Bull. Aust. Math. Soc. **88** (2013), 280–285
doi:10.1017/S000497271200086X

BOUNDS ON MINORS OF BINARY MATRICES

RICHARD P. BRENT✉ and JUDY-ANNE H. OSBORN

(Received 19 August 2012; accepted 13 September 2012; first published online 23 December 2012)

Abstract

We prove an upper bound on sums of squares of minors of $\{+1, -1\}$-matrices. The bound is sharp for Hadamard matrices, a result due to de Launey and Levin ['$(1, -1)$-matrices with near-extremal properties', *SIAM J. Discrete Math.* **23** (2009), 1422–1440], but our proof is simpler. We give several corollaries relevant to minors of Hadamard matrices.

2010 *Mathematics subject classification*: primary 05B20; secondary 15A15, 15B34.

Keywords and phrases: Hadamard matrices, binary matrices, $\{+1, -1\}$-matrices, minors, Cauchy–Binet formula, mean square.

1. Introduction

A $\{+1, -1\}$-matrix (or $\{\pm 1\}$-matrix) is a matrix A whose elements are $+1$ or -1. We consider $n \times n$ $\{\pm 1\}$-matrices; n is called the *order* of the matrix. A *minor of order* m is the determinant of an $m \times m$ submatrix M of A.

Theorem 2.2 gives an upper bound on the mean square of the minors of order m of any $\{\pm 1\}$-matrix A of order $n \geq m$. The upper bound is attained if A is a Hadamard matrix, and this case was proved by de Launey and Levin [2, Proposition 2]. Our proof, using the Cauchy–Binet formula [3, 10], is much simpler than the proof given for the Hadamard case by de Launey and Levin, which requires consideration of the cycle structure of random permutations and an identity involving Stirling numbers.

In Section 3 we give several easy corollaries of Theorem 2.2.

Corollary 3.1 shows that, in the mean square sense, the minors of Hadamard matrices are strictly larger than the minors of random $\{\pm 1\}$-matrices, except for the trivial case of minors of order one.

A difficult, not yet completely solved, problem is to find the asymptotic behaviour of the probability that a random $\{\pm 1\}$-matrix of order n is singular; see [6, 14]. In Corollary 3.3 we consider a simpler but analogous problem concerning zero minors of $\{\pm 1\}$-matrices. The corollary gives a lower bound on the number of zero minors of order m of a $\{\pm 1\}$-matrix of order n. The bound is nontrivial in the cases $2 \leq m \leq 6$.

Corollary 3.4 gives a criterion for when a $\{\pm 1\}$-matrix must have singular minors of small order, and a lower bound on their number. In some cases the result is sharper than that obtained by a standard argument using Dirichlet's pigeonhole principle.

Corollary 3.6 gives exact formulas for the number of zero minors of orders two and three in Hadamard matrices. The formula for minors of order two is implicit in a paper of Little and Thuente [9], but the result for minors of order three appears to be new.

For simplicity we consider only minors of square $\{\pm 1\}$-matrices. The results can be extended without difficulty to minors of rectangular matrices, say $n \times p$ $\{\pm 1\}$-matrices with minors of order $m \le \min(n, p)$. It is also possible to extend some of the results to rectangular submatrices M, say $m \times m'$, where $m \le m'$, if $|\det(M)|^2$ is replaced by $\det(MM^T)$ below.

2. The mean square of minors

Theorem 2.2 gives an upper bound on the mean square of minors of $\{\pm 1\}$-matrices. The bound is sharp because it is attained for Hadamard matrices. For the case where the matrix A is a Hadamard matrix, the result is due to de Launey and Levin [2, Proposition 2], and their proof could perhaps be modified to show that strict inequality occurs when A is not a Hadamard matrix. However, we give a different and simpler proof.

Definition 2.1. If A is a $\{\pm 1\}$-matrix and $m \in \mathbb{N}$, then $S_m(A)$ is the set of all $m \times m$ submatrices of A.

