The Hadamard maximal determinant problem

Padraig Ó Catháin

Dublin City University

44th Australasian Combinatorics Conference,
Otago, New Zealand
14/15 December 2022

Positive Definite Matrices

Proposition

The following are equivalent for an invertible $n \times n$ matrix G.

- *$G = M^*M$ for invertible matrix M.*
- *There exist lin. ind. vectors $m_1, \ldots, m_n$ in the inner product space $\mathbb{C}^n$ such that $G_{i,j} = \langle m_i, m_j \rangle$.*
- *G is (Hermitian) positive definite.*

- We always use the standard inner product in this talk.
- The geometric interpretation allows us to e.g. invoke the Cauchy-Schwarz Inequality for linearly independent vectors:

$$\langle m_i, m_j \rangle^2 < \langle m_i, m_i \rangle \langle m_j, m_j \rangle \rightarrow g_{i,i}g_{j,j} - g_{i,j}g_{j,i} > 0\,.$$

So all principal 2×2 minors of a positive definite matrix are positive.

Sylvester's Criterion

Theorem

A matrix G is Hermitian positive definite if and only if all leading minors are positive.

- Since positive definiteness is a property invariant under simultaneous permutation of rows/columns, all principal minors are positive.
- This is a higher-dimensional analogue of Cauchy-Schwarz.

Corollary

Suppose that G_k is (Hermitian) positive definite. Then

$$\det(G_k) \leqslant g_{k,k} \det(G_{k-1}) .$$

where G_{k-1} is the leading minor of size $k-1$.

$$\det \begin{pmatrix} g_{1,1} & \cdots & g_{1,k-1} & g_{1,k} \\ g_{2,1} & \cdots & g_{2,k-1} & g_{2,k} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k-1,1} & \cdots & g_{k-1,k-1} & g_{k-1,k} \\ g_{k,1} & \cdots & g_{k,k-1} & g_{k,k} \end{pmatrix} = \det \begin{pmatrix} g_{1,1} & \cdots & g_{1,k-1} & g_{1,k} \\ g_{2,1} & \cdots & g_{2,k-1} & g_{2,k} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k-1,1} & \cdots & g_{k-1,k-1} & g_{k-1,k} \\ 0 & \cdots & 0 & g_{k,k} \end{pmatrix} + \det \begin{pmatrix} g_{1,1} & \cdots & g_{1,k-1} & g_{1,k} \\ g_{2,1} & \cdots & g_{2,k-1} & g_{2,k} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k-1,1} & \cdots & g_{k-1,k-1} & g_{k-1,k} \\ g_{k,1} & \cdots & g_{k,k-1} & 0 \end{pmatrix} \tag{1}$$

The first term has determinant $g_{k,k} \det(G_{k-1})$. The second term has a 2×2 minor

$$\det \begin{pmatrix} g_{k-1,k-1} & g_{k-1,k} \\ g_{k,k-1} & 0 \end{pmatrix} = -g_{k-1,k} g_{k-1,k}^* < 0 .$$

Fischer's Inequality

Theorem

For an $n \times n$ Hermitian positive definite matrix $G = \begin{pmatrix} A & B \\ B^* & D \end{pmatrix}$ the inequality $\det(G) \leqslant \det(A)\det(D)$ holds.

- Suppose that A is $k \times k$, and define the k^{th} adjugate of M to be the $\binom{n}{k} \times \binom{n}{k}$ matrix which has as entries the minors of order k.

$$G^{(k)} = \begin{pmatrix} F & f \\ f^* & \det(A) \end{pmatrix}.$$

- Omitting some 'well-known' facts about compound matrices, $\det(F) = \det(G)^{\binom{n-1}{k-1}-1}\det(D)$ and $\det(G^{(k)}) = \det(G)^{\binom{n-1}{k-1}}$,

$$\det(G^{(k)}) = \det(G)^{\binom{n-1}{k-1}} \leqslant \det(G)^{\binom{n-1}{k-1}-1}\det(D)\det(A).$$

- Cancel common factors.

Hadamard's inequality

Theorem

For an $n \times n$ positive definite matrix G the inequality $\det(G) \leqslant \prod_{i=1}^{n} g_{i,i}$ holds.

- Partition G into complementary principal minors, apply Fischer's Inequality and continue recursively.
- If the entries of $n \times n$ matrix M are bounded by 1, then $\langle m_i, m_i \rangle \leqslant n$ for $1 \leqslant i \leqslant n$. So all diagonal entries of Hermitian positive definite $G = M^* M$ are bounded by n.
- $\det(G) = \det(M)^* \det(M) \leqslant n^n$. So

$$\|\det(M)\| \leqslant n^{n/2}.$$

- This is Hadamard's inequality.

