Conference matrices

Peter J. Cameron

CSG, 7 October 2011

1 Hadamard matrices

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

This question was asked by Hadamard. It has some relevance to optimal design theory in statistics where minimising the determinant of the 'information matrix' gives the most accurate estimates of unkown parameters (in a certain sense); the information matrix is the inverse of a matrix obtained from the design, whose determinant thus has to be maximised.

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*
Notes:

- $HH^\top = nI \Rightarrow H^{-1} = n^{-1}H^\top \Rightarrow H^\top H = nI$, 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

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

Theorem 1 *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:

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

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* 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.

2 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 begin with some simple observations.

1. 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.

2. 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.

3. 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.

Using the third property above, 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 2 *If $n \equiv 2 \pmod 4$ then S is symmetric; if $n \equiv 0 \pmod 4$ then S is skew-symmetric.*

Proof 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

$$a+b = m-1, \qquad c+d = m;$$

row 2 gives

$$a+c = m, \qquad b+d = m-1;$$

and the inner product gives

$$a+d = m-1, \qquad b+c = m.$$

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.

3 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. Note that the same conference matrix can give rise to many different strongly regular graphs by choosing a different row and column for the normalisation.

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 $2 \pmod 4$, 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. In this connection, the following parameter is considered. Let C be a symmetric matrix with 0 on the diagonal and ± 1 elsewhere. Then the largest eigenvalue of C^2 is $n-1$, with equality if and only if C is a symmetric conference matrix. The minimum largest eigenvalue of C^2 (over all possible C) has been considered by Goethals, who showed that it is n, $n+1$ or $n+2$ if there is a symmetric conference matrix of order $n+1$, $n+2$, or $n+3$ respectively; the minimum is attained only by deleting 1, 2 or 3 rows and columns from such a conference matrix.

4 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. By similar abuse of language, it is called a *skew-Hadamard matrix*: apart from the diagonal, it is skew. Conversely, if H is a skew-Hadamard matrix, then $H-I$ is a skew conference matrix.

It is conjectured that skew-Hadamard matrices exist for every order divisible by 4. Many examples are known. The simplest are the *Paley matrices*, defined as in the symmetric case, but skew-symmetric because -1 is a non-square in the field of order q in this case.

If C is a skew conference matrix, then S is the adjacency matrix of a *strongly regular tournament* (also called a *doubly regular tournament*: 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.

5 Dennis Lin's problem

Dennis Lin is, for reasons of which I am unaware, 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* respectiely.

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 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:

For orders congruent to 2 (mod 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 achieveing this maximum (or at least coming close)?

The eigenalues of a skew-symmetric real matrix are purely imaginary, and come in complex conjugate pairs $\pm \mathrm{i}a$ for real positive a. Then we see that

$$\sum a^2 = \mathrm{Trace}(CC^\top) = n(n-1),$$

and we have

$$\det(C) = \prod a^2, \qquad \det(H) = \prod (a^2+1).$$

We would not expect that $\det(H)$ is a monotonic function (or even a well-defined function) of $\det(C)$ in general. But if $\det(C)$ is very large, then the values of a^2 will be close together (the maximum product of $n/2$ real numbers with given sum occurs when they are all equal), and so it is more likely that $\det(H)$ will also be large.

The determinant of a hot matrix is bounded above by the maximum determinant of an arbitrary ± 1 matrix, given by a theorem of Ehlich [3] and Wojtas [7]:

Theorem 3 *For $n \equiv 2$ (mod 4), the determinant of an $n \times n$ matrix with entries ± 1 is at most* $2(n-1)(n-2)^{(n-2)/2}$.

Exhaustive search in the 6×6 case easily finds the maximal determinants of hot and cold matrices, which are 81 and 160 respectively; Lin's correspondence is confirmed. Note that the Ehlich–Wojtas bound is met. The 10×10 case is rather large for exhaustive search, but I did a random search; the best determinants I found were 33489 and 64000 respectively, and again Lin's correspondence is confirmed.

