Lower bounds on maximal determinants of binary matrices via the probabilistic method

Richard P. Brent
Australian National University
Canberra, ACT 0200, 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

October 26, 2016

Abstract

Let $D(n)$ be the maximal determinant for $n \times n$ $\{\pm 1\}$-matrices, and $\mathcal{R}(n) = D(n)/n^{n/2}$ be the ratio of $D(n)$ to the Hadamard upper bound. We give several new lower bounds on $\mathcal{R}(n)$ in terms of d, where $n = h + d$, h is the order of a Hadamard matrix, and h is maximal subject to $h \leq n$. A relatively simple bound is

$$\mathcal{R}(n) \geq \left(\frac{2}{\pi e}\right)^{d/2} \left(1 - d^2 \left(\frac{\pi}{2h}\right)^{1/2}\right) \quad \text{for all} \ \ n \geq 1.$$

An asymptotically sharper bound is

$$\mathcal{R}(n) \geq \left(\frac{2}{\pi e}\right)^{d/2} \exp\left(d \left(\frac{\pi}{2h}\right)^{1/2} + O\left(\frac{d^{5/3}}{h^{2/3}}\right)\right).$$

We also show that

$$\mathcal{R}(n) \geq \left(\frac{2}{\pi e}\right)^{d/2}$$

if $n \geq n_0$ and n_0 is sufficiently large, the threshold n_0 being independent of d, or for all $n \geq 1$ if $0 \leq d \leq 3$ (which would follow from the Hadamard conjecture). The proofs depend on the probabilistic method, and generalise previous results that were restricted to the cases $d = 0$ and $d = 1$.

1 Introduction

Let $D(n)$ be the maximal determinant possible for an $n \times n$ matrix with elements in $\{\pm 1\}$. Hadamard [31][1] 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 $\mathcal{R}(n) := D(n)/n^{n/2}$ 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 $\mathcal{R}(n)$.

Let h be the maximal order of a Hadamard matrix 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, so (usually) $d > 0$ 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 [16, Corollary to Thm. 2] shows that $\mathcal{R}(n) > (3/4)^{n/2}$, and [8, Thm. 9] shows that $\mathcal{R}(n) \geq n^{-\delta/2}$, where $\delta := |n - h|$ (in this result $h > n$ is allowed, so it is possible that $\delta < d$). In contrast, we show that, for fixed d, $\mathcal{R}(n)$ is bounded below by a positive constant κ_d. We also show that, for all sufficiently large n, $\mathcal{R}(n) \geq (\pi e/2)^{-d/2}$. We conjecture that the "sufficiently large" condition can be omitted; this is certainly true if $d \leq 3$.

Our lower bound proofs use the probabilistic method pioneered by Erdős (see for example [1, 29]). In many cases the probabilistic method gives sharper bounds than have been obtained by deterministic methods. The probabilistic method does not appear to have been applied previously to the Hadamard maximal determinant problem, except (implicitly) in the case $d = 1$ (so $n \equiv 1 \bmod 4$); in this case the concept of *excess* has been used [30], and lower bounds on the maximal excess were obtained by the probabilistic method [6, 29, 30]. In a sense our results generalise this idea, although we do not directly generalise the concept of excess to cover $d > 1$.

Specifically, in our probabilistic construction we adjoin d extra columns to an $h \times h$ Hadamard matrix A, and fill their $h \times d$ entries with random signs obtained by independently tossing fair coins. Then we adjoin d extra rows, and fill their $d \times (h + d)$ entries with ± 1 values chosen deterministically in a way intended to approximately maximize 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 $(\widetilde{A}/A)$ of A in $\widetilde{A}$ (see §3).

---

[1] For earlier contributions by Desplanques, Lévy, Muir, Sylvester and Thomson (Lord Kelvin), see [43, 54] and [42, pg. 384].

In the case $d = 1$, this method is essentially the same as the known method involving the excess of the Hadamard matrix, and leads to the same bounds that can be obtained by bounding the excess in a probabilistic manner, as in [6, 12, 30]. In this sense our method is a generalisation of methods based on excess.

The structure of the paper is as follows:

Most of these section headings are self-explanatory. §5 describes the probabilistic construction which is common to all our lower bound results. §6 summarises some known results on gaps between Hadamard orders. These results are relevant for bounding d as a function of n.

The main lower-bound results for $\mathcal{R}(n)$, which we now outline, are given in §8.

Theorem 1 obtains a lower bound on the expected value of the determinant in a direct manner, by simply expanding the determinant of the Schur complement as a sum of products. The difficulty with this approach is that we have to consider $d!$ terms. The "diagonal" term is expected to be larger than the other terms, but in general only by a factor of order h, so to obtain good bounds we need h of order at least $d!$. Thus, this approach is only useful for small d. Of course, the Hadamard conjecture implies that $d \leq 3$. However, what can currently be *proved* about gaps between Hadamard orders is much weaker than this (see §6).

For $d \leq 3$, Theorem 1 shows that $\mathcal{R}(n) \geq (\pi e/2)^{-d/2} > 1/9$, coming close to Rokicki *et al*'s conjectured lower bound of $1/2$ (see [48]), and improving on earlier results [8, 16, 17, 39, 40] that failed to obtain a constant lower bound on $\mathcal{R}(n)$ for $d \in \{2, 3\}$.

Theorems 2–5 give slightly weaker bounds than Theorem 1, but under less restrictive conditions on d and h. For example, Theorem 2 gives a nontrivial lower bound whenever $h > \pi d^4/2$. By the results of Livinskyi [41] described in §6, this condition holds for all sufficiently large n. Theorems 3–5

further weaken the conditions on d and h. For example, Theorem 4 is always applicable if $h \geq 664$ and $d \geq 2$ (see Remark 11). For $n < 668$ the Hadamard conjecture holds [37], so $d \leq 3$ and Theorem 1 applies. Thus, at least one of Theorem 1 or Theorem 4 always gives a nontrivial lower bound on $\mathcal{R}(n)$; this lower bound is of order $(\pi e/2)^{-d/2}$.

To prove Theorems 2–5 we need lower bounds on the determinant of a diagonally dominant matrix. Such bounds are provided by Lemmas 14–15 in §7.2. The proofs of Theorems 2–5 also require an upper bound on the variance of the diagonal elements occurring in our probabilistic construction. This is provided by Lemma 11, which gives an exact formula for the variance.

Other ingredients in the proofs of Theorems 2–5 are the "Lovász Local Lemma" of Erdős and Lovász [28] (for the proofs of Theorems 3–4), and the well-known inequalities of Hoeffding [33] (for Theorems 4–5), Chebyshev [15] (for Theorems 2–3) and Cantelli [14] (for Theorems 4–5).

Finally, Theorem 6 gives the result that $\mathcal{R}(n) \geq (\pi e/2)^{-d/2}$ for all $d \geq 0$ and $n \geq n_0$, where n_0 is independent of d. This follows from (a corollary of) Theorem 5 by using known results on gaps between Hadamard orders. We conjecture that the condition $n \geq n_0$ is unnecessary, and that the inequality holds for all positive n. The conjecture could be proved/disproved by a finite (albeit large) computation, since we have an explicit upper bound on n_0.

Theorems 2–4 are not quite strong enough to imply Theorem 6. This is because Theorems 2–4 all involve a multiplicative "correction factor" of the form $(1 - O_d(1/h^{1/2}))$ in the lower bound – for example, the bounds (22)–(23) involve a correction factor $(1 - O(d^2/h^{1/2}))$. Theorem 5 improves the "correction factor" to $(1 - O(d^{5/3}/h^{2/3}))$, which is close enough to unity to imply Theorem 6 (the critical point being that the exponent of h is now greater than $1/2$). The price that we pay for this improvement is that Theorem 5 involves a parameter (λ) which must be chosen in a (close to) optimal way to give a correction factor of the desired form, whereas Theorems 2–4 are explicit and do not involve any free parameters.

The constant $\pi e/2$ occurring in the bound $(\pi e/2)^{-d/2}$ of Theorem 6 is unlikely to be optimal. From the upper bounds of Barba [4], Ehlich [26, 27] and Wojtas [58] for $d \leq 3$, it seems plausible that the optimal constant is $e/2$ and that the factor π in our results is a consequence of using the probabilistic method, which in some sense estimates the mean rather than the maximum of a certain set of determinants.

It is an open question whether our probabilistic construction can be derandomized to give deterministic polynomial-time algorithms to construct matrices satisfying the lower bounds given in §8. However, in practice we have been able to construct such matrices using randomized algorithms based

on the probabilistic construction. The main practical difficulty is in constructing a Hadamard matrix of maximal order $h \leq n$, since numerous constructions for Hadamard matrices are scattered throughout the literature.

In the special case $d = 1$ our arguments simplify, because there is no need to consider a nontrivial Schur complement or to deal with the contribution of the off-diagonal elements. This case was already considered by Brown and Spencer [12], Erdős and Spencer [29, Ch. 15], and (independently) by Best [6]; see also [1, §2.5] and [2, Problem A4]. The consequence for lower bounds on $\mathcal{R}(n)$ when $n \equiv 1 \bmod 4$ was exploited by Farmakis and Kounias [30], and an improvement using 3-normalized Hadamard matrices was considered by Orrick and Solomon [44]. However, 3-normalization does not seem to be helpful in the context of our probabilistic construction.

Some of the results of this paper first appeared in the (unpublished) manuscript [10]. However, at that time we did not have a proof of equation (7) in Lemma 11 below (which gives the variance of the diagonal terms in our probabilistic construction), so we had to avoid using the variance and instead use Lemma 15.2 of [29] (Lemma 12 of [10]), which generally gives weaker results with more complicated proofs.

