A structured form of the Hadamard matrix conjecture

Ilias S. Kotsireas

Wilfrid Laurier University

Waterloo ON, Canada

ikotsire@wlu.ca

Hadamard matrices

Hadamard matrices are $n \times n$ matrices H with ± 1 elements such that $H \cdot H^t = nI_n$.

trivial cases: $n = 1$ and $n = 2$.

well-known necessary condition: $n \equiv 0 \pmod 4$
J. H. van Lint & R. M. Wilson, A course in combinatorics. 2nd ed. CUP 2001.

the sufficiency of this condition is the celebrated Hadamard (matrix) conjecture

"There exists a Hadamard matrix of order n, for every $n \equiv 0 \pmod 4$" (1893)

- smallest unresolved order until 1985: 268
- smallest unresolved order until 2004: 428
- smallest unresolved order until 2014: 668

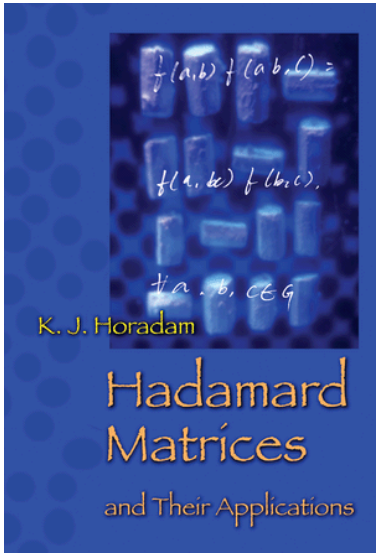
3 unresolved cases < 1000: $668, 716, 892$

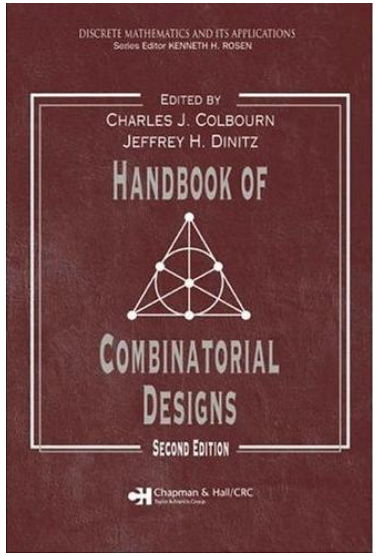
10 unresolved cases < 2000: $1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, 1964$

recent progress: HM of order $1004 = 4 \cdot 251$,
D. Z. Djokovic, O. Golubitsky, I. S. Kotsireas, JCD 22 (2014), no. 6, pp. 270-277.

How many (inequivalent) HMs are there?

Two HMs are **inequivalent** if one cannot be obtained from the other by a series of row/col permutations and/or by multiplying some rows or columns by -1.





- C. Lam, S. Lam, V. D. Tonchev, Bounds on the number of affine, symmetric, and Hadamard designs and matrices. JCTA 92 (2000), no. 2, 186-196.
- C. Lam, S. Lam, V. D. Tonchev, Bounds on the number of Hadamard designs of even order. JCD 9 (2001), no. 5, 363-378.

The number of inequivalent Hadamard matrices of order 40 is at least 3.66×10^{11}.

Constructions for Hadamard matrices

1. Kronecker product construction: $HM(n), HM(m) \longrightarrow HM(nm)$
2. Gruner's theorem: if p and $p+2$ are twin primes, then $\exists \;\; HM(p(p+2)+1)$
3. Quadratic Residues of primes $p \equiv 3 \pmod 4$, `{seq(x^2 mod p,x=1..p)}`
4. Williamson method (1944), Williamson array

$$\begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

where A, B, C, D are symmetric circulant matrices of (odd) order n satisfying $A^2 + B^2 + C^2 + D^2 = (4n) \cdot I_n$

- Williamson's method gave all HMs of order less that 100.
- HM(92), L. D. Baumert, S. W. Golomb, and M. Hall (1962)
  `http://blogs.jpl.nasa.gov/2013/08/slice-of-history-hadamard-matrix/`
- R. Turyn, An infinite class of Hadamard matrices. JCTA 12, (1972)

Problems with HM constructions

"For a long time, Williamson's method has been considered a promising way to tackle the Hadamard conjecture " – Bernhard Schmidt (AMS MathSciNet review)

- D. Z. Djokovic, Discrete Math. 115, pp. 267-271 (1993),
  Williamson method fails for $n = 35$
- W. H. Holzmann, et al. Designs Codes Cryptogr. 46, pp. 343-352 (2008)
  Williamson method fails for $n = 47, 53, 59$

There are literally $100s$ of HM constructions ...
They all suffer from two kinds of disadvantages:

- they produce a **sparse** set of orders
- they **fail** for specific parameter values

Opinion: The Hadamard conjecture is too general.

