Hadamard and conference matrices

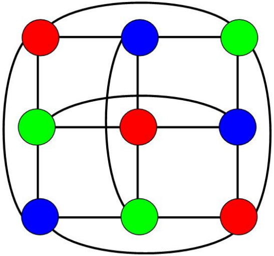
Peter J. Cameron
University of St Andrews & Queen Mary University of London

Mathematics Study Group

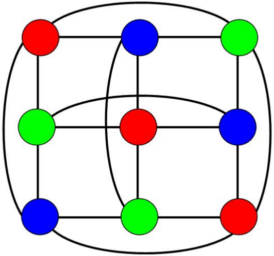
LONDON SOUTH BANK UNIVERSITY

with input from Rosemary Bailey, Katarzyna Filipiak, Joachim Kunert, Dennis Lin, Augustyn Markiewicz, Will Orrick, Gordon Royle

Happy Birthday, MSG!!



Happy Birthday, MSG!!



and many happy returns . . .

Hadamard's theorem

Let H be an $n \times n$ matrix, all of whose entries are at most 1 in modulus. How large can $\det(H)$ be?

Hadamard's theorem

Let H be an $n \times n$ matrix, all of whose entries are at most 1 in modulus. How large can $\det(H)$ be?
Now $\det(H)$ is equal to the volume of the n-dimensional parallelepiped spanned by the rows of H. By assumption, each row has Euclidean length at most $n^{1/2}$, so that $\det(H) \leq n^{n/2}$; equality holds if and only if

- every entry of H is ± 1;
- the rows of H are orthogonal, that is, $HH^\top = nI$.

Hadamard's theorem

Let H be an $n \times n$ matrix, all of whose entries are at most 1 in modulus. How large can $\det(H)$ be?
Now $\det(H)$ is equal to the volume of the n-dimensional parallelepiped spanned by the rows of H. By assumption, each row has Euclidean length at most $n^{1/2}$, so that $\det(H) \leq n^{n/2}$; equality holds if and only if

- every entry of H is ± 1;
- the rows of H are orthogonal, that is, $HH^\top = nI$.

A matrix attaining the bound is a Hadamard matrix.

Hadamard's theorem

Let H be an $n \times n$ matrix, all of whose entries are at most 1 in modulus. How large can $\det(H)$ be?
Now $\det(H)$ is equal to the volume of the n-dimensional parallelepiped spanned by the rows of H. By assumption, each row has Euclidean length at most $n^{1/2}$, so that $\det(H) \leq n^{n/2}$; equality holds if and only if

- every entry of H is ± 1;
- the rows of H are orthogonal, that is, $HH^\top = nI$.

A matrix attaining the bound is a Hadamard matrix.
This is a nice example of a continuous problem whose solution brings us into discrete mathematics.

Remarks

- $HH^\top = nI \Rightarrow H^{-1} = n^{-1}H^\top \Rightarrow H^\top H = nI$, so a Hadamard matrix also has orthogonal columns.

Remarks

- $HH^\top = nI \Rightarrow H^{-1} = n^{-1}H^\top \Rightarrow H^\top H = nI$, so a Hadamard matrix also has orthogonal columns.
- Changing signs of rows or columns, permuting rows or columns, or transposing preserve the Hadamard property.

Remarks

- $HH^\top = nI \Rightarrow H^{-1} = n^{-1}H^\top \Rightarrow H^\top H = nI$, so a Hadamard matrix also has orthogonal columns.
- Changing signs of rows or columns, permuting rows or columns, or transposing preserve the Hadamard property.

Examples of Hadamard matrices include

$$\begin{pmatrix} + \end{pmatrix}, \quad \begin{pmatrix} + & + \\ + & - \end{pmatrix}, \quad \begin{pmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & + \end{pmatrix}.$$

Orders of Hadamard matrices

Theorem

The order of a Hadamard matrix is 1, 2 *or a multiple of* 4.

Orders of Hadamard matrices

Theorem

The order of a Hadamard matrix is $1, 2$ *or a multiple of* 4.

We can ensure that the first row consists of all $+$s by column sign changes. Then (assuming at least three rows) we can bring the first three rows into the following shape by column permutations:

$$\begin{pmatrix} \overbrace{+ \dots +}^{a} & \overbrace{+ \dots +}^{b} & \overbrace{+ \dots +}^{c} & \overbrace{+ \dots +}^{d} \\ + \dots + & + \dots + & - \dots - & - \dots - \\ + \dots + & - \dots - & + \dots + & - \dots - \end{pmatrix}$$

Orders of Hadamard matrices

Theorem

The order of a Hadamard matrix is 1, 2 *or a multiple of* 4.

