On some applications of Hadamard matrices

George Giorgobiani, Vakhtang Kvaratskhelia,
Marine Menteshashvili

Muskhelishvili Institute of Computational Mathematics
of the Georgian Technical University, Georgia

South-Caucasus Computing and Technology Workshop
(SCCTW-2016),
Tbilisi, Georgia, October 3 - 7, 2016

Abstract

In the presentation a short survey of the theory of Hadamard (Sylvester) matrices is given. Moreover, numerical characteristic of Sylvester matrices is introduced and some of its properties are shown.

keywords. Hadamard matrix, Hadamard conjecture, Sylvester matrix.

1. Hadamard matrices

There are various types of matrices in the literature having distinct properties useful for numerous applications, both practical and theoretical. The famous matrix with orthogonal property is a Hadamard matrix, which was first defined by J.J. Sylvester in 1867 and was studied further by J.S. Hadamard in 1893.

Hadamard matrices have plenty of practical applications. It is an important tool for the investigation of some problems of:

- Quantum Computing,
- Coding Theory and Cryptology,
- Statistics,
- Image Analysis,
- Signal Processing,
- Scheduling Theory,
- Combinatorial Designs and so on.

1. Hadamard matrices

There are various types of matrices in the literature having distinct properties useful for numerous applications, both practical and theoretical. The famous matrix with orthogonal property is a Hadamard matrix, which was first defined by J.J. Sylvester in 1867 and was studied further by J.S. Hadamard in 1893.

Hadamard matrices have plenty of practical applications. It is an important tool for the investigation of some problems of:

- Quantum Computing,
- Coding Theory and Cryptology,
- Statistics,
- Image Analysis,
- Signal Processing,
- Scheduling Theory,
- Combinatorial Designs and so on.

1. Hadamard matrices

There are various types of matrices in the literature having distinct properties useful for numerous applications, both practical and theoretical. The famous matrix with orthogonal property is a Hadamard matrix, which was first defined by J.J. Sylvester in 1867 and was studied further by J.S. Hadamard in 1893.

Hadamard matrices have plenty of practical applications. It is an important tool for the investigation of some problems of:

- Quantum Computing,
- Coding Theory and Cryptology,
- Statistics,
- Image Analysis,
- Signal Processing,
- Scheduling Theory,
- Combinatorial Designs and so on.

1. Hadamard matrices

There are various types of matrices in the literature having distinct properties useful for numerous applications, both practical and theoretical. The famous matrix with orthogonal property is a Hadamard matrix, which was first defined by J.J. Sylvester in 1867 and was studied further by J.S. Hadamard in 1893.

Hadamard matrices have plenty of practical applications. It is an important tool for the investigation of some problems of:

- Quantum Computing,
- Coding Theory and Cryptology,
- Statistics,
- Image Analysis,
- Signal Processing,
- Scheduling Theory,
- Combinatorial Designs and so on.

1. Hadamard matrices

There are various types of matrices in the literature having distinct properties useful for numerous applications, both practical and theoretical. The famous matrix with orthogonal property is a Hadamard matrix, which was first defined by J.J. Sylvester in 1867 and was studied further by J.S. Hadamard in 1893.

Hadamard matrices have plenty of practical applications. It is an important tool for the investigation of some problems of:

- Quantum Computing,
- Coding Theory and Cryptology,
- Statistics,
- Image Analysis,
- Signal Processing,
- Scheduling Theory,
- Combinatorial Designs and so on.

1. Hadamard matrices

There are various types of matrices in the literature having distinct properties useful for numerous applications, both practical and theoretical. The famous matrix with orthogonal property is a Hadamard matrix, which was first defined by J.J. Sylvester in 1867 and was studied further by J.S. Hadamard in 1893.

Hadamard matrices have plenty of practical applications. It is an important tool for the investigation of some problems of:

- Quantum Computing,
- Coding Theory and Cryptology,
- Statistics,
- Image Analysis,
- Signal Processing,
- Scheduling Theory,
- Combinatorial Designs and so on.

1. Hadamard matrices

There are various types of matrices in the literature having distinct properties useful for numerous applications, both practical and theoretical. The famous matrix with orthogonal property is a Hadamard matrix, which was first defined by J.J. Sylvester in 1867 and was studied further by J.S. Hadamard in 1893.

