AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **66(3)** (2016), Pages 350–364

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
U.S.A.

In memory of Mirka Miller 1949–2016

Abstract

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

$$\mathcal{R}(n) > \left(\frac{2}{\pi e}\right)^{d/2} \text{ if } 1 \le d \le 3, \text{ and}$$

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

By a recent result of Livinskyi, $d^2/h^{1/2} \to 0$ as $n \to \infty$, so the second 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 $d \ge 2$, our bounds are better for all sufficiently large n. If the Hadamard conjecture is true, then $d \le 3$, so the first bound above shows that $\mathcal{R}(n)$ is bounded below by a positive constant $(\pi e/2)^{-3/2} > 0.1133$.

1 Introduction

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

Let $\mathcal{H}$ be the set of orders of Hadamard matrices, and let $h \in \mathcal{H}$ be maximal subject to $h \le n$. 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 $\mathcal{R}(n) < 1$.

Except in the cases $d \in \{0, 1\}$, previous lower bounds on $\mathcal{R}(n)$ tended to zero as $n \to \infty$. For example, the well-known bound of Clements and Lindström [10, Corollary to Thm. 2] shows that $\mathcal{R}(n) > (3/4)^{n/2}$, and [4, Thm. 9] shows that $\mathcal{R}(n) \ge (ne/4)^{-d/2}$. In contrast, our results imply that, for fixed d, $\mathcal{R}(n)$ is bounded below by a positive constant (depending only on d).

Our lower bound proof uses the probabilistic method pioneered by Erdős (see for example [1, 12]). This method does not appear to have been applied previously to the Hadamard maximal determinant problem, except in the case $d = 1$ (so $n \equiv 1 \bmod 4$); 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 μ and variance σ^2 of elements in the Schur complement generated by the construction (see Lemmas 2.6 and 2.8). 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) ± 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 $\widetilde{A}$. 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 $\widetilde{A}$.

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 on both $\mathcal{D}(n)$ and $\mathcal{R}(n)$. Of course, a lower bound on $\mathcal{D}(n)$ immediately gives an equivalent lower bound on $\mathcal{R}(n)$. However, we use some elementary inequalities to obtain simpler (though slightly weaker) bounds on $\mathcal{R}(n)$. For example, if $d \le 3$ then Theorem 3.6 states that $\mathcal{D}(n) \ge h^{h/2}(\mu^d - \eta)$, where μ and η are certain functions of h and d. Theorem 3.6 also states the (weaker) result that $\mathcal{R}(n) > (\pi e/2)^{-d/2}$. The lower bound on $\mathcal{R}(n)$ clearly shows that the ratio of our bound to the Hadamard bound is at least $(\pi e/2)^{-3/2} > 0.1133$, whereas this conclusion is not immediately obvious from the lower bound on $\mathcal{D}(n)$.

We outline the bounds on $\mathcal{R}(n)$ here. Theorem 3.4 gives a lower bound

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

which is nontrivial whenever $h > \pi d^4/2$. By the results of Livinskyi [19], $d = O(h^{1/6})$ as $h \to \infty$ (see [6, §6] for details), so the condition $h > \pi d^4/2$ holds for all sufficiently large n. Also, as $n \to \infty$, $d^2/h^{1/2} = O(n^{-1/6}) \to 0$, so the lower bound (1) is close to $(\pi e/2)^{-d/2}$. For fixed $d > 1$ and large n, our lower bounds on $\mathcal{R}(n)$ are better than previous bounds (see Table 1 in §4).

Theorem 3.6 applies only for $d \le 3$, but whenever it is applicable it gives sharper results than Theorem 3.4. In fact, Theorem 3.6 shows that the factor $1 - O(d^2/h^{1/2})$ in (1) can be omitted when $d \le 3$, giving $\mathcal{R}(n) > (\pi e/2)^{-d/2}$. Theorem 3.6 is always applicable if the Hadamard conjecture is true, since this conjecture implies that $d \le 3$.

In §4, we give some numerical examples to illustrate Theorems 3.4 and 3.6, and to compare our results with previous bounds on $\mathcal{D}(n)$ and/or $\mathcal{R}(n)$.

