Probabilistic lower bounds on maximal determinants of binary matrices

Richard P. Brent
Australian National University
Canberra, ACT 2600, Australia

Judy-anne H. Osborn
The University of Newcastle
Callaghan, NSW 2308, Australia

Warren D. Smith
Center for Range Voting
21 Shore Oaks Drive, Stony Brook
NY 11790, USA

February 19, 2015

Abstract

Let $D(n)$ be the maximal determinant for $n \times n \{\pm 1\}$-matrices, and $R(n) = D(n)/n^{n/2}$ be the ratio of $D(n)$ to the Hadamard upper bound. Using the probabilistic method, we prove new lower bounds on $D(n)$ and $R(n)$ in terms of the distance $d$ to the nearest (smaller) Hadamard matrix, defined by $d = n - h$, where $h$ is the order of a Hadamard matrix and $h$ is maximal subject to $h \leq n$. The lower bounds on $R(n)$ are

$$R(n) > \left(\frac{2}{\pi e}\right)^{d/2} \quad 1 \leq d \leq 3,$$

and

$$R(n) > \left(\frac{2}{\pi e}\right)^{d/2} \left(1 - d^2 \left(\frac{\pi}{2h}\right)^{1/2}\right) \quad d > 3.$$

Since $d^2/h^{1/2} \to 0$ as $n \to \infty$, the latter bound is close to $(\pi e/2)^{-d/2}$ for large $n$. Previous lower bounds tended to zero as $n \to \infty$ with $d$ fixed, except in the cases $d \in \{0, 1\}$. For $d \geq 2$, our bounds are better for all sufficiently large $n$. If the Hadamard conjecture is true, then $R(n)$ is bounded below by a positive constant $(\pi e/2)^{-3/2} > 0.1133$. 
1 Introduction

Let $D(n)$ be the maximal determinant possible for an $n \times n$ matrix with elements in $\{\pm 1\}$. Hadamard [14] proved that $D(n) \leq n^{n/2}$, and the Hadamard conjecture is that a matrix achieving this upper bound exists for each positive integer $n$ divisible by four. The function $R(n) := D(n)/n^{n/2}$ is a measure of the sharpness of the Hadamard bound. Clearly $R(n) = 1$ if a Hadamard matrix of order $n$ exists; otherwise $R(n) < 1$. In this paper we give lower bounds on $R(n)$.

Let $H$ be the set of orders of Hadamard matrices, and let $h \in H$ be maximal subject to $h \leq n$. Then $d = n - h$ can be regarded as the “gap” between $n$ and the nearest (lower) Hadamard order. We are interested the case that $n$ is not a Hadamard order, i.e. $d > 0$ and $R(n) < 1$.

Except in the cases $d \in \{0, 1\}$, previous lower bounds on $R(n)$ tended to zero as $n \to \infty$. For example, the well-known bound of Clements and Lindström [10, Corollary to Thm. 2] shows that $R(n) > (3/4)^{n/2}$, and [3, Thm. 9] shows that $R(n) \geq n^{-\delta/2}$, where $\delta := |n - h|$ (in this result $h > n$ is allowed, so it is possible that $0 < \delta < d$). In contrast, we show that, for fixed $d$, $R(n)$ is bounded below by a positive constant. We conjecture that $R(n) \geq (\pi e/2)^{-d/2}$; this is certainly true if $d \leq 3$, so it is implied by the Hadamard conjecture.

Our lower bound proof uses the probabilistic method pioneered by Erdős (see for example [11,12]). This method does not appear to have been applied previously to the Hadamard maximal determinant problem, except in the case $d = 1$ (so $n \equiv 1 \mod 4$); in this case the concept of excess has been used [13], and lower bounds on the maximal excess were obtained by the probabilistic method [2,8,12,13].

§2 describes our probabilistic construction and determines the mean $\mu$ and variance $\sigma^2$ of elements in the Schur complement generated by the construction (see Lemmas 6–7). Informally, we adjoin $d$ extra columns to an $h \times h$ Hadamard matrix $A$, and fill their $h \times d$ entries with random (uniformly and independently distributed) $\pm 1$ values. Then we adjoin $d$ extra rows, and fill their $d \times (h + d)$ entries with values chosen deterministically in a way intended to approximately maximise the determinant of the final matrix $\tilde{A}$. To do so, we use the fact that this determinant can be expressed in terms of the $d \times d$ Schur complement of $A$ in $\tilde{A}$.

