University of Wollongong

Research Online

Faculty of Engineering and Information Sciences - Papers: Part B

Faculty of Engineering and Information Sciences

2018

Embedding and Extension Properties of Hadamard Matrices Revisited

Dimitrios Christou
American College of Greece

Marilena Mitrouli
National and Kapodistrian University of Athens

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Follow this and additional works at: https://ro.uow.edu.au/eispapers1

 Part of the Engineering Commons, and the Science and Technology Studies Commons

Recommended Citation

Christou, Dimitrios; Mitrouli, Marilena; and Seberry, Jennifer, "Embedding and Extension Properties of Hadamard Matrices Revisited" (2018). *Faculty of Engineering and Information Sciences - Papers: Part B*. 1372.
https://ro.uow.edu.au/eispapers1/1372

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Embedding and Extension Properties of Hadamard Matrices Revisited

Abstract

2018 2018. Hadamard matrices have many applications in several mathematical areas due to their special form and the numerous properties that characterize them. Based on a recently developed relation between minors of Hadamard matrices and using tools from calculus and elementary number theory, this work highlights a direct way to investigate the conditions under which an Hadamard matrix of order n - k can or cannot be embedded in an Hadamard matrix of order n. The results obtained also provide answers to the problem of determining the values of the spectrum of the determinant function for specific orders of minors of Hadamard matrices by introducing an analytic formula.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Christou, D., Mitrouli, M. & Seberry, J. (2018). Embedding and Extension Properties of Hadamard Matrices Revisited. Special Matrices, 6 (1), 155-165.

This journal article is available at Research Online: https://ro.uow.edu.au/eispapers1/1372

Research Article **Open Access**

Dimitrios Christou, Marilena Mitrouli*, and Jennifer Seberry

Embedding and extension properties of Hadamard matrices revisited

10.1515/spma-2018-0012
Received September 13, 2017; accepted March 12, 2018

Abstract: Hadamard matrices have many applications in several mathematical areas due to their special form and the numerous properties that characterize them. Based on a recently developed relation between minors of Hadamard matrices and using tools from calculus and elementary number theory, this work highlights a direct way to investigate the conditions under which an Hadamard matrix of order $n - k$ can or cannot be embedded in an Hadamard matrix of order n. The results obtained also provide answers to the problem of determining the values of the spectrum of the determinant function for specific orders of minors of Hadamard matrices by introducing an analytic formula.

Keywords: Submatrices; minors; determinant spectrum; differentiation

MSC2010: 05B20, 15A15, 15B10

1 Introduction and motivation

From their initial study in the late 19th century until today, Hadamard matrices, named after the French mathematician *Jacques Hadamard* (1865–1963), are proven to be very useful in several scientific areas, such as computational mathematics and physics, coding theory and cryptography, statistics, informatics, and telecommunications with numerous applications [9].

An Hadamard matrix of order n, denoted by H_n, is an $n \times n$ matrix with elements $+1$ or -1 and mutually orthogonal rows and columns, i.e.,

$$H_n H_n^\top = H_n^\top H_n = n I_n \tag{1}$$

where $H_n^\top$ denotes the transpose of H_n and I_n is the identity matrix of order n. Also, a Hadamard matrix is said to be *normalized* if it has its first row and column all 1's. Hadamard himself showed that the matrices of this kind have the maximal determinant

$$|\det H_n| = n^{n/2} \tag{2}$$

and he observed that such matrices could exist only if n was 1, 2 or a multiple of 4 [8]. Despite the efforts of several mathematicians, Hadamard's observation remains unproven and has formed the basis of one of the great unsolved mathematical problems, referred to as *the Hadamard conjecture*. However, several methods for the construction of Hadamard matrices have been developed with the oldest one given by the English mathematician J.J. Sylvester in 1867 who proved that there are (± 1)-matrices of order 2^t for all positive integers t which have the properties of Hadamard matrices. Such matrices are referred to as *the Sylvester-Hadamard*

Dimitrios Christou: Department of Science and Mathematics, Deree -The American College of Greece, 6 Gravias St. GR-15342, Athens, Greece, E-mail: dchristou@acg.edu
***Corresponding Author: Marilena Mitrouli:** Department of Mathematics, National and Kapodistrian University of Athens, Panepistemiopolis GR-15773, Athens, Greece, E-mail: mmitroul@math.uoa.gr
Jennifer Seberry: School of Computing and Information Technology, University of Wollongong, Wollongong NSW 2522, Australia, E-mail: jennifer_seberry@uow.edu.au

Open Access. © 2018 Dimitrios Christou et al., published by De Gruyter. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.
Unauthenticated
Download Date | 5/15/18 4:44 AM

matrices. Since the construction of an Hadamard matrix of order 428 published by Kharaghani and Tayfeh-Rezaie [10], the smallest order for which no Hadamard matrix is presently known is 668.