We can ensure that the first row consists of all $+$s by column sign changes. Then (assuming at least three rows) we can bring the first three rows into the following shape by column permutations:

$$\left(\begin{array}{cccc} \overbrace{+\ \dots\ +}^{a} & \overbrace{+\ \dots\ +}^{b} & \overbrace{+\ \dots\ +}^{c} & \overbrace{+\ \dots\ +}^{d} \\ +\ \dots\ + & +\ \dots\ + & -\ \dots\ - & -\ \dots\ - \\ +\ \dots\ + & -\ \dots\ - & +\ \dots\ + & -\ \dots\ - \end{array}\right)$$

Now orthogonality of rows gives

$$a+b=c+d=a+c=b+d=a+d=b+c=n/2,$$

so $a=b=c=d=n/4$.

The Hadamard conjecture

The Hadamard conjecture asserts that a Hadamard matrix exists of every order divisible by 4. The smallest multiple of 4 for which no such matrix is currently known is 668, the value 428 having been settled only in 2005.

Symmetric Hadamard matrices

A particularly attractive class of Hadamard matrices are those which are symmetric, have constant diagonal and constant row sum.

Symmetric Hadamard matrices

A particularly attractive class of Hadamard matrices are those which are symmetric, have constant diagonal and constant row sum.
Such matrices must have square order $4s^2$; the row sums are $\pm 2s$. [For the row sum σ is an eigenvalue of H, and hence σ^2 is an eigenvalue of $H^2 = HH^\top$: thus $\sigma^2 = n$.]

Symmetric Hadamard matrices

A particularly attractive class of Hadamard matrices are those which are symmetric, have constant diagonal and constant row sum.

Such matrices must have square order $4s^2$; the row sums are $\pm 2s$. [For the row sum σ is an eigenvalue of H, and hence σ^2 is an eigenvalue of $H^2 = HH^\top$: thus $\sigma^2 = n$.]

They give rise to symmetric 2-$(4s^2, 2s^2 \pm s, s^2 \pm s)$ designs and strongly regular graphs.

Symmetric Hadamard matrices

A particularly attractive class of Hadamard matrices are those which are symmetric, have constant diagonal and constant row sum.

Such matrices must have square order $4s^2$; the row sums are $\pm 2s$. [For the row sum σ is an eigenvalue of H, and hence σ^2 is an eigenvalue of $H^2 = HH^\top$: thus $\sigma^2 = n$.]

They give rise to symmetric 2-$(4s^2, 2s^2 \pm s, s^2 \pm s)$ designs and strongly regular graphs.

In the case where the order is a power of 2, these matrices can be constructed from bent functions (functions on a vector space whose distance from the space of linear functions is maximal).

There are connections with coding theory and cryptography.

Skew-Hadamard matrices

A matrix A is skew if $A^\top = -A$.
A Hadamard matrix can't really be skew, since in characteristic not 2, a skew matrix has zero diagonal. So we compromise and define a skew-Hadamard matrix H to be one which has constant diagonal $+1$ and such that $H - I$ is skew.

Skew-Hadamard matrices

A matrix A is skew if $A^\top = -A$.
A Hadamard matrix can't really be skew, since in characteristic not 2, a skew matrix has zero diagonal. So we compromise and define a skew-Hadamard matrix H to be one which has constant diagonal $+1$ and such that $H - I$ is skew.
The property is preserved by simultaneous row and column sign changes, so we can normalise the matrix so that its first row is $+1$ and its first column (apart from the first entry) is -1.

Skew-Hadamard matrices

A matrix A is skew if $A^\top = -A$.
A Hadamard matrix can't really be skew, since in characteristic not 2, a skew matrix has zero diagonal. So we compromise and define a skew-Hadamard matrix H to be one which has constant diagonal $+1$ and such that $H - I$ is skew.
The property is preserved by simultaneous row and column sign changes, so we can normalise the matrix so that its first row is $+1$ and its first column (apart from the first entry) is -1.
It is conjectured that skew-Hadamard matrices of all orders divisible by 4 exist. The smallest unsolved case is 188.

Doubly regular tournaments

If we delete the first row and column of a skew-Hadamard matrix, and replace the diagonal 1s by 0s, we obtain the adjacency matrix of a doubly regular tournament. This means a tournament on $n = 4t + 3$ vertices, in which each vertex has in- and out-degree $2t + 1$, and for any two distinct vertices v and w, there are t vertices z with $v \to z$ and $w \to z$.

Doubly regular tournaments

If we delete the first row and column of a skew-Hadamard matrix, and replace the diagonal 1s by 0s, we obtain the adjacency matrix of a doubly regular tournament. This means a tournament on $n = 4t + 3$ vertices, in which each vertex has in- and out-degree $2t + 1$, and for any two distinct vertices v and w, there are t vertices z with $v \to z$ and $w \to z$.

Conversely, any doubly regular tournament on n vertices gives a skew-Hadamard matrix on $n + 1$ vertices.

