Lower bounds on maximal determinants

Richard P. Brent
ANU

26 September 2012

joint work with

Judy-anne Osborn
University of Newcastle

Presented at the 56th annual meeting of the Australian Mathematical Society, Ballarat

Abstract

We give general lower bounds on the maximal determinant of $n \times n$ $\{+1, -1\}$ matrices, both with and without the assumption of the Hadamard conjecture. Our bounds improve on results of de Launey and Levin (2009), Koukouvinos, Mitrouli and Seberry (2000), and earlier authors. For details see `http://arxiv.org/abs/1208.1805`.

Outline

- Introduction – the *maxdet* function $D(n)$
- Two strategies for obtaining lower bounds on $D(n)$
- Lower bounds assuming the Hadamard conjecture
- Lower bounds not assuming the Hadamard conjecture

Introduction – $D(n)$

Let $D(n)$ denote the maximum determinant attainable by an $n \times n$ $\{\pm 1\}$ matrix.

Hadamard gave the *upper* bound $D(n) \le n^{n/2}$, and a matrix that achieves this bound is called a *Hadamard matrix*.

There are many constructions for Hadamard matrices. If a Hadamard matrix of order n exists, then $n = 1$, 2, or a multiple of 4. The *Hadamard conjecture* is that Hadamard matrices exist for every positive multiple of 4.

In this talk we consider *lower* bounds on $D(n)$.

The bounds are general in the sense that they apply for all sufficiently large positive n. The aim is to obtain a lower bound that is as close as possible to Hadamard's upper bound.

Determinants of $\{-1, 1\}$ matrices

An $n \times n$ $\{\pm 1\}$ matrix always has determinant divisible by 2^{n-1}, because of a well-known mapping from $\{0, 1\}$ matrices of order $n-1$ to $\{\pm 1\}$ matrices of order n.

The mapping is reversible if we are allowed to normalise the first row and column of the $\{\pm 1\}$ matrix by changing the signs of rows/columns as necessary.

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \xrightarrow{\text{double}} \begin{pmatrix} 2 & 0 & 2 \\ 2 & 2 & 0 \\ 0 & 2 & 2 \end{pmatrix}$$

$$\xrightarrow{\text{border}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix} \xrightarrow[\text{first row}]{\text{subtract}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \end{pmatrix}$$

Two strategies for lower bounds

We'll consider two ways that we can obtain a lower bound on $D(n)$ if Hadamard matrices of order "close" to n exist.

- minors: Choose a Hadamard matrix H of order $h \geq n$, and take an $n \times n$ submatrix of H with a large determinant Δ. There are theorems about minors of Hadamard matrices which give a lower bound on Δ.
- bordering: Choose a Hadamard matrix H of order $h \leq n$, and add a suitable border of $n - h$ rows and columns. For example, if $n = 17$, we can construct a maximal determinant matrix of order 17 by choosing a Hadamard matrix of order 16 and an appropriate border.

Some lemmas

Before considering the minors and bordering ideas in detail, it will be useful to state some lemmas.

The minors lemma gives a lower bound that applies if we use the minors strategy;

the bordering lemma gives a lower bound that applies if we use the bordering strategy.

a useful inequality lemma gives a useful inequality!

Minors of Hadamard matrices

Let H be a Hadamard matrix of order h. Thus $|\det(H)| = h^{h/2}$. It is known that the minors of order $h-1$ have values $\pm h^{h/2-1}$ and the minors of order $h-2$ have values $\pm 2h^{h/2-2}$ or zero.

Szöllősi recently generalised this by showing that, for each minor of order d and value Δ, there corresponds a minor of order $h-d$ and value $\pm h^{h/2-d}\Delta$.

This follows easily from Jacobi's determinant identity (though Szöllősi gave a different proof).

