New constructions for Hadamard matrices

Paul Leopardi

Mathematical Sciences Institute, Australian National University.
For presentation at University of Newcastle.

26 April 2012

Acknowledgements

Richard Brent, Robert Craigen, Kathy Horadam,

Judy-anne Osborn, Jennifer Seberry.

Australian Research Council.

Australian Mathematical Sciences Institute.

Australian National University.

Topics

- Hadamard matrices
- Kronecker product constructions for Hadamard matrices
- Signed groups, Clifford algebras and representations
- Graphs of amicability and anti-amicability

When is the maximum determinant attained?

The *Hadamard maximal determinant problem* is:
"Given n, what is the largest possible determinant of an $n \times n$ matrix H with elements ± 1?"

Hadamard (1893) established an upper bound $n^{n/2}$, which is only attainable if the order n equals $1, 2,$ or a multiple of 4, and which only occurs when the rows of the matrix H are orthogonal.
In this case

$$H^T H = H H^T = n I_{(n)}.$$

It is a famous open problem, conjectured by Paley (1933), whether a *Hadamard matrix* exists for each order a multiple of 4.

Applications of Hadamard matrices

Applications include:

- Error-correcting codes.
  Mariner 9 (1971) used a code based on Hadamard matrices.
- Signal processing.
  The Walsh-Hadamard transform.
- Cryptography.
  The Walsh-Hadamard transform is used in the definition of *bent functions*.
- Quantum computing.
  Hadamard gates are well-known.
- Spectroscopy.

What is known about the Hadamard conjecture?

The conjecture is known to be true for all orders $n = 4k < 668$ (Kharaghani and Tayfeh-Rezaie, 2004).

There are density results due to de Launey and Gordon (2009, 2010), related to work by Horadam (2010), Seberry (1976), and Craigen and Kharaghani (1995, 2006).

If $S(x)$ is the number of $n \leqslant x$ for which a Hadamard matrix of order n exists, the Hadamard conjecture implies that $S(x) \geqslant x/4$. The result of de Launey and Gordon (2010) is

$$S(x) \geqslant \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right).$$

Equivalence classes of Hadamard matrices

If a Hadamard matrix H is multiplied on the left or on the right by a *signed permutation matrix* S, the result is again a Hadamard matrix.

These two types of operation are used to define an equivalence class where Hadamard matrices G and H are *Hadamard equivalent* if and only if there exist signed permutation matrices S and T such that

$$SG = HT.$$

The standard representative of each Hadamard equivalence class is usually taken to have positive first row and first column.

Kronecker product constructions (1)

We aim to find

$$A_k \in \{-1,0,1\}^{n\times n}, \quad B_k \in \{-1,1\}^{p\times p}, \quad k \in \{1,\ldots,n\},$$

such that

$$G = \sum_{k=1}^{n} B_k \otimes A_k, \quad GG^T = npI_{(np)}, \tag{G1}$$

$$H = \sum_{k=1}^{n} A_k \otimes B_k, \quad HH^T = npI_{(np)}. \tag{H1}$$

(Gastineau-Hills 1980, 1982)

Kronecker product constructions (2)

Since

$$HH^T = \sum_{j=1}^{n} A_j \otimes B_j \sum_{k=1}^{n} A_k^T \otimes B_k^T,$$

we impose the stronger conditions

$$\sum_{j=1}^{n} A_j A_j^T \otimes B_j B_j^T = npI_{(np)},$$

$$\sum_{j=1}^{n} \sum_{k=j+1}^{n} \left(A_j A_k^T \otimes B_j B_k^T + A_k A_j^T \otimes B_k B_j^T\right) = 0. \tag{H2}$$

Similarly, (G2) with Kronecker product reversed.

(Gastineau-Hills 1980, 1982)

Kronecker product constructions (3)

Stronger conditions:

$$\sum_{k=1}^{n} A_k A_k^T \otimes B_k B_k^T = np I_{(np)},$$
$$A_j A_k^T \otimes B_j B_k^T + A_k A_j^T \otimes B_k B_j^T = 0 \quad (j \neq k). \tag{H3}$$

Similarly, (G3) with Kronecker product reversed.