Doubly regular tournaments

If we delete the first row and column of a skew-Hadamard matrix, and replace the diagonal 1s by 0s, we obtain the adjacency matrix of a doubly regular tournament. This means a tournament on $n = 4t + 3$ vertices, in which each vertex has in- and out-degree $2t + 1$, and for any two distinct vertices v and w, there are t vertices z with $v \to z$ and $w \to z$.

Conversely, any doubly regular tournament on n vertices gives a skew-Hadamard matrix on $n + 1$ vertices.

In a forthcoming paper, Bailey, Cameron, Filipiak, Kunert and Markiewicz use Hamiltonian decompositions of doubly regular tournaments to construct universally optimal circular repeated-measurements designs.

Doubly regular tournaments

If we delete the first row and column of a skew-Hadamard matrix, and replace the diagonal 1s by 0s, we obtain the adjacency matrix of a doubly regular tournament. This means a tournament on $n = 4t + 3$ vertices, in which each vertex has in- and out-degree $2t + 1$, and for any two distinct vertices v and w, there are t vertices z with $v \to z$ and $w \to z$.

Conversely, any doubly regular tournament on n vertices gives a skew-Hadamard matrix on $n + 1$ vertices.

In a forthcoming paper, Bailey, Cameron, Filipiak, Kunert and Markiewicz use Hamiltonian decompositions of doubly regular tournaments to construct universally optimal circular repeated-measurements designs.

Problem

Does every doubly regular tournament have a Hamiltonian decomposition?

Doubly regular tournaments

If we delete the first row and column of a skew-Hadamard matrix, and replace the diagonal 1s by 0s, we obtain the adjacency matrix of a doubly regular tournament. This means a tournament on $n = 4t + 3$ vertices, in which each vertex has in- and out-degree $2t + 1$, and for any two distinct vertices v and w, there are t vertices z with $v \to z$ and $w \to z$.

Conversely, any doubly regular tournament on n vertices gives a skew-Hadamard matrix on $n + 1$ vertices.

In a forthcoming paper, Bailey, Cameron, Filipiak, Kunert and Markiewicz use Hamiltonian decompositions of doubly regular tournaments to construct universally optimal circular repeated-measurements designs.

Problem

Does every doubly regular tournament have a Hamiltonian decomposition?

Indeed, Kelly conjectured in the 1960s that every regular tournament has a Hamiltonian decomposition.

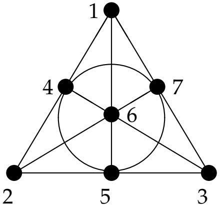
An example

$$\begin{pmatrix} 0 & + & + & - & + & - & - \\ - & 0 & + & + & - & + & - \\ - & - & 0 & + & + & - & + \\ + & - & - & 0 & + & + & - \\ - & + & - & - & 0 & + & + \\ + & - & + & - & - & 0 & + \\ + & + & - & + & - & - & 0 \end{pmatrix} \qquad \begin{pmatrix} + & + & + & + & + & + & + & + \\ - & + & + & + & - & + & - & - \\ - & - & + & + & + & - & + & - \\ - & - & - & + & + & + & - & + \\ - & + & - & - & + & + & + & - \\ - & - & + & - & - & + & + & + \\ - & + & - & + & - & - & + & + \\ - & + & + & - & + & - & - & + \end{pmatrix}$$

An example

$$\begin{pmatrix} 0 & + & + & - & + & - & - \\ - & 0 & + & + & - & + & - \\ - & - & 0 & + & + & - & + \\ + & - & - & 0 & + & + & - \\ - & + & - & - & 0 & + & + \\ + & - & + & - & - & 0 & + \\ + & + & - & + & - & - & 0 \end{pmatrix} \qquad \begin{pmatrix} + & + & + & + & + & + & + & + \\ - & + & + & + & - & + & - & - \\ - & - & + & + & + & - & + & - \\ - & - & - & + & + & + & - & + \\ - & + & - & - & + & + & + & - \\ - & - & + & - & - & + & + & + \\ - & + & - & + & - & - & + & + \\ - & + & + & - & + & - & - & + \end{pmatrix}$$

This is related to the Fano plane:



Paley tournaments

The simplest construction of doubly regular tournaments starts with a finite field of order $q \equiv 3 \pmod 4$. The vertices are the elements of the field, and there is an arc $x \to y$ if and only if $y - x$ is a square. (This is a tournament because -1 is a non-square, and therefore $y - x$ is a square if and only if $x - y$ is not.)

Paley tournaments

The simplest construction of doubly regular tournaments starts with a finite field of order $q \equiv 3 \pmod 4$. The vertices are the elements of the field, and there is an arc $x \to y$ if and only if $y - x$ is a square. (This is a tournament because -1 is a non-square, and therefore $y - x$ is a square if and only if $x - y$ is not.)