2 Notation

We use the usual "O" and "o" notations. $f \ll g$ means the same as $f = O(g)$, and $f \gg g$ means the same as $g \ll f$. The notations $f \asymp g$ or $f = \Theta(g)$ mean that both $f \ll g$ and $f \gg g$. Finally, $f = O_\delta(g)$ means that $f = O(g)$ when a parameter δ is fixed, but the implicit constant may depend on δ.

The binomial coefficient $\binom{m}{k}$ is defined to be zero if $k < 0$ or $k > m$. Thus, we can often avoid specifying upper and lower limits of sums explicitly.

As in §1, $D(n)$ is the maximum determinant function and $\mathcal{R}(n) := D(n)/n^{n/2}$ is its normalization. The set of orders of all Hadamard matrices is denoted by $\mathcal{H}$. If n is given, then $h \in \mathcal{H}$ is always chosen to be maximal

subject to $h \leq n$, so $d := n - h$ is minimal. The case $d = 0$ is trivial because then the Hadamard bound applies, so we assume $d > 0$ if this makes the statement of the results simpler. We assume $n \geq h \geq 4$ to avoid small special cases – it is easy to check if the results also hold for $1 \leq n \leq 3$ and $h \in \{1, 2\}$. In the asymptotic results, we can assume that $d \ll h$. In fact, it follows from (17) below that $d \ll h^{1/6}$.

Constants are denoted by c, c_1, c_2, α, β, etc. Unless otherwise specified, ε is an arbitrarily small positive constant, and $c = \sqrt{2/\pi} \approx 0.7979$.

Matrices are denoted by capital letters A etc, and their elements by the corresponding lower-case letters, e.g. $a_{i,j}$ or simply a_{ij} if the meaning is clear.

The probability of an event S is denoted by $\mathbb{P}[S]$, the expectation of a random variable X is denoted by $\mathbb{E}[X]$, and the variance of X by $\mathbb{V}[X]$.

$\mu(h)$ and $\sigma(h)^2$ are respectively the mean and variance of the "diagonal" elements occurring in our probabilistic construction – for precise definitions see §5.3. We write simply μ and σ^2 if h is clear from the context.

3 The Schur complement lemma

Let

$$\widetilde{A} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \tag{1}$$

be an $n \times n$ matrix written in block form, where A is $h \times h$, and $n = h + d > h$. The *Schur complement* $(\widetilde{A}/A)$ of A in $\widetilde{A}$ is the $d \times d$ matrix $D - CA^{-1}B$ (see for example [20, 32]). It is relevant to our problem in view of the following well-known lemma [13, 49].

Lemma 1 (Schur complement). *If $\widetilde{A}$ is as in (1) and A is nonsingular, then*

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

Proof. Take determinants of each side in the identity

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} I & 0 \\ CA^{-1} & I \end{bmatrix} \begin{bmatrix} A & B \\ 0 & D - CA^{-1}B \end{bmatrix}.$$

$\square$

In our application of Lemma 1, A is a Hadamard matrix of order h, so $\det(A) = h^{h/2}$ (without loss of generality we can assume that the sign is positive). Thus, to maximize $\det(\widetilde{A})$ for given A, we need to maximize $\det(D - CA^{-1}B)$. We can not generally find the exact maximum, but we can find lower bounds on the maximum by using the probabilistic method. For example, the mean is always a lower bound on the maximum.

4 Some binomial sums

Lemma 2 is a binomial sum which has appeared several times in the literature, e.g. Alon and Spencer [1, §2.5], Best [6, proof of Theorem 3], Brown and Spencer [12], Erdős and Spencer [29, proof of Theorem 15.2]. It was also a problem in the 1974 Putnam competition [2, Problem A4]. Lemma 2 can be used to calculate the mean of the diagonal terms that arise when the probabilistic method is used to give lower bounds for the Hadamard maximal determinant problem, as in [10] and our Lemma 11.

Lemma 3 gives a closed-form expression for a double sum which is analogous to the single sum of Lemma 2. Lemma 3 can be used to calculate the second moments of the diagonal terms that arise when inequalities such as Chebyshev's inequality are used to give lower bounds for the maximal determinant problem. In [10, Theorems 2–3] we gave lower bounds without using the second moment, but these results can be improved (and the proofs simplified) by using estimates of the second moment.

For proofs of Lemmas 2–3 see [9]. Generalisations are given in [7].

Lemma 2 (Best *et al*)**.** *For all $k \geq 0$,*

$$\sum_p \binom{2k}{k+p} |p| = k \binom{2k}{k}.$$

Lemma 3 (Brent and Osborn)**.** *For all $k \geq 0$,*

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

5 The probabilistic construction

We now describe the probabilistic construction that is common to the proofs of Theorems 1–5, and prove some properties of the construction. 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 matrix $\widetilde{A}$ of order n. The border is defined by matrices B, C and D as in §3. The matrices A, B, and C have entries in $\{\pm 1\}$. We allow the matrix D to have entries in $\{0, \pm 1\}$, but the zero entries can be replaced by $+1$ 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. To prove this, we observe

that, by Lemma 1, $\det(\widetilde{A}) = \det(A)\det(D - CA^{-1}B)$ is a linear function of each element d_{ij} of D (considered separately), so we can choose any ordering of off-diagonal elements, then successively change each off-diagonal element d_{ij} of D from 0 to $+1$ or -1 in such a way that $|\det(\widetilde{A})|$ does not decrease.

In the proofs of Theorems 1–5 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. In the proof of Theorem 1 it is sufficient to consider $\mathbb{E}[\det(D - CA^{-1}B)]$; in the proofs of Theorems 2–5 the argument is slightly more sophisticated and uses Chebyshev's inequality or Cantelli's inequality.

5.1 Details of the 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

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

where

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

The definition of $\mathrm{sgn}(0)$ here is arbitrary and does not affect the results. To complete the construction, we choose $D = -I$. As mentioned above, it is inconsequential that D is not a $\{\pm 1\}$-matrix.

5.2 Properties of the construction

Define $F = CA^{-1}B$ and $G = -(\widetilde{A}/A) = F - D = F + I$. (The minus sign in the definition of G is chosen for convenience in what follows.) 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. This intuition is justified by Lemma 12.

The following lemma is (in the case $i = j$) due to M. R. Best [6] and independently J. H. Lindsey (see [29, footnote on pg. 88]). The upper bound can be achieved infinitely often, in fact whenever a regular Hadamard matrix of order h exists. For example, this is true if $h = 4q^2$, where q is an odd prime power and $q \not\equiv 7 \pmod 8$, see [59].

Lemma 4. *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 [6]. □

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

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

Proof. The case $i = j$ follows from Best [6, Theorem 3]. The case $i \neq j$ is easy, since B is chosen randomly. □

Lemma 6. *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 $\text{diag}(UU^T) = I$. □

Lemma 7. *If $F = (f_{ij})$ is chosen as above, then*

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

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

$$f_{1j} = \sum_k u_{1k} b_{kj}, \tag{3}$$

where

$$u_{1k} = \frac{1}{h} \sum_{\ell} c_{1\ell} a_{k\ell}$$

and

$$c_{1\ell} = \text{sgn}\left(\sum_m b_{m1} a_{m\ell}\right).$$

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

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

9

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, (2) follows from Lemma 6. $\qquad \square$

Lemma 8. *Let $F = CA^{-1}B$ be chosen as above. Then f_{ij} and $f_{k\ell}$ are independent if and only if $\{i, j\} \cap \{k, \ell\} = \emptyset$.*

Proof. This follows from the fact that f_{ij} depends on columns i and j (and no other columns) of B. $\qquad \square$

Suppose that $i \neq j$, $k \neq \ell$. We cannot assume that f_{ij} and $f_{k\ell}$ are independent. For example, by Lemma 8, f_{12} and f_{21} are not independent. The following lemma bounds $\mathbb{E}[f_{ij}f_{k\ell}]$ without assuming independence.

Lemma 9. *Suppose that $i \neq j$, $k \neq \ell$. Then*

$$|\mathbb{E}[f_{ij}f_{k\ell}]| \leq \mathbb{E}[|f_{ij}f_{k\ell}|] \leq 1. \tag{4}$$

Proof. The first inequality in (4) is immediate. The second inequality follows from the Cauchy-Schwarz inequality and Lemma 7, using

$$\mathbb{E}[|f_{ij}f_{k\ell}|] \leq \sqrt{\mathbb{E}[f_{ij}^2]\mathbb{E}[f_{k\ell}^2]} = 1.$$

$\qquad \square$

Lemma 10. *Let $G = F + I$ be chosen as above. Then*

$$\mathbb{E}\left[\prod_{i=1}^{d} g_{ii}\right] = \left[1 + 2^{-h}h\binom{h}{h/2}\right]^d.$$

Proof. By Lemma 8, the diagonal terms f_{ii} are independent; hence the diagonal terms $g_{ii} = f_{ii} + 1$ are independent. Now $\mathbb{E}[g_{ii}] = \mathbb{E}[f_{ii}] + 1$, so from Lemma 5 we have

$$\mathbb{E}\left[\prod_{i=1}^{d} g_{ii}\right] = \prod_{i=1}^{d}\mathbb{E}[g_{ii}] = \left[1 + 2^{-h}h\binom{h}{h/2}\right]^d.$$

$\qquad \square$

5.3 Mean and variance of elements of G

Using Lemma 3, we can complete the computation of the mean and variance of the elements of the matrix G.

