Inequivalent Hadamard matrices of order $2n$ constructed from Hadamard matrices of order n

S. Georgiou
Department of Statistics and
Actuarial-Financial Mathematics,
University of the Aegean,
Karlovassi 83200, Samos, Greece.

I. Kotsireas
Department of Physics and Computer Science,
Wilfrid Laurier University,
75 University Avenue West,
Waterloo, Ontario N2L 3C5, Canada.

C. Koukouvinos
Department of Mathematics
National Technical University of Athens
Zografou 15773, Athens, Greece

Abstract

In this paper we establish a doubling method to construct inequivalent Hadamard matrices of order $2n$, from Hadamard matrices of order n. Our doubling method uses heavily the symmetric group S_n, where n is the order of a Hadamard matrix. We improve the efficiency of the method by introducing some group-theoretical heuristics. Using the doubling method in conjunction with the standard 4-row profile criterion, we have constructed several millions of new inequivalent Hadamard matrices of orders 48, 56, 64, 72, 80, 88, 96 and several hundreds of inequivalent Hadamard matrices of orders 672 and 856. The Magma code segments, included in this paper, allow one to compute many more inequivalent Hadamard matrices of the above orders and all other orders of the form $8t$.

AMS Subject Classification: Primary 05B20, Secondary 62K05
Key words and phrases: Hadamard matrices, inequivalence, doubling construction, profile criterion.

1 Introduction

Hadamard matrices were studied more than a century ago by J. Hadamard in his classical paper [7]. J. J. Sylvester proposed a recursive method for the construction of Hadamard matrices of orders 2^k, see [30]. Since then, Hadamard matrices have attracted the vivid interest of researchers due to their many applications, the simplicity of the concepts involved and the challenging open problems concerning their existence and equivalence. For more details and construction methods for Hadamard matrices, see the book chapters and books [6], [10], [28], [33].

A Hadamard matrix of order n is an $n \times n$ $(1, -1)$-matrix satisfying $HH^T = nI_n$. A Hadamard matrix is normalized if all entries in its first row and column are equal to 1. Two Hadamard matrices are said to be equivalent if one can be transformed into the other by a series of row or column permutations and negations. It is well known that if n is the order of a Hadamard matrix, then n is necessarily $1, 2$ or a multiple of 4.

The difficulty of a discussion of Hadamard equivalence is mainly due to the lack of a good canonical form. The complete classification of Hadamard matrices up to equivalence, has been established for the four orders 16, 20, 24 and 28. We summarize the exact statements of these results and the relevant references.

- Hadamard matrices of orders less than 16 are unique up to equivalence
- There are precisely five equivalence classes at order 16, see [8]
- There are precisely three equivalence classes at order 20, see [9]
- There are precisely 60 equivalence classes at order 24, see [11, 14]
- There are precisely 487 equivalence classes at order 28, see [15, 16].

The classification of Hadamard matrices of orders $n \geq 32$ still remains a difficult open problem since an algorithmic approach based on an exhaustive search is NP hard. We summarize the partial results for $n = 32$. Lin, Wallis and Lie [22] found 66104 inequivalent Hadamard matrices of order 32. Extensive results appear in [23] and [24]. Thus the lower bound for inequivalent Hadamard matrices of order 32 is 66104.

There are at least 217 inequivalent Hadamard matrices of order 36. This lower bound is obtained as follows: Seberry's home page `http://www.uow.edu.au/~jennie` contains 192 inequivalent Hadamard matrices of order 36. These are supplied by E. Spence (180 matrices) see [29], Z. Janko, (1 matrix of Bush-type) see [12] and V. D. Tonchev (11 matrices) see [31]. Using an efficient algorithm and the Magma software [1] Georgiou and Koukouvinos in [4] improved further this bound to 217 by constructing 25 new Hadamard matrices of order 36.

Recently Topalova [32] classified the Hadamard matrices of order 44 with an automorphism of order 7, and found 384 inequivalent Hadamard matrices of this order. In our search using an efficient algorithm and the Magma software [1] we found that 6 of their transposes, are inequivalent to these. Two more Hadamard matrices were given in N. J. A. Sloane's web page `http://www.research.att.com/~njas/hadamard/` (One is the Williamson type Hadamard matrix and the other is the Paley type Hadamard matrix first given in [27]). In [5] this bound was increased to 500.