If q is prime, then there is an obvious Hamiltonian decomposition: for each non-zero square s, take the Hamiltonian cycle

$$(0, s, 2s, 3s, \ldots, -s).$$

However, if q is not a prime, it is not so obvious how to proceed.

Conference matrices

A conference matrix of order n is an $n \times n$ matrix C with diagonal entries 0 and off-diagonal entries ± 1 which satisfies $CC^\top = (n-1)I$.

Conference matrices

A conference matrix of order n is an $n \times n$ matrix C with diagonal entries 0 and off-diagonal entries ± 1 which satisfies $CC^\top = (n-1)I$.

We have:

- The defining equation shows that any two rows of C are orthogonal. The contributions to the inner product of the ith and jth rows coming from the ith and jth positions are zero; each further position contributes $+1$ or -1; there must be equally many (namely $(n-2)/2$) contributions of each sign. So n is even.

Conference matrices

A conference matrix of order n is an $n \times n$ matrix C with diagonal entries 0 and off-diagonal entries ± 1 which satisfies $CC^\top = (n-1)I$.
We have:

- The defining equation shows that any two rows of C are orthogonal. The contributions to the inner product of the ith and jth rows coming from the ith and jth positions are zero; each further position contributes $+1$ or -1; there must be equally many (namely $(n-2)/2$) contributions of each sign. So n is even.
- The defining equation gives $C^{-1} = (1/(n-1))C^\top$, whence $C^\top C = (n-1)I$. So the columns are also pairwise orthogonal.

Conference matrices

A conference matrix of order n is an $n \times n$ matrix C with diagonal entries 0 and off-diagonal entries ± 1 which satisfies $CC^\top = (n-1)I$.

We have:

- The defining equation shows that any two rows of C are orthogonal. The contributions to the inner product of the ith and jth rows coming from the ith and jth positions are zero; each further position contributes $+1$ or -1; there must be equally many (namely $(n-2)/2$) contributions of each sign. So n is even.
- The defining equation gives $C^{-1} = (1/(n-1))C^\top$, whence $C^\top C = (n-1)I$. So the columns are also pairwise orthogonal.
- The property of being a conference matrix is unchanged under changing the sign of any row or column, or simultaneously applying the same permutation to rows and columns.

Symmetric and skew-symmetric

Using row and column sign changes, we can assume that all entries in the first row and column (apart from their intersection) are $+1$; then any row other than the first has $n/2$ entries $+1$ (including the first entry) and $(n-2)/2$ entries -1. Let C be such a matrix, and let S be the matrix obtained from C by deleting the first row and column.

Symmetric and skew-symmetric

Using row and column sign changes, we can assume that all entries in the first row and column (apart from their intersection) are $+1$; then any row other than the first has $n/2$ entries $+1$ (including the first entry) and $(n-2)/2$ entries -1. Let C be such a matrix, and let S be the matrix obtained from C by deleting the first row and column.

Theorem

If $n \equiv 2 \pmod 4$ then S is symmetric; if $n \equiv 0 \pmod 4$ then S is skew-symmetric.

Proof of the theorem

Suppose first that S is not symmetric. Without loss of generality, we can assume that $S_{12} = +1$ while $S_{21} = -1$. Each row of S has m entries $+1$ and m entries -1, where $n = 2m + 2$; and the inner product of two rows is -1.

Proof of the theorem

Suppose first that S is not symmetric. Without loss of generality, we can assume that $S_{12} = +1$ while $S_{21} = -1$. Each row of S has m entries $+1$ and m entries -1, where $n = 2m + 2$; and the inner product of two rows is -1.

Suppose that the first two rows look as follows:

$$\begin{array}{cccccc} 0 & + & + \cdots + & + \cdots + & - \cdots - & - \cdots - \\ - & 0 & \underbrace{+ \cdots +}_{a} & \underbrace{- \cdots -}_{b} & \underbrace{+ \cdots +}_{c} & \underbrace{- \cdots -}_{d} \end{array}$$

Proof of the theorem

Suppose first that S is not symmetric. Without loss of generality, we can assume that $S_{12} = +1$ while $S_{21} = -1$. Each row of S has m entries $+1$ and m entries -1, where $n = 2m + 2$; and the inner product of two rows is -1.

Suppose that the first two rows look as follows:

$$\begin{array}{cccccc} 0 & + & + \cdots + & + \cdots + & - \cdots - & - \cdots - \\ - & 0 & \underbrace{+ \cdots +}_{a} & \underbrace{- \cdots -}_{b} & \underbrace{+ \cdots +}_{c} & \underbrace{- \cdots -}_{d} \end{array}$$

Now row 1 gives $a + b = m - 1$, $c + d = m$;

Proof of the theorem

Suppose first that S is not symmetric. Without loss of generality, we can assume that $S_{12} = +1$ while $S_{21} = -1$. Each row of S has m entries $+1$ and m entries -1, where $n = 2m + 2$; and the inner product of two rows is -1.