(Gastineau-Hills 1980, 1982)

Kronecker product constructions (4)

Still stronger conditions ($*$ is Hadamard product):

$$\begin{gathered}
A_j * A_k = 0 \quad (j \neq k), \quad \sum_{k=1}^{n} A_k \in \{-1, 1\}^{n \times n}, \\
A_k A_k^T = I_{(n)}, \\
\sum_{k=1}^{n} B_k B_k^T = np I_{(p)}, \\
A_j A_k^T + \lambda_{jk} A_k A_j^T = 0 \quad (j \neq k), \\
B_j B_k^T - \lambda_{jk} B_k B_j^T = 0 \quad (j \neq k), \\
\lambda_{jk} \in \{-1, 1\}.
\end{gathered} \tag{4}$$

(Gastineau-Hills 1980, 1982)

Example: Sylvester-like construction

$$A_1 = \begin{bmatrix} 1 & \cdot \\ \cdot & - \end{bmatrix}, \quad A_2 = \begin{bmatrix} \cdot & 1 \\ 1 & \cdot \end{bmatrix} \quad \Rightarrow \lambda_{12} = 1$$

$$\Rightarrow \text{ We need } \quad B_1 B_1^T + B_2 B_2^T = 2pI_{(p)}, \quad B_1 B_2^T - B_2 B_1^T = 0,$$

e.g.

$$B_1 = \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}, \quad B_2 = \begin{bmatrix} 1 & - \\ 1 & 1 \end{bmatrix},$$

$$G = \begin{bmatrix} 1 & 1 & 1 & - \\ 1 & - & - & - \\ 1 & 1 & - & 1 \\ 1 & - & 1 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 1 & 1 & - \\ 1 & - & 1 & 1 \\ 1 & - & - & - \\ 1 & 1 & - & 1 \end{bmatrix}.$$

Example: Anti-amicable construction

$$A_1 = \begin{bmatrix} 1 & . \\ . & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix} \quad \Rightarrow \lambda_{12} = -1$$

$$\Rightarrow \text{ We need } \quad B_1 B_1^T + B_2 B_2^T = 2pI_{(p)}, \quad B_1 B_2^T + B_2 B_1^T = 0,$$

e.g.

$$B_1 = \begin{bmatrix} - & 1 \\ 1 & 1 \end{bmatrix}, \quad B_2 = \begin{bmatrix} - & - \\ - & 1 \end{bmatrix},$$

$$G = \begin{bmatrix} - & - & 1 & - \\ - & - & - & 1 \\ 1 & - & 1 & 1 \\ - & 1 & 1 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} - & 1 & - & - \\ 1 & 1 & - & 1 \\ - & - & - & 1 \\ - & 1 & 1 & 1 \end{bmatrix}.$$

(Gastineau-Hills 1980, 1982)

More examples

Williamson-like construction (uses 3 amicable B matrices):

$$A_1 = I_{(4)}, \quad \lambda_{1k} = \lambda_{j1} = -1,$$
$$\lambda_{jk} = 1, \quad (j \neq k), \quad j, k \in \{2, 3, 4\}.$$

Octonion-like construction (uses 7 amicable B matrices):

$$A_1 = I_{(8)}, \quad \lambda_{1k} = \lambda_{k1} = -1,$$
$$\lambda_{jk} = 1, \quad (j \neq k), \quad j, k \in \{2, \ldots, 8\}.$$

(Gastineau-Hills 1980, 1982)

Hurwitz-Radon limit

A theorem of Radon puts an upper limit of 8 on the order n such that

$$A_j * A_k = 0 \quad (j \neq k), \quad \sum_{k=1}^{n} A_k \in \{-1, 1\}^{n \times n},$$
$$A_k A_k^T = I_{(n)},$$
$$A_1 A_k^T - A_k A_1^T = 0, \quad A_j A_k^T + A_k A_j^T = 0 \quad (1 < j < k).$$

(Radon 1922, Geramita and Pullman 1974, Geramita and Seberry 1979)

Some Williamson and Octonion constructions

Osborn (2011) classified the Hadamard matrices that can be constructed via the Williamson and the Octonion constructions for p up to 5, by Hadamard equivalence class.

Williamson:
Exactly 1 equivalence class for order 12 (1 class in total).
Exactly 2 equivalence classes for order 20 (3 classes in total).

Octonion:
Exactly 4 equivalence classes for order 24 (60 classes in total).
Exactly 72 equivalence classes for order 40
(more than 3.66×10^{11} classes in total).

(Osborn 2011)

Recap: ingredients

We need n-tuples $(A_1, \ldots, A_n)$, $(B_1, \ldots, B_n)$, with

$$A_k \in \{-1, 0, 1\}^{n \times n},$$

$$B_k \in \{-1, 1\}^{p \times p},$$

satisfying the conditions (4).