Lam, Lam and Tonchev [20, 21] showed that the lower bound for inequivalent Hadamard matrices of order $40, 48, 56, 64, 72, 80, 88$ and 96 is $8.18\times10^{11}, 4.34\times10^{23}, 3.47\times10^{24}, 2\times10^{30}, 1.99\times10^{36}, 3.19\times10^{42}, 9.57\times10^{42}$ and 2.4×10^{49} respectively. Even though these are huge theoretical lower bounds, those matrices were not constructed and are not available for practical applications. Thus, the number of available Hadamard matrices, of those orders, is quite small.

In two recent papers, Kotsireas and Koukouvinos [18, 19] used computational algebra, the Williamson arrays and the full orthogonal design $OD(16; 1, 1, 2, 2, 2, 2, 2, 2, 2)$ of order 16, to construct among others: 25, 9, 65, 64, 149, 52, 2664 new inequivalent Hadamard matrices for orders 48, 56, 64, 72, 80, 88, 96 respectively.

In many applications, such as Statistics, Coding Theory, Image Processing, Cryptography and other, many inequivalent Hadamard matrices are needed. In these cases, the great theoretical result of Lam, Lam and Tonchev [20, 21] and the huge lower bounds on the number of inequivalent Hadamard matrices are of limited use since in practical applications the actual matrices are needed and are essential for comparisons and straightforward applications. In this paper, we proposed a new doubling method for constructing Hadamard Matrices of order $2n$ using Hadamard matrices of order n. By using this method, we constructed for the first time some millions of inequivalent Hadamard matrices of those orders. The purpose of this method is to provide an algorithm that can produce some millions of inequivalent Hadamard matrices, of the desirable order, at any time and by anyone who need to use the inequivalent matrices.

2 Equivalent Hadamard matrices for the doubling construction

In this section, we present a doubling method that can be used for constructing new Hadamard matrices of order $2n$. We also investigate the properties needed to obtain inequivalent Hadamard matrices of order $2n$ from equivalent Hadamard matrices of order n.

Theorem 1 (The doubling method) *Let H_1 and H_2 be Hadamard matrices of order n. Then the matrix defined by*

$$H_{2n}(H_1, H_2) = \begin{pmatrix} H_1 & H_1 \\ H_2 & -H_2 \end{pmatrix} \tag{1}$$

is a Hadamard matrix of order $2n$.

Proof. By a simple calculation we see that $H_{2n}(H_1, H_2)H_{2n}(H_1, H_2)^t = (2n)I_{2n}$. □

Using the method described in Theorem 1 we can obtain Hadamard matrices of order $2n$ using two Hadamard matrices of order n. It is not known if equivalent Hadamard matrices of order n can generate inequivalent Hadamard matrices of order $2n$ via this construction method.

From one Hadamard matrix of order n we can obtain $2^{2n}(n!)^2$ equivalent matrices, by applying permutations and multiplications by -1 to the columns and rows of that matrix. In the next lemmas we investigate if it is possible to use equivalent Hadamard matrices of order n in the doubling construction (1) to obtain inequivalent Hadamard matrices of order $2n$.

Lemma 1 *Let H_1 and H_2 be Hadamard matrices of order n. Define H_2' to be the Hadamard matrix derived from H_2 by multiplying some of its rows by -1. Then the Hadamard matrices defined by $H_{2n}(H_1, H_2)$ and $H_{2n}(H_1, H_2')$ are equivalent.*

Proof. Suppose that H_2' derived from H_2 by multiplying the rows numbered $i_1, i_2, \ldots, i_s$ of H_2 by -1. Then the Hadamard matrix $H_{2n}(H_1, H_2)$ becomes identical to $H_{2n}(H_1, H_2')$ if we multiply by -1 the rows $n + i_1, n + i_2, \ldots, n + i_s$ of either. □