Suppose that the first two rows look as follows:

$$\begin{array}{cccccc} 0 & + & + \cdots + & + \cdots + & - \cdots - & - \cdots - \\ - & 0 & \underbrace{+ \cdots +}_{a} & \underbrace{- \cdots -}_{b} & \underbrace{+ \cdots +}_{c} & \underbrace{- \cdots -}_{d} \end{array}$$

Now row 1 gives $a + b = m - 1$, $c + d = m$;
row 2 gives $a + c = m$, $b + d = m - 1$;

Proof of the theorem

Suppose first that S is not symmetric. Without loss of generality, we can assume that $S_{12} = +1$ while $S_{21} = -1$. Each row of S has m entries $+1$ and m entries -1, where $n = 2m+2$; and the inner product of two rows is -1.
Suppose that the first two rows look as follows:

$$\begin{array}{cccccc} 0 & + & +\cdots+ & +\cdots+ & -\cdots- & -\cdots- \\ - & 0 & \underbrace{+\cdots+}_{a} & \underbrace{-\cdots-}_{b} & \underbrace{+\cdots+}_{c} & \underbrace{-\cdots-}_{d} \end{array}$$

Now row 1 gives $a+b = m-1$, $c+d = m$;
row 2 gives $a+c = m$, $b+d = m-1$;
and the inner product gives $a+d = m-1$, $b+c = m$.

Proof of the theorem

Suppose first that S is not symmetric. Without loss of generality, we can assume that $S_{12} = +1$ while $S_{21} = -1$. Each row of S has m entries $+1$ and m entries -1, where $n = 2m + 2$; and the inner product of two rows is -1.
Suppose that the first two rows look as follows:

$$\begin{array}{cccccc} 0 & + & + \cdots + & + \cdots + & - \cdots - & - \cdots - \\ - & 0 & \underbrace{+ \cdots +}_{a} & \underbrace{- \cdots -}_{b} & \underbrace{+ \cdots +}_{c} & \underbrace{- \cdots -}_{d} \end{array}$$

Now row 1 gives $a + b = m - 1$, $c + d = m$;
row 2 gives $a + c = m$, $b + d = m - 1$;
and the inner product gives $a + d = m - 1$, $b + c = m$.
From these we obtain

$$a = \tfrac{1}{2}((a + b) + (a + c) - (b + c)) = (m - 1)/2,$$

so m is odd, and $n \equiv 0 \pmod 4$.

Proof of the theorem

Suppose first that S is not symmetric. Without loss of generality, we can assume that $S_{12} = +1$ while $S_{21} = -1$. Each row of S has m entries $+1$ and m entries -1, where $n = 2m + 2$; and the inner product of two rows is -1.
Suppose that the first two rows look as follows:

$$\begin{array}{cccccc} 0 & + & +\cdots+ & +\cdots+ & -\cdots- & -\cdots- \\ - & 0 & \underbrace{+\cdots+}_{a} & \underbrace{-\cdots-}_{b} & \underbrace{+\cdots+}_{c} & \underbrace{-\cdots-}_{d} \end{array}$$

Now row 1 gives $a + b = m - 1$, $c + d = m$;
row 2 gives $a + c = m$, $b + d = m - 1$;
and the inner product gives $a + d = m - 1$, $b + c = m$.
From these we obtain

$$a = \tfrac{1}{2}((a+b) + (a+c) - (b+c)) = (m-1)/2,$$

so m is odd, and $n \equiv 0 \pmod 4$.

The other case is similar.

By slight abuse of language, we call a normalised conference matrix C *symmetric* or *skew* according as S is symmetric or skew (that is, according to the congruence on $n \pmod 4$). A "symmetric" conference matrix really is symmetric, while a skew conference matrix becomes skew if we change the sign of the first column.

Symmetric conference matrices

Let C be a symmetric conference matrix. Let A be obtained from S by replacing $+1$ by 0 and -1 by 1.Then A is the incidence matrix of a *strongly regular graph* of Paley type: that is, a graph with $n-1$ vertices in which every vertex has degree $(n-2)/2$, two adjacent vertices have $(n-6)/4$ common neighbours, and two non-adjacent vertices have $(n-2)/4$ common neighbours. The matrix S is called the *Seidel adjacency matrix* of the graph. The complementary graph has the same properties.