For the A matrices, we look at signed groups, Clifford algebras, and at sets of signed permutation matrices in general.

For the B matrices, we look at graphs of amicability and anti-amicability.

Clifford algebras via signed groups (1)

$\mathbb{G}_{p,q}$ is extension of $\mathbb{Z}_2$ by $\mathbb{Z}_2^{p+q}$, defined by the signed group presentation

$$\begin{aligned}\mathbb{G}_{p,q} := \Big\langle -1,\ \mathbf{e}_{\{k\}}\ (k \in S_{p,q})\ \ |\ & \\ & \mathbf{e}_{\{k\}}^2 = -1\ (k < 0), \quad \mathbf{e}_{\{k\}}^2 = 1\ (k > 0), \\ & \mathbf{e}_{\{j\}}\mathbf{e}_{\{k\}} = -\mathbf{e}_{\{k\}}\mathbf{e}_{\{j\}}\ (j \neq k) \Big\rangle,\end{aligned}$$

where $S_{p,q} := \{-q, \ldots, -1, 1, \ldots, p\}$. $\qquad |\mathbb{G}_{p,q}| = 2^{1+p+q}$.

(Porteous 1969, 1995; Lam 1973; Gastineau-Hills 1980, 1982; Lounesto 1997, L 2005)

Clifford algebras via signed groups (2)

Multiplication in $\mathbb{Z}_2^{p+q}$ is isomorphic to XOR of bit vectors, or symmetric set difference of subsets of $S_{p,q}$,
so elements of $\mathbb{G}_{p,q}$ can be written as $\pm\mathbf{e}_T,\ T \subset S_{p,q}$.

$\mathbb{G}_{p,q}$ extends to the real Clifford algebra $\mathbb{R}_{p,q}$, of dimension 2^{p+q}.
For $\mathbf{x} \in \mathbb{R}_{p,q}$,

$$\mathbf{x} = \sum_{T \subset S_{p,q}} x_T \mathbf{e}_T.$$

There are 2^{p+q} basis elements $\mathbf{e}_T$.

The element $-1\mathbf{e}_\emptyset$ in $\mathbb{G}_{p,q}$ is identified with -1 in $\mathbb{R}$.

(Porteous 1969, 1995; Lam 1973; Gastineau-Hills 1980, 1982; Lounesto 1997, L 2005)

Representations for $\mathbb{G}_{m,m}$ and $\mathbb{R}_{m,m}$ (1)

Real monomial representations for $\mathbb{G}_{m,m}$ and $\mathbb{R}_{m,m}$ are generated by Kronecker products of the 2×2 matrices

$$I_{(2)}, \quad J := \begin{bmatrix} . & - \\ 1 & . \end{bmatrix}, \quad K := \begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix}.$$

These representations are *faithful*: $\mathbb{R}_{m,m}$ is isomorphic to $\mathbb{R}^{2^m \times 2^m}$.

Thus $\mathbb{R}^{2^m \times 2^m}$ has a basis consisting of 4^m real monomial matrices.

(Porteous 1969, 1995; Lam 1973; Gastineau-Hills 1980, 1982; Lounesto 1997, L 2005)

Representations for $\mathbb{G}_{m,m}$ and $\mathbb{R}_{m,m}$ (2)

Pairs of basis elements of $\mathbb{R}_{m,m}$ either commute or anticommute.

Representations of basis elements of $\mathbb{R}_{m,m}$ are either symmetric or skew, and so the matrices A_j, A_k satisfy

$$A_k A_k^T = I_{(2^m)}, \quad A_j A_k^T + \lambda_{jk} A_k A_j^T = 0 \quad (j \neq k), \quad \lambda_{jk} \in \{-1, 1\}.$$

We can choose $n := 2^m$ of these such that

$$A_j * A_k = 0 \quad (j \neq k), \quad \sum_{k=1}^{n} A_k \in \{-1, 1\}^{n \times n}.$$

(Porteous 1969, 1995; Lam 1973; Gastineau-Hills 1980, 1982; Lounesto 1997, L 2005)

Example: $\mathbb{R}_{2,2}$ (1)

The real Clifford algebra $\mathbb{R}_{2,2}$ is isomorphic to the real matrix algebra $\mathbb{R}^{4\times 4}$.

