On the classification of Hadamard matrices of order 32

H. Kharaghani[a,1] B. Tayfeh-Rezaie[b]

[a] *Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, T1K3M4, Canada*

[b] *School of Mathematics, Institute for Research in Fundamental Sciences (IPM), P.O. Box 19395-5746, Tehran, Iran*

December 5, 2009

Abstract

All equivalence classes of Hadamard matrices of order at most 28 have been found by 1994. Order 32 is where a combinatorial explosion occurs on the number of Hadamard matrices. We find all equivalence classes of Hadamard matrices of order 32 which are of certain types. It turns out that there are exactly 13,680,757 Hadamard matrices of one type and 26,369 such matrices of another type. Based on experience with the classification of Hadamard matrices of smaller order, it is expected that the number of the remaining two types of these matrices, relative to the total number of Hadamard matrices of order 32, to be insignificant.

AMS Subject Classification: 05B20, 05B05, 05B30.
Keywords: Hadamard matrices, classification of combinatorial objects, isomorph-free generation, orderly algorithm.

1 Introduction

A *Hadamard* matrix of order n is a $(-1, 1)$ square matrix H of order n such that $HH^t = nI$, where H^t is the transpose of H and I is the identity matrix. It is well known that the order of a Hadamard matrix is 1,2 or a multiple of 4. The old Hadamard conjecture states that the converse also holds, i.e. there is a Hadamard matrix for any order which is divisible by 4. Order 668 is the smallest for which the existence of a Hadamard matrix is in doubt [11]. For surveys on Hadamard matrices, we refer the reader to [1, 7, 19].

[1] Supported by an NSERC-Group Discovery Grant. Corresponding author. E-mail: kharaghani@uleth.ca.

Two Hadamard matrices are called *equivalent* if one is obtained from the other by a sequence of permutations and negations of rows and columns. The equivalence classes of Hadamard matrices for small orders have been determined by several authors. It is well known that for any order up to 12, there is a unique Hadamard matrix. For orders 16,20,24,28, there exist 5 [5], 3 [6], 60 [8, 15] and 487 [13, 14, 16, 21] inequivalent Hadamard matrices, respectively. The order 32 is where a combinatorial explosion occurs on the number of Hadamard matrices.

Our main objective in this paper is to determine all equivalence classes of Hadamard matrices of order 32 which are of type zero (see below for the definition of types). In order 32, any Hadamard matrix is of one of the types 0,1,2 or 3. A classification of Hadamard matrices of type one will follow from the classification of type zero. We choose to apply an orderly algorithm to perform the classification. Orderly algorithms are based on the notion of canonical form. We introduce a new canonical form for Hadamard matrices of type zero which is crucial to make the classification computationally possible. It turns out that there are exactly 13,680,757 such matrices of type zero and 26,369 matrices of type one. Our experience shows that a classification of Hadamard matrices of types 2 and 3 using a similar method is very time consuming and practically impossible. Based on data of smaller orders, it is expected that the number of the remaining two types of these matrices, relative to the total number of Hadamard matrices of order 32, to be insignificant.

2 Types

Let H be a Hadamard matrix of order n. Let j_m denote the all one column vector of dimension m. By permutation and negation of rows and columns, if necessary, any four columns of H may be transformed uniquely to the following form:

$$\begin{bmatrix} j_a & j_a & j_a & j_a \\ j_b & j_b & j_b & -j_b \\ j_b & j_b & -j_b & j_b \\ j_a & j_a & -j_a & -j_a \\ j_b & -j_b & j_b & j_b \\ j_a & -j_a & j_a & -j_a \\ j_a & -j_a & -j_a & j_a \\ j_b & -j_b & -j_b & -j_b \end{bmatrix}, \tag{1}$$

where $a + b = n/4$ and $0 \leq b \leq \lfloor n/8 \rfloor$. Following [14], any set of four columns which is transformed to the above form is said to be of *type* b. Note that any permutation and negation of rows and columns leaves the type unchanged. A Hadamard matrix is of *type* b ($0 \leq b \leq \lfloor n/8 \rfloor$), if it has a set of four columns of type b and no set of four columns of type less than b. The following lemma is due to Kimura [14].