Rokicki *et al* [22] showed, by extensive computation, that $\mathcal{R}(n) \ge 1/2$ for $n \le 120$, 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. The best that we can do is to improve the term of order $d^2/h^{1/2}$ in the bound (1) at the expense of a more complicated proof – for details see [6].

2 The probabilistic construction

We now describe our probabilistic construction and prove some of its properties. In the case $d = 1$ our construction reduces to that of Best [2].

Let A be a Hadamard matrix of order $h \ge 4$. We add a border of d rows and columns to give a larger (square) matrix $\widetilde{A}$ of order n. The border is defined by matrices B, C and D as shown:

$$\widetilde{A} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}. \tag{2}$$

The $d \times d$ matrix $D - CA^{-1}B$ is known as the *Schur complement* of A in $\widetilde{A}$ after Schur [23]. The *Schur complement lemma* (see for example [11]) gives

$$\det(\widetilde{A}) = \det(A)\det(D - CA^{-1}B). \tag{3}$$

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 one of $+1$ or -1 without decreasing $|\det(\widetilde{A})|$, so any lower bounds that we obtain on $\max(|\det(\widetilde{A})|)$ 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 3.2 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 $\det(\widetilde{A})$.

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

$$c_{ij} = \operatorname{sgn}(A^T B)_{ji}\,,$$

where

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

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 $hF = CA^T B$.

Since B is random, we expect the elements of $A^T B$ to be usually of order $h^{1/2}$. 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 2.6 and 2.8.

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 2.1–2.2 are essentially due to Best [2] and Lindsey.[1]

Lemma 2.1. *If $h \geq 2$ and $F = (f_{ij})$ is chosen as above, then*

$$\mathbb{E}[f_{ij}] = \begin{cases} 2^{-h} h \dbinom{h}{h/2} & \textit{if } \; i = j, \\ 0 \;\; \textit{if } \; i \neq j. \end{cases}$$

Proof. The case $i = j$ follows as in Best [2, proof of Theorem 3]. The case $i \neq j$ is easy, since B is chosen randomly. □

Lemma 2.2. *If $F = (f_{ij})$ is chosen as above, then $|f_{ij}| \leq h^{1/2}$ for $1 \leq i, j \leq d$.*

Proof. The matrix $Q := h^{-1/2} A^T$ is orthogonal with rows and columns of unit length (in the Euclidean norm). Thus $||Qb||_2 = ||b||_2 = h^{1/2}$ for each column b of B. Since $h^{1/2} F = C.QB$, each element $h^{1/2} f_{ij}$ of $h^{1/2} F$ is the inner product of a row of C (having length $h^{1/2}$) and a column of QB (also having length $h^{1/2}$). It follows from the Cauchy-Schwartz inequality that $|h^{1/2} f_{ij}| \leq h^{1/2} \cdot h^{1/2} = h$, so $|f_{ij}| \leq h^{1/2}$. □

[1] See [12, footnote on pg. 88].

Lemma 2.3. *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. □

Lemma 2.4. *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 $1 \le i \le d$,*

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

Proof. Since A is Hadamard, $UU^T = h^{-1}CC^T$. Also, since $c_{ij} = \pm 1$, $\mathrm{diag}(CC^T) = hI$. Thus $\mathrm{diag}(UU^T) = I$. □

Lemma 2.5. *If $F = (f_{ij})$ is chosen as above, then*

$$\mathbb{E}[f_{ij}^2] = 1 \text{ for } i \neq j. \tag{4}$$

Proof. We can assume, without loss of generality, that $i = 1$, $j > 1$. Write $F = UB$, where $U = CA^{-1} = h^{-1}CA^T$. Now

$$f_{1j} = \sum_k u_{1k} b_{kj}, \tag{5}$$

where

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

Observe that $c_{1\ell}$ and u_{1k} depend only on the first column of B. Thus, f_{1j} 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