Lemma 2 *Let H_1 and H_2 be Hadamard matrices of order n. Define H_2' to be the Hadamard matrix derived from H_2 by permuting some of its rows. Then the Hadamard matrices defined by $H_{2n}(H_1, H_2)$ and $H_{2n}(H_1, H_2')$ are equivalent.*

Proof. Suppose that H_2' derived from H_2 by applying the permutation of rows $\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$, where $(i_1, i_2, \ldots, i_n)$ a permutation of $(1, 2, \ldots, n)$. Then the Hadamard matrix $H_{2n}(H_1, H_2)$ becomes identical to $H_{2n}(H_1, H_2')$ if we apply the permutation

$$\pi' = \begin{pmatrix} 1 & 2 & \ldots & n & n+1 & n+2 & \ldots & 2n \\ 1 & 2 & \ldots & n & n+i_1 & n+i_2 & \ldots & n+i_n \end{pmatrix}$$

to the rows of either. □

Lemma 3 *Let H_1 and H_2 be Hadamard matrices of order n. Define H_2' to be the Hadamard matrix derived from H_2 by multiplying some of its columns by -1. Then the Hadamard matrices defined by $H_{2n}(H_1, H_2)$ and $H_{2n}(H_1, H_2')$ are equivalent.*

Proof. Suppose that H_2' derived from H_2 by multiplying the columns numbered $i_1, i_2, \ldots, i_s$ of H_2 by -1. Then the Hadamard matrix $H_{2n}(H_1, H_2)$ becomes identical to $H_{2n}(H_1, H_2')$ if we exchange the pairs of columns $(i_1, n+i_1)$, $(i_2, n+i_2)$ and $(i_s, n+i_s)$ of either. □

Lemma 4 *Let H_1 and H_2 be Hadamard matrices of order n. Then the Hadamard matrices defined by $H_{2n}(H_1, H_2)$ and $H_{2n}(H_2, H_1)$ are equivalent.*

Proof. We have that $H_{2n}(H_1, H_2) = \begin{pmatrix} H_1 & H_1 \\ H_2 & -H_2 \end{pmatrix}$. By multiplying the last n columns by -1 we obtain the equivalent Hadamard matrix $\begin{pmatrix} H_1 & -H_1 \\ H_2 & H_2 \end{pmatrix}$. By applying the permutation $\begin{pmatrix} 1 & 2 & \ldots & n \\ n+1 & n+2 & \ldots & 2n \end{pmatrix}$ to the rows of that matrix we obtain the equivalent Hadamard matrix $\begin{pmatrix} H_2 & H_2 \\ H_1 & -H_1 \end{pmatrix}$, which is $H_{2n}(H_2, H_1)$. □

Remark 1 From Lemmas 1, 2, 3 and 4 we conclude that equivalent Hadamard matrices of order n might generate inequivalent Hadamard matrices of order $2n$ and that permutations of columns are necessary for achieving the inequivalence. When doubling, the permutations of rows, multiplications of rows or columns by -1, and permuting the matrices H_1 and H_2, generate equivalent Hadamard matrices of order $2n$.

Corollary 1 *Suppose there exist k inequivalent Hadamard matrices of order n. Then, the number of inequivalent Hadamard matrices of order $2n$ obtained by the doubling construction is less or equal to $\frac{k(k+1)n!}{2}$.*

Proof.

Select two matrices (H_i, H_j), $i, j \in \{1, 2, \ldots, k\}$. From Lemma 4 we have that matrices (H_i, H_j) and (H_j, H_i) generate equivalent Hadamard matrices of order $2n$. Thus i should be less or equal to j. So, we have that

$$\#\{(i,j) : i, j = 1, 2, \ldots, k \text{ and } i \leq j\} = \sum_{i=1}^{k} i = \frac{k(k+1)}{2}.$$

For each of these choices we can apply $n!$ permutations of columns to either of the H_i or H_j matrices. Thus, the number of inequivalent Hadamard

matrices of order $2n$ obtained by the doubling construction is less or equal to $\frac{k(k+1)n!}{2}$. □

The problem of classifying Hadamard matrices up to equivalence is extremely hard. This is mainly due to the lack of efficient algorithms to determine equivalence of two Hadamard matrices of the same order. Algorithms based on necessary and sufficient criteria for equivalence of Hadamard matrices are cumbersome to use with, as soon as we have a few million matrices to check for equivalence. A useful alternative to a complete test for equivalence is the profile criterion which is presented in the next section.

