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*

May 28, 2012

Abstract

Two Hadamard matrices are considered equivalent if one is obtained from the other by a sequence of operations involving row or column permutations or negations. We complete the classification of Hadamard matrices of order 32. It turns out that there are exactly 13710027 such matrices up to equivalence.

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 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 [12]. For surveys on Hadamard matrices, we refer the reader to [2, 7, 20].

Two Hadamard matrices are called *equivalent* if one is obtained from the other by a sequence of operations involving row or column permutations or negations. The equivalence classes of Hadamard matrices for small orders have been determined by several authors. It is well known

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

that for any order up to 12, there is a unique Hadamard matrix. For orders 16, 20, 24, 28, there are 5 [5], 3 [6], 60 [8, 16] and 487 [14, 15, 17, 23] inequivalent Hadamard matrices, respectively. Order 32 is where a combinatorial explosion occurs on the number of Hadamard matrices.

We continue the work started earlier in [11] to complete the classification of Hadamard matrices of order 32. Any such matrix is of type 0, 1, 2 or 3, as described in Section 2. In [11], all equivalence classes of Hadamard matrices of order 32 of types 0 and 1 were determined. Here, we deal with the remaining types, i.e. types 2 and 3. We apply an orderly algorithm, similar to the one used in [11], which is based on the notion of canonical form. It turns out that there are exactly 2900 Hadamard matrices of order 32 and of type 2. We also establish the uniqueness of type 3 Hadamard matrices of order 32. Consequently, the total number of Hadamard matrices of order 32 up to equivalence is found to be 13710027.

2 Definition of types

Let H be a Hadamard matrix of order n. Let j_m denote the all one column vector of dimension m. By a sequence of row or column permutations or negations, 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 [15], any set of four columns which is transformed to the above form is said to be of *type b*. Note that type is an equivalence invariant and so any permutation or 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.

In order 32 any Hadamard matrix is necessarily of type 0, 1, 2 or 3, see [11] for details. For orders less than 32, the number of Hadamard matrices of different types is shown in Table 1. We have used the library of Hadamard matrices given in [22] 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. For some possible types of Hadamard matrices and also the relation between the type of a matrix and its transpose, see Lemmas 1–4 in [11].

Table 1 Number of small 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 Definition of canonicity

The problem of classification of combinatorial objects is an old and still important topic in combinatorics. The main purpose as it is understood from the name given to the subject, i.e. *isomorph-free exhaustive generation* (see [9, 19]), is to produce a unique representative for each of the isomorphism classes of objects. The objects of interest may belong to various fields of combinatorics such as design theory, graph theory, coding theory, etc. The use of computers in such problems is indispensable, because of the nature of problems which deal with a lot of cases and computation. Hence, the classification is very much related to algorithms and computing. In the last decades, new developments on algorithmic aspects along with increase in computing power and capacity have led to many novel classifications of interesting combinatorial objects.

Any general approach to the isomorph-free exhaustive generation involves two parallel routines with interactions to each other. First one needs a suitable and efficient method to construct the objects in question and then a procedure to reject the isomorphic copies during the construction phase. The general method for constructing objects, is the backtrack algorithm which has quite a long history, see for example [4, 25]. The method in its general form can be found in many textbooks including [9]. For the isomorph rejection phase, the simplest and most natural method is the so called orderly generation which was independently introduced by Faradžev [3] and Read [21] in the 1970s. Algorithms based on this scheme are called *orderly algorithms*. The method has introduced the notion of canonical form of objects. A canonical form is a special representative for each isomorphism class. The suitable definition of canonical form is extremely dependent on the combinatorial properties of objects. As a general rule, it has to be defined in such a way that the subobjects generated during the construction process inherit some properties of the canonical form.

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 $1 \leq i \leq m$, the initial corresponding $i - 1$ rows are the same in the two matrices and there is a j, $1 \leq j \leq n$ such that $a_{ij} = -b_{ij} = -1$ and $a_{ik} = b_{ik}$ for all $1 \leq k < j$. A $(-1, 1)$ matrix M of order $m \times n$ is said to be in the *natural canonical form*

if $M' \leq M$ for any matrix M' which is obtained from permutations and/or negations of rows and columns of M.

