Towards new constructions of Butson-type Hadamard matrices

On the discovery of a complex Hadamard matrix of order 94

Ferenc Szöllősi
szollosi@riko.shimane-u.ac.jp

Talk at the
International Workshop on Discrete Mathematics and Algorithms 2026
March 17, 2026, Matsue, Japan

This research was supported in part by a JSPS KAKENHI Grant Number 24K06829.

Outline

In this talk we introduce real and complex Hadamard matrices, and briefly touch upon their graph theoretical model, and some computational aspects.

- Real Hadamard matrices
  Kronecker product; the Williamson and the Goethels–Seidel constructions.
  Equivalence of Hadamard matrices, the Hadamard graph.
- Complex Hadamard matrices
  Butson-type complex Hadamard matrices, Turyn's construction.
  The Kharaghani–Seberry block construction, and a modification.
- Some algorithms
  Searching for $\{-1,1\}$-sequences with zero autocorrelation.
  Some new results.
- Outlook and open problems

Introduction

Definition

A real Hadamard matrix H of order n is a square $\{-1, 1\}$-matrix with pairwise orthogonal rows. In other words, $HH^T = nI_n$.

An easy parity argument shows that if H exists, then $n = 1, 2$, or $4k$ for $k \geq 1$.

The Hadamard conjecture

There exists a real Hadamard matrix for every doubly even orders.

There are many infinite constructions.

Lemma

If H and K are Hadamard matrices of order n and m, respectively, then $H \otimes K$ is a Hadamard matrix of order nm.

Proof: $(H \otimes K)(H \otimes K)^T = HH^T \otimes KK^T = nI_n \otimes mI_m = nmI_{nm}$.
The smallest outstanding order is $n = 668 = 4 \cdot 167$.

The Williamson construction

One of the earliest constructions is due to Williamson, who realized that arranging symmetric circulant matrices of order p into a 4×4 array yields a Hadamard matrix of order $4p$, subject to the condition:

$$AA^T + BB^T + CC^T + DD^T = 4pI_p.$$

This is called the Williamson array, and the matrices (A, B, C, D) are called Williamson matrices.

$$H = \begin{bmatrix} A & B & C & D \\ B & -A & D & -C \\ C & -D & -A & B \\ D & C & -B & -A \end{bmatrix}.$$

Conjecture

Williamson matrices exists for every odd p.

True for $p < 35$, but false for $p \in \{35, 47, 53, 59\}$.
The lack of Williamson matrices lead to various generalizations.

The Goethels–Seidel array

It turns out, that the symmetry condition can be removed, if we manipulate the blocks A, B, C, and D a bit. Let R be the back-diagonal matrix. It is clear that if X is circulant, then XR is symmetric. The following is called the Goethels–Seidel array.

Theorem

Let A, B, C, and D be circulant matrices of order p, such that

$$AA^T + BB^T + CC^T + DD^T = 4pI_p.$$

Then

$$H = \begin{bmatrix} A & BR & CR & DR \\ -BR & A & -D^TR & C^TR \\ -CR & D^TR & A & -B^TR \\ -DR & -C^TR & B^TR & A \end{bmatrix}.$$

is a real Hadamard matrix of order $4p$.

This is a prolific method of constructing real Hadamard matrices.

Summary so far

We want to construct real Hadamard matrices of order $4p$, just like this:

$$\left[\begin{array}{cccc} A & B & C & D \\ B & -A & D & -C \\ C & -D & -A & B \\ D & C & -B & -A \end{array}\right] \rightsquigarrow \left[\begin{array}{ccccc|ccccc|ccccc|ccccc}
1 & 1 & - & - & 1 & 1 & - & 1 & 1 & - & - & 1 & 1 & 1 & 1 & 1 & - & - & - & - \\
1 & 1 & 1 & - & - & - & 1 & - & 1 & 1 & 1 & - & 1 & 1 & 1 & - & 1 & - & - & - \\
- & 1 & 1 & 1 & - & 1 & - & 1 & - & 1 & 1 & 1 & - & 1 & 1 & - & - & 1 & - & - \\
- & - & 1 & 1 & 1 & 1 & 1 & - & 1 & - & 1 & 1 & 1 & - & 1 & - & - & - & 1 & - \\
1 & - & - & 1 & 1 & - & 1 & 1 & - & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & 1 \\
\hline
1 & - & 1 & 1 & - & - & - & 1 & 1 & - & 1 & - & - & - & - & 1 & - & - & - & - \\
- & 1 & - & 1 & 1 & - & - & - & 1 & 1 & - & 1 & - & - & - & - & 1 & - & - & - \\
1 & - & 1 & - & 1 & 1 & - & - & - & 1 & - & - & 1 & - & - & - & - & 1 & - & - \\
1 & 1 & - & 1 & - & 1 & 1 & - & - & - & - & - & - & 1 & - & - & - & - & 1 & - \\
- & 1 & 1 & - & 1 & - & 1 & 1 & - & - & - & - & - & - & 1 & - & - & - & - & 1 \\
\hline
- & 1 & 1 & 1 & 1 & - & 1 & 1 & 1 & 1 & - & - & 1 & 1 & - & 1 & - & 1 & 1 & - \\
1 & - & 1 & 1 & 1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & 1 & - & 1 & - & 1 & 1 \\
1 & 1 & - & 1 & 1 & 1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & 1 & - & 1 & - & 1 \\
1 & 1 & 1 & - & 1 & 1 & 1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & 1 & - & 1 & - \\
1 & 1 & 1 & 1 & - & 1 & 1 & 1 & 1 & - & - & 1 & 1 & - & - & - & 1 & 1 & - & 1 \\
\hline
1 & - & - & - & - & - & 1 & 1 & 1 & 1 & - & 1 & - & - & 1 & - & - & 1 & 1 & - \\
- & 1 & - & - & - & 1 & - & 1 & 1 & 1 & 1 & - & 1 & - & - & - & - & - & 1 & 1 \\
- & - & 1 & - & - & 1 & 1 & - & 1 & 1 & - & 1 & - & 1 & - & 1 & - & - & - & 1 \\
- & - & - & 1 & - & 1 & 1 & 1 & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - \\
- & - & - & - & 1 & 1 & 1 & 1 & 1 & - & 1 & - & - & 1 & - & - & 1 & 1 & - & -
\end{array}\right]$$

In essence, we want to combine four $\{-1,1\}$-sequences of length $(p-1)/2$.

Equivalence of Hadamard matrices

The following are the main challenges:

- Generating one real Hadamard matrix;
- Generating all real Hadamard matrices;
- Generating all real Hadamard matrices up to equivalence;

of a given order $n \equiv 0 \pmod 4$.

Definition

Two real Hadamard matrices H and K are equivalent, if $H = P_1 D_1 K D_2 P_2$ for some ± 1 diagonal matrices D_1, D_2 and some permutation matrices P_1 and P_2.

In other words, H and K are equivalent, if the rows and columns of K can be permuted in a way, such that if the rows and columns of the permuted matrix are multiplied by certain ± 1 entries we get H.

Currently this is decided by modeling Hadamard matrices by graphs, and then checking whether the corresponding graphs are isomorphic by McKay–Piperno's `nauty` package.

Let's create a graph theoretical model $\Gamma(H)$ of the 2×2 real Hadamard matrix!
If H is of order n, then $\Gamma(H)$ has $4n + 3$ vertices.

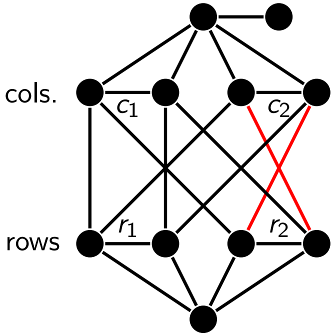
$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

We have two rows r_1 and r_2, and two columns c_1 and c_2.

The rows and columns are modeled by edges; each has an 'odd' and an 'even' endpoint. They can be distinguished from each other by the top pendant vertex.

If $H_{ij} = +1$ then we connect r_i and c_j with parallel edges (odd-odd, even-even); otherwise we use crossing edges.

Figure: The graph $\Gamma(H)$



It is easy to see that performing the equivalence operations lead to isomorphic graphs.
Also, from a graph like this the Hadamard matrix can be reconstructed, up to equivalence.

Complex Hadamard matrices

Since we can't solve the Hadamard conjecture, we generalize the problem.

Definition

A square matrix H of order n with $|h_{ij}| = 1$ having pairwise complex orthogonal rows is called a complex Hadamard matrix. In other words, $HH^* = nI_n$.

We focus on the quaternary case, that is, when $h_{ij}^4 = 1$, equivalently $h_{ij} \in \{\pm 1, \pm \mathbf{i}\}$. Matrices with root of unity entries are also called as Butson-type Hadamard matrices.

It is known that complex Hadamard matrices exist for orders up to 92, and the previously largest outstanding case was order 70, constructed by Dragomir Đoković in 1993.

Theorem[Turyn]

If H is a complex Hadamard matrix of order n, then there exists a real Hadamard matrix of order $2n$.

So, from complex one may construct real. But what about the converse direction?

The KHARAGHANI–SEBERRY construction

Let A, B, C, D be Williamson matrices of order p. Then

$$K = \frac{1}{2}\begin{bmatrix} A+B+\mathbf{i}(A-B) & C+D+\mathbf{i}(C-D) \\ -C-D+\mathbf{i}(C-D) & A+B-\mathbf{i}(A-B) \end{bmatrix}$$

is a complex Hadamard matrix of order $2p$.