Lemma 1 *There is no Hadamard matrix of order n and type zero, if $n \equiv 4 \pmod 8$.*

We have a similar result for $n \equiv 0 \pmod 8$.

Lemma 2 *There is no Hadamard matrix of order n and type $n/8$, if $n \equiv 0 \pmod 8$.*

Proof. Let H be a Hadamard matrix of order n and type $n/8$. Without loss of generality we may assume that the first three columns of H are as follows:

$$\begin{bmatrix} j_m & j_m & j_m \\ j_m & j_m & -j_m \\ j_m & -j_m & j_m \\ j_m & -j_m & -j_m \end{bmatrix}, \tag{2}$$

where $m = n/4$. Let $\mathbf{c}$ be any other column of H. Then, the sum of entries at the positions $(i-1)m+1$ to im of $\mathbf{c}$ is zero for $i = 1, 2, 3, 4$. Now, the column vector $[j_m \ -j_m \ -j_m \ j_m]^t$ is orthogonal to all column vectors of H which leads to a contradiction. □

We thus conclude that in order 32 any Hadamard matrix is necessarily of type 0,1,2 or 3. The following lemma is proved in [16] (see also [13]).

Lemma 3 *Let H be a type one Hadamard matrix of order n, $n \equiv 4 \pmod 8$. Then H^t is of type one.*

Similarly, for the case $n \equiv 0 \pmod 8$, we have the following lemma due to W. P. Orrick (private communication). The lemma shows that a classification of Hadamard matrices of type zero would yield a classification of type one matrices. The proof of the lemma relies on the fact that by (1), a set of four columns of a Hadamard matrix is of type zero if and only if the 4-dimensional row vectors obtained from these columns take only four different possibilities up to vector negation.

Lemma 4 *Let H be a type one Hadamard matrix of order n, $n \equiv 0 \pmod 8$. Then H^t is of type zero.*

Proof. Let $n = 4m$. Without loss of generality we may assume that the first four columns of H are in the form (1), where $a = m-1$ and $b = 1$. We show that the set S of columns $m, m+1, 2m+1, 4m$ in H^t is of type zero. Let $\mathbf{e} = (e_1, e_2, \ldots, e_n)^t$ be any column of H distinct from the first four columns and assume that $a = e_m, b = e_{m+1}, c = e_{2m+1}$ and $d = e_{4m}$. Let $x = \sum_{i=1}^{m} e_i$. Note that m is even, and so is x. Since $\mathbf{e}$ is orthogonal to the first three columns of H, we have $x = -\sum_{i=m+1}^{2m} e_i = -\sum_{i=2m+1}^{3m} e_i = \sum_{i=3m+1}^{4m} e_i$. Now since $\mathbf{e}$ is also orthogonal

to the fourth column of H, we obtain $2x - a + b + c - d = 0$. Therefore, $x = 0, \pm 2$ which implies that $(a, b, c, d) \in \{(1, 1, 1, 1), (1, 1, -1, -1), (1, -1, 1, -1), (1, -1, -1, 1)\}$ up to vector negation. It now follows that the 4-dimensional row vectors obtained from S take only four possibilities up to vector negation. Hence, S is of type zero and the assertion is immediate. □

The number of Hadamard matrices of order $4m$ ($m < 8$) for different types is shown in Table 1. We have used the library of Hadamard matrices given in [20] to compile this table. Note that for orders 24 and 28, the transpose of the unique matrix of type 2 is also of type 2.

