# A META-SOFTWARE SYSTEM FOR ORTHOGONAL DESIGNS AND HADAMARD MATRICES 

I. S. KOTSIREAS, C. KOUKOUVINOS* AND D. E. SIMOS


#### Abstract

In this paper, we construct inequivalent Hadamard matrices based on several new and old full orthogonal designs, using circulant and symmetric block matrices. Not all orthogonal designs produce inequivalent Hadamard matrices, because the corresponding systems of equations do not possess solutions. The systems of equations arising when we search for inequivalent Hadamard matrices from full orthogonal designs using circulant and symmetric block matrices, can be concisely described using the periodic autocorrelation function of the generators of the block matrices. We use Maple, Magma, C and Unix tools to find many new inequivalent Hadamard matrices.


AMS Mathematics Subject Classification : 05B20, 68R05, 68W30.
Key words and phrases : Hadamard matrices, meta-programming, orthogonal designs.

## 1. Introduction

Definition 1.1. Let $x_{1}, \ldots, x_{t}$ be commuting indeterminates. An orthogonal design $X$ of order $n$ and type $\left(s_{1}, \ldots, s_{t}\right)$ denoted $\operatorname{OD}\left(n ; s_{1}, \ldots, s_{t}\right)$, where $s_{1}, \ldots$, $s_{t}$ are positive integers, is a matrix of order $n$ with entries from $\left\{0, \pm x_{1}, \ldots, \pm x_{t}\right\}$, such that

$$
X X^{t}=\left(\sum_{i=1}^{t} s_{i} x_{i}^{2}\right) I_{n}
$$

where $X^{t}$ denotes the transpose of $X$ and $I_{n}$ denotes the identity matrix of order $n$.

Orthogonal designs are used in Combinatorics, Statistics, Coding Theory, Telecommunications and other areas. For more details on orthogonal designs see $[5,28]$ and on Hadamard matrices see [2].

[^0]The concepts of the periodic (PAF) and non-periodic (NPAF) autocorrelation functions are described in [17].

## 2. Applications of Hadamard matrices

We give some references to works describing applications of Hadamard matrices. We do not aim to provide a comprehensive, or by all means complete, treatment of the subject, as this is not the purpose of the present paper. We are merely interesting in giving a flavor of the many different application areas involved, in order to exhibit that while Hadamard matrices are specialized types of orthogonal designs their applications are of a broader interest.

As first noted in [26], Hadamard matrices are used in Statistics where they generate optimal statistical designs used in weighing experiments. Hadamard matrices play an important role also in Coding Theory where they generated the so called Hadamard codes ([22]), i.e. error-correcting codes that correct the maximum number of errors. It is worthwhile to note that, a Hadamard code was used during the 1971 space probe Mariner 9 mission by NASA to correct for picture transmission error. The Mariner 9 mission and the Coding Theory used in that project are the subjects of [27] and [29].

Hadamard matrices are used in Telecommunications where they generate sequences used in digital communications and in Optics for the improvement of the quality and resolution of image scanners. More details, regarding their applications in communications and signal/image processing can be found in [30]. Last but not least, Hadamard matrices play an important role in Numerical Analysis in the study of the growth factor of Gaussian Elimination with Complete Pivoting ([3]). Hadamard matrices, are the only known matrices till today that achieve a growth factor equal to their dimension.

## 3. Sequences with zero periodic autocorrelation function and orthogonal designs

The classical Williamson array

$$
H=\left(\begin{array}{cccc}
A & B & C & D \\
-B & A & -D & C \\
-C & D & A & -B \\
-D & -C & B & A
\end{array}\right)
$$

has been used to construct inequivalent Hadamard matrices [6]. Specifically, let $U$ be the matrix of order $n$

$$
U=\left(\begin{array}{ccccc}
0 & 1 & 0 & \ldots & 0 \\
0 & 0 & 1 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ldots & \vdots \\
0 & 0 & 0 & \ldots & 1 \\
1 & 0 & 0 & \ldots & 0
\end{array}\right)
$$

which has the property $U^{n}=I_{n}$. The matrix $U$ is used to define the block matrices of order $n$ in the classical Williamson array, as polynomials in $U$ with $\pm 1$ coefficients. Then the block matrices will commute with each other. Moreover, by imposing symmetry conditions on the coefficients, the block matrices will be symmetric, in view of the fact that $U^{T}=U^{-1}$. The four matrices $A, B, C, D$ are defined by polynomials in $U$ as follows:

