

Old and new results on Hadamard matrices of order 6

FERENC SZÖLLŐSI
szollosi@riko.shimane-u.ac.jp

The 8th Workshop on Design Theory,
Hadamard Matrices and Applications
Sevilla University
May 30, 2025

Sadly, I am now old enough to have “old results”.

Visit to University of Manitoba in 2011 to write my PhD thesis. Thinking of a **census of $BH(n, 6)$ matrices**. First open case was $BH(25, 6)$. We knew that there is no $BH(5, 6)$. Computer search with structural assumptions: let $P = S - N$ be the Paley matrix of order 5... and the computer says...

$$I \otimes (I - \omega^2(J - I)) - \omega S \otimes (P + I) + \omega N \otimes (P - I) \in BH(25, 6).$$

Prof. Craigen suggested to *maybe* simplify this to something more elegant:

$$H = P \otimes P + J \otimes I + \omega I \otimes J.$$

Note that $J \otimes I$ and $I \otimes J$ are not disjoint, but luckily $1 + \omega = -\omega^2$.

This construction is a joint work with Professor Robert Craigen and will be included in a forthcoming publication in the near future. We summarize it in the following

Theorem 1.4.41. *Let p be a prime number and P be the Paley-matrix of order p . Then the matrix $H = P \otimes P + J \otimes I + \omega I \otimes J$ is a $BH(p^2, 6)$ matrix.*

Happy birthday Prof. Craigen!

Introduction and main new results

Problem statement

Classify all dephased complex Hadamard matrices having three distinct columns, each containing at least one entry equal to -1 .

“Cannot be more complicated, than Karlsson’s classification.”

Theorem[with Á.K. Matszangosz, 2024]

If H is as above, then H belongs to $F_6^T(a, b)$, or $X_6(\alpha)$.

$$F_6^T = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^2 & a & aw & aw^2 \\ 1 & w^2 & w & b & bw^2 & bw \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & w & w^2 & -a & -aw & -aw^2 \\ 1 & w^2 & w & -b & -bw^2 & -bw \end{bmatrix}, \quad X_6 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \frac{1}{ab} & \frac{a}{b^2} & \frac{d}{b} & \frac{1}{bc} & \frac{c}{bd} \\ 1 & \frac{b}{a^2} & \frac{1}{ab} & \frac{c}{a} & \frac{d}{ac} & \frac{1}{ad} \\ 1 & \frac{1}{ad} & \frac{1}{bc} & -1 & -\frac{1}{bc} & -\frac{1}{ad} \\ 1 & \frac{c}{a} & \frac{c}{bd} & -\frac{c}{a} & -1 & -\frac{c}{bd} \\ 1 & \frac{d}{ac} & \frac{d}{b} & -\frac{d}{b} & -\frac{d}{ac} & -1 \end{bmatrix}$$

Let’s just remember that $|z|^2 = 1 \Leftrightarrow \bar{z} = 1/z$.

Plan of attack

Split the proof based on the number of rows, containing these entries:

- If there is only one row, then it should be the family $F_6^T(a, b)$
- If there are three rows, then it should be $X_6(\alpha)$
- If there are only two rows, then... ??

It turns out, that no new families arise in the last case, as there will be automatically additional entries equal to -1 in the matrix.

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & * & * \\ 1 & * & -1 & * \\ 1 & * & * & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & * \\ 1 & * & * & -1 \end{bmatrix}$$

$F_6^T(a, b) \qquad X_6(\alpha) \qquad F_6^T(a, b), X_6(\alpha)$

Small submatrices, so orthogonality equations cannot be immediately used.

Part 1: The case of one row

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

Theorem[Well-known to those who know it well]

Let H be a complex Hadamard matrix of order 6. Then the following are equivalent:

- Every normalized matrix in the equivalence class of H contains a submatrix of the form above;
- Some normalized matrix in the equivalence class of H contains a submatrix of the form above;
- H is a member of the transposed Fourier family $F_6^T(a, b)$, up to equivalence.

Proof: Standard matrix completion using orthogonality, and the fact that having a 2×3 rank-1 submatrix is an invariant.

So this pattern above is a **complete invariant**.

Beyond orthogonality: The Haagerup identities

U. Haagerup classified 5×5 complex Hadamard matrices using a discovery of an algebraic identity between the entries of a $3 \times (n - 2)$ submatrix of complex Hadamard matrices.

Theorem[essentially due to Haagerup, 1996]

Let H be an $n \times n$ complex Hadamard matrix, and consider any of its $3 \times (n - 2)$ block, spanned by the (partial) rows $h_i, h_j, h_k \in \mathbb{C}^{n-2}$.

$$\begin{bmatrix} h_{i1} & h_{i2} & \dots & h_{i,n-2} \\ h_{j1} & h_{j2} & \dots & h_{j,n-2} \\ h_{k1} & h_{k2} & \dots & h_{k,n-2} \end{bmatrix}.$$

Let $I := \langle h_i, h_j \rangle$, $J := \langle h_j, h_k \rangle$, $K := \langle h_k, h_i \rangle$.

