Bounds on minors of binary matrices

Judy-anne Osborn
University of Newcastle

14 December 2012

joint work with
Richard P. Brent

I am interested in Hadamard matrices

I am interested in Hadamard matrices

Eg.

$$H_{12} = \begin{pmatrix}
+ & + & + & + & - & - & - & + & + & + & - & - \\
+ & + & + & - & + & - & + & - & + & - & + & - \\
+ & + & + & - & - & + & + & + & - & - & - & + \\
+ & - & - & + & - & - & + & - & - & - & - & - \\
- & + & - & - & + & - & - & + & - & - & - & - \\
- & - & + & - & - & + & - & - & + & - & - & - \\
- & + & + & + & - & - & - & - & - & - & + & + \\
+ & - & + & - & + & - & - & - & - & + & - & + \\
+ & + & - & - & - & + & - & - & - & + & + & - \\
+ & - & - & - & - & - & - & + & + & - & + & + \\
- & + & - & - & - & - & + & - & + & + & - & + \\
- & - & + & - & - & - & + & + & - & + & + & -
\end{pmatrix}$$

I am interested in Hadamard matrices

Eg.

$$H_{12} = \begin{pmatrix} + & + & + & + & - & - & - & + & + & + & - & - \\ + & + & + & - & + & - & + & - & + & - & + & - \\ + & + & + & - & - & + & + & + & - & - & - & + \\ + & - & - & + & - & - & + & - & - & - & - & - \\ - & + & - & - & + & - & - & + & - & - & - & - \\ - & - & + & - & - & + & - & - & + & - & - & - \\ - & + & + & + & - & - & - & - & - & - & + & + \\ + & - & + & - & + & - & - & - & - & + & - & + \\ + & + & - & - & - & + & - & - & - & + & + & - \\ + & - & - & - & - & - & - & + & + & - & + & + \\ - & + & - & - & - & - & + & - & + & + & - & + \\ - & - & + & - & - & - & + & + & - & + & + & - \end{pmatrix}$$

What do we know of the minors of Hadamard matrices?

Outline

- de Launey and Levin, on minors of Hadamard matrices
- Main result: our generalisation
- our (simpler) proof
- Corollary 1
- Corollary 2

de Launey and Levin

Theorem. [de Launey and Levin (2009), Proposition 2]

Let A be a Hadamard matrix of order n. Then for M chosen uniformly at random from square order m submatrices of A,

$$E(\det(M)^2) = \frac{n^m}{\binom{n}{m}}$$

de Launey and Levin

Theorem. [de Launey and Levin (2009), Proposition 2]

Let A be a Hadamard matrix of order n. Then for M chosen uniformly at random from square order m submatrices of A,

$$E(\det(M)^2) = \frac{n^m}{\binom{n}{m}}$$

Questions

1. What about non-Hadamard matrices $A \in \{\pm 1\}^{n \times n}$?

de Launey and Levin

Theorem. [de Launey and Levin (2009), Proposition 2]

Let A be a Hadamard matrix of order n. Then for M chosen uniformly at random from square order m submatrices of A,

$$E(\det(M)^2) = \frac{n^m}{\binom{n}{m}}$$

Questions

1. What about non-Hadamard matrices $A \in \{\pm 1\}^{n \times n}$?
2. de Launey & Levin's proof is hard: is there a simpler proof?

de Launey and Levin

Theorem. [de Launey and Levin (2009), Proposition 2]

Let A be a Hadamard matrix of order n. Then for M chosen uniformly at random from square order m submatrices of A,

$$E(\det(M)^2) = \frac{n^m}{\binom{n}{m}}$$

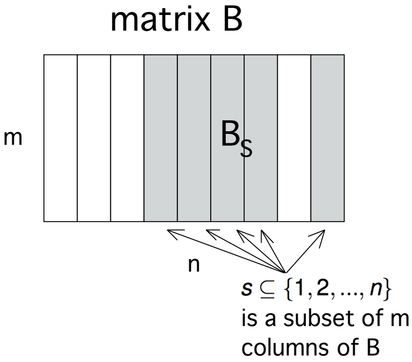
Questions

1. What about non-Hadamard matrices $A \in \{\pm 1\}^{n \times n}$?

2. de Launey & Levin's proof is hard: is there a simpler proof?