Hadamard's maximal determinant problem

- It is not hard to check that Hadamard's bound is attained if and only if there exist n mutually orthogonal vectors with entries of norm 1 in dimension n.
- In the real field, entries are in $\{\pm 1\}$ and the dimension is $1, 2$ or $4k$ for $k \in \mathbb{N}$.
- Over a field containing k^{th} roots of unity, character tables of abelian groups of exponent k give solutions to the maximal determinant problem. **But there are others.**
- For a set of entries $E \subset \mathbb{C}$ of norm $\leqslant 1$, write $d_{n,E}$ for the maximal determinant of an $n \times n$ matrix with entries in E.
- **Question (Hadamard conjectures):** When is $|d_{n,E}| = n^{n/2}$?
- **Question (Hadamard bounds):** Do there exist polynomial functions $c(n), C(n)$ depending on E such that

$$\frac{1}{c(n)} n^n \leqslant |d_{n,E}| \leqslant \frac{1}{C(n)} n^n?$$

Paley Construction

- Let $\mathbb{F}_q$ be a finite field, with $q \equiv 3 \mod 4$ and let χ be the quadratic character, set $\chi(0) = 0$.
- Define the *Paley core* matrix

$$Q = (\chi(x-y))_{0 \leqslant x,y \leqslant p-1}.$$

- Let r_a be the row labelled by a. Then

$$\begin{aligned}\langle r_a, r_b \rangle &= \sum_{x \neq a,b} \chi(a-x)\chi(b-x) = \sum_{y \neq a-b,0} \chi(y)\chi(b-a+y) \\ &= \sum_{y \neq a-b,0} \chi(y)\chi(y)\chi\left(\frac{b-a}{y}+1\right) = \sum_{y \neq a-b,0} \chi\left(\frac{b-a}{y}+1\right) \\ &= -\chi(1).\end{aligned}$$

- Since Q is skew, $(Q+I)(Q+I)^\top = QQ^\top + I = (p+1)I - J$. Adding a column of -1's gives orthogonal rows, and a row of 1's completes the Paley Hadamard matrix of order $q+1$.

- Paley: There exists a Hadamard matrix of order $q+1$ where $q \equiv 3 \mod 4$ is a prime power.
- Paley II: There exists a Hadamard matrix of order $2(q+1)$ where $q \equiv 1 \mod 4$ is a prime power.
- Menon Diference sets: There exists a Hadamard matrix of order $4q^4$ for any prime power q.
- Kronecker products and computational results cover all orders up to $668 = 4 \cdot 191$.
- Seberry-Craigen: For any odd n there exists a Hadamard matrix of order $2^{c(n)}n$ where $c(n) \sim c_1 + c_2 \log(n)$.

Asymptotic Existence of real matrices

Theorem (Craigen-Livinskyi, 2012)

For any odd integer n there exists $t = \lceil \alpha \log_2(n) + \beta \rceil$ such that there exists a (real) Hadamard matrix of order $2^t n$. One can take $\alpha = 1/5$ and $\beta = 13$.

Corollary (Craigen-Livinskyi)

The gap between orders of Hadamard matrices of size n is bounded by $O(n^{1/6})$.

- Proof is via signed group weighing matrices and zero-correlation sequences.
- Corollary comes from estimating the difference between the orders of matrices constructed for n and $n+2$.
- Independent of existence of primes close to n.

Proposition

Suppose that $n \equiv 2 \mod 4$ *and that* $E = \{\pm 1\}$. *Then* $d_{n,E} \leqslant \sqrt{2n-2}(n-2)^{n-2/2}$.

- When $n \equiv 2 \mod 4$ there do not exist three mutually orthogonal $\{\pm 1\}$-vectors. Non-zero inner products can be chosen to be congruent to $n \mod 4$.
- The graph in which vertices are connected if rows are orthogonal is triangle free. By Turán's theorem, the densest triangle free graphs are complete bipartite.
- The largest determinant of a Gram matrix satisfying these conditions is

$$\begin{pmatrix} (n-2)I + 2J & 0 \\ 0 & (n-2)I + 2J \end{pmatrix}.$$

- Bound attained if there exist circulant A, B satisfying $AA^\top + BB^\top = (n-2)I + 2J$.

