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 ± 1 which satisfied the equality of the inequality:

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

or $X X^{\mathsf{T}} = I_n$

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***.

$n = 1$	$n = 2$	$n = 4$
H_1	H_2	H_4
$[1]$,	$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$,	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

Jacques Salomon Hadamard
1865 – 1963

Basic properties:

a) $\boldsymbol{H H^{\mathsf{T}} = n I_n}$ b) $\boldsymbol{|\det H| = n^{n/2}}$ c) $\boldsymbol{H H^{\mathsf{T}} = H^{\mathsf{T}} H}$

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.

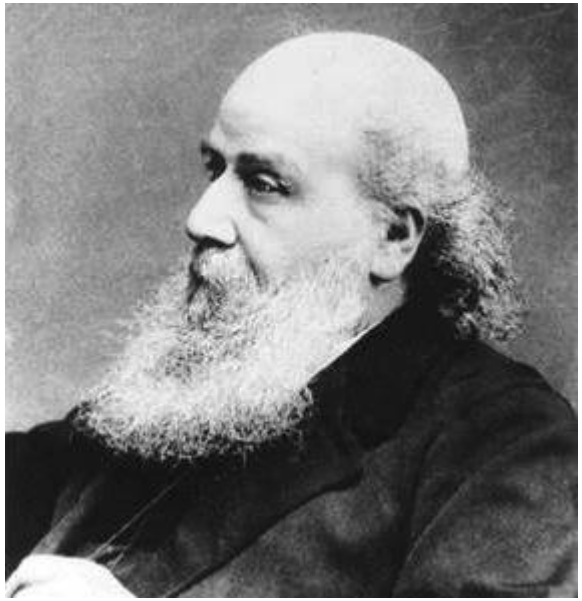
Sylvester-Hadamard matrices

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 $\mathbf{2^t}$ constructed using Sylvester's construction are usually referred to as ***Sylvester-Hadamard*** matrices.