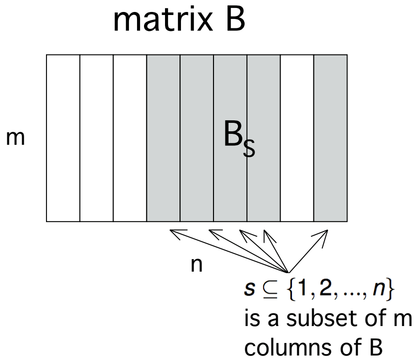
Answers: Yes to both.

We'll find useful: the Cauchy-Binet formula (1812)



$$\det(BB^T) = \sum_{|s|=m} \det(B_s)^2$$

We'll find useful: the Cauchy-Binet formula (1812)



$$\det(BB^T) = \sum_{|s|=m} \det(B_s)^2$$

Proof and history: Muir, 1906; or Brualdi & Schneider, 1983.

Main result

Theorem 1. Let A be a square $\{\pm 1\}$ matrix of order $n \geq m \geq 1$. Then for M be chosen uniformly at random from square order m submatrices of A,

$$E(\det(M)^2) \leq \frac{n^m}{\binom{n}{m}}$$

Main result

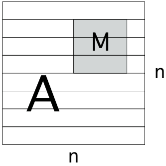
Theorem 1. Let A be a square $\{\pm 1\}$ matrix of order $n \geq m \geq 1$. Then for M be chosen uniformly at random from square order m submatrices of A,

$$E(\det(M)^2) \leq \frac{n^m}{\binom{n}{m}}$$

When $m > 1$, equality holds iff A is a Hadamard matrix.

Proof: Trivial for $m = 1$, so assume $m \geq 2$

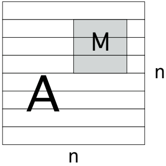
Proof: Trivial for $m = 1$, so assume $m \geq 2$



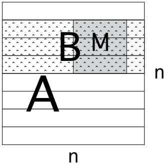
$$E(\det(M)^2) = \frac{\sum_{|\text{rows}|=m} \sum_{|\text{columns}|=m} \det(M)^2}{\binom{n}{m}^2}$$

Proof: Trivial for $m = 1$, so assume $m \geq 2$

$$E(\det(M)^2) = \frac{\sum_{|\text{rows}|=m} \sum_{|\text{columns}|=m} \det(M)^2}{\binom{n}{m}^2}$$



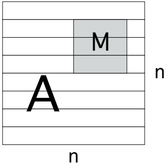
$$= \frac{\sum_{|\text{rows}|=m} \det(BB^T)}{\binom{n}{m}^2} \text{ by Cauchy-Binet}$$



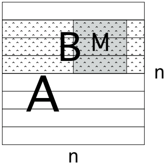
Proof:

Trivial for $m = 1$, so assume $m \geq 2$

$$E(\det(M)^2) = \frac{\sum_{|\text{rows}|=m} \sum_{|\text{columns}|=m} \det(M)^2}{\binom{n}{m}^2}$$



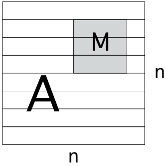
$$= \frac{\sum_{|\text{rows}|=m} \det(BB^T)}{\binom{n}{m}^2}$$ by Cauchy-Binet



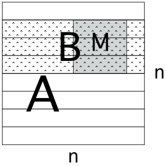
$$\leq \frac{\sum_{|\text{rows}|=m} n^m}{\binom{n}{m}^2}$$ by Hadamard's inequality, with equality iff all rows orthogonal

Proof: Trivial for $m = 1$, so assume $m \geq 2$

$$E(\det(M)^2) = \frac{\sum_{|\text{rows}|=m} \sum_{|\text{columns}|=m} \det(M)^2}{\binom{n}{m}^2}$$



$$= \frac{\sum_{|\text{rows}|=m} \det(BB^T)}{\binom{n}{m}^2} \quad \text{by Cauchy-Binet}$$



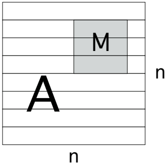
$$\leq \frac{\sum_{|\text{rows}|=m} n^m}{\binom{n}{m}^2}$$

by Hadamard's inequality, with equality iff all rows orthogonal

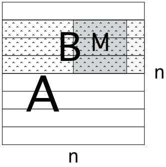
$$= \frac{\binom{n}{m} n^m}{\binom{n}{m}^2}$$

