Bounds on minors of binary matrices

Richard P. Brent

Australian National University

Canberra, ACT 0200, Australia

`minors@rpbrent.com`

Judy-anne H. Osborn

The University of Newcastle

Callaghan, NSW 2308, Australia

`Judy-anne.Osborn@newcastle.edu.au`

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 (2009), but our proof is simpler. We give several corollaries relevant to minors of Hadamard matrices, and generalise a result of Turán on determinants of random $\{+1, -1\}$ matrices.

1   Introduction

A $\{+1, -1\}$-matrix (abbreviated "$\{\pm 1\}$-matrix" below) 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 1 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 [8, Proposition 2]. Our proof, using the Cauchy-Binet formula [2, 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 §3 we give several easy corollaries of Theorem 1.

Corollary 1 shows that, in the mean square sense, the minors of Hadamard matrices are strictly larger than the minors of random $\{\pm1\}$-matrices, except for the trivial case of minors of order 1.

A difficult, not yet completely solved, problem is to find the asymptotic behaviour of the probability that a random $\{\pm1\}$-matrix of order n is singular, see [5, 14]. In Corollary 2 we consider a simpler but analogous problem concerning zero minors of $\{\pm1\}$-matrices. The corollary gives a lower bound on the number of zero minors of order m of a $\{\pm1\}$ matrix of order n. The bound is nontrivial in the cases $2 \le m \le 6$.

Corollary 3 gives a criterion for when a $\{\pm1\}$ 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 "pigeon-hole" principle.

Corollary 4 gives exact formulæ for the number of zero minors of orders 2 and 3 in Hadamard matrices. The formula for minors of order 2 is implicit in a paper of Little and Thuente [9], but the result for minors of order 3 appears to be new.

Finally, Theorem 2 generalises a well-known result of Turán [15] on the mean-square determinant of a random $\{\pm1\}$-matrix.

For simplicity, in §§2–3 we consider only minors of square $\{\pm1\}$-matrices. The results can be extended without difficulty to minors of rectangular matrices, say $n \times p$ $\{\pm1\}$-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 $\det(MM^T)$.

2   The mean square of minors

Theorem 1 gives an upper bound on the mean square of minors of $\{\pm1\}$ matrices. The bound is sharp because it is attained for Hadamard matrices. For the case that the matrix A is a Hadamard matrix, the result is due to de Launey and Levin [8, 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 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 1. *Let A be a square $\{\pm 1\}$ matrix of order $n \geq m > 1$. Then the mean value $E(\det(M)^2)$ of $\det(M)^2$, taken over all $M \in S_m(A)$, satisfies*

$$E(\det(M)^2) \leq n^m / \binom{n}{m}. \tag{1}$$

Moreover, equality holds in (1) iff 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

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

From Hadamard's inequality [3], the left side of (2) is bounded above by n^m, with equality occurring iff the rows of B are orthogonal. Thus

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

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

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

Now, dividing by $|S_m(A)| = \binom{n}{m}^2$ to give the mean value over all submatrices of order m, we obtain the inequality (1). It is clear from the proof that equality occurs in (1) iff 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. $\square$

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 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 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 1,

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

$\square$

Definition 2. *Let A be a square $\{\pm 1\}$ matrix of order $n \geq m \geq 1$. Then*

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

Corollary 2. *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 iff 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 an order m $\{\pm 1\}$ matrix is divisible by 2^{m-1}. Thus, each nonzero minor of order m has square at least 4^{m-1}, and

$$\sum_{M \in S_m(A)} \det(M)^2 \geq 4^{m-1} Y(m, A). \tag{3}$$

However, from Theorem 1 we have

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

4

Thus $4^{m-1}Y(m, A) \leq n^m \binom{n}{m}$, 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 $1 < m \leq 3$. Then there is only one nonzero value of $\det(M)^2$, namely 4^{m-1}. Thus, equality occurs in (3), and the last sentence of the corollary follows from the last sentence of Theorem 1. $\square$

Corollary 3 shows that a sufficiently large $\{\pm 1\}$ matrix always has singular submatrices of order $m \leq 6$. In fact, such submatrices occur with positive density at least p_m, where p_m is given in Table 1.

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

Table 1: Lower bound on zero minor probability p_m,
and threshold $n_0(m)$, see Corollary 3.
For p_m, $\widehat{p}_m$ see eqns. (5)–(6).

