# Classification of skew-Hadamard matrices of order 32 and association schemes of order 31

Akihide Hanaki[1] Hadi Kharaghani[2]
Ali Mohammadian[3] Behruz Tayfeh-Rezaie[4]

[1]Department of Mathematics, Faculty of Science, Shinshu University, Matsumoto 390-8621, Japan
[2]Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, T1K 3M4, Canada
[3]School of Mathematical Sciences, Anhui University, Hefei 230601, Anhui, China
[4]School of Mathematics, Institute for Research in Fundamental Sciences (IPM), P.O. Box 19395-5746, Tehran, Iran

hanaki@shinshu-u.ac.jp kharaghani@uleth.ca
ali_m@ahu.edu.cn tayfeh-r@ipm.ir

**Abstract**

Using a backtracking algorithm along with an essential change to the rows of representatives of known 13710027 equivalence classes of Hadamard matrices of order 32, we make an exhaustive computer search feasible and show that there are exactly 6662 inequivalent skew-Hadamard matrices of order 32. Two skew-Hadamard matrices are considered SH-equivalent if they are similar by a signed permutation matrix. We determine that there are precisely 7227 skew-Hadamard matrices of order 32 up to SH-equivalence. This partly settles a problem posed by Kim and Solé. As a consequence, we provide the classification of association schemes of order 31.

**Keywords:** Association Scheme, Classification, Skew-Hadamard Matrix.

**AMS Mathematics Subject Classification:** 05B20, 05E30, 15B34.

## 1 Introduction

A *Hadamard matrix* of order $n$ is an $n \times n$ matrix $H$ with entries in $\{-1, 1\}$ such that $HH^\top = nI$, where $H^\top$ 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 [15]. It is a longstanding open question whether Hadamard matrices of order $n$ exist for any $n$ divisible by 4. The smallest order for which there is no known Hadamard matrix is 668 [12]. Hadamard matrices have been extensively investigated and have found many applications in several diverse fields.

A Hadamard matrix $H$ is said to be *skew-Hadamard* if $H + H^\top = 2I$. Skew-Hadamard matrices, being equivalent to doubly regular tournaments [3], form a class of Hadamard matrices, which has been widely studied. They are used to construct several combinatorial objects, such as association schemes, self-dual codes, strongly regular graphs, and more. As with Hadamard matrices, it is an open question whether skew-Hadamard matrices of order $n$ exist for any $n$ divisible by 4. The smallest unknown order of a skew-Hadamard matrix is 276 [5].

A *permutation matrix* (respectively, *signed permutation matrix*) is a matrix with entries in $\{0, 1\}$ (respectively, $\{-1, 0, 1\}$) which has exactly one nonzero entry in each row and each column. Two Hadamard matrices $H$ and $K$ are said to be H-*equivalent* if there exist two signed permutation matrices $P$ and $Q$ such that $K = PHQ$, otherwise, they are called H-*inequivalent*. All H-inequivalent Hadamard matrices of orders up to 32 have been classified [11]. Two skew-Hadamard matrices $H$ and $K$ are said to be SH-*equivalent* if there exists a signed permutation matrix $P$ such that $K = P^{-1}HP$, otherwise, they are called SH-*inequivalent*. All H-inequivalent and SH-inequivalent skew-Hadamard matrices of orders up to 28 have been classified [1, 18].

In 2008, Kim and Solé proposed the problem to find exhaustive lists of H-inequivalent skew-Hadamard matrices of orders 32 and 64 [13]. In this paper, we determine the number of H-inequivalent and SH-inequivalent skew-Hadamard matrices of order 32. It turns out that there are exactly 6662 skew-Hadamard matrices of order 32 up to H-equivalence, and there are exactly 7227 skew-Hadamard matrices of order 32 up to SH-equivalence. The resulting classification is shown in Table 1.

| order | 1 | 2 | 4 | 8 | 12 | 16 | 20 | 24 | 28 | 32 |
|---|---|---|---|---|---|---|---|---|---|---|
| # H-inequivalent Hadamard matrices | 1 | 1 | 1 | 1 | 1 | 5 | 3 | 60 | 487 | 13710027 |
| # H-inequivalent skew-Hadamard matrices | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 16 | 54 | 6662 |
| # SH-inequivalent skew-Hadamard matrices | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 16 | 65 | 7227 |

**Table 1.** The number of H-inequivalent Hadamard matrices, H-inequivalent skew-Hadamard matrices, and SH-inequivalent skew-Hadamard matrices of orders up to 32.

