10}x_8 + x_{11}x_9 + x_{12}x_{10} + x_{13}x_{11} + x_{17}x_{15}$$
$$+ x_{18}x_{16} + x_{21}x_{19} + x_{22}x_{20} = 0$$
$$x_{12} + x_9 + x_{17} + x_{16} + x_{21} - x_{20} = 0$$
$$x_5 - x_7 + x_2 - x_4 + x_{11} - x_{13} + x_8 - x_{10} + x_{16} - x_{17} + x_{20} + x_{22} + x_{19} + x_{21} = 0$$
$$x_1x_6 + x_3x_1 + x_5x_2 + x_6x_3 + x_7x_4 + x_{11}x_8 + x_{12}x_9 + x_{13}x_{10} + x_{14}x_{18} + x_{15}x_{14} + x_{18}x_{15}$$
$$+ x_{22}x_{19} = 0$$
$$x_{11} + x_{10} + x_{16} + x_{18} + x_{15} + x_{17} + x_{20} - x_{22} + x_{19} - x_{21} = 0$$
$$x_4 - x_6 + x_3 - x_5 + x_{10} - x_{12} + x_9 - x_{11} + x_{15} - x_{18} + x_{19} + x_{21} + x_{20} + x_{22} = 0$$
$$x_1x_5 + x_2x_7 + x_4x_1 + x_6x_2 + x_7x_3 + x_8x_{13} + x_{12}x_8 + x_{13}x_9 + x_{14}x_{17} + x_{16}x_{14} = 0$$

By solving this system of equations (Step 4) we find, among others, the following solutions of weight $9, 14, 16$:

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}
0	-1	0	0	0	0	-1	-1	-1	0	-1	1	0
0	-1	-1	-1	0	-1	1	0	-1	0	1	-1	-1
0	-1	-1	-1	-1	-1	1	1	-1	0	0	1	-1

x_{14}	x_{15}	x_{16}	x_{17}	x_{18}	x_{19}	x_{20}	x_{21}	x_{22}
0	1	1	-1	0	0	0	0	0
0	1	0	1	-1	0	-1	0	1
0	1	0	0	-1	1	-1	-1	1

The first one gives the orthogonal design of order 36 on three variables, $OD(36; 5, 9, 9)$ (Step 5, by replacing ± 1 by $\pm c$ respectively).

$$(5, 9, 9)$$

b	0	$-b$	$-c$	0	0	0	0	$-c$
b	a	$-b$	$-c$	$-c$	0	$-c$	c	0
b	a	0	a	$-b$	c	c	$-c$	0
b	a	b	$-a$	b	0	0	0	0

The second one gives the orthogonal design of order 36 on three variables, $OD(36; 5, 9, 14)$ (Step 5, by replacing ± 1 by $\pm c$ respectively).

$$(5, 9, 14)$$

b	0	$-b$	$-c$	$-c$	$-c$	0	$-c$	c
b	a	$-b$	0	$-c$	0	c	$-c$	$-c$
b	a	0	a	$-b$	c	0	c	$-c$
b	a	b	$-a$	b	0	$-c$	0	c

The third one gives the orthogonal design of order 36 on three variables, $OD(36; 5, 9, 16)$ (Step 5, by replacing ± 1 by $\pm c$ respectively).

$$
\begin{array}{ccccccccc}
 & & & & \overset{(5,9,16)}{} & & & & \\
b & 0 & -b & -c & -c & -c & -c & -c & c \\
b & a & -b & c & -c & 0 & 0 & c & -c \\
b & a & 0 & a & -b & c & 0 & 0 & -c \\
b & a & b & -a & b & c & -c & -c & c
\end{array}
$$

3.2.3 The merge algorithm

This algorithm relies on the two previously mentioned algorithms (the matrix based algorithm and the extension algorithm) given in [14, 37, 67] and in [27, 66] respectively.

The merge algorithm combines features of both algorithms with a new result given here to obtain a new, much faster, algorithm. It is an exhaustive search algorithm (i.e. if the orthogonal design exists it will be found otherwise it does not exist constructed from four sequences).

Notation 1 For the remainder of this section we use the following notations.

1. $\mathcal{N}$ denotes the set of non negative integers.

2. $\mathcal{N}^k$ denotes the space $\mathcal{N}^k = \underbrace{\mathcal{N} \times \mathcal{N} \times \cdots \times \mathcal{N}}_{k\ times}$ with elements

$$
\mathbf{v} \in \mathcal{N}^k, \ \mathbf{v^T} = [v_1, v_2, \ldots, v_k], \ v_i \in \mathcal{N}, \ i = 1, 2, \ldots, k.
$$

3. $\mathcal{N}^{k \times \ell}$ will be the matrix space with dimension $k \times \ell$ and elements from $\mathcal{N}$. That is if $M \in \mathcal{N}^{k \times \ell}$ then

$$
M = \begin{bmatrix} m_{11} & m_{12} & \ldots & m_{1\ell} \\ m_{21} & m_{22} & \ldots & m_{2\ell} \\ \vdots & \vdots & & \vdots \\ m_{k1} & m_{k2} & \ldots & m_{k\ell} \end{bmatrix} = \begin{bmatrix} \mathbf{m_1^T} \\ \mathbf{m_2^T} \\ \vdots \\ \mathbf{m_k^T} \end{bmatrix}
$$

with $m_{ij} \in \mathcal{N}$, $\mathbf{m_i} \in \mathcal{N}^\ell$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, \ell$. □

Let D be an $OD(4n; u_1, u_2, \ldots, u_t)$ with entries from the set $\{0, \pm x_1, \pm x_2, \ldots, \pm x_t\}$ where $x_1, x_2, \ldots, x_t$ are commuting variables. Using the terminology of [37], the symbols M_i represent the non-isomorphic *entry matrices* of the orthogonal design.

¿From the above construction of the sequences, we observe that we can permute rows and/or columns of the sum matrix P and the entry matrix M without obtaining an essentially different sum or entry matrix. It would be as though we interchanged the variables and/or the sequences of the orthogonal design. When we form the content of the sequences, we should take into account that the row and column order of the sum and the entry matrices must agree. That is to say that the same permutations of rows and/or columns should be operated to both these matrices. In the same way, we can multiply by -1 any rows and/or columns of the sum matrix P without obtaining an essentially different sum matrix.

Herein (because we use many non-isomorphic entry matrices from different orthogonal designs) we will use the *type* of the orthogonal design in the symbol of the entry matrices, so that

seeing the entry matrix we can tell from which orthogonal design it comes. For D we will write $M_{(u_1, u_2, \ldots, u_t), i}$ for its non-isomorphic entry matrices. Then we can write the entry matrices using their rows as follows

$$
M_{(u_1, u_2, \ldots, u_t), i} = \begin{bmatrix} \mathbf{v_1^T} \\ \mathbf{v_2^T} \\ \vdots \\ \mathbf{v_t^T} \end{bmatrix} \in \mathcal{N}^{t \times 4}, \ \mathbf{v_j} \in \mathcal{N}^4, \ j = 1, 2, \ldots, t.
$$

Let $\mathcal{D}_{(u_1, u_2, \ldots, u_t)}$ be the set of all non isomorphic entry matrices of the orthogonal design $OD(4n; u_1, u_2, \ldots, u_t)$. We will write $M_{(u_1, u_2, \ldots, u_t), i}\big|_{\mathcal{D}_{u_k, u_j}}$ for the entry matrix $M_{(u_1, u_2, \ldots, u_t), i}$ after we eliminate all rows except from rows k and j. That is

$$
M_{(u_1, u_2, \ldots, u_t), i}\big|_{\mathcal{D}_{u_k, u_j}} = \begin{bmatrix} \mathbf{v_k^T} \\ \\ \mathbf{v_j^T} \end{bmatrix} \in \mathcal{N}^{2 \times 4}.
$$

In order to illustrate the above notations and definitions we give the following example.