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

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 2.4. □

Lemma 2.6. *Let A be a Hadamard matrix of order $h \ge 4$ and B, C be $\{\pm 1\}$-matrices chosen as above. Let $G = F + I$ where $F = CA^{-1}B$. Then*

$$\mathbb{E}[g_{ii}] = 1 + \frac{h}{2^h}\binom{h}{h/2}, \tag{6}$$

$$\mathbb{E}[g_{ij}] = 0 \text{ for } 1 \le i,j \le d,\ i \neq j, \tag{7}$$

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

$$\mathbb{V}[g_{ij}] = 1 \text{ for } 1 \le i,j \le d,\ i \neq j. \tag{9}$$

Proof. Since $G = F + I$, the results (6), (7) and (9) follow from Lemma 2.1 and Lemma 2.5 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, $hF = CA^TB$. We compute the second moment about the origin of the diagonal elements hf_{ii} of hF. Since h is a Hadamard order and $h \ge 4$, we can write $h = 4k$ where $k \in \mathbb{Z}$. Consider h independent random variables $X_j \in \{\pm 1\}$, $1 \le j \le h$, 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

$$\begin{aligned}\mathbb{E}[|S_1S_2|] = 4\mathbb{E}[|p^2-q^2|] &= \frac{4}{2^{4k}} \sum_p \sum_q \binom{2k}{k+p}\binom{2k}{k+q}|p^2-q^2| \\ &= \frac{4}{2^{4k}} \cdot 2k^2 \binom{2k}{k}^2 = \frac{h^2}{2^{h+1}}\binom{2k}{k}^2.\end{aligned}$$

Here the closed form for the double sum is a special case of [3, Prop. 1.1]. By the definitions of B, C and F, we see that hf_{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_jY_ℓ (for $j \ne \ell$) has the same distribution as $|S_1S_2|$. 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

$$h^2\mathbb{E}[f_{ii}^2] = h\mathbb{E}[S_1^2] + h(h-1)\mathbb{E}[|S_1S_2|] = h^2 + h(h-1) \cdot \frac{h^2}{2^{h+1}}\binom{2k}{k}^2.$$

This gives

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

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

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

To estimate μ and σ^2 from Lemma 2.6, we need a sufficiently accurate estimate for a central binomial coefficient $\binom{2m}{m}$ (where $m = h/2$ or $h/4$). An asymptotic expansion for $\ln\binom{2m}{m}$ may be deduced from Stirling's asymptotic expansion of $\ln\Gamma(z)$, as in [15]. However, [15] does not give an error bound. We state such a bound in the following Lemma, which may be of independent interest.

Lemma 2.7. *If k and m are positive integers, then*

$$\ln \binom{2m}{m} = m \ln 4 - \frac{\ln(\pi m)}{2} - \sum_{j=1}^{k-1} \frac{B_{2j}(1-4^{-j})}{j(2j-1)} m^{1-2j} + e_k(m), \tag{10}$$

where

$$|e_k(m)| < \frac{|B_{2k}|}{k(2k-1)} m^{1-2k}. \tag{11}$$

Proof. Using the facts that m is real and positive, and that the sign of the Bernoulli number B_{2k} is $(-1)^{k-1}$, we obtain from Olver [20, (4.03) and (4.05) of Ch. 8] that

$$\ln \Gamma(m) = (m - \tfrac{1}{2}) \ln m - m + \frac{\ln(2\pi)}{2} + \sum_{j=1}^{k-1} \frac{B_{2j}}{2j(2j-1)} m^{1-2j} - (-1)^k r_k(m), \tag{12}$$

where

$$0 < r_k(m) < \frac{|B_{2k}|}{2k(2k-1)} m^{1-2k}. \tag{13}$$

Now

$$\binom{2m}{m} = \frac{(2m)!}{m!m!} = \frac{2}{m} \frac{\Gamma(2m)}{\Gamma(m)^2},$$

so from (12) and the same equation with $m \mapsto 2m$ we obtain (10) with

$$e_k(m) = (-1)^k (2r_k(m) - r_k(2m)).$$

Using the bound (13), this gives

$$e_k(m) = \frac{(-1)^k |B_{2k}|}{k(2k-1)} m^{1-2k} \theta,$$

where $-2^{-2k} < \theta < 1$. In particular, $|\theta| < 1$, so we obtain the desired bound (11). □

We now show that $\mu(h)$ is of order $h^{1/2}$, and that $\sigma(h)$ is bounded.