## 2 Skew-Hadamard matrices of order 32

All H-equivalence classes of Hadamard matrices of order 32 were classified in [11]. It turned out that the number of H-inequivalent Hadamard matrices of order 32 is exactly 13710027. To find which of the classes contains a skew-Hadamard matrix, we use the following simple yet important observation from [14]. A Hadamard matrix $H$ is H-equivalent to a skew-Hadamard matrix if and only if there exists a signed permutation matrix $P$ such that $HP$ is a skew-Hadamard matrix. So, instead of multiplying $H$ from the left and the right by signed permutation matrices, we need only to consider multiplication from the right. Also, one can see that the signs of nonzero entries of $P$ is uniquely determined since the diagonal entries of $HP$ are all 1. Let $\mathcal{R}$ be the set of representatives of 13710027 $\mathsf{H}$-inequivalent Hadamard matrices of order 32. For each Hadamard matrix $H \in \mathcal{R}$, the following procedure is applied. We try to find a signed permutation matrix $P$ such that $HP$ is a skew-Hadamard matrix. The matrix $P$ is constructed column by column through a backtracking algorithm. At step $i$, when the column $i$ of $P$ is chosen, it is checked that the principal submatrix of $HP$ on the first $i$ rows and columns to be skew with diagonal entries being 1. If not, then we backtrack. The procedure is ended if either all columns of $P$ are chosen, which in this case $HP$ will be a skew-Hadamard matrix or no such $P$ is found. The experiment with some randomly chosen elements of $\mathcal{R}$ shows that it would take a long time to check all elements of $\mathcal{R}$. We guessed that the reason for this is the high symmetry hidden in the first rows of elements of $\mathcal{R}$, which prohibits the algorithm from backtracking in earlier steps. In order to resolve this problem and make the computation feasible, we chose a random permutation on the rows and applied it to every element of $\mathcal{R}$. The trick worked, and the time was reasonably reduced so that we could run the algorithm on the whole set $\mathcal{R}$. The computation time was about one week on a 2.6 GHz PC. The same code was run twice on two different machines with different operating systems, and we received similar results. Therefore, the probability of any hardware error is extremely small. We also implemented some parts of the algorithm twice with different codes. Another test for the correctness of the program was the confirmation of all the numbers given in Table 1 for orders up to 28. We summarize our results in the following theorem.

**Theorem 2.1.** *There are exactly* 6662 $\mathsf{H}$*-inequivalent skew-Hadamard matrices of order* 32*.*

Now we turn our attention to $\mathsf{SH}$-equivalence. We run the algorithm described above on the set $\mathcal{S}$ of representatives of 6662 $\mathsf{H}$-inequivalent skew-Hadamard matrices of order 32 and, for each Hadamard matrix $H \in \mathcal{S}$, we find all signed permutation matrices $P_1, \ldots, P_\ell$ such that $HP_i$ is a skew-Hadamard matrix for all $i$. If $K$ is a skew-Hadamard matrix in the $\mathsf{H}$-equivalence class of $H$, then $K = PHQ$ for some signed permutation matrices $P$ and $Q$ and so $P^{-1}KP = H(QP)$ which means that $K$ is $\mathsf{SH}$-equivalent to $HP_i$ for some $i$. Therefore, it suffices to check $\mathsf{SH}$-equivalence in the set $\{HP_1, \ldots, HP_\ell\}$. Our program shows that $\ell$ is at most 16 and $\ell = 1$ for most of the cases. Hence, it is fast and easy to perform $\mathsf{SH}$-equivalence. We obtain the following theorem.

**Theorem 2.2.** *There are exactly* 7227 $\mathsf{SH}$*-inequivalent skew-Hadamard matrices of order* 32*.*

The complete lists of skew-Hadamard matrices of order 32 are available electronically at [19]. Similar lists for orders up to 32 have been posted on [21].