Example 12 Suppose we are searching for the $OD(4n; u_1, u_2, u_3, u_4) = OD(20; 2, 3, 6, 9)$. There is up to isomorphism only one sum matrix

$$
P = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ -1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}
$$

satisfying $PP^T = diag(2, 3, 6, 9)$ as described in Theorem 22. ¿From this matrix P we obtain the following three non-isomorphic entry matrices.

$$
M_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 3 & 1 & 2 & 0 \\ 0 & 2 & 2 & 5 \end{bmatrix}, \ M_2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 4 & 0 \\ 2 & 2 & 0 & 5 \end{bmatrix}, \ M_3 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 3 \end{bmatrix}.
$$

Using our terminology these are:

$$
M_{(u_1, u_2, u_3, u_4), 1} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 3 & 1 & 2 & 0 \\ 0 & 2 & 2 & 5 \end{bmatrix}, \quad M_{(u_1, u_2, u_3, u_4), 2} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 4 & 0 \\ 2 & 2 & 0 & 5 \end{bmatrix},
$$

$$
M_{(u_1, u_2, u_3, u_4), 3} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 3 \end{bmatrix}.
$$

With this terminology we can easily see that by setting the first variable equal to zero (i.e. eliminating the first row $\mathbf{v_1^T}$) in the above entry matrices, we obtain the following entry matrices

of an orthogonal design $OD(20; 3, 6, 9)$:

$$M_{(u_2,u_3,u_4),1} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 3 & 1 & 2 & 0 \\ 0 & 2 & 2 & 5 \end{bmatrix}, M_{(u_2,u_3,u_4),2} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 4 & 0 \\ 2 & 2 & 0 & 5 \end{bmatrix},$$

$$M_{(u_2,u_3,u_4),3} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 3 \end{bmatrix}.$$

Similarly the entry matrices of an orthogonal design $OD(20; 5, 6, 9)$ obtained by setting first and second variable be the same symbol (i.e. replacing rows $\mathbf{v_1^T}, \mathbf{v_2^T}$ by row $\mathbf{v_1^T} + \mathbf{v_2^T}$) are

$$M_{(u_1+u_2,u_3,u_4),1} = \begin{bmatrix} 2 & 2 & 1 & 0 \\ 3 & 1 & 2 & 0 \\ 0 & 2 & 2 & 5 \end{bmatrix}, M_{(u_1+u_2,u_3,u_4),2} = \begin{bmatrix} 1 & 1 & 4 & 0 \\ 2 & 2 & 0 & 5 \end{bmatrix},$$

$$M_{(u_1+u_2,u_3,u_4),3} = \begin{bmatrix} 2 & 2 & 1 & 0 \\ 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 3 \end{bmatrix}.$$

$\square$

Now from [37] we have that from an orthogonal design over t variables we can obtain an orthogonal design over $t - 1$ variables by "killing" one variable (i.e. setting one variable equal to zero) or "equating" two variables (i.e. setting two variables be the same symbol). If we do these many times we obtain the following lemma:

Lemma 14 *If an orthogonal design $OD(4n; u_1, u_2, \ldots, u_t)$ exist then the following orthogonal designs exist:*

  i) *All orthogonal designs $OD(4n; u_{i_1}, u_{i_2}, \ldots, u_{i_k})$ for all $k = 1, 2, \ldots, t$, over k variables and for all $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, t\}$.*

  ii) *All orthogonal designs*

$$OD\left(4n; \sum_{j=k_0=1}^{k_1} u_{i_j}, \sum_{j=k_1+1}^{k_2} u_{i_j}, \ldots, \sum_{j=k_{m-1}+1}^{k_m} u_{i_j}\right)$$

  over m variables where $1 \le m \le t$, $1 \le k_i \le t$, $\forall\ i = 1, 2, \ldots m$, $k_1 \le k_2 \le \ldots \le k_m$, $u_{i_j} \ne u_{i_\ell}$, $\forall\ j, \ell = 1, 2, \ldots, k_m$ and $i \ne \ell$, $\bigcup\limits_{j=1}^{k_m} u_{i_j} \subseteq \{u_1, u_2, \ldots, u_t\}$.

Proof. By equating and killing variables we obtain the desirable result. $\square$

¿From the above lemma it is obvious that

Corollary 7 *If there exist $k : 1 \le k \le t$ and $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, t\}$ such that an orthogonal design $OD(4n; u_{i_1}, u_{i_2}, \ldots, u_{i_k})$ does not exist then an orthogonal design $OD(4n; u_1, u_2, \ldots, u_t)$ can not exist.*

Our method relies on searching for $OD(4n; u_k, u_j)$, $1 \le k, j \le t$, in two variables, which is much faster, rather than using the matrix based algorithm, described in [37] for $OD(4n; u_1, u_2, \ldots, u_t)$, in t variables, which is much slower. Then we use the extension algorithm to construct the orthogonal design we want.

Moreover we do not have to check all non-isomorphic entry matrices $M_{(u_k, u_j), i}$ but only a few of them. We also can select the k, j in such way that we minimize the set of $M_{(u_k, u_j), i}$ we have to search.

Let D be the orthogonal design $OD(4n; u_1, u_2, \ldots, u_t)$. The steps of our algorithm are:

Step 0: Find all non-isomorphic entry matrices $M_{(s_1, s_2, \ldots, s_u), i}$ for D as it is described in [37].

Step 1: For $k, j \in \{1, 2, \ldots, u\}, k < j$ find all non-isomorphic entry matrices $M_{(s_k, s_j), i}$ for the orthogonal design $OD(4n; s_k, s_j)$.

Step 2: For all the above $\binom{u}{2}$ combinations check if $M_{(s_1, s_2, \ldots, s_u), i}\big|_{\mathcal{D}_{(s_k, s_j)}}$ is equal with any $M_{(s_k, s_j), \ell} \in \mathcal{D}_{(s_k, s_j)}$. Ignore similar matrices $M_{(s_1, s_2, \ldots, s_u), i}\big|_{\mathcal{D}_{(s_k, s_j)}}$ produced after using the two rows of $M_{(s_1, s_2, \ldots, s_u), i}$ and eliminate all others rows. These are the matrices that can be extended to $M_{(s_1, s_2, \ldots, s_u), i}$ and thus these might produce the orthogonal design D.

Step 3: Select the k, j which give the smallest number of entry matrices $M_{(s_1, s_2, \ldots, s_u), i}\big|_{\mathcal{D}_{(s_k, s_j)}}$.

Step 4: Apply first algorithm (matrix based algorithm) to the selected entry matrices specified in Step 3, and find all $OD(4n; s_k, s_j)$.

Step 5: For each $OD(4n; s_k, s_j)$ found in Step 4, apply the second algorithm (extension algorithm), by replacing each zero by a unique variable x_p, $p = 1, 2, \ldots, 4n - (s_k + s_j)$.

Step 6: Exhaustively search all possibilities then if the solution exists, it will be found, otherwise an $OD(4n; s_1, s_2, \ldots, s_u)$ does not exist constructed by four sequences.

Example 13 We will apply our algorithm to search for an orthogonal design $D = OD(36; u_1, u_2, u_3) = OD(36; 6, 7, 21)$.