$$
\begin{align*}
& A=a_{0} I_{n}+a_{1} U+\cdots \\
& B=b_{0} I_{n}+b_{1} U+\cdots a_{n-1} U^{n-1} \\
& C=c_{1} I_{n}+c_{1} U+\cdots b_{n-1} U^{n-1}  \tag{1}\\
& D=d_{0} I_{n}+d_{1} U+\cdots
\end{align*}+c_{n-1} U^{n-1} 1+d_{n-1} U^{n-1} .
$$

where the $4 n$ coefficients $a_{0}, \ldots, a_{n-1}, b_{0}, \ldots, b_{n-1}, c_{0}, \ldots, c_{n-1}, d_{0}, \ldots, d_{n-1}$ satisfy the additional symmetry conditions

$$
\begin{equation*}
a_{n-i}=a_{i}, b_{n-i}=b_{i}, c_{n-i}=c_{i}, d_{n-i}=d_{i}, i=1, \ldots, n-1 . \tag{2}
\end{equation*}
$$

Then the requirement $H H^{t}=(4 n) I_{4 n}$ gives rise to a system of polynomial equations in the $2 n+2$ indeterminates (take $n$ to be odd)

It is conceivable to use the same process with more general arrays that the Williamson array, i.e. with full orthogonal designs, to look for inequivalent Hadamard matrices.

Let $m$ be a multiple of 4 and let $O D\left(m ; a_{1}, \ldots, a_{k}\right)$ be a full orthogonal de$\operatorname{sign}\left(a_{1}+\cdots+a_{k}=m\right)$ of order $m$ with $k$ variables $(k \leq \rho(m)$ where $\rho(m)$ denotes the Radon function [5]). Then we can replace each variable appearing in the full orthogonal design by a matrix of order $n$ that we build with the matrix $U$ and the necessary number of indeterminates. We wrote a meta-meta program (described in the next section) to implement this idea more systematically. After using our program with several different orthogonal designs, we give the following formalism which allows one to use the PAF concept [17] to provide a concise description of the systems of polynomial equations that arise in the search for inequivalent Hadamard matrices from orthogonal designs. This formalism enables one to determine whether certain blocks are suitable for the construction of a Hadamard matrix from a given orthogonal design as a system of linear equations.

In particular, consider $n$ to be an odd integer such that $n \geq 3$ and set $p=\frac{n-1}{2}$. For all values of $i$ from 1 to $k$, suppose that each of the $a_{i}$ equal variables in the rows/columns of the orthogonal design is replaced by an $n \times n$ circulant and symmetric matrix of indeterminates $A_{i}$. When $A_{i}$ is constructed as a polynomial via the matrix $U$, then a sequence of $p+1$ indeterminates $A_{i}^{p}=\left[a_{i}^{0}, \ldots, a_{i}^{p}\right]$ suffices to fully describe $A_{i}$. Denote by $O$ the resulting $m n \times m n$ matrix. Then the relationship $O O^{t}=(m n) I_{m n}$ gives rise to the following system of $p$ polynomial
equations in $k(p+1)$ binary unknowns:

$$
\begin{array}{ccc}
a_{1} P A F_{A_{1}^{p}(1)} & +\cdots+a_{k} P A F_{A_{k}^{p}}(1) & +\frac{m}{2}=0 \\
\vdots & \vdots & \vdots  \tag{3}\\
a_{1} P A F_{A_{1}^{p}}(p) & +\cdots+a_{k} P A F_{A_{k}^{p}}(p) & +\frac{m}{2}=0
\end{array}
$$

In addition, when $g=\operatorname{gcd}\left(a_{1}, \ldots, a_{k}, \frac{m}{2}\right)>1$, these equations can be simplified by dividing throughout by $g$.
Example 3.1. To illustrate the application of the previous formalism, suppose we are given the full orthogonal design of order $16, O D(16 ; 1,2,2,2,2,2,2,3)$ in 8 variables $a, b, c, d, e, f, g, h$ :