Theorem 2.2. *Let A be a square $\{\pm 1\}$-matrix of order $n \ge m > 1$. Then the mean value $E(\det(M)^2)$ of $\det(M)^2$, taken over all $M \in S_m(A)$, satisfies*

$$E(\det(M)^2) \le n^m \Big/ \binom{n}{m}. \tag{2.1}$$

Moreover, equality holds in (2.1) if and only if A is a Hadamard matrix.

Proof. Consider the $m \times n$ matrix B formed by taking any m rows of A, and apply the Cauchy–Binet formula to B, obtaining

$$\det(BB^T) = \sum_{M \in S_m(B)} \det(M)^2. \tag{2.2}$$

From Hadamard's inequality [4], the left-hand side of (2.2) is bounded above by n^m, with equality occurring if and only if the rows of B are orthogonal. Thus

$$\sum_{M \in S_m(B)} \det(M)^2 \le n^m.$$

Summing over all $\binom{n}{m}$ ways in which we can choose B, we obtain

$$\sum_{M \in S_m(A)} \det(M)^2 \le n^m \binom{n}{m}.$$

https://doi.org/10.1017/S000497271200086X Published online by Cambridge University Press

Now, dividing by $|S_m(A)| = \binom{n}{m}^2$ to give the mean value over all submatrices of order m, we obtain (2.1). It is clear from the proof that equality occurs in (2.1) if and only if the rows of B are pairwise orthogonal for all choices of B. Since $m \geq 2$, this implies that the rows of A are pairwise orthogonal, and hence A is a Hadamard matrix. □

3. Corollaries

Turán [15] showed that the expected value of $\det(A)^2$ for $\{\pm 1\}$-matrices A of order m, chosen uniformly at random, is $m!$. Corollary 3.1 shows that, for submatrices M of Hadamard matrices, the mean value of $\det(M)^2$ is always greater than the expected value for random $\{\pm 1\}$-matrices, excluding the trivial case $m = 1$ for which equality occurs.

Corollary 3.1. *Let H be a Hadamard matrix of order $n \geq m > 1$. Then the mean value $E(\det(M)^2)$ of $\det(M)^2$, taken over all $M \in S_m(H)$, satisfies*

$$E(\det(M)^2) > m!.$$

Proof. From Theorem 2.2,

$$E(\det(M)^2) = n^m \Big/ \binom{n}{m} = m! \prod_{k=1}^{m-1} \left(1 - \frac{k}{n}\right)^{-1} > m!.$$

This concludes the proof. □

Definition 3.2. Let A be a square $\{\pm 1\}$-matrix of order $n \geq m \geq 1$. Then:

(i) $Z(m, A)$ is the number of zero minors of order m of A; and
(ii) $Y(m, A)$ is the number of nonzero minors of order m of A.

Corollary 3.3. *Let A be a square $\{\pm 1\}$-matrix of order $n \geq m > 1$. Then*

$$Y(m, A) \leq 4\left(\frac{n}{4}\right)^m \binom{n}{m}$$

and

$$Z(m, A) \geq \binom{n}{m}\left(\binom{n}{m} - 4\left(\frac{n}{4}\right)^m\right).$$

Moreover, if $m \leq 3$, then equality occurs if and only if A is a Hadamard matrix.