Table 1 Number of Hadamard matrices of different types

	Order	4	8	12	16	20	24	28
	0	1	1	0	5	0	58	0
Type	1	0	0	1	0	3	1	486
	2	0	0	0	0	0	1	1

3 Canonical form

The isomorph-free exhaustive generation of combinatorial objects is an important topic in combinatorics (see [9, 17]). For a specific family of objects with given properties, the objective is to generate a representative for each of the isomorphism classes of objects. Any algorithm for an isomorph-free exhaustive generation in general involves two parallel routines. These constitute the construction of objects and the rejection of isomorphic copies of objects. The two routines are usually performed parallel to each other with interactions. For the construction phase, the most natural and widely used method is backtracking which has quite an old history, see for example [4, 23]. The method in its general form can be found in many textbooks including [9]. For the isomorph rejection, the simplest and most natural method is the so called orderly generation which was independently introduced by Read [18] and Faradžev [3] in the 1970s. Algorithms based on this scheme are called orderly algorithms. The method involves the notion of canonical form of objects. A canonical form is a special representative for each isomorphism class (equivalence class in the case of Hadamard matrices) and the main objective in the process of classification is to generate these special representatives. Each representative is constructed step by step (via an algorithm such as backtracking) and the canonicity is defined in such a way that all the constructed subobjects are also in the canonical form.

In order to generate Hadamard matrices we choose to apply a backtrack procedure to construct these objects row by row along with an orderly algorithm to eliminate equivalent solutions. We begin by defining a natural canonical form in the context of Hadamard matrices. First we need to define a lexicographical order $<$ on the set of all m by n $(-1, 1)$ matrices where m and n are two positive integers. Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be two $(-1, 1)$ matrices of order $m \times n$. We

say that $A < B$ if for some $1 \le i \le m$, the first corresponding $i-1$ rows are the same in the two matrices and there is a j, $1 \le j \le n$ such that $a_{ij} = -b_{ij} = -1$ and $a_{ik} = b_{ik}$ for all $1 \le k < j$. A $(-1, 1)$ matrix M of order $m \times n$ is said to be in *natural canonical form* if $M' \le M$ for any matrix M' which is obtained from the permutations and/or negations of rows and columns of M. It is natural to use this canonical form to classify all Hadamard matrices of a given order via the orderly method. Spence [21] classified Hadamard matrices of order 24 and 28 using the modified version of this canonical form for $(0, 1)$ matrices. Our experience showed that applying the same method for Hadamard matrices of order 32 leads to prohibitive computations. Thus we were forced to consider a modified definition of natural canonical form.

Let H be a Hadamard matrix of order n and of type zero. Trace the entries of H (from top to bottom in columns and from left to right in rows) in the following manner to make a row vector V_H of dimension n^2 from H: Column 1, column 2, column 3, column 4, the remaining entries in row 1, the remaining entries in row 2, ..., the remaining entries in row n. We say that H is in the *canonical form* if

$$V_Q \le V_H$$

for any matrix Q equivalent to H. Note that V_Q and V_H are considered as matrices and the order is the one defined above. The main features of this canonical form are as follows.

Lemma 5 *Let H be a Hadamard matrix of order $4m$ and of type zero which is in the canonical form. Then*

(i) *The rows and columns of H are in decreasing order.*

(ii) *The first four columns of H are in the following form:*

$$\begin{bmatrix} j_m & j_m & j_m & j_m \\ j_m & j_m & -j_m & -j_m \\ j_m & -j_m & j_m & -j_m \\ j_m & -j_m & -j_m & j_m \end{bmatrix}.$$

(iii) *The first three rows of H are in the following form:*

$$\begin{bmatrix} j_m^t & j_m^t & j_m^t & j_m^t \\ j_m^t & j_m^t & -j_m^t & -j_m^t \\ j_m^t & -j_m^t & j_m^t & -j_m^t \end{bmatrix}.$$

(iv) *In each column, except for the first four columns, there are $m/2$ ones and $m/2$ minus ones at the positions $(i-1)m+1$ to im for $i = 1, 2, 3, 4$.*

(v) *Let V_i be a vector whose k-th component is the $(k+4)$-th entry of the $(im+1)$-th row of H for $i = 1, 2, 3$. Then $V_3 < V_2 < V_1$.*

Remark 1 Note that with this definition of canonical form one of the basic properties of the natural canonical form, namely, the canonicity of the submatrices formed from the first top rows of H is no longer valid.

