On a new class of Hadamard matrices

Petr Lisoněk
Simon Fraser University, Burnaby, BC, Canada

Joint work with Jasleen Phangara, SFU

15th Nordic Combinatorial Conference (NORCOM 2025)
Reykjavík, Iceland

17 June 2025

Definitions, notation

$z \in \mathbb{C}$ is *unimodular* if $|z| = 1$

H is *complex Hadamard matrix* of order n if all its entries are unimodular and $HH^* = nI_n$, where I_n is the $n \times n$ identity matrix.

Butson type complex Hadamard matrix of order n: all entries are q-th roots of unity for some q.
Notation: $\mathrm{BH}(n, q)$
Example: *Fourier matrix* $\mathcal{F}_n = (\zeta_n^{ij})_{0 \le i,j \le n-1}$ is a $\mathrm{BH}(n, n)$

Equivalence

Two complex Hadamard matrices are *equivalent* if one can be obtained from the other one by a series of operations of the following types:

- row permutation
- column permutation
- scaling a row by a unimodular scalar
- scaling a column by a unimodular scalar.

Each complex Hadamard matrix is equivalent to a *dephased matrix* whose first row and first column consist entirely of 1s.

Classification

For $n \leq 5$ complex Hadamard matrices of order n have been classified up to equivalence. For $n = 6$ the classification is believed to be complete, but this is not proved. For $n > 6$ the problem is wide open.

Catalog of complex Hadamard matrices
by W. Bruzda, W. Tadej and K. Życzkowski

`https://chaos.if.uj.edu.pl/~karol/hadamard/`

Classifications of $\mathrm{BH}(n, q)$ for $n \leq 21$ and $q \leq 17$
by P. Lampio, P. Östergård, and F. Szöllősi

`https://wiki.aalto.fi/display/Butson/Matrices+up+to+monomial+equivalence`

New class: S-Hadamard matrices

Let $A \circ B$ denote the element-wise product of matrices $A = (a_{i,j})$ and $B = (b_{i,j})$, usually called *Schur product* or Hadamard product. That is $(A \circ B)_{i,j} = a_{i,j} b_{i,j}$.

Definition

We say that matrix H is *S-Hadamard* if H is complex Hadamard and its Schur square $H \circ H$ is also complex Hadamard.

This seems to be a new class of matrices not studied previously. It will be the focus of the rest of the talk.

Note that the equivalence relation introduced for complex Hadamard matrices also applies to S-Hadamard matrices.

S-Hadamard matrices

Proposition

For odd n the matrix $\mathcal{F}_n$ is S-Hadamard.

This follows from a straightforward calculation based on the fact that $i \mapsto 2i \bmod n$ is a bijection for odd n.

Proposition

There are no S-Hadamard matrices of order 2 and 4.

This is because any complex Hadamard matrix of order 2 or 4 is equivalent to a matrix with two real rows, as can be seen in the classification results.

A Plethora of BH type S-Hadamard matrices

Results of classification of BH type matrices due to P. Lampio, P. Östergård, and F. Szöllősi are readily available online at the link shown above. The data is very nicely formatted and ready to use.

We found that in the range covered in this classification ($n \leq 21$ and $q \leq 17$) there are 401 non-isomorphic BH type S-Hadamard matrices.

A few of these matrices are explained by an infinite family which we show below, but there still remain hundreds of matrices to be investigated.

We now turn to searching for S-Hadamard matrices which are not necessarily of BH type.

Our computational method

We formulate the problem of finding S-Hadamard matrices as a continuous optimization problem with $2(n-1)^2$ real variables $\mathrm{Re}(h_{i,j})$ and $\mathrm{Im}(h_{i,j})$ for $2 \leq i,j \leq n$. The unimodularity and orthogonality conditions can be represented as a set of equations of the form $F_k = 0$ where each F_k is a real-valued multivariate polynomial. We then solve the optimization problem:

minimize $\sum_k F_k^2$

Since the objective function is non-negative, we know that an S-Hadamard matrix was found exactly if the value of the objective function is 0 (up to a numerical error) at the local optimum found by the optimization algorithm.

S-Hadamard matrices: computation results so far

Conjecture

There is no S-Hadamard matrix of order 8.

Fact

There exist S-Hadamard matrices of order 6, 10 and 12.

Conjecture

All S-Hadamard matrices of order 6 are equivalent to the unique $\mathrm{BH}(6,3)$.
All S-Hadamard matrices of order 10 are equivalent to the unique $\mathrm{BH}(10,5)$.

We'll see in a moment that these two matrices belong to an infinite family of S-Hadamard matrices which we'll construct using finite fields.

S-Hadamard matrices: computation results so far

Fact

There exist S-Hadamard matrices of order 12 which are not of the BH type.