Lemma 11. *Let A be a Hadamard matrix of order $h \geq 4$ and B, C be $\{\pm 1\}$-matrices chosen as above. Let $G = CA^{-1}B + I$. Then*

$$
\mathbb{E}[g_{ii}] = 1 + \frac{h}{2^h} \binom{h}{h/2}, \tag{5}
$$

$$
\mathbb{E}[g_{ij}] = 0 \text{ for } 1 \leq i, j \leq d, \ i \neq j, \tag{6}
$$

$$
\mathbb{V}[g_{ii}] = 1 + \frac{h(h-1)}{2^{h+1}} \binom{h/2}{h/4}^2 - \frac{h^2}{2^{2h}} \binom{h}{h/2}^2, \tag{7}
$$

$$
\mathbb{V}[g_{ij}] = 1 \text{ for } 1 \leq i, j \leq d, \ i \neq j. \tag{8}
$$

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

Now $hF = CA^T B$ (since A is a Hadamard matrix). 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

$$
S_1 = \sum_{j=1}^{4k} X_j
$$

and

$$
S_2 = \sum_{j=1}^{2k} X_j - \sum_{j=2k+1}^{4k} X_j.
$$

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}

11

possible (equally likely) choices and using Lemma 3, we see that

$$
\begin{aligned}
\mathbb{E}[|S_1 S_2|] &= 4\mathbb{E}[|p^2 - q^2|] \\
&= \frac{4}{2^{4k}} \sum_p \sum_q \binom{2k}{k+p}\binom{2k}{k+q}|p^2 - q^2| \\
&= \frac{4}{2^{4k}} \cdot 2k^2 \binom{2k}{k}^2 \\
&= \frac{h^2}{2^{h+1}} \binom{2k}{k}^2 .
\end{aligned}
$$

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 $Y_j Y_\ell$ (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 $\mathbb{V}[g_{ii}]$ now follows from

$$
\mathbb{V}[g_{ii}] = \mathbb{V}[f_{ii}] = \mathbb{E}[f_{ii}^2] - \mathbb{E}[f_{ii}]^2 .
$$

$\square$

For convenience we write $\mu = \mu(h) := \mathbb{E}[g_{ii}]$ and $\sigma^2 = \sigma(h)^2 := \mathbb{V}[g_{ii}]$. If h is understood from the context we may write simply μ and σ^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 monotonic increasing and of order $h^{1/2}$, but $\sigma(h)$ is bounded and monotonic decreasing.

Lemma 12. *For $h \in 4\mathbb{Z}$, $h \geq 4$, $\mu(h)$ is monotonic increasing, and $\sigma(h)^2$ is monotonic decreasing. Moreover, the following inequalities hold:*

$$\sqrt{\frac{2h}{\pi}} + 0.9 < \mu(h) < \sqrt{\frac{2h}{\pi}} + 1, \tag{9}$$

and

$$\mu(h) = 1 + \sqrt{\frac{2h}{\pi}}\left(1 - \frac{1}{4h} + \frac{\alpha(h)}{h^2}\right), \tag{10}$$

where

$$0 \leq \alpha(h) \leq (4\sqrt{\pi} - 7)/2 < 0.04491. \tag{11}$$

Also,

$$0.04507 \approx 1 - 3/\pi = \lim_{h\to\infty} \sigma(h)^2 < \sigma(h)^2 \leq \sigma(4)^2 = 0.25, \tag{12}$$

and

$$\sigma(h)^2 = \left(1 - \frac{3}{\pi}\right) + \frac{11}{4\pi h} - \frac{\beta(h)}{h^2}, \tag{13}$$

where

$$0 \leq \beta(h) \leq 12 - 37/\pi < 0.23. \tag{14}$$

Proof. From the well-known asymptotic expansion of $\ln\Gamma(z)$ we obtain, as in [35], an asymptotic expansion for the logarithm of the central binomial coefficient:

$$\ln\binom{2m}{m} \sim m\ln 4 - \frac{\ln(\pi m)}{2} - \sum_{k\geq 1} \frac{B_{2k}(1 - 4^{-k})}{k(2k-1)} m^{1-2k}. \tag{15}$$

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 and the asymptotic expansion is strictly enveloping in the sense of Pólya and Szegö[2], so upper and lower bounds may be found by truncating the series after an even or an odd number of terms.

The inequalities (9)–(14) now follow from a straightforward but tedious computation, using the expressions for $\mu(h)$ and $\sigma(h)^2$ in Lemma 11 and approximations obtained from (15) with $m = h/2$ and $m = h/4$. Note that the leading terms (of order h) cancel in the computation of $\sigma(h)^2$.

---

[2]See, for example, Corollaries 2–3 of arXiv:1608.04834v2.

The monotonicity of $\mu(h)$ and $\sigma(h)^2$ follows from the inequalities (10)–(11) and (13)–(14) respectively. For example, from (13), using the bounds on $\beta(h)$ in (14), we have

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

$\square$

Remark 1. Because $\mu(h)$ is of order $h^{1/2}$ but $\sigma(h)^2$ is of order 1, the distribution of g_{ii} is concentrated around the mean, and we expect values smaller than $(1-\varepsilon)\mu(h)$ to occur with low probability. For fixed positive ε, the probability should tend to zero as $h \to \infty$. We can use Chebyshev's or Cantelli's inequality to obtain bounds on this probability.

6 Gaps between Hadamard orders

In order to apply our results to obtain a lower bound on $\mathcal{R}(n)$ for given n, we need to know the order h of a Hadamard matrix with $h \leq n$ and $n - h$ as small as possible. Thus, it is necessary to consider the size of possible gaps in the sequence $(h_i)_{i \geq 1}$ of Hadamard orders. We define the *Hadamard gap function* $\gamma : \mathbb{R} \to \mathbb{Z}$ by

$$\gamma(x) := \max\{h_{i+1} - h_i \,|\, h_i \leq x\} \cup \{0\}. \tag{16}$$

In [8, 40] it was shown, using the Paley and Sylvester constructions, that $\gamma(n)$ can be bounded using the prime-gap function. For example, if p is an odd prime, then $2(p+1)$ is a Hadamard order. However, only rather weak bounds on the prime-gap function are known. A different approach which produces asymptotically-stronger bounds employs results of Seberry [56], as subsequently sharpened by Craigen [21] and Livinskyi [41]. These results take the following form: for any odd positive integer q, a Hadamard matrix of order $2^t q$ exists for every integer

$$t \geq \alpha \log_2(q) + \beta,$$

where α and β are constants. Seberry [56] obtained $\alpha = 2$. Craigen [21] improved this to $\alpha = 2/3$, $\beta = 16/3$, and later obtained $\alpha = 3/8$ in unpublished work with Tiessen quoted in [34, Thm. 2.27] and [22, 23].[3] Livinskyi [41]

---

[3]There are typographical errors in [34, Thm. 2.27] and in [23, Thm. 1.43], where the floor function should be replaced by the ceiling function. This has the effect of increasing the additive constant β.

found $\alpha = 1/5$, $\beta = 64/5$. The results of Craigen and of Livinskyi depend on the construction of Hadamard matrices via signed groups, Golay numbers and Turyn-type sequences [5, 36, 50, 55].

The connection between these results and the Hadamard gap function is given by Lemma 13. From the lemma and the results of Livinskyi, the Hadamard gap function satisfies

$$\gamma(n) = O(n^{1/6}). \tag{17}$$

This is much sharper than $\gamma(n) = O(n^{21/40})$ arising from the best current result for prime gaps (by Baker, Harman and Pintz [3]), although not as sharp as the result $\gamma(n) = O(\log^2 n)$ that would follow from Cramér's prime-gap conjecture [8, 24, 51, 53].

Lemma 13. *Suppose there exist positive constants α, β such that $2^t q \in \mathcal{H}$ for all odd positive integers q and all integers $t \geq \alpha \log_2(q) + \beta$. Then the Hadamard gap function $\gamma(n)$ satisfies*

$$\gamma(n) = O_\beta(n^{\alpha/(1+\alpha)}).$$

Proof. Consider consecutive odd integers q_0, $q_1 = q_0 + 2$ and corresponding $h_i = 2^t q_i$, where $t = \lceil \alpha \log_2(q_1) + \beta \rceil$. By assumption there exist Hadamard matrices of orders h_0, h_1. Also, $2^\beta q_1^\alpha \leq 2^t < 2^{\beta+1} q_1^\alpha$. Thus

$$h_1 = 2^t q_1 \geq 2^\beta q_1^{1+\alpha}$$

and

$$h_1 - h_0 = 2^{t+1} < 2^{\beta+2} q_1^\alpha \leq 2^{\beta+2}(h_1/2^\beta)^{\alpha/(1+\alpha)} \leq 4 \cdot 2^{\beta/(1+\alpha)} h_1^{\alpha/(1+\alpha)}.$$

Now $2^t \leq h_0$, so $h_1 = h_0 + 2^{t+1} \leq 3h_0$. Also, $\frac{\alpha}{1+\alpha} < 1$ and $\frac{1}{1+\alpha} < 1$. Thus

$$h_1 - h_0 < 12 \cdot 2^\beta h_0^{\alpha/(1+\alpha)} = O_\beta(h_0^{\alpha/(1+\alpha)}).$$

$\square$

7 Preliminary results

We now state some well-known results (Propositions 1–4) and prove some lemmas that are needed in §8.

7.1 Probability inequalities

Proposition 1 is the well-known inequality of Chebyshev [15], and Proposition 2 is a one-sided analogue due to Cantelli [14].