Hadamard matrices have plenty of practical applications. It is an important tool for the investigation of some problems of:

- Quantum Computing,
- Coding Theory and Cryptology,
- Statistics,
- Image Analysis,
- Signal Processing,
- Scheduling Theory,
- Combinatorial Designs and so on.

Definition 1.1

A Hadamard matrix is a square matrix with entries equal to ± 1 whose rows (and hence columns) are mutually orthogonal.

In other words, a Hadamard matrix of order n is a $\{1, -1\}$-matrix H satisfying the equality

$$HH^T = nI_n,$$

where I_n is the identity matrix of order n.

1. Hadamard matrices

In 1867 Sylvester proposed a recurrent method for the construction of Hadamard matrices of order $2n$ if a Hadamard matrix of order n is given.

Namely, if H is a Hadamard matrix of order n, then the matrix

$$\begin{bmatrix} H, & H \\ H, & -H \end{bmatrix}$$

is a Hadamard matrix of order $2n$.

There are several operations on Hadamard matrices which preserve the Hadamard property. For example:

- (a) permuting rows, and changing the sign of some of them;
- (b) permuting columns, and changing the sign of some of them;
- (c) transposition.

There are several operations on Hadamard matrices which preserve the Hadamard property. For example:

- (a) permuting rows, and changing the sign of some of them;
- (b) permuting columns, and changing the sign of some of them;
- (c) transposition.

There are several operations on Hadamard matrices which preserve the Hadamard property. For example:

- (a) permuting rows, and changing the sign of some of them;
- (b) permuting columns, and changing the sign of some of them;
- (c) transposition.

2. Hadamard determinantal inequality

In 1893 Hadamard presented his famous determinant bound, which gives rise to the term Hadamard matrix.

Let us formulate this result and note that this problem so far remains unsolved for matrices of general size.

Theorem 2.1

(J.S. Hadamard, 1893). *Let $A = (a_{ij})$ be a real matrix of order n whose entries satisfy the condition $|a_{ij}| \leq 1$ for all $i, j = 1, 2, \ldots, n$. Then*

$$|\det A| \leq n^{n/2};$$

equality holds if and only if A is a Hadamard matrix.

2. Hadamard determinantal inequality

One side of this theorem is proved in an elementary way.

Indeed, it is easy to see that if we denote by $a_1, a_2, \ldots, a_n$ the rows of the matrix A, then it is known that $|\det(A)|$ is the volume of the parallelepiped with sides $a_1, a_2, \ldots, a_n$; so

$$|\det(A)| \leq \|a_1\| \cdot \|a_2\| \cdot \ldots \cdot \|a_n\|,$$

where $\|a_i\|$ is the Euclidean length of a_i; equality holds if and only if $a_1, a_2, \ldots, a_n$ are mutually orthogonal. By hypothesis of the theorem

$$\|a_i\| = \left(a_{i1}^2 + a_{i2}^2 + \ldots + a_{in}^2\right)^{1/2} \leq n^{1/2},$$

with equality if and only if $|a_{ij}| = 1$ for all j.

It follows from these inequalities that actually

$$|\det(A)| \leq n^{n/2}.$$

2. Hadamard determinantal inequality

- Hadamard's bound implies that $\{1, -1\}$-matrices of size n have determinant at most $n^{n/2}$.
- Hadamard observed that a construction of Sylvester, mentioned above, produces examples of matrices that attain the bound when n is a power of 2, and constructed examples of Hadamard matrices of sizes of 12 and 20.
- He also showed that the bound is only attainable when n is equal to 1, 2, or a multiple of 4.

2. Hadamard determinantal inequality

- Hadamard's bound implies that $\{1, -1\}$-matrices of size n have determinant at most $n^{n/2}$.
- Hadamard observed that a construction of Sylvester, mentioned above, produces examples of matrices that attain the bound when n is a power of 2, and constructed examples of Hadamard matrices of sizes of 12 and 20.
- He also showed that the bound is only attainable when n is equal to 1, 2, or a multiple of 4.