There is one particular construction that seems to be one of the most prominent candidates to furnish a proof of the Hadamard conjecture:

two circulant cores construction (2cc)

- 2cc introduces some **structure** into the more general Hadamard Conjecture. This structure is described in terms of two circulant matrices whose first rows have constant autocorrelation.
- 2cc **does not fail** for any value of the parameter, covers full range of multiples of 4.

1. I. S. Kotsireas, J. Seberry et al. Hadamard ideals and Hadamard matrices with two circulant cores
   European J. Combin., 27(5):658–668, 2006.
2. I. S. Kotsireas, Structured Hadamard Conjecture
   Springer Proceedings in Mathematics & Statistics Volume 43, 2013, pp. 215–227
   in: Number Theory and Related Areas Eds: J. M. Borwein, I. Shparlinski, and W. Zudilin
3. I. S. Kotsireas, A. Razoumov, work in progress, 2014, JPDC

Circulant matrices
Periodic Autocorrelation Function

A $n \times n$ matrix $C(A)$ is called **circulant** if every row (except the first) is obtained by the previous row by a right cyclic shift by one.

$$C(A) = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_2 & a_3 & \dots & a_0 & a_1 \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \end{bmatrix}$$

The **periodic autocorrelation function (PAF)** of a finite sequence $A = [a_0, \dots, a_{n-1}]$ is defined as: ($k + s$ is taken modulo n)

$$P_A(s) = \sum_{k=0}^{n-1} a_k a_{k+s}, \ \ s = 0, \dots, n-1,$$

PAF properties

- Consider a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n and the circulant matrix $C(A)$ whose first row is equal to A.

  Then $P_A(i)$ is the inner product of the first row of $C(A)$ and the $i+1$ row of $C(A)$.

- **symmetry property**

$$P_A(s) = P_A(n-s), s = 1, \ldots, n-1.$$

- **2^{nd} ESF property**

$$P_A(1) + P_A(2) + \ldots + P_A(n-1) = 2e_2(a_0, \ldots, a_{n-1})$$

2cc construction for Hadamard matrices

Let ℓ be an odd integer, such that $\ell > 1$ and set $m = \frac{\ell-1}{2}$. If there exist two ± 1 sequences $A = [a_0, \ldots, a_{\ell-1}]$ and $B = [b_0, \ldots, b_{\ell-1}]$ of length ℓ each, such that

$$P_A(s) + P_B(s) = -2, \text{ for } s = 1, \ldots, m$$

then $\exists$ a 2cc Hadamard matrix of order $2\ell + 2$ given by

$$H_{2\ell+2} = \left[\begin{array}{cc|ccc} - & - & + & \cdots & + \\ - & + & + & \cdots & + \\ \hline + & + & & & \\ \vdots & \vdots & \multicolumn{3}{c}{C(A) \qquad C(B)} \\ + & + & & & \\ \hline + & - & & & \\ \vdots & \vdots & \multicolumn{3}{c}{C(B)^t \qquad -C(A)^t} \\ + & - & & & \end{array}\right]$$

Example: Let $\ell = 5$, $m = 2$ and consider the two sequences $A = [1, 1, -1, -1, 1]$ and $B = [-1, 1, -1, 1, 1]$. Then we have that

s	$P_A(s)$	$P_B(s)$	$P_A(s) + P_B(s)$
1	1	-3	-2
2	-3	1	-2

and the corresponding 2cc matrix H_{12} is a 12×12 Hadamard matrix.

Necessary condition:

$$(a_0 + \cdots + a_{\ell-1})^2 + (b_0 + \cdots + b_{\ell-1})^2 = 2$$

w.l.o.g. $a_0 + \cdots + a_{\ell-1} = 1$ and $b_0 + \cdots + b_{\ell-1} = 1$.

ℓ	order of $H_{2\ell+2}$	total number of matrices			
3	8	9	=	1×3^2	exhaustive searches for 2cc Hadamard matrices
5	12	50	=	2×5^2	
7	16	196	=	4×7^2	
9	20	972	=	12×9^2	
11	24	2,904	=	24×11^2	
13	28	7,098	=	42×13^2	
15	32	38,700	=	172×15^2	
17	36	93,058	=	322×17^2	
19	40	161,728	=	448×19^2	
21	44	433,944	=	984×21^2	
23	48	1,235,744	=	$2,336 \times 23^2$	
25	52	2,075,000	=	$3,320 \times 25^2$	
27	56	5,353,776	=	$7,344 \times 27^2$	
29	60	12,401,386	=	$14,746 \times 29^2$	
31	64	22,472,024	=	$23,384 \times 31^2$	

Commutative Algebra formulation of the structured Hadamard conjecture

Consider the polynomial ring in 2ℓ variables $a_0, \ldots, a_{\ell-1}$, $b_0, \ldots, b_{\ell-1}$.