Proposition 1 (Chebyshev). *Let X be a random variable with finite mean $\mu = \mathbb{E}[X]$ and finite variance $\sigma^2 = \mathbb{V}[X]$. Then, for all $\lambda > 0$,*

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

Proposition 2 (Cantelli). *Let X be a random variable with finite mean $\mu = \mathbb{E}[X]$ and finite variance $\sigma^2 = \mathbb{V}[X]$. Then, for all $\lambda > 0$,*

$$\mathbb{P}[X - \mu \geq \lambda] \leq \frac{\sigma^2}{\sigma^2 + \lambda^2} \quad and \quad \mathbb{P}[X - \mu \leq -\lambda] \leq \frac{\sigma^2}{\sigma^2 + \lambda^2}\,.$$

Proposition 3 is a two-sided version of Hoeffding's tail inequality. A one-sided version is proved in [33, Theorem 2]. Hoeffding's inequality gives a sharper bound than Chebyshev's inequality in the case that the random variable X is a sum of independent, bounded random variables X_i.

Proposition 3 (Hoeffding). *Let $X_1, \ldots, X_h$ be independent random variables with sum $X = X_1 + \cdots + X_h$. Assume that $X_i \in [a_i, b_i]$ and, for some $i \leq h$, $a_i < b_i$. Then, for all $\lambda > 0$,*

$$\mathbb{P}[\,|X - E[X]| \geq \lambda\,] \ \leq\ 2 \exp\left(\frac{-2\lambda^2}{\sum_{i=1}^{h}(b_i - a_i)^2}\right)\,.$$

We also need the "symmetric" case of the Lovász Local Lemma [28], where "symmetric" means that the upper bound on the probability of each event is the same. We state the formulation given in [1, Corollary 5.1.2], with a slight change of notation.

Proposition 4 (Lovász Local Lemma, symmetric case). *Let $E_1, E_2, \ldots E_m$ be events in an arbitrary probability space. Suppose that each event E_i is mutually independent of all the other events E_j except for at most D of them, and that $\mathbb{P}[E_i] \leq p$ for $1 \leq i \leq m$. If*

$$ep(D + 1) \leq 1, \tag{18}$$

then

$$\mathbb{P}\left[\bigwedge_{i=1}^{m} \overline{E_i}\right] > 0$$

(in other words, with positive probability none of the events E_i holds).

16

Remark 2. It follows from a theorem of Shearer [52] that the inequality (18) can be replaced by $epD \leq 1$. This improvement would make little difference to our results, so we use the better-known condition (18).

7.2 Perturbation bounds

We state some lower bounds on the determinant of a matrix which is close to the identity matrix. Lemma 14 generalises and sharpens some inequalities due to Ostrowski [45, 46] and von Koch [38]. Note that the condition on e_{ii} in Lemma 14 is one-sided. This is useful if we want to apply Cantelli's inequality, as in the proofs of Theorems 4–5 below.

Lemma 14. *If $M = I - E \in \mathbb{R}^{d \times d}$, where $|e_{ij}| \leq \varepsilon$ for $i \neq j$ and $e_{ii} \leq \delta$ for $1 \leq i \leq d$, where $\delta \geq 0$ and $\delta + (d-1)\varepsilon \leq 1$, then*

$$\det(M) \geq (1 - \delta - (d-1)\varepsilon)(1 - \delta + \varepsilon)^{d-1} .$$

Proof. See [11, Corollary 1]. □

Lemma 15. *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*

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

Proof. This is implied by the case $\delta = \varepsilon$ of Lemma 14. It is also implicit in a bound due to Ostrowski [46, eqn. (5,5)]. □

7.3 An inequality involving h and n

Lemma 16 allows us to deduce inequalities involving n^n from corresponding inequalities involving h^n.

Lemma 16. *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

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

□

8   Probabilistic lower bounds

In this section we prove several lower bounds on $D(n)$ and $\mathcal{R}(n)$ where, as usual, $n = h + d$ and h is the order of a Hadamard matrix. Theorem 1 assumes that $d \leq 3$; Theorems 2–6 allow $d > 3$. Theorem 1 can be extended to allow $d > 3$, but only on the assumption that n is sufficiently large – see Theorem 1 of [10].

First we state a Lemma which is useful in its own right, and is required for the proof of Theorem 1.

Lemma 17. *If $n = h + d$ where $4 \leq h \in \mathcal{H}$ and $1 \leq d \leq 3$, then*

$$D(n) \geq h^{h/2}(\mu^d - \eta),$$

where $\mu = \mu(h)$ is as in §5.3, and

$$\eta = \eta(h, d) = \begin{cases} 0 & \text{if } d = 1, \\ 1 & \text{if } d = 2, \\ 5h^{1/2} + 3 & \text{if } d = 3. \end{cases}$$

Proof. We use the probabilistic construction and notation of §5. Let A be a Hadamard matrix of order h. Define matrices B, C, D, F and G as in §5.

For notational convenience we give the proof for the case $d = 3$. The cases $d \in \{1, 2\}$ are similar (but easier).

Since $G = F + I$, we have $g_{ii} = f_{ii} + 1$ and

$$G = \begin{bmatrix} g_{11} & f_{12} & f_{13} \\ f_{21} & g_{22} & f_{23} \\ f_{31} & f_{32} & g_{33} \end{bmatrix}.$$

Expanding $\deg(G)$ we obtain $d! = 6$ terms. The "diagonal" term is $g_{11}g_{22}g_{33}$. There are 3 terms involving one diagonal element, for example $-f_{12}f_{21}g_{33}$, and 2 terms involving no diagonal elements, for example $f_{12}f_{23}f_{31}$. Define the *type* of a term to be the number of diagonal elements that it contains. Thus the diagonal term has type 3 (or type d in general). Let T_k be an upper bound on the magnitude of the expectation of a term of type k. Then

$$E[\det(G)] \geq E[g_{11}g_{22}g_{33}] - 3T_1 - 2T_0. \tag{19}$$

Now, by Lemmas 4 and 9,

$$|E[f_{12}f_{23}f_{31}]| \leq E[|f_{12}f_{23}|] \cdot \max |f_{31}| \leq 1 \cdot h^{1/2} = h^{1/2},$$

so we can take $T_0 = h^{1/2}$. Similarly,

$$|E[f_{12}f_{21}g_{33}]| \le E[|f_{12}f_{23}|] \cdot \max |g_{31}| \le h^{1/2} + 1,$$

so we can take $T_1 = h^{1/2} + 1$. Also, from Lemma 10 and the definition of $\mu(h)$, we have

$$E[g_{11}g_{22}g_{33}] = \mu^3.$$

Thus, from (19), we obtain

$$E[\det(G)] \ge \mu^3 - 3(h^{1/2} + 1) - 2h^{1/2} = \mu^3 - 5h^{1/2} - 3.$$

We have shown that, with $\eta = \eta(h, d)$ as in the statement of the Lemma,

$$E[\det(G)] \ge \mu^d - \eta \tag{20}$$

holds for $d = 3$. The proofs for $1 \le d \le 2$ are similar but simpler.

From (20), there exists some assignment of signs to the elements of B such that, for the resulting matrix G, we have

$$\det(G) \ge \mu^d - \eta. \tag{21}$$

Hence, by the Schur complement lemma (Lemma 1),

$$D(n) \ge h^{h/2} \det(G) \ge h^{h/2}(\mu^d - \eta).$$

$\square$

Remark 3. The restriction $d \le 3$ in Lemma 17 is not necessary. In the general case, a similar argument, given in [10, pg. 13], shows that

$$D(n) \ge h^{h/2}(\mu(h)^d - \eta(h, d)),$$

where

$$\eta(h, d) \le (d! - 1)(h^{1/2} + 1)^{d-2} \quad \text{for} \quad d \ge 2.$$

It follows from Lemma 12 that $\eta(h, d)/\mu(h)^d = O(d!(\pi/2)^{d/2}/h)$. Because of the factor $d!(\pi/2)^{d/2}$ in this bound, the general result is useless unless d is small, say $d \le 3$ or $d \le 4$. Theorems 2–5 overcome this difficulty by using Lemma 14 or Lemma 15, avoiding the expansion of $\det(G)$ as a sum of $d!$ terms.

We now deduce Theorem 1 from Lemma 17. For $d > 3$ a similar result holds, but we can only prove it for n sufficiently large – see Theorem 6 and also the weaker result of [10, Corollary 2].

Theorem 1. *If $0 \leq d \leq 3$, $h \in \mathcal{H}$, $h \geq 4$, and $n = h + d$, then*

$$\mathcal{R}(n) \geq \left(\frac{2}{\pi e}\right)^{d/2}.$$

Moreover, the inequality is strict if $d > 0$.