## 3 Association schemes of order 31

As a corollary of the classification of skew-Hadamard matrices of order 32, we can achieve the classification of association schemes of order 31. First, we give a definition of association schemes in matrix form. An *association scheme* of order $n$ and class $d$ is a set of nonzero $n \times n$ matrices $\mathcal{S} = \{A_0, A_1, \dots, A_d\}$ with entries in $\{0,1\}$ such that

(i) $A_0 = I$;

(ii) Every entry of $\sum_{i=0}^{d} A_i$ is 1;

(iii) For any $i, j \in \{0, 1, \dots, d\}$, $A_i^\top$ and $A_i A_j$ are linear combinations of $A_0, A_1, \dots, A_d$.

It is well known that, for any $i \in \{0, 1, \dots, d\}$, all row and column sums of $A_i$ are the same. We call this number the *valency* of $A_i$ and denote by $k_i$. Indeed, $k_0$ which is called the *trivial valency* is equal to 1. An association scheme is said to be *symmetric* if all its elements are symmetric matrices. An association scheme is called *Schurian* if it forms a basis for the centralizer algebra of a transitive group of permutation matrices. Two association schemes $\mathcal{S}$ and $\mathcal{T}$ are said to be *isomorphic* if there exists a permutation matrix $P$ such that $\mathcal{T} = P^{-1}\mathcal{S}P$.

We now consider the case $n = 31$. It is proved that the nontrivial valencies of association schemes of prime orders are the same [10]. Letting $k_1 = \cdots = k_d = k$, we have $1 + dk = 31$ and thus $d \in \{1, 2, 3, 5, 6, 10, 15, 30\}$. It is known that there exists exactly one Schurian association scheme of order 31 and class $d$ for any $d \in \{1, 2, 3, 5, 6, 10, 15, 30\}$ [16, Theorem 7.3]. This result along with a method similar to the ones in [8, 9] and a computer calculation by backtracking implies the next lemma.

**Lemma 3.1.** *For each $d \in \{1, 3, 5, 6, 10, 15, 30\}$, there is a unique association scheme of order 31 and class $d$.*

The following is devoted to the case $d = 2$. In this case, association schemes are nonsymmetric. There is a known correspondence between skew-Hadamard matrices and nonsymmetric association schemes of class 2. Let $n \equiv 3 \pmod 4$ and $\mathcal{S} = \{A_0, A_1, A_2\}$ be a nonsymmetric association scheme of order $n$. Then,

$$H(\mathcal{S}) = \left[\begin{array}{c|ccc} 1 & 1 & \cdots & 1 \\ \hline -1 & & & \\ \vdots & & A_0 + A_1 - A_2 & \\ -1 & & & \end{array}\right] \tag{1}$$

is a skew-Hadamard matrix of order $n+1$. Conversely, association schemes can be obtained from a skew-Hadamard matrix $H$ of order $n+1$. Let $D_i$ be the diagonal matrix whose diagonal vector is the $i$th row vector of $H$. Clearly, $D_i^{-1} H D_i$ is of the form

$$\begin{array}{cc} & \begin{array}{ccccccc} \phantom{1} & \phantom{\cdots} & \phantom{1} & i & \phantom{1} & \phantom{\cdots} & \phantom{1} \end{array} \\ i & \left[\begin{array}{ccc|c|ccc} & & & -1 & & & \\ & & & \vdots & & & \\ & & & -1 & & & \\ \hline 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ \hline & & & -1 & & & \\ & & & \vdots & & & \\ & & & -1 & & & \end{array}\right] \end{array}. \tag{2}$$

Define an $n \times n$ matrix $R_i$ by deleting the $i$th row and column of $D_i^{-1}HD_i$. We get an association scheme $H^{(i)}$ by reversing the above operation, namely, $H^{(i)} = \{A_0, A_1, A_2\}$, where $A_0 = I$, $A_1 = (J - 2I + R_i)/2$, $A_2 = (J - R_i)/2$, and $J$ denotes the all one matrix. For details, see [7]. We remark that the association scheme depends on the choice of $i$. We give a small example.

**Example 3.2.** Consider a skew-Hadamard matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$$

and let compute $H^{(4)}$. We have

$$D_4 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } D_4^{-1}HD_4 = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Now, we get the nonsymmetric association scheme $H^{(4)} = \{A_0, A_1, A_2\}$, where

$$A_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, A_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

We use the following lemma to obtain all nonsymmetric association schemes of class 2 from skew-Hadamard matrices.