Example

For a Hadamard matrix of order $h = 12$, the following values occur as minors of order d:

- $d = 1$: $\{1\}$
- $d = 2$: $\{0, 2\}$
- $d = 3$: $\{0, 4\}$
- $d = 4$: $\{0, 8, 16\}$
- $d = 5$: $\{0, 16, 32, 48\}$
- $d = 6$: $\{0, 32, 64, 96, 128, 160\}$
- $d = 7$: $\{0, 16, 32, 48\} \times 12^1$
- $d = 8$: $\{0, 8, 16\} \times 12^2$
- $d = 9$: $\{0, 4\} \times 12^3$
- $d = 10$: $\{0, 2\} \times 12^4$
- $d = 11$: $\{1\} \times 12^5$

Minors and bordering lemmas

Using Szöllősi's theorem, we have:

Minors lemma. Suppose $0 < n < h$ where h is the order of a Hadamard matrix. Then $D(n) \geq 2^{d-1} h^{h/2-d}$, where $d = h - n$.

The complementary result is:

Bordering lemma. Suppose $0 < h < n$ and h is the order of a Hadamard matrix. Then $D(n) \geq 2^{n-h} h^{h/2}$.

Useful inequality lemma

We know that

$$\lim_{n\to\infty}\left(1-\frac{\alpha}{n}\right)^n = e^{-\alpha}.$$

This asymptotic result can be turned into two inequalities:

Lemma. If $\alpha \in \mathbb{R}$, $n \in \mathbb{N}$, and $n > |\alpha| > 0$, then

$$\left(1-\frac{\alpha}{n}\right)^n < e^{-\alpha} < \left(1-\frac{\alpha}{n}\right)^{n-\alpha}.$$

Bounds assuming the Hadamard conjecture

For the time being we assume the Hadamard conjecture. Thus, given $n > 0$, there exists a Hadamard matrix of order h with $|n - h| \le 2$. This is certainly true for $n \le 664$.

Later we'll see that the same ideas can be applied without assuming the Hadamard conjecture, but using knowledge of some constructions for Hadamard matrices, e.g. the Paley and Sylvester constructions.

There are four cases, depending on n mod 4. The case $n \equiv 0 \pmod 4$ is easy, since (by our assumption) there exists a Hadamard matrix of order n, and

$$D(n) = n^{n/2}.$$

Now consider the remaining three cases.

The other three cases

We <u>underline</u> the better bounds.

- $n \equiv 1 \pmod 4$: Hadamard matrices of order $n-1$, $n+3$ exist. Thus, using the bordering and minors lemmas,

$$D(n) \ge \max(\underline{2(n-1)^{(n-1)/2}}, 4(n+3)^{(n-3)/2}).$$

- $n \equiv 2 \pmod 4$: Hadamard matrices of order $n-2$, $n+2$ exist. Thus

$$D(n) \ge \max(4(n-2)^{(n-2)/2}, \underline{2(n+2)^{(n-2)/2}}).$$

- $n \equiv 3 \pmod 4$: Hadamard matrices of order $n-3$, $n+1$ exist. Thus

$$D(n) \ge \max(8(n-3)^{(n-3)/2}, \underline{(n+1)^{(n-1)/2}}).$$

Overall result

Combining the results for the four equivalence classes (mod 4), we get:

Theorem. Assume the Hadamard conjecture. For $n \geq 4$,

$$D(n) \geq 2(n+2)^{n/2-1} \sim 2en^{n/2-1}.$$

Corollary. Assume the Hadamard conjecture. For $n \geq 4$,

$$1 \geq \frac{D(n)}{n^{n/2}} \geq \frac{4}{n}\,.$$

Previous results

Previous authors such as Koukouvinos, Mitrouli and Seberry (2001), de Launey and Levin (2009) essentially used only the minors lemma, so obtained

$$1 \geq \frac{D(n)}{n^{n/2}} \geq \frac{c}{n^{3/2}},$$

for some $c > 0$.

Our improvement is due to using the bordering lemma in the case $n \equiv 1 \bmod 4$.

Sharper results

We can improve on the results given above in the cases $n \equiv 1 \text{ or } 2 \pmod 4$.

The *excess* of a $\{\pm 1\}$ matrix $H = (h_{i,j})$ is $\sigma(H) := \sum_{i,j} h_{i,j}$. We define

$$\sigma(n) := \max \sigma(H),$$

where the maximum is taken over all Hadamard matrices of order n.

Then, for $h \geq 4$ the order of a Hadamard matrix,

$$\sqrt{2/\pi} \leq \sigma(h)/h^{3/2} \leq 1$$

by results of Best (1977) and Enomoto and Miyamoto (1980).