I was able to make the following small contribution to a lower bound:

Theorem 4 *Let A be a skew conference matrix of order $n+2$, where n is congruent to 2 (mod 4). Let C be the matrix obtained by deleting two rows of A and the corresponding two columns. Then* $\det(C) = (n+1)^{(n-2)/2}$.

Proof A has eigenvalues $\pm\sqrt{n+1}$, each with multiplicity $(n+2)/2$. So the numbers $\pm\sqrt{n+1}$ are also eigenalues of C, with multiplicity at least $(n-2)/2$, and there is only one further pair of conjugate eigenalues, say $\pm\sqrt{x}$. Then

$$(n-2)(n+1)+2x = n(n-1).$$

We deduce that $x^2 = 1$, and so $\det(C) = (n+1)^{(n-2)/2}$, as claimed.

The analogous result for a hot matrix is obiously $2(n+2)^{(n-2)/2}$.

6 Comments from Will Orrick

After I publicised this problem, I had some comments from Will Orrick. He pointed out that the bound of Ehlich and Wojtas is attained in some cases by hot matrices of the form $\begin{pmatrix} A & B \\ B^\top & C \end{pmatrix}$, where A, B, C are circulants and A and C are hot. This enormously reduces the size of the search space. Examples exist for $n = 6$, $n = 14$, $n = 26$, and $n = 42$.

He showed that a hot matrix of order n can achieve the Ehlich–Wojtas bound only if $2n-3$ is a perfect square. Here is the argument in his words:

> Let H be a hot matrix attaining the bound. By suitable permutations and negations of rows, H may be transformed into a matrix such that the Gram matrix, $HH^\top$, has the standard optimal form, $(n-2)I + 2I_2 \otimes J_{n/2}$. Here I_2 is the 2×2 identity, $J_{n/2}$ is the $(n/2)\times(n/2)$ all ones matrix, and $\otimes$ represents the Kronecker product. Performing the same permutations and negations on columns that we performed on rows preserves hotness, and therefore $H^\top H$ has the same form.
>
> Writing $H = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, where A, B, C, D are $(n/2)\times(n/2)$ matrices, Ehlich showed that the row/column sums of the four submatrices, which we denote a, b, c, d, satisfy $a = d$, $b = -c$, $a^2 + b^2 = 2n-2$. Since A must be hot, we have $a = 1$ as before, and therefore $b^2 = 2n-3$.

Orrick conjectured that the maximum determinant of a hot matrix of order n is at least $cn^{n/2}$ for some constant c. (Note that deleting two rows and columns of a skew-Hadamard matrix of order $n+2$ falls short by a factor of about c/n.)

Finally, he is a bit sceptical about the truth of Lin's correspondence in general. He has found pairs of hot matrices with determinants around $0.45n^{n/2}$ where the determinants of the corresponding cold matrices are ordered in the opposite way.

References

[1] V. Belevitch, Conference networks and Hadamard matrices, *Ann. Soc. Sci. Bruxelles* **82**, Ser. I. (1968), 13-32.

[2] P. J. Cameron, P. Delsarte and J.-M. Goethals, Hemisystems, orthogonal configurations, and dissipative conference matrices, *Philips J. Res.* **34** (1979), 147–162.

[3] H. Ehlich, Determinantenabschätzungen für binäre Matrizen, *Math. Z.* **83** (1964), 123–132.

[4] J.-M. Goethals and J. J. Seidel, Orthogonal matrices with zero diagonal. *Canad. J. Math.* **19** (1967), 1001–1010.

[5] H. Kharaghani and B. Tayfeh-Rezaie, B, A Hadamard matrix of order 428, *Journal of Combinatorial Designs* **13** (2005), 435–440.

[6] Constructions of $n \times n$ skew-Hadamard matrices for $n = 4, 8, 12, \ldots, 96, 100$, `http://rangevoting.org/SkewHad.html`

[7] M. Wojtas, On Hadamard's inequality for the determinants of order non-divisible by 4, *Colloq. Math.* **12** (1964), 73–83.