Upper bounds, real case

- If $n \equiv 0 \mod 4$ then it is conjectured that the $d_n = n^{n/2}$.
- If $n \equiv 1 \mod 4$ then the optimal Gram matrix is $(n-1)I_n + J_n$ with determinant $\sqrt{2n-1}(n-1)^{n-1/2} \sim 0.8578n^{n/2}$. This bound is attained only if $2n-1$ is a square. The bound is attained when $n = (q+1)^2 + q^2$ for odd prime power q (Brouwer).
- If $n \equiv 2 \mod 4$ then the optimal Gram matrix is $\left((n-2)I_{n/2} + 2J_{n/2}\right) \otimes I_2$ with determinant $(2n-2)(n-2)^{n-2/2}n \sim 0.7358n^{n/2}$. This bound is attained only if $2n-2$ is a sum of two squares. The bound is attained when $n = 4q^2 + 4q + 2$ (Brouwer) or $n = 2q^2 + 2q + 2$ (Spence).
- If $n \equiv 3 \mod 4$ the optimal Gram matrices are not known, but the determinant is bounded above by $0.6545n^{n/2}$. The bound is not known to ever be sharp. An infinite family attaining ~ 0.48 of the bound exists when $n = 2q^2 + 2q + 3$ for odd prime power q.
- Survey: Browne, Egan Hegarty & Ó C. *The Hadamard Maximal Determinant Problem*, EJC, 2021

Upper bounds, real case, overview

	0	1	2	3
Upper Bound $\times n^{n/2}$	1	0.857	0.735	0.654
Best Family	1	0.857	0.735	**0.314**
Gap size	$O(n^{1/6})$	$O(n^{1/2+\epsilon})$	$O(n^{1/2+\epsilon})$	-

- Gap size is an upper bound on the distance between matrices achieving the bound, where n is the matrix size.
- The constant ϵ measures the distance between primes of size $O(\sqrt{n})$. Unconditionally, this can be taken as $\frac{1}{80}$. Conditional on plausible conjectures in number theory, $\epsilon = 0$ is permitted.

Corollary

For every congruence class $\mod 4$*, the Hadamard bound is tight (infinitely often) up to a constant factor* $C \geqslant 0.314$*.*

Lower bounds, real case

Theorem (Cohn, 1967)

There exists a ± 1 *matrix with determinant* $|d_n| \geqslant n^{n/2} e^{-0.62n}$.

- Write d_n for the largest determinant of a $\{\pm 1\}$ matrix, and set $|d_n| = n^{n/2} e^{-\phi(n)}$.
- Let p be the largest prime such that $2p + 2 < n$, and let $f(n)$ be a function satisfying

$$(2p+2)\log(2p+2) \geqslant (n - f(n))\log(n)\,.$$

- Compare $n^{n/2}$ to $\begin{pmatrix} H_{2p+2} & 0 \\ 0 & I_{n-2p-2} \end{pmatrix}$.
- Bounded by gaps between primes. Cohn used $p_{n+1} - p_n = O(n^{61/98})$.
- Cramér's conjecture, that $p_{n+1} - p_n \leqslant O(\log^2(n))$ would (only) give $e^{-\log^3(n)}$ in the result.

Lower bounds from the probabilistic method

- Let M be a matrix with entries in $\{\pm 1\}$ chosen uniformly at random. Recall the Laplace expansion of the determinant: $\sum_{\sigma \in S_n} \chi(\sigma) \prod M_{i,i^\sigma}$ where χ is the alternating character.
- Estimate $\det(MM^\top)$. By linearity of expectation, $\chi(\sigma)\chi(\tau) \prod M_{i,i^\sigma} \prod M_{i,i^\tau} = 0$ unless $\sigma = \tau$, in which case it is 1.
- Turán: The expected value of $\det(MM^\top) = n!$.
- By Stirling's approximation, $\log(n!) \sim n \log n - n - \Theta(\log n)$ while $\log(n^n) = n \log n$. So a random determinant is (only) a factor e^{-n} smaller than the Hadamard bound.
- This beats Cohn: $|d_n| \geqslant n^{n/2} e^{-0.5n}$ vs $|d_n| \geqslant n^{n/2} e^{-0.62n}$.

Lower bounds from neighbouring Hadamard matrices

Proposition

Let H be a Hadamard matrix of order $n-1$. Then $\det(M) = \det(H)(1 + n^{-1}\sum_{i,j} h_{ij})$, *where*

$$M = \begin{pmatrix} H & \mathbf{1} \\ -\mathbf{1}^\top & 1 \end{pmatrix}.$$

- Schur complement: For any block matrix in which A is invertible,

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

- Apply this result to M, observing that $\mathbf{1}^\top H \mathbf{1} = \sum_{i,j} h_{ij}$. The maximal *excess* of a Hadamard matrix of order n is $n\sqrt{n}$ with equality when all row-sums are equal.
- $1/\sqrt{2}$ of the Barba bound, or 0.61 of the Hadamard bound.