Set $m = \frac{\ell-1}{2}$.

Consider the ideal defined by $m + 2 + 2\ell$ linear and quadratic polynomials

$$\begin{aligned} \mathcal{H}_\ell = \quad & \langle P_A(1) + P_B(1) + 2, \ldots, P_A(m) + P_B(m) + 2, \\ & a_0 + \ldots + a_{\ell-1} - 1, b_0 + \ldots + b_{\ell-1} - 1, \\ & a_0^2 - 1, \ldots, a_{\ell-1}^2 - 1, b_0^2 - 1, \ldots, b_{\ell-1}^2 - 1 \rangle \end{aligned}$$

The structured Hadamard conjecture amounts in proving that the ideal $\mathcal{H}_\ell$ is non-empty, for all odd $\ell > 1$.

Exact formulas for # of Hadamard matrices of order n

1. Shalom Eliahou
   Enumerative combinatorics and coding theory
   Enseign. Math. (2), 40(1-2):171–185, 1994.

2. Warwick de Launey and Daniel A. Levin
   A Fourier-analytic approach to counting partial Hadamard matrices
   Cryptogr. Commun., 2(2):307–334, 2010.

- The Eliahou formula uses Coding Theory.
- The de Launey-Levin formula uses multidimensional integrals associated with lattice walks.
- Both formulas require a certain amount of technical definitions before they can be stated in a self-contained manner and are difficult (practically impossible) to evaluate for large n.
- It is far from evident why these two formulae (should) agree for all $n \equiv 0 \pmod 4$.

Eliahou Theory

Fundamental link between the number of solutions of polynomial equations (in binary variables) with positive integer coefficients and certain associated binary linear codes and their weight enumerators.

- Let $f(x_1, \ldots, x_n)$ be a polynomial with non-negative integer coefficients. Then the enumeration of the values assumed by f on the boolean cube $\{-1, +1\}^n$ is equivalent to the enumeration of the weights in an associated binary linear code L_f.
- This correspondence in conjunction with the MacWilliams identity is used to enumerate Hadamard matrices of fixed order.
- **Question:** Is there a $p \in \{-1, +1\}^n$ s.t. $f(p) = 0$?
- How many such binary zeros does f admit?
- The **value enumerator** of f is the Laurent polynomial in T, T^{-1}:

$$V_f(T) = \sum_{p \in \{-1,+1\}^n} T^{f(p)}$$

- The coefficient of T^u in $V_f(T)$ is the # binary points p s.t. $f(p) = u$, $u \in Z$.

- w.l.o.g. we can consider polynomials f that are composed of **square-free** monomials only.
- removing squares does not alter the value of f: $x^2y - y$ takes the constant value 0
- Let M_n denote the set of square-free monomials in the n variables $x_1, \ldots, x_n$.
- Let f be decomposed as $f = u_1 + \cdots + u_N$ with monomials $u_i \in M_n, i = 1, \ldots, N$. The monomials u_i need not be distinct and they can be equal to 1.
- Associate with f the $n \times N$ matrix $\Phi_f = (\Phi_{ij})$ over F_2 defined by

$$\Phi_{ij} = \begin{cases} 1, \text{if } x_i \text{ divides } u_j \\ 0, \text{otherwise} \end{cases}$$

- Define L_f to be the binary linear code generated by the n rows of the matrix Φ_f.
- The dual code $K_f = L_f^{\perp}$ admits Φ_f as a parity check matrix.
- Alternative description of the code L_f: with a $p \in \{-1, +1\}^n$ we associate:
  (1) a **subset** $v_f(p) \subset \{1, \ldots, N\}$ defined as: $v_f(p) = \{i \in [1, \ldots, n] \mid u_i(p) = -1\}$
  (2) a **codeword** $c_f(p)$ in F_2^N defined as: $c_f(p) = \sum_{i \in v_f(p)}$ where $E_1, \ldots, E_N$ is the standard basis of F_2^N.