$$
\left[\begin{array}{cccccccccccccccc}
a & b & b & b & c & c & d & d & e & e & f & f & g & g & h & h \\
-b & a & b & -b & c & -c & d & -d & e & -e & f & -f & g & -g & h & -h \\
b & b & -a & -b & -d & -d & c & c & -f & -f & e & e & -h & -h & g & g \\
b-b & b & -a & -d & d & c & -c & -f & f & e & -e & -h & h & g & -g & \\
-c & -c & -d & -d & a & b & b & b & g & g & -h & -h & -e & -e & f & f \\
-c & c & -d & d & -b & a & b & -b & g & -g & -h & h & -e & e & f & -f \\
d & d & -c & -c & b & b & -a & -b & h & h & g & g & -f & -f & -e & -e \\
d & -d & -c & c & b & -b & b & -a & h & -h & g & -g & -f & f & -e & e \\
-e & -e & -f & -f & -g & -g & h & h & a & b & b & b & c & c & -d & -d \\
-e & e & -f & f & -g & g & h & -h & -b & a & b & -b & c & -c & -d & d \\
f & f & -e & -e & -h & -h & -g & -g & b & b & -a & -b & d & d & c & c \\
f & -f & -e & e & -h & h & -g & g & b & -b & b & -a & d & -d & c & -c \\
-g & -g & -h & -h & e & e & -f & -f & -c & -c & d & d & a & b & b & b \\
-g & g & -h & h & e & -e & -f & f & -c & c & d & -d & -b & a & b & -b \\
h & h & -g & -g & f & f & e & e & -d & -d & -c & -c & b & b & -a & -b \\
h & -h & -g & g & f & -f & e & -e & -d & d & -c & c & b & -b & b & -a
\end{array}\right]
$$

and that we are replacing each variable by a symmetric and circulant matrix of order $n$. Then we can write down directly the system of polynomial equations that arise in an efficient fashion for hard computation in a machine.

- $n=3, m=16, p=1$

$$
a_{0} a_{1}+3 b_{0} b_{1}+2 c_{0} c_{1}+2 d_{0} d_{1}+2 e_{0} e_{1}+2 f_{0} f_{1}+2 g_{0} g_{1}+2 h_{0} h_{1}+8=0
$$

The above equation has 4096 solutions, when all variables take $\pm 1$ values.
One solution (in the format $\left[a_{0} a_{1} b_{0} b_{1} c_{0} c_{1} d_{0} d_{1} e_{0} e_{1} f_{0} f_{1} g_{0} g_{1} h_{0} h_{1}\right]$ ) is given by:

$$
[-1,-1,-1,-1,-1,1,-1,1,-1,1,1,-1,-1,1,1,-1]
$$

These solutions give rise to 4096 Hadamard matrices of order $16 \cdot 3=$ 48. Now we search for inequivalent Hadamard matrices of order 48 using Magma, within this set of 4096 Hadamard matrices.

- $n=5, m=16, p=2$

$$
a_{0} a_{2}+a_{1} a_{2}+3 b_{0} b_{2}+3 b_{1} b_{2}+2 c_{0} c_{2}+2 c_{1} c_{2}+2 d_{0} d_{2}+2 d_{1} d_{2}+
$$

$$
2 e_{0} e_{2}+2 e_{1} e_{2}+2 f_{0} f_{2}+2 f_{1} f_{2}+2 g_{0} g_{2}+2 g_{1} g_{2}+2 h_{0} h_{2}+2 h_{1} h_{2}+8=0
$$

$$
\begin{gathered}
a_{0} a_{1}+a_{1} a 2+3 b_{0} b_{1}+3 b_{1} b_{2}+2 c_{0} c_{1}+2 c_{1} c_{2}+2 d_{0} d_{1}+2 d_{1} d_{2}+ \\
2 e_{0} e_{1}+2 e_{1} e_{2}+2 f_{0} f_{1}+2 f_{1} f_{2}+2 g_{0} g_{1}+2 g_{1} g_{2}+2 h_{0} h_{1}+2 h_{1} h_{2}+8=0
\end{gathered}
$$

The above equations have 92160 solutions, when all variables take $\pm 1$ values. One solution (in the format $\left[a_{0} a_{1} a_{2} b_{0} b_{1} b_{2} c_{0} c_{1} c_{2} d_{0} d_{1} d_{2} e_{0} e_{1} e_{2} f_{0} f_{1}\right.$ $\left.f_{2} g_{0} g_{1} g_{2} h_{0} h_{1} h_{2}\right]$ ) is given by:
$[-1,-1,1,-1,-1,1,-1,-1,-1,-1,-1,1,-1,1,-1,-1$,
$1,-1,-1,1,1,-1,1,-1]$
These solutions give rise to 92160 Hadamard matrices of order $16 \cdot 5=$ 80. Now we search for inequivalent Hadamard matrices of order 80 using Magma, within this set of 92160 Hadamard matrices.