Lemma 2.8. *For $h \in 4\mathbb{Z}$, $h \geq 4$, we have*

$$\sigma(h)^2 < 1 \tag{14}$$

and

$$\sqrt{\frac{2h}{\pi}} + 0.9 < \mu(h) < \sqrt{\frac{2h}{\pi}} + 1. \tag{15}$$

Proof. From Lemma 2.7 with $k = 2$ and m a positive integer, we have

$$\binom{2m}{m} = \frac{4^m}{\sqrt{\pi m}} \exp\left[-\frac{1}{8m} + \frac{\theta_m}{180m^3}\right], \tag{16}$$

where $|\theta_m| < 1$.

First consider the bounds (16) on $\mu(h)$. Taking $m = h/2$ and using the expression (6) for $\mu(h)$, the inequality (15) is equivalent to

$$\sqrt{\frac{m}{\pi}} - \frac{1}{20} < \frac{m}{4^m}\binom{2m}{m} < \sqrt{\frac{m}{\pi}}\,.$$

The upper bound is immediate from (16), since $-\frac{1}{8m} + \frac{1}{180m^3} < 0$.

For the lower bound, a computation verifies the inequality for $m = 2$, since $\sqrt{2/\pi} - \frac{1}{20} < \frac{3}{4} = \frac{m}{4^m}\binom{2m}{m}$. Hence, we can assume that $m \geq 4$. The lower bound now follows from (16), since

$$\frac{m}{4^m}\binom{2m}{m} > \sqrt{\frac{m}{\pi}}\,\exp\left[-\frac{1}{8m} - \frac{1}{180m^3}\right] > \sqrt{\frac{m}{\pi}}\left[1 - \frac{1}{8m} - \frac{1}{180m^3}\right]$$

and

$$\sqrt{\frac{m}{\pi}}\left[\frac{1}{8m} + \frac{1}{180m^3}\right] < \frac{1}{20}\,.$$

Now consider the upper bound (14) on $\sigma(h)^2$. From (16) we have

$$\binom{h/2}{h/4}^2 < \frac{2^{h+2}}{\pi h}\exp\left[-\frac{1}{h} + \frac{32}{45h^3}\right]$$

and

$$\binom{h}{h/2}^2 > \frac{2^{2h+1}}{\pi h}\exp\left[-\frac{1}{2h} - \frac{4}{45h^3}\right]\,.$$

Using these inequalities in (8) and simplifying gives

$$\begin{aligned}\sigma(h)^2 < 1 + \frac{2h}{\pi}&\left[\exp\left(-\frac{1}{h} + \frac{32}{45h^3}\right) - \exp\left(-\frac{1}{2h} - \frac{4}{45h^3}\right)\right]\\ &- \frac{2}{\pi}\exp\left(-\frac{1}{h} + \frac{32}{45h^3}\right)\,. \qquad (17)\end{aligned}$$

It is easy to see that the term in square brackets is negative for $h \geq 4$, so (17) implies (14). □

Remark 2.9. *We can show from* (17) *and a corresponding lower bound on* $\sigma(h)^2$ *that* $\sigma(h+4)^2 < \sigma(h)^2$, *so* $\sigma(h)^2$ *is monotonic decreasing and bounded above by* $\sigma(4)^2 = \frac{1}{4}$. *Also, for large* h *we have* $\sigma(h)^2 = (1 - 3/\pi) + O(1/h)$. *Since these results are not needed below, we omit the details.*

3 A probabilistic lower bound

We now prove lower bounds on $\mathcal{D}(n)$ and $\mathcal{R}(n)$ where, as usual, $n = h + d$ and h is the order of a Hadamard matrix. The key result is Lemma 3.2. Theorem 3.4 simply converts the result of Lemma 3.2 into lower bounds on $\mathcal{D}(n)$ and $\mathcal{R}(n)$, giving away a little for the sake of simplicity in the latter case.