Proof. Define $c := \sqrt{2/\pi}$ and $K := 0.9/c$. The result is trivial if $d = 0$, so assume that $1 \leq d \leq 3$. Since d is bounded, we can ignore functions of d multiplying the "O" terms. Lemma 17 gives

$$D(n) \geq h^{h/2}(\mu^d - \eta),$$

and from Lemma 12 we have $\mu \geq ch^{1/2} + 0.9$, so $\mu^d \geq c^d h^{d/2}(1 + dKh^{-1/2})$. Thus

$$D(n) \geq c^d h^{n/2}\left(1 + dKh^{-1/2} - \frac{\eta}{c^d h^{d/2}}\right).$$

From Lemma 16, $(h/n)^n \geq \exp(-d - d^2/h)$, so

$$\mathcal{R}(n) = \frac{D(n)}{n^{n/2}} \geq c^d e^{-d/2}\left(1 + dKh^{-1/2} - \frac{\eta}{c^d h^{d/2}}\right)e^{-d^2/(2h)}.$$

Since $c^d e^{-d/2} = (2/(\pi e))^{d/2}$, K is positive, and $\eta/h^{d/2} = O(h^{-1})$, the term $dKh^{-1/2}$ dominates the $O(h^{-1})$ terms, and the result follows for all sufficiently large h. In fact, some computation shows that this argument is sufficient for $d \in \{1, 2\}$ and all $h \geq 4$. For $d = 3$ we obtain

$$\mathcal{R}(n) \geq \left(\frac{2}{\pi e}\right)^{3/2}\left(1 + \frac{3K}{h^{1/2}} - \frac{5h^{1/2} + 3}{c^3 h^{3/2}}\right)e^{-4.5/h}.$$

This shows that $\mathcal{R}(n) \geq (2/(\pi e))^{3/2}$ for $h \geq 28$. Thus, we only have to consider the cases $n \in \{7, 11, 15, 19, 23, 27\}$. Now for $n = 4k - 1$, where $4k \in \mathcal{H}$, an easy argument of Sharpe [57] involving minors of a Hadamard matrix of order $4k$, as in [39, Theorem 2], shows that

$$D(4k - 1) \geq \frac{D(4k)}{4k} = (4k)^{2k-1},$$

so

$$\mathcal{R}(4k - 1) \geq (4k)^{2k-1}/(4k - 1)^{(4k-1)/2}.$$

This is sufficient to show that $\mathcal{R}(n) > (2/(\pi e))^{3/2}$ for $n = 4k - 1 \leq 27$. $\square$

Corollary 1. *The Hadamard conjecture implies that $\mathcal{R}(n)$ is bounded below by a positive constant.*

Proof. If the Hadamard conjecture is true, then for $4 < n \not\equiv 0 \pmod 4$, we can take $h = 4\lfloor n/4 \rfloor$ and $d = n - h \leq 3$ in Theorem 1. This gives

$$1 > \mathcal{R}(n) > \left(\frac{2}{\pi e}\right)^{d/2} \geq \left(\frac{2}{\pi e}\right)^{3/2} > 0.1133 \,.$$

$\square$

Remark 4. It is interesting to compare our Theorem 1 (or the slightly sharper Lemma 17) with Theorem 2 of Koukouvinos, Mitrouli and Seberry [39], assuming the existence of the relevant Hadamard matrices. In the case $n \equiv 2 \bmod 4$, the bound given by our Theorem 1 (respectively Lemma 17) is better for $n \geq 22$ (resp. 14) than the bound $2(n+2)^{(n-2)/2}/n^{n/2} \sim 2e/n$ implied by [39, Theorem 2]. In the case $n \equiv 3 \bmod 4$, the bound given by our Theorem 1 (resp. Lemma 17) is better for $n \geq 211$ (resp. 135) than the bound $(n+1)^{(n-1)/2}/n^{n/2} \sim (e/n)^{1/2}$ implied by [39, Theorem 2].

We now prove several theorems which apply for arbitrarily large d. The proofs depend on the fact that $\sigma(h)$ is bounded (see Lemma 11). This enables us to use Chebyshev's inequality (or Cantelli's inequality).

Theorems 2–5 give lower bounds on $\det(G)/\mu^d$; these are easily translated into lower bounds on $D(n)$, since $D(n) \geq h^{h/2} \det(G)$ (by the Schur complement lemma), and $\mu > \sqrt{2h/\pi} + 0.9$ (by Lemma 12). Each of the Theorems 2–5 is followed by a corollary which gives a corresponding lower bound on $\mathcal{R}(n)$.

Theorem 2. *Suppose $d \geq 1$, $4 \leq h \in \mathcal{H}$, $n = h + d$, G as in §5.2. Then, with positive probability*

$$\frac{\det G}{\mu^d} \geq 1 - \frac{d^2}{\mu} \,. \tag{22}$$

Proof. Let λ be a positive parameter to be chosen later, and $\mu = \mu(h)$. For the purposes of this proof, we say that G is *good* if the conditions of Lemma 15 apply with $M = \mu^{-1}G$ and $\varepsilon = \lambda/\mu$. Otherwise G is *bad*.

Assume $1 \leq i, j \leq d$. From Lemma 11, $V[g_{ij}] = 1$ for $i \neq j$; from Lemma 12, $V[g_{ii}] = \sigma(h)^2 \leq 1/4$. It follows from Chebyshev's inequality (Proposition 1) 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,
$$\mathbb{P}[G \text{ is bad}] \leq \frac{d(d-1)}{\lambda^2} + \frac{d\sigma^2}{\lambda^2} = \frac{d(d+\sigma^2-1)}{\lambda^2} < \frac{d^2}{\lambda^2} \,.$$

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 15 to $\mu^{-1}G$, obtaining $\det(\mu^{-1}G) \geq 1 - d\varepsilon = 1 - d\lambda/\mu = 1 - d^2/\mu$. $\qquad\square$

Remark 5. With the optimal choice $\lambda = \sqrt{d(d+\sigma^2-1)}$ we obtain the less elegant but slightly sharper result that, with positive probability,
$$\frac{\det(G)}{\mu^d} \geq 1 - \frac{\sqrt{d^3(d+\sigma^2-1)}}{\mu} \,.$$

Corollary 2. *Under the conditions of Theorem 2,*
$$\mathcal{R}(n) \geq \left(\frac{2}{\pi e}\right)^{d/2} \left(1 - d^2\sqrt{\frac{\pi}{2h}}\right) \,. \tag{23}$$

Proof. 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 (23) is positive. From Lemma 12, $ch^{1/2} < \mu$, so $d^2 < \mu$.

From Theorem 2 and the Schur complement Lemma,
$$\mathcal{R}(n) \geq \frac{h^{h/2}\mu^d}{n^{n/2}} \left(1 - \frac{d^2}{\mu}\right) \,.$$

Using $ch^{1/2} < \mu$, this gives
$$\mathcal{R}(n) \geq c^d(h/n)^{n/2}(1 - d^2/\mu).$$

By Lemma 16, $(h/n)^n > \exp(-d - d^2/h)$, so
$$\mathcal{R}(n) \geq c^d e^{-d/2} f = \left(\frac{2}{\pi e}\right)^{d/2} f, \tag{24}$$

where
$$f = \exp\left(-\frac{d^2}{2h}\right)\left(1 - \frac{d^2}{\mu}\right). \tag{25}$$

Thus, to prove (23), it suffices to prove that
$$f \geq 1 - \frac{d^2}{ch^{1/2}} \,.$$

Since
$$\exp\left(-\frac{d^2}{2h}\right) \geq 1 - \frac{d^2}{2h},$$

it suffices to prove that

$$\left(1 - \frac{d^2}{2h}\right)\left(1 - \frac{d^2}{\mu}\right) \geq 1 - \frac{d^2}{ch^{1/2}}. \tag{26}$$

Expanding and simplifying shows that the inequality (26) is equivalent to

$$2h + \mu \leq d^2 + \mu\sqrt{2\pi h}. \tag{27}$$

Now, by Lemma 12, $\mu > c\sqrt{h} + 0.9$, so $\mu\sqrt{2\pi h} > 2h + 0.9\sqrt{2\pi h}$ (using $c\sqrt{2\pi} = 2$). Thus, to prove (27), it suffices to show that $\mu \leq d^2 + 0.9\sqrt{2\pi h}$. Using Lemma 12 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. $\square$

Remark 6. Corollary 2 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 [41], this condition holds for all sufficiently large n (assuming as always that we choose the maximal h for given n). From Theorem 1, the second factor in (23) can be omitted if $d \leq 3$.

We now improve on Theorem 2, if d is sufficiently large, by using the Lovász Local Lemma [28] (Proposition 4).

Theorem 3. *Suppose $d \geq 1$, $4 \leq h \in \mathcal{H}$, $n = h + d$, G as in §5.2. Then with positive probability*

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

Proof. If $d = 1$ the result is easy, since $\det G = g_{11} \geq \mathbb{E}[g_{11}] = \mu$ with positive probability. Thus, we can assume that $d \geq 2$.

Let λ be a positive parameter to be chosen later. As in Theorem 2, for the purposes of this proof we say that G is *good* if the conditions of Lemma 15 apply with $M = \mu^{-1}G$ and $\varepsilon = \lambda/\mu$. Otherwise G is *bad*.

Let E_{ij} be the event that $|g_{ij}| > \lambda$ (if $i \neq j$) or $|g_{ii} - \mu| > \lambda$ (if $i = j$). Thus G is good if none of the E_{ij} holds.

From Lemma 11 (if $i \neq j$) and Lemma 12 (if $i = j$), we have $\mathbb{V}[g_{ij}] \leq 1$ in both cases. Thus, from Chebyshev's inequality, $\mathbb{P}[E_{ij}] \leq \lambda^{-2}$.

Now, by Lemma 8, E_{ij} is independent of $E_{k\ell}$ if $\{i, j\} \cap \{k, \ell\} = \emptyset$. Thus, in Proposition 4 we can take $D = 4d - 5$, and the proposition shows that G is good with positive probability provided that $\lambda^2 \geq 4e(d - 1)$. We take the smallest positive λ satisfying this inequality, i.e. $\lambda = 2\sqrt{e(d - 1)}$. Now the result follows from the inequality

$$\frac{\det G}{\mu^d} \geq 1 - \frac{d\lambda}{\mu}, \tag{28}$$

which holds whenever G is good, by Lemma 15 applied to $M = \mu^{-1}G$. $\qquad\square$

Corollary 3. *Under the conditions of Theorem* 3,

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

Proof (sketch). This is similar to the proof of (24)–(25) above, using the bound of Theorem 3 instead of the bound of Theorem 2. $\qquad\square$

Remark 7. In Corollary 2 we absorbed the factor $e^{-d^2/(2h)}$ into the final bound. We do not attempt to do this in Corollary 3 because the exponent of d in the "main term" is $3/2$ rather than 2. However, by (17) above, $d \ll h^{1/6}$, so $(d^2/h)/(d^{3/2}/h^{1/2}) = (d/h)^{1/2} \ll h^{-5/12}$, and the factor $\exp(-d^2/(2h)) = 1 - \Theta(d^2/h)$ is much closer to 1 than the factor $1 - \Theta(d^{3/2}/h^{1/2})$ if h is large.

