FURTHER INSIGHTS INTO THE EMBEDDING PROPERTIES OF HADAMARD MATRICES

Dimitrios Christou
Department of Science and Mathematics
Deree – The American College of Greece

Marilena Mitrouli
Department of Mathematics
National and Kapodistrian University of Athens

July 2 – 6, 2018

3rd Conference on Numerical Analysis and Scientific Computation with Applications
NASCA 2018
Further insights into the embedding properties of Hadamard matrices

Topics:

- Hadamard matrices – Basic properties and applications
- Embedded properties of Hadamard matrices and existence of Hadamard submatrices.

Research Problem:

When can an Hadamard matrix of order \( n - k \) be embedded in a Hadamard matrix of order \( n \)?

What are the characteristics of such an embedding property?

- Conclusions
Hadamard matrices

Hadamard was interested in finding the maximal determinant of square matrices with entries from the unit disc.

He showed (Bull. Sciences Math. 1893) that this maximal determinant, $n^{n/2}$, was achieved by matrices $X = [x_{ij}]_{n \times n}$ with entries $\pm 1$ which satisfied the equality of the inequality:

$$| \det X |^2 \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |x_{ij}|^2$$

or

$$XX^T = I_n$$

Jacques Salomon Hadamard
1865 – 1963
Hadamard matrices

A square matrix with elements ±1 and size $n$, whose distinct row vectors are orthogonal is an

**Hadamard matrix of order $n$.**

\[
H_1, \quad \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}
\]

**Basic properties:**

a) $HH^T = nI_n$

b) $|\det H| = n^{n/2}$

c) $HH^T = H^TH$
The Hadamard conjecture

Furthermore, Hadamard observed that such matrices could exist only if \( n \) was 1, 2, or a multiple of 4.

This observation has formed the basis of one of the greatest unsolved mathematical problems.

**The Hadamard Conjecture**

*There is a Hadamard matrix of order \( n \) for any natural number \( n \) multiple of 4.*

Jacques Salomon Hadamard
1865 – 1963

Despite the efforts of several mathematicians, Hadamard’s observation remains unproven, even though it is widely believed that it is true.
Sylvester-Hadamard matrices

However, such matrices were first studied by Sylvester *(Phil. Mag. 1867)* who observed that if $H$ is an Hadamard matrix, then

\[
\begin{bmatrix}
H & H \\
H & -H
\end{bmatrix}
\]

is also an Hadamard matrix.

The matrices of order $2^t$ constructed using Sylvester’s construction are usually referred to as *Sylvester-Hadamard* matrices.

**Lemma (Sylvester 1867)**

There is an Hadamard matrix of order $2^t$ for all natural numbers $t$. 

James Joseph Sylvester

1814 – 1897
Visualization of Sylvester-Hadamard matrices

\[ H_n = H_1 \otimes H_{n-1}, \quad n = 2, 3, ... \]

■ = 1
☐ = -1
Hadamard’s matrices

Sylvester's construction (1867) yields Hadamard matrices of order 1, 2, 4, 8, 16, 32, etc. Hadamard matrices of orders 12 and 20 were subsequently constructed by Hadamard in 1893.

- **White square** = 1
- **Orange square** = –1
Construction of Hadamard matrices

Different *construction techniques* of Hadamard matrices have been developed for a wide variety of applications:

- **Sylvester’s** technique (1867)
- **Paley’s** technique (1933)
- **Williamson’s** technique (1944)
- **Ahmed & Rao’s** technique (1975)
- **Henderson’s** technique (1978)
- **Golay’s** technique (1982)
- **Lee & Kaveh’s** technique (1986)
- ...and others

428 × 428 Hadamard matrix
H. Kharaghani and B. Tayfeh-Rezaie, 2005
Construction of Hadamard matrices

Facts for Hadamard matrices:

✓ In 2005, Hadi Kharaghani and Behruz Tayfeh-Rezaie published their construction of an Hadamard matrix of order 428. As a result, the smallest order for which no Hadamard matrix is presently known is 668.

✓ As of 2008, there are 12 multiples of 4 less than or equal to 2000 for which no Hadamard matrix of that order is known. They are: 668, 716, 892, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, and 1964.