In fact a 3-parametric family of such matrices exists, which we'll construct later on. The parameters can take any unimodular values.

Generalized Hadamard matrices

Definition

Let G be a group of order g and let λ be a positive integer. A *generalized Hadamard matrix* over G is a $g\lambda \times g\lambda$ matrix $M = (m_{i,j})$ whose entries are elements of G and for each $1 \leq k < \ell \leq g\lambda$, each element of G occurs exactly λ times among the differences $m_{k,j} - m_{\ell,j}$, $1 \leq j \leq g\lambda$. Such matrix is denoted $\mathrm{GH}(g, \lambda)$.

Many infinite families of $\mathrm{GH}(g, \lambda)$ are known (direct constructions and recursive constructions).

Butson and Jungnickel used the finite field $\mathbb{F}_q$ to construct $\mathrm{GH}(q, 2)$ for all odd prime powers q. For q odd prime this immediately produces $\mathrm{BH}(2q, q)$ by exponentiation; in particular the $\mathrm{BH}(6, 3)$ and $\mathrm{BH}(10, 5)$ mentioned earlier are obtained.

An S-Hadamard matrix construction

Theorem (L. 2019)

Suppose that $g > 2$ and a $\mathrm{GH}(g, \lambda)$ over $\mathbb{Z}_g$ exists. Then we can construct an S-Hadamard matrix of order $g\lambda$ of the BH type.

This can be used together with the Butson-Jungnickel construction when g is an odd prime, but other suitable ingredients exist as well, e.g. the $\mathrm{GH}(4, 4)$ over $\mathbb{Z}_4$ due to Harada, Lam and Tonchev (2005).

S-Hadamard matrices of order 12

Fact

Up to equivalence there are exactly two $\mathrm{BH}(12,3)$*, namely* M *and* M^* *where* M *is given below. They are both S-Hadamard.*

De Launey's (Graphs and Combinatorics 1989) constructed BH(12,3), where $\omega = \exp(2\pi\mathbf{i}/3)$, $B = \left(\begin{smallmatrix} \omega & \omega^2 \\ \omega^2 & \omega \end{smallmatrix}\right)$, $T = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and $J = I_2 + T$, as

$$M = \left(\begin{array}{cc|cc|cc} \omega J & \omega^2 J & B & B & B & TB \\ \omega^2 J & \omega J & B & B & TB & B \\ \hline B & TB & \omega^2 J & J & \omega^2 B & \omega^2 B \\ TB & B & J & \omega^2 J & \omega^2 B & \omega^2 B \\ \hline B & B & \omega^2 B & \omega^2 TB & \omega^2 J & J \\ B & B & \omega^2 TB & \omega^2 B & J & \omega^2 J \end{array}\right).$$

S-Hadamard matrices of order 12

We've seen that for even orders less than 12, all S-Hadamard matrices that do exist seem to be of the BH type. This however changes at order 12.

Theorem (L., Phangara 2024)

There exists a 3-parametric family of S-Hadamard matrices, given below, where the parameters a, b, c can take any unimodular values.

We'll now briefly outline the process of discovering this family, and making the matrices more structured.

S-Hadamard matrices of order 12

Using our computational method, we found a non-BH type order 12 S-Hadamard matrix by fixing entry (2,2) of the matrix to be a random unimodular complex number. Using PSLQ to form integer relations among the phases of the entries of this matrix, we formed the symbolic matrix S shown below.

$$S = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & a & b & \omega^2 b & \omega^2 & \omega b & \omega^2 b & \omega b & b & \omega^2 a & \omega & \omega a \\
1 & c & \omega & \omega b & \omega^2 & b & \omega & \omega^2 b & 1 & \omega c & \omega^2 & \omega^2 c \\
1 & \omega c & \omega^2 c & \frac{\omega bc}{a} & \omega & \frac{\omega^2 bc}{a} & c & \frac{bc}{a} & c & \omega^2 c & \omega^2 & \omega c \\
1 & \omega^2 c & c & \frac{bc}{a} & \omega & \frac{\omega bc}{a} & \omega c & \frac{\omega^2 bc}{a} & \omega c & \omega^2 c & \omega^2 & c \\
1 & \omega c & \omega c & \frac{\omega^2 bc}{a} & \omega & \frac{bc}{a} & \omega^2 c & \frac{\omega bc}{a} & \omega^2 c & c & \omega^2 & c \\
1 & \omega^2 & \omega & \omega & 1 & \omega & 1 & \omega & \omega^2 & \omega^2 & 1 & \omega^2 \\
1 & \omega & 1 & \omega^2 & 1 & \omega^2 & \omega & \omega^2 & \omega^2 & \omega & 1 & \omega \\
1 & \omega a & \omega^2 b & b & \omega^2 & \omega b & \omega b & b & \omega^2 b & a & \omega & \omega^2 a \\
1 & c & \omega^2 & b & \omega & \omega^2 b & \omega^2 & \omega b & \omega & \omega c & 1 & \omega^2 c \\
1 & \omega^2 c & \omega^2 & \omega b & 1 & b & \omega^2 & \omega^2 b & \omega & c & \omega & \omega c \\
1 & \omega^2 a & \omega b & \omega^2 b & \omega^2 & \omega^2 b & b & b & \omega b & \omega a & \omega & a
\end{pmatrix}$$