Frequently, in several applications it is useful to know if specific Hadamard matrices are embedded in other Hadamard matrices of higher order, i.e. if an Hadamard matrix of order m is a submatrix of an Hadamard matrix of order n, when $m < n$. We denote this by $H_m \in H_n$. Regarding the existing embedding properties of the Hadamard matrices [4, 13], it is known that H_4 is embedded in H_n for any order $n > 4$ and H_n is embedded in H_{2n} due to the doubling construction [15], which means that the matrix

$$H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}$$

is always a Hadamard matrix of order $2n$ when H_n is a Hadamard matrix of order n. These properties can be expressed as

$$H_4 \in H_n \text{ and } H_n \in H_{2n} \tag{3}$$

In 1965, Cohn [3] proved that H_n can have a Hadamard submatrix H_m when $m \le \frac{n}{2}$. Using matrix algebra, Vijayan [17] proved that $(n-k)\times n$ row-orthogonal matrices with ± 1 elements can be extended to $n\times n$ Hadamard matrices when $k \le 4$. More recently, Evangelaras *et al.* [5] used the distance distribution from coding theory to search for normalized Hadamard matrices of order n embedded in normalized Hadamard matrices of order $m \ge 2n$, and Brent [2] generalized Cohn's result to maximal determinant submatrices of Hadamard matrices showing that if H_n has a maximal determinant submatrix M of order m, then $m < (\frac{n}{2} + 5\ln n)$ or $m \ge n - 2$. Several other researchers have dealt with this problem in the past employing mostly combinatorial methods and the approaches that have been developed so far are either constructive [12] or employ the Hadamard conjecture [7] providing partially inconclusive results.

In this paper, we examine the conditions under which an Hadamard matrix of order $n-k$ can be embedded in an Hadamard matrix of order n, denoted by $H_{n-k} \in H_n$. The current approach is based on a relation between the minors of Hadamard matrices presented in [16] and, by employing differential calculus and elementary number theory, first, we show that $H_{n-4} \notin H_n$ and $H_{n-8} \notin H_n$. Then, for any positive integers n and k multiples of 4, we proceed with the generalization

$$H_{n-k} \notin H_n \text{ for } k < \frac{n}{2} \tag{4}$$

which is equivalent to Cohn's result in [3]. The above relation (4) was also considered in [2] where it is proven using Szöllősi's result [16] about the minors of a Hadamard matrix and calculus techniques.

In Section 2, we analyze this approach in more depth providing an alternative proof of Szöllősi's result and an analytic description of the steps of the proof of (4), starting from $H_{n-4} \notin H_n$. Then, we provide a new number theoretic proof for $H_{n-8} \notin H_n$. Finally, in Section 3, we study the problem whether H_{n-k} can exist embedded in H_n when $4 \le k < n$, and the connection between the order of the matrix H_{n-k} and the values which form the spectrum of the determinant function for (± 1)-matrices [4, 11].

2 Embedding properties via minors

The current study of the embedding and extension properties of Hadamard matrices is motivated by the results obtained from [16] which lead to a simple relation connecting the minors of a (± 1)-matrix. The proof of this result was based on the properties of the generalized matrix determinant. A simplified proof of the same result has recently been presented by Banica *et al.* [1]. A more elegant, direct proof employing only the Jacobi identity [6] is given next.

Proposition 1. *Let H_n an Hadamard matrix of order $n \ge 4$. If M_k denotes the absolute value of a $k \times k$ minor of H_n where $k = d$ or $n - d$, then for any $1 < d < n$ it holds:*

$$M_{n-d} = n^{\frac{n}{2}-d} M_d \tag{5}$$

Unauthenticated
Download Date | 5/15/18 4:44 AM

Proof. An Hadamard matrix of order n can be considered as a block-matrix of the form

$$H_n = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

where A is a $(n-d)\times(n-d)$ (±1)-matrix and D is a $d\times d$ (±1)-matrix for $1 < d < n$. If $U = \left(\sqrt{n}\right)^{-1} H_n$, then U is orthogonal, because

$$U\,U^\top = \frac{1}{\sqrt{n}} H_n \frac{1}{\sqrt{n}} H_n^\top = \frac{1}{n} H_n H_n^\top = \frac{1}{n} nI_n = I_n$$

Consequently, U is invertible and its inverse has the form:

$$U^{-1} = U^\top = \frac{1}{\sqrt{n}} \begin{bmatrix} A^\top & C^\top \\ B^\top & D^\top \end{bmatrix}$$

Using Jacobi's determinant identity [6] for U, it follows:

$$\begin{aligned}
\det\left(\frac{1}{\sqrt{n}}A\right) &= \det U \cdot \det\left(\frac{1}{\sqrt{n}}D^\top\right) \quad \overset{|\det U|=1}{\Leftrightarrow} \\
\left|\det\left(n^{-\frac{1}{2}}A\right)\right| &= \left|\det\left(n^{-\frac{1}{2}}D^\top\right)\right| \quad \Leftrightarrow \\
n^{-\frac{n-d}{2}}\,|\det A| &= n^{-\frac{d}{2}}\left|\det D^\top\right| \quad \overset{|\det D^\top|=|\det D|}{\Leftrightarrow} \\
|\det A| &= n^{\frac{n}{2}-d}\,|\det D|
\end{aligned}$$

Since the absolute determinant of a matrix remains invariant under row or column interchange, the last equation holds for any $(n-d)\times(n-d)$ and $d\times d$ minors of H_n. □

The next lemma specifies the values of the determinant of a square (±1)-matrix of order $n \le 6$ and gives a more general property for the determinant of order $n > 6$. These values will be useful in the following.

