On 64-modular Hadamard matrices

Shalom Eliahou

Université du Littoral Côte d'Opale, Calais

Hadamard 2025

May 26-30, Sevilla

Modular Hadamard matrices

▷ Let $m \in \mathbb{N}$. An *m*-modular Hadamard matrix is a square matrix A of order n, with entries in $\{\pm 1\}$, such that

$$AA^T \equiv nI_n \mod m.$$

▷ Introduced by Marrero-Butson in 1972.

▷ Case $m = 0$: true Hadamard matrices.

▷ Notation:

$$H_m(n) = \{m\text{-modular Hadamard matrices of order } n\}$$

The *m*-modular Hadamard conjecture

Let $m \in \mathbb{N}$. Then $H_m(n) \neq \emptyset$ for all $n \in 4\mathbb{N}$.

Solved cases (chronological)

1. $m = 12$: Marrero-Butson [1972]. (They only mention $m = 6$)
2. $m = 32$: E-Kervaire [2001, 2005]. (The current record)
3. $m = 5$: Lee-Szöllősi [2014].
4. $m = 7, 11$: Kuperberg [2016]. Asymptotic solution.
   [E.g. for $m = 7$, solution for $n \geq 4.5 \cdot 10^{36}$]

▷ The case $m \in 4\mathbb{N}$ is closer to the classical one: for $n \geq 3$,

$$H_m(n) \neq \emptyset \implies n \in 4\mathbb{N}.$$

[Proof as in the classical case]

▷ Remainder of the talk: some progress towards the case $m = 64$.

From modular to classical

Of course, $H_0(n) \subseteq H_m(n)$ for all m, n. Conversely:

Lemma

If $m > n$, then $H_m(n) = H_0(n)$.

Proof.

The dot product of two $\{\pm 1\}$-rows of size n lies in $[-n, n]$. If it is 0 mod m where $m > n$, then it is 0. □

Corollary

Hadamard's conjecture holds if and only if its m-modular version holds for infinitely many $m \in \mathbb{N}$.

▷ Hence a powerful incentive to tackle the m-modular version for m as large as possible. For instance, for $m \in \{2^k \mid k \geq 1\}$.

Autocorrelation coefficients

Let $A=(a_0,\ldots,a_{\ell-1})$ be a ± 1 sequence. For $0\le k\le \ell-1$, the kth-aperiodic correlation coefficient is

$$c_k(A)=\sum_{i=0}^{\ell-1-k} a_i a_{i+k}.$$

E.g. $c_0(A)=\sum a_i^2=\ell$, $c_{\ell-1}(A)=a_0 a_{\ell-1}$. The Hall polynomial of A is

$$A(z)=\sum_{i=0}^{\ell-1} a_i z^i.$$

The $c_k(A)$ show up in this formula in $\mathbb{Z}[z,z^{-1}]$:

$$A(z)A(z^{-1})=c_0(A)+\sum_{k=1}^{\ell-1} c_k(A)(z^k+z^{-k}).$$

Golay quadruples

▷ A **Golay quadruple** is a quadruple (A, B, C, D) of ± 1 sequences of same length ℓ such that $c_k(A) + c_k(B) + c_k(C) + c_k(D) = 0$ for all $1 \leq k \leq \ell - 1$. Equivalently,

$$A(z)A(z^{-1}) + B(z)B(z^{-1}) + C(z)C(z^{-1}) + D(z)D(z^{-1}) = 4\ell.$$

▷ An ***m*-modular Golay quadruple** satisfies the weaker condition $c_k(A) + c_k(B) + c_k(C) + c_k(D) \equiv 0 \bmod m$ for all $1 \leq k \leq \ell - 1$. Equivalently,

$$A(z)A(z^{-1}) + B(z)B(z^{-1}) + C(z)C(z^{-1}) + D(z)D(z^{-1}) \equiv 4\ell \bmod m.$$

▷ Notation:

$$GQ_m(\ell) = \text{set of } m\text{-modular Golay quadruples of length } \ell.$$

From Golay to Hadamard

Theorem

There is a map $GQ_m(\ell) \to H_m(4\ell)$.

Proof.

Let $(A, B, C, D) \in GQ_m(\ell)$. Still denote by A, B, C, D their respective circulant matrices. Put them in the Goethals-Seidel array:

$$M = GS(A,B,C,D) = \begin{pmatrix} A & -BR & -CR & -DR \\ BR & A & -D^T R & C^T R \\ CR & D^T R & A & -B^T R \\ DR & -C^T R & B^T R & A \end{pmatrix}$$

where R is the *anti-identity*. Then $MM^T \in H_m(4\ell)$. □

The Golay-Turyn Conjecture [1951, 1974]

There is a Golay quadruple of any length $\ell \geq 1$.

▷ It implies Hadamard's conjecture.

▷ It implies Lagrange's four-square theorem:

Every $n \in \mathbb{N}$ is the sum of four squares of integers.

[In $A(z)A(z^{-1}) + B(z)B(z^{-1}) + C(z)C(z^{-1}) + D(z)D(z^{-1}) = 4\ell$, set $z = 1$]

The *m*-modular version

Let $m \in \mathbb{N}$. There is an m-modular Golay quadruple of any length $\ell \geq 1$.