2. Hadamard determinantal inequality

- Hadamard's bound implies that $\{1, -1\}$-matrices of size n have determinant at most $n^{n/2}$.
- Hadamard observed that a construction of Sylvester, mentioned above, produces examples of matrices that attain the bound when n is a power of 2, and constructed examples of Hadamard matrices of sizes of 12 and 20.
- He also showed that the bound is only attainable when n is equal to 1, 2, or a multiple of 4.

3. Hadamard conjecture

In 1933 English mathematician R. Paley stated that the order $n\,(n \geq 4)$ of any Hadamard matrix is divisible by 4. This is easy to prove. The converse statement has been a long-standing conjecture.

Conjecture 3.1

For every positive integer n, there exists a Hadamard matrix of order $4n$.

This conjecture obviously is true for the positive integers which are power of 2.

The current smallest order for which the existence of a Hadamard matrix is unknown is 668.

4. Sylvester matrices

The sequence of the matrices defined by the following recurrence relation:

$$\mathcal{S}^{(0)} = [1], \quad \mathcal{S}^{(n)} = \begin{bmatrix} \mathcal{S}^{(n-1)}, & \mathcal{S}^{(n-1)} \\ \mathcal{S}^{(n-1)}, & -\mathcal{S}^{(n-1)} \end{bmatrix}, \quad n = 1, 2, \ldots$$

are a particular case of the Hadamard matrices and are named the Sylvester (or Walsh) matrices.

$\mathcal{S}^{(n)} = \left[s_{ij}^{(n)} \right]$ is a square matrix of order 2^n, where $s_{ij}^{(n)} = \pm 1$.

Example 4.1

$$\mathcal{S}^{(1)} = \begin{bmatrix} 1, & 1 \\ 1, & -1 \end{bmatrix}, \quad \mathcal{S}^{(2)} = \begin{bmatrix} 1, & 1, & 1, & 1 \\ 1, & -1 & 1, & -1 \\ 1, & 1 & -1, & -1 \\ 1, & -1 & -1, & 1 \end{bmatrix}, \quad \textit{and so on.}$$

5. Numerical characteristic of Sylvester matrices

For a Sylvester matrix $\mathcal{S}^{(n)} = \left[s_{ij}^{(n)}\right]$ let us consider the functions

$$\varrho^{(n)}(m) = \sum_{j=1}^{2^n} \left| \sum_{i=1}^{m} s_{ij}^{(n)} \right|, \quad m = 1, 2, \ldots, 2^n,$$

and

$$\varrho^{(n)} = \max_{1 \le m \le 2^n} \varrho^{(n)}(m).$$

It is easy to see that for any positive integer n the following simple estimations are valid

$$2^n \le \varrho^{(n)} \le 2^{2n}.$$

Example 5.2

For the Sylvester matrix $\mathcal{S}^{(1)} = \left[s_{ij}^{(1)}\right]$ *we have*

$$\varrho^{(1)}(1) = 1 + 1 = 2, \quad \varrho^{(1)}(2) = 2 + 0 = 2,$$

so

$$\varrho^{(1)} = \max\{2, 2\} = 2,$$

and for the Sylvester matrix $\mathcal{S}^{(2)} = \left[s_{ij}^{(2)}\right]$ *we have*

$$\varrho^{(2)}(1) = 1 + 1 + 1 + 1 = 4, \quad \varrho^{(2)}(2) = 2 + 0 + 2 + 0 = 4,$$

$$\varrho^{(2)}(3) = 3 + 1 + 1 + 1 = 6, \quad \varrho^{(2)}(4) = 4 + 0 + 0 + 0 = 4,$$

so

$$\varrho^{(2)} = \max\{4, 4, 6, 4\} = 6.$$

6. Main Theorem

- $\varrho^{(n)}$ is numerical characteristic of matrix and, in particular, it is a norm of a matrix on the linear space of all square matrices of order 2^n.
- This function was successfully applied for the investigation of convergence of series in different functional spaces.
- Now our goal is estimation of this characteristic.

- $\varrho^{(n)}$ is numerical characteristic of matrix and, in particular, it is a norm of a matrix on the linear space of all square matrices of order 2^n.
- This function was successfully applied for the investigation of convergence of series in different functional spaces.
- Now our goal is estimation of this characteristic.