4 Search for type zero

In this section we present an orderly algorithm to generate all equivalence classes of type zero Hadamard matrices of order 32. The algorithm will eventually produce the canonical form, as defined in the previous section, for every equivalence class. Before starting the main search, there is a need for some preliminary computations.

Let H denote the canonical form of a Hadamard matrix of order $n = 32$ which is of type zero. Let H_8 be the partial Hadamard submatrix consisting of the first eight rows of H. We find all possible candidates for H_8. From Lemma 5 the first four columns and the first three rows of H_8 are uniquely determined. We then fill the rest of H_8, using Lemma 5(i) and the fact that H_8 should be a partial Hadamard matrix. Finally, the solutions are checked to be in the canonical form (the canonicity test is explained below). As a result, we find a total of 31 candidates for H_8. We label these as $H_8^{30} < H_8^{29} < \cdots < H_8^0$. We need an invariant σ to identify each of H_8^i. For any $0 \leq i \leq 30$, we partition the set of columns of H_8^i in such a way that any two columns belong to the same part if and only if they are identical (as column vectors) and define $\sigma(H_8^i)$ to be a four dimensional vector (x_1, x_2, x_3, x_4), where x_j $(1 \leq j \leq 4)$ is the number of parts of size j. This is not necessarily a total invariant. For example, H_8^{21} and H_8^{22} have the same corresponding vector $(12, 8, 0, 1)$. One may introduce a total invariant to distinguish H_8^i, but this particular invariant has the advantage of being easy to compute and works well for our purpose. There is also a need to find and retain some automorphisms of H_8^i: Permute the rows of H_8^i, multiply the columns if necessary to make sure that the first row constitutes of only ones and then sort the columns in decreasing order. For each permutation of the rows, we retain the corresponding column permutation and the negation vector if the resulting matrix is the same as H_8^i.

We are now ready to describe the search method. Each of H_8^i, $i = 0, 1, \ldots, 30$, should be extended to all possible choices of H. This process involves two ingredients; the generation of the matrix and the canonicity test. These two parts of the extension process must be executed simultaneously. There are 24 rows to fill in the generation phase. At each generation step all possible candidates for the corresponding row of H are obtained. The candidates are chosen in such a fashion that they fulfill the properties provided by Lemma 5. In reference to part (iv) of Lemma 5 one can also apply Denny's observation (see [2]) to speed up the search: Let $8(i-1)+1 \leq j \leq 8i$ for some $2 \leq i \leq 4$. Then the row j must be chosen such that the leftmost 1 is placed in the first column with less than four ones at positions $8(i-1)+1$ to $j-1$.

Next we explain the canonicity test. The basic idea of the canonicity test that we use here

