Improved lower bounds on the Hadamard maxdet problem, Part I

Judy-anne Osborn
University of Newcastle, NSW

1 October 2013

joint work with

Richard P. Brent
Warren D. Smith

Presented at the 57th annual meeting of the Australian Mathematical Society, Sydney

Abstract

The Hadamard maximal determinant problem asks for the maximum determinant of a $\{+1, -1\}$-matrix of order n. Hadamard proved the upper bound $n^{n/2}$ which is attained if and only if a Hadamard matrix of order n exists. Various lower bounds have been given within the last half century, mostly relying on deterministic constructions. There are also some lower bounds by Best, and by Brown and Spencer, based on the idea of maximum excess, but these only apply if $n \equiv 1 \bmod 4$.

Our improved lower bounds are obtained by generalizing the idea of maximum excess using the Schur complement. In order to obtain bounds that make best use of the probabilistic method, we use not only the expected value of the diagonal elements in the Schur complement but also their variance.

Part I of the talk will give the calculation of the variance, which involves proving an unusual two-dimensional binomial identity.

Outline – Part I

- Introduction – the *maxdet* functions $D(n)$ and $R(n)$
- Bordering
- Deterministic lower bounds
- The concept of *excess*
- A generalisation using the Schur complement
- A probabilistic construction
- The mean and variance of the off-diagonal elements
- The mean and variance of the diagonal elements
- An unusual double binomial sum

Introduction – $D(n)$ and $R(n)$

Let $D(n)$ denote the maximum determinant attainable by an $n \times n$ $\{\pm 1\}$-matrix.

Hadamard (1893) gave the *upper* bound $D(n) \leq n^{n/2}$, and a matrix that achieves this bound is called a *Hadamard matrix*.

It is often convenient to consider the normalised function $R(n) := D(n)/n^{n/2}$. Hadamard's inequality is $R(n) \leq 1$.

There are many constructions for Hadamard matrices. If a Hadamard matrix of order n exists, then $n = 1$, 2, or a multiple of 4. The *Hadamard conjecture* is that Hadamard matrices exist for every positive multiple of 4. It has been verified for $n \leq 664$.

We are interested in *lower* bounds on $D(n)$ or $R(n)$.

The bordering approach

To construct a large-determinant matrix of order n, a good approach is to add a suitable border to Hadamard matrix H of order $h \leq n$.

We always choose h as large as possible, subject to $h \leq n$. It is convenient to define $d := n - h$.

Many constructions are known for Hadamard matrices, so d is "usually" small.

By a result of Livinskyi (2012), $d = O(n^{1/6})$, and Warren Smith (unpublished) claims $d = O(n^{\varepsilon})$ for all $\varepsilon > 0$.

If the Hadamard conjecture is true, then $0 \leq d \leq 3$.

Deterministic results

A deterministic construction [BO 2012] gives the lower bound

$$R(n) \geq \left(\frac{4}{ne}\right)^{d/2},$$

which is sharper than the well-known Clements and Lindström bound $(3/4)^{n/2}$, but still weak because n occurs in the denominator.

It is conjectured that

$$R(n) \geq c(d),$$

where the right-hand-side depends only on d.

Computations show that $R(n) \geq 1/2$ for all $n \leq 120$.

The concept of *excess*

The *excess* of a $\{\pm 1\}$-matrix $H = (h_{i,j})$ is

$$\sigma(H) := \sum_i \sum_j h_{i,j}.$$

We define

$$\sigma(h) := \max \sigma(H),$$

where the max is taken over Hadamard matrices of order h.

If $h \geq 4$ is the order of a Hadamard matrix, then

$$\sigma(h) \geq (2/\pi)^{1/2} h^{3/2}$$

by a (probabilistic) result of Best (1977).

The case $d = 1$

Schmidt and Wang (1977) showed that

$$D(h+1) \geq h^{h/2}(1 + \sigma(h)/h).$$

Combining this with Best's inequality on the previous slide gives

$$D(h+1) \geq h^{h/2}(1 + \sqrt{2h/\pi}).$$

This implies that

$$R(h+1) \geq \left(\frac{2}{\pi e}\right)^{1/2} \approx 0.48\,.$$

Thus, for $d = 1$ the lower bound is within a constant factor of the Hadamard upper bound.

Excess and the Schur complement

Let $e := (1, 1, \ldots, 1)^T$. Schmidt and Wang's result depends on

$$\det \begin{pmatrix} H & e \\ e^T & -1 \end{pmatrix} = -\det(H) \left(1 + \frac{\sigma(H)}{h}\right)$$

which is a special case of the Schur complement identity

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(A) \det(D - CA^{-1}B).$$

Here $D - CA^{-1}B$ is the *Schur complement* of A in $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$.

Using the Schur complement

To generalise the results for $d = 1$ to larger d, we consider a Hadamard matrix A of order h, and try to add a border of d rows and d columns so that the resulting $\{\pm 1\}$-matrix

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

has large determinant.