- $n=7, m=16, p=3$

$$
a_{0} a_{2}+a_{1} a_{3}+a_{2} a_{3}+3 b_{0} b_{2}+3 b_{1} b_{3}+3 b_{2} b_{3}+2 c_{0} c_{2}+2 c_{1} c_{3}+2 c_{2} c_{3}+2 d_{0} d_{2}+
$$

$$
2 d_{1} d_{3}+2 d_{2} d_{3}+2 e_{0} e_{2}+2 e_{1} e_{3}+2 e_{2} e_{3}+2 f_{0} f_{2}+2 f_{1} f_{3}+2 f_{2} f_{3}+2 g_{0} g_{2}+
$$

$$
2 g_{1} g_{3}+2 g_{2} g_{3}+2 h_{0} h_{2}+2 h_{1} h_{3}+2 h_{2} h_{3}+8=0
$$

$$
a_{2} a_{3}+a_{0} a_{1}+a_{1} a_{2}+3 b_{2} b_{3}+2 c_{2} c_{3}+2 d_{2} d_{3}+2 e_{2} e_{3}+2 f_{2} f_{3}+2 g_{2} g_{3}+
$$

$$
2 h_{2} h_{3}+3 b_{0} b_{1}+3 b_{1} b_{2}+2 c_{0} c_{1}+2 c_{1} c_{2}+2 d_{0} d_{1}+2 d_{1} d_{2}+2 e_{0} e_{1}+2 e_{1} e_{2}+
$$

$$
2 f_{0} f_{1}+2 f_{1} f_{2}+2 g_{0} g_{1}+2 g_{1} g_{2}+2 h_{0} h_{1}+2 h_{1} h_{2}+8=0
$$

$$
a_{1} a_{3}+a_{1} a_{2}+a_{0} a_{3}+3 b_{1} b_{3}+2 c_{1} c_{3}+2 d_{1} d_{3}+2 e_{1} e_{3}+2 f_{1} f_{3}+2 g_{1} g_{3}+
$$

$$
2 h_{1} h_{3}+3 b_{1} b_{2}+2 c_{1} c_{2}+2 d_{1} d_{2}+2 e_{1} e_{2}+2 f_{1} f_{2}+2 g_{1} g_{2}+2 h_{1} h_{2}+3 b_{0} b_{3}+
$$

$$
2 c_{0} c_{3}+2 d_{0} d_{3}+2 e_{0} e_{3}+2 f_{0} f_{3}+2 g_{0} g_{3}+2 h_{0} h_{3}+8=0
$$

The above equations have 1105920 solutions, when all variables take $\pm 1$ values. One solution (in the format $\left[a_{0} a_{1} a_{2} a_{3} b_{0} b_{1} b_{2} b_{3} c_{0} c_{1} c_{2} c_{3} d_{0} d_{1} d_{2} d_{3}\right.$ $\left.\left.e_{0} e_{1} e_{2} e_{3} f_{0} f_{1} f_{2} f_{3} g_{0} g_{1} g_{2} g_{3} h_{0} h_{1} h_{2} h_{3}\right]\right)$ is given by:
$[-1,-1,-1,1,-1,-1,-1,1,-1,-1,-1,1,-1,-1,-1,1$,
$-1,-1,1,-1,-1,-1,1,-1,1,-1,1,-1,-1,1,-1,1]$
These solutions give rise to 1105920 Hadamard matrices of order 16 . $7=112$. Now we search for inequivalent Hadamard matrices of order 112 using Magma, within this set of 1105920 Hadamard matrices.

## 4. Meta-meta programming for orthogonal designs

Meta-programming is not a new concept, and has been successfully employed before in cases where software reuse, the process of creating software systems from existing software rather than building software systems from scratch, was neeeded [19]. Before continuing we will list some uses of meta-programming:

- Generation - metacode that generates code
- Transformation - metacode that modifies code (similar to generation)
- Translation - transformation into another language
- Analysis - metacode that analyzes code

The metasoftware we have developed for orthogonal designs and Hadamard matrices in order to search for inequivalent Hadamard matrices makes efficient use of all previous four methods of meta-programming. In particular, the metaprogram is using bash shell as its metalanguage whilst the object-language that each program is manipulated are the Computer Algebra Systems, Maple and

Magma. Maple provides an excellent way for performing symbolic and numerical computations, especially when we have to interpret methods that are based on combinatorial mathematics. We implemented a Maple package containing the necessary constructions for the generation of Hadamard matrices from orthogonal designs in Maple, in order to achieve the best possible flexibility in terms of portability with other Computational Algebra Systems, such as Magma. We finally used Magma to automatically perform the searches for inequivalent Hadamard matrices. Earlier attempts of software systems capable to perform searches for inequivalent Hadamard matrices could be found in [4], [11], [12], [13], [15] and [16]. A recent application of the presented metasoftware can be found in [18]. The metasoftware given below, could be seen as a unification and further expansion of the aforementioned works which leads to the production of large databases of new inequivalent Hadamard matrices. All details of the presented metasoftware from an algorithmic perspective are presented in this Section, in Algorithm 1.

