

A 64-modular Hadamard matrix of order 668

SHALOM ELIAHOU*

Univ. Littoral Côte d'Opale

UR 2597 - LMPA - Laboratoire de Mathématiques Pures et Appliquées

Joseph Liouville, F-62100 Calais, France

`shalom.eliahou@univ-littoral.fr`

Abstract

Since 2005, the smallest open case in Hadamard's conjecture from 1893 is $n = 668$. A 32-modular Hadamard matrix of that order has been known since 2001, and the modulus $m = 32$ has remained the record since then. In this note, we improve it and reach $m = 64$, by constructing a square matrix H of order $n = 668$, with coefficients ± 1 , such that $HH^\top \equiv nI_n \pmod{64}$.

1 Introduction

A *Hadamard matrix* is a square matrix H of order n , with entries ± 1 exclusively, satisfying

$$HH^\top = nI_n.$$

Hadamard's conjecture (1893) states that there exists a Hadamard matrix of order n for every $n \in 4\mathbb{N} = \{4\ell \mid \ell \in \mathbb{N}\}$. At the time of writing, the remaining open cases $n \leq 1000$ in Hadamard's conjecture are 668, 716 and 892. In sharp contrast, the density of open cases in the whole of $4\mathbb{N}$ remains frozen at 1. Illustrating the slowness of progress on this problem, the two predecessors of 668 as smallest open case in Hadamard's conjecture are 268 and 428, solved in 1985 by Sawade [14] and in 2005 by Kharaghani and Tayfeh-Rezaie [9], respectively.

Given an integer $m \in \mathbb{N}$, an *m -modular Hadamard matrix* is still a square matrix H of order n with entries ± 1 , but satisfying the weaker condition

$$HH^\top \equiv nI_n \pmod{m}.$$

(The case $m = 0$ corresponds to true Hadamard matrices.) This notion was introduced by Marrero and Butson [12, 13]. The m -modular version of Hadamard's conjecture states that there exists an m -modular Hadamard matrix of order n for every $n \in 4\mathbb{N}$.

* Also at: CNRS, FR 2037, France.

While true Hadamard matrices are m -modular Hadamard matrices for all $m \in \mathbb{N}$, a modest partial converse holds: *any m -modular Hadamard matrix of order $n < m$ is a true Hadamard matrix.* Indeed, the dot product of two rows with entries ± 1 is an integer $k \in [-n, n]$, and $[-n, n] \cap m\mathbb{Z} = \{0\}$ whenever $m > n$. This has the following consequence. See e.g. [2, 3].

Proposition 1.1. *Hadamard’s conjecture is equivalent to the validity of the m -modular Hadamard’s conjecture for any infinite set of moduli m .*

This observation yields a powerful incentive to tackle the m -modular Hadamard’s conjecture for moduli $m \in \mathbb{N}$ as large as possible, as a sort of staircase to Hadamard’s conjecture proper.

The m -modular Hadamard conjecture has been solved for $m = 32$ in [2], the record since 2001. For completeness, it is currently solved for $m \in \{5, 12, 32\}$ and their divisors only. The cases $m = 5$ and $m = 12$ are achieved in [11] and [12, 13], respectively. There are also asymptotic solutions (i.e., for large orders $n \in 4\mathbb{N}$ only) for $m \in \{7, 11\}$ in [10].

The purpose of this note is to tackle the widely open case $m = 64$ and present a 64-modular Hadamard matrix of order $n = 668$. More generally, in a forthcoming paper [4], we shall construct 64-modular Hadamard matrices for all orders $n = 4\ell$ such that $\ell \in \mathbb{N}$ is congruent to either 1, 3 or 5 mod 16, or 7 mod 32. This result was first presented in May 2025 at the conference *Hadamard 2025* in Sevilla [8]. Note that $668 = 4 \cdot 167$ and $167 \equiv 7 \pmod{32}$.

Our construction rests on Golay quadruples, their m -modular counterparts, and the Goethals-Seidel array which produces Hadamard matrices of order 4ℓ from Golay quadruples of length ℓ .

See [15] for a general reference on construction methods of Hadamard matrices.

2 Golay pairs and quadruples

Let $s = (a_0, \dots, a_{\ell-1})$ be a sequence of length ℓ in some commutative ring R . For $k \geq 0$, the k th *aperiodic autocorrelation coefficient* of s is

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

Definition 2.1. A *Golay pair* is a pair (A, B) of ± 1 sequences of length ℓ such that for all $1 \leq k \leq \ell - 1$, one has

$$c_k(A) + c_k(B) = 0. \tag{1}$$

Definition 2.2. A *Golay quadruple* is a quadruple (A, B, C, D) of ± 1 sequences of length ℓ such that for all $1 \leq k \leq \ell - 1$, one has

$$c_k(A) + c_k(B) + c_k(C) + c_k(D) = 0. \tag{2}$$

Golay pairs and quadruples were introduced under the names *complementary series* and *supplementary series* in [6, 7].