Step 0: The following ten matrices are all the non-isomorphic entry matrices $M_{(u_1, u_2, u_3), i}$ for D as it is described in [37]:

$$
1) \begin{bmatrix} 3 & 1 & 2 & 0 \\ 3 & 1 & 1 & 2 \\ 2 & 6 & 6 & 7 \end{bmatrix}, \quad
2) \begin{bmatrix} 3 & 1 & 2 & 0 \\ 1 & 3 & 1 & 2 \\ 4 & 4 & 6 & 7 \end{bmatrix}, \quad
3) \begin{bmatrix} 3 & 1 & 2 & 0 \\ 1 & 1 & 1 & 4 \\ 4 & 6 & 6 & 5 \end{bmatrix},
$$

$$4) \begin{bmatrix} 3 & 1 & 2 & 0 \\ 1 & 1 & 3 & 2 \\ 4 & 6 & 4 & 7 \end{bmatrix}, \quad 5) \begin{bmatrix} 1 & 1 & 4 & 0 \\ 3 & 1 & 1 & 2 \\ 4 & 6 & 4 & 7 \end{bmatrix}, \quad 6) \begin{bmatrix} 1 & 1 & 4 & 0 \\ 1 & 1 & 3 & 2 \\ 6 & 6 & 2 & 7 \end{bmatrix},$$

$$7) \begin{bmatrix} 1 & 1 & 4 & 0 \\ 1 & 1 & 1 & 4 \\ 6 & 6 & 4 & 5 \end{bmatrix}, \quad 8) \begin{bmatrix} 1 & 1 & 2 & 2 \\ 3 & 1 & 1 & 2 \\ 4 & 6 & 6 & 5 \end{bmatrix}, \quad 9) \begin{bmatrix} 1 & 1 & 2 & 2 \\ 1 & 1 & 3 & 2 \\ 6 & 6 & 4 & 5 \end{bmatrix},$$

$$10) \begin{bmatrix} 1 & 1 & 2 & 2 \\ 1 & 1 & 1 & 4 \\ 6 & 6 & 6 & 3 \end{bmatrix} \qquad \qquad \square$$

Step 1: We have that

$$|\mathcal{D}_{(u_1,u_2)}| = 10, \ |\mathcal{D}_{(u_1,u_3)}| = 53, \ |\mathcal{D}_{(u_2,u_3)}| = 21$$

Step 2: By setting the first variable equal to zero (i.e. eliminating the first row $\mathbf{v_1^T}$) we get only 5 non-isomorphic entry matrices $M_{(u_1,u_2,u_3),i}|_{\mathcal{D}_{(u_2,u_3)}}$ from the 21 entry matrices of the orthogonal design $OD(36;7,21)$. Those come from the matrices $M_{(u_1,u_2,u_3),i}$ numbered i=1,2,3,8, and 10 above by deleting the first row.

By setting the second variable equal to zero we get 10 non-isomorphic entry matrices $M_{(u_1,u_2,u_3),i}|_{\mathcal{D}_{(u_1,u_3)}}$ from the 53 entry matrices of the orthogonal design $OD(36;6,21)$. Those come from the matrices $M_{(u_1,u_2,u_3),i}$ numbered $i = 1, 2, \ldots, 10$ above by deleting the second row.

By setting the third variable equal to zero we get only 10 non-isomorphic entry matrices $M_{(u_1,u_2,u_3),i}|_{\mathcal{D}_{(u_1,u_2)}}$ from the 10 entry matrices of the orthogonal design $OD(36;6,7)$. Those come from the matrices $M_{(u_1,u_2,u_3),i}$ numbered $i = 1, 2, \ldots, 10$ above by deleting the third row.

Step 3: Clearly in the case $k = 2$ and $j = 3$ we have fewer entry matrices to check than in any of the other cases, i.e five.

Step 4: Now we get all the quadruples of sequences with PAF=0 or NPAF=0, which can be used for the construction of $OD(36;7,21)$, via the Goethals-Seidel Array. This is applied to all five entry matrices described in steps 2 and 3.

Step 5: For each $OD(4n;u_k,u_j) = OD(36;7,21)$ found in Step 4, apply the second algorithm (extension algorithm), by replacing the zero of the sequences by the unique variables x_p, $p = 1, 2, \ldots, 8$.

We want to make clear that if an $OD(36;6,7,21)$ existed it would have been found. We did not find any solutions by step 5 and thus, since our search is exhaustive for the orthogonal design $OD(36;6,7,21)$, this design does not exist using four sequences. $\qquad \square$

Example 14 Applying our algorithm we try to find the $OD(36;6,8,19)$ and the $OD(36;7,8,19)$. There are 22 non-isomorphic entry matrices $M_{(6,8,19),i}$ corresponding to the orthogonal design $OD(36;u_1,u_2,u_3)=OD(36;6,8,19)$ and 22 for the second orthogonal design $OD(36;u_4,u_2,u_3) = OD(36;7,8,19)$.

By setting the first variable equal to zero we get only 17 non-isomorphic entry matrices $M_{(6,8,19),i}\big|_{\mathcal{D}_{(u_2,u_3)}}$ for the $OD(36;8,19)$.

We observe that the matrices $M_{(6,8,19),i}\big|_{\mathcal{D}_{(u_2,u_3)}}$ are exactly the same as the matrices $M_{(7,8,19),i}\big|_{\mathcal{D}_{(u_2,u_3)}}$ for the second orthogonal design.

Thus by searching those 17 non-isomorphic entry matrices we can perform an exhaustive search for both orthogonal designs. Using the matrix based algorithm we would have had to check 44 entry matrices using three variables for both designs.

Applying our algorithm and following the same process as in the previous example we find, among others, the following solutions, which have PAF=0:

$$OD(36;6,8,19)$$

```
b  -c   0   b   b   b   a   c  -a
b   b  -b   b   c  -a  -b   c   a
c   b  -b  -b  -a  -b   b  -a   0
b  -b  -b  -c   b  -a   b  -a   0
```

$$OD(36;7,8,19)$$

```
a  -b  -b  -b   c  -a  -c  -b  -c
b  -a   a   b  -c  -b   b  -b  -c
b  -b   a   a   b   b  -b   0  -c
a  -b  -b  -b   b   a   b   0   c
```

□

The interesting reader can find more on this algorithm in [28].

Remark 3 Using the above algorithms, cases where $n \equiv 0(\ mod\ 4)$, have been studied. In particular all orthogonal designs of orders $4n$, $n = 1, 3, 5, 7, 9$ had been completely studied, (see [26, 28, 62, 63, 67, 70]).

3.3   Amicable sets of matrices and constructions of orthogonal designs using the Kharaghani array

A pair of matrices A, B is said to be amicable (anti-amicable) if $AB^T - BA^T = 0$ ($AB^T + BA^T = 0$). Following [56] a set $\{A_1, A_2, \ldots, A_{2n}\}$ of square real matrices is said to be *amicable* if

$$\sum_{i=1}^{n} \left(A_{\sigma(2i-1)} A_{\sigma(2i)}^T - A_{\sigma(2i)} A_{\sigma(2i-1)}^T \right) = 0 \tag{31}$$

for some permutation σ of the set $\{1, 2, \ldots, 2n\}$. For simplicity, we will always take $\sigma(i) = i$ unless otherwise specified. So

$$\sum_{i=1}^{n} \left(A_{2i-1} A_{2i}^T - A_{2i} A_{2i-1}^T \right) = 0. \tag{32}$$

44

Clearly a set of mutually amicable matrices is amicable, but the converse is not true in general. Throughout the section R_k denotes the back diagonal identity matrix of order k.