Proof: Trivial for $m = 1$, so assume $m \geq 2$

$$E(\det(M)^2) = \frac{\sum_{|\text{rows}|=m} \sum_{|\text{columns}|=m} \det(M)^2}{\binom{n}{m}^2}$$



$$= \frac{\sum_{|\text{rows}|=m} \det(BB^T)}{\binom{n}{m}^2}$$ by Cauchy-Binet

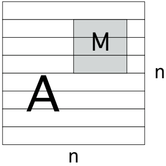


$$\leq \frac{\sum_{|\text{rows}|=m} n^m}{\binom{n}{m}^2}$$ by Hadamard's inequality, with equality iff all rows orthogonal

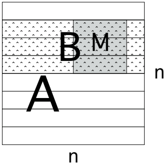
$$= \frac{\binom{n}{m} n^m}{\binom{n}{m}^2} = \frac{n^m}{\binom{n}{m}}$$

Proof: Trivial for $m = 1$, so assume $m \geq 2$

$$E(\det(M)^2) = \frac{\sum_{|\text{rows}|=m} \sum_{|\text{columns}|=m} \det(M)^2}{\binom{n}{m}^2}$$



$$= \frac{\sum_{|\text{rows}|=m} \det(BB^T)}{\binom{n}{m}^2}$$ by Cauchy-Binet



$$\leq \frac{\sum_{|\text{rows}|=m} n^m}{\binom{n}{m}^2}$$ by Hadamard's inequality, with equality iff all rows orthogonal

$$= \frac{\binom{n}{m} n^m}{\binom{n}{m}^2} = \frac{n^m}{\binom{n}{m}}$$

Q.E.D.

Turán and Corollary 1

Theorem (Turán)

Let M be chosen uniformly at random from the set of square $\{\pm 1\}$ matrices of order m. Then

$$E(\det(M)^2) = m!$$

Corollary (1, to our Main Theorem, or de Launey & Levin)

Let H be a Hadamard matrix of order $n \geq m > 1$. Let M be chosen uniformly at random from the set of square order m submatrices of H. Then

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

Proof of Corollary 1

Let H be Hadamard, M be a square submatrix of order $m > 1$ chosen uniformly at random. Then by Theorem 1,

$$E(\det(M)^2) = \frac{n^m}{\binom{n}{m}}$$

Proof of Corollary 1

Let H be Hadamard, M be a square submatrix of order $m > 1$ chosen uniformly at random. Then by Theorem 1,

$$\begin{aligned} E(\det(M)^2) &= \frac{n^m}{\binom{n}{m}} \\ &= \frac{n^m m!}{n(n-1)(n-2)\ldots(n-(m-1))} \end{aligned}$$

Proof of Corollary 1

Let H be Hadamard, M be a square submatrix of order $m > 1$ chosen uniformly at random. Then by Theorem 1,

$$\begin{aligned} E(\det(M)^2) &= \frac{n^m}{\binom{n}{m}} \\ &= \frac{n^m m!}{n(n-1)(n-2)...(n-(m-1))} \\ &> m! \end{aligned}$$

Proof of Corollary 1

Let H be Hadamard, M be a square submatrix of order $m > 1$ chosen uniformly at random. Then by Theorem 1,

$$\begin{aligned} E(\det(M)^2) &= \frac{n^m}{\binom{n}{m}} \\ &= \frac{n^m m!}{n(n-1)(n-2)...(n-(m-1))} \\ &> m! \end{aligned}$$

Q.E.D.

Example:

$$H_{12} = \begin{pmatrix}
+ & + & + & + & - & - & - & + & + & + & - & - \\
+ & + & + & - & + & - & + & - & + & - & + & - \\
+ & + & + & - & - & + & + & + & - & - & - & + \\
+ & - & - & + & - & - & + & - & - & - & - & - \\
- & + & - & - & + & - & - & + & - & - & - & - \\
- & - & + & - & - & + & - & - & + & - & - & - \\
- & + & + & + & - & - & - & - & - & - & + & + \\
+ & - & + & - & + & - & - & - & - & + & - & + \\
+ & + & - & - & - & + & - & - & - & + & + & - \\
+ & - & - & - & - & - & - & + & + & - & + & + \\
- & + & - & - & - & - & + & - & + & + & - & + \\
- & - & + & - & - & - & + & + & - & + & + & -
\end{pmatrix}$$