The corresponding frame group $\mathbb{G}_{2,2}$ is generated as a signed group by the four matrices

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

Example: $\mathbb{R}_{2,2}$ (2)

The group has 32 elements and the basis of $\mathbb{R}_{2,2}$ has 16 elements. The basis matrices form 4 equivalence classes of 4 elements each, where equivalence is given by the support. To form a 4-tuple of basis matrices satisfying (4), we take a transversal, for example,

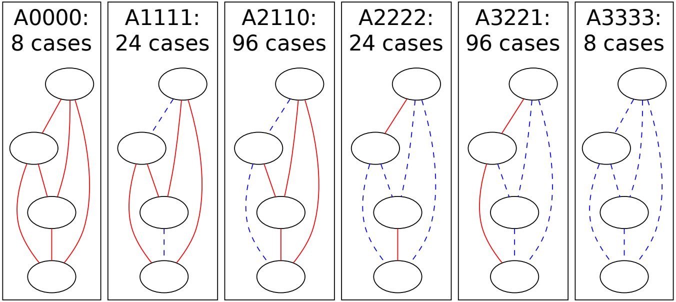
$$A_1 := \begin{bmatrix} - & . & . & . \\ . & 1 & . & . \\ . & . & - & . \\ . & . & . & 1 \end{bmatrix}, \quad A_2 := \begin{bmatrix} . & 1 & . & . \\ 1 & . & . & . \\ . & . & . & - \\ . & . & - & . \end{bmatrix},$$

$$A_3 := \begin{bmatrix} . & . & 1 & . \\ . & . & . & - \\ - & . & . & . \\ . & 1 & . & . \end{bmatrix}, \quad A_4 := \begin{bmatrix} . & . & . & 1 \\ . & . & 1 & . \\ . & 1 & . & . \\ 1 & . & . & . \end{bmatrix}.$$

In this case, $\lambda_{1,2} = \lambda_{1,3} = \lambda_{1,4} = \lambda_{2,3} = \lambda_{2,4} = \lambda_{3,4} = 1$.

Example: $\mathbb{R}_{2,2}$ (3)

An exhaustive enumeration of the $4^4 = 256$ different 4-tuples of 4×4 basis matrices reveals six inequivalent graphs of amicability:



A0000: 8 cases

A1111: 24 cases

A2110: 96 cases

A2222: 24 cases

A3221: 96 cases

A3333: 8 cases

Solid: $\lambda_{j,k} = -1$, dashed: $\lambda_{j,k} = 1$.

Signed permutation matrices (1)

So, for $n = 2^m$, we can always use a real representation of a Clifford algebra to construct an n-tuple of $\{-1, 0, 1\}$ ingredient matrices of satisfying our condition (4).

But what can we say about the set of all n-tuples for such n, and what happens when n is not a power of 2?

We recap these conditions.

$$A_j * A_k = 0 \quad (j \neq k), \quad \sum_{k=1}^{n} A_k \in \{-1, 1\}^{n \times n}, \tag{4a}$$

$$A_k A_k^T = I_{(n)}, \tag{4b}$$

$$A_j A_k^T + \lambda_{jk} A_k A_j^T = 0 \quad (j \neq k), \tag{4c}$$

Signed permutation matrices (2)

So, each A_k is a signed permutation matrix. If we multiply each A_k on the left by some fixed signed permutation matrix S, we permute and change the signs of the all the corresponding rows of each A_k, so (4a) is still satisfied.

Since $SS^T = I_{(n)}$, (4b) and (4c) are also satisfied, and in particular, multiplication by S does not affect the values of $\lambda_{j,k}$ in (4c).

Similarly, if we multiply each A_k on the right by S.

We therefore have an equivalence class of n-tuples under these two types of transformation, and without loss of generality, can set $A_1 = I_{(n)}$. In this representative case, each of the other $A_k, k > 1$ must be symmetric or skew, with zero diagonal.

Symmetric Latin squares (1)

If we now take a linear combination of the corresponding permutation matrices $P_k = |A_k|$, we have a *symmetric Latin square with constant diagonal*. This type of Latin square must have even order.

Sequence A003191 in Sloane's Online Encyclopedia of Integer Sequences lists the number of such Latin squares for each even order. The entire listed sequence is

$$1, 1, 6, 5972, 1\,225\,533\,120,$$

corresponding to orders 2, 4, 6, 8 and 10, respectively.

The sole examples of orders 2 and 4 can be obtained via the Clifford algebra representation.