For the proof of Lemma 3.2 we need the following bound on the determinant of a matrix which is "close" to the identity matrix. It is due to Ostrowski [21, eqn. (5,5)]; see also [7, Corollary 1].

Lemma 3.1 (Ostrowski)**.** *If* $M = I - E \in \mathbb{R}^{d\times d}$, $|e_{ij}| \le \varepsilon$ *for* $1 \le i, j \le d$, *and* $d\varepsilon \le 1$, *then*

$$\det(M) \ge 1 - d\varepsilon.$$

The idea of Lemma 3.2 is that we can, with positive probability, apply Lemma 3.1 to the matrix $M = \mu^{-1}G$, thus obtaining a lower bound on the maximum value attained by $\det(G)$.

Lemma 3.2. *Suppose* $d \ge 1$, $4 \le h \in \mathcal{H}$, $n = h + d$, G *as in* §2.2. *Then, with positive probability,*

$$\frac{\det G}{\mu^d} \ge 1 - \frac{d^2}{\mu}. \tag{18}$$

Proof. Let λ be a positive parameter to be chosen later, and $\mu = \mu(h)$. We say that G is *good* if the conditions of Lemma 3.1 apply with $M = \mu^{-1}G$ and $\varepsilon = \lambda/\mu$. Otherwise G is *bad*.

Assume $1 \le i, j \le d$. From Lemma 2.6, $\mathbb{V}[g_{ij}] = 1$ for $i \ne j$; from Lemma 2.8, $\mathbb{V}[g_{ii}] = \sigma^2 < 1$. It follows from Chebyshev's inequality [9] that

$$\mathbb{P}[|g_{ij}| \ge \lambda] \le \frac{1}{\lambda^2} \text{ for } i \ne j,$$

and

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

Thus,

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

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 3.1 to $\mu^{-1}G$, obtaining $\mu^{-d}\det(G) = \det(\mu^{-1}G) \ge 1 - d\varepsilon = 1 - d\lambda/\mu = 1 - d^2/\mu$. □

The following lemma is useful for deducing lower bounds on $\mathcal{R}(n)$.

Lemma 3.3. *If* $n = h + d > h > 0$, *then*

$$(h/n)^n > \exp(-d - d^2/h).$$

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

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

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

$$\left(\frac{h}{n}\right)^n > \exp\left(\frac{-d}{1 - d/n}\right) = \exp(-d - d^2/h).$$ □

We are now ready to prove our main result. Theorem 3.4 gives lower bounds on $\mathcal{D}(n)$ and $\mathcal{R}(n)$. If the reader needs a lower bound for a specific value of n, then the inequality (19) should be used. The inequality (20) is slightly weaker than what can be obtained simply by dividing both sides of (19) by $n^{n/2}$, but it shows more clearly the asymptotic behaviour if n and h are large but d is small.

Theorem 3.4. *Suppose $d \geq 1$, $4 \leq h \in \mathcal{H}$, and $n = h + d$. Then*

$$\mathcal{D}(n) \geq h^{h/2}\mu^d(1 - d^2/\mu), \tag{19}$$

where $\mu = 1 + \frac{h}{2^h}\binom{h}{h/2}$. Also,

$$\mathcal{R}(n) > \left(\frac{2}{\pi e}\right)^{d/2}\left(1 - d^2\sqrt{\frac{\pi}{2h}}\right). \tag{20}$$

Proof. Lemma 3.2 and the Schur complement lemma imply that there exists an $n \times n$ $\{\pm 1\}$-matrix with determinant at least $h^{h/2}\mu^d(1 - d^2/\mu)$. Thus, (19) follows from the definition of $\mathcal{D}(n)$.