In the case $d = 1$, this method is essentially the same as the known method involving the excess of matrices Hadamard-equivalent to $A$, and leads to the same bounds that can be obtained by bounding the excess in a probabilistic manner.
In §3 we give lower bound results for both $D(n)$ and $R(n)$. The results for $D(n)$ are generally slightly sharper. However, it is easier to compare bounds on $R(n)$ because of the normalisation. We outline the bounds on $R(n)$ here. Theorem 1 gives a lower bound

$$\mathcal{R}(n) > \left(\frac{2}{\pi e}\right)^{d/2} \left(1 - d^2 \left(\frac{\pi}{2h}\right)^{1/2}\right)$$

which is nontrivial whenever $h > \pi d^{1/2}$. By the results of Livinskyi [19], $d = O(h^{1/6})$ as $h \to \infty$ (see [3] §6 for details), so the condition $h > \pi d^{1/2}$ holds for all sufficiently large $n$. For fixed $d > 1$ and large $n$, the lower bounds on $R(n)$ are better than previous bounds that tended to zero with $n$ (see Table 1 in §4).

Slightly sharper results for large $n$ are given in [6]. They depend on the same probabilistic construction, which leads to a factor $(\pi e/2)^{-d/2}$ in the bounds – the improvements are only to the less significant term $O(d^2/h^{1/2})$.

We give sharper results for the cases $1 \leq d \leq 3$. In these cases, Theorem 2 shows that the factor $1 - O(d^2/h^{1/2})$ of Theorem 1 can be omitted, giving $\mathcal{R}(n) > (\pi e/2)^{-d/2}$. In particular, if the Hadamard conjecture is true, then $d \leq 3$ and $\mathcal{R}(n) > (\pi e/2)^{-3/2} > 0.1133$.

In §4 we give some numerical examples to illustrate Theorems 1–2 and compare our results with previous bounds on $D(n)$ and/or $R(n)$.

Rokicki et al [21] showed, by extensive computation, that $\mathcal{R}(n) \geq 1/2$ for $n \leq 120$, and conjectured that this inequality always holds. It seems difficult to bridge the gap between the constants $1/2$ and $(\pi e/2)^{-3/2}$ by the probabilistic method.

Acknowledgements

We thank Robert Craigen for informing us of the work of his student Ivan Livinskyi [19], and Will Orrick for a copy of the unpublished report [21]. The first author was supported in part by Australian Research Council grant DP140101417.

2 The probabilistic construction

We now describe the probabilistic construction that we use and prove some of its properties. Our construction is a generalisation of Best’s, which is the case $d = 1$. 
Let \( A \) be a Hadamard matrix of order \( h \geq 4 \). We add a border of \( d \) rows and columns to give a larger (square) matrix \( \tilde{A} \) of order \( n \). The border is defined by matrices \( B \), \( C \) and \( D \) as shown:

\[
\tilde{A} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}.
\]

The \( d \times d \) matrix \( D - CA^{-1}B \) is known as the Schur complement of \( A \) in \( \tilde{A} \) after Schur \[22\]. The Schur complement lemma (see for example \[11\]) gives

\[
\det(\tilde{A}) = \det(A) \det(D - CA^{-1}B).
\]

In our construction the matrices \( A \), \( B \), and \( C \) have entries in \( \{\pm 1\} \). We allow the matrix \( D \) to have entries in \( \{0, \pm 1\} \), but each zero entry can be replaced by at least one of \(+1\) or \(-1\) without decreasing \( |\det(\tilde{A})| \), so any lower bounds that we obtain on \( \max(|\det(A)|) \) are valid lower bounds on maximal determinants of \( n \times n \ \{\pm 1\}\)-matrices. Note that the Schur complement is not in general a \( \{\pm 1\}\)-matrix.

In the proof of Lemma \[9\] we show that our choice of \( B \), \( C \) and \( D \) gives a Schur complement \( D - CA^{-1}B \) that, with positive probability, has sufficiently large determinant. From equation \(3\) and the fact that \( A \) is a Hadamard matrix, a large value of \( \det(D - CA^{-1}B) \) implies a large value of \( \det(A) \).

### 2.1 Details of the probabilistic construction

Let \( A \) be any Hadamard matrix of order \( h \). \( B \) is allowed to range over the set of all \( h \times d \ \{\pm 1\}\)-matrices, chosen uniformly and independently from the \( 2^{hd} \) possibilities. The \( d \times h \) matrix \( C = (c_{ij}) \) is a function of \( B \). We choose

\[
c_{ij} = \text{sgn}(A^T B)_{ji},
\]

where

\[
\text{sgn}(x) := \begin{cases} +1 & \text{if } x \geq 0, \\ -1 & \text{if } x < 0. \end{cases}
\]

To complete the construction, we choose \( D = -I \). As mentioned above, it is inconsequential that \( D \) is not a \( \{\pm 1\}\)-matrix.

