On equivalence of Hadamard matrices and projection properties

S. Georgiou and C. Koukouvinos
Department of Mathematics
National Technical University of Athens
Zografou 15773, Athens Greece
email: [sgeorg, ckoukouv]@math.ntua.gr

Abstract

The classification of Hadamard matrices of orders $n \geq 32$ is still remains an open and difficult problem. The definition of equivalent Hadamard matrices gets to have huge complexity as n is getting bigger. One efficient criterion (K-boxes) used for the construction of inequivalent Hadamard matrices in order 28.

In this paper we use inequivalent projections of Hadamard matrices and their symmetric Hamming distances to check inequivalent Hadamard matrices. Using this criterion we developed two algorithms. The first one achieves to find all inequivalent projections in k columns as well as to classify Hadamard matrices and the second, which is faster than the first, uses the symmetric Hamming distance distribution of projections to classify Hadamard matrices. As an example, we apply the second algorithm to the known inequivalent Hadamard matrices of orders $n = 4, 8, 12, 16, 20, 24$ and 28.

AMS Subject Classification: Primary 05B20, Secondary 62K15
Key words and phrases: Projection, Hadamard matrices, equivalence, algorithm, Hamming distance, symmetric Hamming distance.

1 Introduction

An n-dimensional Hadamard matrix is an n by n matrix of $1's$ and $-1's$ with $HH^T = nI_n$. A Hadamard matrix is said to be *normalized* if it has its first row and column all 1's. If not we can normalize the Hadamard matrix by multiplying rows and columns by -1 where is 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 [3, 4]. There are precisely 60 equivalence classes at order 24, see [5, 6]. There are precisely 487 equivalence classes at order 28, see [7, 8]. 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 tell whether or not they are equivalent, as their order increases.

In this paper we use inequivalent projections of Hadamard matrices to check inequivalent Hadamard matrices. Using this criterions we developed two algorithms. The first one achieves to find all inequivalent projections in k columns and classify the Hadamard matrices of that order. The second uses the symmetric Hamming distance distribution of their projections to classify the Hadamard matrices. As an example we apply this criterion to orders 16 and 20.

In the next section we describe some of the known criterions for the equivalence of Hadamard matrices. The following criterion (profile) was given in [1].

2 The profile criterion

Cooper, Milas and Wallis in [1] suggested the profile criterion to investigate the equivalence of Hadamard matrices. Later Lin, Wallis and Zhu in [11, 12, 13] 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 :

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

As we said before 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 [1]) $P_{ijk\ell} \equiv 4n \ (mod\ 8)$.

We shall write $\pi(m)$ for the number of sets $\{i, j, k, \ell\}$ of four distinct rows such that $P_{ijk\ell} = m$. 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 inequivalent classes of order 16 gave four distinct profiles.

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

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

The 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 [12]. We now give a modified version of the one that was given in [1]. We observe that all the facts which hold for the rows of a Hadamard matrix are also hold for its columns, as well.

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 $Q(m) = s$. From the definition and the above we have 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 all case of Hadamard matrices.

3 The K-Matrices and K-boxes criterions

Let $H = (h_{ij})$ be an Hadamard matrix of order n with $0 \leq i, j \leq n-1$. H is equivalent $H' = (h'_{i,j})$ with $h'_{i,0} = h'_{0,j}1, \ 0 \leq i, j \leq n-1$. From H we have an incidence matrix $D(H)$ of a symmetric $2-(v,k,\lambda)$ design associated with H, where $v=n-1,\ k=(v-1)/2,\ \lambda=(k-1)/2$:

$$D(H)=(d_{i,j}),\ i,j=1,2,\ldots,n-1 \text{ where } d_{i,j}=\begin{cases}1, & \text{if } h_{i,j}=1\\ 0, & \text{if } h_{i,j}=-1\end{cases}$$