Lemma 1 ([4]). Let B be an $n\times n$ matrix with elements ±1. It holds that

i) $\det B$ is an integer and 2^{n-1} divides $\det B$,
ii) when $n \le 6$, the only possible values for $\det B$ are given in Table 1, and they do all occur.

According to Lemma 1-(i), if M_k denotes the absolute value of a $k\times k$ minor of a (±1)-matrix of order $n \ge k$, then

$$M_k = p\,2^{k-1} \tag{6}$$

where p is either a positive integer, or zero.

Table 1: Possible absolute values of the determinant of $n\times n$ matrices with elements ±1.

n	1	2	3	4	5	6
$\det B$	1	0, 2	0, 4	0, 8, 16	0, 16, 32, 48	0, 32, 64, 96, 128, 160

Definition 1 ([11]). The *spectrum of the determinant function for* (±1)*-matrices* is defined to be the set of values taken by $p = 2^{1-k}\,|\det R_k|$ as the matrix R_k ranges over all $k\times k$ (±1)-matrices.

Orrick and Solomon give a list of values for p in [11]. They instance all values for $k = 1, 2, \ldots, 11,$ and 13. Also, conjectures have been formulated for $k = 12, 14, 15, 16,$ and 17.

Unauthenticated
Download Date | 5/15/18 4:44 AM

2.1 Embeddability of Hadamard matrices of order $n-4$

Considering the above results, we begin the study of the embedding of Hadamard matrices of order $n-k$ when $n > 8$ and $k = 4$. The following proposition can be established.

Proposition 2. *An Hadamard matrix of order $n-4$ cannot be embedded in an Hadamard matrix of order n for any $n = 4t$ with integer $t > 2$.*

$$H_{n-4} \notin H_n, \quad n > 8 \tag{7}$$

Proof. If $t = 1$, then $n = 4$ and $H_{n-4} = H_0$ which does not exist. If $t = 2$, then $n = 8$ and $H_{n-4} = H_4 \in H_8 = H_n$ which is true according to (3). Therefore, an integer $t > 2$ must be considered in the following.

Assuming that an Hadamard matrix of order $n-4$ can be embedded in an Hadamard matrix of order n, the relation (5) for $d = 4$ implies that

$$|\det H_{n-4}| = n^{\frac{n}{2}-4} M_4 \tag{8}$$

where M_4 is the absolute value of a 4×4 minor of H_n. However, it is known that

$$|\det H_{n-4}| = (n-4)^{\frac{n-4}{2}} \tag{9}$$

and, according to Lemma 1-(ii), the possible non zero values that M_4 can take are 8 or 16. Considering both cases, the value of M_4 will be denoted by m in the following.

Combining (8) and (9), it follows that:

$$\begin{aligned}
(n-4)^{\frac{n-4}{2}} &= n^{\frac{n}{2}-4} \cdot m \quad \Leftrightarrow \\
e^{\frac{n-4}{2}\ln(n-4)} &= e^{\frac{n-8}{2}\ln(n)} \cdot e^{\ln(m)} \quad \Leftrightarrow \\
\frac{n-4}{2}\ln(n-4) &= \frac{n-8}{2}\ln(n) + \ln(m) \quad \overset{n=4t}{\Leftrightarrow} \\
(4t-4)\ln(4t-4) &= (4t-8)\ln(4t) + 2\ln(m) \quad \Leftrightarrow \\
(t-1)\ln(4(t-1)) &= (t-2)\ln(4t) + \frac{\ln(m)}{2} \quad \Leftrightarrow \\
(t-1)\big(\ln 4 + \ln(t-1)\big) &= (t-2)\big(\ln 4 + \ln(t)\big) + \ln(\sqrt{m}) \quad \Leftrightarrow \\
(t-1)\ln 4 + (t-1)\ln(t-1) &= (t-2)\ln 4 + (t-2)\ln(t) + \ln(\sqrt{m}) \quad \Leftrightarrow
\end{aligned}$$

$$(t-1)\ln(t-1) - (t-2)\ln t = \ln\left(\frac{\sqrt{m}}{4}\right) \tag{10}$$

Since $t > 2$, every term in (10) can be divided by the non-zero algebraic expression $(t-1)(t-2)$. Then, (10) is transformed into

$$\frac{\ln(t-1)}{t-2} - \frac{\ln(t)}{t-1} = \frac{\ln\left(\frac{\sqrt{m}}{4}\right)}{(t-1)(t-2)} \tag{11}$$

Using the function $f(x) = \frac{\ln(x)}{x-1}$, the above equation (11) can be expressed in the form:

$$f(t-1) - f(t) = \frac{\ln\left(\frac{\sqrt{m}}{4}\right)}{(t-1)(t-2)} \tag{12}$$