### 2.2 Properties of the construction

Define \( F = CA^{-1}B \) and \( G = F - D = F + I \) (so \(-G\) is the Schur complement defined above). Note that, since \( A \) is a Hadamard matrix, \( A^T = hA^{-1} \), so \( hF = CA^T B \).
The definition of $C$ ensures that there is no cancellation in the inner products defining the diagonal entries of $hF = C \cdot (A^T B)$. Thus, we expect the diagonal entries $f_{ii}$ of $F$ to be nonnegative and of order $h^{1/2}$, but the off-diagonal entries $f_{ij}$ ($i \neq j$) to be of order unity with high probability. Similarly for the elements of $G$. This intuition is justified by Lemmas 1, 5–7.

In the following we denote the expectation of a random variable $X$ by $\mathbb{E}[X]$, and the variance by $\mathbb{V}[X] = \mathbb{E}[X^2] - \mathbb{E}[X]^2$.

Lemmas 1, 2 are essentially due to M. R. Best [2] and J. H. Lindsey.

**Lemma 1.** If $h \geq 2$ and $F = (f_{ij})$ is chosen as above, then

\[
\mathbb{E}[f_{ij}] = \begin{cases} 
2^{-h}h \left( \frac{h}{h/2} \right) & \text{if } i = j, \\
0 & \text{if } i \neq j.
\end{cases}
\]

**Proof.** The case $i = j$ follows from Best [2, Theorem 3]. The case $i \neq j$ is easy, since $B$ is chosen randomly. \hfill \square

**Lemma 2.** If $F = (f_{ij})$ is chosen as above, then $|f_{ij}| \leq h^{1/2}$ for $1 \leq i, j \leq d$.

**Proof.** This follows from the Cauchy-Schwarz inequality as in Theorem 1 of Best [2]. \hfill \square

**Lemma 3.** If $F$ is chosen as above and $\{i, j\} \cap \{k, \ell\} = \emptyset$, then $f_{ij}$ and $f_{k\ell}$ are independent.

**Proof.** This follows from the fact that $f_{ij}$ depends only on the fixed matrix $A$ and on columns $i$ and $j$ of $B$. \hfill \square

**Lemma 4.** Let $A \in \{\pm 1\}^{h \times h}$ be a Hadamard matrix, $C \in \{\pm 1\}^{d \times h}$, and $U = CA^{-1}$. Then, for each $i$ with $1 \leq i \leq d$,

\[
\sum_{j=1}^{h} u_{ij}^2 = 1.
\]

**Proof.** Since $A$ is Hadamard, $A^T A = hI$. Thus $UU^T = h^{-1}CC^T$. Since $c_{ij} = \pm 1$, $\text{diag}(CC^T) = hI$. Thus $\text{diag}(UU^T) = I$. \hfill \square

**Lemma 5.** If $F = (f_{ij})$ is chosen as above, then

\[
\mathbb{E}[f_{ij}^2] = 1 \text{ for } i \neq j.
\]  

\footnote{See [12] footnote on pg. 68}.
Proof. We can assume, without essential loss of generality, that $i = 1, j > 1$. Write $F = UB$, where $U = CA^{-1} = h^{-1}CA^T$. Now

$$f_{ij} = \sum_k u_{1k} b_{kj}, \quad (5)$$

where

$$u_{1k} = \frac{1}{h} \sum_{\ell} c_{1\ell} a_{k\ell}, \quad c_{1\ell} = \text{sgn} \left( \sum_m b_{m1} a_{m\ell} \right).$$

Observe that $c_{1\ell}$ and $u_{1k}$ depend only on the first column of $B$. Thus, $f_{ij}$ depends only on the first and $j$-th columns of $B$. If we fix the first column of $B$ and take expectations over all choices of the other columns, we obtain

$$\mathbb{E}[f_{ij}^2] = \mathbb{E} \left[ \sum_k \sum_{\ell} u_{1k} u_{1\ell} b_{kj} b_{\ell j} \right].$$

The expectation of the terms with $k \neq \ell$ vanishes, and the expectation of the terms with $k = \ell$ is $\sum_k u_{1k}^2$. Thus, (4) follows from Lemma 4.

Lemma 6. Let $A$ be a Hadamard matrix of order $h \geq 4$ and $C$ be $\{\pm 1\}$-matrices chosen as above. Let $G = F + I$ where $F = CA^{-1}B$. Then

$$\mathbb{E}[g_{ii}] = 1 + \frac{h}{2h} \left( \frac{h}{2} \right), \quad (6)$$

$$\mathbb{E}[g_{ij}] = 0 \text{ for } 1 \leq i, j \leq d, i \neq j, \quad (7)$$

$$\mathbb{V}[g_{ii}] = 1 + \frac{h(h-1)}{2h+1} \left( \frac{h/2}{h/4} \right)^2 - \frac{h^2}{2h} \left( \frac{h}{2} \right)^2, \quad (8)$$

$$\mathbb{V}[g_{ij}] = 1 \text{ for } 1 \leq i, j \leq d, i \neq j. \quad (9)$$

Proof. Since $G = F + I$, the results (6), (7) and (9) follow from Lemma 4 and Lemma 5 above. Thus, we only need to prove (8). Since $g_{ii} = f_{ii} + 1$, it is sufficient to compute $\mathbb{V}[f_{ii}]$.