A set of matrices $\{B_1, B_2, \ldots, B_n\}$ of order m with entries in $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ is said to satisfy an additive property of type $(s_1, s_2, \ldots, s_u)$ if

$$\sum_{i=1}^{n} B_i B_i^T = \sum_{i=1}^{u} (s_i x_i^2) I_m. \tag{33}$$

Let $\{A_i\}_{i=1}^{8}$ be an amicable set of circulant matrices (or type 1) of type $(s_1, s_2, \ldots, s_u)$ of order t. Then the Kharaghani array from [56]

$$H = \begin{pmatrix} A_1 & A_2 & A_4 R_n & A_3 R_n & A_6 R_n & A_5 R_n & A_8 R_n & A_7 R_n \\ -A_2 & A_1 & A_3 R_n & -A_4 R_n & A_5 R_n & -A_6 R_n & A_7 R_n & -A_8 R_n \\ -A_4 R_n & -A_3 R_n & A_1 & A_2 & -A_8^T R_n & A_7^T R_n & A_6^T R_n & -A_5^T R_n \\ -A_3 R_n & A_4 R_n & -A_2 & A_1 & A_7^T R_n & A_8^T R_n & -A_5^T R_n & -A_6^T R_n \\ -A_6 R_n & -A_5 R_n & A_8^T R_n & -A_7^T R_n & A_1 & A_2 & -A_4^T R_n & A_3^T R_n \\ -A_5 R_n & A_6 R_n & -A_7^T R_n & -A_8^T R_n & -A_2 & A_1 & A_3^T R_n & A_4^T R_n \\ -A_8 R_n & -A_7 R_n & -A_6^T R_n & A_5^T R_n & A_4^T R_n & -A_3^T R_n & A_1 & A_2 \\ -A_7 R_n & A_8 R_n & A_5^T R_n & A_6^T R_n & -A_3^T R_n & -A_4^T R_n & -A_2 & A_1 \end{pmatrix} \tag{34}$$

is a Kharaghani type orthogonal design $OD(8m; s_1, s_2, \ldots, s_u)$.

We present an algorithm which uses the known sets of four circulant matrices to construct an amicable set of eight matrices suitable for the array given by (34).

The algorithm

Step 1 Find four circulants matrices A, B, C, D of order n with variables a, b, c, d satisfying

$$AA^T + BB^T + CC^T + DD^T = (r_1 a^2 + r_2 b^2 + r_3 c^2 + r_4 d^2) I_n$$

for some integers r_i, by using any of the above algorithms.

Step 2 Form four new circulant matrices E, F, G, H from A, B, C, D just by replacing a, b, c, d with e, f, g, h respectively. Obviously the new matrices satisfy the previous conditions but on variables e, f, g, h.

Step 3 Search the set $\{A, B, C, D, E, F, G, H\}$ for a combination suitable to form an amicable set of eight matrices.

Step 4 If we find such a set, we replace the matrices in the array given by (34).

Notation 2 With the expression $circ(a, b, c, \ldots, z)$ we will denote the circulant matrix with first row the sequence in the brackets.

Example 15 Let $A = circ(a, b, c)$, $B = circ(d, -a, b)$, $C = circ(-c, d, a)$ and $D = circ(-b, c, d)$. Then $AA^t + BB^t + CC^t + DD^t = 3(a^2 + b^2 + c^2 + d^2)I_3$. We form the matrices $E = circ(e, f, g)$, $F = circ(h - e, f)$, $G = circ(-g, h, e)$ and $H = circ(-f, g, h)$. Then obviously we have that $EE^T + FF^T + GG^T + HH^T = 3(e^2 + f^2 + g^2 + h^2)I_3$. A computer search finds that

$$AH^T - HA^T + BG^T - GB^T + CF^T - FC^T + DE^T - ED^T = 0$$

So, we have found an amicable set of eight circulant matrices, the $\{A,H,B,G,C,F,D,E\}$. If we substitute these matrices in the array of the corollary, we get an $OD(24; 3, 3, 3, 3, 3, 3, 3, 3)$.

45

Example 16 Let $A = circ(a, b, b, d, -d)$, $B = circ(-b, a, a, c, -c)$, $C = circ(d, c, c, -a, a)$, $D = circ(-c, d, d, -b, b)$. Then $AA^T + BB^T + CC^T + DD^T = 5(a^2 + b^2 + c^2 + d^2)I_5$. We form the matrices $E = circ(e, f, f, h, -h)$, $F = circ(-f, e, e, g, -g)$, $G = circ(h, g, g, -e, e)$, $H = circ(-g, h, h, -f, f)$ just by substituting the variables a,b,c,d for e,f,g,h respectively. Then we have $EE^T + FF^T + GG^T + HH^T = 5(e^2 + f^2 + g^2 + h^2)I_5$. A computer search finds the amicable set

$$AE^T - EA^T + BH^T - HB^T + GC^T - CG^T + DF^T - FD^T = 0$$

So, we have the $\{A, E, B, H, G, C, D, F\}$ amicable set of matrices. If we substitute these matrices in Kharaghani array we obtain the $OD(40; 5, 5, 5, 5, 5, 5, 5, 5)$.

Remark 4 Using the above algorithm, and the Kharaghani array many new orthogonal designs of orders $8n$ are constructed, (see [20, 29, 30, 31, 49, 50, 56, 71, 72]).

4 Short amicable sets and Kharaghani type orthogonal designs

4.1 Preliminary results and basic definitions

Short amicable set were defined in [32] as a set of matrices $\{A_i\}_{i=1}^4$ of order m and type (u_1, u_2, u_3, u_4), abbreviated as $4 - SAS(m; u_1, u_2, u_3, u_4; G)$, if (32) and (33) are satisfied for $n = 4$ and $u \leq 4$. $4 - SAS(m; u_1, u_2, u_3, u_4; G)$ can be used in either the Goethals-Seidel array or the *short Kharaghani array*

$$\begin{bmatrix} A & B & CR & DR \\ -B & A & DR & -CR \\ -CR & -DR & A & B \\ -DR & CR & -B & A \end{bmatrix}$$

to form an $OD(4m; u_1, u_2, u_3, u_4)$. In all cases, the group G of the matrices in the *amicable set* is such that the extension by Seberry and Whiteman [89] of the group from circulant to type 1 allows the same extension to R.

In general a set of $2n$ matrices of order m and type $(s_1, s_2, \ldots, s_u)$ that satisfy equations (32) and (33) will be denoted as $2n - SAS(m; s_1, s_2, \ldots, s_u; G)$. Moreover if these matrices are circulant they will be denoted as $2n - SCAS(m; s_1, s_2, \ldots, s_u; Z_m)$.

In [32] where short amicable sets were first defined, it was mentioned that:

Remark 5   1. If there exists a $2 - SAS(n; s_1, s_2; G)$ and a $2 - SAS(n; s_3, s_4; G)$ then there exists a $4 - SAS(n; s_1, s_2, s_3, s_4; G)$.

2. If there exists a $2 - SAS(n; s_1, s_2; G)$, $2 - SAS(n; s_3, s_4; G)$, $2 - SAS(n; s_5, s_6; G)$ and a $2 - SAS(n; s_7, s_8; G)$ there exists an $8 - AS(n; s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8; G)$.

3. If there exists a $4 - SAS(n; s_1, s_2, s_3, s_4; G)$ and a $4 - SAS(n; s_5, s_6, s_7, s_8; G)$ there exists an $8 - AS(n; s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8; G)$.