The real function f is well defined and differentiable in the interval $(2, +\infty)$. Moreover, for every $x \in (2, +\infty)$ it holds:

$$f(x) > 0 \text{ and } \frac{df}{dx} = \frac{\left(1 - \frac{1}{x}\right) - \ln(x)}{(x-1)^2} < 0$$

The latter shows that f is a strictly decreasing function in the interval $(2, +\infty)$. Hence, for any $t > 2$ it holds:

$$t - 1 < t \Leftrightarrow f(t-1) > f(t) \Leftrightarrow f(t-1) - f(t) > 0 \tag{13}$$

Consequently, the left part of the equation (12) is always positive whereas its right part is either negative (for $m = 8$) or zero (for $m = 16$). Therefore, the assumption that was made in the derivation of the equation (8) is invalid for any $n = 4t$ with integer $t > 2$. Thus, H_{n-4} cannot be embedded in H_n. □

Unauthenticated
Download Date | 5/15/18 4:44 AM

2.2 Embeddability of Hadamard matrices of order $n - 8$

In the case of H_{n-k} with $k = 4$ the possible non-zero values that M_k can take on are only two. Conversely, when $k = 8$ the determinant spectrum [11] includes more than two values which depend on a specific integer p. Hence, a different approach must be followed for H_{n-k} when $n > 16$ and $k = 8$. The next proposition illustrates this approach and its proof is based on elementary number theory.

Proposition 3. *An Hadamard matrix of order $n - 8$ cannot be embedded in an Hadamard matrix of order n for any $n = 4t$ with integer $t > 4$.*

$$H_{n-8} \notin H_n, \quad n > 16 \tag{14}$$

Proof. For $t = 1, 2$ no matrix H_{n-8} can be determined and an integer $t > 2$ will be considered in the following.

Assuming that an Hadamard matrix of order $n - 8$ can be embedded in an Hadamard matrix of order n, the relation (5) for $d = 8$ implies that

$$|\det H_{n-8}| = n^{\frac{n}{2}-8} M_8 \tag{15}$$

where M_8 is the absolute value of a 8×8 minor of H_n. Moreover, it is known that

$$|\det H_{n-8}| = (n-8)^{\frac{n-8}{2}} \tag{16}$$

and, according to (6), $M_8 = p \cdot 2^7$, where p is a positive integer. For the 8×8 case it has been confirmed that the possible existing values for the integer p are $1, 2, \ldots, 18, 20, 24$, and 32 [11].

Combining (15) and (16), it follows that:

$$(n-8)^{\frac{n-8}{2}} = n^{\frac{n}{2}-8}\, p\, 2^7 \quad \overset{n=4t,\, t>2}{\Longleftrightarrow} \quad p = 2\, t^4 \left(\frac{t-2}{t}\right)^{2(t-2)} \tag{17}$$

The above equation (17) is satisfied by the pairs of values $(t, p) = (3, 18)$ and $(t, p) = (4, 32)$ which correspond to the valid cases of $H_4 \in H_{12}$ and $H_8 \in H_{16}$, respectively. However, *for integers $t > 4$ the term p in (17) cannot be an integer*. A proof of this statement based on elementary number theory is presented below.

Assuming that p is an integer for any integer $t > 4$, the equation (17) is written equivalently in the form of an equality between two integers:

$$p\, t^{2t} = 2\, t^8 (t-2)^{2(t-2)} \tag{18}$$

The next two cases are considered:

i) *$t = 2^m$ for integer $m \geq 3$*

The prime factorization of the left-hand side of (18) shows that the least power of two is 2^{2mt}, whereas the prime factorization of the right-hand side of (18) shows that the least power of two is exactly $2^{1+8m+2t-4}$. Therefore, considering that p might also be a power of two, it follows that:

$$2mt \leq 8m + 2t - 3 \quad \Leftrightarrow \quad t \leq 4 + \frac{5}{2(m-1)}$$

The above inequality implies that $t \leq 5$ which contradicts the hypothesis for the integer t in this case, i.e. $t \geq 2^3 = 8$.

ii) *t is divisible by a prime integer $r \geq 3$*

If $m \geq 1$ is an integer such that r^m is the maximum power of r that divides t, then the prime factorization of the left-hand side of (18) shows that the least power of r is r^{2mt}, whereas the prime factorization of the right-hand side of (18) shows that the least power of r is exactly r^{8m}. Considering again that p might also be a power of r, it follows that:

$$2mt \leq 8m \quad \Leftrightarrow \quad t \leq 4$$

The above inequality contradicts the general hypothesis for the integer t, i.e. $t > 4$.

Unauthenticated
Download Date | 5/15/18 4:44 AM

Consequently, there is no integer $t > 4$ which can give a valid p for the minor M_8. Therefore, the assumption that was made in the derivation of the equation (15) is invalid for any $n = 4t$ with integer $t > 4$ and as a result H_{n-8} cannot be embedded in H_n. □

Remark 1. The problem of the non-existence of integers p satisfying (17) can also be investigated using tools from calculus. Specifically, if p in (17) is regarded as a real function of t, then $p(t)$ is differentiable in the interval $(4, +\infty)$ with first derivative:

$$\frac{dp}{dt} = \frac{4\,t^7}{(t-2)^4}\left(\frac{t-2}{t}\right)^{2\,t}\left(t\ln\left(\frac{t-2}{t}\right)+4\right)$$

It can easily be proven that $\frac{dp}{dt} > 0$ for every $t > 4$, which implies that $p(t)$ is a strictly increasing function in the interval $(4, +\infty)$. As a result, for every $t > 4$, it holds

$$p(t) > p(4) \;\Leftrightarrow\; p > 32$$

which contradicts the fact that $p \le 32$ [11].