Since $|\det(A)| = h^{h/2}$ is fixed, this amounts to choosing the border (B, C and D) so that the Schur complement $D - CA^{-1}B$ has a large determinant.

Since A is Hadamard, $AA^T = hI$, so $A^{-1} = h^{-1}A^T$.

It is convenient to define $F := CA^{-1}B = h^{-1}CA^TB$ and we'll later need $G := F + I$.

The probabilistic construction

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

where A is an $h \times h$ Hadamard matrix, B is $h \times d$, C is $d \times h$, and D is $d \times d$. Thus $\widetilde{A}$ is $n \times n$, where $n = h + d$.

We choose B uniformly at random from the 2^{hd} possibilities, then choose $c_{ij} = \mathrm{sgn}(A^T B)_{ji}$.

Note that row i of C depends on column i of B.

The diagonal elements f_{ii} in $F = h^{-1} C A^T B$ are given by

$$f_{ii} = h^{-1} \sum_{1 \le j \le h} |(A^T B)_{ji}| \, .$$

There is no cancellation here, so $\mathbb{E}[f_{ii}]$ is of order $h^{1/2}$.

The diagonal elements of F

More precisely, for $h > 1$,

$$\mathbb{E}[f_{ii}] = 2^{-h} h \binom{h}{h/2} \sim \left(\frac{2h}{\pi}\right)^{1/2} .$$

This is due to Brown and Spencer (1971), and independently Best (1977). It depends on the binomial sum

$$\sum_p \binom{2k}{k+p} |p| = k \binom{2k}{k} , \quad (h = 2k).$$

This identity was a problem in the 1974 Putnam competition.

Off-diagonal elements

Suppose $i \neq j$, $1 \leq i, j \leq d$. The off-diagonal elements f_{ij} of F are, of course, only relevant if $d > 1$.

Since row i of C is independent of column j of B, it is easy to see that

$$\mathbb{E}[f_{ij}] = 0$$

and we [BOS arXiv:1211.3248v2] can also prove that

$$\mathbb{V}[f_{ij}] = 1,$$

where $\mathbb{V}[X] := \mathbb{E}[(X - \mathbb{E}[X])^2]$ denotes the variance of a random variable X.

Variance of the diagonal elements

It is more difficult to find the variance of the diagonal elements f_{ii} of F. We recently showed that, for $h \geq 4$,

$$\begin{aligned} \mathbb{V}[f_{ii}] &= 1 + 2^{-h}\binom{h}{2}\binom{h/2}{h/4}^2 - 2^{-2h}h^2\binom{h}{h/2}^2 \\ &= \left(1 - \frac{3}{\pi}\right) + O(h^{-1}) \leq \frac{1}{4}. \end{aligned}$$

Note that $1 - 3/\pi \approx 0.045$ is small (and independent of h).

Thus, the distribution of f_{ii} is "concentrated" near its mean.

An unusual double binomial sum

The expression for $\mathbb{V}[f_{ii}]$ depends on a double binomial sum that is analogous to the single binomial sum giving $\mathbb{E}[f_{ii}]$, but more difficult to prove.

Theorem (BO, arXiv:1309.2795)

For all $k \geq 0$,

$$\sum_p \sum_q \binom{2k}{k+p}\binom{2k}{k+q} |p^2 - q^2| = 2k^2 \binom{2k}{k}^2 .$$

Sketch of proof

Write the sum as $S_1 = S_2 + S_3$, where S_2 consists of the terms for which $p = 0$ or $q = 0$, so

$$S_2 = 2\binom{2k}{k}\sum_p \binom{2k}{k+p} p^2 = k2^{2k}\binom{2k}{k},$$

and S_3 consists of the other terms. Using symmetry, we have

$$S_3 = 8\sum_{p>q>0}\binom{2k}{k+p}\binom{2k}{k+q}(p^2 - q^2).$$

Thus, we have removed the absolute value function, at the expense of having to sum over a triangular region $0 < q < p \leq k$.

Sketch of proof (continued)

Now, writing $p^2 - q^2 = (p-k)(p+k) - (q-k)(q+k)$ and using some well-known binomial identities, we get

$$
\begin{aligned}
S_3 \quad = \quad & 16k(2k-1) \times \\
& \left\{ \left[\sum_{p>q>0} \binom{2k-2}{k+p}\binom{2k-2}{k+q-1} - \sum_{p>q\geq 0} \binom{2k-2}{k+p}\binom{2k-2}{k+q-1} \right] \right. \\
+ \quad & \left. \left[\sum_{p>q\geq 0} \binom{2k-2}{k+p-1}\binom{2k-2}{k+q} - \sum_{p>q>0} \binom{2k-2}{k+p-1}\binom{2k-2}{k+q} \right] \right\} .
\end{aligned}
$$

The expressions inside each pair of square brackets both involve a kind of two-variable telescoping sum – the only terms that do not cancel are those for $q = 0$. The resulting one-dimensional sums can be evaluated explicitly, and the result follows. For details see arXiv:1309.2795v2. □

Stay tuned for Part II