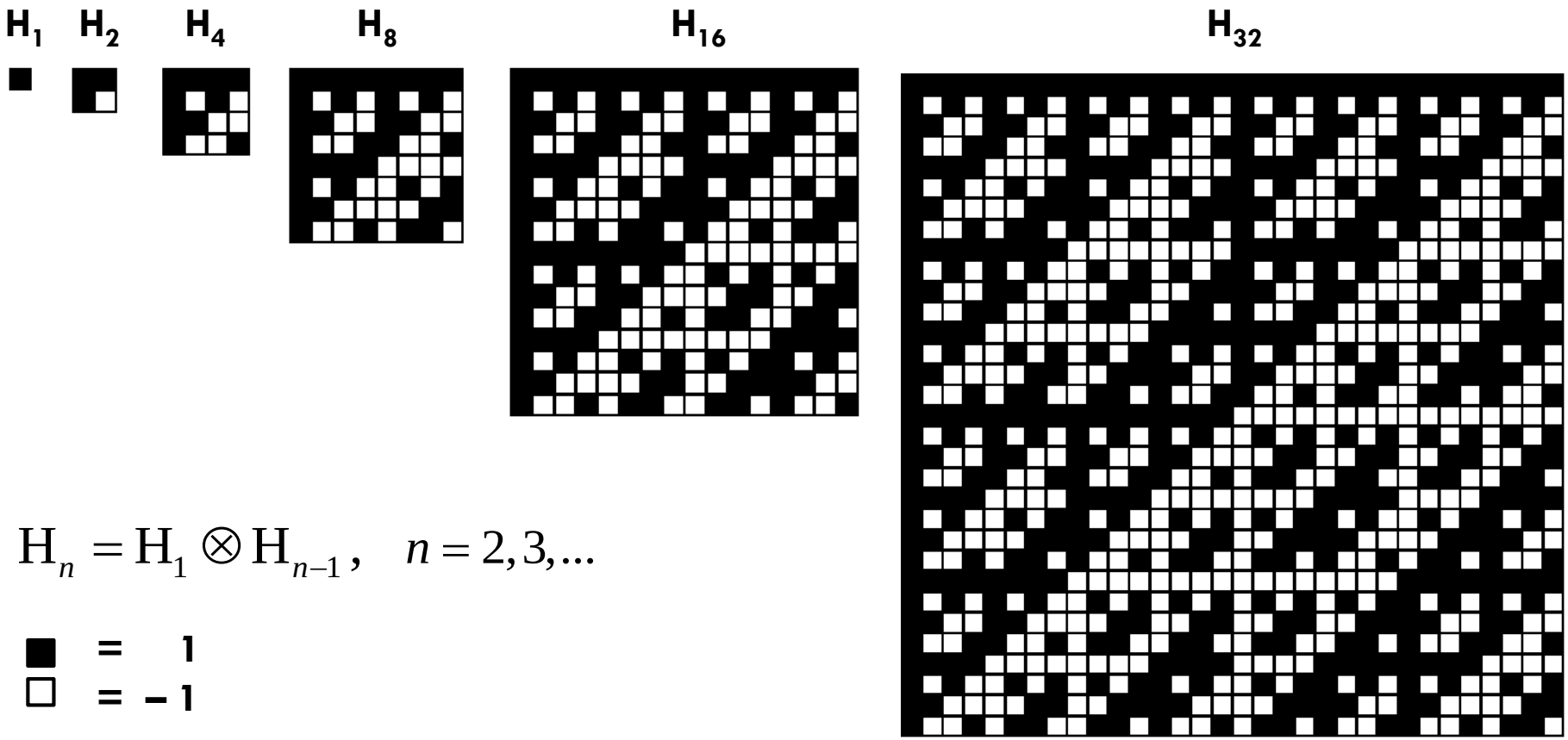


James Joseph Sylvester
1814 – 1897

***Lemma* (*Sylvester* 1867)**

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

Visualization of Sylvester-Hadamard matrices



$$\mathrm{H}_n = \mathrm{H}_1 \otimes \mathrm{H}_{n-1}, \quad n = 2, 3, \ldots$$

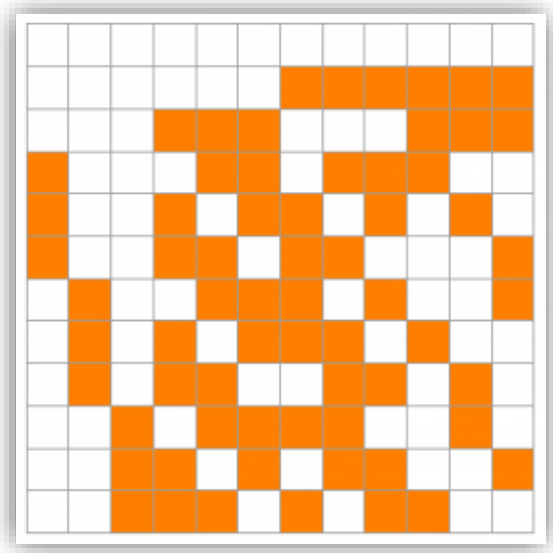
■ = 1

□ = −1

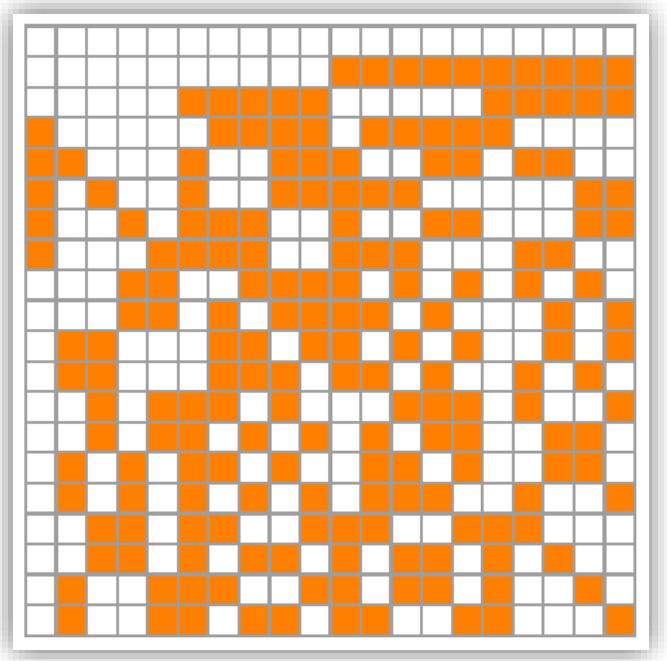
Hadamard's matrices

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.