3 Embeddability of Hadamard matrices

In the proof of Proposition 3, the parameter p plays a key role in the study of the embedding properties of Hadamard matrices. Given a positive integer k, by the Hadamard conjecture the absolute value of the maximal determinant of a (± 1)-matrix of order k is always less than or equal to $k^{\frac{k}{2}}$ [8]. Therefore, for any minor M_k it holds:

$$\left.\begin{array}{l} M_k = p\,2^{k-1} \\ M_k \le k^{\frac{k}{2}} \end{array}\right\} \Leftrightarrow\; p\,2^{k-1} \le k^{\frac{k}{2}} \;\Leftrightarrow\; p \le 2\left(\frac{k}{4}\right)^{\frac{k}{2}} \tag{19}$$

If $\hat{p}$ is used to denote the maximum value of p, then (19) implies that

$$\hat{p} := \max(p) = 2\left(\frac{k}{4}\right)^{\frac{k}{2}} \overset{k=4r}{\Leftrightarrow} \hat{p} = 2\,r^{2r} \tag{20}$$

The relation (19) forms a necessary condition for the embeddability of Hadamard matrices. Hence, by studying the range of values that p can take, the results obtained from Propositions 2 and 3 can be generalized for an Hadamard matrix of order $n - k$.

3.1 Embeddability of Hadamard matrices of order $n - k$

Let $n = 4\,t$ and $k = 4\,r$ where $t,\ r$ are positive integers. Generally, $0 < k < n$ and thus, $0 < r < t$. The cases of $\{t > 2, r = 1\}$ and $\{t > 4, r = 2\}$ have been examined in Propositions 2 and 3. The case of $\{t > 2, r > 2\,;\ t > r\}$ will be considered in the following.

Assuming that an Hadamard matrix of order $n - k$ can be embedded in an Hadamard matrix of order n, the relation (5) for $d = k$ implies that

$$|\det H_{n-k}| = n^{\frac{n}{2}-k} M_k \tag{21}$$

Furthermore, it holds:

$$|\det H_{n-k}| = (n-k)^{\frac{n-k}{2}} \tag{22}$$

If we combine (6), (21) and (22), we get the next important algebraic relation which connects p, and consequently the spectrum of the determinant function, with the order of the matrix H_{n-k} :

$$p = 2\,t^{2r}\left(\frac{t-r}{t}\right)^{2(t-r)} \tag{23}$$

Unauthenticated
Download Date | 5/15/18 4:44 AM

If $t = 2r$, or equivalently $n = 2k$, the integer p attains its maximum value $\hat{p}$, thus $p = \hat{p}$. Then, $H_{n-k} = H_k \in H_{2k} = H_n$ which holds as mentioned in (3). Therefore, in the following, we shall examine the existence of positive integers t, r satisfying the inequalities:

$$p < \hat{p} \quad , \quad t > r \tag{24}$$

Let $\theta = \frac{r}{t}$. Since $t > r$, it follows that $0 < \theta < 1$ and $0 < 1 - \theta < 1$. Then,

$$p < \hat{p} \quad \Leftrightarrow \quad 2\,t^{2r}\left(1 - \frac{r}{t}\right)^{2t\left(1-\frac{r}{t}\right)} < 2\,r^{2r} \quad \Leftrightarrow$$

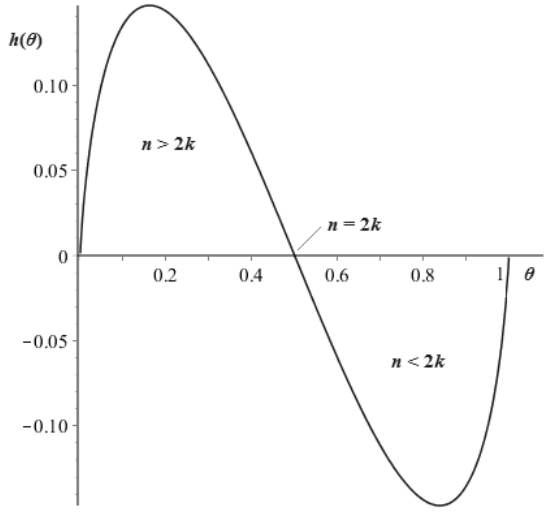
$$(1-\theta)\ln(1-\theta) - \theta\ln\theta < 0 \tag{25}$$

Now, for every $\theta \in (0, 1)$ we consider the real function:

$$h(\theta) = (1-\theta)\ln(1-\theta) - \theta\ln\theta \tag{26}$$

Using calculus, it can be proven that $h(\theta) \geq 0$, if $\theta \in \left(0, \frac{1}{2}\right]$, and $h(\theta) < 0$, if $\theta \in \left(\frac{1}{2}, 1\right)$. The graph of the function $h(\theta)$ is illustrated in Figure 1.