Since $A$ is a Hadamard matrix, $hF = CA^T B$. We compute the second moment about the origin of the diagonal elements $hf_{ii}$ of $hF$. Since $h$ is a Hadamard order and $h \geq 4$, we can write $h = 4k$ where $k \in \mathbb{Z}$. Consider $h$ independent random variables $X_j \in \{\pm 1\}, 1 \leq j \leq h$, where $X_j = +1$ with probability $1/2$. Define random variables $S_1, S_2$ by

$$S_1 = \sum_{j=1}^{4k} X_j, \quad S_2 = \sum_{j=1}^{2k} X_j - \sum_{j=2k+1}^{4k} X_j.$$
Consider a particular choice of $X_1, \ldots, X_h$ and suppose that $k + p$ of $X_1, \ldots, X_{2k}$ are +1, and that $k + q$ of $X_{2k+1}, \ldots, X_{4k}$ are +1. Then we have $S_1 = 2(p + q)$ and $S_2 = 2(p - q)$. Thus, taking expectations over all $2^{4k}$ possible (equally likely) choices, we see that

$$
\mathbb{E} \left[ |S_1 S_2| \right] = 4 \mathbb{E} \left[ |p^2 - q^2| \right] = \frac{4}{2^{4k}} \sum_p \sum_q \binom{2k}{k + p} \binom{2k}{k + q} |p^2 - q^2| 
$$

$$
= \frac{4}{2^{4k}} \cdot 2k^2 \binom{2k}{k} = \frac{h^2}{2^{h+1}} \binom{2k}{k}^2 ,
$$

where the evaluation of the double sum is given in [4, Theorem 1]. By the definitions of $B$, $C$ and $F$, we see that $h f_{ii}$ is a sum of the form $Y_1 + Y_2 + \cdots + Y_h$, where each $Y_j$ is a random variable with the same distribution as $|S_1|$, and each product $Y_j Y_\ell$ (for $j \neq \ell$) has the same distribution as $|S_1 S_2|$. Also, $Y_j^2$ has the same distribution as $|S_1|^2 = S_1^2$. The random variables $Y_j$ are not independent, but by linearity of expectations we obtain

$$
h^2 \mathbb{E}[f_{ii}^2] = h \mathbb{E}[S_1^2] + h(h - 1) \mathbb{E}[|S_1 S_2|] = h^2 + h(h - 1) \cdot \frac{h^2}{2^{h+1}} \binom{2k}{k}^2 .
$$

This gives

$$
\mathbb{E}[f_{ii}^2] = 1 + \frac{h(h - 1)}{2^{h+1}} \binom{2k}{k}^2 .
$$

The result for $\nabla[g_{ii}]$ now follows from $\nabla[g_{ii}] = \mathbb{E}[f_{ii}] = \mathbb{E}[f_{ii}^2] - \mathbb{E}[f_{ii}]^2$. 

For convenience we write $\mu(h) := \mathbb{E}[g_{ii}] = \mathbb{E}[f_{ii}] + 1$ and $\sigma(h)^2 := \nabla[g_{ii}]$. If $h$ is understood from the context we write simply $\mu$ and $\sigma^2$ respectively.

We now give some asymptotic approximations to $\mu(h)$ and $\sigma(h)^2$ that are accurate for large $h$. We also show that $\mu(h)$ is of order $h^{1/2}$, but $\sigma(h)$ is bounded and monotonic decreasing.

**Lemma 7.** For $h \in 4\mathbb{Z}$, $h \geq 4$, $\sigma(h)^2$ is monotonic decreasing. Moreover, the following inequalities hold:

$$
\sqrt{\frac{2h}{\pi}} + 0.9 < \mu(h) < \sqrt{\frac{2h}{\pi}} + 1 ,
$$

$$
\sigma(h)^2 \leq \sigma(4)^2 = 0.25 ,
$$

and

$$
\sigma(h)^2 = \left(1 - \frac{3}{\pi} \right) + \frac{11}{4\pi h} - \frac{\beta(h)}{h^2} ,
$$

where

$$
\beta(h) = \frac{\sqrt{2h}}{\pi} \left( \sqrt{\frac{2h}{\pi}} + 0.9 \right) .
$$
where

\[ 0 \leq \beta(h) \leq 12 - 37/\pi < 0.23. \quad (13) \]

Proof. From the well-known asymptotic expansion of \( \ln \Gamma(z) \) we obtain, as in [15], an asymptotic expansion for the logarithm of the central binomial coefficient:

\[
\ln \left( \frac{2m}{m} \right) \sim m \ln 4 - \frac{\ln(\pi m)}{2} - \sum_{k \geq 1} \frac{B_{2k}(1 - 4^{-k})}{k(2k - 1)} m^{1-2k}. \quad (14)
\]

Here the \( B_{2k} \) are Bernoulli numbers, and \((-1)^{k+1}B_{2k}\) is positive. The sum is not convergent, but the terms in the sum alternate in sign, so upper and lower bounds may be found by truncating the series after an even or an odd number of terms.