The computational implementation of the natural canonical form is not hard and so it is the first choice in the classification of Hadamard matrices of a given order. In fact, we will use this form in classifying Hadamard matrices of order 32 when both the matrix and its transpose are for type 3. Spence [23] applied the general approach described above to confirm the classification of Hadamard matrices of order at most 28. He used a backtrack algorithm to generate matrices (in fact, incidence matrices of the corresponding designs) row by row along with an orderly algorithm to eliminate equivalent solutions. In orderly algorithm he made use of the natural canonical form. Here, we use a similar method to complete the classification of Hadamard matrices of order 32 started in [11]. Our method in this paper and [11] is essentially standard and somehow comparable to the one used in [23]. However, our experience showed that using the natural canonical form for Hadamard matrices of order 32 leads to prohibitive computations. Thus we were forced to consider a modified definition of the natural canonical form. The main novelty in our method is the introduction of a new canonical form which seems quite efficient for our purpose. The new form relies on the type of the matrices to be classified. For example, in [11], we introduced a new definition to make the computation feasible for type 0 Hadamard matrices. Here, we adopt it, with some necessary modifications, for type 2 Hadamard matrices. Note that while the new canonical form makes the formidable task of classification possible, it causes the implementation of the canonicity test to be much more complicated; a price to be paid for success

Let H be a type 2 Hadamard matrix of order $n = 4m + 8$. We may assume that the first four columns of H are in the following form:

$$\begin{bmatrix} j_2 & j_2 & j_2 & j_2 \\ j_2 & j_2 & -j_2 & -j_2 \\ j_2 & -j_2 & j_2 & -j_2 \\ j_2 & -j_2 & -j_2 & j_2 \\ j_m & j_m & j_m & -j_m \\ j_m & j_m & -j_m & j_m \\ j_m & -j_m & j_m & j_m \\ j_m & -j_m & -j_m & -j_m \end{bmatrix}. \tag{2}$$

Now delete the first four columns of H and denote the resulting matrix by V_H. We say that H is in the *canonical form* if

$$V_Q \leq V_H$$

for any matrix Q which is equivalent to H and its deleted first four columns are identical to those of (2). The following lemma gives the main features of this canonical form.

Lemma 1 *Let H be a Hadamard matrix of order $4m+8$ (m even) and of type 2 which is in canonical form. Then*

(i) *Rows $9, 10, \ldots, 4m+8$ are in decreasing order. Also columns $5, 6, \ldots, 4m+8$ are in decreasing order. (The order is as defined above).*

(ii) *The first four columns of H are identical to those of (2).*

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

$$\begin{bmatrix} j_m^t & j_m^t & j_{m+2}^t & j_{m+2}^t \\ j_m^t & j_m^t & -j_{m+2}^t & -j_{m+2}^t \\ j_m^t & -j_m^t & j_{m+2}^t & -j_{m+2}^t \end{bmatrix}.$$

(iv) *Let $H = (h_{ij})$ and let $a = h_{1j} + h_{2j} - h_{3j} - h_{4j} - h_{5j} - h_{6j} + h_{7j} + h_{8j}$ for $j > 4$. Then $a \in \{0, \pm 4, \pm 8\}$ and $h_{1j} + h_{2j} + \sum_{i=9}^{m+8} h_{ij} = a/2$.*

Proof. Since the first three parts are straightforward, we only present the proof of Part (iv). Let x, y, z, w, p, q, r, s be the inner products of column j with the blocks of rows of column 1 in (2), that is, the first 4 blocks consist of 2 rows each, and the last 4 blocks consist of m rows each. Since every block has an even number of rows, each of x, y, z, w, p, q, r, s is even. The fact that the inner product of column j and any of the columns $1, 2, 3, 4$ must be 0 gives

$$x + y + z + w + p + q + r + s = 0, \tag{3}$$
$$x + y - z - w + p + q - r - s = 0, \tag{4}$$
$$x - y + z - w + p - q + r - s = 0, \tag{5}$$
$$x - y - z + w - p + q + r - s = 0. \tag{6}$$

Taking the sum of (3)-(6) and dividing by 2, we conclude that $2x + p + q + r - s = 0$, that is,

$$p + q + r - s \equiv 0 \pmod 4, \tag{7}$$

since x is even. Adding (7) to (6), we obtain $x - y - z + w + 2(q + r - s) \equiv 0 \pmod 4$, which implies $a = x - y - z + w \equiv 0 \pmod 4$, since q, r, s are even.

Next, observe that $h_{1j} + h_{2j} + \sum_{i=9}^{m+8} h_{ij} = x + p$ and that $a = x - y - z + w$. Solve (3) through (6) for x, y, z, w to obtain $2x = -p - q - r + s, 2y = -p - q + r - s, 2z = -p + q - r - s, 2w = p - q - r - s$. We conclude that $a = 2(x + p)$ as required. □

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 initial rows of H is no longer valid.