Figure 1: Graph of the function $h(\theta) = (1-\theta)\ln(1-\theta) - \theta\ln\theta$



Studying the sign of the function $h(\theta)$, where $\theta = \frac{r}{t} = \frac{k}{n} \in (0, 1)$, provides important information about the behavior of p for the various values of the integers n and k when $n > k$.

3.2 Main results on the embeddability – extendability of Hadamard matrices

The preceding analysis provides conclusive results on the embedding problem of Hadamard matrices H_{n-k} which form the next theorem.

Theorem 1. *An Hadamard matrix of order $n - k$ cannot be embedded in an Hadamard matrix of order n for any positive integers n and k multiples of 4 when $k < \frac{n}{2}$. That is*

$$H_{n-k} \notin H_n, \quad 4 \leq k < \frac{n}{2} \tag{27}$$

Proof. If $n > 2k$, then $t > 2r$ and $\theta < \frac{1}{2}$. Consequently, it is $h(\theta) > 0$, which implies that the inequality (25) cannot be satisfied by the specific values of θ. Therefore, for $n > 2k$ there are no integers p satisfying

Unauthenticated
Download Date | 5/15/18 4:44 AM

the conditions (24) and the equation (21), which supports the embedding property of the matrix H_{n-k}, is not valid. □

However, the sign analysis of the function $h(\theta)$ also reveals that for $n \le 2k < 2n$ there are positive integers p which satisfy $p \le \hat{p}$.

If $n = 2k$, then $h(\theta) = 0 \Leftrightarrow p = \hat{p}$. This is the case of $H_k \in H_{2k}$ which is true according to (3). Conversely, if $n < 2k < 2n$, there are values of p such that $p < \hat{p}$. Considering (23) for $t = \frac{n}{4}$ and $r = \frac{k}{4}$, the discrete function

$$\mathcal{P}(n,k) = 2\left(\frac{n}{4}\right)^{\frac{k}{2}}\left(\frac{n-k}{n}\right)^{\frac{n-k}{2}} \text{ for } \frac{n}{2} \le k < n \text{ and } \begin{cases} n = 8, 12, 16, \dots \\ k = 4, 8, 12, \dots \end{cases} \tag{28}$$

provides values for the parameter p which satisfy (21), expressed as

$$|\det H_{n-k}| = 2^{(n-k)-1}\left(\frac{n}{4}\right)^{\frac{n}{2}-k} p \tag{29}$$

The above results form the basis to pose the following conjecture.

Conjecture 1. Consider a Hadamard matrix H_n. If $H_n^{(k)}$ is a $k \times k$ submatrix of H_n, where $n \ge 8$ and $k \ge 4$ are integers multiples of 4 such that $\frac{n}{2} \le k < n$, and $|\det H_n^{(k)}| = p\, 2^{k-1}$ with $p = \mathcal{P}(n,k)$, then an Hadamard matrix of order $n-k$ may exist embedded in the Hadamard matrix of order n, i.e.,

$$H_{n-k} \in H_n, \quad 4 \le \frac{n}{2} \le k < n \tag{30}$$

3.3 Connection of p with the available determinant spectrum and verification of the results

Both results (27) and (30) reveal a characteristic embedding and extension pattern for Hadamard matrices and their proof is based on the properties of the minors of Hadamard matrices. The key element in this study is the range of the values of the parameter p. Theorem 1 provides conclusive results for every $p > \hat{p}$. Conversely, (30) holds for specific values of p which can be obtained from (28).

For a fixed order $n \ge 8$, the relation (30) holds for every $k = \frac{n}{2}$ and $k = n-4$, since they are linked to the already known cases $H_n \in H_{2n}$ and $H_4 \in H_n$, respectively. Furthermore, for $4 \le k \le 16$ the computed values of $p = \mathcal{P}(n,k)$ are already included in the available and confirmed spectrum for $k = 4, 8$, and in the conjectured spectrum for $k = 12, 16$ given by Orrick and Solomon in [11].

We also examined some cases where $k > \frac{n}{2}$ using the Hadamard matrices of order 20, 24, and 28 (Paley-type) given by Sloane in [14][1]. The following results, obtained by using Matlab and a quad-core AMD-A10/8Gb-Ram machine, verify Conjecture 1 for $n = 20, 24, 28$ and $k = 12, 16, 20$.