12 × 12 Hadamard matrix



20 × 20 Hadamard matrix



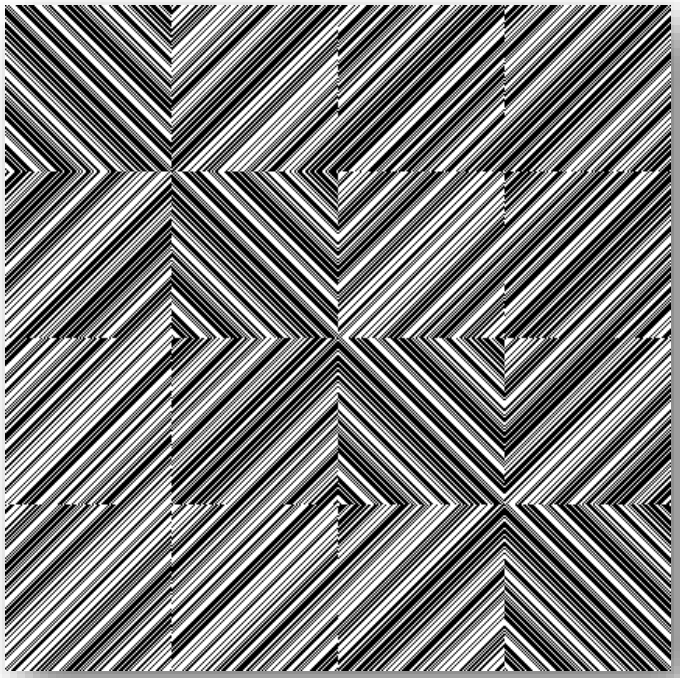
White square = 1
Orange square = –1

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, $\boldsymbol{H}_4 \in \boldsymbol{H}_n$ and $\boldsymbol{H}_n \in \boldsymbol{H}_{2n}$

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 $\boldsymbol{n-4}$ or $\boldsymbol{n-8}$ *exist embedded in an Hadamard matrix of order n, for* $\boldsymbol{n = 4t}$ *with integer* $\boldsymbol{t > 2}$ *?*

$$H_8 \in H_{12} \;,\; H_{12} \in H_{16} \;,\; H_{16} \in H_{20} \;,\ldots,\; H_{n-4} \in H_n$$

$$H_{12} \in H_{20} \;,\; H_{16} \in H_{24} \;,\; H_{20} \in H_{28} \;,\ldots,\; H_{n-8} \in H_n$$

?

Problem 2 (Generalization)

Can an Hadamard matrix of order $\boldsymbol{n-k}$ *exist embedded in an Hadamard matrix of order n, for* $\boldsymbol{n = 4t}$ and $\boldsymbol{k = 4r}$ with $\boldsymbol{0 < 2r < t}$ *?*

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* <u>*having a Hadamard submatrix M*</u> *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. Szöllòsi, 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:*

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

Minors of Hadamard matrices

We investigate the existence of a Hadamard matrix of order $n - k$ embedded in an Hadamard matrix of order n considering the following relation:

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

Lemma (*Day & Peterson*, 1988)

Let B be an $n \times n$ matrix with elements ± 1.
It holds that:

a) ***detB*** *is an integer and* $\mathbf{2^{n-1}}$ *divides* ***detB***

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

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

$\det B = p\, 2^{n-1}$

Minors of Hadamard matrices

Definition

The ***spectrum of the determinant function*** for (±1)-matrices is defined to be the set of values $\boldsymbol{p}$ taken by $\mathbf{|det}\ \boldsymbol{R_k}\mathbf{|} = \boldsymbol{p}\ \mathbf{2^{k-1}}$ as the matrix R_k ranges over all $k \times k$ (±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,…, 11 and 13. Also, conjectures have been formulated for k = 12, 14, 15, 16 and 17.

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

Given a positive integer k, it is known that $M_k \le k^{\frac{k}{2}}$ 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 $\boldsymbol{n = 4t}$, $\boldsymbol{k = 4r}$ for integers $\boldsymbol{r > 0}$ and $\boldsymbol{t > r}$ it holds:

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

A <u>necessary condition</u> for the general embedding problem is the following:

$$p \le \hat{p}$$

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

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

$$p \le \hat{p} \quad \overset{\text{Using Calculus}}{\Leftrightarrow} \quad (1-\theta)\ln(1-\theta) - \theta \ln \theta \le 0$$