Also, by a result of Schmidt and Wang (1977),

$$D(h+1) \geq h^{h/2}(1 + \sigma(h)/h).$$

The case $n \equiv 1 \pmod 4$

Combining the inequalities on the previous slide gives

$$D(h+1) \geq h^{h/2}(1 + \sqrt{2h/\pi}).$$

Taking $n = h+1$, so this is the case $n \equiv 1 \pmod 4$, we deduce

$$D(n) \geq \left(\frac{2}{\pi e}\right)^{1/2} n^{n/2}.$$

The lower bound is within a constant factor 0.48 of the Hadamard upper bound, and within a constant factor $\pi^{-1/2} \approx 0.56$ of the Barba upper bound.

Improved overall result

Using the improved result for the case $n \equiv 1 \pmod 4$, and a (related) improved result for $n \equiv 2 \pmod 4$, we get:

Corollary Assume the Hadamard conjecture. If $n \geq 1$ then

$$1 \geq \frac{D(n)}{n^{n/2}} \geq \frac{1}{\sqrt{3n}}\,.$$

This improves the previous lower bound $4/n$ if $n > 48$.

Unconditional bounds

Now we drop the assumption of the Hadamard conjecture. Let

$$\mathcal{H} = \{h \in \mathbb{N} \mid h \text{ is the order of a Hadamard matrix}\},$$

and

$$\delta(n) := \min_{h \in \mathcal{H}} |n - h|.$$

The Hadamard conjecture is equivalent to the statement that $\delta(n) \leq 2$ for all $n \in \mathbb{N}$.

The unconditional bound in terms of $\delta(n)$

Theorem. Let $n \in \mathbb{N}$ and $\delta = \delta(n) = \min_{h \in \mathcal{H}} |n - h|$. Then

$$\frac{D(n)}{n^{n/2}} \ge \left(\frac{4}{ne}\right)^{\delta/2}.$$

Remark. de Launey and Levin (2009) essentially showed that $D(n)/n^{n/2} \ge (1/n)^{\delta}$, so we have halved the exponent.
As before, this is because we use the bordering lemma if it gives a sharper result than the minors lemma.

Sketch of proof

Let h be such that $|n-h| = \delta$, so $h = n \pm \delta$.
If $\delta = 0$ then $D(n) = n^{n/2}$, so suppose $\delta \geq 1$.
We consider two cases, depending on the sign of $n-h$.

If $h < n$ we use the bordering lemma, which gives

$$D(n) \geq 2^{\delta} h^{h/2}.$$

If $h > n$ we use the minors lemma, which implies that

$$D(n) \geq h^{h/2-\delta}.$$

Taking $\alpha = n - h$ in the useful inequality lemma gives the inequality that we need in both cases. For details see arXiv 1208.1805v2. □

Bounding $\delta(n)$ via prime gaps

If p is an odd prime, then $h = 2(p+1)$ is the order of a Hadamard matrix.

- If $p \equiv 1 \bmod 4$ this follows from the second Paley construction.
- If $p \equiv 3 \bmod 4$ then the first Paley construction gives a Hadamard matrix of order $p+1$, so applying the Sylvester "doubling" construction to this gives a Hadamard matrix of order $2(p+1)$.

Thus

$$\delta(n) \le \lambda(n/2 - 1),$$

where $\lambda : \mathbb{R} \to \mathbb{Z}$ is the *prime gap* function

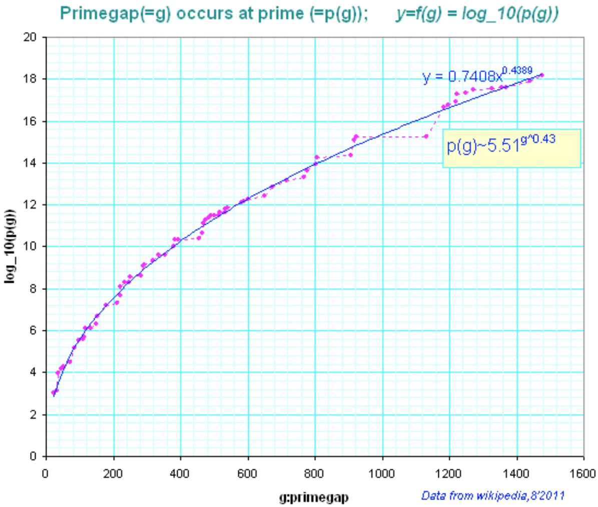
$$\lambda(x) := \max\{p_{i+1} - p_i \mid p_i \le x\} \cup \{0\}.$$

What is known about the prime gap function $\lambda(n)$?