✓ For any order $n$, $H_4 \in H_n$ and $H_n \in H_{2n}$
Applications of Hadamard matrices

- **Signal processing, Coding and Cryptography**
  - Design of experiments
  - Object recognition
  - Coding of digital signals (CDMA telecommunications)

- **Spectral analysis or signal separation**
  - Mass spectroscopy
  - Polymer chemistry
  - Signal and information processing
  - Geophysics
  - Acoustics
  - Nuclear medicine and nuclear physics

- **Other novel applications**
  Digital logic design, pattern recognition, data compression, magnetic resonance imaging, neuroscience and quantum computing
Embedded Hadamard matrices
Problem motivation

Problem 1:

Can an Hadamard matrix of order \( n - 4 \) or \( n - 8 \) exist embedded in an Hadamard matrix of order \( n \), for \( n = 4t \) with integer \( t > 2 \)?

\[
H_8 \in H_{12}, \quad H_{12} \in H_{16}, \quad H_{16} \in H_{20}, \quad \ldots, \quad H_{n-4} \in H_n
\]

\[
H_{12} \in H_{20}, \quad H_{16} \in H_{24}, \quad H_{20} \in H_{28}, \quad \ldots, \quad H_{n-8} \in H_n
\]

Problem 2 (Generalization)

Can an Hadamard matrix of order \( n - k \) exist embedded in an Hadamard matrix of order \( n \), for \( n = 4t \) and \( k = 4r \) with \( 0 < 2r < t \)?

What are the characteristics of such an embedding property?
Embedded Hadamard matrices

**Theorem (Cohn, 1965)**

If an $H_{n+m}$ exists and $n > m$, then no $n$-rowed minor is an $H_n$.

**Example:** $n = 20$ and $m = 8$, then $H_{20}$ is not embedded in $H_{28}$

**Theorem (Brent & Osborn, 2013)**

Let $H_n$ be an Hadamard matrix of order $n$ having a Hadamard submatrix $M$ of order $m < n$. Then, $m \leq \frac{n}{2}$.

**Example:** $n = 20$ and $m = 8$, then $H_8$ is embedded in $H_{20}$
Minors of Hadamard matrices

The current approach is based on the analysis of the result derived from the next proposition by simply using calculus techniques.

**Proposition** (F. Szöllösi, 2010)

Let $M_d$ the absolute value of a $d \times d$ minor of the Hadamard matrix $H_n$ of order $n$,

$$M_d = \left| \det H_{d,n} \right|$$

where $H_{d,n}$ denotes the $d \times d$ submatrix of $H_n$.

Then, there is a one-to-one correspondence between the minors of size $d$ and $n-d$ described by the equation:

$$M_{n-d} = n^{n-d} M_d$$
We investigate the existence of a Hadamard matrix of order $n - k$ embedded in an Hadamard matrix of order $n$ considering the following relation:

$$\left| \det H_{n-k} \right| = n^{2-k} M_k$$

**Lemma (Day & Peterson, 1988)**

Let $B$ be an $n \times n$ matrix with elements $\pm 1$.

It holds that:

a) $\det B$ is an integer and $2^{n-1}$ divides $\det B$

b) when $n \leq 6$, the only possible values for $\det B$ are the following, and they do all occur:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\det B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0, 2</td>
</tr>
<tr>
<td>3</td>
<td>0, 4</td>
</tr>
<tr>
<td>4</td>
<td>0, 8, 16</td>
</tr>
<tr>
<td>5</td>
<td>0, 16, 32, 48</td>
</tr>
<tr>
<td>6</td>
<td>0, 32, 64, 96, 128, 160</td>
</tr>
</tbody>
</table>

$$\det B = p \ 2^{n-1}$$
Minors of Hadamard matrices

Definition

The *spectrum of the determinant function* for \((\pm 1)-\)matrices is defined to be the set of values \(p\) taken by \(|\text{det } R_k| = p \cdot 2^{k-1}\) as the matrix \(R_k\) ranges over all \(k \times k\) \((\pm 1)-\)matrices.

W. Orrick and B. Solomon give a list of values for \(p\) in

http://www.indiana.edu/~maxdet/spectrum.html

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.
When is $H_{n-k}$ embedded in $H_n$?

Given a positive integer $k$, it is known that $M_k \leq k^2$ and $M_k = p 2^{k-1}$.

Therefore, if $k = 4r$, where $r > 0$, the maximum value of the integer $p$, denoted by $\hat{p}$ is given by

$$\hat{p} = 2 \left( \frac{k}{4} \right)^{\frac{k}{2}}$$

For $n = 4t$, $k = 4r$ for integers $r > 0$ and $t > r$ it holds:

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

A necessary condition for the general embedding problem is the following:

$$p \leq \hat{p}$$
When is $H_{n-k}$ embedded in $H_n$?

Let $\theta = \frac{k}{n}$. Since $n > k$, then $0 < \theta < 1$ and $0 < 1 - \theta < 1$.