Let M be a submatrix of order 2 chosen uniformly at random in H_{12}. Then

$$E(\det(M)^2) = 2.181818... > 2$$

Corollary 2

Definition

$Z(m, A) = |$zero minors of order m of $\{\pm 1\}$ matrix $A|$

Corollary 2

Definition

$Z(m, A) = |\text{zero minors of order } m \text{ of } \{\pm 1\} \text{ matrix } A|$

Corollary (2, to our Main Theorem)

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

$$Z(m, A) \geq \binom{n}{m}^2 - 4\binom{n}{m}\left(\frac{n}{4}\right)^m$$

Corollary 2

Definition

$Z(m, A) = |\text{zero minors of order } m \text{ of } \{\pm 1\} \text{ matrix } A|$

Corollary (2, to our Main Theorem)

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

$$Z(m, A) \geq \binom{n}{m}^2 - 4\binom{n}{m}\left(\frac{n}{4}\right)^m$$

When $m \leq 3$, equality occurs iff A is a Hadamard matrix.

Corollary 2

Definition

$Z(m, A) = |\text{zero minors of order } m \text{ of } \{\pm 1\} \text{ matrix } A|$

Corollary (2, to our Main Theorem)

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

$$Z(m, A) \geq \binom{n}{m}^2 - 4\binom{n}{m}\left(\frac{n}{4}\right)^m$$

When $m \leq 3$, equality occurs iff A is a Hadamard matrix.

Proof - see the paper

Corollary 2

Definition

$Z(m, A) = |$zero minors of order m of $\{\pm 1\}$ matrix $A|$

Corollary (2, to our Main Theorem)

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

$$Z(m, A) \geq \binom{n}{m}^2 - 4\binom{n}{m}\left(\frac{n}{4}\right)^m$$

When $m \leq 3$, equality occurs iff A is a Hadamard matrix.

Proof - see the paper

Example: $Z(2, H_{12}) = 1980$, from 4356 submatrices of order 2.

Explicitly for H_{12}

m	$\left\lvert \frac{\text{minor}}{2^{m-1}} \right\rvert^{\text{frequency}}$
1:	1^{144}
2:	0^{1980}, 1^{2376}
3:	0^{24640}, 1^{23760}
4:	0^{109890}, 1^{126720}, 2^{8415}
5:	0^{205920}, 1^{318384}, 2^{95040}, 3^{7920}
6:	0^{150480}, 1^{348480}, 2^{239184}, 3^{76032}, 4^{31680}, 5^{7920}
7:	0^{205920}, 3^{318384}, 6^{95040}, 9^{7920}
8:	0^{109890}, 9^{126720}, 18^{8415}
9:	0^{24640}, 27^{23760}
10:	0^{1980}, 81^{2376}
11:	243^{144}
12:	1458^{1}

$$H_{12} = \begin{pmatrix} + & + & + & + & - & - & - & + & + & + & - & - \\ + & + & + & - & + & - & + & - & + & - & + & - \\ + & + & + & - & - & + & + & + & - & - & - & + \\ + & - & - & + & - & - & + & - & - & - & - & - \\ - & + & - & - & + & - & - & + & - & - & - & - \\ - & - & + & - & - & + & - & - & + & - & - & - \\ - & + & + & + & - & - & - & - & - & - & + & + \\ + & - & + & - & + & - & - & - & - & + & - & + \\ + & + & - & - & - & + & - & - & - & + & + & - \\ + & - & - & - & - & - & - & + & + & - & + & + \\ - & + & - & - & - & - & + & - & + & + & - & + \\ - & - & + & - & - & - & + & + & - & + & + & - \end{pmatrix}$$

NB: North-south symmetry follows from Szöllősi, 2010.

References

R. P. Brent and J. H. Osborn, Bounds on minors of binary matrices, *Bulletin of the Australian Mathematical Society*, to appear. Also arXiv:1208.3330v3, 14 Sept. 2012.

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

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

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.

T. Muir, *A Treatise on the Theory of Determinants*, Dover, NY, 1960.

F. Szöllősi, Exotic complex Hadamard matrices and their equivalence, *Cryptography and Communications* **2** (2010), 187–198.

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