We wrote a meta-meta program that accepts as input a text file with an orthogonal design and produces a Maple file that produces a C file that can be compiled and executed to solve exhaustively the system of equations corresponding to this orthogonal design. The meta-meta program is using bash shell, and the CodeGeneration Maple package. Some of the principal difficulties in the design of this program lie in the dynamic production of the values of the variables that capture the characteristics of the orthogonal design in the input text file, i.e. the order, the number of variables and the list of different variables. We give below in pseudo-code the meta-meta program we have used.

In particular, the systems of equations arising from the search for inequivalent Hadamard matrices from full orthogonal designs using circulant and symmetric block matrices, can be solved using high-performance computing. Not all orthogonal designs produce inequivalent Hadamard matrices, because the corresponding systems of equations may (or may not) posses solutions, as it was shown in [10]. We used Maple to automatically generate C programs that we subsequently parallelized via a bash/sed/awk script. In detail, two-phase metaprogram that accepts as input a text file with an orthogonal design and produces a Maple file that produces a C file that can be compiled and executed to solve exhaustively the system of equations corresponding to this orthogonal design. The meta-meta program is using bash shell, and the CodeGeneration Maple package. The use of scripting and meta-programming with Maple's automatic code generation functionalities, ensure efficient and correct prototyping. During the second phase, the program uses Magma to build a Hadamard matrix corresponding to each solution found and then uses the buckets algorithm, given in [8], to locate inequivalent Hadamard matrices. The constructive bounds on the number of inequivalent Hadamard matrices are constantly updated on the Web. Another important outcome of this on-going project is the interaction with Coding Theory, via self-dual code constructions based on Hadamard matrices for instance.

```
Algorithm 1 HMOD
    procedure \(\operatorname{HMOD}(O D, n) \quad \triangleright \mathrm{n}\) is the size of block matrices
Require: \(n\) odd
Ensure: Generation of binary vectors corresponding to Hadamard matrices
    validate that given \(O D\) is an orthogonal design
    do awk to detect the order and the variables of the \(O D\)
    assign variable names to the variables of the \(O D\)
    calculate the order of Hadamard matrices
    assign a list to the \(k\) variables of the \(O D\)
    set \(p\) equal to \((n-1) / 2\)
    transform in Maple format given inputs
    create Maple input file from \(O D\) and the variables of the \(O D \triangleright\) Begin Maple
    phase
            begin for loop from 1 to \(k\)
    create the sequence of \(p+1\) indeterminates
    replace the \(O D\) variables with symmetric circulant matrices
        end for loop
        begin for loop from 1 to \(p\)
    compute \(P A F\) equations from relation (3)
        end for loop
    do sed to create a Maple file containing the polynomial equations
    call procedure Maple2C to convert the equations in C format \(\triangleright\) End Maple phase
    compile the C file \(\quad \triangleright\) Begin C phase
    execute the C executable \(\triangleright\) End C phase
    do sed/awk to convert the output into solutions in Magma format
    return solutions as binary vectors representing the Hadamard matrices
    end procedure
    procedure Maple2C(PolEqs) \(\triangleright\) PolEqs are the polynomial equations in Maple
    format
Require: Polynomial equations in Maple format
Ensure: Conversion to C format
    call CodeGeneration Maple package
    declare types of variables in C and procedures to be converted
    execute C conversion of polynomial equations
    return the polynomial equations in C format
    end procedure
```


## 5. Specific full orthogonal designs

Using algorithm 1 we searched for inequivalent Hadamard matrices with the 41 full orthogonal designs listed below. The first orthogonal design in the list below is the classical Williamson array, that we included in our search simply for consistency check purposes. The remaining 40 full orthogonal designs appear in the book [5] or were found in the papers [7], [9], [14].