Corollary 3. *Let A be a $\{\pm 1\}$ matrix of order n, and suppose $2 \leq m \leq 6$. Then A has a singular submatrix of order m if $n \geq n_0(m)$, where $n_0(m)$ is as in Table 1.*

Proof. A has a singular submatrix of order m iff $Z(m, A) > 0$, and from Corollary 2 a sufficient condition for this is that

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

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

Remark 1. Consider A as in Corollary 3. 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 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 gives a slightly stronger result for $m \in \{4, 5\}$. Also, the proof of Corollary 3 shows that the density of singular submatrices as $n \to \infty$ is at least

$$p_m = \lim_{n \to \infty} \left(1 - 4 \left(\frac{n}{4} \right)^m \bigg/ \binom{n}{m} \right) = 1 - 4^{1-m} m! . \tag{5}$$

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

$$\widehat{p}_m = 1 - \prod_{k=1}^{m-1} (1 - 2^{1-m} k) . \tag{6}$$

Table 1 gives the values of $\widehat{p}_m$ for $2 \leq m \leq 6$ to 4 decimal places; we see that $p_m > \widehat{p}_m$ for $4 \leq m \leq 5$. [End of remark 1.]

The frequencies of small singular submatrices of Hadamard matrices are given in Corollary 4. The corollary is restricted to $m \leq 3$ 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 4 by enumeration of the singular submatrices of order $m \in \{2, 3\}$, but we give a shorter proof using Corollary 2.

Corollary 4. *Let H be a Hadamard matrix of order n. Then*

$$Z(2, H) = n^2(n-1)(n-2)/8, \quad and \tag{7}$$

$$Z(3, H) = n^2(n-1)(n-2)(n-4)(5n-4)/288. \tag{8}$$

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

Remark 2. We expect random $\{\pm 1\}$-matrices of order 2 to be singular with probability $1/2$, and matrices of order 3 to be singular with probability $5/8$, see [5, 11]. These probabilities agree with the limiting probabilities that we obtain from Corollary 4 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 2 and 3 of Hadamard matrices of order n behave like the minors of random $\{\pm 1\}$ matrices in the limit as $n \to \infty$.

Remark 3. From Szöllősi's theorem [13, Proposition 5.5] or Jacobi's determinant identity [1, 4],

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

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 [6, 7, 8, 12].

4   Generalisation of a result of Turán

The following theorem generalises the result of Turán [15] mentioned in §3.

Theorem 2. *If $B \in \{\pm 1\}^{m \times n}$ is chosen uniformly at random, then*

$$E(\det(BB^T)) = m! \binom{n}{m}.$$

Proof. The proof uses the Cauchy-Binet theorem much as in the proof of Theorem 1. We write

$$\det(BB^T) \;\; = \sum_{M \in S_m(B)} \det(M)^2,$$

where $S_m(B)$ is the set of all $m \times m$ submatrices of B, and take expectations. There are $\binom{n}{m}$ choices of M, and by Turán's theorem each choice contributes $m!$ to the expectation. $\square$

7

Remark 4. Changing notation, de Launey and Levin [8, Proposition 2] says that, if H is a Hadamard matrix of order h, and B is chosen uniformly at random from the $n \times m$ submatrices of H, then

$$E(\det(B^T B)) = h^m \binom{n}{m} \Big/ \binom{h}{m}.$$

The right-hand-side tends to $m!\binom{n}{m}$ as $h \to \infty$. Thus, in this sense, fixed-size submatrices of large Hadamard matrices tend to behave like random matrices.

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] F. R. Gantmacher, *The Theory of Matrices*, Chelsea, 1990.

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

[4] C. G. J. Jacobi, De formatione et proprietatibus determinantium, *Crelle's J.* **22** (1841), 285–318; also *Ges. Werke*, Vol. 3, Reimer, 1884, 356–392.

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

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

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

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

[9] C. H. C. Little and D. J. Thuente, The Hadamard conjecture and circuits of length four in a complete bipartite graph, *J. Austral. Math. Soc. (Series 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. AMS* **14** (1907), 121–123.

[13] F. Szöllősi, Exotic complex Hadamard matrices and their equivalence, *Cryptography and Communications* **2** (2010), 187–198. Also arXiv:1001.3062v2, 9 Feb. 2010.

[14] T. Tao and V. Vu, On random ± 1 matrices: singularity and determinant, *Random Structures and Algorithms* **28** (2006), 1–23. Also arXiv:math/0411095v5, 30 June 2008.

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