has first been introduced in [12]. The general scheme, bypassing the details, for the canonicity test of the constructed matrix H is as follows. Since H is constructed using Lemma 5, by part (ii) of this lemma, the rows of H are partitioned into four blocks, say H_j $(1 \leq j \leq 4)$, where H_j constitutes the rows $8(j-1)+1$ to $8j$ of H. Assume that $H_1 = H_8^{i_0}$. Choose any set of four columns of H. If it is of type zero, then with respect to this set the rows are partitioned into a set S of four blocks each consisting of eight rows (see (1) with $b = 0$). For each block $B \in S$ the invariant σ is computed and used to find an i such that B is Hadamard equivalent to H_8^i. Note that since σ is not a total invariant, we sometimes have more than one candidate for i. The proper index i is identified by determining a permutation τ that converts B to H_8^i. If $i < i_0$, then clearly H is not in the canonical form and we are done. If $i > i_0$, then we have nothing to say and so we ignore the block B. If $i = i_0$, then we proceed to obtain the set P of permutations converting B to H_8^i by composing τ with all retained automorphisms of H_8^i. For each element of P, we compare the remaining blocks of S with H_i $(2 \leq i \leq 4)$ and if we find a permutation that gives a larger matrix (which means that H is not in the canonical form), we stop the procedure. Note that this last part is usually quite fast, since once we choose an element of P, by the fact that the rows and columns of H are in decreasing order (Lemma 5(i)), there are not too many candidate permutations to convert a block of S to H_2 (and then another block to H_3 and finally the last block to H_4). In fact most of the time, all that is needed for comparing a block of S with $H_i, i \geq 2$, is to sort the rows of that block of S after applying the column permutation. The canonicity test is time consuming and thus is not feasible to be applied at each row. We only apply the test when rows 9–12, 16, 24 and 32 are chosen. Of course, for the case H_8^0, we are also required to apply the canonicity test at rows 17 to 20. The above method also works for partial matrices with some minor modifications.

Table 2 indicates the number of Hadamard matrices corresponding to each H_8^i. The approximate computation time, in CPU hours (scaled on a 2.4 GHz CPU), for each case is also provided. We ran the program two times (with slight changes in the process of parallel executions at the second run) and obtained the same results. Hence at least we can be assure that the probability of hardware errors has been quite small. In passing, it is worth mentioning that our program found the known 58 type zero Hadamard matrices of order 24 (see Table 1) in less than two minutes on a single computer. We summarize the main result of this paper in the following theorem.

Theorem 1 *There are exactly* $13,680,757$ *equivalence classes of type zero Hadamard matrices of order* 32.

The complete list of type zero Hadamard matrices of order 32 (also the transpose of type one matrices; see the next section) is available electronically at [22] or [10]. The size of the zipped file is about 220 megabytes. The matrices from the extension of any of the 31 cases described above are also available in a smaller file. The matrices are retained in the hexadecimal format,

i.e. the strings of four subsequent entries in each matrix are encoded with hexadecimal digits. For example 0 and F represent -1 -1 -1 -1 and 1 1 1 1, respectively.

Table 2 Number of equivalence classes of type zero Hadamard matrices of order 32

i	# of matrices	Time (h)	i	# of matrices	Time (h)
0	3,058,931	14815	16	204,796	260
1	2,916,470	325	17	83,888	115
2	1,598,742	850	18	0	0
3	1,075,714	45	19	21,577	55
4	1,087,616	110	20	2,918	15
5	8,091	3	21	119,295	110
6	236,662	80	22	43,737	60
7	1,158,803	180	23	365,410	800
8	1,189,261	245	24	33,167	250
9	37,425	20	25	69,344	790
10	47,062	35	26	1,117	31
11	1,457	3	27	17,104	500
12	43,744	70	28	5,941	480
13	1,709	10	29	44	40
14	24,910	40	30	29	67
15	225,793	260			

Table 3 Number of equivalence classes of type one Hadamard matrices of order 32

i	# of matrices	i	# of matrices	i	# of matrices
0	0	11	16	21	295
1	0	12	253	22	185
2	0	13	32	23	6,801
3	0	14	82	24	993
4	0	15	2,856	25	3,065
5	0	16	5,007	26	61
6	0	17	2,004	27	1,011
7	0	18	0	28	426
8	0	19	428	29	3
9	2,656	20	0	30	6
10	189				

5 Type one matrices

By Lemma 4, a classification of Hadamard matrices of type zero would yield a classification of type one matrices. We checked type zero Hadamard matrices of order 32 that were found in the previous section and it turned out that only for a small fraction the transpose is of type one. The computation took only a few minutes on a single computer. Table 3 gives the number of Hadamard matrices corresponding to each of H_8^i $(0 \leq i \leq 30)$ which are of type one. The result is summarized in the following theorem.