6. Main Theorem

- $\varrho^{(n)}$ is numerical characteristic of matrix and, in particular, it is a norm of a matrix on the linear space of all square matrices of order 2^n.
- This function was successfully applied for the investigation of convergence of series in different functional spaces.
- Now our goal is estimation of this characteristic.

- The following result gives a precise value of the function $\varrho^{(n)}$:

Theorem 6.1

(Main Theorem). *For every positive integer n we have*

$$\varrho^{(n)} = \max_{1 \le m \le 2^n} \varrho^{(n)}(m) = \frac{3n+7}{9} \cdot 2^n + (-1)^n \cdot \frac{2}{9}.$$

For any n the maximum is attained at the points

$$m_n = \frac{2^{n+1} + (-1)^n}{3} \quad \text{and} \quad m_n^{'} = \frac{5 \cdot 2^{n-1} + (-1)^{n-1}}{3}.$$

- From this theorem immediately follows the following

Corollary 6.2

For any positive integer n the following inequality is valid

$$\varrho^{(n)} \le n \cdot 2^n$$

6. Main Theorem

- The following result gives a precise value of the function $\varrho^{(n)}$:

Theorem 6.1

(Main Theorem). *For every positive integer n we have*

$$\varrho^{(n)} = \max_{1 \le m \le 2^n} \varrho^{(n)}(m) = \frac{3n+7}{9} \cdot 2^n + (-1)^n \cdot \frac{2}{9}.$$

For any n the maximum is attained at the points

$$m_n = \frac{2^{n+1} + (-1)^n}{3} \quad \textit{and} \quad m_n^{'} = \frac{5 \cdot 2^{n-1} + (-1)^{n-1}}{3}.$$

- From this theorem immediately follows the following

Corollary 6.2

For any positive integer n the following inequality is valid

$$\varrho^{(n)} \le n \cdot 2^n.$$

6. Main Theorem

- The following result gives a precise value of the function $\varrho^{(n)}$:

Theorem 6.1

(Main Theorem). *For every positive integer n we have*

$$\varrho^{(n)} = \max_{1 \le m \le 2^n} \varrho^{(n)}(m) = \frac{3n+7}{9} \cdot 2^n + (-1)^n \cdot \frac{2}{9}.$$

For any n the maximum is attained at the points

$$m_n = \frac{2^{n+1} + (-1)^n}{3} \quad \text{and} \quad m_n^{'} = \frac{5 \cdot 2^{n-1} + (-1)^{n-1}}{3}.$$

- From this theorem immediately follows the following

Corollary 6.2

For any positive integer n the following inequality is valid

$$\varrho^{(n)} \le n \cdot 2^n.$$

6. Main Theorem

- The following result gives a precise value of the function $\varrho^{(n)}$:

Theorem 6.1

(Main Theorem). *For every positive integer n we have*

$$\varrho^{(n)} = \max_{1 \le m \le 2^n} \varrho^{(n)}(m) = \frac{3n+7}{9} \cdot 2^n + (-1)^n \cdot \frac{2}{9}.$$

For any n the maximum is attained at the points

$$m_n = \frac{2^{n+1} + (-1)^n}{3} \quad \text{and} \quad m_n^{'} = \frac{5 \cdot 2^{n-1} + (-1)^{n-1}}{3}.$$

- From this theorem immediately follows the following

Corollary 6.2

For any positive integer n the following inequality is valid

$$\varrho^{(n)} \le n \cdot 2^n.$$

7. Open Problem

- $\mathcal{S}^{(n)} = \left[s_{ij}^{(n)} \right]$ – a Sylvester matrix of order 2^n;
- $a_i = \left(s_{i1}^{(n)}, s_{i2}^{(n)}, \ldots, s_{i2^n}^{(n)} \right), \quad a_i \in \mathbb{R}^{2^n}, \quad i = 1, 2, \ldots 2^n.$
- By the Main Theorem of the Presentation we have:

$$\varrho^{(n)} = \left\| \sum_{k=1}^{m_n} a_k \right\|_{l_1} = (3n+7)2^n/9 + 2(-1)^n/9,$$

where $m_n = (2^{n+1} + (-1)^n)/3$ and $\| \cdot \|_{l_1}$ is the l_1-norm in $\mathbb{R}^{2^n}$,

(i.e. if $b = (\beta_1, \beta_2, \ldots, \beta_{2^n})$, then $\|b\|_{l_1} = \sum_{j=1}^{2^n} |\beta_j|$).