Let's use Vinogradov's notation $f(n) \ll g(n)$ as a synonym for $f(n) = O(g(n))$. You can guess what $f(n) \gg g(n)$ means!

- Hoheisel (1930) showed that $\lambda(n) \ll n^c$ for some $c < 1$. His result had $c = 1 - 1/33000$.
- Many papers improved Hoheisel's result by reducing the constant c from $1 - \varepsilon$ almost to $1/2 + \varepsilon$.
- The best result so far is that of Baker, Harman and Pintz (2001), who showed that $\lambda(n) \ll n^{21/40}$.
- Assuming the Riemann hypothesis, Cramér (1936) showed that $\lambda(n) \ll n^{1/2} \log n$.
- *Cramér's conjecture* [Cramér/Shanks] is $\lambda(n) \ll (\log n)^2$. The implied constant might be $2e^{-\gamma}$ [Granville].
- The *average* gap between primes $p \le n$ is asymptotic to $\log n$, so $\lambda(n) \gg \log n$.

Evidence for Cramér's conjecture



Data from wikipedia,8'2011

Conclusion

Combining our theorem that gives a bound on $D(n)$ in terms of $\delta(n)$ with the theorem of Baker, Harman and Pintz, we obtain:

$$n^{n/2} \geq D(n) \geq n^{n/2 - O(n^{21/40})}.$$

Corollary.

$$0 \leq n \log n - 2 \log D(n) \ll n^{21/40} \log n.$$

Remark. This improves on Clements and Lindström (1965), who showed that

$$0 \leq n \log n - 2 \log D(n) \ll n.$$

Further improvements

Craigen and Livinskyi (following pioneering work by Seberry) show that, for any odd integer q, a Hadamard matrix of order $2^t q$ exists for all

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

for certain constants α, β.

Using such results, we can reduce the exponent $21/40$ coming from the Harman-Baker-Pintz theorem to $\alpha/(1+\alpha)$.

Craigen [unpublished] obtained $\alpha < 1/2$.

Livinskyi claims a result with $\alpha \leq 1/5$. The proof depends on properties of complex Golay sequences.
This gives an exponent $\alpha/(1+\alpha) \leq 1/6$, i.e.

$$0 \leq n \log n - 2 \log D(n) \ll n^{1/6}.$$

References

R. C. Baker, G. Harman and J. Pintz, The difference between consecutive primes, II, *Proc. LMS* **83** (2001), 532–562.

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

M. R. Best, The excess of a Hadamard matrix, *Indag. Math.* **39** (1977), 357–361.

R. P. Brent and J. H. Osborn, General lower bounds on maximal determinants of binary matrices, arXiv:1208.1805v2

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

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

References cont

H. Ehlich, Determinantenabschätzungen für binäre Matrizen, *Math. Z.* **83** (1964), 123–132; *ibid* **84** (1964), 438–447.

H. Enomoto and M. Miyamoto, On maximal weights of Hadamard matrices, *J. Combin. Theory* A **29** (1980), 94–100.

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

G. Hoheisel, Primzahlprobleme in der Analysis, *Sitz. Preuss. Akad. Wiss.* **2** (1930), 1–13.

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.

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

References cont

I. Livinskyi, *Asymptotic existence of Hadamard matrices*, M.Sc. thesis, University of Manitoba, 2012.

R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys* **12** (1933), 311–320.

K. W. Schmidt and E. T. H. Wang, The weights of Hadamard matrices, *J. Combin. Theory* A **23** (1977), 257–263.

D. Shanks, On maximal gaps between successive primes, *Mathematics of Computation* **18** (1964), 646–651.

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

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