The inequalities (10) and (12)–(13) now follow from a straightforward computation, using the expressions for \( \mu(h) \) and \( \sigma(h)^2 \) in Lemma 6 and approximations obtained from (14) with \( m = h/2 \) and \( m = h/4 \). Note that the leading terms (of order \( h \)) cancel in the computation of \( \sigma(h)^2 \).

From (12), using the bounds on \( \beta(h) \) in (13), we have

\[
\sigma(h + 4)^2 \leq 1 - \frac{3}{\pi} + \frac{11}{4\pi(h + 4)} < 1 - \frac{3}{\pi} + \frac{11}{4\pi h} - \frac{0.23}{h^2} \leq \sigma(h)^2.
\]

Thus, \( \sigma(h)^2 \) is monotonic decreasing for \( h \in 4\mathbb{Z} \). Finally, the inequality (11) follows from the monotonicity of \( \sigma(h)^2 \).

3 A probabilistic lower bound

We now prove lower bounds on \( D(n) \) and \( R(n) \) where, as usual, \( n = h + d \) and \( h \) is the order of a Hadamard matrix. The key result is Lemma 9. Theorem 1 simply converts the result of Lemma 9 into lower bounds on \( D(n) \) and \( R(n) \), giving away a little for the sake of simplicity in the latter case.

For the proof of Lemma 9 we need the following bound on the determinant of a matrix which is “close” to the identity matrix. It is due to Ostrowski [20, eqn. (5.5)]; see also [7, Corollary 2].

Lemma 8 (Ostrowski). If \( M = I - E \in \mathbb{R}^{d \times d} \), \( |e_{ij}| \leq \varepsilon \) for \( 1 \leq i, j \leq d \), and \( d \varepsilon \leq 1 \), then

\[
\det(M) \geq 1 - d\varepsilon.
\]
Lemma 9. Suppose $d \geq 1$, $4 \leq h \in \mathcal{H}$, $n = h + d$, $G$ as in §2.2. Then, with positive probability,

$$\frac{\det G}{\mu^d} \geq 1 - \frac{d^2}{\mu}. \quad (15)$$

Proof. Let $\lambda$ be a positive parameter to be chosen later, and $\mu = \mu(h)$. We say that $G$ is good if the conditions of Lemma 8 apply with $M = \mu^{-1}G$ and $\varepsilon = \lambda/\mu$. Otherwise $G$ is bad.

Assume $1 \leq i, j \leq d$. From Lemma 6, $V[g_{ij}] = 1$ for $i \neq j$; from Lemma 7, $V[g_{ii}] = \sigma(h)^2 \leq 1/4$. It follows from Chebyshev’s inequality [9] that

$$\mathbb{P}[|g_{ij}| \geq \lambda] \leq \frac{1}{\lambda^2} \quad \text{for } i \neq j,$$

and

$$\mathbb{P}[|g_{ii} - \mu| \geq \lambda] \leq \frac{\sigma^2}{\lambda^2}.$$

Thus,

$$\mathbb{P}[G \text{ is bad}] \leq \frac{d(d-1)}{\lambda^2} + \frac{d\sigma^2}{\lambda^2} < \frac{d^2}{\lambda^2}.$$

Taking $\lambda = d$ gives $\mathbb{P}[G \text{ is bad}] < 1$, so $\mathbb{P}[G \text{ is good}]$ is positive. Whenever $G$ is good we can apply Lemma 8 to $\mu^{-1}G$, obtaining $\mu^{-d}\det(G) = \det(\mu^{-1}G) \geq 1 - d\varepsilon = 1 - d\lambda/\mu = 1 - d^2/\mu$. \qed

The following lemma is useful for deducing inequalities for $\mathcal{R}(n)$ from inequalities for $D(n)$.