Thus we can obtain many classes of $4 - SAS(n; s_1, s_2, s_3, s_4; G)$ combining together two pairs of the given $2 - SAS(n; s_1, s_2; G)$ and $2 - SAS(n; s_3, s_4; G)$. Moreover, in Table 4.2, we give some $4 - SAS(m; u_1, u_2, u_3, u_4; Z_m)$ that can not be constructed by this method.

Generally, unless we have other information regarding the structure, we are unable to ensure that the matrix R with the desired properties for the Kharaghani, Goethals-Seidel or short Kharaghani arrays exists unless the amicable sets have been group generated (circulant or type 1) or constructed from blocks of these kinds. Thus is we have the required matrix R_i for the group G_i, $i = 1, 2$ then $R_G = R_1 \times R_2$ will be the required matrix for $G = G_1 \times G_2$, (see [89]).

Let A_1 and A_2 be matrices of order m. We define $circ(A_1, A_2) = \begin{bmatrix} A_1 & A_2 \\ A_2 & A_1 \end{bmatrix}$. Amicable sets made from $2n$ such block circulant matrices will be called *block amicable sets, short block amicable sets* or *2-short block amicable sets*, $2n - SBAS(2m; s_1, s_2, \ldots, s_u; G)$, $n = 1, 2, 4$, where, using R_t for the back-diagonal matrix of order t, $G = Z_2 \times Z_m$ and $R_G = R_2 \times R_m$. Here, if A_1 and A_2 are circulant, then we use the backdiagonal matrix of the same order for R ensuring $A_i(A_j R)^T = A_j R A_i^T$. The required $R_G = R_2 \times R$.

We denote the product $Z_p \times Z_p \times \cdots \times Z_p (r\ times)$ by $EA(p^r)$ the Elementary Abelian group. Moreover $-a$ is denoted by $\bar{a}$.

Throughought this section we use the symbol 0_m to denote the sequence of length m with all elements zero and the symbol O_t to denote the $t \times t$ matrix with all entries zero.

For the undefined terms we refer the reader to the book by Geramita and Seberry [37].

4.2   Constructions

Theorem 23 *Write 0_s for the sequence of s zeros, and let a, b, c and d be commuting variables. Use the matrices A_1, A_2, A_3 and A_4 given by*

$$A_1 = circ(0_s b a \bar{b} 0_s), \qquad A_2 = circ(0_s c 0 c 0_s),$$
$$A_3 = circ(0_s \bar{c} d c 0_s), \qquad A_4 = circ(0_s b 0 b 0_s),$$

can be used in the Goethals-Seidel array to obtain an $OD(8s + 12; 1, 1, 4, 4)$.

Proof.   Observe that

$$A_1 A_1^T + A_2 A_2^T + A_3 A_3^T + A_4 A_4^T = (a^2 + d^2 + 4b^2 + 4d^2) I_n$$

and

$$A_1 A_1^T - A_2 A_2^T + A_3 A_3^T - A_4 A_4^T = 0.$$

Thus A_2, A_2, A_3, A_4 are a short amicable set and satisfy the additive property (33) so they can be used in the Goethals-Seidel array to obtain an $OD(8s + 12; 1, 1, 4, 4)$. $\square$

The Melding Construction
Suppose the matrices A_1, A_2, A_3 and A_4 are are short amicable sets, on the set of commuting variables $\{0, \pm x_1, \pm x_2, \cdots, \pm x_u\}$ or from $\{0, \pm 1\}$, and satisfy the additive property

$$\sum_{i=1}^{4} \left(A_i A_i^T \right) = \sum_{j=1}^{u} p_j x_j^2 I_n, \tag{35}$$

and the matrices A_5, A_6, A_7 and A_8 are also short amicable sets, on the set of commuting variables $\{0, \pm y_1, \pm y_2, \cdots, \pm y_v\}$ or from $\{0, \pm 1\}$, and satisfy the additive property

$$\sum_{i=5}^{8} \left(A_i A_i^T \right) = \sum_{j=1}^{v} q_j y_j^2 I_n. \tag{36}$$

47

Then the eight matrices will form an amicable set so we can use the two together in the Kharaghani array to obtain an $OD(8n; p_1, p_2, \cdots, p_u, q_1, q_2, \cdots, q_v)$. □

order	type	group	order	type	group	order	type	group	order	type	group
n	1, 1	Z_n	$6n$	4, 4	Z_{6n}	$10n$	4, 4	Z_{10n}	$14n$	8, 8	Z_{14n}
$2n$	2, 2	Z_{2n}	$6n$	5, 5	Z_{6n}	$10n$	9, 9	Z_{10n}	$14n$	10, 10	Z_{14n}
$4n$	1, 4	Z_{4n}	$7n$	4, 4	Z_{7n}	$12n$	8, 8	Z_{12n}	$14n$	13, 13	Z_{14n}
$4n$	4, 4	Z_{4n}	$8n$	8, 8	Z_{8n}	$13n$	9, 9	Z_{13n}			

Table 2: Order and type for small 2-short amicable sets for all $n \geq 1$.

Using table 2, remark 5 and the above Melding Construction we obtain many 4-short amicable sets and 8-amicable sets.

Type	A_1 A_2	A_3 A_4	ZERO
(1,1,1,1)	a c	b d	NPAF n
(1,1,1,4)	0 -d a d 0 d 0 d	0 b 0 0 0 c 0 0	NPAF $4n$
(1,1,2,2)	a 0 b 0	c d c -d	NPAF $2n$
(1,1,2,8)	0 -c a c 0 c b c	0 -c b -c 0 -c d c	NPAF $4n$
(1,1,4,4)	a b -a c 0 c	a 0 a c d -c	NPAF $3n$
(1,1,5)	-a a a c 0 0	a 0 a 0 b 0	NPAF $4n$
(1,1,5,5)	-c a c 0 c -d c 0	-d b d 0 d c d 0	NPAF $4n$
(1,1,8,8)	0 -c -d a d c 0 c d 0 d c	0 c -d 0 -d c 0 -c d b -d c	NPAF $6n$
(1,2,2,4)	0 -d a d 0 d 0 d	c 0 b 0 c 0 -b 0	NPAF $4n$
(1,4,4,4)	0 -b a b 0 b 0 b	d c -d c -c d c d	NPAF $4n$
(2,2,2,2)	a b c d	a -b c -d	NPAF $2n$
(2,2,4,4)	a 0 b 0 a 0 -b 0	d c -d c -c d c d	NPAF $4n$
(2,2,5,5)	0 a 0 0 b 0 0 a 0 0 -b 0	c -d 0 -d c d d c 0 c d -c	NPAF $6n$
(2,2,8,8)	-d c a c d 0 -d -c a -c d 0	d -c b c d 0 -d -c b c -d 0	NPAF $6n$

Table 3: Short amicable sets.