Using Calculus

\[ p \leq \hat{p} \iff (1 - \theta) \ln(1 - \theta) - \theta \ln \theta \leq 0 \]

Studying the sign of the real function

\[ h(\theta) = (1 - \theta) \ln(1 - \theta) - \theta \ln \theta \]

provides very important information about the behavior of $p$ for the various values of the integers $n$ and $k$ when $n > k$. 
When is $H_{n-k}$ embedded in $H_n$?

$$h(\theta) = (1-\theta)\ln(1-\theta) - \theta\ln\theta$$

- $n > 2k \iff h(\theta) > 0 \iff p > \hat{p}$
  $$H_{n-k} \not\subseteq H_n$$

- $n = 2k \iff h(\theta) = 0 \iff p = \hat{p}$
  $$H_k \subseteq H_{2k}$$

- $n < 2k \iff h(\theta) < 0 \iff p < \hat{p}$
  $$H_{n-k} \subseteq H_n$$

But for what values of $p$ is this true?
When is $H_{n-k}$ embedded in $H_n$?

**Proposition:**

The discrete function

$$\mathcal{P}(n, k) = 2 \left( \frac{n}{4} \right)^{\frac{k}{2}} \left( \frac{n-k}{n} \right)^{\frac{n-k}{2}}$$

for $\frac{n}{2} \leq k < n$ and

$$\begin{cases} n = 8, 12, 16, \ldots \\ k = 4, 8, 12, \ldots \end{cases}$$

provides the values for the parameter $p$ which satisfies the equations:

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

or

$$|\det H_{n-k}| = 2^{(n-k)-1} \left( \frac{n}{4} \right)^{\frac{n}{2} - k} p$$
**When is** $H_{n-k}$ **embedded in** $H_n$?

<table>
<thead>
<tr>
<th>$n$</th>
<th>$k$</th>
<th>Spectrum for order $k$</th>
<th>$H_{n-k} \in H_n$ ($n \leq 2k$)</th>
<th>Values of $p$</th>
<th>Status of $p$ in the spectrum*</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>4</td>
<td>Available</td>
<td>$H_4 \in H_8$</td>
<td>2</td>
<td>Included</td>
</tr>
<tr>
<td>12</td>
<td>8</td>
<td>Available</td>
<td>$H_4 \in H_{12}$</td>
<td>18</td>
<td>Included</td>
</tr>
<tr>
<td>16</td>
<td>8</td>
<td>Available</td>
<td>$H_8 \in H_{16}$</td>
<td>32</td>
<td>Included</td>
</tr>
<tr>
<td>16</td>
<td>12</td>
<td>Conjectured</td>
<td>$H_4 \in H_{16}$</td>
<td>512</td>
<td>Included</td>
</tr>
<tr>
<td>20</td>
<td>12</td>
<td>Conjectured</td>
<td>$H_8 \in H_{20}$</td>
<td>800</td>
<td>Included</td>
</tr>
<tr>
<td>24</td>
<td>12</td>
<td>Conjectured</td>
<td>$H_{12} \in H_{24}$</td>
<td>1458</td>
<td>Included</td>
</tr>
<tr>
<td>20</td>
<td>16</td>
<td>Conjectured</td>
<td>$H_4 \in H_{20}$</td>
<td>31250</td>
<td>Included</td>
</tr>
<tr>
<td>24</td>
<td>16</td>
<td>Conjectured</td>
<td>$H_8 \in H_{24}$</td>
<td>41472</td>
<td>Included</td>
</tr>
<tr>
<td>28</td>
<td>16</td>
<td>Conjectured</td>
<td>$H_{12} \in H_{28}$</td>
<td>71442</td>
<td>Included</td>
</tr>
<tr>
<td>32</td>
<td>16</td>
<td>Conjectured</td>
<td>$H_{16} \in H_{32}$</td>
<td>131072</td>
<td>Included</td>
</tr>
<tr>
<td>24</td>
<td>20</td>
<td>Unavailable</td>
<td>$H_4 \in H_{24}$</td>
<td>3359232</td>
<td>Must exist</td>
</tr>
<tr>
<td>28</td>
<td>20</td>
<td>Unavailable</td>
<td>$H_8 \in H_{28}$</td>
<td>3764768</td>
<td>Must exist</td>
</tr>
<tr>
<td>32</td>
<td>20</td>
<td>Unavailable</td>
<td>$H_{12} \in H_{32}$</td>
<td>5971968</td>
<td>Must exist</td>
</tr>
<tr>
<td>36</td>
<td>20</td>
<td>Unavailable</td>
<td>$H_{16} \in H_{36}$</td>
<td>10616832</td>
<td>Must exist</td>
</tr>
<tr>
<td>40</td>
<td>20</td>
<td>Unavailable</td>
<td>$H_{20} \in H_{40}$</td>
<td>19531250</td>
<td>Must exist</td>
</tr>
</tbody>
</table>

\[
p = 2 \left( \frac{n}{4} \right)^{\frac{k}{2}} \left( \frac{n-k}{n} \right)^{\frac{n-k}{2}}
\]

\[
h(\theta) = (1-\theta) \ln(1-\theta) - \theta \ln \theta
\]

* W. P. Orrick, B. Solomon, Spectrum of the determinant function, 2010
Conclusions

**Theorem:** 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

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

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

$$H_{n-k} \in H_n, \quad 4 \leq \frac{n}{2} \leq k < n$$
Conclusions

Embeddability of Hadamard matrices $H_{n-k}$ for $4 \leq k \leq 24$ and $8 \leq n \leq 28$.