3 Criteria for Hadamard Inequivalence

3.1 The profile criterion

Cooper, Milas and Wallis in [2] suggested the profile criterion to investigate the equivalence of Hadamard matrices. Later Lin, Wallis and Zhu in [22, 25, 26] 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 :

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

It is a well-known fact that $P_{ijk\ell} \equiv 4n \ (mod\ 8)$, see [2].
We shall write $\pi(m)$ for the number of sets $\{i, j, k, \ell\}$ of four distinct rows such that $P_{ijk\ell} = m$. From the definition and the above we have 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

$$\begin{array}{ll} \pi(4) = 1 & \\ \pi(0) = 56, & \pi(8) = 14 \\ \pi(4) = 495, & \pi(12) = 0 \end{array}$$

respectively.

The five equivalence classes of order 16 have four distinct profiles.

$$\begin{array}{lllll} class\ H_0: & \pi(0) = 1680, & \pi(8) = 0, & \pi(16) = 140 \\ class\ H_1: & \pi(0) = 1488, & \pi(8) = 256, & \pi(16) = 76 \\ class\ H_2: & \pi(0) = 1392, & \pi(8) = 384, & \pi(16) = 44 \\ class\ H_3: & \pi(0) = 1344, & \pi(8) = 448, & \pi(16) = 28 \\ class\ H_4: & \pi(0) = 1344, & \pi(8) = 448, & \pi(16) = 28 \end{array}$$

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

The profile criterion cannot distinguish between the three equivalence classes of Hadamard matrices of order $n = 20$, because it gives the same profile for all three of them. The three classes of order 20 all have the same profile:

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

The main advantage of the profile criterion is its increased efficiency, compared to the complete equivalence test algorithms. The profile of a Hadamard matrix is invariant under the definition of equivalence. Thus, if two Hadamard matrices have different profiles then they are inequivalent (also called *profile-inequivalent*) but the converse is not necessarily true. If two Hadamard matrices have equal profiles, they may be equivalent or inequivalent. In Magma, the profile criterion is implemented as the command `HadamardInvariant`.

3.2 The graph isomorphism criterion

The graph isomorphism criterion is a necessary and sufficient condition for Hadamard equivalence. In Magma, the graph isomorphism criterion is implemented as the command `IsHadamardEquivalent`.

4 The doubling method

In this section we present the doubling method in an algorithmic form, using a concise pseudo-code. In subsequent sections, we will present several improvements of this algorithm as well as segments of Magma code that can be used directly, to implement the algorithm and its variants.

INPUT: A set $\mathcal{H}$ of Hadamard matrices of order n
OUTPUT: A set of inequivalent Hadamard matrices of order $2n$

(a) form a set of permutations $\mathcal{P}$, a subset of S_n
(b) for every Hadamard matrix H of order n in $\mathcal{H}$
  for every permutation σ in $\mathcal{P}$
    check whether H^σ is a new inequivalent matrix of order $2n$
  end for
end for

Pseudo-code for the doubling method

The different choices in steps (a) and (b) of the algorithm, lead to different variants of the doubling method.

1. *randomized and non-randomized doubling*, in step (a) of the algorithm, one can choose randomly elements from S_n to form a set of permutations $\mathcal{P}$, or one can use a ranking algorithm to enumerate systematically elements of S_n.

2. *doubling with 4-profile and doubling with graph isomorphism and buckets*, in step (b) of the algorithm, one can use the 4-profile criterion to establish Hadamard inequivalence, or one can use the graph isomorphism criterion with buckets. When we use the 4-profile criterion, we can just store the computed 4-profiles and at the end of the computation, identify the different ones, using simple operating system scripts. When we use the graph isomorphism criterion however, which is implemented as a boolean predicate (i.e. gives a true/false answer) then we need in addition to use the buckets algorithm [17], in order to identify inequivalent Hadamard matrices.