48

Type	A_1 A_2	A_3 A_4	ZERO
(3,3)	a b a 0	b-a b 0	NPAF $2n$
(4,4,4,4)	a a b-b d d-c c	b b-a a c c d-d	NPAF $4n$
(4,4,8,8)	d a -c c a -d -d -b c c b -d	d b c -c b -d d -a c c a d	NPAF $6n$
(5,5)	a a -a b b -b	a 0 a b 0 b	NPAF $3n$
(5,5,5,5)	-a b a 0 a b b a -b 0 -b a	-c d c 0 c d d c -d 0 -d c	NPAF $6n$
(6,6)	a -b a b a b	a a -a b b -b	NPAF $3n$
(6,6,12)	c a c b-c a -c b-c-a c b	c a c-a c-a -c b c-b-c-b	NPAF $6n$
(8,8)	a a a-a b b b-b	b b-b b a a-a a	NPAF $4n$
(8,8,8,8)	a a a-a b b-b b c c c-c d d-d d	b b b-b a a-a a d d d-d c c-c c	NPAF $8n$
(10,10,10,10)	dijoint	from Golay	NPAF $n \geq 10$
(13,13)	c 0 -c c -c 0 0 c c g 0 -g g -g 0 0 g g	c c -c c c c 0 0 -c g g -g g g g 0 0 -g	NPAF $9n$
(13,13,13,13)	from disjoint length 18	sequences weight 13	NPAF $n \geq 18$
(16,16,16,16)	disjoint	from Golay	NPAF $n \geq 16$
(17,17,17,17)	disjoint length 26	sequences weight 17	NPAF $n \geq 26$
(20,20,20,20)	dijoint	from Golay	NPAF $n \geq 20$
(25,25,25,25)	disjoint length 36	sequences weight 25	NPAF $n \geq 36$
(26,26,26,26)	disjoint	from Golay	NPAF $n \geq 26$
(14,14)	a b -b -b b a a b -a a a -a b b	-b a -b a -b b b a b a b a -a -a	NPAF $7n$
(17,17)	a -a a a a a -a a 0 c -c c c c c -c c 0	c -c -c c c c c -c -c a -a -a a a a a -a -a	PAF $9n$

Table 3: (continued).

4.3 Some general results

We now consider the use of sequences with zero non-periodic autocorrelation function to make an amicable set of matrices. We refer the reader to [88, 90] for any undefined terms.

The next theorem was proved in [73].

Theorem 24 (General construction) *Let X, Y be two disjoint $(0, \pm 1)$ sequences with zero non-periodic autocorrelation function of length n and weight k, Let a, b, c, d be commuting*

Type	ZERO
(1,1,1,1)	NPAF $n \geq 1$
(2,2,2,2)	NPAF $n \geq 2$
(4,4,4,4)	NPAF $n \geq 4$
(5,5,5,5)	NPAF $n \geq 6$
(8,8,8,8)	NPAF $n \geq 8$
(10,10,10,10)	NPAF $n \geq 10$
(13,13,13,13)	NPAF $n \geq 18$
(16,16,16,16)	NPAF $n \geq 16$
(17,17,17,17)	NPAF $n \geq 26$
(20,20,20,20)	NPAF $n \geq 20$
(25,25,25,25)	NPAF $n \geq 36$
(26,26,26,26)	NPAF $n \geq 26$

Table 4: Short amicable sets from corollary 8

variables and write aV, bW for the circulant (type 1) matrices of order n formed by using the first rows with the elements of X multiplied by a and the elements of Y multiplied by b respectively.

Let A_i be the circulant matrices of order n given by

$$A_1 = aV + bW \quad A_2 = cV + dW \quad A_3 = dV - cW \quad A_4 = bV - aW \tag{37}$$

then $\{A_i\}_{i=1}^{4}$ is a short amicable set satisfying

$$\sum_{i=1}^{2} \left(A_{2i-1} A_{2i}^T - A_{2i} A_{2i-1}^T \right) = 0, \tag{38}$$

and the additive property

$$\sum_{i=1}^{4} \left(A_i A_i^T \right) = k(a^2 + b^2 + c^2 + d^2) I_n. \tag{39}$$

Corollary 8 *Let X, Y be a pair of disjoint $(0, \pm 1)$ sequences with zero non-periodic autocorrelation function of length n and weight k. Then there exists a short amicable set which can be used to form an $OD(4n; k, k, k, k)$.*

For $\alpha, \beta, \gamma, \delta, \epsilon, \phi, \psi, \mu, \nu$ non-negative integers, Koukouvinos and Seberry [69, p. 160] show that there exist two disjoint $(0, \pm 1)$ sequences, with zero non-periodic autocorrelation function, of length $\geq n$, $n \in N = \{2 \times 2^\alpha 6^\beta 10^\gamma 9^\delta 14^\epsilon 18^\phi 26^\psi 24^\mu 34^\nu\}$ and weight k, $k \in K = \{2^\alpha 5^\beta 10^\gamma 13^\delta 17^\epsilon 25^\phi 26^\psi 34^\mu 50^\nu\}$. These give the results presented in Table 4.

For more details about short amicable sets and their use in the construction of Kharaghani type orthogonal designs the interesting reader is refer to [32, 73].

References

[1] Apple Computer. Inside Macintosh: Networking with Open Transport, 1997. Available from http://developer.apple.com/techpubs/mac/pdf/Networking0T.pdf.

[2] K. T. Arasu and J. Seberry, Circulant weighing designs, *J. Combin. Designs*, 4 (1996), 439-447.

[3] K. T. Arasu and J. Seberry, On circulant weighing matrices, *Australas. J. Combin.*, 17 (1998), 21-37.

[4] L. D. Baumert, Hadamard matrices of orders 116 and 232, *Bull. Amer. Math. Soc.*, 72 (1966), 237.

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

[6] L. D. Baumert, and M. Hall Jr., Hadamard matrices of the Williamson type, *Math. Comput.*, 19 (1965), 442-447.

[7] T. Chadjipantelis and S. Kounias, Supplementary difference sets and D-optimal designs for $n \equiv 2(mod\ 4)$, *Discrete Math.*, 57 (1985), 211-216.

[8] J. Cooper, J. Milas, and W. D. Wallis, Hadamard equivalence, in *Combinatorial Mathematics*, Lecture Notes in Mathematics, Vol. 686, Springer-Verlag, Berlin, Heidelberg, New York, 1978, 126–135.

[9] R. Craigen, *Hadamard Matrices and Designs*, The CRC Handbook of Combinatorial Designs, eds. C. J. Colbourn and J. H. Dinitz, CRC Press, Boca Raton, Fla., (1996), 370–377.

[10] A. Dey and R. Mukerjee, *Fractional factorial plans*, J. Wiley and Sons, New York, 1999.

[11] D. Z. Djokovic, Williamson matrices of orders $4 \cdot 29$ and $4 \cdot 31$, *J. Combin. Theory Ser. A*, 59 (1992), 442–447.

[12] D. Z. Djokovic, Williamson matrices of orders 4n for n=33,35,39, *Discrete Math.*, 115 (1993), 267–271.

[13] D. Z. Djokovic, Note on Williamson matrices of orders 25 and 37, *J. Combin. Math. Combin. Comput.*, 18 (1995), 171–175.

[14] P. Eades and J. Seberry Wallis, An infinite family of skew-weighing matrices, *Combinatorial Mathematics IV*, in Lecture Notes in Mathematics, Vol. 560, Springer-Verlag, Berlin-Heidelberg-New York, pp. 27-40, 1976.

[15] S. Eliahou, M. Kervaire, and B. Saffari, A new restriction on the lengths of Golay complementary sequences, *J. Combin. Theory Ser. A*, 55 (1990), 49-59.

[16] K.-T. Fang and G. Ge, An efficient algorithm for the classification of Hadamard matrices, (submitted).

[17] R. J. Fletcher, M. Gysin, and J. Seberry, Application of the discrete Fourier transform to the search for generalized Legendre pairs and Hadamard matrices, *Australas. J. Combin.*, 23 (2001), 75-86.

[18] Al. Geist, A. Beguelin, J. Dongarra, W. Jiang, R. Manchek, and V. Sunderam. PVM:Parallel Virtual Machine–A User's Guide and Tutorial for Networked Parallel Computing. MIT Press, 1994. Available as Postscript from http://www.netlib.org/pvm3/book/pvm-book.ps.