Then, we have the following **polynomial system of equations** in \mathbb{C}^{3n-5} , after replacing \bar{z} by $1/z$ and clearing the denominators:

$$\begin{cases} IJK = 4 - |I|^2 - |J|^2 - |K|^2 \\ IJK = \overline{IJK} \\ u \prod_{\ell \in \{i,j,k\}} \prod_{m=1}^{n-2} h_{\ell,m} = 1. \end{cases}$$

We will frequently use these identities when studying 3×4 matrices.

Part 2: The case of three rows

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & * & * \\ 1 & * & -1 & * \\ 1 & * & * & -1 \end{bmatrix}$$

Theorem[with Matszangosz]

Let H be a complex Hadamard matrix of order 6. Then the following are equivalent:

- 1 Every normalized submatrix in the equivalence class of H contains M ;
- 2 Some normalized submatrix in the equivalence class of H contains M ;
- 3 H is a member of the 2-circulant family $X_6(\alpha)$.

Naive matrix completion not going to work. There are too many cases.

Proof: We revisit the concept of **regular** complex Hadamard matrices, introduced by T. Banica and coauthors.

Once again, the pattern of -1 entries is a complete invariant.

Regular complex Hadamard matrices

Definition

A pair of rows $\{u, v\} \in \mathbb{C}^6$ with unimodular entries is called **cancelling**, if the 2×6 matrix $[u, v]$ decomposes (up to column permutation...) to three 2×2 complex Hadamard matrices.

So up to column permutation, we see a pattern like this:

$$\left[\begin{array}{cc|cc|cc} a & b & c & d & e & f \\ g & -gb/a & h & -hd/c & i & -if/e \end{array} \right],$$

and when we calculate the inner product of $\langle u, v \rangle$, then we get two-term sub-sums cancelling each other:

$$\langle u, v \rangle = (a/g - a/g) + (c/h - c/h) + (e/i - e/i) = 0.$$

Theorem[Banica et al., 2009]

Let H be a 6×6 complex Hadamard. Then the following are equivalent:

- every pair of rows of H are cancelling. (Called: 2-regular matrices)
- H is a member of the Dita-family $D_6(c)$.

Some consequences

Exercise: If $|z_1| = |z_2| = |z_3| = |z_4| = 1$, and $z_1 + z_2 + z_3 + z_4 = 0$, then $(z_1 + z_2)(z_1 + z_3)(z_1 + z_4) = 0$.

Solution: Draw a parallelogram.

Lemma

Assume that a 2×6 matrix with unimodular entries and orthogonal rows $u, v \in \mathbb{C}^6$ has a 2×2 complex Hadamard matrix (up to column permutation). Then the rows of this matrix are cancelling.

Proof:

$$\left[\begin{array}{cc|cccc} a & b & c & d & e & f \\ g & -gb/a & h & j & i & k \end{array} \right],$$

$$0 = \langle u, v \rangle = (a/g - a/g) + c/h + d/j + e/i + f/k,$$

so up to relabelling, $c/h + d/j = 0$ and consequently $e/i + f/k = 0$.

Further consequences

Let's revisit our pattern. Now we know entries -1 imply cancelling rows.

$$\left[\begin{array}{cccc|cc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & a & b & * & * \\ 1 & d & -1 & c & * & * \\ 1 & e & f & -1 & * & * \end{array} \right]$$

Because of the previous lemma, rows $\{r_1, r_2\}$, $\{r_1, r_3\}$, and $\{r_1, r_4\}$ are pairwise cancelling. What about, say, rows $\{r_2, r_3\}$? If $c = -b$, then the first three rows are pairwise cancelling.

Plan: Prove that a triplet of pairwise cancelling rows forces the matrix to be $D_6(c)$, and then consider the complementary "no such triplet" case. Algebraically, we consider whether or not the quantity

$$(a + b)(d + c)(e + f)(d + e)(a + f)(b + c)$$

equals 0.

The case $(a + b)(d + c)(e + f)(d + e)(a + f)(b + c) = 0$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & a & b \\ 1 & c & -1 & d \\ 1 & e & f & -1 \end{bmatrix}$$

Theorem

Assume that a 6×6 complex Hadamard matrix has the above submatrix subject to $(a + b)(d + c)(e + f)(d + e)(a + f)(b + c) = 0$.

Then H is a member of the Dita family $D_6(c)$.