Remark 8. Corollary 3 gives a nontrivial lower bound if $h > 2\pi ed^2(d - 1)$. This is a weaker condition than the condition $h > \pi d^4/2$ of Corollary 2 (see Remark 6) if $d \geq 10$. For $2 \leq d \leq 9$, Corollary 2 is sharper than Corollary 3.

We can improve on Theorem 3 and Corollary 3 by treating the diagonal and off-diagonal elements of G differently. For the diagonal elements we can use Cantelli's inequality since "large" diagonal elements are harmless – only "small" diagonal elements are "bad". For the off-diagonal elements we can use Hoeffding's inequality, because each off-diagonal element can be written as a sum of independent random variables (this is not true for the diagonal elements). The Lovász Local Lemma can be applied much as in the proof of Theorem 3. To handle the different bounds on diagonal and off-diagonal elements we need Lemma 14. The parameters λ and t are chosen so that the probability of an off-diagonal element being "bad" is the same as the probability of a diagonal element being "bad" (more precisely, our upper

24

bounds on these probabilities are the same). This choice is not optimal, but simplifies the application of the Lovász Local Lemma, since we can use the symmetric case of the Lemma. For a choice of λ and t giving unequal probabilities (but not using the Lovász Local Lemma), see Theorem 5.

Theorem 4. *Suppose $d \geq 2$, $4 \leq h \in \mathcal{H}$, $n = h+d$, $\lambda = (4e(d-1)-1)^{1/2}\sigma/\mu$, $t = (2\ln(8e(d-1)))^{1/2}/\mu$, and G as in §5.2. If $\lambda + (d-1)t \leq 1$, then with positive probability we have*

$$\frac{\det G}{\mu^d} \geq (1 - \lambda - (d-1)t)(1 - \lambda + t)^{d-1}. \tag{29}$$

Proof. Define $M := \mu^{-1}G$. For the purposes of this proof we say that a diagonal element m_{ii} of M is *bad* if $m_{ii} < 1 - \lambda$ (note the one-sided constraint); otherwise m_{ii} is *good* (so a good m_{ii} can be large, but not too small). We say that an off-diagonal element m_{ij} $(i \neq j)$ is *bad* if $|m_{ij}| > t$; otherwise m_{ij} is *good*. We say that G is *good* if all the elements of M are good; otherwise G is *bad*. If G is bad, then the conditions of Lemma 14 apply to M with $(\delta, \varepsilon) = (\lambda, t)$.

Define $p := 1/(4e(d-1))$ and $\tau := \sigma/\mu$, so $\lambda = (1/p - 1)^{1/2}\tau$. By Cantelli's inequality, the probability that a diagonal element m_{ii} is bad is

$$\mathbb{P}[m_{ii} < 1 - \lambda] \leq \frac{\tau^2}{\tau^2 + \lambda^2} = p.$$

We can apply Hoeffding's inequality to the off-diagonal elements m_{ij} $(i \neq j)$ since equation (3) shows that, in the case $i = 1$ (which we consider without loss of generality), m_{1j} $(= f_{1j})$ for $1 < j \leq d$ is a sum of h independent random variables $u_{1k}b_{kj}$, where the elements b_{kj} $(1 \leq k \leq h)$ of the j-th column of B are distributed independently and randomly in $\{\pm 1\}$, and the multipliers u_{1k}, which may be regarded as constants since they are independent[4] of the j-th column of B, satisfy $\sum_{k=1}^{h} u_{1k}^2 = 1$ in view of Lemma 6. Thus m_{1j} is a sum of h independent, bounded random variables, with bounds $[-|u_{1k}|, +|u_{1k}|]$ $(1 \leq k \leq h)$. It follows that, by Hoeffding's inequality (Proposition 3), the probability that an off-diagonal element m_{ij} $(i \neq j)$ is bad is

$$\mathbb{P}[|m_{ij}| > t] \leq 2\exp(-\mu^2 t^2/2) = p.$$

From Lemma 8, each m_{ij} depends on at most $4d - 4$ of the $m_{k\ell}$, and it follows from the Lovász Local Lemma (Proposition 4 with $D = 4(d-1)-1$)

---

[4]They are not independent of the first column of B, which is why the argument does not apply to m_{11} (or f_{11}). Similarly, the argument does not apply to other diagonal elements m_{ii} (or f_{ii}).

and the definition of p that $\mathbb{P}[G \text{ is good}] > 0$. Thus, from Lemma 14, with positive probability we have

$$\det M \geq (1 - \lambda - (d-1)t)(1 - \lambda + t)^{d-1}.$$

Since $\det G = \mu^d \det M$, this completes the proof. $\qquad\square$

Remark 9. The condition $\lambda + (d-1)t \leq 1$ is equivalent to

$$\mu \geq (4e(d-1) - 1)^{1/2}\sigma + (d-1)(2\ln(8e(d-1)))^{1/2}, \qquad (30)$$

but $\mu > (2h/\pi)^{1/2}$, so the condition is satisfied if $(d^2 \ln d)/h$ is sufficiently small. A simple sufficient condition is

$$h \geq \pi d^2(4 + \ln d). \qquad (31)$$

This can be proved using the inequalities $\mu > (2h/\pi)^{1/2}$ and $\sigma \leq 1/4$; we omit the details. By results of Craigen [21] or Livinskyi [41], the inequality (31) (and hence also (30)) holds for all sufficiently large n (assuming, as always, that h is maximal and d minimal with $h + d = n$).

Remark 10. In the proof of Theorem 2 we did not use the Lovász Local Lemma, and we obtained a sharper result than that of Theorem 3 for $d < 10$ (see Remark 8). Similarly, we can improve Theorem 4 by not using the Lovász Local Lemma for small d. Instead of taking $p = 1/(4e(d-1))$ we take $p = 1/d^2 - \varepsilon$, and later let $\varepsilon \to 0$. In this way we obtain the inequality (29) with $\lambda = (d^2 - 1)^{1/2}\sigma/\mu$, $t = (2\ln(2d^2))^{1/2}/\mu$, which is an improvement on Theorem 4 for $d < 10$.

Remark 11. At least one of Theorem 1 or Theorem 4 is always applicable. In the region $n < 668$ the Hadamard conjecture has been verified, so $d \leq 3$ and Theorem 1 applies. Consider the complementary region $n \geq 668$. For $1 \leq d \leq 6$ the condition (31) holds. For $d \geq 7$ the condition (31) is weaker than the condition $h \geq 6d^3$ considered in [10]. Thus, it is sufficient to check the 13 cases $(h, d) = (h, h' - h + 1)$, where the exceptional intervals (h, h') are listed in [10, Table 1]. We find numerically that condition (30) holds for all of these. For example, the first entry with $(h, h') = (664, 672)$ is covered as the right side of (30) is $19.09\ldots$ but $\mu(664) = 21.55\ldots > 19.09$. Thus Theorem 4 is always applicable for $d \geq 4$.

Corollary 4. *Under the conditions of Theorem 4, we have*

$$R(n) \geq \left(\frac{2}{\pi e}\right)^{d/2} (1 - \lambda - (d-1)t)(1 - \lambda + t)^{d-1} e^{-d^2/(2h)} . \qquad (32)$$

For $d = o(h/\log h)^{1/2}$ this gives

$$R(n) \geq \left(\frac{2}{\pi e}\right)^{d/2} \exp\left(O(d^{3/2}/h^{1/2})\right) . \qquad (33)$$

Remark 12. Corollary 4 gives a nontrivial bound for $d \ll h^{1/2-\varepsilon}$, whereas Corollary 3 gives nothing useful if $d \gg h^{1/3+\varepsilon}$. Also, the constant implied by the "O" notation is smaller for Corollary 4 than for Corollary 3 – if both d and h are large, the implied constant in Corollary 4 is $(1-3/\pi)\sqrt{2\pi e} \approx 0.186$, whereas in Corollary 3 the corresponding constant is $\sqrt{2\pi e} \approx 4.13$.

Proof of Corollary 4. The proof of the inequality (32) is similar to the proof of (24)–(25) above, using the bound of Theorem 4 instead of the bound of Theorem 2.

To prove (33), it is sufficient to show that

$$(1 - \lambda - (d-1)t)(1 - \lambda + t)^{d-1} e^{-d^2/(2h)} = \exp\left(O(d^{3/2}/h^{1/2})\right) . \qquad (34)$$

Taking logarithms, and assuming for the moment that

$$\lambda + (d-1)t \leq 1/2, \qquad (35)$$

we see that (34) is equivalent to showing that

$$\lambda + (d-1)t + (d-1)(\lambda - t) + \frac{d^2}{2h} = O(d^{3/2}/h^{1/2}),$$

which simplifies to

$$d\lambda + \frac{d^2}{2h} = O(d^{3/2}/h^{1/2}). \qquad (36)$$

Using the definitions of λ and t, and the facts that $\sigma = O(1)$ and $\mu \sim ch^{1/2}$, we see that $\lambda = O((d/h)^{1/2})$, $t = O((\ln d)^{1/2}/h^{1/2})$. Thus, the dominant term on the left side of (36) is $d\lambda = O(d^{3/2}/h^{1/2})$, and the condition (35) is satisfied (for sufficiently large h) if $d(\ln d)^{1/2}/h^{1/2} = o(1)$. The latter condition follows from the assumption $d = o(h/\log h)^{1/2}$. $\qquad \square$

The following theorem gives asymptotically better results than Theorem 4. The proof uses the independence of the diagonal elements g_{ii} but does not use the Lovász Local Lemma. It might be possible to sharpen the inequality (40) via the Lovász Local Lemma, but this would complicate the argument while giving only a small improvement in the final result (only the right-hand side of (37) and the function $L(d)$ defined by (43) would change).