Proof. Using a well-known mapping from $\{\pm 1\}$-matrices of order m to $\{0, 1\}$-matrices of order $m - 1$, it is easy to prove that the determinant of a $\{\pm 1\}$-matrix of order m is divisible by 2^{m-1}. Thus, each nonzero minor of order m has square at least 4^{m-1}, and

$$\sum_{M \in S_m(A)} \det(M)^2 \geq 4^{m-1} Y(m, A). \tag{3.1}$$

https://doi.org/10.1017/S000497271200086X Published online by Cambridge University Press

Table 1. Zero minor probability p_m and threshold $n_0(m)$.

m	p_m	$\widehat{p}_m$	$n_0(m)$	$2^{m-1}+1$
2	0.5000	0.5000	3	3
3	0.6250	0.6250	5	5
4	0.6250	0.5898	8	9
5	0.5312	0.5001	15	17
6	0.2969	0.3924	45	33

However, from Theorem 2.2 we have

$$\sum_{M\in S_m(A)} \det(M)^2 \le n^m \binom{n}{m}.$$

Thus $4^{m-1}Y(m,A) \le n^m\binom{n}{m}$, which gives the inequality for $Y(m,A)$. The inequality for $Z(m,A)$ follows from the observation that

$$Y(m,A) + Z(m,A) = \binom{n}{m}^2,$$

since the total number of minors of order m is $\binom{n}{m}^2$. Finally, suppose that $1 < m \le 3$. Then there is only one nonzero value of $\det(M)^2$, namely 4^{m-1}. Thus, equality occurs in (3.1), and the last sentence of the corollary follows from the last sentence of Theorem 2.2. □

Corollary 3.4 shows that a sufficiently large $\{\pm 1\}$-matrix always has singular submatrices of order $m \le 6$. In fact, such submatrices occur with positive density at least p_m, where p_m is given in Table 1.

Corollary 3.4. *Let A be a $\{\pm 1\}$-matrix of order n, and suppose that $2 \le m \le 6$. Then A has a singular submatrix of order m if $n \ge n_0(m)$, where $n_0(m)$ is as in Table 1.*

Proof. A has a singular submatrix of order m if and only if $Z(m,A) > 0$, and from Corollary 3.3 a sufficient condition for this is that

$$\binom{n}{m} > 4\left(\frac{n}{4}\right)^m. \tag{3.2}$$

Since $m! < 4^{m-1}$ for $2 \le m \le 6$ we see that (3.2) holds for $2 \le m \le 6$ provided that n is sufficiently large. In fact, a computation shows that we need $n \ge n_0(m)$, where $n_0(m)$ is given in Table 1. □

Remark 3.5. Consider A as in Corollary 3.4. If $n > 2^m$ then, by Dirichlet's pigeonhole principle, any $m \times n$ submatrix B of A must have two identical columns, so A must have a singular $m \times m$ submatrix. In fact, by normalising the first row of B to

https://doi.org/10.1017/S000497271200086X Published online by Cambridge University Press

be $(+1, +1, \ldots, +1)$, the statement is true for $n > 2^{m-1}$. Comparing $n_0(m)$ and $2^{m-1} + 1$ (see Table 1), we see that Corollary 3.4 gives a slightly stronger result for $m \in \{4, 5\}$. Also, the proof of Corollary 3.4 shows that the density of singular submatrices as $n \to \infty$ is at least

$$p_m = \lim_{n\to\infty} \left(1 - 4\left(\frac{n}{4}\right)^m \Big/ \binom{n}{m}\right) = 1 - 4^{1-m} m!.$$

Using an extension of the argument above that used the pigeonhole principle, we obtain a corresponding density

$$\widehat{p_m} = 1 - \prod_{k=1}^{m-1} (1 - 2^{1-m} k)\,.$$

Table 1 gives the values of $\widehat{p_m}$ for $2 \le m \le 6$ to four decimal places; we see that $p_m > \widehat{p_m}$ for $4 \le m \le 5$.

The frequencies of small singular submatrices of Hadamard matrices are given in Corollary 3.6. The corollary is restricted to $m \le 3$ because for $m > 3$ we find by computation that $Z(m, H)$ depends on the Hadamard equivalence class of H. For example, this is true if $n = 16$ and $m = 4$, when there are four possible values of $Z(m, H)$. It is straightforward to prove Corollary 3.6 by enumeration of the singular submatrices of order $m \in \{2, 3\}$, but we give a shorter proof using Corollary 3.3.