Proof: There are two (families of) pairwise cancelling triplets. Gröbner calculation shows that any additional orthogonal row *satisfying Haagerup's identities* is necessarily cancelling to the initial triplet.

Note, however, the following intriguing, **incompletable** example:

$$W = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i & \frac{1-i}{2} & \frac{-1+i}{\sqrt{2}} \\ 1 & -1 & \frac{-1+i}{\sqrt{2}} & \frac{1+i}{\sqrt{2}} & \frac{-1-i}{\sqrt{2}} & \frac{1-i}{\sqrt{2}} \\ 1 & \frac{2\sqrt{2}+i}{3} & \frac{-1-i}{\sqrt{2}} & \frac{-4-\sqrt{2}+(4-\sqrt{2})i}{6} & \frac{-1+2\sqrt{2}i}{3} & -i \end{bmatrix}$$

The case $(a + b)(d + c)(e + f)(d + e)(a + f)(b + c) \neq 0$

How to transform the condition $f \neq 0$ to a *polynomial equation*?

Pick an auxiliary variable u , and add the equation $uf = 1$ to your system.

This is called the *Rabinowitsch trick*.

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & a & b \\ 1 & c & -1 & d \\ 1 & e & f & -1 \end{bmatrix}$$

Lemma

Assume that a 6×6 complex Hadamard matrix has the above submatrix subject to $(a + b)(d + c)(e + f)(d + e)(a + f)(b + c) \neq 0$.

Then $ac = be = df$.

Proof: We may consider the Haagerup identities. Gröbner calculation shows that $ac - be \neq 0$ is impossible. Similarly by symmetry, $ac - df \neq 0$ is not possible. Thus $ac = be = df$ as claimed.

The case $ac = be = df$

By the previous Lemma, this block has only four variables in it:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & a & b \\ 1 & c & -1 & d \\ 1 & e & f & -1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & a & b \\ 1 & c & -1 & d \\ 1 & ac/b & ac/d & -1 \end{bmatrix}$$

Theorem

Assume that a 6×6 complex Hadamard matrix has the above submatrix subject to $(a + b)(d + c)(e + f)(d + e)(a + f)(b + c) \neq 0$.

Then H is a member of the 2-circulant family $X_6(\alpha)$.

Proof: Matrix completion with Gröbner basis calculation.

$$\left[\begin{array}{cccc|cc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & a & b & -a & -b \\ 1 & c & -1 & d & -d & -c \\ 1 & ac/b & ac/d & -1 & * & * \end{array} \right]$$

There are only two cases: $[*, *] \in \{[-ac/b, -ac/d], [-ac/d, -ac/b]\}$.

The completed matrix, if exists, is (a subfamily of) $X_6(\alpha)$.

Part 3: The case of two rows

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & * \\ 1 & * & * & -1 \end{bmatrix}$$

Theorem[with Matszangosz]

Assume that H is a 6×6 complex Hadamard matrix with the submatrix above. Then H belongs to $F_6^T(a, b)$ or to $X_6(\alpha)$.

Proof: Block decomposition based on Karlsson's breakthrough result.

Theorem[Karlsson, 2011]

Assume that a 6×6 complex Hadamard matrix H has a 2×2 sub-Hadamard matrix K . Then H is equivalent to a block-partitioned matrix where all 9 blocks of order 2 are complex Hadamard:

$$\begin{bmatrix} K & H_2 & H_3 \\ H_4 & H_5 & H_6 \\ H_7 & H_8 & H_9 \end{bmatrix}.$$

Using Karlsson's partition

Lemma

Let H be a complex Hadamard matrix of order 6 with submatrix:

$$M = \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & b & p & q \\ 1 & -b & w & -qw/p \end{array} \right].$$

Then, $(b - qw)(1 + w + w^2) = 0$.

Proof: We use three of the Haagerup identities on 3×4 and 4×3 blocks:

$$\begin{cases} \mathcal{P}_1 := \mathcal{H}((1, 2, 3), (1, 2, 3, 4)) = 0 \\ \mathcal{P}_2 := p^2 \mathcal{H}((1, 2, 4), (1, 2, 3, 4)) = 0 \\ \mathcal{P}_3 := \mathcal{H}((1, 2, 4), (1, 2, 3, 4)) = 0, \text{ for } M^T \\ \mathcal{P}_4 := ubpqw + 1 = 0, \end{cases}$$

and discover *witness polynomials* \mathcal{Q}_i , such that one may directly verify the identity $\sum_{i=1}^4 \mathcal{P}_i \mathcal{Q}_i = (b - qw)(1 + w + w^2)$.