Theorem 5. *If $d \geq 2$, $4 \leq h \in \mathcal{H}$, $n = h + d$, $\lambda \in (0, 1)$, $t \geq 0$, $\tau = \sigma/\mu$, G, σ and μ as in §5.2, and*

$$\exp(\mu^2 t^2/2 - d\tau^2/\lambda^2) \geq 2d(d-1), \tag{37}$$

then

$$\frac{\det G}{\mu^d} \geq (1 - \lambda - (d-1)t)(1 - \lambda + t)^{d-1} \tag{38}$$

occurs with positive probability.

Remark 13. The inequality (38) is the same as the inequality (29) occurring in Theorem 4, but the choice of (λ, t) is different in Theorem 4.

Proof of Theorem 5. For the purposes of this proof we say that a matrix G is *good* if $g_{ii} \geq \mu(1-\lambda)$ and $|g_{ij}| \leq \mu t$ for all $i \neq j$ (this definition is equivalent to the one used in the proof of Theorem 4). From Cantelli's inequality we have

$$\mathbb{P}[g_{ii} \geq \mu(1-\lambda)] \geq \frac{\lambda^2}{\tau^2 + \lambda^2} > \exp(-\tau^2/\lambda^2).$$

Since the g_{ii} are independent, we deduce that

$$\mathbb{P}[\min\{g_{ii} : 1 \leq i \leq d\} \geq \mu(1-\lambda)] > \exp(-d\tau^2/\lambda^2). \tag{39}$$

Also, as in the proof of Theorem 4, Hoeffding's inequality implies that

$$\mathbb{P}[|g_{ij}| \geq \mu t] \leq 2\exp(-\mu^2 t^2/2) \text{ for } i \neq j.$$

Thus

$$\mathbb{P}[\max\{|g_{ij}| : 1 \leq i, j \leq d, i \neq j\} \geq \mu t] \leq 2d(d-1)\exp(-\mu^2 t^2/2). \tag{40}$$

From the inequalities (39) and (40) we see[5] that the condition

$$\exp(-d\tau^2/\lambda^2) \geq 2d(d-1)\exp(-\mu^2 t^2/2) \tag{41}$$

---

[5]Informally, (39) gives a lower bound on the probability that the diagonal elements g_{ii} are all good, and (40) gives an upper bound on the probability that at least one of the off-diagonal elements g_{ij} is bad. If the first probability exceeds the second, then a good G occurs with positive probability.

implies that, with positive probability, a random choice of B gives a good matrix G. Thus, *some* choice of B gives a good matrix G. However, the condition (41) is equivalent to the condition (37) in the statement of the Theorem. To conclude the proof, it suffices to observe that the lower bound (38) on $\det(G)$ for a good matrix G follows from Lemma 14 applied to $M = \mu^{-1}G$. $\qquad\square$

Remark 14. There are two parameters, λ and t, occurring in Theorem 5. In stating the Theorem we excluded the case $d = 1$, because if $d = 1$ then t is irrelevant and we may take λ arbitrarily close to 0, giving $|\det(G)| \geq \mu^d$, as obtained previously by Brown and Spencer [12] and (independently) by Best [6]. To obtain the best bound (38) for $d \geq 2$ we choose t so that equality holds in (37). Thus, in the following, we choose

$$t^2 = \frac{2(d\tau^2/\lambda^2 + L(d))}{\mu^2}, \tag{42}$$

where

$$L(d) := \ln[2d(d-1)]. \tag{43}$$

The optimal $\lambda \in (0,1)$ may be found by a straightforward numerical optimisation. In most cases there is no need for this, as Corollary 5 gives a result that is close to optimal.

Corollary 5. *Suppose that $1 < d = o(h^{2/5})$ and we choose*

$$\lambda = \left(\frac{2d(d-1)\sigma^2}{\mu^4}\right)^{1/3} \tag{44}$$

in Theorem 5. Then we obtain

$$\mathcal{R}(n) \geq \left(\frac{2}{\pi e}\right)^{d/2} \exp\left(d\sqrt{\frac{\pi}{2h}} - \frac{3d\lambda}{2} + O((d\lambda)^{3/2})\right). \tag{45}$$

Remark 15. The choice (44) is motivated as follows. When λ and t are small, the lower bound (38) is

$$\det(G)/\mu^d \geq \exp\left(-d\lambda - \frac{d(d-1)t^2}{2} + O(d^3t^3)\right),$$

so to obtain a good lower bound on $\det(G)$ we should minimise

$$\lambda + \frac{(d-1)t^2}{2}.$$

29

Since t^2 is given by (42), we should minimise

$$\lambda + (d-1)(d\tau^2/\lambda^2 + L(d))/\mu^2 .$$

Since the term involving $L(d)$ is independent of λ, we ignore it and minimize

$$f(\lambda) := \lambda + \frac{d(d-1)\tau^2}{\mu^2\lambda^2} .$$

Differentiating $f(\lambda)$ with respect to λ, setting $f'(\lambda) = 0$, and using $\tau = \sigma/\mu$, we obtain (44). Also, $\min_{x>0} f(x) = 3\lambda/2$, where λ is given by (44).

Since $\mu \asymp h^{1/2}$ and $\sigma \asymp 1$, we see that $\lambda \asymp (d/h)^{2/3}$. Thus $d\lambda \asymp d^{5/3}/h^{2/3}$, which is asymptotically smaller than the terms of order $d^{3/2}/h^{1/2}$ occurring in Theorem 3 and Corollaries 3–4. Thus Corollary 5 is asymptotically sharper. This is significant in the proof of Theorem 6 below.

Proof of Corollary 5. Substitution of (44) and (42) into the bound (38), then taking logarithms and estimating the errors involved as in Remark 15, shows that

$$|\det G| \geq \mu^d \exp\left(-\frac{3d\lambda}{2} + O((d\lambda)^{3/2}) + O(d^2/h)\right). \qquad (46)$$

Now $d\lambda \asymp (d^5/h^2)^{1/3}$, so $d\lambda = o(1)$ iff $d = o(h^{2/5})$. Also, from Lemma 12,

$$\mu = \left(\frac{2h}{\pi}\right)^{1/2} \exp\left[\left(\frac{\pi}{2h}\right)^{1/2} + O\left(\frac{1}{h}\right)\right]. \qquad (47)$$

Using the Schur complement lemma and Lemma 16, it follows from (46)–(47) that

$$\mathcal{R}(n) \geq \left(\frac{2}{\pi e}\right)^{d/2} \exp(\Delta),$$

where

$$\Delta = d\sqrt{\frac{\pi}{2h}} - \frac{3d\lambda}{2} + O((d\lambda)^{3/2}) + O(d^2/h).$$

Since $d^2/h \ll (d\lambda)^{3/2} \asymp d^{5/2}/h$, the second "$O$" term can be subsumed by the first "O" term. $\qquad\square$

We now extend Theorem 1 to cases $d > 3$, provided that n is sufficiently large, where the threshold n_0 is independent of d. This improves Theorem 1 above, which assumes $d \leq 3$. It also improves Corollary 2 of [10], where $d > 3$ is allowed, but the threshold is a rapidly-growing function of d.

Theorem 6. *Assume that $n = h + d$, where $d \geq 0$, $h \in \mathcal{H}$, and d is minimal. There exists an absolute constant n_0 such that, for all $n \geq n_0$,*

$$\mathcal{R}(n) \geq \left(\frac{2}{\pi e}\right)^{d/2}.$$

Moreover, the inequality is strict if $d > 0$.

Proof. For $d \leq 3$ the result follows from Theorem 1, so we may assume that $d \geq 4$. In Corollary 5, $\lambda \asymp (d/h)^{2/3}$. Thus $\lambda h^{1/2} \asymp (d/h^{1/4})^{2/3}$. From (17), $d = o(h^{1/4})$, so $\lambda = o(h^{-1/2})$. Thus, for sufficiently large h, the argument $d(\sqrt{\pi/(2h)} - O(\lambda))$ of the exponential in (45) is positive, implying that $\mathcal{R}(n) > (2/(\pi e))^{d/2}$. □

Remark 16. Using Corollary 6 of [10], which follows from Theorem 5.4 of Livinskyi [41], we can show that $n_0 = 10^{45}$ is sufficient in Theorem 6. No doubt this value of n_0 can be reduced considerably. Since this paper is long enough, we resist the temptation to attempt any such reduction here. As mentioned in §1, we conjecture that Theorem 6 holds with $n_0 = 1$.

9   Numerical examples

Consider the case $n = 668$. At the time of writing it is not known whether a Hadamard matrix of this order exists. Assuming it does not, we take $h = 664$, $d = 4$, $n = h + d = 668$. Thus $\mu \approx 21.55231$, $\sigma^2 \approx 0.04638855$. Column 2 of Table 1 gives various lower bounds on $\det(G)/\mu^d$ (for G that occurs with positive probability). These may be converted to lower bounds on $\mathcal{R}(n)$ if desired; the constant of proportionality is $\mu^d h^{h/2}/n^{n/2} \approx 0.06583$. We give $\det(G)/\mu^d$ as it is a useful "figure of merit" to compare different probabilistic approaches – the upper limit of these approaches is $\det(G)/\mu^d = 1$.