Lemma 10. If $n = h + d > h > 0$, then

$$\left(\frac{h}{n}\right)^n > \exp(-d - d^2/h).$$

Proof. Writing $x = d/n$, the inequality $\ln(1 - x) > -x/(1 - x)$ implies that

$$\left(1 - x\right)^n > \exp\left(-\frac{nx}{1 - x}\right).$$

Since $1 - x = h/n$, we obtain

$$\left(\frac{h}{n}\right)^n > \exp\left(\frac{-d}{1 - d/n}\right) = \exp(-d - d^2/h). \quad \Box$$
Theorem 1. Suppose $d \geq 1$, $4 \leq h \in \mathcal{H}$, and $n = h + d$. Then

$$D(n) \geq h^{3/2} \mu^d (1 - d^2 / \mu) \quad \text{where} \quad \mu = 1 + \frac{h}{2h} \left( \frac{h}{h/2} \right),$$

and

$$\mathcal{R}(n) > \left( \frac{2}{\pi e} \right)^{d/2} \left( 1 - d^2 \sqrt{\frac{\pi}{2h}} \right).$$

Proof. Lemma 9 and the Schur complement lemma imply that there exists an $n \times n \{\pm 1\}$-matrix with determinant at least $h^{3/2} \mu^d (1 - d^2 / \mu)$. Thus, (16) follows from the definition of $D(n)$.

We now show that (17) follows from (16) by some elementary inequalities.

Write $c := \sqrt{2/\pi}$. We can assume that $d^2 < ch^{1/2}$, for there is nothing to prove unless the right side of (17) is positive. From Lemma 7, $ch^{1/2} < \mu$, so $d^2 < \mu$. Also, from (16),

$$\mathcal{R}(n) \geq \frac{h^{3/2} \mu^d}{n^{3/2}} \left( 1 - \frac{d^2}{\mu} \right).$$

Using $ch^{1/2} < \mu$, this gives

$$\mathcal{R}(n) > c^d (h/n)^{3/2} (1 - d^2 / \mu).$$

By Lemma 10 $(h/n)^n > \exp(-d - d^2 / h)$, so

$$\mathcal{R}(n) > c^d e^{-d^2 / h} f = \left( \frac{2}{\pi e} \right)^{d/2} f,$$

where

$$f = \exp \left( - \frac{d^2}{2h} \left( 1 - \frac{d^2}{\mu} \right) \right).$$

Thus, to prove (17), it suffices to prove that $f \geq 1 - d^2 / (ch^{1/2})$. Since $\exp(-d^2/(2h)) \geq 1 - d^2/(2h)$, it suffices to prove that

$$\left( 1 - \frac{d^2}{2h} \right) \left( 1 - \frac{d^2}{\mu} \right) \geq 1 - \frac{d^2}{ch^{1/2}}.$$

Expanding and simplifying shows that the inequality (21) is equivalent to

$$2h + \mu \leq d^2 + \mu \sqrt{2\pi h}.$$
Now, by Lemma 7, \( \mu > c \sqrt{h} + 0.9 \), so \( \mu \sqrt{2\pi h} > 2h + 0.9 \sqrt{2\pi h} \) (using \( c \sqrt{2\pi} = 2 \)). Thus, to prove (22), it suffices to show that \( \mu \leq d^2 + 0.9 \sqrt{2\pi h} \).

Using Lemma 7 again, we have \( \mu \leq ch^{1/2} + 1 \), so it suffices to show that

\[
ch^{1/2} + 1 \leq 0.9 \sqrt{2\pi h} + d^2.
\]

This follows from \( c \leq 0.9 \sqrt{2\pi} \) and \( 1 \leq d^2 \), so the proof is complete.

**Remark 1.** The inequality (17) of Theorem 1 gives a nontrivial lower bound on \( R(n) \) iff the second factor in the bound is positive, i.e. iff \( h > \pi d^4/2 \).

By Livinskyi’s results [19], this condition holds for all sufficiently large \( n \) (assuming as always that we choose the maximal \( h \leq n \) for given \( n \)).

The Hadamard conjecture implies that \( d \leq 3 \). Theorem 2 improves on Theorem 1 under the assumption that \( d \leq 3 \). In the proof of Theorem 2 we simply expand \( \det(G) \), obtaining \( d! \) terms. By Lemma 3, the expectation of the diagonal term is \( \mathbb{E}[g_{11} \cdots g_{dd}] = \mu^d \). The expectation of the off-diagonal terms can be bounded to give the desired lower bound on \( D(n) \). The same approach gives weak results for \( d > 3 \) because of the large number of off-diagonal terms (see [5, Theorem 1]).

**Theorem 2.** If \( 1 \leq d \leq 3 \), \( h \in \mathcal{H} \), and \( n = h + d \), then

\[
D(n) \geq h^{d/2}(\mu^d - \eta) \quad \text{and} \quad R(n) > \left( \frac{2}{\pi e} \right)^{d/2},
\]

where

\[
\eta = \begin{cases} 
    d - 1 & \text{if } 1 \leq d \leq 2, \\
    5h^{d/2} + 3 & \text{if } d = 3.
\end{cases}
\]

**Proof.** It is easy to verify the result for \( h \in \{1, 2\} \), so suppose that \( h \geq 4 \). For notational convenience we give the proof for the case \( d = 2 \). The cases \( d \in \{1, 3\} \) are similar.