Symmetric conference matrices

Let C be a symmetric conference matrix. Let A be obtained from S by replacing $+1$ by 0 and -1 by 1.Then A is the incidence matrix of a *strongly regular graph* of Paley type: that is, a graph with $n-1$ vertices in which every vertex has degree $(n-2)/2$, two adjacent vertices have $(n-6)/4$ common neighbours, and two non-adjacent vertices have $(n-2)/4$ common neighbours. The matrix S is called the *Seidel adjacency matrix* of the graph.

The complementary graph has the same properties.

Symmetric conference matrices are associated with other combinatorial objects, among them regular two-graphs, sets of equiangular lines in Euclidean space, switching classes of graphs. A conference matrix can produce many different strongly regular graphs by choosing different rows and columns for the normalisation.

Symmetric conference matrices

Let C be a symmetric conference matrix. Let A be obtained from S by replacing $+1$ by 0 and -1 by 1.Then A is the incidence matrix of a *strongly regular graph* of Paley type: that is, a graph with $n-1$ vertices in which every vertex has degree $(n-2)/2$, two adjacent vertices have $(n-6)/4$ common neighbours, and two non-adjacent vertices have $(n-2)/4$ common neighbours. The matrix S is called the *Seidel adjacency matrix* of the graph.

The complementary graph has the same properties.

Symmetric conference matrices are associated with other combinatorial objects, among them regular two-graphs, sets of equiangular lines in Euclidean space, switching classes of graphs. A conference matrix can produce many different strongly regular graphs by choosing different rows and columns for the normalisation.

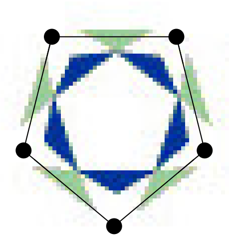
Again the Paley construction works, on a field of order $q \equiv +1 \pmod 4$; join x to y if $y-x$ is a square. (This time, -1 is a square, so $y-x$ is a square if and only if $x-y$ is.)

An example

The Paley graph on 5 vertices is the 5-cycle. We obtain a symmetric conference matrix by bordering the Seidel adjacency matrix as shown.

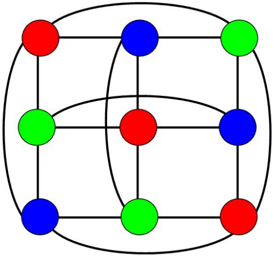
An example

The Paley graph on 5 vertices is the 5-cycle. We obtain a symmetric conference matrix by bordering the Seidel adjacency matrix as shown.



$$\begin{pmatrix} 0 & + & + & + & + & + \\ + & 0 & - & + & + & - \\ + & - & 0 & - & + & + \\ + & + & - & 0 & - & + \\ + & + & + & - & 0 & - \\ + & - & + & + & - & 0 \end{pmatrix}$$

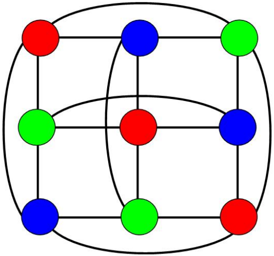
Another example



$$\begin{pmatrix} 0 & - & - & - & + & + & - & + & + \\ - & 0 & - & + & - & + & + & - & + \\ - & - & 0 & + & + & - & + & + & - \\ - & + & + & 0 & - & - & - & + & + \\ + & - & + & - & 0 & - & + & - & + \\ + & + & - & - & - & 0 & + & + & - \\ - & + & + & - & + & + & 0 & - & - \\ + & - & + & + & - & + & - & 0 & - \\ + & + & - & + & + & - & - & - & 0 \end{pmatrix}$$

A new first row and column, with 0 in the $(1,1)$ position and other entries $+$, gives a symmetric conference matrix of order 10.

Another example



$$\begin{pmatrix}
0 & - & - & - & + & + & - & + & + \\
- & 0 & - & + & - & + & + & - & + \\
- & - & 0 & + & + & - & + & + & - \\
- & + & + & 0 & - & - & - & + & + \\
+ & - & + & - & 0 & - & + & - & + \\
+ & + & - & - & - & 0 & + & + & - \\
- & + & + & - & + & + & 0 & - & - \\
+ & - & + & + & - & + & - & 0 & - \\
+ & + & - & + & + & - & - & - & 0
\end{pmatrix}$$

A new first row and column, with 0 in the $(1,1)$ position and other entries $+$, gives a symmetric conference matrix of order 10.

The MSG logo is the Paley graph on GF(9). (Exercise: Prove this!)

A theorem of van Lint and Seidel asserts that, if a symmetric conference matrix of order n exists, then $n-1$ is the sum of two squares. Thus there is no such matrix of order 22 or 34. They exist for all other orders up to 42 which are congruent to 2 (mod 4), and a complete classification of these is known up to order 30.

A theorem of van Lint and Seidel asserts that, if a symmetric conference matrix of order n exists, then $n-1$ is the sum of two squares. Thus there is no such matrix of order 22 or 34. They exist for all other orders up to 42 which are congruent to 2 (mod 4), and a complete classification of these is known up to order 30.