**Lemma 3.3.** *Let $H_1, \dots, H_m$ be representatives of all the* $\mathsf{SH}$*-equivalence classes of skew-Hadamard matrices of order $n+1$. Then*

$$\mathscr{A}_n = \left\{ H_k^{(i)} \;\middle|\; k = 1, \dots, m \text{ and } i = 1, \dots, n+1 \right\}$$

*contains representatives of all the isomorphism classes of nonsymmetric association schemes of order $n$ and class 2.*

*Proof.* Let $\mathcal{S}$ be a nonsymmetric association scheme of order $n$ and class 2 and let $H(\mathcal{S})$ be a skew-Hadamard matrix defined in (1). There exist $H \in \{H_1, \dots, H_m\}$ and a signed permutation matrix $P$ such that $H(\mathcal{S}) = P^{-1}HP$. Moreover, there exist a permutation matrix $Q$ and a diagonal matrix $D$ such that $P = DQ$. Let $\sigma$ be the permutation on $\{1, \dots, n+1\}$ given by $Q$, that is, $\sigma(i) = j$ if $Q_{ij} = 1$. Then, $QH(\mathcal{S})Q^{-1}$ is of the form given in (2) with $i = \sigma^{-1}(1)$. Since $QH(\mathcal{S})Q^{-1} = D^{-1}HD$, the diagonal vector of $D$ must be the $i$th row vector of $H$ or its negation. This means that $H^{(i)}$ is obtained from $D^{-1}HD$ by deleting the $i$th row and column. So, if $R$ is the matrix obtained from $Q$ by deleting the $i$th row and the first column, then $\mathcal{S} = R^{-1}H^{(i)}R$. This completes the proof. $\square$

We need to compute isomorphisms in $\mathscr{A}_{31}$. This can be done by GRAPE Package [17] on GAP [20]. Suppose that $\mathcal{S} = \{A_0, A_1, A_2\}$ and $\mathcal{T} = \{B_0, B_1, B_2\}$ are two association schemes in $\mathscr{A}_{31}$. We denote by $G(A)$ the directed graph corresponding to a matrix $A$ whose entries are in $\{0,1\}$. Then $\mathcal{S}$ and $\mathcal{T}$ are isomorphic as association schemes if and only if "IsIsomorphicGraph($G(A_1)$, $G(B_1)$) or IsIsomorphicGraph($G(A_1)$, $G(B_2)$)" is true on GAP. However, we could not finish the computation by using this function directly. We define an invariant obtained from [2]. Let $A$ be an $n \times n$ matrix with entries in $\{0,1\}$. For mutually distinct indices $i, j, k \in \{1, \dots, n\}$, we define

$$m\big(\{i,j,k\}\big) = \left|\left\{\ell \in \{1,\dots,n\} \,\middle|\, A_{i\ell} = A_{j\ell} = A_{k\ell} = 1\right\}\right|$$

and we consider the multiset

$$M(A) = \left\{m\big(\{i,j,k\}\big) \,\middle|\, i,j,k \in \{1,\dots,n\} \text{ are mutually distinct}\right\}.$$

The next lemma is clear by definition.

**Lemma 3.4.** *Let $\{A_0, A_1, A_2\}$ and $\{B_0, B_1, B_2\}$ be isomorphic nonsymmetric association schemes. Then $\{M(A_1), M(A_2)\} = \{M(B_1), M(B_2)\}$.*

So, $\{M(A_1), M(A_2)\}$ is an invariant of a nonsymmetric association scheme $\{A_0, A_1, A_2\}$. Note that this invariant is closely related to the 4-profile of Hadamard matrices [4].

**Example 3.5.** Denote by $H$ the first skew-Hadamard matrix in the list of SH-inequivalent skew-Hadamard matrices of order 32 given in [19]. If we let $H^{(1)} = \{A_0, A_1, A_2\}$, then

$$\begin{aligned}\big\{M(A_1), M(A_2)\big\} \;=\; & \Big\{\Big\{0^{2}, 1^{54}, 2^{582}, 3^{2707}, 4^{990}, 5^{156}, 6^{2}, 7^{2}\Big\},\\ & \Big\{0^{4}, 1^{44}, 2^{617}, 3^{2626}, 4^{1094}, 5^{88}, 6^{21}, 7^{1}\Big\}\Big\},\end{aligned}$$

where the exponents indicate the multiplicities.