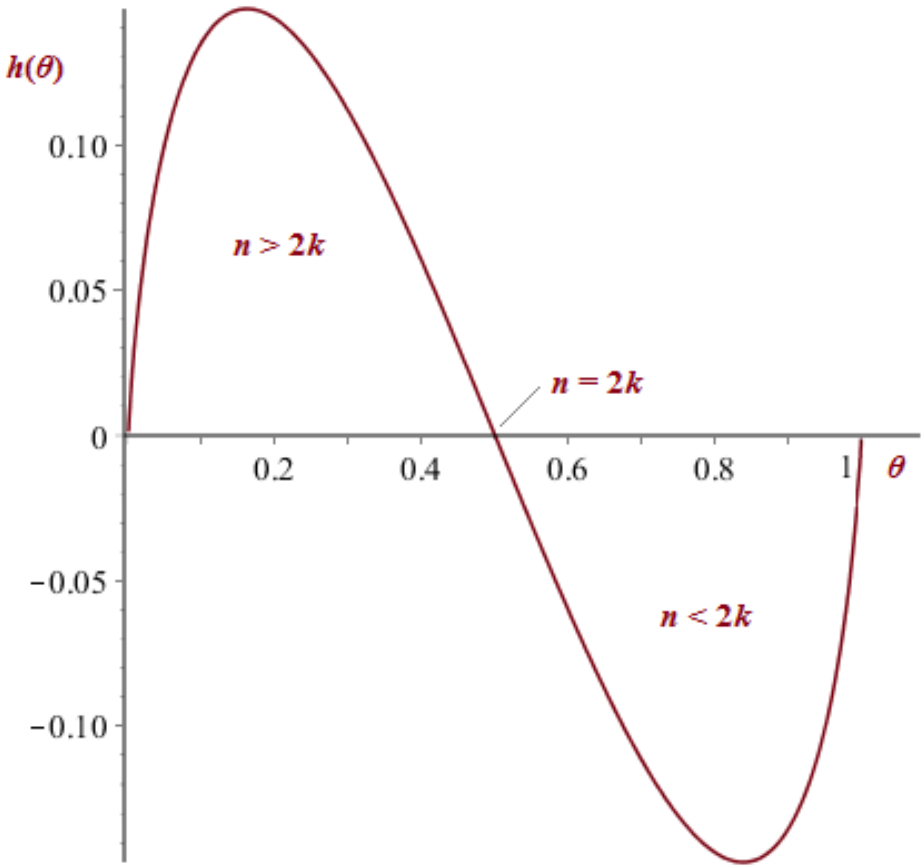
Studying the sign of the real function

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

provides very important information about the behavior of p for the various values of the integers n and k when $n > k$.

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

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



- $n > 2k \;\Leftrightarrow\; h(\theta) > 0 \;\Leftrightarrow\; p > \hat{p}$

  $H_{n-k} \notin H_n$

- $n = 2k \;\Leftrightarrow\; h(\theta) = 0 \;\Leftrightarrow\; p = \hat{p}$

  $H_k \in H_{2k}$

- $n < 2k \;\Leftrightarrow\; h(\theta) < 0 \;\Leftrightarrow\; p < \hat{p}$

  $H_{n-k} \in H_n$

But for what values of p is this true?

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

Proposition :

The discrete function

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

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

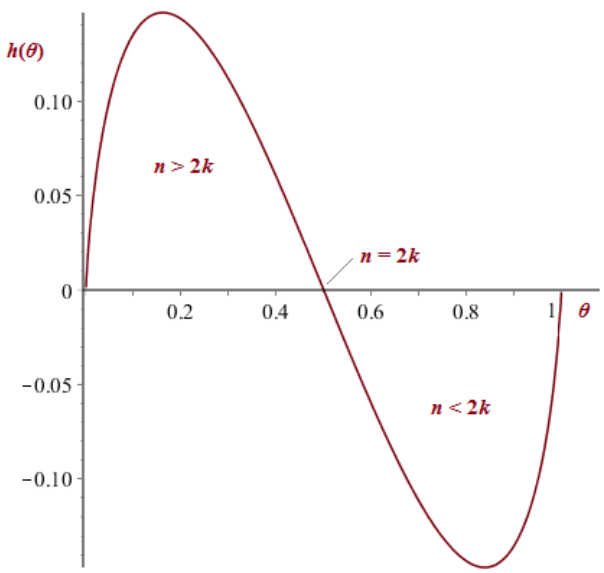
$$|\det H_{n-k}| = n^{\frac{n}{2}-k} M_k \qquad \text{or} \qquad |\det H_{n-k}| = 2^{(n-k)-1}\left(\frac{n}{4}\right)^{\frac{n}{2}-k} p$$