4 Type 2 Hadamard matrices of order 32

In this section we present an orderly algorithm to generate all equivalence classes of type 2 Hadamard matrices of order 32. The algorithm will eventually produce the canonical form, as defined in the previous section, for every equivalence class. Since Hadamard matrices of order 32 of types 0 and 1 are already known [11], we may assume that the transpose of the matrices are not of type 0 or 1. Therefore, we only need to search for Hadamard matrices of type 2 with their transpose being of type 2 or 3. Before starting the main search, we need to do some preliminary computations.

For the remainder of this section, let H denote the canonical form of a Hadamard matrix of order 32 and of type 2 whose transpose is of type 2 or 3. 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 1 the first four columns and the first three rows of H_8 are uniquely determined. We then fill in the rest of H_8, using Lemma 1(i) and the fact that H_8 should be a partial Hadamard matrix. The resulting solutions are filtered through the condition (iv) of Lemma 1. Finally, the remaining solutions are tested (as explained below) to be in the canonical form. As a result, we find a total of 10319 candidates for H_8. There is also a need to find and retain the automorphisms of (2) assuming $m = 1$. We find a total of 3072 such automorphisms. For each automorphism, we retain the row permutation and the corresponding row negation vector. We do not need to keep the column permutation or the corresponding column negation vector.

We are now ready to describe the search method. Each candidate of H_8, obtained above, 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 1. At each step we also check that the added new row keeps the type of the transpose of the constructed matrix to be 2 or 3. More precisely, we consider the new row with any three of the previous rows and find the type of the four rows constituted. If their type is 0 or 1, then we ignore that candidate and proceed to the next one. Similarly, at rows 14, 20 and 26 we check if the partial matrix is extendable to a matrix of type 2. This check is necessary because sometimes one recognizes in advance the type of a set of four partial columns before proceeding to the next stage.

Next we explain the canonicity test. The basic idea of the canonicity test we use here first appeared in [13]. The general scheme, bypassing the details, for the canonicity test of the constructed matrix H is as follows. Choose any set of four columns of H. If it is of type 2, label them as the first four columns and transform the first four columns to the form (2) by suitable row/column permutations/negations. Subsequently, we apply the automorphisms of (2) to H and check if the resulting matrix is a larger matrix (which means that H is not in the canonical

form). If for all possible choices of four columns and all automorphisms of (2), the resulting matrices are equal or smaller than H, then we conclude that H is in the canonical form and retain it as a representative of its equivalence class. The above method also works for partial matrices generated during the construction phase with some minor modifications and so it can be used to eliminate some intermediate solutions. Here is a brief explanation. One finds that a set S of four partial columns is going to be of type 2 independent of the values we will set for the entries of the remaining rows of S afterwards. Label them as the first four columns and transform some rows (say i rows) of the first four columns to the i initial rows of the form (2) by suitable row/column permutations/negations. Let H' be the matrix consisting of the new i rows. Apply those automorphisms of (2) to H' which leave the first four columns unchanged and check if the resulting matrix is a larger matrix (which means that H is not in the canonical form). If for all possible choices of four columns and all automorphisms of (2), the resulting matrices are equal or smaller than H, then we conclude that the partial matrix H is in the canonical form and proceed to the next step. 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, 10, 14, 20, 26 and 32 are chosen.

We ran our program on a cluster of 48 2.2 GHz CPU. It took about nine months to accomplish the job. Our program produced 1478 matrices. We tested the matrices obtained in [11] and found 1422 and 0, type 2 Hadamard matrices of order 32 such that their transposes are of type 0 or 1, respectively. We have the following result.

Theorem 1 *There are exactly* 2900 *equivalence classes of type* 2 *Hadamard matrices of order* 32*.*

5 Type 3 and the main result

In this section we classify type 3 Hadamard matrices of order 32. Since we already know all Hadamard matrices of order 32 which are of type 0, 1, 2, it suffices to look for type 3 matrices whose transpose are also of type 3. In [1], the authors showed by a computer search that the Paley Hadamard matrix of order 32 is the unique such matrix. We confirmed their result by a different approach. We used the natural canonical form defined in Section 3 to perform our search. The solutions were constructed row by row. At every step, each candidate for the new row is checked for the following constraints: (i) it must be orthogonal to the previous rows, (ii) it must be smaller than the previous row, (iii) the columns must be in decreasing order, (iv) the type of the new row with any three of the previous rows must be 3 or 4, (v) the type of any four partial columns must be 3 or 4, if the type is known, and finally (vi) the partial matrix must be in the natural canonical form. For time saving, the canonicity test is carried out at selected rows, i.e. rows 1–16, 24, 32.