As with Hadamard matrices, there are modular versions of Golay pairs and quadruples, obtained by replacing the equalities (1) and (2) by congruences mod m , i.e.

$$c_k(A) + c_k(B) \equiv 0 \pmod m \tag{3}$$

and

$$c_k(A) + c_k(B) + c_k(C) + c_k(D) \equiv 0 \pmod m \tag{4}$$

for all $1 \leq k \leq \ell - 1$, respectively. These variants were introduced in [1] and [2], respectively.

It is well-known, since the work of Goethals and Seidel in [5], that Golay quadruples give rise to Hadamard matrices. This link effortlessly extends to the m -modular context [2, 3].

Theorem 2.3. *Let $m \in \mathbb{N}$. An m -modular Golay quadruple of length ℓ gives rise to an m -modular Hadamard matrix of order 4ℓ .*

Proof. Let (A, B, C, D) be an m -modular Golay quadruple of length ℓ . 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* matrix, i.e. with $R_{i,\ell+1-i} = 1$ for all i and 0 elsewhere. Then M is an m -modular Hadamard matrix of order $n = 4\ell$. □

The Golay-Turyn conjecture, informally stated in [7, 16], postulates that there exists a Golay quadruple of any length $\ell \in \mathbb{N}$.

2.1 Special Golay quadruples

Our strategy for constructing m -modular Golay quadruples is to search for ones of a very special form that we now describe. Consider the involution $' : \{\pm 1\}^\ell \rightarrow \{\pm 1\}^\ell$ given by

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

where $h = \lceil \ell/2 \rceil$. In words, this map switches all signs in the second half of s if $\ell = 2h$, and in its short second half if $\ell = 2h - 1$.

For any $s \in \{\pm 1\}^\ell$, the pair (s, s') enjoys the property that $c_k(s) + c_k(s') = 0$ for all $k \geq \lceil \ell/2 \rceil$, as easily verified. Hence, for quadruples (A, B, C, D) of the form (s, s', t, t') with $s, t \in \{\pm 1\}^\ell$, half of the Golay conditions in (2) or (4) are already satisfied.

Golay quadruples of this special form seem to be quite abundant and might possibly exist in every length ℓ . (This would be a sharper form of the above-mentioned

Golay-Turyn conjecture.) Now, in actual m -modular Golay quadruples (s, s', t, t') , the Hadamard component-wise product $q = st$ tends to have a simpler structure than that of s and t . See Fact 3.1 below for a sharp illustration.

The above comments lead to the following search strategy. We first look for relatively simple sequences $q \in \{\pm 1\}^\ell$ whose pattern looks promising based on solutions of smaller length. We then search for sequences $s \in \{\pm 1\}^\ell$, if any, such that the quadruple

$$(s, s', (sq), (sq)')$$

has the desired property.

3 The case $m = 64$ and $n = 668$

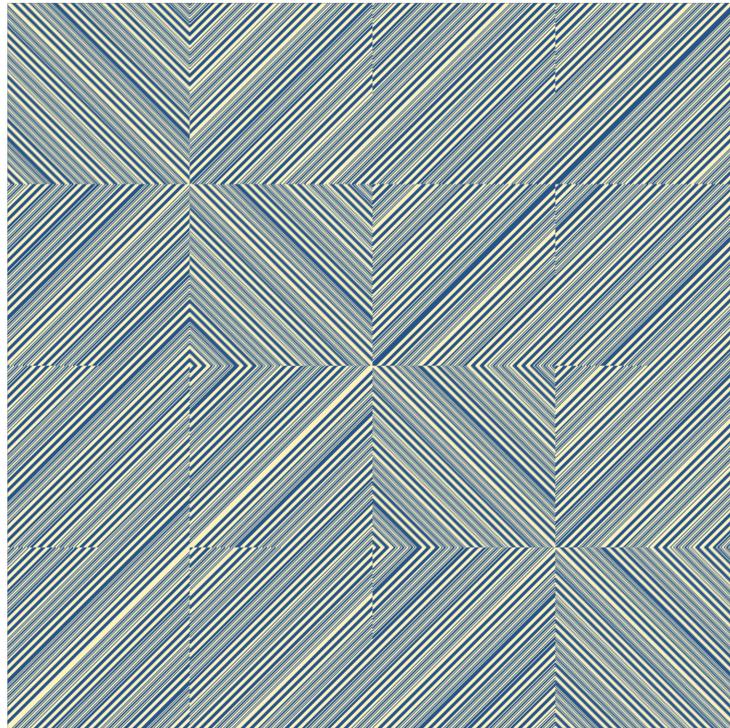


Figure 1: A 64-modular Hadamard matrix of order $n = 668$

We may now construct a 64-modular Hadamard matrix of order $n = 668$. It rests on a special 64-modular Golay quadruple $(s, s', (sq), (sq)')$ of length $\ell = n/4 = 167$ and on Theorem 2.3. This quadruple was found through a mix of theory, computer experiments and some guesswork on patterns spotted at shorter lengths. More details on this construction will be given in [4].