We now show that (20) follows from (19) 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 (20) is positive. From Lemma 2.8, $ch^{1/2} < \mu$, so $d^2 < \mu$. Also, from (19),

$$\mathcal{R}(n) \geq \frac{h^{h/2}\mu^d}{n^{n/2}}\left(1 - \frac{d^2}{\mu}\right). \tag{21}$$

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

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

By Lemma 3.3, $(h/n)^n > \exp(-d - d^2/h)$, so

$$\mathcal{R}(n) > c^d e^{-d/2} f = \left(\frac{2}{\pi e}\right)^{d/2} f, \tag{22}$$

where

$$f = \exp\left(-\frac{d^2}{2h}\right)\left(1 - \frac{d^2}{\mu}\right). \tag{23}$$

Thus, to prove (20), 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

$$\left(1 - \frac{d^2}{2h}\right)\left(1 - \frac{d^2}{\mu}\right) \geq 1 - \frac{d^2}{ch^{1/2}}. \tag{24}$$

Expanding and simplifying shows that the inequality (24) is equivalent to

$$2h + \mu \leq d^2 + \mu\sqrt{2\pi h}. \tag{25}$$

Now, by Lemma 2.8, $\mu > c\sqrt{h} + 0.9$, so $\mu\sqrt{2\pi h} > 2h + 0.9\sqrt{2\pi h}$ (using $c\sqrt{2\pi} = 2$). Thus, to prove (25), it suffices to show that $\mu \le d^2 + 0.9\sqrt{2\pi h}$. Using Lemma 2.8 again, we have $\mu \le ch^{1/2} + 1$, so it suffices to show that

$$ch^{1/2} + 1 \le 0.9\sqrt{2\pi h} + d^2.$$

This follows from $c \le 0.9\sqrt{2\pi}$ and $1 \le d^2$, so the proof is complete. □

Remark 3.5. The inequality (20) of Theorem 3.4 gives a nontrivial lower bound on $\mathcal{R}(n)$ 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 $h \le n$ for given n).

The Hadamard conjecture implies that $d \le 3$. Theorem 3.6 improves on Theorem 3.4 under the assumption that $d \le 3$. The proof of Theorem 3.6 is conceptually simpler than that of Theorem 3.4, since it does not require any bounds on the variance $\sigma(h)^2$. In the proof of Theorem 3.6 we simply expand $\det(G)$, obtaining $d!$ terms. By Lemma 2.3, 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 $\mathcal{D}(n)$. The same approach gives weak results for $d > 3$ because of the large number $(d! - 1)$ of off-diagonal terms (see [5, Theorem 1]).

Theorem 3.6. *If* $1 \le d \le 3$, $h \in \mathcal{H}$, $n = h + d$, *and* μ *as in* (19), *then*

$$\mathcal{D}(n) \ge h^{h/2}(\mu^d - \eta) \ \ \text{and} \ \ \mathcal{R}(n) > \left(\frac{2}{\pi e}\right)^{d/2},$$

where

$$\eta = \begin{cases} d - 1 \ \text{if } 1 \le d \le 2, \\ 5h^{1/2} + 3 \ \text{if } d = 3. \end{cases}$$

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

Since $G = F+I$, we have $g_{ii} = f_{ii}+1$ and $\det(G) = g_{11}g_{22} - f_{12}f_{21}$. By Lemma 2.3, 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 2.5,

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

Thus

$$\mathbb{E}[\det(G)] = \mathbb{E}[g_{11}g_{22}] - \mathbb{E}[f_{12}f_{21}] \ge \mu^2 - 1.$$

[2] A detailed proof for the case $d = 3$ is given in [6, proof of Lemma 17].

There must exist some G_0 with $\det(G_0) \ge \mathbb{E}[\det(G)] \ge \mu^2 - 1$; hence

$$\mathcal{D}(n) \ge h^{h/2}(\mu^2 - 1).$$

This proves the required lower bound for $\mathcal{D}(n)$ if $d = 2$. We now deduce the required lower bound for $\mathcal{R}(n) = \mathcal{D}(n)/n^{n/2}$. Define $c := \sqrt{2/\pi}$ and $K := 0.9/c$. From Lemma 2.8, $\mu \ge c(h^{1/2} + K)$, so $\mu^2 \ge c^2 h(1 + 2Kh^{-1/2})$. Thus, using $n = h + 2$,

$$\mathcal{D}(n) \ge c^2 h^{n/2}\left(1 + 2Kh^{-1/2} - \frac{\eta}{c^2 h}\right).$$

From Lemma 3.3 with $d = 2$, $(h/n)^{n/2} \ge e^{-1-2/h} \ge e^{-1}(1 - 2/h)$, so

$$\mathcal{R}(n) = \frac{\mathcal{D}(n)}{n^{n/2}} \ge \left(\frac{2}{\pi e}\right)\left(1 + 2Kh^{-1/2} - \frac{1}{c^2 h}\right)\left(1 - \frac{2}{h}\right).$$

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

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 $h \le n$ 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 [4, Lemma 7]. In this paper we have used a probabilistic construction.