Symmetric Latin squares (2)

Order 2:

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix}$$

Order 4:

$$\begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix}$$

Symmetric Latin squares (3)

Order 6:

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

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

Symmetric Latin squares (4)

Recalling condition (4c),

$$A_j A_k^T + \lambda_{jk} A_k A_j^T = 0 \quad (j \neq k),$$

we see that $A_j A_k^T$ must either be symmetric or skew, and so each corresponding product of permutation matrices $P_j P_k^T$ for our representative case must be symmetric, for each pair $j, k > 1$.

If we enumerate all six cases of symmetric Latin squares of order 6 with constant diagonal, we find that *none* of these cases yields permutation matrices P_2, P_3 with $P_2 P_3^T$ symmetric.

Anti-amicable pairs of $\{-1,1\}$ matrices

Given the A_k, this fixes λ_{jk}.

We now must find an n-tuple of $\{-1,1\}$ matrices with a complementary graph of amicability and anti-amicability.

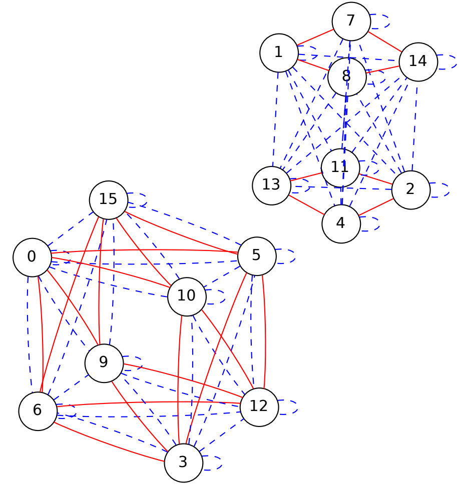
For anti-amicable pairs of matrices in $\{-1,1\}^{p \times p}$,

$$B_1 B_2^T + B_2 B_1^T = 0,$$

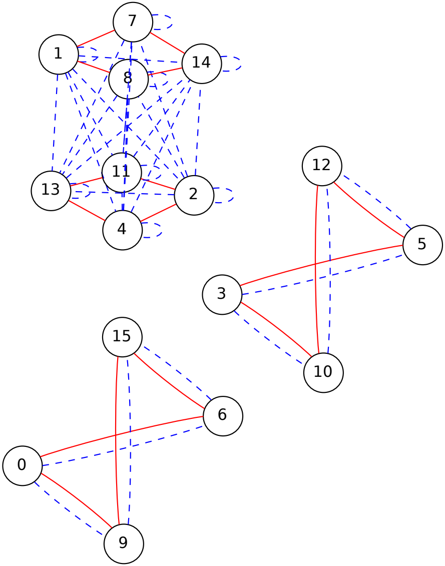
therefore $B_1 B_2^T$ is skew, so p must be even.

(Gastineau-Hills 1980, 1982)

$\{-1,1\}^{2\times 2}$, Amicable, Anti-amicable

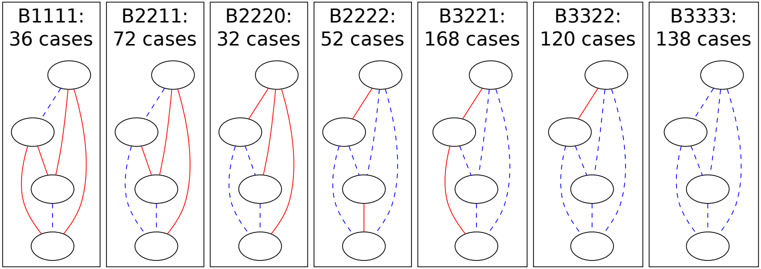


$\{-1,1\}^{2\times 2}$, $B_1B_1^T + B_2B_2^T = 4I_{(2)}$



$\{-1,1\}^{2\times 2}$, $B_1B_1^T + B_2B_2^T + B_3B_3^T + B_4B_4^T = 8I_{(2)}$

An exhaustive search of the $\binom{19}{4} = 3876$ distinct multisets of 4 matrices of type $\{-1,1\}^{2\times 2}$ reveals seven inequivalent graphs:



B1111: 36 cases

B2211: 72 cases

B2220: 32 cases

B2222: 52 cases

B3221: 168 cases

B3322: 120 cases

B3333: 138 cases

Solid: $\lambda_{j,k} = -1$, dashed: $\lambda_{j,k} = 1$.