Theorem 2 *There are exactly* $26,369$ *equivalence classes of type one Hadamard matrices of order* 32*.*

Acknowledgments

The work was completed while the second author was visiting the University of Lethbridge. He is grateful for the support he received. All the computations were done on a cluster of 48 CPU cores at the School of Mathematics of Institute for Research in Fundamental Sciences (IPM). We greatly appreciate the assistance provided by the cluster administrator M. Changi Ashtiani. The authors also thank the referees for the helpful comments which considerably improved the presentation of the paper.

References

[1] R. Craigen and H. Kharaghani, Hadamard matrices and Hadamard designs, in: *Handbook of Combinatorial Designs* (C. J. Colbourn and J. H. Dinitz, eds.), Second Edition, pp. 273–280, Chapman & Hall/CRC Press, Boca Raton, FL, 2007.

[2] P. C. Denny and R. Mathon, A census of t-$(t+8, t+2, 4)$ designs, $2 \leq t \leq 4$, Experimental design and related combinatorics, *J. Statist. Plann. Inference* **106** (2002), 5–19.

[3] I. A. Faradžev, Constructive enumeration of combinatorial objects, in: *Problmes combinatoires et thorie des graphes* (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976), pp. 131–135, Colloq. Internat. CNRS, 260, CNRS, Paris, 1978.

[4] S. W. Golomb and L. D. Baumert, Backtrack programming, *J. Assoc. Comput. Mach.* **12** (1965), 516–524.

[5] M. Hall, Jr., Hadamard matrices of order 16, *J.P.L. Research Summary* 36–10, **1** (1961), 21–26.

[6] M. Hall, Jr., Hadamard matrices of order 20, *J.P.L. Technical Report*, 32–761, 1965.

[7] K. J. Horadam, *Hadamard Matrices and Their Applications,* Princeton University Press, Princeton, NJ, 2007.

[8] 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* **27** (1979), 289–306.

[9] P. Kaski and P. R. J. Östergård, *Classification Algorithms for Codes and Designs,* Number 15 in Algorithms and Computation in Mathematics, Springer-Verlag, Berlin Heidelberg, 2006.

[10] H. kharaghani, A classification of Hadamard matrices of order 32 of type zero and one, http://cs.uleth.ca/˜hadi.

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

[12] G. B. Khosrovshahi and B. Tayfeh-Rezaie, Classification of simple 2-$(11, 3, 3)$ designs, *Discrete Math.* **309** (2009), 515–520.

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

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

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

[16] H. Kimura and H. Ohmori, Construction of Hadamard matrices of order 28, *Graphs Combin.* **2** (1986), 247–257.

[17] B. D. McKay, Isomorph-free exhaustive generation, *J. Algorithms* **26** (1998), 306–324.

[18] R. C. Read, Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations, *Ann. Discrete Math.* **2** (1978), 107–120.

[19] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, in: *Contemporary Design Theory: A Collection of Surveys*, (J. H. Dinitz and D. R. Stinson, eds.), pp. 431–560, John Wiley & Sons, Inc., New York, 1992.

[20] N. J. A. Sloane, A Library of Hadamard Matrices, http://www.research.att.com/∼njas/hadamard/index.html.

[21] E. Spence, Classification of Hadamard matrices of order 24 and 28, *Discrete Math.* **140** (1995), 185–243.

[22] B. Tayfeh-Rezaie, Hadamard matrices of order 32, http://math.ipm.ac.ir/tayfeh-r/Hadamard32.htm.

[23] R. J. Walker, An enumerative technique for a class of combinatorial problems, 1960 Proc. Sympos. Appl. Math., Vol. 10, pp. 91–94, American Mathematical Society, Providence, R.I.