For any different four rows i,j,k and m of H, we define $a_{i,j,k,m}$ as follows:

$$a_{i,j,k,m}(r)=\begin{cases}1, & \text{if } h_{i,r}h_{j,r}h_{k,r}h_{m,r}=1\\ 0, & \text{if } h_{i,r}h_{j,r}h_{k,r}h_{m,r}=-1\end{cases}$$

Then $a_{i,j,k,m}(0)+\cdots+a_{i,j,k,m}(n-1)$ is divisible by 4 (see [10]). Let x be an integer with $0\le x\le n/4$. For fixed i and j, let $k'_{i,j}(x)$ be a number of pairs, k and m, of rows such that $a_{i,j,k,m}(0)+\cdots+a_{i,j,k,m}(n-1)=4x$. For $0\le x\le n/8$ put

$$k_{i,j}(x)=\begin{cases}k'_{i,j}(x)+k'_{i,j}(n/4-x), & \text{if } x\neq n/4-x\\ k'_{i,j}(x), & \text{if } x=n/8.\end{cases}$$

Then $k_{i,j}(x)$ does not change by multiplication of rows i or j by -1. By a permutation of coordinates we assume that $k_{i,j}(x)\le k_{i,m}(x)$ if $j\le m$. Put

$$K_{i,j}(x)=\begin{cases}k_{i,j}(x), & \text{if } i>j\\ k_{i,j+1}(x), & \text{if } i\le j.\end{cases}$$

The rows of the $n\times(n-1)$ matrix $K_{i,j}(x)$ are ordered lexicographically, that is, if $i<i'$ then $K_{i,j}(x)=K_{i',j}(x)$ for $j=1,2,\ldots,n-1$, or there exist an integer j such that $K_{i,j}(x)=K_{i',j'}(x)$ for $j'<j$ and $K_{i,j}(x)<K_{i',j}(x)$. The matrix $K_x(H)=(K_{i,j}(x))$ is called an associated *x-th K-matrix* of H. By the construction of $K_x(H)$ we have the following:

Theorem 1 ([10]) *Let H_1 and H_2 be Hadamard matrices of order n which are equivalent, then $K_x(H_1)=K_x(H_2)$ for all $0\le x\le n/8$.*

Proposition 2 *If $n\equiv 4 \pmod 8$ them $K_0(H)$ is the zero matrix and $K(H)$ in [9] is $K_1(H)$ for $n=28$.*

Theorem 2 *Let $n\equiv 4 \pmod 8$ and a, b be two integers with $1\le a,b\le (n-4)/8$ or $n\equiv 0 \pmod 8$ and a, b be two integers with $0\le a,b\le n/8$ then if we know $K_m(H)$ for all $m\neq a,b$, $K_a(H)$ and $K_b(H)$ can be obtained.*

As mentioned in [10] some inequivalent Hadamard matrices of order $n=28$ have the same K-matrices (only 476 inequivalent Hadamard matrices of order 28 can be obtained). Another method of classification of Hadamard matrices is the K-boxes criterion (a modified version of K-matrices criterion).

For any different six rows i, j, i', j', k' of H we define $a_{i,j,k,i',j',k'}$

$$a_{i,j,k,i',j',k'}(r) = \begin{cases} 1, & \text{if } h_{i,r}h_{j,r}h_{k,r}h_{i',r}h_{j',r}h_{k',r} = 1 \\ 0, & \text{if } h_{i,r}h_{j,r}h_{k,r}h_{i',r}h_{j',r}h_{k',r} = -1 \end{cases}$$

Let x be an integer with $0 \le x \le n$. For fixed i, j and k let $k'_{i,j,k}(x)$ be a number of triples i', j' and k' of rows such that $a_{i,j,k,i',j',k'}(0) + \cdots + a_{i,j,k,i',j',k'}(n-1) = x$. For $0 \le x \le n/2$, put

$$k_{i,j,k}(x) = \begin{cases} k'_{i,j,k}(x) + k'_{i,j,k}(n-x), & \text{if } x \ne n-x \\ k'_{i,j,k}(x), & \text{if } x = n/2. \end{cases}$$