TABLE 1. List of orthogonal designs used by algorithm 1

| OD $(4 ; 1,1,1,1)$ | OD $(16 ; 1,1,1,1,3,3,3,3)$ |
| :--- | :--- |
| OD $(16 ; 1,2,2,2,2,2,2,3)$ | OD $(24 ; 1,1,1,1,2,2,8,8)$ |
| OD $(24 ; 1,1,1,1,5,5,5,5)$ | OD $(24 ; 1,1,2,2,3,3,6,6)$ |
| OD $(24 ; 1,4,4,15)$ | OD $(24 ; 2,2,2,2,4,4,4,4)$ |
| OD $(24 ; 3,3,3,3,3,3,3,3)$ | OD $(32 ; 4,4,4,4,4,4,4,4)$ |
| OD $(32 ; 4,4,4,4,8,8)$ | OD $(40 ; 1,1,1,1,9,9,9,9)$ |
| OD $(40 ; 1,1,1,2,9,26)$ | OD $(40 ; 1,1,2,2,17,17)$ |
| OD $(40 ; 2,2,2,2,8,8,8,8)$ | OD $(40 ; 2,2,5,5,5,5,8,8)$ |
| OD $(40 ; 5,5,5,5,5,5,5,5)$ | OD $(56 ; 1,1,2,2,25,25)$ |
| OD $(56 ; 4,4,4,4,10,10,10,10)$ | OD $(56 ; 7,7,7,7,7,7,7,7)$ |
| OD $(64 ; 16,16,16,16)$ | OD $(64 ; 4,4,4,4,12,12,12,12)$ |
| OD $(64 ; 4,4,8,8,8,8,8,8,8)$ | OD $(64 ; 4,8,8,8,8,8,8,12)$ |
| OD $(64 ; 8,8,8,8,16,16)$ | OD $(64 ; 8,8,8,8,8,8,8,8)$ |
| OD $(96 ; 4,4,4,4,20,20,20,20)$ | OD $(96 ; 8,8,8,8,16,16,16,16)$ |
| OD $(128 ; 16,16,16,16,16,16,16,16)$ | OD $(128 ; 8,16,16,16,16,16,16,24)$ |
| OD $(128 ; 8,8,16,16,16,16,16,16,16)$ | OD $(128 ; 8,8,8,8,24,24,24,24)$ |
| OD $(144 ; 12,12,12,12,24,24,24,24)$ | OD $(144 ; 4,4,4,4,32,32,32,32)$ |
| OD $(112 ; 14,14,14,14,14,14,14,14)$ | OD $(80 ; 4,4,10,10,10,10,16,16)$ |
| OD $(112 ; 8,8,8,8,20,20,20,20)$ | OD $(80 ; 4,4,4,4,16,16,16,16)$ |
| OD $(144 ; 18,18,18,18,18,18,18,18)$ | OD $(96 ; 12,12,12,12,12,12,12,12)$ |
| OD $(80 ; 10,10,10,10,10,10,10,10)$ |  |

## 6. Inequivalent Hadamard matrices

The importance of using orthogonal designs to look for inequivalent Hadamard matrices of several orders, is exhibited by the fact that the larger the order of the orthogonal design and the fewer the number of variables in it, the less equations and variables we need to look for inequivalent Hadamard matrices of large orders. To illustrate this point, consider the full orthogonal design

$$
O D(144 ; 4,4,4,4,32,32,32,32)
$$

of order 144 in 8 variables. When we use algorithm HMOD with $n=5$, then we are constructing Hadamard matrices of order 432 by solving an easy system of 2 equations in 32 binary variables. However, if we were to use the classical Williamson array for instance, to construct Hadamard matrices of order 432, then we would need to consider block matrices of order $n=108$, which is currently entirely outside the scope of any known algorithm.
The computations are using Magma V 2.13 and are still on-going. With $N_{n}$ in the following tables we denote the number of inequivalent Hadamard matrices found for each order $n$.

Table 2. Constructive lower bounds for inequivalent Hadamard matrices of order 40 to 168

| $n$ | 40 | 48 | 72 | 80 | 96 | 112 | 120 | 160 | 168 |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| $N_{n}$ | 8 | 10 | 238 | 30 | 3 | 122 | 5161 | 8 | 6760 |

TABLE 3. Constructive lower bounds for inequivalent Hadamard matrices of order 192 to 448

| $n$ | 192 | 200 | 240 | 280 | 320 | 400 | 448 |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| $N_{n}$ | 14 | 7246 | 148 | 2940 | 34 | 818 | 10 |

Remark 6.1. We note that the presented Hadamard matrices in the Tables, that are constructed using orthogonal designs, are inequivalent since for each order we found that the corresponding 4-profiles are different.