The *minors* approach takes a Hadamard matrix H_+ of order $h_+ \ge n$ 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 Szöllősi [24], and this is better for $h_+ \le n + 6$ than the probabilistic approach of [18] – see [4, Remarks 6 and 22].

To illustrate Theorem 3.4, 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 $h_+ := n + 4 \in \mathcal{H}$.
The deterministic bordering approach [4, Lemma 7] gives a lower bound $\mathcal{R}(n) \ge 2^d h^{h/2}/n^{n/2} \approx 4.88 \times 10^{-6}$. The deterministic minors approach gives a lower bound $\mathcal{R}(n) \ge 16 h_+^{h_+/2-4}/n^{n/2} \approx 2.60 \times 10^{-4}$. The probabilistic bordering approach of Theorem 3.4 gives a lower bound (eqn. (21) above) $\mathcal{R}(n) \ge h^{h/2}\mu^d(1 - d^2/\mu)/n^{n/2} \approx 1.69 \times 10^{-2}$, where μ is as in (19). For comparison, our conjectured lower bound is $(\pi e/2)^{-d/2} \approx 5.48 \times 10^{-2}$.

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

d	KMS [16]	B&O [4]	Theorem 3.6
1	$4\left(\frac{e}{n}\right)^{3/2} \approx \frac{17.93}{n^{3/2}}$	$\left(\frac{2}{\pi e}\right)^{1/2} \approx 0.4839$	$\left(\frac{2}{\pi e}\right)^{1/2} \approx 0.4839$
2	$\frac{2e}{n} \approx \frac{5.437}{n}$	$\left(\frac{8}{\pi e^2 n}\right)^{1/2} \approx \frac{0.5871}{n^{1/2}}$	$\frac{2}{\pi e} \approx 0.2342$
3	$\left(\frac{e}{n}\right)^{1/2} \approx \frac{1.649}{n^{1/2}}$	$\left(\frac{e}{n}\right)^{1/2} \approx \frac{1.649}{n^{1/2}}$	$\left(\frac{2}{\pi e}\right)^{3/2} \approx 0.1133$

To illustrate Theorem 3.6, Table 1 summarises the asymptotics of some lower bounds on $\mathcal{R}(n)$ for $d = (n \bmod 4) \in \{1, 2, 3\}$, 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 [4, Table 1], and Theorem 3.6 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 $\mathcal{R}(n)$ for various values of $n \equiv 2 \bmod 4$ (so $d = 2$).

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

n	KMS [16]	B&O [4]	Thm. 3.4	Thm. 3.6
10	0.4147	0.1856	–	0.3752
14	0.3183	0.1569	–	0.3609
18	0.2581	0.1384	0.0127	0.3498
98	0.0538	0.0593	0.1601	0.2897
998	0.0054	0.0186	0.2142	0.2524
limit	0.0000	0.0000	0.2342	0.2342

In the case $d = 3$, a computation shows that the first bound of our Theorem 3.6 is sharper than the bound $\mathcal{D}(n) \geq (n+1)^{(n-1)/2}$ of [16, Thm. 2] if $n \geq 135$ (where the latter bound assumes that $n + 1 \in \mathcal{H}$).

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 [22]. We also thank an anonymous referee who helped us to improve both the rigor and clarity of the paper.

The first author was supported in part by Australian Research Council grant DP140101417.

References

[1] N. Alon and J. H. Spencer, *The Probabilistic Method*, 3rd ed., Wiley, 2008.

[2] M. R. Best, The excess of a Hadamard matrix, *Nederl. Akad. Wetensch. Proc. Ser. A* **80** = *Indag. Math.* **39** (1977), 357–361.