Then $k_{i,j,k}(x)$ does not change by multiplication of rows i, j or k by -1. By a permutation of coordinates we assume that $k_{i,j,k} \le k_{i,j,k'}$ if $k < k'$. Put

$$K'_{i,j,k}(x) = \begin{cases} k_{i,j,k}(x), & \text{if } i > j \\ k_{i,j+1,k}(x), & \text{if } i \le j. \end{cases}$$

Next put

$$K_{i,j,k}(x) = \begin{cases} K'_{i,j,k}(x), & \text{if } i > k \\ K'_{i,j,k+1}(x), & \text{if } i \ge k \ge j, \text{ or } i \le k < j \\ K'_{i,j,k+2}(x), & \text{if } i, j \le k \end{cases}$$

Then, for $0 \le i \le n-1$, the matrix $K_{i,x}(H) = (K_{i,j,k}(x))$ is of type $(n-1) \times (n-2)$. For i we rearrange the matrix $K_{i,x}(H)$ as in the case of K-matrices. We rearrange the collection of matrices $K_{i,x}(H)$ with $0 \le i \le n-1$ in the following: if $i < i'$, then matrix $K_{i,x}(H)$ equals the matrix $K_{i',x}(H)$, or there exist integers s and t such that if $j < s$, then $K_{i,j,k}(x) = K_{i',j,k}(x)$ for all k, if $k < t$, then $K_{i,s,k}(x) = K_{i',s,k}(x)$ and $K_{i,s,t}(x) = K_{i',s,t}(x)$. We call this collection $KB_x(H)$ of n matrices $K_{i,x}(H)$ *K-box* of degree x associate with H.

Theorem 3 ([10]) *If H_1 and H_2 are equivalent Hadamard matrices of order n then $KB_x(H_1) = KB_x(H_2)$ for all $0 \le x \le n/2$.*

In the next section we present two new criterions to test inequivalence in Hadamard matrices of order n which are based on their projection properties and their Hamming distances.

4 The new criterions and the algorithms

In this section we describe two new criterions that can be used to decide if two Hadamard matrices are inequivalent.

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).

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.

Definition 1 *Two projections, in k columns, 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) Sign changes in the rows (multiply one or more rows by -1).

(c) Permutations of the columns

(d) Permutations 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 $k = 3$.

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

(iii) From the projections found in step (ii) find the inequivalent ones using definition 1.

(iv) Check if the set of all projections of the first Hadamard matrix is different (non equivalent) with the set of all projections of the second Hadamard matrix.

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

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

In what follows by $log(x)$ we mean $log_a(x), \quad a > 1$.

Lemma 1 *Let h_k be a projection, in k columns, of a Hadamard matrix of order n. Then h_k cannot contains a full 2^k design if $k > \frac{log(n)}{log(2)}$.*

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

$$2^k > n \Longrightarrow k \cdot log(2) > log(n) \Longrightarrow k > \frac{log(n)}{log(2)}.$$

Now if k is not an integer we take the next integer number. Thus, if k is not an integer we have that $k \geq \left[\frac{log(n)}{log(2)}\right] + 1$. □

Remark 1 If 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 $k > \frac{log(n)}{log(2)}$.

Example 1 We give some orders of Hadamard matrices and the bound for k.

- For $n = 2^m$ we obtain $k \geq m + 1$.
- 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 $k \geq 5$.