In addition, one could check the generated Hadamard matrices from orthogonal designs for inequivalence using the graph isomorphism criterion, which is more time consuming [1, 23], but locates much more inequivalent Hadamard matrices.

The complete classification for Hadamard matrices of order n is well known for $n \equiv 0(\bmod 4), n \leq 28$. For $n=32,36$ there are at least $3,578,006$ and $4,745,357$ inequivalent Hadamard matrices respectively, see [25]. On the other hand, there are some theoretical results which provide huge lower bounds, see $[20,21,24]$ but these matrices are not available. From this perspective we believe that our lower bounds on the number of inequivalent Hadamard matrices, which are presented in this section have value for practitioners in the fields of Combinatorics and Statistics (see Section 2) since these are constructive. Moreover, the given inequivalent Hadamard matrices are only a sample; considering that the list of the 41 full orthogonal designs given in Section 5, is by no means complete. The main aim of the presented metasoftware is to establish a computational framework for the automated construction of inequivalent Hadamard matrices, whenever this is desired by the specialists of Design Theory and its applications.

## Acknowledgements

The research of the first author was supported in part by an NSERC grant. The research of the third author was financially supported by a scholarship awarded by the Secretariat of the Research Committee of National Technical University of Athens. All computations in Computer Algebra System, Maple were performed remotely at the Centre de calcul formel MEDICIS, École Polytechnique, Paris, France. All computations in Computational Algebra System, Magma and in programming language, C were performed remotely at SHARCnet high performance computing clusters.

## References

1. W. Bosma and J. Cannon, Handbook of Magma Functions, Version 2.9, Sydney, July, 2002.
2. R. Craigen, Hadamard Matrices and Designs, In: Colbourn, C.J., Dinitz, J.H., (eds.) The CRC Handbook of Combinatorial Designs. pp. 370-377. CRC Press, Boca Raton, Fla., 1996.
3. J. Day and B. Peterson, Growth in gaussian elimination, The American Mathematical Monthly 95 (1988), 489-513.
4. S. Georgiou, I.S. Kotsireas and C. Koukouvinos, Inequivalent Hadamard matrices of order $2 n$ constructed from Hadamard matrices of order $n$, J. Combin. Math. Combin. Comput. 63 (2007), 65-79.
5. A.V. Geramita and J. Seberry, Orthogonal Designs. Quadratic Forms and Hadamard Matrices. Lecture Notes in Pure and Applied Mathematics, 45. Marcel Dekker, Inc., New York, 1979.
6. M. Hall, Jr., Combinatorial Theory, Reprint of the 1986 second edition, Wiley Classics Library, Wiley, New York, 1998.
7. W.H. Holzmann and H. Kharaghani, On the Plotkin arrays, Australas. J. Combin. 22 (2000), 287-299.
8. I.S. Kotsireas and C. Koukouvinos, Inequivalent Hadamard matrices with buckets, J. Discrete Math. Sci. Cryptogr. 7 (2004), 307-317.
9. I.S. Kotsireas and C. Koukouvinos, Orthogonal designs via computational algebra, J. of Comb. Designs 14 (2006), 351-362.
10. I.S. Kotsireas and C. Koukouvinos, Inequivalent Hadamard matrices from Orthogonal Designs. In: Proceedings of the 2007 International Workshop on Parallel Symbolic Computation, pp. 95-97. ACM, London, Ontario, Canada, 2007.
11. I.S. Kotsireas and C. Koukouvinos, New skew-Hadamard matrices via computational algebra, Australas. J. Combin. 41 (2008), 235-248.
12. I.S. Kotsireas, C. Koukouvinos, and G. Pinheiro, Metasoftware for Hadamard matrices, Int. J. Appl. Math. 18 (2005), 263-278.
13. I.S. Kotsireas, C. Koukouvinos and J. Seberry, Hadamard ideals and Hadamard matrices with two circulant cores, European J. Combin. 27 (2006), 658-668.
14. I.S. Kotsireas, C. Koukouvinos and D.E. Simos, Large orthogonal designs via amicable sets of matrices, Int. J. Appl. Math. 12 (2006), 217-232.
15. I.S. Kotsireas, C. Koukouvinos and D.E. Simos, Inequivalent Hadamard matrices from base sequences, Util. Math. 78 (2009), 3-9.
16. I.S. Kotsireas, C. Koukouvinos and D.E. Simos, Inequivalent Hadamard matrices from near normal sequences, J. Combin. Math. Combin. Comput. 75 (2010), 105-115.
17. C. Koukouvinos, Sequences with Zero Autocorrelation, In: Colbourn, C.J., Dinitz, J.H., (eds.) The CRC Handbook of Combinatorial Designs. pp. 452-456. CRC Press, Boca Raton, Fla., 1996.
18. C. Koukouvinos and D.E. Simos, Improving the lower bounds on inequivalent Hadamard matrices through orthogonal designs and meta-programming techniques, Appl. Numer. Math. 60 (2010), 370-377.
19. C.W. Krueger, Software reuse, ACM computing surveys 24 (1992), 131-183.
20. 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.
21. C. Lam, S. Lam and V.D. Tonchev, Bounds on the number of Hadamard designs of even order, J. Combin. Designs 9 (2001), 363-378.
22. F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, The Netherlands, North-Holland, Amsterdam, 1977.
23. B.D. McKay, Hadamard equivalence via graph isomorphism, Discrete Math. 27 (1979), 213-214.
24. E. Merchant, Exponentially many Hadamard designs, Des. Codes. Crypt. 38 (2006), 297308.
25. W.P. Orrick, Switching operations for Hadamard matrices, SIAM J. Discrete Math. 22 (2008), 31-50.
26. L.R. Plackett and J.P. Burman, The design of optimum multifactorial experiments, Biometrika 33 (1946), 305-325.
27. E.C. Posner, Combinatorial Structures in Planetary Reconnaissance, In: Mann, H.B., (eds) Error Correcting Codes, Wiley, N.Y., 1968.
28. J. Seberry and R. Craigen, Orthogonal Designs, In: Colbourn, C.J., Dinitz, J.H., (eds.) The CRC Handbook of Combinatorial Designs, pp. 400-406. CRC Press, Boca Raton, Fla., 1996.
29. J.H. Van Lint, Coding, decoding and Combinatorics, In: Wilson, R.J., (eds.) Applications of Combinatorics, Shiva, Cheshire, 1982.
30. R.K. Yarlagadda and J.E. Hershey, Hadamard Matrix Analysis and Synthesis: With Applications to Communications and Signal/Image Processing, Kluwer Acad. Pub., Boston, 1997.