Corollary 3.6. *Let H be a Hadamard matrix of order n. Then*

$$Z(2, H) = \frac{n^2(n-1)(n-2)}{8}$$

and

$$Z(3, H) = \frac{n^2(n-1)(n-2)(n-4)(5n-4)}{288}.$$

Proof. This is just the last part of Corollary 3.3, where we have explicitly computed and simplified the expressions for $Z(m, H)$ in the cases $m = 2$ and $m = 3$. □

Remark 3.7. We expect random $\{\pm 1\}$-matrices of order two to be singular with probability $1/2$, and matrices of order three to be singular with probability $5/8$; see [6, 11]. These probabilities agree with the limiting probabilities that we obtain from Corollary 3.6 as $n \to \infty$. More precisely,

$$Z(2, H) \Big/ \binom{n}{2}^2 = \frac{1}{2} - O\left(\frac{1}{n}\right) \quad \text{and} \quad Z(3, H) \Big/ \binom{n}{3}^2 = \frac{5}{8} - O\left(\frac{1}{n}\right).$$

In this sense the minors of order two and three of Hadamard matrices of order n behave like the minors of random $\{\pm 1\}$-matrices in the limit as $n \to \infty$.

https://doi.org/10.1017/S000497271200086X Published online by Cambridge University Press

REMARK 3.8. From Szöllősi's theorem [13, Proposition 5.5] or Jacobi's determinant identity [1, 5],

$$Z(m, H) = Z(n - m, H).$$

Thus, the minors of order $m \geq n - 3$ of Hadamard matrices of order n take only a small number of distinct values and certainly do *not* behave like the minors of random $\{\pm 1\}$-matrices as $n \to \infty$. Previously, such results were obtained by a more detailed study of the structure of Hadamard matrices; see, for example, [2, 7, 8, 12].

References

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

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

[3] F. R. Gantmacher, *The Theory of Matrices,* Vol. 1 (AMS Chelsea Publishing, Providence, RI, 2000).

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

[5] C. G. J. Jacobi, 'De formatione et proprietatibus determinantium', *Crelle's J.* **22** (1841), 285–318; also *Gesammelte Werke*, Bd. 3 (Chelsea Publishing Company, New York, 1969).

[6] J. Kahn, J. Komlós and E. Szemerédi, 'On the probability that a random ±1-matrix is singular', *J. Amer. Math. Soc.* **8** (1995), 223–240.

[7] C. Koukouvinos, E. Lappas, M. Mitrouli and J. Seberry, 'An algorithm to find formulae and values of minors for Hadamard matrices: II', *Linear Algebra Appl.* **371** (2003), 111–124.

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

[9] C. H. C. Little and D. J. Thuente, 'The Hadamard conjecture and circuits of length four in a complete bipartite graph', *J. Aust. Math. Soc. (Ser. A)* **31** (1981), 252–256.

[10] T. Muir, *A Treatise on the Theory of Determinants* (Dover, New York, 1960).

[11] OEIS Foundation Inc., 'The on-line encyclopedia of integer sequences', 2012, http://oeis.org/A057982. Also A046747.

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

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

[14] T. Tao and V. Vu, 'On random ±1 matrices: singularity and determinant', *Random Structures Algorithms* **28** (2006), 1–23.

[15] P. Turán, 'On extremal problems concerning determinants', *Math. Naturwiss. Anz. Ungar. Akad. Wiss.* **59** (1940), 95–105.

RICHARD P. BRENT, Australian National University,
Canberra, ACT 0200, Australia
e-mail: minors@rpbrent.com

JUDY-ANNE H. OSBORN, The University of Newcastle,
Callaghan, NSW 2308, Australia
e-mail: Judy-anne.Osborn@newcastle.edu.au

https://doi.org/10.1017/S000497271200086X Published online by Cambridge University Press