The witness polynomials

These are (optional) by-products of a Gröbner basis calculation:

$$Q_1 = -buw + quw^4,$$

$$Q_2 = -pquw - b^2qu^2w,$$

$$Q_3 = -2quw + pquw - quw^2 - pq^3u^2w^3 - 2pq^3u^2w^3,$$

$$Q_4 = 8b + 8bw - 8qw + 2b^3puw + 2b^2quw + 2bpq^2uw + 8bw^2 - 8qw^2 \\ + 4b^2quw^2 + 8bpq^2uw^2 + 2bp^2q^2uw^2 - 8qw^3 + 2b^2quw^3 \\ + 8bpq^2uw^3 + 4bp^2q^2uw^3 - 2bq^2uw^4 + 4bpq^2uw^4.$$

So, if the fate of the world depended on this proof, then the verification

$$\sum_{i=1}^4 P_i Q_i = 8(b - qw)(1 + w + w^2)$$

could be carried out.

The case $b - qw \neq 0$

By our Lemma before, we have $1 + w + w^2 = 0$.

$$\left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & b & p & q \\ 1 & -b & w & -qw/p \end{array} \right]$$

Proposition

Let H be a 6×6 complex Hadamard matrix having the specific submatrix above subject to $b - qw \neq 0$. Then H is a member of $F_6^T(a, b)$, or a sub-family of the Fourier family $F_6(c, d)$:

$$H(a) = \left[\begin{array}{cccc|cc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & a & -a \\ 1 & 1 & w & w & w^2 & w^2 \\ 1 & -1 & w & -w & aw^2 & -aw^2 \\ \hline 1 & 1 & w^2 & w^2 & w & w \\ 1 & -1 & w^2 & -w^2 & aw & -aw \end{array} \right], \quad 1 + w + w^2 = 0, |a| = 1.$$

Note that $H(a)$, in general, does not have three columns with -1 entries.

The end of the proof: $b - qw = 0$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & * \\ 1 & * & * & -1 \end{bmatrix} \rightsquigarrow \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & b & p & q \\ 1 & -b & w & -qw/p \end{array} \right]$$

So assume that H contains a substructure as above. Then permute the columns to have a Karlsson decomposition.

- If $b - qw \neq 0$, then we have F_6^T or there are further -1 entries somewhere in the last two columns of $H(a)$, and we are done.
- If $b - qw = 0$, then $w := b/q$, and the Karlsson decomposition looks like this:

$$\left[\begin{array}{cc|cc|cc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & a & -a \\ \hline 1 & b & p & q & x & y \\ 1 & -b & b/q & -b/p & z & -yz/x \end{array} \right].$$

Lengthy matrix completion with Gröbner calculation discovers additional entries -1 within the matrix, which leads to the previously discussed cases.

Outlook (Remark 5)

Let H be a complex Hadamard matrix such that its upper left 4×4 submatrix is equivalent to the following:

$$\left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & a & -a \\ \hline 1 & b & p & q \\ 1 & -b & w & -qw/p \end{array} \right]$$

Then, we have: $(1+a)(ab-qw)(1+w+w^2)(a^2+aw+w^2) = 0$.

This may be proved similarly using Gröbner bases and witness polynomials. However... the witness polynomials we found have degree up to 17, up to 10.000 terms, and coefficients with 116 digits.

To fully classify all 6×6 Hadamard matrices, one might try to see what, if anything, can be said about the submatrix

$$\left[\begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & a & b & c \\ 1 & d & e & f \\ 1 & g & h & i \end{array} \right],$$

by using Haagerup's identities.

Summary

- In the previous talk Matolcsi explained that MUB triplets $\{X, Y, Z\}$ in \mathbb{C}^6 might be characterized by certain algebraic equations.
- These equations imply that the *transition matrices* $\sqrt{6}XY^*$, $\sqrt{6}YZ^*$, and $\sqrt{6}ZX^*$ contain three -1 entries in three distinct (rows or) columns.
- Thus these matrices belong to $F_6(a, b)$, $F_6^T(a, b)$, or to $X_6(\alpha)$.
- If any of the transition matrices belong to $F_6(a, b)$ or $F_6^T(a, b)$ then, due to standard results, we conclude that there are no 7 MUBs in \mathbb{C}^6 .
- And there remains the last unresolved case where none of the transition matrices come from the Fourier families, but all of them come from $X_6(\alpha)$. This hopefully never happens, and we are “done”.

Don't forget the Rabinowitsch trick! $f \neq 0 \Leftrightarrow uf = 1$.

Thank you for your attention

FERENC SZÖLLŐSI

Associate professor

Shimane University, Japan

szollosi@riko.shimane-u.ac.jp



Any questions?

Reference: Á. K. MATSZANGOSZ, F. SZÖLLŐSI: A characterization of complex Hadamard matrices appearing in families of MUB triplets, *Des. Codes Cryptogr.*, **92**, 4313–4333 (2024).