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

Proof. We know that $log_a(x)$ function is continuous, and increasing (since $a > 1$) function. Moreover, $\frac{log(n)}{log(2)} = log_2(n)$. Thus since $log_2(2^m) = m$, we have that if $2^m < n < 2^{m+1}$ then $m < log_2(n) < m + 1$ and so $k \geq m + 1$. □

Theorem 4 *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 $\binom{n}{k}$ projections in total. From the equivalence of the Hadamard matrices we have that each projection of the first Hadamard matrix is equivalent with one projection of the second Hadamard matrix and vise versa. □

We will now check the complexity of the first new algorithm. First, we observe that all possible projections of a Hadamard matrix of order n in k columns are $\binom{n}{k}$. We note that the finding of inequivalent projections is computationally-intensive work, if we apply the definition of inequivalent projections. 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 and the sign changes in the rows (multiply one or more rows by -1) required 2^n possible multiplications. The permutations of the columns and rearrangements of the rows need $k!$ possible permutations. That is in total we have $2^{k+n} \cdot k! \cdot \binom{n}{k} = \frac{2^{k+n} n!}{(n-k)!}$ cases to check and that's a large complexity when k or n 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 their symmetric Hamming distance distribution.

The symmetric Hamming distance of two $(1, -1)$ vectors of length n, is defined to be the smallest number of positions with the same entries and different entries. For example, the Hamming distance and symmetric Hamming distance of the two vectors $(1, 1, -1, 1, -1, -1, 1, -1)$ and $(1, -1, 1, -1, -1, 1, -1, 1)$ are 6 and 2 respectively. It is clear that if we have a Hadamard matrix H of order n, then the Hamming distance as well as the symmetric Hamming distance of any two distinct rows is $n/2$.

The *Hamming distance distribution* $(W(x))$ and the *symmetric Hamming distance distribution* $(SW(x))$, of a projection in k columns, is defined to be

$$W_k(x) = a_0 + a_1 x^1 + \ldots + a_k x^k \quad \text{and}$$

$$SW_k(x) = \begin{cases} \sum\limits_{i=0}^{(k-1)/2} (a_i + a_{k-i}) x^i, & \text{when k is odd} \\ \sum\limits_{i=0}^{(k-2)/2} (a_i + a_{k-i}) x^i + a_{\frac{k}{2}} x^{\frac{k}{2}}, & \text{when k is even} \end{cases}$$

respectively, where a_m is the number describing how many pairs of rows of the projection have distance m.

Example 2 Consider the projections for $k = 3$ and $n = 8$. A Hadamard matrix of order 8 is

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

Since $k = 3$ the projections are all possible 3-sets of columns. We will just illustrate with the sets of columns 2, 3, 4 and 2, 3, 5.

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

We now consider the distance between all pairs of rows 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 and its symmetric Hamming distance distribution is

$$W_3(x) = 0 + 12x + 12x^2 + 4x^3, \quad SW_3(x) = 4 + 24x$$

respectively, while the second set has 0 (4 times) and 2 (24 times) so its Hamming distance distribution and its symmetric Hamming distance distribution is

$$W_3(x) = 4 + 24x^2, \quad SW_3(x) = 4 + 24x$$

respectively. □

The Hamming distance distribution $W_k(x)$ is invariant only to permutations of columns or rows, or negations of columns while the symmetric Hamming distance distribution $SW_k(x)$ is invariant to permutations and negations of both rows and columns.

Lemma 3 *Two equivalent projections have the same symmetric 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 rows in a given projection in k columns. The result follows from the fact that the symmetric Hamming distance of these two rows is not affected if we apply some sing changes or permutations to both rows and columns. □

Lemma 4 *All projections of two Hadamard matrices H_1, H_2 of order n in $k = 1, 2$ columns are the same (actually these give only one inequivalent projection) even thought the Hadamard matrices are inequivalent.*

Proof. Since any Hadamard matrix is equivalent to its normalized form, we can suppose that H_1, H_2 are normalized. Thus any column of H_1, H_2 have half $1's$ and half $-1's$. The assertion for $k = 1$ follows. For the case $k = 2$, since any two columns of a Hadamard matrix are orthogonal, it is easy to see that any projection in $k = 2$ columns is equivalent to a projection which is $n/4$ times the full 2^2 design. □

Lemma 5 *Let H be a Hadamard matrix of order n. Any two rows of the Hadamard matrix have Hamming distace distribution and symmetric Hamming distace distribution $W_n(x) = SW_n(x) = x^{n/2}$.*