The simplest construction is that by Paley, in the case where $n-1$ is a prime power: the matrix S has rows and columns indexed by the finite field of order $n-1$, and the (i,j) entry is $+1$ if $j-i$ is a non-zero square in the field, -1 if it is a non-square, and 0 if $i=j$.

A theorem of van Lint and Seidel asserts that, if a symmetric conference matrix of order n exists, then $n-1$ is the sum of two squares. Thus there is no such matrix of order 22 or 34. They exist for all other orders up to 42 which are congruent to 2 (mod 4), and a complete classification of these is known up to order 30.

The simplest construction is that by Paley, in the case where $n-1$ is a prime power: the matrix S has rows and columns indexed by the finite field of order $n-1$, and the (i,j) entry is $+1$ if $j-i$ is a non-zero square in the field, -1 if it is a non-square, and 0 if $i=j$.

Symmetric conference matrices first arose in the field of conference telephony.

Skew conference matrices

Let C be a "skew conference matrix". By changing the sign of the first column, we can ensure that C really is skew: that is, $C^\top = -C$. Now $(C+I)(C^\top + I) = nI$, so $H = C + I$ is a Hadamard matrix. It is a skew-Hadamard matrix, as defined earlier; apart from the diagonal, it is skew. Conversely, if H is a skew-Hadamard matrix, then $H - I$ is a skew conference matrix.

Skew conference matrices

Let C be a "skew conference matrix". By changing the sign of the first column, we can ensure that C really is skew: that is, $C^\top = -C$. Now $(C+I)(C^\top + I) = nI$, so $H = C + I$ is a Hadamard matrix. It is a skew-Hadamard matrix, as defined earlier; apart from the diagonal, it is skew. Conversely, if H is a skew-Hadamard matrix, then $H - I$ is a skew conference matrix.

If C is a skew conference matrix, then S is the adjacency matrix of a doubly regular tournament, as we saw earlier. (Recall that this is a directed graph on $n-1$ vertices in which every vertex has in-degree and out-degree $(n-2)/2$ and every pair of vertices have $(n-4)/4$ common in-neighbours (and the same number of out-neighbours).

Skew conference matrices

Let C be a "skew conference matrix". By changing the sign of the first column, we can ensure that C really is skew: that is, $C^\top = -C$. Now $(C+I)(C^\top + I) = nI$, so $H = C + I$ is a Hadamard matrix. It is a skew-Hadamard matrix, as defined earlier; apart from the diagonal, it is skew. Conversely, if H is a skew-Hadamard matrix, then $H - I$ is a skew conference matrix.

If C is a skew conference matrix, then S is the adjacency matrix of a doubly regular tournament, as we saw earlier. (Recall that this is a directed graph on $n-1$ vertices in which every vertex has in-degree and out-degree $(n-2)/2$ and every pair of vertices have $(n-4)/4$ common in-neighbours (and the same number of out-neighbours).

Again this is equivalent to the existence of a skew conference matrix.

Dennis Lin's problem

Dennis Lin is interested in skew-symmetric matrices C with diagonal entries 0 (as they must be) and off-diagonal entries ± 1, and also in matrices of the form $H = C + I$ with C as described. He is interested in the largest possible determinant of such matrices of given size. Of course, it is natural to use the letters C and H for such matrices, but they are not necessarily conference or Hadamard matrices. So I will call them *cold matrices* and *hot matrices* respectively.

Dennis Lin's problem

Dennis Lin is interested in skew-symmetric matrices C with diagonal entries 0 (as they must be) and off-diagonal entries ± 1, and also in matrices of the form $H = C + I$ with C as described. He is interested in the largest possible determinant of such matrices of given size. Of course, it is natural to use the letters C and H for such matrices, but they are not necessarily conference or Hadamard matrices. So I will call them *cold matrices* and *hot matrices* respectively.

Of course, if n is a multiple of 4, the maximum determinant for C is realised by a skew conference matrix (if one exists, as is conjectured to be always the case), and the maximum determinant for H is realised by a skew-Hadamard matrix. In other words, the maximum-determinant cold and hot matrices C and H are related by $H = C + I$.

Of course, if n is a multiple of 4, the maximum determinant for C is realised by a skew conference matrix (if one exists, as is conjectured to be always the case), and the maximum determinant for H is realised by a skew-Hadamard matrix. In other words, the maximum-determinant cold and hot matrices C and H are related by $H = C + I$.

In view of the skew-Hadamard conjecture, I will not consider multiples of 4 for which a skew conference matrix fails to exist.

A skew-symmetric matrix of odd order has determinant zero; so there is nothing interesting to say in this case. So the remaining case is that in which n is congruent to 2 (mod 4).