i) $n = 20$, $k = 12$, and $p = \mathcal{P}(20, 12) = 800$

There exists a 12×12 submatrix $H_{20}^{(12)} = [a_{ij}]$ of H_{20} where

$$i \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 14, 20\},$$
$$j \in \{1, 2, 3, 4, 7, 8, 13, 14, 17, 18, 19, 20\}$$

such that

$$|\det H_{20}^{(12)}| = 800 \cdot 2^{11} = 1638400$$

The above result implies that H_8 may exist embedded in H_{20}. We can confirm that there is an 8×8 submatrix $A = [a_{ij}]$ of H_{20} where

$$i \in \{1, 2, 3, 4, 5, 6, 9, 12\},$$

1 had.20.pal, had.24.pal, had.28.pal2

Unauthenticated
Download Date | 5/15/18 4:44 AM

$$j \in \{1, 2, 3, 4, 8, 14, 15, 18\}$$

which satisfies (1) and (29). That is

$$A A^\top = A^\top A = 8 I \text{ and}$$
$$|\det A| = 2^{(20-12)-1} \cdot \left(\frac{20}{4}\right)^{\frac{20}{2}-12} \cdot 800 = 4096 = |\det H_8|$$

ii) $n = 24$, $k = 16$, and $p = \mathcal{P}(24, 16) = 41472$

There exists a 16×16 submatrix $H_{24}^{(16)} = [a_{ij}]$ of H_{24} where

$$i \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 15, 18, 22, 23\},$$
$$j \in \{1, 3, 6, 7, 9, 10, 12, 13, 14, 15, 16, 18, 19, 21, 23, 24\}$$

such that

$$|\det H_{24}^{(16)}| = 41472 \cdot 2^{15} = 1358954496$$

The above result implies that H_8 may exist embedded in H_{24}. We can confirm that there is an 8×8 submatrix $A = [a_{ij}]$ of H_{24} where

$$i \in \{1, 2, 3, 4, 5, 6, 12, 21\},$$
$$j \in \{2, 5, 7, 10, 11, 17, 18, 19\}$$

which satisfies (1) and (29). That is

$$A A^\top = A^\top A = 8 I \text{ and}$$
$$|\det A| = 2^{(24-16)-1} \cdot \left(\frac{24}{4}\right)^{\frac{24}{2}-16} \cdot 41472 = 4096 = |\det H_8|$$

iii) $n = 28$, $k = 20$, and $p = \mathcal{P}(28, 20) = 3764768$

There exists a 20×20 submatrix $H_{28}^{(20)} = [a_{ij}]$ of H_{28} where

$$i \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 19, 23, 27\},$$
$$j \in \{1, 2, 3, 4, 5, 7, 9, 11, 13, 14, 15, 16, 17, 19, 20, 22, 23, 24, 26, 27\}$$

such that

$$|\det H_{28}^{(20)}| = 3764768 \cdot 2^{19} = 1973822685184$$

The above result implies that H_8 may exist embedded in H_{28}. We can confirm that there is an 8×8 submatrix $A = [a_{ij}]$ of H_{28} where

$$i \in \{1, 2, 3, 4, 5, 6, 16, 17\},$$
$$j \in \{4, 6, 9, 14, 15, 19, 21, 26\}$$

which satisfies (1) and (29). That is

$$A A^\top = A^\top A = 8 I \text{ and}$$
$$|\det A| = 2^{(28-20)-1} \cdot \left(\frac{28}{4}\right)^{\frac{28}{2}-20} \cdot 3764768 = 4096 = |\det H_8|$$

Unauthenticated
Download Date | 5/15/18 4:44 AM

iv) $n = 28$, $k = 16$, and $p = \mathcal{P}(28, 16) = 71442$

There exists a 16×16 submatrix $H_{28}^{(16)} = [a_{ij}]$ of H_{28} where

$$i \in \{1, 2, 3, 4, 6, 8, 9, 11, 15, 16, 17, 18, 20, 22, 23, 25\},$$
$$j \in \{1, 2, 3, 4, 6, 8, 9, 11, 15, 16, 17, 18, 20, 22, 23, 25\}$$

such that

$$|\det H_{28}^{(16)}| = 71442 \cdot 2^{15} = 2341011456$$

The above result implies that H_{12} may exist embedded in H_{28}. We can confirm that there is a 12×12 submatrix $A = [a_{ij}]$ of H_{28} where

$$i \in \{1, 2, 3, 4, 8, 11, 15, 16, 17, 18, 22, 25\},$$
$$j \in \{1, 2, 3, 4, 8, 11, 15, 16, 17, 18, 22, 25\}$$

which satisfies (1) and (29). That is

$$A A^\top = A^\top A = 12 I \text{ and}$$
$$|\det A| = 2^{(28-16)-1} \cdot \left(\frac{28}{4}\right)^{\frac{28}{2}-16} \cdot 71442 = 2985984 = |\det H_{12}|$$

The aforementioned submatrices are not unique. There are several different row and column arrangements (i, j) which also satisfy the conditions for (30) to hold. In Table 2, we summarize the confirmed results obtained from (27) and (30) for $n = 8, 12, \ldots, 28$ and $k = 4, 8, \ldots, 24$.

Table 2: Embeddability of Hadamard matrices H_{n-k} for $4 \le k \le 24$ and $8 \le n \le 28$.