Proof. Let $r = \{r_1, r_2, \ldots, r_n\}$ and $p = \{p_1, p_2, \ldots, p_n\}$ be the two rows of the Hadamard matrix. From the orthogonality of the rows we have that $\sum_{i=1}^{n} r_i p_i = 0$. This means that $n/2$ of the n pairs $(r_i, p_i) \in \{(1,1), (-1,-1)\}$ and the other $n/2$ pairs $(r_i, p_i) \in \{(-1,1), (1,-1)\}$, and thus the Hamming distace distribution and the symmetric Hamming distace distribution $W_n(x) = SW_n(x) = x^{n/2}$. □

Definition 2 Let H be a Hadamard matrix of order n and P_k a set of k columns of H. We define the *complementary projection* of P_k to be the set of the columns of H which are not contained in P_k. Obviously the complementary projection of P_k consist of $n - k$ columns.

Remark 2 Let H_1, H_2 be two Hadamard matrices of order n. Suppose $r = \{r_1, r_2, \ldots, r_k\}$ and $p = \{p_1, p_2, \ldots, p_k\}$ be two rows of a projection of H_1 and $q = \{q_1, q_2, \ldots, q_k\}$ and $s = \{s_1, s_2, \ldots, s_k\}$ be two rows of a projection of H_2. Then $SW(x)$ of rows r, p is equal to $SW(x)$ of rows q, s if and only if the symmetric Hamming distance distribution of the corresponding rows of their complementary projections is equal.

Example 3 The complementary projections of the projections given in example 2 are

$$\begin{array}{rrrrr} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 \end{array} \quad \textit{and} \quad \begin{array}{rrrrr} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 \end{array}$$

with symmetric Hamming distance distribution $SW_{8-3}(x) = SW_5(x) = 4 + 24x$.

From Lemmas 3, 4 and 5 it is obvious that:

Corollary 1 *All projections of two Hadamard matrices H_1, H_2 of order n in $k = 1, 2$ and $k = n$ columns have the same symmetric Hamming distance distribution.*

Using Remark 2 and the above lemmas we can conclude:

Corollary 2 *Let H_1, H_2 be two Hadamard matrices of order n. We need only to check the symmetric Hamming distance distribution of projections for $k = 3, 4, \ldots, n/2$ because if these have the same symmetric Hamming distance distribution, then the corresponding complementary projections will have the same symmetric Hamming distance distribution as well.*

In this way the modified algorithm (symmetric Hamming distance distribution algorithm) is much faster than the previous one but it only gives us an answer to the question if the two Hadamard matrices are equivalent or not and does not give us all inequivalent projections of the Hadamard matrices.

The Symmetric Hamming distance distribution algorithm:

(i) Set $k = 3$.

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

(iii) In the projections found in step (ii) calculate the symmetric Hamming distance distributions for any two rows of the projection. These are $\binom{n}{2}$ symmetric Hamming distance distributions and save different symmetric Hamming distance distributions and how many times each of them appear.

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

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

(vi) If now $k < n/2$ then go to step (ii) and continue, otherwise stop and say that this algorithm can not decide for the equivalence of these Hadamard matrices.

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

5 Application of the new criterion in Hadamard matrices of small orders

In this section we apply our new algorithm in the cases of Hadamard matrices of small orders.

When the Hadamard matrices are equivalent we have to check the symmetric Hamming distance distributions for all projections into $k = 3, \ldots, n/2$ columns. As an examples we give all symmetric Hamming distances of the unique Hadamard matrices of orders $n = 8, 12$ and for all $k = 3, 4, \ldots, n/2$.

If the Hadamard matrices are inequivalent there exist $k \in \{2, 3, \ldots, n/2\}$ such that the symmetric Hamming distance distributions for the projections in k columns are different for each Hadamard matrix.