Our program on a single computer found a unique solution in just a few hours. We checked the transposes of all type 0, 1, and 2 matrices and none was of type 3. Consequently, we have the following.

Theorem 2 *There is only one type* 3 *Hadamard matrix of order* 32*.*

We summarize the results of the classification of Hadamard matrices of order 32 in the following theorem. The number of matrices of each type is presented in Table 2. The complete list of Hadamard matrices of order 32 is available electronically at [10, 24].

Theorem 3 *There are exactly* 13710027 *equivalence classes of Hadamard matrices of order* 32*.*

Table 2 Number of Hadamard matrices of different types

	Type	0	1	2	3
Type of the transpose	0	13652966	26369	1422	0
	1	26369	0	0	0
	2	1422	0	1478	0
	3	0	0	0	1
	Total	13680757	26369	2900	1

6 Automorphism groups

Brendan McKay, *the nauty master*, based on our findings [10, 24], has calculated the order of automorphism group of Hadamard matrices of order 32. We present his results [18] in Table 3. Using these results he finds that there are

632634847177185494294225485054080109697559980840399277708620193565997245853400563712000000000000000

Hadamard matrices of order 32 altogether (not considering equivalence).

He also confirmed that all matrices given in [10, 24] are inequivalent. Furthermore, he found that there are 3993 equivalence classes which are equivalent to their transposes. Following Ian Wanless' terminology [26] this means that there are 6857010 *resemblance classes* of Hadamard matrices of order 32. Finally, using a result of Spence [23] and the 13710027 matrices in [10, 24] he computed that there are 10374196953 nonisomorphic 2-(31,15,7) designs and 355293682 nonisomorphic 3-(32,16,7) designs. We greatly appreciate and acknowledge his contributions to our work.

Table 3 Number of automorphisms of Hadamard matrices of order 32 [18]

#Automorphisms	#Matrices	#Automorphisms	#Matrices
2	7943811	2048	832
4	2855780	2304	4
6	3066	2688	6
8	1644201	3072	134
10	19	3840	2
12	3315	4096	315
16	789232	4608	8
18	32	6144	85
20	44	7168	2
24	2433	8064	2
32	316427	8192	177
36	82	9216	2
40	9	10240	8
42	6	10752	4
48	2320	12288	43
56	14	14336	6
60	9	16384	71
64	83914	24576	41
72	31	29760	1
96	1141	32768	22
112	18	36864	2
120	20	49152	8
128	40037	65536	12
144	44	73728	2
192	850	98304	8
224	2	122880	3
256	13949	131072	8
288	6	172032	1
320	9	196608	6
336	5	294912	2
384	619	393216	6
448	10	516096	4
512	4502	589824	5
576	12	688128	4
768	267	786432	5
896	4	917504	1
1024	1766	1048576	1
1152	15	16515072	2
1344	4	18874368	1
1536	155	20478689280	1

Remark 2 This has been a huge undertaking, we have been very careful in our computations and a major part of the computations were double checked. However, considering the complexities involved and the possibility of hardware errors, it would be more reassuring if our data is confirmed by other researchers.

Acknowledgments

The work was completed while the second author was visiting the University of Lethbridge. He is grateful for their hospitality. The computation was performed at the Mathematics Computing Center of the Institute for Research in Fundamental Sciences (IPM) (http://math.ipm.ac.ir/mcc). We greatly appreciate the assistance provided by the system administrator, Mr. Ashtiani. The authors also thank the referees for the helpful comments which considerably improved the presentation of the paper.

References

[1] K. Betsumiya, M. Harada and H. Kimura, Hadamard matrices of order 32 and extremal ternary self-dual codes, *Des. Codes Cryptogr.* **58** (2011), 203–214.

[2] 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.

[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, in Research Summary No. 36–10, Volume I, Jet Propulsion Laboratory, Pasadena, 1961, pp. 21–26.

[6] M. Hall, Jr., *Hadamard Matrices of Order* 20, Tech. Report 32–761, Jet Propulsion Laboratory, Pasadena, 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, Hadamard matrices of order 32, http://cs.uleth.ca/~hadi.

[11] H. Kharaghani and B. Tayfeh-Rezaie, On the classification of Hadamard matrices of order 32, *J. Combin. Des.* **18** (2010), 328–336.

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

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

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

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

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

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

[18] B. D. McKay, private communication.

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

[20] 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.

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

[22] N. J. A. Sloane, A library of Hadamard matrices, http://www.research.att.com/∼njas/hadamard/index.html.

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

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

[25] 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.

[26] I. M. Wanless, Permanents of matrices of signed ones, *Linear Multilinear Algebra*, **53** (2005), 427–433.