We confirmed using computer algebra that S is S-Hadamard for any unimodular a, b, c.

S-Hadamard matrices of order 12

Egan, Flannery, and Ó Catháin (Classifying cocyclic Butson Hadamard matrices, 2014) provide Magma code which, given two BH matrices H_1, H_2 of the same order, decides if they are equivalent and if so, finds an isomorphism defined by monomial matrices P, Q such that $PH_1Q = H_2$. The paper and the Magma code are posted at

`https://www.daneflannery.com/classifying-cocyclic-butson-hadamard-matrices`

Let S' be S in which a, b, c are assigned some powers of ω. We know that each such S' is equivalent to M or M^* given above. Using the code by Egan, Flannery, and Ó Catháin, we determined that all matrices S' are in fact equivalent to M.

S-Hadamard matrices of order 12

Let S_1 be S where a, b, c are all set to 1. Using this code again, we find monomial matrices P_1, Q_1 such that $P_1 S_1 Q_1 = M$.

Applying P_1, Q_1 to S, we see that S is equivalent to the more structured S-Hadamard matrix

$$H = M \circ \begin{pmatrix} K & KP & KP^2 \\ PK & PKP & PKP^2 \\ P^2K & P^2KP & P^2KP^2 \end{pmatrix}$$

where M is the de Launey's BH(12,3),
$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ and $K = \begin{pmatrix} 1 & b & c & 1 \\ 1 & b & a & b \\ 1 & 1 & 1 & 1 \\ 1 & \frac{bc}{a} & c & c \end{pmatrix}$.

Application: Kochen-Specker theorem

Kochen-Specker theorem (1965) is an important result in quantum mechanics. It demonstrates the *contextuality of quantum mechanics*, which is one of its properties that may become crucial in building quantum computers.

M. Howard, J. Wallman, V. Veitch, J. Emerson, Contextuality supplies the 'magic' for quantum computation. Nature **510** (2014), 351–355.

Kochen-Specker sets

Kochen-Specker theorem can be proved in several ways. One type of its proofs can be constructed as follows:

Definition

We say that $(\mathcal{V}, \mathcal{B})$ is a *Kochen-Specker pair in* $\mathbb{C}^n$ if it meets the following conditions:

(1) $\mathcal{V}$ is a finite set of vectors in $\mathbb{C}^n$.

(2) $\mathcal{B} = (B_1, \ldots, B_k)$ where k is odd, and for all for $i = 1, \ldots, k$ we have that B_i is an orthogonal basis of $\mathbb{C}^n$ and $B_i \subset \mathcal{V}$.

(3) For each $v \in \mathcal{V}$ the number of i such that $v \in B_i$ is even.

Sometimes this is called a parity proof of KS theorem. The term KS set is used often.

Some known Kochen-Specker pairs

Kochen-Specker (1965) - 117 vectors in $\mathbb{R}^3$

Cabello et al. (1998) - 18 vectors in $\mathbb{R}^4$, 9 bases

Lisoněk et al. (2014) - 21 vectors in $\mathbb{C}^6$, 7 bases (the "simplest" Kochen-Specker set), initially found by computer, all bases are BH(6,3) matrices

Now we give insight into the structure of the simplest KS set, and we show that it is the initial member of an infinite family of KS sets which we construct using S-Hadamard matrices.

An infinite family of Kochen-Specker sets

Theorem

Suppose that there exists an S-Hadamard matrix of order n where n is even. Then we can construct a Kochen-Specker pair $(\mathcal{V}, \mathcal{B})$ in $\mathbb{C}^n$ such that $|\mathcal{V}| \leq \binom{n+1}{2}$ and $|\mathcal{B}| = n + 1$.

Proof.

Let H be the given S-Hadamard matrix and assume H is dephased.

Let the elements of $\mathcal{V}$ be denoted $v^{\{r,s\}}$ where $1 \leq r, s \leq n + 1$, $r \neq s$. Note $v^{\{r,s\}} = v^{\{s,r\}}$ for all $r \neq s$.