The four variants of the doubling method (randomized doubling with 4-profile,
non-randomized doubling with 4-profile, randomized doubling with graph isomorphism and buckets, non-randomized doubling with graph isomorphism and buckets) possess different advantages. When the 4-profile is employed, the programs run quite fast, but the amount of inequivalent matrices located becomes stationary rather quickly and we are missing inequivalent matrices who happen to have equal profiles. When the graph isomorphism criterion with buckets is employed, the programs run slower, but in general we find more inequivalent matrices and we are not missing any inequivalent matrices.

5 The subgroup and centralizer group-theoretical heuristics

In this section we present two group-theoretical heuristics that improve the execution time of the randomized version of the doubling method, regardless of which criterion we use to detect Hadamard inequivalence. The randomized version of the doubling method operates by randomly picking an element of S_n and using this permutation to interchange the columns of Hadamard matrices.

The cyclic subgroup heuristic operates by considering together with a random permutation σ, the cyclic subgroup generated by σ in S_N, and using all its elements, to interchange columns of Hadamard matrices. The cyclic

subgroup generated by σ in S_N is defined as the set of all powers of σ

$$\langle\sigma\rangle = \{1, \sigma, \sigma^2, \ldots, \sigma^{k-1}\},$$

where k is the order of σ in S_n

Similarly, the centralizer heuristic operates by considering together with a random permutation σ, its centralizer in S_n, and using all its elements, to interchange columns of Hadamard matrices. The centralizer of an element $\sigma \in S_n$ is defined as the set of all elements of S_n which permute with σ

$$C_{S_n}(\sigma) = \{\tau \in S_n : \tau\sigma = \sigma\tau\}.$$

The centralizer $C_{S_n}(\sigma)$ is a subgroup of S_n.
Typically, we have that $|\langle\sigma\rangle| \leq |C_{S_n}(\sigma)|$, the size of the centralizer subgroup is bigger than the size of the cyclic subgroup.

6 Properties of the symmetric group S_n

The symmetric group S_n has many interesting properties that could potentially be used to optimize the doubling method. For example, S_n is a 2-generator group for every n. This means that S_n is generated by two elements, permutations. It can be seen that the transposition $\tau = (12)$ and the permutation $\sigma = (123\ldots n)$ suffice:

$$S_n = \langle(12), (123\ldots n)\rangle, \text{ for } n \geq 3.$$

This assertion can be proved by showing that $\langle\tau, \sigma\rangle$ contains all transpositions in S_n. This structural property of S_n means that we have

$$S_n = \{\tau^{n_1}\sigma^{n_2}\cdots\tau^{n_{r-1}}\sigma^{n_r}, \text{ where } n_1, n_2, \ldots, n_{r-1}, n_r \in Z, \text{ and } r \in N^*\}.$$

This structural property of S_n can potentially be used to optimize the selection of random elements from S_n during the doubling method or even lead to theoretical result that make predictions on the nature of the profiles of the doubled matrices, simply by looking at the permutations they are generated from.

7 Magma code segments for the doubling method

In this section, we present Magma code segments that can be used as building blocks for efficient implementations of the doubling method with its variants and heuristic optimizations.

7.1 Randomized and non-randomized doubling

Step (a) in the pseudo-code for the doubling method can be realized:

- by randomly picking permutations from S_n (using a default or a customizable seed)

```
G := SymmetricGroup(n);      x := Random(G);
P := RandomProcess(G : Slots:= m, Scramble := s);
x := Random(P);
met := ElementToSequence(x);
H:=Transpose(Matrix(Transpose(H)[met]));
```

- by constructing sets of permutations systematically

```
G := SymmetricGroup(n);
f := NumberingMap(G);
finv := Inverse(f);
for k := lowerBound to upperBound do
  x := finv(k);
  met := ElementToSequence(x);
  H:=Transpose(Matrix(Transpose(H)[met]));
end for;
```

7.2 4-profile criterion and graph isomorphism criterion with buckets

Step (b) in the pseudo-code for the doubling method can be realized:

- by using the necessary (for Hadamard inequivalence) 4-profile criterion. The 4-profiles of the doubled matrices are computed using the Magma command `HadamardInvariant` and saved into a text file. The resulting text file is then processed with the operating system commands `sort`, `uniq` to identify the different 4-profiles. It is more efficient to use operating system commands to identify the different 4-profiles, as opposed to using Magma commands for that.