[19] S. Georgiou and C. Koukouvinos, On multipliers of supplementary difference sets and D-optimal designs for $n \equiv 2\bmod 4$, *Utilitas Math.*, 56 (1999), 127-136.

[20] S. Georgiou and C. Koukouvinos, On amicable sets of matrices and orthogonal designs, *Int. J. Appl. Math.*, 4 (2000), 211-224.

[21] S. Georgiou and C. Koukouvinos, On sequences with zero autocorrelation and orthogonal designs, *J Combin. Th. Ser A*, 94, (2001), 15-33.

[22] S. Georgiou and C. Koukouvinos, On generalized Legendre pairs and multipliers of the corresponding supplementary difference sets, *Utilitas Math.*, (to appear).

[23] S. Georgiou and C. Koukouvinos, On equivalence of Hadamard matrices and projection properties, *Ars Combin.*, (to appear).

[24] S. Georgiou and C. Koukouvinos, On inequivalent Hadamard matrices of order 36, (submitted).

[25] S. Georgiou and C. Koukouvinos, On inequivalent Hadamard matrices of order 44, (submitted.)

[26] S. Georgiou, C. Koukouvinos, M. Mitrouli, and J. Seberry, Necessary and Sufficient Conditions for two variable orthogonal designs in order 44:Addendum, *J. Combin. Math. Combin. Comput.*, 34 (2000), 59-64.

[27] S. Georgiou, C. Koukouvinos, M. Mitrouli and J. Seberry, Necessary and sufficient conditions for three and four variable orthogonal designs in order 36, *J. Statist. Plann. Inference*, (to appear).

[28] S. Georgiou, C. Koukouvinos, M. Mitrouli and J. Seberry, A new algorithm for computer searches for orthogonal designs, *J. Combin. Math. Combin. Comput.*, (to appear).

[29] S. Georgiou, C. Koukouvinos, and J. Seberry, On full orthogonal designs in order 72, *J. Combin. Math. Combin. Comput.*, (to appear).

[30] S. Georgiou, C. Koukouvinos, and J. Seberry, On full orthogonal designs in order 56, *Ars. Combin.*, (to appear).

[31] S. Georgiou, C. Koukouvinos and J. Seberry, Some results on Kharaghani type orthogonal designs, *Utilitas Math.*, (to appear).

[32] S. Georgiou, C. Koukouvinos and J. Seberry, Short amicable sets, (submitted).

[33] A. V. Geramita, J. M. Geramita, and J. Seberry Wallis, Orthogonal designs, *Linear and Multilinear Algebra*, 3 (1976), 281-306.

[34] A. V. Geramita, and J. Seberry Wallis, Orthogonal designs III: Weighing matrices, *Utilitas Math.*, 6 (1974), 209-236.

[35] A. V. Geramita, and J. Seberry Wallis, Orthogonal designs II, *Aequationes Math.*, 13 (1975), 299-313.

[36] A. V. Geramita, and J. Seberry Wallis, Orthogonal designs IV: Existence questions, *J.Combin. Theory Ser. A*, 19 (1975), 66-83.

[37] A. V. Geramita, and J. Seberry, *Orthogonal designs: Quadratic forms and Hadamard matrices*, Marcel Dekker, New York-Basel, 1979.

[38] A. V. Geramita, and J. H. Verner, Orthogonal designs with zero diagonal, *Canad. J. Math.*, 28 (1976), 215-224.

[39] J. M. Goethals and J. J. Seidel, Orthogonal matrices with zero diagonal, *Canad.J.Math.*, 19 (1967), 1001-1010.

[40] J. M. Goethals and J. J. Seidel, A skew Hadamard matrix of order 36, *J. . Math. Soc.*, 11 (1970), 343–344.

[41] M. J. E. Golay, Complementary sequences, *IRE Trans. Inform. Theory*, 7 (1961), 82-87.

[42] W. Gropp, L. Ewing, and A. Skjellum, Using MPI: Portable Parallel Programming with the Message-Passing Interface, MIT Press, 1994.

[43] M. Gysin, New D-optimal designs via cyclotomy and generalized cyclotomy, *Australas. J. Combin.*, 15 (1997), 247-255.

[44] M. Gysin and J. Seberry, An experimental search and new combinatorial designs via a generalization of cyclotomy, *J. Combin. Math. Combin. Comput.*, 27 (1998), 143-160.

[45] M. Gysin and J. Seberry, On new families of supplementary difference sets over rings with short orbits, *J. Combin. Math. Combin. Comput.*, 28 (1998), 161-186.

[46] M. Hall Jr., Hadamard matrices of order 16, *JPL Research Summary* No. 36-10, Vol. 1 (1961), 21–26.

[47] M. Hall Jr., Hadamard matrices of order 20, *JPL Technical Report* No. 32-76, Vol.1 (1965).

[48] M. Hall Jr., *Combinatorial Theory*, Blaisdell, Waltham, Mass., 1967.

[49] W.H. Holzmann, and H. Kharaghani, On the Plotkin arrays, *Australas. J. Combin.*, 22 (2000), 287-299.

[50] W.H. Holzmann, and H. Kharaghani, On the orthogonal designs of order 24, *Discrete Appl. Math.*, 102 (2000), 103-114.

[51] W.H. Holzmann, and H. Kharaghani, On the orthogonal designs of order 40, *J. Statist. Plann. Inference*, 96 (2001), 415-429.

[52] J. Horton and J. Seberry, When the necessary conditions are not sufficient: sequences with zero autocorrelation function, *Bull. Inst. Combin. Appl.*, 27 (1999), 51-61.

[53] J. Horton, C. Koukouvinos and J. Seberry, A search for Hadamard matrices constructed from Williamson matrices, *Bull. Inst. Combin. Appl.*, (to appear).

[54] N. Ito, J. S. Leon and J. Q. Longyear, Classification of $3 - (24, 12, 5)$ designs and 24-dimensional Hadamard matrices, *J. Combin. Theory Ser. A,* 31 (1981), 66–93.

[55] Z. Janko, The existence of a Bush-type Hadamard matrix of order 36 and two new infinite classes of symmetric designs, *J. Combin. Theory Ser. A*, 95 (2001), 360–364.

[56] H. Kharaghani, Arrays for orthogonal designs, *J. Combin. Designs*, 8 (2000), 166-173.

[57] H. Kimura, Hadamard matrices of order 28 with automorphism groups of order two, *J. Combin. Theory Ser. A,* 43 (1986), 98–102.

[58] H. Kimura, On equivalence of Hadamard matrices, *Hokkaido Mathematical Journal*, 17 (1988), 139–146.

[59] H. Kimura, New Hadamard matrices of order 24, *Graphs Combin.*, 5 (1989), 236–242.

[60] H. Kimura, Classification of Hadamard matrices of order 28 with Hall sets, *Discrete Math.*, 128 (1994), 257–268.

[61] H. Kimura, Classification of Hadamard matrices of order 28, *Discrete Math.*, 133 (1994), 171–180.

[62] C. Koukouvinos, Some new orthogonal designs of order 36, *Utilitas Math.*, 51 (1997), 65-71.

[63] C. Koukouvinos, Some new three and four variable orthogonal designs in order 36, *J. Statist. Plann. Inference*, 73 (1998), 21-27.

[64] C. Koukouvinos and S. Kounias, Hadamard matrices of the Williamson type of order 4m, m=pq: An exhaustive search for m=33, *Discrete Math.*, 68 (1988), 45–47.