Lower bounds from neighbouring Hadamard matrices

Theorem (Brent-Osborn-Smith)

Let H be a Hadamard matrix of order $n-d$. Then $M = \begin{pmatrix} H & R \\ D & S \end{pmatrix}$ *satisfies* $\det(M) \geqslant n^{n/2} \left(\frac{2}{\pi e}\right)^{d/2} \left(1 - d^2\sqrt{\pi(2n-2d)^{-1}}\right)$.

- R is Random, D is deterministic, S is Small (and replaced by I_d for computations).
- $\det(M) = \det(H)\det(S - DH^{-1}R) \sim \det(H)\det(I_d - n^{-1}DH^{\top}R)$.
- Entries of D chosen to maximise $\sum_j d_{ij}x_{ji}$, where $H^{\top}R = [x_{ij}]_{i,j}$.
- Via the probabilistic method, $DH^{\top}R$ has all eigenvalues of magnitude $\sqrt{n-d}$ with high probability, and the result follows by carefully bounding probabilities of tail events.
- If the Hadamard conjecture holds, then the maximal determinant at order n is at least $0.11n^{n/2}$ for all n.

Lower bounds, real case, overview

- Cohn's bound: $d_n \geqslant e^{-0.62n} n^{n/2}$ for all n.
- Brent-Osborn-Smith: $d_{h+t} \geqslant \frac{1}{2}(0.234)^t n^{n/2}$ when $t < h^{1/4}$.
- Conditional on the Hadamard conjecture, lower bound of $0.11 n^{n/2}$.
- Upper bounds are within a constant of best possible. Lower bounds are (conjecturally) **exponentially** bad.
- With the strongest possible number theoretic conjectures, lower bounds are still (conjecturally) **super-polynomially** bad.

Further matrices: Momihara, Suda, Xiang

- 9 new families of matrices at orders $n \equiv 2 \mod 4$ using cyclotomic methods
- Bordered multi-circulant matrices
- Explicit family at orders $2q^2$ for which ratio of the determinant with the bound tends to 1.
- 3 explicit families at order $q+1$ where $q \equiv 1 \mod 4$ with determinants around 0.8 of the bound.
- 'Explicit' evaluations of the determinants in terms Gauss and Jacobi sums.

Complex Hadamard matrices

- Hadamard conjecture and Hadamard maximal determinant problem are well posed for any bounded subset $E \subseteq \mathbb{C}$.
- Nonexistence: if $MM^* = nI_n$ and n is odd, then $n = ss^*$ for some $s \in \mathbb{Z}[\omega_6]$. Odd primes which are $2 \mod 3$ do **not** split, so cannot divide the square-free part of n. The maximal determinant is not attained at orders $5, 11, 15, 17, 23, \ldots$.
- Exist at Hadamard orders, and orders $2^a 3^b$.

Complex Hadamard matrices, existence

Proposition (Szollosi-Craigen)

There exists a maximal determinant matrix of order n^2 with entries in $\langle \omega_6 \rangle$.

- The Paley core satisfies $PP^\top = pI - J$ and $PJ = 0$. Define:

$$H = P \otimes P + J \otimes I + \omega^2 I \otimes J\,.$$

- Then

$$\begin{aligned} HH^\top &= (pI - J) \otimes (pI - J) + J^2 \otimes I + I \otimes J^2 + (\omega + \omega^2) J \otimes J \\ &= (pI - J) \otimes (pI - J) + p\,(I \otimes J + J \otimes I) - J \otimes J \\ &= p^2 I \otimes I\,. \end{aligned}$$

- Taking Kronecker products completes the proof.
- Real Hadamard matrices of order $4p^2$ are known for most, but not all, classes of primes $\mod 16$. But the proofs are much harder.

Questions

- Do the probabilistic methods of Brent-Osborn-Smith generalise to:
  - Maximal determinant matrices rather than Hadamard matrices?
  - Complex Hadamard matrices, say over k^{th} roots?
- Can the asymptotic existence methods of Seberry, Craigen and collaborators (orthogonal designs, signed groups) be generalised to give existence results for complex max. det. matrices with better constants than occur in the real case?
- What is the expected absolute value of the determinant of a group invariant matrix? For cyclic groups, it seems appreciably larger than for an unstructured matrix.
- **Question:** Do there exist families of near-optimal matrices (in the sense of Momihara-Suda-Xiang) at odd orders?

Go raibh maith agaibh!