5.1 Hadamard matrices of order $n = 8, 12$

We know that there exist only one Hadamard matrix of these orders up to equivalence, see [2] for example. For the order $n = 4$ we have $k \leq n/2 = 2$ and thus all projection have the same symmetric Hamming distance distribution. The results of the application of the symmetric Hamming distance distribution algorithm for these orders $n \geq 8$ are given in Table 1. Since there is only one Hadamard matrix in each case we give all symmetric Hamming distance distributions for all projections into $k = 3, \ldots, n/2$ columns.

H_{name}	n	k	Symmetric Hammind distance	times
H_8	8	3	4,24	56
H_8	8	4	0,16,12	56
H_8	8	4	4,0,24	14
H_{12}	12	3	12,54	220
H_{12}	12	4	4,32,30	495
H_{12}	12	5	1,15,50	792
H_{12}	12	6	0,6,30,30	792
H_{12}	12	6	1,0,45,20	132

Table 1: Application of the symmetric Hamming distance distribution algorithm for $n = 8$ and 12

5.2 Hadamard matrices of order $n = 16$

We know that there are exactly five inequivalent Hadamard matrices of this order, see [3]. The results of the application of the symmetric Hamming distance distribution algorithm for this order are given in Table 2. Observe that for $k = 3$ the symmetric Hamming distance distributions of all projections of all five matrices are exactly the same. For $k = 4, 5$ and 6 we have four different symmetric Hamming distance distributions (thus four inequivalent Hadamard matrices) and we have to go up to $k = 7$ to obtain all five of them.

5.3 Hadamard matrices of order $n = 20$

We know that there are exactly three inequivalent Hadamard matrices of this order, see [4]. The results of the application of the symmetric Hamming distance distribution algorithm for this order are given in Table 3. Observe that for $k = 3, 4$ and 5, the symmetric Hamming distance distributions of

H_{name}	n	k	Symmetric Hammind distance	times
$H_{16.0} - H_{16.4}$	16	3	24,96	560
$H_{16.0}$	16	4	8,64,48	1680
$H_{16.0}$	16	4	24,0,96	140
$H_{16.1}$	16	4	8,64,48	1488
$H_{16.1}$	16	4	12,48,60	256
$H_{16.1}$	16	4	24,0,96	76
$H_{16.2}$	16	4	8,64,48	1392
$H_{16.2}$	16	4	12,48,60	384
$H_{16.2}$	16	4	24,0,96	44
$H_{16.3}$	16	4	8,64,48	1344
$H_{16.3}$	16	4	12,48,60	448
$H_{16.3}$	16	4	24,0,96	28
$H_{16.4}$	16	4	8,64,48	1344
$H_{16.4}$	16	4	12,48,60	448
$H_{16.4}$	16	4	24,0,96	28
$H_{16.3} - H_{16.4}$	16	5	0,40,80	1344
$H_{16.3} - H_{16.4}$	16	5	4,28,88	2688
$H_{16.3} - H_{16.4}$	16	5	8,16,96	336
$H_{16.3} - H_{16.4}$	16	6	0,12,72,36	1792
$H_{16.3} - H_{16.4}$	16	6	0,16,56,48	3696
$H_{16.3} - H_{16.4}$	16	6	2,12,54,52	1792
$H_{16.3} - H_{16.4}$	16	6	4,8,52,56	672
$H_{16.3} - H_{16.4}$	16	6	8,0,48,64	56
$H_{16.3}$	16	7	0,0,48,72	448
$H_{16.3}$	16	7	0,4,36,80	8064
$H_{16.3}$	16	7	0,8,24,88	1680
$H_{16.3}$	16	7	1,7,21,91	1024
$H_{16.3}$	16	7	4,4,12,100	224
$H_{16.4}$	16	7	0,0,48,72	448
$H_{16.4}$	16	7	0,4,36,80	8064
$H_{16.4}$	16	7	0,8,24,88	2016
$H_{16.4}$	16	7	2,6,18,94	896
$H_{16.4}$	16	7	8,0,0,112	16

Table 2: Application of symmetric Hamming distance distribution algorithm for $n = 16$

all projections of all three matrices are exactly the same. For $k = 6$ all three have different symmetric Hamming distance distributions and thus we obtain all three inequivalent Hadamard matrices.