7. Open Problem

- $\mathcal{S}^{(n)} = \left[s_{ij}^{(n)} \right]$ – a Sylvester matrix of order 2^n;
- $a_i = \left(s_{i1}^{(n)}, s_{i2}^{(n)}, \ldots, s_{i2^n}^{(n)} \right), \quad a_i \in \mathbb{R}^{2^n}, \quad i = 1, 2, \ldots 2^n$.
- By the Main Theorem of the Presentation we have:

$$\varrho^{(n)} = \left\| \sum_{k=1}^{m_n} a_k \right\|_{l_1} = (3n+7)2^n/9 + 2(-1)^n/9,$$

where $m_n = (2^{n+1} + (-1)^n)/3$ and $\| \cdot \|_{l_1}$ is the l_1-norm in $\mathbb{R}^{2^n}$,

(i.e. if $b = (\beta_1, \beta_2, \ldots, \beta_{2^n})$, then $\|b\|_{l_1} = \sum_{j=1}^{2^n} |\beta_j|$).

7. Open Problem

- $\mathcal{S}^{(n)} = \left[s_{ij}^{(n)} \right]$ – a Sylvester matrix of order 2^n;
- $a_i = \left(s_{i1}^{(n)}, s_{i2}^{(n)}, \dots, s_{i2^n}^{(n)} \right), \quad a_i \in \mathbb{R}^{2^n}, \quad i = 1, 2, \dots 2^n.$
- By the Main Theorem of the Presentation we have:

$$\varrho^{(n)} = \left\| \sum_{k=1}^{m_n} a_k \right\|_{l_1} = (3n+7)2^n/9 + 2(-1)^n/9,$$

where $m_n = (2^{n+1} + (-1)^n)/3$ and $\| \cdot \|_{l_1}$ is the l_1-norm in $\mathbb{R}^{2^n}$,

(i.e. if $b = (\beta_1, \beta_2, \dots, \beta_{2^n})$, then $\|b\|_{l_1} = \sum_{j=1}^{2^n} |\beta_j|$).

7. Open Problem

- $\Pi^{(n)}$ – the set of all permutations of the sequence $\{1, 2, \ldots, 2^n\}$;
- Consider the following expression:

$$\left\| \sum_{k=1}^{m_n} a_{\pi(k)} \right\|_{l_1}, \quad \pi \in \Pi^{(n)}.$$

- We can prove that for any $\pi \in \Pi^{(n)}$

$$\left\| \sum_{k=1}^{m_n} a_{\pi(k)} \right\|_{l_1} \leq 2^{3n/2}.$$

- Note that we do not know how precise the last inequality is.

7. Open Problem

- $\Pi^{(n)}$ – the set of all permutations of the sequence $\{1, 2, \ldots, 2^n\}$;
- Consider the following expression:

$$\left\| \sum_{k=1}^{m_n} a_{\pi(k)} \right\|_{l_1}, \quad \pi \in \Pi^{(n)}.$$

- We can prove that for any $\pi \in \Pi^{(n)}$

$$\left\| \sum_{k=1}^{m_n} a_{\pi(k)} \right\|_{l_1} \leq 2^{3n/2}.$$

- Note that we do not know how precise the last inequality is.

7. Open Problem

- $\Pi^{(n)}$ – the set of all permutations of the sequence $\{1, 2, \dots, 2^n\}$;
- Consider the following expression:

$$\left\| \sum_{k=1}^{m_n} a_{\pi(k)} \right\|_{l_1}, \quad \pi \in \Pi^{(n)}.$$

- We can prove that for any $\pi \in \Pi^{(n)}$

$$\left\| \sum_{k=1}^{m_n} a_{\pi(k)} \right\|_{l_1} \leq 2^{3n/2}.$$

- Note that we do not know how precise the last inequality is.