Lin made the first half of the following conjecture, and the second half seems as well supported:

Lin made the first half of the following conjecture, and the second half seems as well supported:

Conjecture

For orders congruent to $2 \pmod 4$*, if* C *is a cold matrix with maximum determinant, then* $C + I$ *is a hot matrix with maximum determinant; and, if* H *is a hot matrix with maximum determinant, then* $H - I$ *is a cold matrix with maximum determinant.*

Lin made the first half of the following conjecture, and the second half seems as well supported:

Conjecture

For orders congruent to $2 \pmod 4$*, if* C *is a cold matrix with maximum determinant, then* $C + I$ *is a hot matrix with maximum determinant; and, if* H *is a hot matrix with maximum determinant, then* $H - I$ *is a cold matrix with maximum determinant.*

Of course, he is also interested in the related questions:

- What is the maximum determinant?

Lin made the first half of the following conjecture, and the second half seems as well supported:

Conjecture

For orders congruent to $2 \pmod 4$*, if* C *is a cold matrix with maximum determinant, then* $C + I$ *is a hot matrix with maximum determinant; and, if* H *is a hot matrix with maximum determinant, then* $H - I$ *is a cold matrix with maximum determinant.*

Of course, he is also interested in the related questions:

- What is the maximum determinant?
- How do you construct matrices achieving this maximum (or at least coming close)?

Hot matrices

Ehlich and Wojtas (independently) considered the question of the largest possible determinant of a matrix with entries ± 1 when the order is not a multiple of 4. They showed:

Hot matrices

Ehlich and Wojtas (independently) considered the question of the largest possible determinant of a matrix with entries ± 1 when the order is not a multiple of 4. They showed:

Theorem

For $n \equiv 2 \pmod 4$, the determinant of an $n \times n$ matrix with entries ± 1 is at most $2(n-1)(n-2)^{(n-2)/2}$.

Hot matrices

Ehlich and Wojtas (independently) considered the question of the largest possible determinant of a matrix with entries ± 1 when the order is not a multiple of 4. They showed:

Theorem

For $n \equiv 2 \pmod 4$, the determinant of an $n \times n$ matrix with entries ± 1 is at most $2(n-1)(n-2)^{(n-2)/2}$.

Of course this is also an upper bound for the determinant of a hot matrix.

Hot matrices

Ehlich and Wojtas (independently) considered the question of the largest possible determinant of a matrix with entries ± 1 when the order is not a multiple of 4. They showed:

Theorem

For $n \equiv 2 \pmod 4$, the determinant of an $n \times n$ matrix with entries ± 1 is at most $2(n-1)(n-2)^{(n-2)/2}$.

Of course this is also an upper bound for the determinant of a hot matrix.

We believe there should be a similar bound for the determinant of a cold matrix.

Meeting the Ehlich–Wojtas bound

Will Orrick (personal communication) showed:

Meeting the Ehlich–Wojtas bound

Will Orrick (personal communication) showed:

Theorem

A hot matrix of order n can achieve the Ehlich–Wojtas bound if and only if $2n-3$ is a perfect square.

Meeting the Ehlich–Wojtas bound

Will Orrick (personal communication) showed:

Theorem

A hot matrix of order n can achieve the Ehlich–Wojtas bound if and only if $2n-3$ is a perfect square.

This allows $n = 6$, 14, 26 and 42, but forbids, for example, $n = 10$, 18 and 22.

Computational results

These are due to me, Will Orrick, and Gordon Royle.

Computational results

These are due to me, Will Orrick, and Gordon Royle.
Lin's conjecture is confirmed for $n = 6$ and $n = 10$. The maximum determinants of hot and cold matrices are $(160, 81)$ for $n = 6$ (the former meeting the EW bound) and $(64000, 33489)$ for $n = 10$ (the EW bound is 73728). In each case there is a unique maximising matrix up to equivalence.

Computational results

These are due to me, Will Orrick, and Gordon Royle.

Lin's conjecture is confirmed for $n = 6$ and $n = 10$. The maximum determinants of hot and cold matrices are $(160, 81)$ for $n = 6$ (the former meeting the EW bound) and $(64000, 33489)$ for $n = 10$ (the EW bound is 73728). In each case there is a unique maximising matrix up to equivalence.

Random search by Gordon Royle gives strong evidence for the truth of Lin's conjecture for $n = 14$, 18, 22 and 26, and indeed finds only a few equivalence classes of maximising matrices in these cases.

Will Orrick searched larger matrices, assuming a special bi-circulant form for the matrices. He was less convinced of the truth of Lin's conjecture; he conjectures that the maximum determinant of a hot matrix is at least $cn^{n/2}$ for some positive constant c, and found pairs of hot matrices with determinants around $0.45n^{n/2}$ where the determinants of the corresponding cold matrices are ordered the other way.