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

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

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

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



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

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 $|\det H_n^{(k)}| = p\, 2^{k-1}$ 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.,

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

Conclusions

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

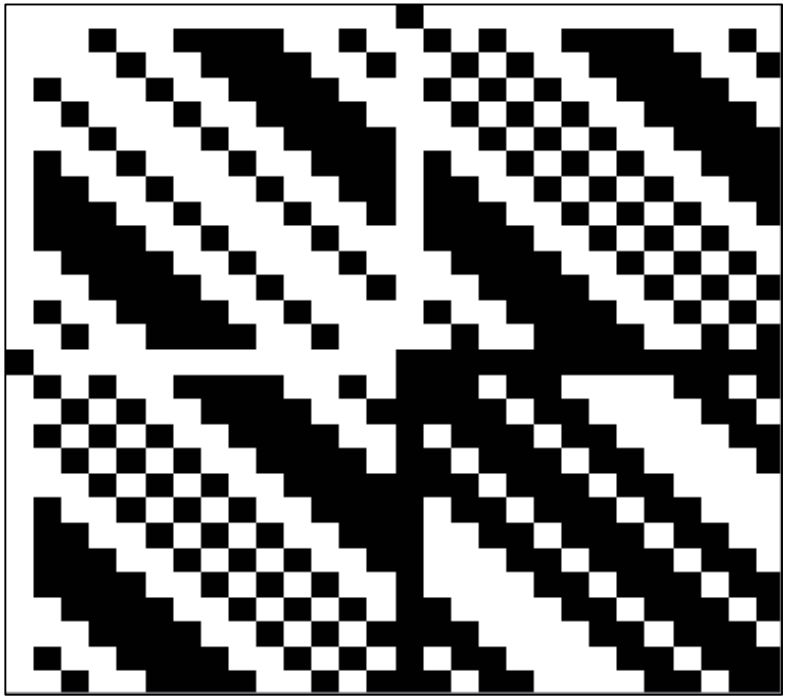
Order	$k = 4$	$k = 8$	$k = 12$	$k = 16$	$k = 20$	$k = 24$
$n = 8$	$H_4 \in H_8$					
$n = 12$	$H_8 \notin H_{12}$	$H_4 \in H_{12}$				
$n = 16$	$H_{12} \notin H_{16}$	$H_8 \in H_{16}$	$H_4 \in H_{16}$			
$n = 20$	$H_{16} \notin H_{20}$	$H_{12} \notin H_{20}$	$H_8 \in H_{20}$	$H_4 \in H_{20}$		
$n = 24$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

All the above results have been verified using search algorithms implemented in MAPLE.

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

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

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



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

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

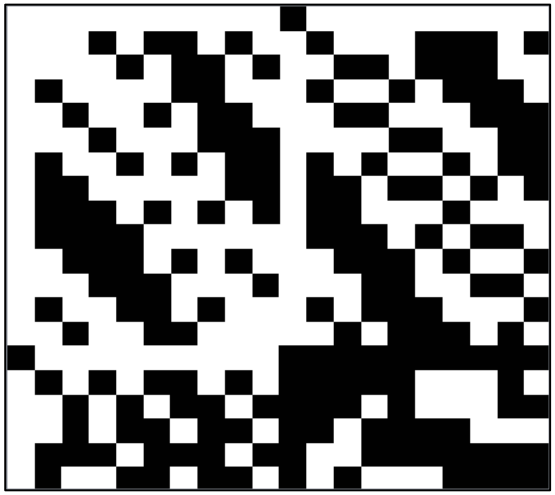
then it may H_8 exist embedded in H_{28}.

□ = 1
■ = −1

N. J. A. Sloane. A library of Hadamard matrices. http://neilsloane.com/hadamard/index.html

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

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



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

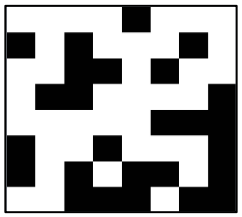
$$H_{28}^{(20)} = [a_{ij}] \text{ of } H_{28} \text{ where}$$