7. Open Problem

- $\Pi^{(n)}$ – the set of all permutations of the sequence $\{1, 2, \ldots, 2^n\}$;
- Consider the following expression:

$$\left\| \sum_{k=1}^{m_n} a_{\pi(k)} \right\|_{l_1}, \quad \pi \in \Pi^{(n)}.$$

- We can prove that for any $\pi \in \Pi^{(n)}$

$$\left\| \sum_{k=1}^{m_n} a_{\pi(k)} \right\|_{l_1} \leq 2^{3n/2}.$$

- Note that we do not know how precise the last inequality is.

7. Numerical characteristic of Hadamard matrices

The authors also do not know yet the answer to the following conjecture:

Conjecture 7.2

For any positive integer $n \geq 1$ *and for any permutation of integers* $\pi \in \Pi$ *we have*

$$\left\| \sum_{i=1}^{m_n} a_{\pi(k)} \right\|_{l_1} \geq (3n+7)2^n/9 + 2(-1)^n/9.$$

Note that we have conducted a lot of computer experiments. The results do not contradict this Conjecture, though a theoretical proof is not known yet.

8. Conclusions

Therefore, let us summarize this presentation.

- We recalled the definitions of Hadamard and Sylvester matrices;
- We recalled the well-known **Hadamard's Conjecture**;
- We introduced the numerical characteristic $\varrho^{(n)}$ of the Sylvester matrix;
- We calculated the precise value of this characteristic **Main theorem**;
- We formulated our **Open Problem**.
- Finally, in the References some of our related papers are listed.

8. Conclusions

Therefore, let us summarize this presentation.

- We recalled the definitions of Hadamard and Sylvester matrices;
- We recalled the well-known **Hadamard's Conjecture**;
- We introduced the numerical characteristic $\varrho^{(n)}$ of the Sylvester matrix;
- We calculated the precise value of this characteristic **Main theorem**;
- We formulated our **Open Problem**.
- Finally, in the References some of our related papers are listed.

8. Conclusions

Therefore, let us summarize this presentation.

- We recalled the definitions of Hadamard and Sylvester matrices;
- We recalled the well-known **Hadamard's Conjecture**;
- We introduced the numerical characteristic $\varrho^{(n)}$ of the Sylvester matrix;
- We calculated the precise value of this characteristic **Main theorem**;
- We formulated our **Open Problem.**
- Finally, in the References some of our related papers are listed.

8. Conclusions

Therefore, let us summarize this presentation.

- We recalled the definitions of Hadamard and Sylvester matrices;
- We recalled the well-known **Hadamard's Conjecture**;
- We introduced the numerical characteristic $\varrho^{(n)}$ of the Sylvester matrix;
- We calculated the precise value of this characteristic **Main theorem**;
- We formulated our **Open Problem**.
- Finally, in the References some of our related papers are listed.

8. Conclusions

Therefore, let us summarize this presentation.

- We recalled the definitions of Hadamard and Sylvester matrices;
- We recalled the well-known **Hadamard's Conjecture**;
- We introduced the numerical characteristic $\varrho^{(n)}$ of the Sylvester matrix;
- We calculated the precise value of this characteristic **Main theorem**;
- We formulated our **Open Problem.**
- Finally, in the References some of our related papers are listed.

8. Conclusions

Therefore, let us summarize this presentation.

- We recalled the definitions of Hadamard and Sylvester matrices;
- We recalled the well-known **Hadamard's Conjecture**;
- We introduced the numerical characteristic $\varrho^{(n)}$ of the Sylvester matrix;
- We calculated the precise value of this characteristic **Main theorem**;
- We formulated our **Open Problem**.
- Finally, in the References some of our related papers are listed.

REFERENCES

- *G. Giorgobiani, V. Kvaratskhelia, M. Menteshashvili.* Some properties of Hadamard matrices. Computer Science and Information Technologie (CSIT), 2015. Revised Selected Papers, September 28 – October 2, 2015, Yerevan, Armenia, IEEE, 64–66.
- *A. Figula, V. Kvaratskhelia.* Some numerical characteristics of Sylvester and Hadamard matrices. Publ. Math. Debrecen, 86/1-2, 2015, 149–168.
- *V. Kvaratskhelia.* Some inequalities related to Hadamard matrices. Functional Analysis and Its Applications 36, 2002, 81–85.

THANK YOU FOR YOUR ATTENTION!