So, from (certain) symmetric, circulant matrices of order p, we can construct

- a real Hadamard matrix of order $4p$; and
- a complex Hadamard matrix of order $2p$.

Can we construct a complex Hadamard matrix of order 94, using Williamson matrices of order $p = 47$? Sadly no, since such matrices do not exist.
The main idea is to modify slightly the array K, and somehow relax the symmetry condition.
This has already done in the real case when Goethels and Seidel generalized Williamson's method.

A modified array

To the best of my knowledge, the following is a new construction.

Theorem[F. Sz., 2026+]

Let A, B, C, D be circulant $\{-1,1\}$-matrices of order p, such that $A = A^T$, $B = B^T$, and $AA^T + BB^T + CC^T + DD^T = 4pI_p$. Let R be the back-diagonal matrix. Then

$$\frac{1}{2}\begin{bmatrix} A+B+\mathbf{i}(A-B) & C+DR+\mathbf{i}(C-DR) \\ C^T+DR-\mathbf{i}(C^T-DR) & -A-B+\mathbf{i}(A-B) \end{bmatrix}$$

is a complex Hadamard matrix of order $2p$.

So, with this array instead of using Williamson matrices, we may use circulant matrices where only two of them are symmetric.
There is a vast literature on circulant matrices studied by Đoković and coauthors. Sadly, for $p = 47$ we were unable to find anything relevant to this.
Thus, we constructed them from scratch.

The Sum Of Squares (SOS) decomposition

Let σ_X denote the row sum of the matrix X. We have the following SOS decomposition.

Lemma

Let A, B, C, and D be circulant matrices of order p, such that

$$AA^T + BB^T + CC^T + DD^T = 4pI_p.$$

Then $\sigma_A^2 + \sigma_B^2 + \sigma_C^2 + \sigma_D^2 = 4p$.

Proof: Multiply the above equation by the constant vector 1 from the left and right, respectively.

Lemma

If a matrix M is a block of a Hadamard matrix H of order n, then all eigenvalues λ_k of M must satisfy $|\lambda_k| \leq \sqrt{n}$.

This can be shown by using that $H/\sqrt{n}$ is a unitary matrix, hence its blocks are contractions.

Autocorrelation

Write $A = \mathrm{circ}([a_0, a_1, \ldots, a_{p-1}])$, etc., and consider the equation

$$AA^T + BB^T + CC^T + DD^T = 4pI_p.$$

Since this involves circulant matrices, it is enough to consider the first row, and write:

$$\sum_{k=0}^{p-1} (a_k a_{k+s} + b_k b_{k+s} + c_k c_{k+s} + d_k d_{k+s}) = 4p\delta_{0s}$$

for $s = 0, 1, \ldots, (p-1)/2$ (indices are modulo p). Let's introduce the short-hand notation $\mathcal{I}(a) \in \mathbb{Z}^{(p-1)/2}$ for the autocorrelation (or: inner products) vector, whose coordinates are

$$\mathcal{I}(a)_s = \sum_{k=1}^{p-1} a_k a_{k+s},$$

where indices on the right-hand side are understood modulo p. Therefore, we aim to find four sequences of length p, such that:

$$\mathcal{I}(a) + \mathcal{I}(b) = -(\mathcal{I}(c) + \mathcal{I}(d)).$$

A quick recap using the previous running example

Consider $p = 5$, and the Williamson matrices shown previously:

$$A = \begin{bmatrix} 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 \end{bmatrix}, C = \begin{bmatrix} -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 \end{bmatrix}, D = \begin{bmatrix} 1 & -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & -1 & 1 \end{bmatrix}.$$

We have $AA^T + BB^T + CC^T + DD^T = 20I_5$, and $1^2 + (-1)^2 + 3^2 + (-3)^2 = 4 \cdot 5 = 20$.
Let $a = [1, 1, -1, -1, 1]$, $b = [1, -1, 1, 1, 1 - 1]$, $c = [-1, 1, 1, 1, 1]$, $d = [1, -1, -1, -1, -1]$.
Now, since A is a circulant matrix, AA^T is also circulant, furthermore it is symmetric:

$$AA^T = \begin{bmatrix} 5 & 1 & -3 & -3 & 1 \\ 1 & 5 & 1 & -3 & -3 \\ -3 & 1 & 5 & 1 & -3 \\ -3 & -3 & 1 & 5 & 1 \\ 1 & -3 & -3 & 1 & 5 \end{bmatrix},$$

so the relevant information is: $\mathcal{I}([1, 1, -1, -1, 1]) = [1, -3]$.
We want to find $a, b, c, d \in \{-1, 1\}^{(p-1)/2}$, such that: $\mathcal{I}(a) + \mathcal{I}(b) + \mathcal{I}(c) + \mathcal{I}(d) = [0, 0]$.