Since \( G = F + I \), we have \( g_{ii} = f_{ii} + 1 \) and \( \det(G) = g_{11}g_{22} - f_{12}f_{21} \). By Lemma 3 the diagonal elements \( g_{11} \) and \( g_{22} \) are independent, so

\[
\mathbb{E}[g_{11}g_{22}] = \mathbb{E}[g_{11}]\mathbb{E}[g_{22}] = \mu^2.
\]

By the Cauchy-Schwarz inequality and Lemma 5

\[
\mathbb{E}[f_{12}f_{21}]^2 \leq \mathbb{E}[f_{12}^2]\mathbb{E}[f_{21}^2] = 1.
\]

\[\text{A detailed proof for the case } d = 3 \text{ is given in [6, proof of Lemma 17].}\]
Thus
\[ \mathbb{E}[\det(G)] = \mathbb{E}[g_{11}g_{22}] - \mathbb{E}[f_{12}f_{21}] \geq \mu^2 - 1. \]

There must exist some \( G_0 \) with \( \det(G_0) \geq \mathbb{E}[\det(G)] \geq \mu^2 - 1 \); hence
\[ D(n) \geq h^{h/2}(\mu^2 - 1). \]

This proves the required lower bound for \( D(n) \) if \( d = 2 \). We now deduce the required lower bound for \( R(n) = D(n)/n^{n/2} \). Define \( c := \sqrt{2/\pi} \) and \( K := 0.9/c \). From Lemma 7, \( \mu \geq c(h^{1/2} + K) \), so \( \mu^2 \geq c^2 h(1 + 2Kh^{-1/2}) \). Thus, using \( n = h + 2 \),
\[ D(n) \geq c^2 h^{n/2} \left( 1 + 2Kh^{-1/2} - \frac{\eta}{c^2h} \right). \]

From Lemma 10 with \( d = 2 \), \( (h/n)^{n/2} \geq e^{-1-2/h} \geq e^{-1}(1 - 2/h) \), so
\[ R(n) = \frac{D(n)}{n^{n/2}} \geq \left( \frac{2}{\pi e} \right) \left( 1 + 2Kh^{-1/2} - \frac{1}{c^2h} \right) \left( 1 - \frac{2}{h} \right). \]

Since \( K \) is positive, the term \( 2Kh^{-1/2} \) dominates the \( O(h^{-1}) \) terms, and the result \( R(n) \geq 2/(\pi e) \) follows for all sufficiently large \( h \). In fact, a small computation shows that the inequality holds for all \( h \geq 4 \).

\[ \square \]

4 Numerical examples

In this section we give some numerical comparisons between our lower bounds and previously-known bounds.

There are two well-known approaches to constructing a large-determinant \( \{\pm 1\} \)-matrix of order \( n \). The bordering approach takes a Hadamard matrix \( H \) of order \( h \leq n \) and adjoins a border of \( d = n - h \) rows and columns. The border is constructed in a manner intended to result in a large determinant. Previously, deterministic constructions were used – see for example \[3, \text{Lemma 7}\]. In this paper we have used a probabilistic construction.

The minors approach takes a Hadamard matrix \( H_+ \) of order \( h_+ \geq n \) and finds an \( n \times n \) submatrix with large determinant. This approach was used deterministically by Koukouvinos et al \[16, 17\], and probabilistically by de Launey and Levin \[18\]. The deterministic approach can be generalised using a theorem of Szöllőzi \[23\], and this is better for \( h_+ \leq n + 6 \) than the probabilistic approach of \[18\] – see \[3\] Remarks 6 and 22.

To illustrate Theorem 1, consider the case \( n = 668, d = 4 \). At the time of writing, \( n \) is the smallest positive multiple of 4 that is not known to be in \( \mathcal{H} \). It is known that \( h := n - 4 \in \mathcal{H} \) and \( h_+ := n + 4 \in \mathcal{H} \).
Theorem 2

\[ \frac{4}{n} \approx 17.93, \quad \frac{2}{\pi e} \approx 0.4839, \quad \frac{2}{\pi e} \approx 0.4839 \]

\[ \frac{2e}{n} \approx 5.437, \quad \frac{8}{\pi e^2 n} \approx 0.5871, \quad \frac{2}{\pi e} \approx 0.2342 \]

\[ \frac{(e/n)^{1/2}}{n^{1/2}} \approx 1.649, \quad \frac{e^{1/2}}{n^{1/2}} \approx 1.649, \quad \frac{2}{\pi e} \approx 0.1133 \]

Table 1: Asymptotics of lower bounds on \( R(n) \) as \( n \to \infty \).