- This defines a **MAP** (group homomorphism) $c_f : \{-1,+1\}^n \to F_2^N$ with properties:

$$Im(c_f) = L_f \qquad Ker(c_f) = \{p \mid f(p) = N\} \qquad f(p) = N - 2 \mid c(p) \mid$$

- Theorem: (the weight enumerator of $_f$ determines the value enumerator of f)

$$V_f(T) = 2^{n-\dim L_f} T^N P_L(1/T^2)$$

- For every $u \in Z$, the **binary fiber** of u is defined as

$$f^{-1}(u) = \{p \in \{-1,+1\}^n | f(p) = u\}.$$

- Eliahou theory furnishes a way to compute the cardinality of the binary fiber, $\forall u \in Z$.

  Theorem:

  $$|f^{-1}(u)| = 2^{n-\dim L_f} \cdot \text{ coefficient of } (XY)^{(N-u)/2} \text{ in the weight enumerator of } L_f$$

  Note that we make use of the **bivariate** weight enumerator of L_f.

Many (but not all) combinatorial objects that are defined via $\{-1,+1\}$ sequences of constant autocorrelation can be defined as solutions of systems of polynomial equations $f_1(x_i) = \cdots = f_k(x_i) = 0$ over the boolean cube, which can be reduced to one equation $f = f_1^2 + \ldots + f_k^2$.

Eliahou Theory for 2cc HMs

Set $f_H = \sum_{s=1}^{m} (P_A(s) + P_B(s) + 2)^2$, $m = \dfrac{\ell - 1}{2}$ and compute the cardinality of the binary fiber of 0, for f_H (polynomial in 2ℓ variables a_i, b_i).

Example: $\ell = 3$, $n = 2\ell = 6$, $m = 1$,
$f_H = (P_A(1) + P_B(1) + 2)^2 = (a_1a_2 + a_2a_3 + a_3a_1 + b_1b_2 + b_2b_3 + b_3b_1 + 2)^2$
$f_H = 5 + 3(P_A(1) + P_B(1)) + P_A(1)P_B(1)$
which implies that f_H has $N = 5 + 3 \cdot 6 + 9 = 32$ and the associated 6×32 matrix Φ_{f_H} is

$$\begin{bmatrix}
0,0,0,0,0,1,1,1,0,0,0,1,1,1,1,1,1,0,0,0,1,1,1,0,0,0,0,0,0,0,0,0 \\
0,0,0,0,0,1,1,1,1,1,1,0,0,0,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0 \\
0,0,0,0,0,0,0,0,1,1,1,1,1,1,0,0,0,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0 \\
0,0,0,0,0,1,0,1,1,0,1,1,0,1,0,0,0,0,0,0,0,0,0,1,1,1,0,0,0,1,1,1 \\
0,0,0,0,0,1,1,0,1,1,0,1,1,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,0,0,0 \\
0,0,0,0,0,0,1,1,0,1,1,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1
\end{bmatrix}$$

Let L_{f_H} denote the binary linear code generated by the 6 rows of the matrix Φ_{f_H}.

The bivariate weight enumerator of the binary linear code L_{f_H} can be computed with Magma:

$$X^{32} + 6X^{20}Y^{12} + 9X^{16}Y^{16}.$$

The dimension of the binary linear code L_{f_H} can also be computed in Magma and is equal to 4.

$$\begin{aligned} |f^{-1}(0)| &= 2^{n-\dim L_{f_H}} \cdot \text{ coefficient of } (XY)^{N/2} \text{ in the weight enumerator of } L_{f_H} = \\ &= 2^{6-4} \cdot 9 = 4 \cdot 9 = 36 \end{aligned}$$

which means that the equation $f_H = 0$ has 36 solutions in $\{-1, +1\}^6$.

we constructed the codes L_{f_H} and computed their weight enumerators for $\ell = 3$, 5, 7, 9, 11, 13, 15, 17, 19 using Magma.

ℓ	$n(=2\ell)$	N	$\dim L_{f_H}$	coeff. of $X^{N/2}Y^{N/2}$ in the weight enum. of L_{f_H}
3	6	32	4	9
5	10	144	8	50
7	14	384	12	196
9	18	800	16	972
11	22	1440	20	2,904
13	26	2352	24	7,098
15	30	3584	28	38,700
17	34	5184	32	93,058
19	38	7200	36	161,728

Table 1: Eliahou theory results for Hadamard matrices with two circulant cores

Coding Theory formulation of the structured Hadamard conjecture

For all odd $\ell > 1$, set $n = 2\ell, m = \frac{\ell-1}{2}$ and form

$$f_H = \sum_{s=1}^{m} (P_A(s) + P_B(s) + 2)^2$$

Reduce all the squares in f_H, i.e. compute N

Form the $n \times N$ matrix Φ_{f_H} and consider the binary linear code L_{f_H} it generates

Prove that $\dim L_{f_H} = 2\ell - 2$

Prove that there are codewords of weight $N/2$ in L_{f_H}