To exhibit our binary sequences, we use the *run-length encoding*, which gives the lengths of the successive maximal constant subsequences. We also need a more

compact form of that encoding. For instance, consider the following binary sequence of length 22:

$$++++-----++-+-++-++++.$$

Its run-length encoding is $(4, 4, 2, 1, 2, 1, 2, 1, 5)$, and $(4)^2(2, 1)^3(5)$ in more compact form.

Fact 3.1. *Let $q, s \in \{\pm 1\}^{167}$ be the binary sequences encoded as follows and starting with +1:*

$$q : (83, 2, 81, 1)$$

$$s : (4)^5(2, 1, 1)^5(1, 5)(4)^4(2, 1, 1)^6(4)^4(3)(1, 2, 1)^5(3)(4)^4(3)(1, 2, 1)^5$$

Let $(A, B, C, D) = (s, s', (sq), (sq)')$ and $H = GS(A, B, C, D)$. Then (A, B, C, D) is a 64-modular Golay quadruple of length $\ell = 167$, and H is a 64-modular Hadamard matrix of order $4\ell = 668$.

The matrix H is displayed in Figure 1, with +1 coded in pale yellow and -1 in dark blue. The statement on (A, B, C, D) is easy to verify by computer. More specifically, denoting $c_i = c_i(A) + c_i(B) + c_i(C) + c_i(D)$ for $1 \leq i \leq 166$, these 166 integer coefficients c_i are all 0 with the following 13 exceptions:

c_4	c_8	c_{12}	c_{16}	c_{26}	c_{30}	c_{34}	c_{38}	c_{42}	c_{46}	c_{50}	c_{54}	c_{58}
-512	384	-256	128	-64	128	-192	256	-320	256	-192	128	-64

The statement on the matrix H follows from Theorem 2.3. Here are some details on H and its Gram matrix $G = HH^T$:

- Each row of H is truly orthogonal (i.e. over \mathbb{Z}) to 641 other rows of H . That is, each row of G contains 641 true zeros.
- In each row of G , the only 26 nonzero off-diagonal entries are

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

of multiplicity 4, 6, 4, 4, 2, 2, 2, 2, respectively.

Conclusion

To the best of our knowledge, the matrix H constructed in this note is the closest approximation to date of the still elusive true Hadamard matrices of order $n = 668$. It is a significant improvement upon the previous best approximation, dating back to 2001, namely by a 32-modular Hadamard matrix of this order [2]. It will be interesting to see how long that new record will remain in place. Or, for that matter, for how many more years the order $n = 668$ will remain the smallest open case in Hadamard’s conjecture proper.

Acknowledgements

The author would like to thank the Editors of this journal whose extremely efficient help and comments made the publication of this note in its present form possible.

References

- [1] S. Eliahou, M. Kervaire and B. Saffari, On Golay Polynomial Pairs, *Adv. Appl. Math.* 12 (1991), 235–292.
- [2] S. Eliahou and M. Kervaire, Modular sequences and modular Hadamard matrices, *J. Combin. Des.* 9 (2001), 187–214.
- [3] S. Eliahou and M. Kervaire, A Survey on Modular Hadamard Matrices, *Discrete Math.* 302 (2005), 85–106.
- [4] S. Eliahou, An update on modular Hadamard matrices, (in preparation).
- [5] J. M. Goethals and J. J. Seidel, A skew Hadamard matrix of order 36, *J. Aust. Math. Soc. A* 11 (1970), 343–344.
- [6] M. J. E. Golay, Multi-Slit Spectrometry, *J. Opt. Soc. Amer.* 39 (1949), 437–444.
- [7] M. J. E. Golay, Static Multislit Spectrometry and Its Application to the Panoramic Display of Infrared Spectra, *J. Opt. Soc. Amer.* 41 (1951), 468–472.
- [8] Hadamard 2025: 8th Workshop on Design Theory, Hadamard Matrices and Applications, <https://gestioneventos.us.es/hadamard2025>
- [9] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428, *J. Combin. Des.* 13 (2005), 435–440.
- [10] V. Kuperberg, Hadamard matrices modulo p and small modular Hadamard matrices, *J. Combin. Des.* 24 (2016), 393–405.
- [11] M. H. Lee and F. Szöllősi, Hadamard matrices modulo 5, *J. Combin. Des.* 22 (2014), 171–178.
- [12] O. Marrero and A. T. Butson, Modular Hadamard matrices and related designs II, *Canad. J. Math.* 24 (1972), 1100–1109.
- [13] O. Marrero and A. T. Butson, Modular Hadamard matrices and related designs, *J. Combin. Theory, Ser. A* 15 (1973), 257–269.
- [14] K. Sawade, A Hadamard matrix of order 268, *Graphs Combin.* 1 (1985), 185–187.
- [15] J. R. Seberry and M. Yamada, *Hadamard matrices—constructions using number theory and algebra*, John Wiley, 2020.
- [16] R. Turyn, Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings, *J. Combin. Theory, Ser. A* 16 (1974), 313–333.

(Received 24 Sep 2025)