Column 5 of Table 1 gives the corresponding bounds for $d = 7$, $n = 671$. This is a difficult case since it is the smallest with $d = 7$ (assuming as before that $664 \notin \mathcal{H}$). Theorem 2 and Remark 5 give negative bounds since d^4/h is too large. Similarly for Theorem 3 since d^3/h is too large (even when $d = 4$). However, Theorem 4 gives a useful bound (in agreement with Remark 11), as does Theorem 5.

The entries in the rows labelled "Corollary 5" use (44) to define λ; the entries in rows labelled "Theorem 5" use optimal values of λ; t is defined by (42) in both cases.

Bound	$d = 4, n = 668$			$d = 7, n = 671$		
	$|G|/\mu^d$	λ	t	$|G|/\mu^d$	λ	t
Theorem 2	0.2576	—	—	—	—	—
Remark 5	0.3521	—	—	—	—	—
Theorem 4	0.6781	0.05619	0.1341	0.0742	0.08010	0.1448
Remark 10	0.7565	0.03870	0.1222	0.1326	0.06924	0.1405
Corollary 5	0.7975	0.01728	0.1394	0.1125	0.02624	0.1531
Theorem 5	0.7990	0.01937	0.1352	0.1667	0.04238	0.1441

Table 1: Lower bounds for $h = 664$, $d \in \{4, 7\}$, $n = h + d$.

Table 2 gives various lower bounds on $\det(G)/\mu^d$ for the cases $h = 996$, $d \in \{2, 3\}$, so $n \in \{998, 999\}$. Here $\mu \approx 26.17449$ and $\sigma^2 \approx 0.04594917$. Lemma 17 is applicable, as $d \leq 3$. Lemma 17 does not state an explicit bound for $\det(G)/\mu^d$; Table 2 gives the value $1 - \eta/\mu^d$ that occurs in the proof of Lemma 17 – see the inequality (21). Since $\eta/\mu^d = O_d(h^{-1})$, it is not surprising that Lemma 17 gives the sharpest bound for $d \leq 3$.

Bound	$d = 2, n = 998$			$d = 3, n = 999$		
	$|G|/\mu^d$	λ	t	$|G|/\mu^d$	λ	t
Lemma 17	0.9985	—	—	0.9910	—	—
Theorem 2	0.8472	—	—	0.6562	—	—
Remark 5	0.8895	—	—	0.7160	—	—
Theorem 3	0.7480	—	—	0.4655	—	—
Theorem 4	0.9402	0.02573	0.0948	0.8581	0.03730	0.1049
Remark 10	0.9658	0.01418	0.0779	0.9058	0.02316	0.0919
Corollary 5	0.9741	0.00732	0.1066	0.9287	0.01055	0.1119
Theorem 5	0.9741	0.00733	0.1065	0.9288	0.01102	0.1010

Table 2: Lower bounds for $h = 996$, $d \in \{2, 3\}$, $n = h + d$.

References

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

[2] Anonymous, Putnam Competition, 1974, `http://www.math-olympiad.com/35th-putnam-mathematical-competition-1974-problems.htm`.

[3] R. C. Baker, G. Harman and J. Pintz, The difference between consecutive primes, II, *Proc. London Mathematical Society* **83** (2001), 532–562.

[4] G. Barba, Intorno al teorema di Hadamard sui determinanti a valore massimo, *Giorn. Mat. Battaglini* **71** (1933), 70–86.

[5] D. Best, D. Ž. Đoković (Djoković), H. Kharaghani and H. Ramp, Turyn-type sequences: classification, enumeration and construction, *J. Combin. Designs* **21** (2013), 24–35. Also arXiv:1206.4107v1, 19 June 2012.

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

[7] R. P. Brent, H. Ohtsuka, J. H. Osborn and H. Prodinger, *Some binomial identities involving absolute values*, in preparation, Feb. 2014.

[8] R. P. Brent and J. H. Osborn, General lower bounds on maximal determinants of binary matrices, *The Electronic Journal of Combinatorics* **20**(2), 2013, #P15, 12 pp. Also arXiv:1208.1805v6, 14 April 2013.

[9] R. P. Brent and J. H. Osborn, *Note on a double binomial sum relevant to the Hadamard maximal determinant problem*, arXiv:1309.2795v2, 12 Sept. 2013, 6 pp.

[10] 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.

[11] R. P. Brent, J. H. Osborn and W. D. Smith, *Bounds on determinants of perturbed diagonal matrices*, arXiv:1401.7084v5, 13 March 2014, 17 pp.

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

[13] R. A. Brualdi and H. Schneider, Determinantal identities: Gauss, Schur, Cauchy, Sylvester, Kronecker, Jacobi, Binet, Laplace, Muir, and Cayley, *Lin. Alg. Appl.* **52/53** (1983), 769–791.

[14] F. P. Cantelli, Intorno ad un teorema fondamentale della teoria del rischio, *Bollettino Associazione Attuari Italia* (1910), 1–23.

[15] P. Chebyshev, Des valeurs moyennes, *Journal de Mathématiques pures et appliquées* **2**, 12 (1867), 177–184.

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

[17] J. H. E. Cohn, On the value of determinants, *Proc. Amer. Math. Soc.* **14** (1963), 581–588.

[18] C. J. Colbourn and J. H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996.

[19] C. J. Colbourn and J. H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, second edition, CRC Press, Boca Raton, 2007.

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

[21] R. Craigen, Signed groups, sequences, and the asymptotic existence of Hadamard matrices, *J. Comb. Theory*, Series A **71** (1995), 241–254.

[22] R. Craigen, Hadamard matrices and designs, in [18, Chapter IV.24].

[23] R. Craigen and H. Kharagani, Hadamard matrices and Hadamard designs, in [19, Chapter V.1].

[24] H. Cramér, On the order of magnitude of the difference between consecutive prime numbers, *Acta Arithmetica* **2** (1936), 23–46.

[25] J. H. Dinitz and D. R. Stinson (eds.), *Contemporary Design Theory: A Collection of Surveys*, J. Wiley, New York, 1992.

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

[27] H. Ehlich, Determinantenabschätzungen für binäre Matrizen mit $n \equiv$ 3 mod 4, *Math. Z.* **84** (1964), 438–447.

[28] P. Erdős and L. Lovász, Problems and results on 3-chromatic hypergraphs and some related questions, in *Infinite and Finite Sets* (A. Hajnal, R. Rado and V. T. Sós, eds.), North-Holland, Amsterdam, 1975, 609–628.

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

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

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

[32] N. J. Higham, *Accuracy and Stability of Numerical Algorithms*, SIAM, Philadelphia, 1996.

[33] W. Hoeffding, Probability inequalities for sums of bounded random variables, *J. Amer. Statistical Association* **58** (1963), 13–30.

[34] K. J. Horadam, *Hadamard Matrices and their Applications*, Princeton University Press, Princeton, New Jersey, 2007.

[35] 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.

[36] H. Kharaghani and C. Koukouvinos, Complementary, base and Turyn sequences, in [19], 317–321.

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

[38] H. von Koch, Über das Nichtverschwinden einer Determinante nebst Bemerkungen über Systeme unendlich vieler linearer Gleichungen, *Jber. Deutschen Math. Verein.* **22** (1913), 285–291.

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

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

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

[42] V. Maz'ya and T. Shaposhnikova, *Jacques Hadamard, A Universal Mathematician*, History of Mathematics, Vol. 14, AMS and LMS, 1998.

[43] T. Muir, Hadamard's approximation theorem since 1900, *Trans. Royal Soc. of South Africa* **13** (1925), 299–308.

[44] W. P. Orrick and B. Solomon, Large determinant sign matrices of order $4k + 1$, *Discrete Mathematics* **307** (2007), 226–236.

[45] A. M. Ostrowski, Sur la détermination des bornes inférieures pour une classe des déterminants, *Bull. Sci. Math.* (2) **61** (1937), 19–32. Reprinted in [47, pp. 17–30].

[46] 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. Reprinted in [47, pp. 60–74].

[47] A. M. Ostrowski, *Alexander Ostrowski: Collected Mathematical Papers*, Vol. 1 (Determinants, Linear Algebra, Algebraic Equations), Birkhäuser, 1983.

[48] 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.

[49] I. Schur, Über Potenzreihen, die im Innern des Einheitskreises beschränkt sind, *J. Reine Angew. Math.* **147** (1917), 205–232. Reprinted in *Issai Schur Gesammelte Abhandlungen*, Springer, Berlin, 1973, Vol. II, 137–164.

[50] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, in [25], 431–560.

[51] D. Shanks, On maximal gaps between successive primes, *Math. Comput.* **18** (1964), 646–651.

[52] J. Shearer, On a problem of Spencer, *Combinatorica* **5** (1985), 241–245.

[53] T. O. e Silva, *Gaps between consecutive primes*, `http://www.ieeta.pt/~tos/gaps.html`.

[54] J. J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers, *Philosophical Magazine* **34** (1867), 461–475.

[55] R. J. Turyn, Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings, *J. Combin. Theory A* **16** (1974), 313–333.

[56] J. Seberry Wallis, On the existence of Hadamard matrices, *J. Comb. Theory* **21** (1976), 188–195.

[57] F. R. Sharpe, The maximum value of a determinant, *Bull. Amer. Math. Soc.* **14** (1907), 121–123.

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

[59] T. Xia, M. Xia and J. Seberry, Regular Hadamard matrices, maximum excess and SBIBD, *Australasian J. Combinatorics* **27** (2003), 263–275.