▷ Highest currently solved modulus: $m = 16$.

▷ For $m = 32$: almost complete solution, only open for $\ell \equiv 13 \bmod 16$.

Linear families of 64-modular GQ

Proposition

There are 64-modular Golay quadruples of length ℓ for:

- ℓ *even* mod 16
- $\ell \equiv 1,3,5 \bmod 16$
- $\ell \equiv 7 \bmod 32$

- The cases $\ell \equiv 1,5 \bmod 16$ are from [E-Kervaire, 2005].
- The case $\ell \equiv 3 \bmod 16$ is from [E, unpublished, 2022].
- The case $\ell \equiv 7 \bmod 32$ is from [E, unpublished, May 2025]. It is especially interesting: for $\ell = 167 = 32 \cdot 5 + 7$,

$$4\ell = 668.$$

Ingredients

▷ Consider the involution $'$: $\{\pm 1\}^\ell \to \{\pm 1\}^\ell$ given by

$$s = (x_1, \dots, x_\ell) \mapsto s' = (x_1, \dots, x_{h-1}, -x_h, \dots, -x_\ell)$$

where $h = \lceil \ell/2 \rceil$. A **special pair** is a pair of the form (s, s').

▷ A **special quadruple** is a quadruple of the form (s, s', t, t') with $s, t \in \{\pm 1\}^\ell$.

▷ We seek special Golay quadruples.

▷ A good comparator is $q \in \{\pm 1\}^\ell$ s.t. there exists $s \in \{\pm 1\}^\ell$ s.t.

$$(s, s', qs, (qs)')$$

is a Golay quadruple. (Or m-good in the m-modular case.)

Solutions

Here are 64-modular Golay quadruples $(s, s', qs, (qs)')$ *in run-length code*. (For instance, $++---+$ is coded as 231.)

▷ Length $\ell = 16k + 3$ [Summer 2022]:

$$q = (8k+1)2(8k-1)1$$
$$s = 4^k(211)^k212(112)^{k-1}134^{k-1}11$$

▷ Length $\ell = 32k + 7$ [May 2025]:

$$q = (16k+3)2(16k+1)1$$
$$s = 4^k(211)^k(15)4^{k-1}(211)^{k+1}4^{k-1}3(121)^k34^{k-1}3(121)^k$$

▷ They yield 64-modular Hadamard matrices of order 4ℓ for all such ℓ, via the Goethals-Seidel array. In particular, for $668 = 4 \cdot 167$. Result:

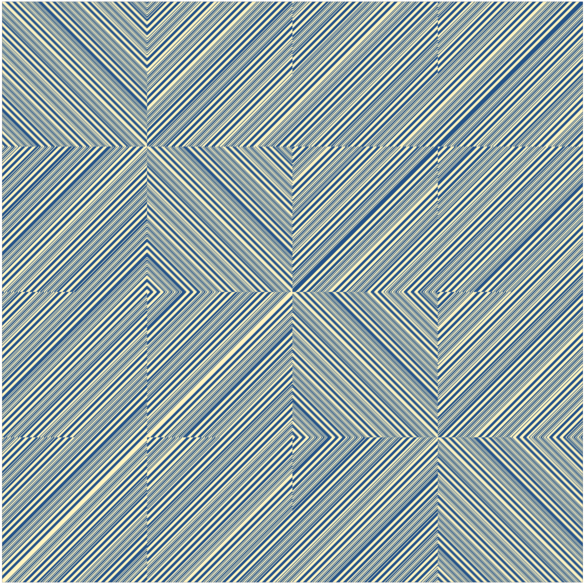

Figure: A 64-modular Hadamard matrix A of order 668

Some features of A

▷ **Interesting ones:** each row of AA^T, of length 668, counts

- 641 true zeros,
- hence 26 nonzero off-diagonal entries, all in the set

$$64 \cdot \{-1, 2, -3, 4, -4, -5, 6, -8\},$$

with respective multiplicities $(4, 6, 4, 4, 2, 2, 2, 2)$.

▷ **Less interesting ones:**

- $n^{0.79\,n/2} < |\det(A)| < n^{0.8\,n/2}$. But for a random binary matrix B of order $n = 668$, one often gets $|\det(B)| \sim n^{0.84\,n/2}$.
- A contains a partial Hadamard submatrix of order 64×668. But there is one of order 332×668... by concatenating Hadamard matrices of order 332 and 336. Is it the current record?

Upshot

▷ For orders $n = 4\ell$ with ℓ odd, the 64-modular Hadamard conjecture is

- **settled** for $\ell \equiv 1, 3, 5 \bmod 16$ and $\ell \equiv 7 \bmod 32$
- **open** for $\ell \equiv 9, 11, 13, 15 \bmod 16$ and $\ell \equiv 23 \bmod 32$

▷ In Hadamard's conjecture, the currently open cases below 1000 are $668, 716, 892$.

▷ In the 64-modular case, only 892 remains open in this range. Indeed,

$$668 = 4 \cdot 167 \text{ and } 167 \equiv 7 \bmod 32,$$
$$716 = 4 \cdot 179 \text{ and } 179 \equiv 3 \bmod 16.$$

Thank you for your attention!