<table>
<thead>
<tr>
<th>Order</th>
<th>k = 4</th>
<th>k = 8</th>
<th>k = 12</th>
<th>k = 16</th>
<th>k = 20</th>
<th>k = 24</th>
</tr>
</thead>
<tbody>
<tr>
<td>n = 8</td>
<td>$H_4 \in H_8$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n = 12</td>
<td>$H_8 \notin H_{12}$</td>
<td>$H_4 \in H_{12}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n = 16</td>
<td>$H_{12} \notin H_{16}$</td>
<td>$H_8 \in H_{16}$</td>
<td>$H_4 \in H_{16}$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n = 20</td>
<td>$H_{16} \notin H_{20}$</td>
<td>$H_{12} \notin H_{20}$</td>
<td>$H_8 \in H_{20}$</td>
<td>$H_4 \in H_{20}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>n = 24</td>
<td>$H_{20} \notin H_{24}$</td>
<td>$H_{16} \notin H_{24}$</td>
<td>$H_{12} \in H_{24}$</td>
<td>$H_8 \in H_{24}$</td>
<td>$H_4 \in H_{24}$</td>
<td></td>
</tr>
<tr>
<td>n = 28</td>
<td>$H_{24} \notin H_{28}$</td>
<td>$H_{20} \notin H_{28}$</td>
<td>$H_{16} \notin H_{28}$</td>
<td>$H_{12} \in H_{28}$</td>
<td>$H_8 \in H_{28}$</td>
<td>$H_4 \in H_{28}$</td>
</tr>
</tbody>
</table>

All the above results have been verified using search algorithms implemented in MAPLE.
Example 1: $H_8 \in H_{28}$

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

$H_{28}$ (2nd Paley type)

**Argument:** If $p = 3764768$ exists in the spectrum, meaning that $H_{28}$ has a $20 \times 20$ submatrix with minor:

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

then it may $H_8$ exist embedded in $H_{28}$.

$\square = 1$
$\blacksquare = -1$

Example 1: $H_8 \in H_{28}$

$H_{28}^{(20)}$ submatrix of $H_{28}$

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

$H_{28}^{(20)} = [a_{ij}]$ of $H_{28}$ where

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

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

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

$H_8 \in H_{28}$

$A = [a_{ij}]$ of $H_{28}$ where

$i \in \{1, 2, 3, 4, 5, 6, 16, 17\}$,

$j \in \{4, 6, 9, 14, 15, 19, 21, 26\}$

$|\det A| = 2^{(28-20)-1} \cdot \left(\frac{28}{4}\right)^{\frac{28}{2}-20} \cdot 3764768 = 4096 = |\det H_8|$
Example 2: $H_{12} \in H_{28}$

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

$H_{28}$ (2nd Paley type)

**Argument:** If $p = 71442$ exists in the spectrum, meaning that $H_{28}$ has a $16 \times 16$ submatrix with minor:

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

then it may $H_{12}$ exist embedded in $H_{28}$.

\[ \square = 1 \]
\[ \blacksquare = -1 \]

Example 2: $H_{12} \in H_{28}$

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

$H_{28}^{(16)} = [a_{ij}]$ of $H_{28}$ where

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

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

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

$H_{12} \in H_{28}$

$A = [a_{ij}]$ of $H_{28}$ where $i \in \{1, 2, 3, 4, 8, 11, 15, 16, 17, 18, 22, 25\}$,

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

$|\det A| = 2^{(28-16)-1} \cdot \left(\frac{28}{4}\right)^{28-16} \cdot 71442 = 2985984 = |\det H_{12}|$
Prof. Marilena Mitrouli
Department of Mathematics
National and Kapodistrian University of Athens

Prof. Emer. Jennifer Seberry
School of Computing and Information Technology
University of Wollongong

Dr. Dimitris Christou
Department of Science and Mathematics
Deree – The American College of Greece

D. Christou, M. Mitrouli, and J. Seberry,
Embedding and Extension Properties of Hadamard Matrices Revisited
References


Thank you for your attention