[65] C. Koukouvinos and S. Kounias, There are no circulant symmetric Williamson matrices of order 39, *J. Combin. Math. Combin. Comput.*, 7 (1990), 161–169.

[66] C. Koukouvinos, M. Mitrouli and J. Seberry, Necessary and sufficient conditions for some two variable orthogonal designs in order 44, *J. Combin. Math. Combin. Comput.*, 28 (1998), 267-286.

[67] C. Koukouvinos, M. Mitrouli, J. Seberry, and P. Karabelas, On sufficient conditions for some orthogonal designs and sequences with zero autocorrelation function, *Australas. J. Combin.*, 13 (1996), 197-216.

[68] C. Koukouvinos, N. Platis and J. Seberry, Necessary and sufficient conditions for some two variable orthogonal designs in order 36, *Congr. Numerantium*, 114 (1996), 129-139.

[69] C. Koukouvinos and J. Seberry, New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function - a review, *J. Statist. Plann. Inference*, 81 (1999), 153-182.

[70] C. Koukouvinos and J. Seberry, New orthogonal designs and sequences with two and three variables in order 28, *Ars Combin.*, 54 (2000), 97-108.

[71] C. Koukouvinos and J. Seberry, Infinite families of orthogonal designs : I, *Bull. Inst. Combin. Appl.*, (to appear).

[72] C. Koukouvinos and J. Seberry, Orthogonal designs of Kharaghani type: I, *Ars Combin.*, (to appear).

[73] C. Koukouvinos and J. Seberry, Short amicable sets and Kharaghani type orthogonal designs, *Bull. Austral. Math. Soc.*, (to appear).

[74] C. Koukouvinos, J. Seberry, A. L. Whiteman, and M. Y. Xia, Optimal designs, supplementary difference sets and multipliers, *J. Statis. Planning Inference*, 62 (1997), 81-90.

[75] S. Kounias, C. Koukouvinos, N. Nikolaou and A. Kakos, The non-equivalent circulant $D-$optimal designs for $n \equiv 2 \bmod 4$, $n \leq 54$, $n = 66$, *J. Combin. Th. Ser A*, 65 (1994), 26-38.

[76] C. Lam, S. Lam and V. D. Tonchev, Bounds on the number of affine, symmetric, and Hadamard designs and matrices, *J. Combin. Theory Ser. A*, 92 (2000), 186–196.

[77] C. Lin, W. D. Wallis, and Zhu Lie, Extended 4-profiles of Hadamard matrices, *Ann. Discrete Math.*, 51 (1992), 175–180.

[78] C. Lin, W. D. Wallis, and Zhu Lie, Equivalence classes of Hadamard matrices of order 32, *Congr. Numerantium*, 95 (1993), 179–182.

[79] C. Lin, W. D. Wallis, and Zhu Lie, Generalized 4-profiles of Hadamard matrices, *J. Comb. Inf. Syst. Sci.*, 18 (1993), 397–400.

[80] C. Lin, W. D. Wallis, and Zhu Lie, Equivalence classes of Hadamard matrices of order 32, *Congr. Numerantium*, 95 (1993), 179–182.

[81] C. Lin, W. D. Wallis, and Zhu Lie, Hadamard Matrices of Order 32, Preprint #92-20, Department of Mathematical Science, University of Nevada, Las Vegas, Nevada.

[82] C. Lin, W. D. Wallis, and Zhu Lie, Hadamard Matrices of Order 32 II, Preprint #93-05, Department of Mathematical Science, University of Nevada, Las Vegas, Nevada.

[83] D. K. J. Lin and N. R. Draper, Screening properties of certain two-level designs, *Metrika*, 42 (1995), 99–118.

[84] W.H. Press, B.P. Flannery, S.A. Teukolsky and W.T. Vettering, *Numerical Recipes in Pascal: The Art of Scientific Computing*, Cambridge Univ Press, New York, 1989.

[85] M.R. Schroeder, *Number Theory in Science and Communication*, Springer–Verlag, New York, 1984.

[86] Hadamard matrices of order 100 and 108, *Bull. Nagoya Inst. Technology*, 29 (1977), 147–153.

[87] Jennifer Seberry, Hadamard Matrices, hhttp://www.uow. edu.au/~jennie/hadamard.html.

[88] J. Seberry Wallis, Orthogonal designs V: Orders divisible by eight, *Utilitas Math.* 9 (1976), 263-281.

[89] J. Seberry, and R. Craigen, Orthogonal designs, in *Handbook of Combinatorial Designs*, C.J.Colbourn and J.H.Dinitz (Eds.), CRC Press, (1996), 400-406.

[90] J. Seberry and A.L. Whiteman, New Hadamard matrices and conference matrices obtained via Mathon's construction, *Graphs and Combinatorics*, 4 (1988), 355-377.

[91] J. Seberry, and M. Yamada, Hadamard matrices, sequences and block designs, *Contemporary Design Theory:A Collection of Surveys*, eds. J.Dinitz and D.Stinson, J.Wiley, New York, (1992), 431- 560.

[92] E. Spence, Regular two-graphs on 36 vertices, *Linear Alg. Appl.*, 226-228 (1995), 459–497.

[93] R.G. Stanton and D.A. Sprott, A family of difference sets, *Canad. J. Math.*, 10 (1958), 73-77.

[94] W. R. Stevens, UNIX Network Programming: Networking APIs: Sockets and XTI, volume 1, Prentice Hall, second edition, 1998.

[95] T. Storer, *Cyclotomy and difference sets*, Lectures in Advanced Mathematics 2, Markham Publishing Company, Chicago, 1967.

[96] V. D. Tonchev, Hadamard matrices of order 36 with automorphism of order 17, *Nagoya Math. J.*, 104 (1986), 163–174.

[97] S. Topalova, Hadamard matrices of order 44 with automorphisms of order 7, *Discrete Math.*, (to appear).

[98] S.A. Tretter, *Introduction to Discrete–time Signal Processing*, John Wiley & Sons, New York, 1976.

[99] R. J. Turyn, An infinite class of Williamson matrices, *J. Combin. Theory Ser. A*, 12 (1972), 319-321.

[100] R. J. Turyn, Hadamard matrices, Baumert-Hall units, four symbol sequences, pulse compression and surface wave encoding *J. Combin. Theory Ser. A*, 16 (1974), 313-333.

[101] J. Wallis, Orthogonal $(0, 1, -1)$-matrices, *Proceedings of the First Australian Conference on Combinatorial Mathematics*, (ed. Jennifer Wallis and W.D.Wallis), TUNRA Ltd, Newcastle, Australia, pp. 61-84, 1972.

[102] W. D. Wallis, A. P. Street, and J. Seberry Wallis, *Combinatorics: Room Squares, Sum-Free Sets Hadamard Matrices*, Lecture Notes in Mathematics, Vol. 292, Springer-Verlag, Berlin, Heidelberg, New York, 1972.

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

[104] A. L. Whiteman, An infinite family of Hadamard matrices of Williamson type, *J. Combin. Theory Ser. A*, 14 (1973), 334–340.

[105] J. Williamson, Hadamard's determinant theorem an the sum of four squares. *Duke Math. J.*, 11 (1944), 65-81.

[106] M. Yamada, On the Williamson type j matrices of orders $4 \cdot 29, 4 \cdot 41$ and $4 \cdot 37$, *J. Combin. Theory Ser. A*, 27 (1979), 378–381.

[107] C. H. Yang, On Hadamard matrices constructible by circulant submatrices, *Math. Comput.*, 25 (1971), 181-186.