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

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

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

$H_8 \in H_{28}$



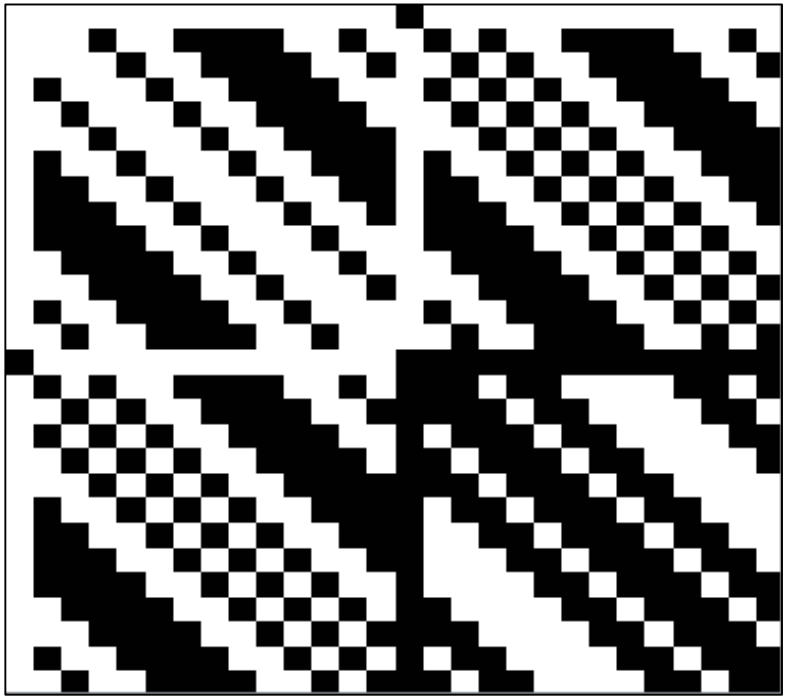
$$A = [a_{ij}] \text{ of } H_{28} \text{ where } \begin{array}{l} i \in \{1, 2, 3, 4, 5, 6, 16, 17\}, \\ j \in \{4, 6, 9, 14, 15, 19, 21, 26\} \end{array}$$

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

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

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

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



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

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

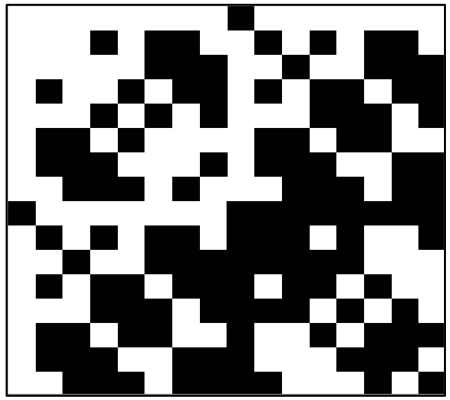
then it may H_{12} exist embedded in H_{28}.

□ = 1
■ = −1

N. J. A. Sloane. A library of Hadamard matrices. http://neilsloane.com/hadamard/index.html

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

$H_{28}^{(16)}$ *submatrix of* H_{28}



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

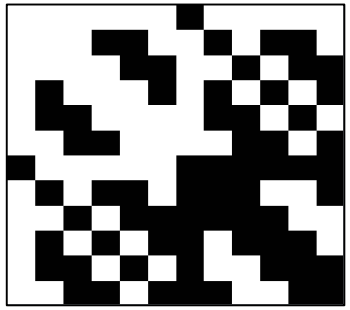
$$H_{28}^{(16)} = [a_{ij}] \text{ of } H_{28} \text{ where}$$

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

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

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

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



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

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

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
Special Matrices, Vol.6, (2018), pp. 155–165

References

1. J. Hadamard, Résolution d'une question relative aux déterminants. *Bull. Sci. Math.* 17, (1893), 240–246.

2. R. P. Brent and J-A. H. Osborn, On minors of maximal determinant matrices. *J. Integer Seq.*, 16, (2013), 1 – 30.

3. J.H.E. Cohn, Hadamard matrices and some generalisations. *Amer. Math. Monthly*, 72(5), (1965), 515 – 518.

4. J. Day and B. Peterson, Growth in Gaussian elimination, *Amer. Math. Monthly*, 95, (1988), 489–513.

5. F. Szöllòsi, Exotic Complex Hadamard matrices and their equivalence. *Cryptogr. Commun.*, 2, (2010), 187 – 198.

6. J. Seberry, T. Xia, C. Koukouvinos, M. Mitrouli, The maximal determinant and subdeterminants of ±1 matrices, *Linear Algebra Appl.*, 373, (2003), 297 – 310.

Thank you

for your attention