H_{name}	n	k	Symmetric Hammind distance	times
$H_{20.0} - H_{20.2}$	20	3	40,150	1140
$H_{20.0} - H_{20.2}$	20	4	16,96,78	4560
$H_{20.0} - H_{20.2}$	20	4	24,64,102	285
$H_{20.0} - H_{20.2}$	20	5	5,55,130	10944
$H_{20.0} - H_{20.2}$	20	5	9,43,138	4560
$H_{20.0}$	20	6	0,30,90,70	6270
$H_{20.0}$	20	6	1,24,105,60	4560
$H_{20.0}$	20	6	2,26,88,74	15390
$H_{20.0}$	20	6	3,20,103,64	6840
$H_{20.0}$	20	6	4,22,86,78	5130
$H_{20.0}$	20	6	6,18,84,82	570
$H_{20.1}$	20	6	0,30,90,70	4320
$H_{20.1}$	20	6	1,24,105,60	5760
$H_{20.1}$	20	6	2,26,88,74	19440
$H_{20.1}$	20	6	3,20,103,64	5040
$H_{20.1}$	20	6	4,22,86,78	2880
$H_{20.1}$	20	6	6,18,84,82	720
$H_{20.1}$	20	6	7,12,99,72	600
$H_{20.2}$	20	6	0,30,90,70	5600
$H_{20.2}$	20	6	1,24,105,60	4960
$H_{20.2}$	20	6	2,26,88,74	16800
$H_{20.2}$	20	6	3,20,103,64	6240
$H_{20.2}$	20	6	4,22,86,78	4320
$H_{20.2}$	20	6	6,18,84,82	640
$H_{20.2}$	20	6	7,12,99,72	200

Table 3: Application of the symmetric Hamming distance distribution algorithm for $n = 20$

5.4 Hadamard matrices of order $n = 24$

We know that there are exactly 60 inequivalent Hadamard matrices of this order, see [5, 6]. For Hadamard matrices of order 24 it is not convenient to give all different symmetric Hamming distance distributions for all k.

We shall only discuss the results our algorithm gives. For $k = 3$ all sixty matrices give the same symmetric Hamming distance distributions thus we obtain only one of the sixty inequivalent Hadamard matrices. For $k = 4$ and $k = 5$ the algorithm finds 35 different symmetric Hamming distance distributions and thus 35 of the sixty inequivalent Hadamard matrices. Finally for $k = 6$ we obtain 60 different symmetric Hamming distance distributions and thus all 60 inequivalent Hadamard matrices.

5.5 Hadamard matrices of order $n = 28$

In the case $n = 28$ there are 487 inequivalent Hadamard matrices, see [7, 8]. If we apply our algorithm to this case we obtain the following results. For $k = 3$ all 487 matrices give the same symmetric Hamming distance distributions thus we obtain only one of the 487 inequivalent Hadamard matrices. The algorithm moves to $k = 4$ and finds 60 different symmetric Hamming distance distributions and thus 60 of the 487 inequivalent Hadamard matrices. Also for $k = 5$ we obtain 60 different symmetric Hamming distance distributions and thus 60 of the 487 inequivalent Hadamard matrices. Finally for $k = 6$ we obtain 487 different symmetric Hamming distance distributions, and thus all 487 inequivalent Hadamard matrices.

We do not now the exact number of inequivalent Hadamard matrices of order ≥ 32. However, it is known that the number of inequivalent Hadamard matrices of order 32 is ≥ 66000, see [2] and of order 36 is ≥ 192 see Seberry's home page http://www.uow.edu.au/ ~jennie. The study of inequivalent Hadamard matrices of order 36 will be in a forthcoming paper.

References

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

[2] 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.

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

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

[5] 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.

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

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

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

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

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

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

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

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

[14] 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.