Ilias S. Kotsireas is an Associate Professor at Wilfrid Laurier University, Department of Physics and Computer Science. He received his Bachelor in Mathematics (1990) from the University of Athens, and obtained both his MSc (1995) and PhD (1998) in Computer Science from Université Paris 6. He is the author of several papers in the field of Computer Algebra and Combinatorics and on the Editorial board of three related journals. His research interests include computer algebra, symbolic computation and combinatorial designs.
Wilfrid Laurier University, Department of Physics and Computer Science, 75 University Avenue West, Waterloo, Ontario N2L 3C5, Canada.
e-mail: ikotsire@wlu.ca
Christos Koukouvinos is a Professor at the National Technical University of Athens, Department of Mathematics. He holds a Bachelor in Mathematics (1983) and a PhD (1988) in Statistics both obtained from the University of Thessaloniki. He is the author of numerous papers in the field of Statistics and Combinatorics and on the Editorial board of seven related journals. He was awarded the prestigious Hall Medal of the Institute of Combinatorics and its Applications (ICA) in 1996. He is a Fellow of the ICA and was member of Council of the ICA from 2000 to 2003. His research interests include statistical experimental and optimal designs, combinatorial designs and coding theory.
Department of Mathematics, National Technical University of Athens, Zografou 15773, Athens, Greece.
e-mail: ckoukouv@math.ntua.gr
Dimitris E. Simos received his Bachelor in Mathematics (2006) from the University of Athens, and MSc in Applied Mathematical Sciences (2007) from the National Technical University of Athens. He is currently a PhD candidate at National Technical University of Athens since 2008. He is the author of several papers in the field of Combinatorics. He is an Associate Fellow of the Institute of Combinatorics and its Applications (ICA). His research interests include combinatorial designs, coding theory, cryptography, symbolic computation and heuristics.
Department of Mathematics, National Technical University of Athens, Zografou 15773, Athens, Greece.
e-mail: dsimos@math.ntua.gr


[^0]:    Received January 10, 2011. Accepted June 7, 2011. * Corresponding author. (c) 2011 Korean SIGCAM and KSCAM.