Order	$k = 4$	$k = 8$	$k = 12$	$k = 16$	$k = 20$	$k = 24$
$n = 8$	$H_4 \in H_8$					
$n = 12$	$H_8 \notin H_{12}$	$H_4 \in H_{12}$				
$n = 16$	$H_{12} \notin H_{16}$	$H_8 \in H_{16}$	$H_4 \in H_{16}$			
$n = 20$	$H_{16} \notin H_{20}$	$H_{12} \notin H_{20}$	$H_8 \in H_{20}$	$H_4 \in H_{20}$		
$n = 24$	$H_{20} \notin H_{24}$	$H_{16} \notin H_{24}$	$H_{12} \in H_{24}$	$H_8 \in H_{24}$	$H_4 \in H_{24}$	
$n = 28$	$H_{24} \notin H_{28}$	$H_{20} \notin H_{28}$	$H_{16} \notin H_{28}$	$H_{12} \in H_{28}$	$H_8 \in H_{28}$	$H_4 \in H_{28}$

4 Conclusions

In this paper, we investigated the conditions under which Hadamard matrices of order $n - k$ can exist embedded in other Hadamard matrices of order n. The same problem can be seen as an extension problem from order n to order $n + k$. We considered the problem when $k < \frac{n}{2}$ and $k \ge \frac{n}{2}$. In our study, we analyzed the embedding properties of Hadamard matrices via their minors and revisited the method of proving $H_{n-k} \notin H_n$ when $k < \frac{n}{2}$, which was originally presented in [3]. A systematic approach was followed to this problem, first by looking at the cases $H_{n-4} \notin H_n$ and $H_{n-8} \notin H_n$, and then considering the general case $H_{n-k} \notin H_n$ which is presented in Theorem 1. For their proof, we used tools from elementary number theory and calculus which also allowed us to study the problem further when $k \ge \frac{n}{2}$. The results obtained may reveal a characteristic

Unauthenticated
Download Date | 5/15/18 4:44 AM

embedding pattern for all Hadamard matrices. In particular, for $k = \frac{n}{2}$ it is known that $H_k \in H_{2k}$ and for $k > \frac{n}{2}$ it is inferred that if a Hadamard matrix of order n has a $k \times k$ submatrix with minor $p\, 2^{k-1}$ and the value of p is specifically given by (28), then a Hadamard matrix of order $n-k$ may exist embedded in the Hadamard matrix of order n. For orders $n \leq 28$ and $k \leq 16$ multiples of 4, we noticed that the values of p obtained from (28) also appear in the spectrum of the determinant function given in [11] and this partially verifies the conditions of Conjecture 1.

Acknowledgement: The authors would like to thank Prof. Emeritus A. Tsarpalias of the Dept. of Mathematics at the National and Kapodistrian University of Athens for his contribution in the proof of Proposition 3.

References

[1] T. Banica, I. Nechita, and M. M. Schlenker. Submatrices of Hadamard matrices: Complementation results. *Electron. J. Linear Algebra*, 27:197–212, 2014.
[2] R. P. Brent and J-A. H. Osborn. On minors of maximal determinant matrices. *J. Integer Seq.*, 16:1–30, 2013.
[3] J. H. E. Cohn. Hadamard matrices and some generalisations. *Amer. Math. Monthly*, 72(5):515–518, 1965.
[4] J. Day and B. Peterson. Growth in Gaussian elimination. *Amer. Math. Monthly*, 29(2):489–513, 1988.
[5] H. Evangelaras, C. Koukouvinos, and K. Mylona. On Hadamard embeddability. *J. Discrete Math. Sci. Cryptogr.*, 9(3):503–512, 2006.
[6] F. R. Gantmacher. *Applications of the Theory of Matrices*. Dover Publications, New York, 1959.
[7] A. V. Geramita and J. Seberry. Orthogonal designs: Quadratic forms and Hadamard matrices. volume 45 of *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, Inc. New York, 1979.
[8] J. Hadamard. Résolution d'une question relative aux déterminants. *Bull. Sci. Math.*, 17:240–246, 1893.
[9] K. J. Horadam. *Hadamard Matrices and Their Applications*. Princeton University Press, Princeton, NJ, 2007.
[10] H. Kharaghani and B. Tayfeh-Rezaie. A Hadamard matrix of order 428. *J. Combin. Des.*, 13(6):435–440, 2005.
[11] W. P. Orrick and B. Solomon. Spectrum of the determinant function. http://www.indiana.edu/~maxdet/spectrum.html.
[12] J. Seberry and M. Mitrouli. Some remarks on Hadamard matrices. *Cryptogr. Commun.*, 2:187–198, 2010.
[13] J. Seberry, T. Xia, C. Koukouvinos, and M. Mitrouli. The maximal determinant and subdeterminants of ±1 matrices. *Linear Algebra Appl.*, 373:297–310, 2003.
[14] N. J. A. Sloane. A library of Hadamard matrices. http://neilsloane.com/hadamard/index.html.
[15] J. J. Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tile work, and the theory of numbers. *Phil. Mag.*, 34(4):461–475, 1867.
[16] F. Szöllősi. Exotic complex Hadamard matrices and their equivalence. *Cryptogr. Commun.*, 2:187–198, 2010.
[17] K. Vijayan. Hadamard matrices and submatrices. *J. Aust. Math. Soc.*, 22:469–475, 1976.

Unauthenticated
Download Date | 5/15/18 4:44 AM