- by using the necessary and sufficient (for Hadamard inequivalence) graph isomorphism criterion and buckets. During the formation of doubled matrices, we maintain a list of inequivalent matrices. Each new matrix is checked for inequivalence with all the matrices in the list using the Magma command `IsHadamardEquivalent`. If the new matrix is found to be equivalent with a matrix in the list, then it is discarded, otherwise it is added to the list [17].

When we use the 4-profile criterion, we discover a lot of inequivalent matrices in a short period of time, but we also miss inequivalent matrices which happen to have the same profiles. For this reason there seems to be a fast saturation in the number of inequivalent matrices discovered using the 4-profile criterion.
When we use the graph isomorphism criterion with buckets we discover more inequivalent matrices and we do not miss any inequivalent matrices but a longer period of time is needed because we are working with a necessary and sufficient condition for Hadamard inequivalence.

7.3 Subgroup and centralizer group-theoretical heuristics

The Magma code segment for the subgroup heuristic is

```
G :=SymmetricGroup(n);  x := Random(G);
xSubgroup := sub<G | x>;     for y in xSubgroup do
```

The Magma code segment for the centralizer heuristic is

```
G :=SymmetricGroup(n);  x := Random(G);
xCentralizer := Centralizer(G,x);   for y in xCentralizer do
```

Using the subgroup and centralizer group-theoretical heuristics, we can discover the same amount of inequivalent matrices as with the un-optimized code, but in far less execution time.

8 Some Results for small and large orders of Hadamard matrices

Using these Magma procedures, we constructed several millions of new inequivalent Hadamard matrices of orders 48, 56, 64, 72, 80, 88, and 96. We also constructed inequivalent Hadamard matrices of orders 672 and 856. The number of the constructed inequivalent Hadamard matrices of these orders, are given below.
The computations have been performed using Magma 2.11 remotely at the *Centre de calcul formel MEDICIS, École Polytechnique* Paris, France. The inequivalent matrices produced are available from the web page `http://www.math.ntua.gr/people/ckoukouv/en_index.html` under the menu item `designs/hadamard` and in addition from the MEDICIS mirror web page `http://www.cargo.wlu.ca/doubling/`.
We denote by n the order of the Hadamard matrices used as the input of the doubling method. We denote by N_{2n} the number of inequivalent Hadamard

matrices of order $2n$ we have constructed by the doubling method. These results represent a drastic improvement of the known inequivalent Hadamard matrices for these orders. We whould like to make it clear that these results are far from the theoretical lower bounds on the number of inequivalent Hadamard matrices. The different and very useful concept is that the inequivalent Hadamard matrices mentioned in this paper are constructed and are available in the web to anyone who might need them.
We applied the doubling method for two different sets of orders of Hadamard matrices, that can be categorized as the set of small orders and the set of large orders. The results for small and large orders are described in the tables below.

$(n, 2n)$	$(24, 48)$	$(28, 56)$	$(32, 64)$	$(36, 72)$	$(40, 80)$
N_{2n}	$3,013,006$	$2,216,264$	$1,696,940$	$1,339,890$	$4,025,308$
$(n, 2n)$	$(44, 88)$	$(48, 96)$			
N_{2n}	$3,196,189$	$1,508,441$			

Table 1. Small orders Profile-inequivalent Hadamard matrices constructed by the doubling method

$(n, 2n)$	$(336, 672)$	$(428, 856)$
N_{2n}	334	689

Table 2. Large orders Profile-inequivalent Hadamard matrices constructed by the doubling method

The initial sets of inequivalent matrices that we used as input in the doubling method, came from different sources, that we list below.