Computer search

Here is a simplified algorithm for searching for the required matrices:

(A1) Fix an odd p, and row sums σ_A, σ_B, σ_C, σ_D, such that their SOS is $4p$.

(A2) Generate all symmetric circulant $\{-1, 1\}$ matrices with row sum σ_A and σ_B, and keep only those whose eigenvalues in absolute value are at most $2\sqrt{p}$.

(A3) Calculate and store all possible sum of inner products $\Sigma := \mathcal{I}(a) + \mathcal{I}(b)$ in a set S.

(A4) Repeatedly choose random $\{-1, 1\}$-vectors c and d with row sum σ_C and σ_D, and check if $s := -\mathcal{I}(c) - \mathcal{I}(d) \in S$. If this is the case, then save c, d, and s, and move to (A5).

(A5) Find a and b such that $\mathcal{I}(a) + \mathcal{I}(b) = s$ and output (a, b, c, d).

In practice, this takes a lot of memory, so we introduced a bound $\mathcal{B}$ and stored only those sum of inner products Σ, whose norm

$$\|\Sigma\| := \sum_{k=1}^{(p-1)/2} \Sigma_k^2$$

does not exceed $\mathcal{B}$. The larger the bound is, the more likely we find suitable matrices, but also the search becomes more time consuming and memory intensive. For $p = 47$ we found that $\mathcal{B} = 1200$ is good.

Results

After a day of search and $8 \cdot 10^9$ trials, we found the following sequences:

$$\left[\begin{array}{c|c|c}
1 & 1\,1\,1\,-\,1\,-\,1\,1\,-\,-\,-\,1\,-\,1\,1\,-\,-\,-\,-\,-\,1\,1\,1 & 1\,1\,1\,-\,-\,-\,-\,-\,1\,1\,-\,1\,-\,-\,-\,1\,1\,-\,1\,-\,1\,1\,1 \\
1 & 1\,-\,1\,-\,1\,1\,1\,-\,1\,-\,1\,1\,-\,-\,-\,1\,1\,-\,-\,1\,-\,1\,1 & 1\,1\,-\,1\,-\,-\,1\,1\,-\,-\,-\,1\,1\,-\,1\,-\,1\,1\,1\,-\,1\,-\,1 \\
1 & 1\,1\,1\,1\,1\,1\,1\,1\,-\,-\,-\,1\,1\,-\,1\,-\,1\,1\,-\,-\,1\,-\,- & -\,-\,-\,1\,-\,-\,1\,1\,-\,1\,1\,1\,1\,-\,1\,1\,1\,-\,-\,1\,-\,1\,- \\
1 & 1\,1\,1\,1\,1\,-\,-\,1\,1\,1\,1\,-\,1\,1\,-\,1\,-\,1\,-\,-\,1\,1\,- & 1\,1\,-\,-\,-\,1\,-\,1\,1\,-\,1\,1\,1\,-\,-\,-\,1\,1\,-\,1\,1\,-\,-
\end{array}\right].$$

This corresponds to $3^2 + 7^2 + 9^2 + 9^2 = 4 \cdot 47$ with $\|\Sigma\| = 796 \leq 1200$. Thus, a combination of our block construction with these sequences yield the following new result.

Theorem[F. Sz., 2026+]

A complex Hadamard matrix of order 94 exists.

The next outstanding case seems to be $p = 59$, i.e., a complex Hadamard of order 118. Maybe with supercomputers...

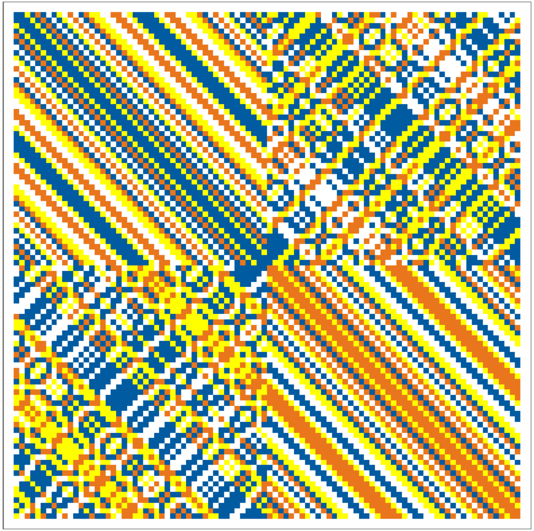
Thank you for your attention

FERENC SZÖLLŐSI
associate professor
Shimane University, Matsue, Japan
szollosi@riko.shimane-u.ac.jp

Any questions?

Open problems:

- Efficient generation of real and complex Hadamard matrices
- A real Hadamard matrix of order $4 \cdot 167 = 668$
- A complex Hadamard matrix of order $2 \cdot 59 = 118$.



Preprint is available on arXiv: https://arxiv.org/abs/2603.09572