[3] R. P. Brent, C. Krattenthaler and S. O. Warnaar, Discrete analogues of Mehta-type integrals, *J. Combin. Theory Ser. A* **144** (2016), 80–138.

[4] R. P. Brent and J. H. Osborn, General lower bounds on maximal determinants of binary matrices, *Electron. J. Comb.* **20**(2) (2013), #P15, 12 pp.

[5] R. P. Brent, J. H. Osborn and W. D. Smith, *Lower bounds on maximal determinants of* ± 1 *matrices via the probabilistic method*, arXiv:1211.3248v3, 5 May 2013, 32 pp.

[6] R. P. Brent, J. H. Osborn and W. D. Smith, *Lower bounds on maximal determinants of binary matrices via the probabilistic method*, arXiv:1402.6817v2, 13 March 2014, 37 pp.

[7] R. P. Brent, J. H. Osborn and W. D. Smith, Bounds on determinants of perturbed diagonal matrices, *Linear Alg. Appl.* **466** (2015), 21–26.

[8] T. A. Brown and J. H. Spencer, Minimization of ± 1 matrices under line shifts, *Colloq. Math.* **23** (1971), 165–171. Erratum *ibid* pg. 177.

[9] P. Chebyshev, Des valeurs moyennes, *J. Math. Pure Appl.* **2** (1867), 177–184.

[10] G. F. Clements and B. Lindström, A sequence of (± 1)-determinants with large values, *Proc. Amer. Math. Soc.* **16** (1965), 548–550.

[11] R. W. Cottle, Manifestations of the Schur complement, *Linear Alg. Appl.* **8** (1974), 189–211.

[12] P. Erdős and J. Spencer, *Probabilistic Methods in Combinatorics*, Akadémiai Kiadó, Budapest, 1974. Also published by Academic Press, New York, 1974.

[13] N. Farmakis and S. Kounias, The excess of Hadamard matrices and optimal designs, *Discrete Math.* **67** (1987), 165–176.

[14] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. des Sci. Math.* **17** (1893), 240–246.

[15] D. Kessler and J. Schiff, *The asymptotics of factorials, binomial coefficients and Catalan numbers*, `http://u.math.biu.ac.il/~schiff/Papers/prepap3.pdf`, April 2006.

[16] C. Koukouvinos, M. Mitrouli and J. Seberry, Bounds on the maximum determinant for $(1, -1)$ matrices, *Bull. Inst. Combinatorics and its Applications* **29** (2000), 39–48.

[17] C. Koukouvinos, M. Mitrouli and J. Seberry, An algorithm to find formulæ and values of minors for Hadamard matrices, *Linear Alg. Appl.* **330** (2001), 129–147.

[18] W. de Launey and D. A. Levin, $(1, -1)$-matrices with near-extremal properties, *SIAM J. Discrete Math.* **23** (2009), 1422–1440.

[19] I. Livinskyi, *Asymptotic existence of Hadamard matrices*, M.Sc. thesis, University of Manitoba, `http://hdl.handle.net/1993/8915`, 2012.

[20] F. W. J. Olver, *Asymptotics and Special Functions*, Academic Press, New York, 1974.

[21] A. M. Ostrowski, Sur l'approximation du déterminant de Fredholm par les déterminants des systèmes d'equations linéaires, *Ark. Math. Stockholm* **26A** (1938), 1–15.

[22] T. Rokicki, I. Kazmenko, J-C. Meyrignac, W. P. Orrick, V. Trofimov and J. Wroblewski, *Large determinant binary matrices: results from Lars Backstrom's programming contest*, unpublished report, July 31, 2010.

[23] I. Schur, Über Potenzreihen, die im Innern des Einheitskreises beschränkt sind, *J. Reine Angew. Math.* **147** (1917), 205–232.

[24] F. Szöllősi, Exotic complex Hadamard matrices and their equivalence, *Cryptogr. Commun.* **2** (2010), 187–198.

(Received 19 Jan 2015; revised 29 Jan 2016, 1 Aug 2016)