We construct the elements of $\mathcal{V}$ as follows:

- For $1 < s \leq n + 1$ let $v^{\{1,s\}} = h_{s-1}$.
- For $2 < s \leq n + 1$ let $v^{\{2,s\}} = h_{s-1} \circ h_{s-1}$.
- For $2 < r < s \leq n + 1$ let $v^{\{r,s\}} = h_{r-1} \circ h_{s-1}$.

An infinite family of Kochen-Specker sets (continued)

For $1 \leq r \leq n+1$ let

$$B_r = \{v^{\{r,i\}} \,:\, 1 \leq i \leq n+1,\ i \neq r\}$$

and let $\mathcal{B} = (B_1, \ldots, B_{n+1})$. We will now prove that each B_r is an orthogonal basis of $\mathbb{C}^n$. There are several cases to distinguish.

Note that for $x, y, z \in \mathbb{C}^n$ such that z is unimodular we have

$$\langle z \circ x, z \circ y \rangle = \langle x \circ z, y \circ z \rangle = \sum_{i=1}^{n} x_i z_i \overline{y_i z_i} = \langle x, y \rangle.$$

For $2 < r, s, t \leq n+1$ and r, s, t distinct we have

$$\langle v^{\{r,s\}}, v^{\{r,t\}} \rangle = \langle h_{r-1} \circ h_{s-1}, h_{r-1} \circ h_{t-1} \rangle = \langle h_{s-1}, h_{t-1} \rangle = 0.$$

An infinite family of Kochen-Specker sets (continued)

Let $r = 1$. For $1 < s < t \leq n + 1$ we have

$$\langle v^{\{1,s\}}, v^{\{1,t\}} \rangle = \langle h_{s-1}, h_{t-1} \rangle = 0.$$

Let $r = 2$. For distinct s, t we have

$$\langle v^{\{2,s\}}, v^{\{2,t\}} \rangle \quad = \quad \langle h_{s-1} \circ h_{s-1}, h_{t-1} \circ h_{t-1} \rangle = 0,$$

by the additional defining property of S-Hadamard matrices.

An infinite family of Kochen-Specker sets (continued)

Now let $2 < r \leq n+1$. For $t > 2$, $t \neq r$ we have

$$\begin{aligned} \langle v^{\{r,1\}}, v^{\{r,t\}} \rangle &= \langle h_{r-1}, h_{r-1} \circ h_{t-1} \rangle = \langle h_{r-1} \circ h_1, h_{r-1} \circ h_{t-1} \rangle = \\ &= \langle h_1, h_{t-1} \rangle = 0 \end{aligned}$$

as well as

$$\begin{aligned} \langle v^{\{r,2\}}, v^{\{r,t\}} \rangle &= \langle h_{r-1} \circ h_{r-1}, h_{r-1} \circ h_{t-1} \rangle \\ &= \langle h_{r-1}, h_{t-1} \rangle = 0. \end{aligned}$$

Finally we have

$$\begin{aligned} \langle v^{\{r,1\}}, v^{\{r,2\}} \rangle &= \langle h_{r-1}, h_{r-1} \circ h_{r-1} \rangle \\ &= \langle h_1 \circ h_{r-1}, h_{r-1} \circ h_{r-1} \rangle = \langle h_1, h_{r-1} \rangle = 0. \end{aligned}$$

An infinite family of Kochen-Specker sets (continued)

We note that $|\mathcal{B}| = n+1$ is odd since n is assumed to be even. We will complete the proof by verifying that each element of $\mathcal{V}$ belongs to an even number of bases B_r. If the mapping $\{i,j\} \mapsto v^{\{i,j\}}$ is injective, then each $v^{\{i,j\}}$ belongs to exactly two entries of $\mathcal{B}$, namely B_i and B_j. If the list $(v^{\{i,j\}})_{1 \le i < j \le n+1}$ contains repeated vectors, then let x be a vector that occurs exactly t times in this list. Then by the previous argument x belongs to exactly $2t$ entries of $\mathcal{B}$, since $j \neq k$ implies $v^{\{i,j\}} \neq v^{\{i,k\}}$ as $\langle v^{\{i,j\}}, v^{\{i,k\}} \rangle = 0$.

References

P. Lisoněk, Kochen-Specker sets and Hadamard matrices. Theoret. Comput. Sci. 800 (2019), 142–145.

P. Lisoněk, P. Badziąg, J.R. Portillo, A. Cabello, Kochen-Specker set with seven contexts. Physical Review A **89** (2014), 042101.

G. Cañas, M. Arias, S. Etcheverry, E.S. Gómez, A. Cabello, G.B. Xavier, G. Lima, Applying the simplest Kochen-Specker set for quantum information processing. Phys. Rev. Lett. **113** (2014), 090404.