This invariant is very useful, because there are 88745 distinct values for $\mathscr{A}_{31}$. Consequently, we have the classification of association schemes of order 31.

**Theorem 3.6.** *There exist exactly* 98307 *isomorphism classes of association schemes of order* 31*.*

*Proof.* By the GRAPE function with help of the invariant described above, we found 98300 isomorphism classes of nonsymmetric association schemes of order 31 and class 2. Symmetric association schemes of class 2 are correspondent to strongly regular graphs. Since no strongly regular graph exists in order 31, there are no symmetric association schemes of order 31 and class 2. From Lemma 3.1, there are also 7 other association schemes. The result follows. $\square$

All data and programs used in this section are available electronically at [6]. Also, the complete lists of association schemes of orders $3, \dots, 34$, and 38 have been posted on [22].

## Acknowledgments

Akihide Hanaki was supported by JSPS KAKENHI Grant Number JP17K05165. Hadi Kharaghani was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC). The paper was written while Ali Mohammadian was visiting the Institute for Research in Fundamental Sciences (IPM) in July 2019. He wishes to express his gratitude for the hospitality and support he received from IPM. The authors gratefully acknowledge valuable suggestions from the referees which helped to considerably improve the presentation of the paper.

## References

[1] A.H. Baartmans, C. Lin, W.D. Wallis, Symmetric and skew equivalence of Hadamard matrices of order 28, *Ars. Combin.* **41** (1995), 25–31.

[2] E. Bannai, Private communication, 2015.

[3] E. Brown and K.B. Reid, Doubly regular tournaments are equivalent to skew Hadamard matrices, *J. Combinatorial Theory Ser. A* **12** (1972), 332–338.

[4] J. Cooper, J. Milas, and W.D. Wallis, Hadamard equivalence, *Combinatorial Mathematics*, in: Lecture Notes in Math., vol. 686, Springer, pp. 126–135, 1978.

[5] D.Ž. Đoković, Skew-Hadamard matrices of orders 188 and 388 exist, *Int. Math. Forum* **3** (2008), 1063–1068.

[6] A. Hanaki, Classification of association schemes of order 31, http://math.shinshu-u.ac.jp/~hanaki/as/as31.

[7] A. Hanaki, Skew-symmetric Hadamard matrices and association schemes, *SUT J. Math.* **36** (2000), 251–258.

[8] A. Hanaki and I. Miyamoto, Classification of association schemes with 18 and 19 vertices, *Korean J. Comput. Appl. Math.* **5** (1998), 543–551.

[9] A. Hanaki and I. Miyamoto, Classification of association schemes with 16 and 17 vertices, *Kyushu J. Math.* **52** (1998), 383–395.

[10] A. Hanaki and K.Uno, Algebraic structure of association schemes of prime order, *J. Algebraic Combin.* **23** (2006), 189–195.

[11] H. Kharaghani and B. Tayfeh-Rezaie, Hadamard matrices of order 32, *J. Combin. Des.* **21** (2013), 212–221.

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

[13] J.-L. Kim and P. Solé, Skew Hadamard designs and their codes, *Des. Codes Cryptogr.* **49** (2008), 135–145.

[14] J.Q. Longyear, Criteria for a Hadamard matrix to be skew-equivalent, *Canad. J. Math.* **28** (1976), 1216–1223.

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

[16] D.S. Passman, *Permutation Groups*, Revised edition, Dover Publications, Mineola, New York, 2012.

[17] L.H. Soicher, GRAPE — Graph algorithms using permutation groups, Version 4.8.2, Refereed GAP package, 2019, available at: http://gap-packages.github.io/grape.

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

[19] B. Tayfeh-Rezaie, Skew-Hadamard matrices of order 32, http://math.ipm.ac.ir/~tayfeh-r/SkewHadamard32.htm.

[20] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.10.2, 2019.

[21] Zenodo, Skew-Hadamard matrices up to order 32, http://zenodo.org/record/3613659.

[22] Zenodo, Classification of small association schemes, http://zenodo.org/record/3627736.