<table>
<thead>
<tr>
<th>( d )</th>
<th>KMS 16</th>
<th>B&amp;O 3</th>
<th>Theorem 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4 ( \frac{e^{3/2}}{n^{3/2}} \approx 17.93 )</td>
<td>( \frac{2}{\pi e} \approx 0.4839 )</td>
<td>( \frac{2}{\pi e} \approx 0.4839 )</td>
</tr>
<tr>
<td>2</td>
<td>( \frac{2e}{n} \approx 5.437 )</td>
<td>( \frac{8}{\pi e^2 n} \approx 0.5871 )</td>
<td>( \frac{2}{\pi e} \approx 0.2342 )</td>
</tr>
<tr>
<td>3</td>
<td>( \frac{(e/n)^{1/2}}{n^{1/2}} \approx 1.649 )</td>
<td>( \frac{e^{1/2}}{n^{1/2}} \approx 1.649 )</td>
<td>( \frac{2}{\pi e} \approx 0.1133 )</td>
</tr>
</tbody>
</table>

Table 2: Comparison of lower bounds on \( R(n) \) for \( d = 2 \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>KMS 16</th>
<th>B&amp;O 3</th>
<th>Thm. 1</th>
<th>Thm. 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.4147</td>
<td>0.1856</td>
<td>–</td>
<td>0.3752</td>
</tr>
<tr>
<td>14</td>
<td>0.3183</td>
<td>0.1569</td>
<td>–</td>
<td>0.3609</td>
</tr>
<tr>
<td>18</td>
<td>0.2581</td>
<td>0.1384</td>
<td>0.0127</td>
<td>0.3498</td>
</tr>
<tr>
<td>38</td>
<td>0.1325</td>
<td>0.0952</td>
<td>0.1004</td>
<td>0.3193</td>
</tr>
<tr>
<td>82</td>
<td>0.0639</td>
<td>0.0648</td>
<td>0.1516</td>
<td>0.2945</td>
</tr>
<tr>
<td>998</td>
<td>0.0054</td>
<td>0.0186</td>
<td>0.2142</td>
<td>0.2524</td>
</tr>
<tr>
<td>limit</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.2342</td>
<td>0.2342</td>
</tr>
</tbody>
</table>

The deterministic bordering approach [3, Lemma 7] gives a lower bound

\[ R(n) \geq 2^d h^{h/2} / n^{1/2} \approx 4.88 \times 10^{-6}. \tag{23} \]

The deterministic minors approach gives a lower bound

\[ R(n) \geq 16 h^{h/2-4} / n^{1/2} \approx 2.60 \times 10^{-4}. \tag{24} \]

The probabilistic bordering approach of Theorem 1 gives a lower bound (18)

\[ R(n) \geq h^{h/2} \mu^d (1 - d^2/\mu) / n^{1/2} \approx 1.69 \times 10^{-2}, \tag{25} \]

where \( \mu \) is as in (16). Clearly the bound (23) is a significant improvement on the bounds (24). It is not too far from our conjectured lower bound of \( (\pi e/2)^{-d/2} \approx 5.48 \times 10^{-2} \).

The bound of Clements and Lindström [10], which does not depend on minors or bordering, is much weaker: \( R(n) \geq (3/4)^{n/2} \approx 1.86 \times 10^{-42} \).
To illustrate Theorem 2, Table 1 summarises the asymptotics of some lower bounds on \( R(n) \) for \( d = n \mod 4 \in \{1, 2, 3\} \), assuming that \( n - d \in \mathcal{H} \), \( n + 4 - d \in \mathcal{H} \). The bounds are those given in Koukouvinos et al. [16], Brent and Osborn [3, Table 1], and Theorem 2 of the present paper. It can be seen that we improve on the previous bounds by a factor of order at least \( n^{1/2} \) for \( d \in \{2, 3\} \).

Since asymptotics may be misleading for small \( n \), Table 2 gives lower bounds on \( R(n) \) for various values of \( n \equiv 2 \mod 4 \) (so \( d = 2 \)). The bound of [16] is best for \( n \leq 10 \), but for \( n \geq 14 \) the first bound of Theorem 2 is best. The bound of [3] is never best, but it is better than that of [16] for \( n \geq 82 \). The first bound of Theorem 1 is always worse than that of Theorem 2 (when the latter is applicable, i.e. for \( d \leq 3 \)), but they are asymptotically equal as \( n \to \infty \).

In the case \( d = 3 \), the minors approach fares better (provided \( n + 1 \in \mathcal{H} \)). The asymptotics given in Table 1 suggest that the crossover point should be at \( n \approx \pi^2 e^4 / 8 \approx 211 \). In fact, the crossover point is somewhat smaller: a computation shows that the first bound of our Theorem 2 is sharper than the bound \( D(n) \geq (n + 1)^{(n-1)/2} \) of [16, Thm. 2] if \( n \geq 135 \).

References