- √ 60 inequivalent Hadamard matrices of order 24
  √ 487 inequivalent Hadamard matrices of order 28

  N. J. A. Sloane web page
- √ 19 inequivalent Hadamard matrices of order 32
  √ 217 inequivalent Hadamard matrices of order 36
  √ 98 inequivalent Hadamard matrices of order 40
  √ 500 inequivalent Hadamard matrices of order 44
  √ 53 inequivalent Hadamard matrices of order 48

  C. Koukouvinos web page
- 4 inequivalent Hadamard matrices of order 336, see [3]
- the Hadamard matrix of order 428, see [13].

The main computational overhead of the doubling method is in the computation of the profiles of the Hadamard matrices. This can be seen in the

case of the large orders 336 and 428, for which the computation of the profile for one Hadamard matrix in Magma, takes approximatively 35 minutes and 1 hour, respectively.
The Hadamard matrices found by the doubling construction are profile-inequivalent to the Hadamard matrices constructed in [18] and [19].

Moreover, the Hadamard matrices presented in this paper is a small, but useful, a sample of the matrices that can be found by applying in practice the proposed method. We think that the procedure presented is very useful to anyone applying inequivalent Hadamard matrices of orders $8t$ because by using our algorithm, any interested researcher can generate his own huge list of inequivalent Hadamard matrices of the desired order.

Acknowledgements. This research was financially supported from the General Secretariat of Research and Technology by a grant PENED 03ED740.

References

[1] J.J. Cannon and C. Playoust, *An Introduction to Algebraic Programming with Magma*, University of Sydney, 1996.

[2] 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.

[3] J. Cousineau, I.S. Kotsireas and C. Koukouvinos, Genetic algorithms for orthogonal designs, *Australas. J. Combin.*, (to appear).

[4] S. Georgiou and C.Koukouvinos, On inequivalent Hadamard matrices of order 36, *Ars Combinatoria*, 70 (2004), 19–31.

[5] S. Georgiou and C. Koukouvinos, On inequivalent Hadamard matrices of order 44, *Ars Combinatoria*, 70 (2004), 169–181.

[6] S. Georgiou, C. Koukouvinos, and J. Seberry, Hadamard matrices, orthogonal designs and construction algorithms, in *Designs 2002: Further Computational and Constructive Design Theory*, (Ed. W.D. Wallis), Kluwer Academic Publishers, Norwell, Massachusetts, 2003, 133–205.

[7] J. Hadamard, Resolution d'une question relative aux determinants, *Bull. des Sci. Math.*, 17 (1893), 240–246.

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

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

[10] M. Hall, Jr. *Combinatorial Theory*, Reprint of the 1986 second edition, Wiley Classics Library, 1998. Wiley, New York.

[11] 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.

[12] 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.

[13] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428, *J. Combin. Designs*, 13 (2005), 435–440.

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

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

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

[17] I.S. Kotsireas and C. Koukouvinos, Inequivalent Hadamard matrices with buckets, *J. Discrete Math. Sci. Cryptogr.*, 7, (2004), 307–317.

[18] I.S. Kotsireas and C. Koukouvinos, Constructions for Hadamard matrices of Williamson type, *J. Combin. Math. Combin. Comput.*, (to appear).

[19] I.S. Kotsireas and C. Koukouvinos, Orthogonal designs via computational Algebra, (submitted).

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

[23] 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.

[24] 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.

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

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

[27] R.E.A.C. Paley, On orthogonal matrices, *J. Math. Phys.*, 12 (1933), 311–320.

[28] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, in *Contemporary Design Theory - a Collection of Surveys*, eds J. H. Dinitz and D. R. Stinson, John Wiley and Sons, New York, 431–560, 1992.

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

[30] J.J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign-successions and tesselated pavements in two or more colors, with applications to Newton's rule, ornamental-tile-work, and theory of numbers, *Philos. Mag.*, 34 (1867), 461–475.

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

[32] S. Topalova, Classification of Hadamard matrices of order 44 with automorphisms of order 7, *Discrete Math.*, 260 (2003), 275–283.

[33] 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.