Hadamard's Maximum Determinant Problem

In 1893, Hadamard considered the following question:

Let A be an $n \times n$ matrix with entries of absolute value at most $M > 0$. How large can the absolute value of the determinant of A be?

Somewhat surprisingly, the problem is easier in the case when the entries of A are complex numbers. Hadamard finds the complete solution in the complex case and leaves a conjecture that has become famous in the real case.

Denote by $\|\mathbf{z}\|$ the Euclidian norm of a vector $\mathbf{z} = (\alpha_1, \alpha_2, ..., \alpha_n) \in \mathbf{C}^n$, that is

$$\|\mathbf{z}\|^2 = |\alpha_1|^2 + |\alpha_2|^2 + ... + |\alpha_n|^2.$$

Theorem 1.1. *(Hadamard, 1893) Let A be an $n \times n$ complex matrix with linearly independent columns $\mathbf{z}_1, \mathbf{z}_2, ..., \mathbf{z}_n$. Then*

$$|det(A)|^2 = |det(\overline{A}^t A)| \leq \prod_{k=1}^{n} \|\mathbf{z}_k\|^2,$$

with equality iff $\overline{A}^t A$ is a diagonal matrix(columns are orthogonal).

Proof

Using the Gram-Schmidt process, construct inductively mutually orthogonal vectors $\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_n$ such that $\mathbf{y}_k$ is a linear combination of $\mathbf{z}_1, \mathbf{z}_2, ..., \mathbf{z}_k$ in which the coefficient of $\mathbf{z}_k$ is 1. Define:

$$\mathbf{y}_k = \mathbf{z}_k - \sum_{i=1}^{k-1} \alpha_{ki}\mathbf{y}_i, \text{ where } \alpha_{ki} = \frac{\langle \mathbf{z}_k | \mathbf{y}_i \rangle}{\langle \mathbf{y}_i | \mathbf{y}_i \rangle}.$$

a) $\mathbf{y}_k \neq 0$ since $\mathbf{z}_1, \mathbf{z}_2, ..., \mathbf{z}_k$ are linearly independent.

b) $\langle \mathbf{y}_k | \mathbf{y}_i \rangle = \langle \mathbf{z}_k | \mathbf{y}_i \rangle - \alpha_{k1} \langle \mathbf{y}_1 | \mathbf{y}_i \rangle - ... - \alpha_{ki} \langle \mathbf{y}_i | \mathbf{y}_i \rangle = \langle \mathbf{z}_k | \mathbf{y}_i \rangle - \frac{\langle \mathbf{z}_k | \mathbf{y}_i \rangle}{\langle \mathbf{y}_i | \mathbf{y}_i \rangle} \langle \mathbf{y}_i | \mathbf{y}_i \rangle = 0.$

Denote by B the matrix with columns $\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_n$. Because $\mathbf{y}_k$'s are mutually orthogonal, $\overline{B}^t B = diag(\|\mathbf{y}_1\|^2, \|\mathbf{y}_2\|^2, ..., \|\mathbf{y}_n\|^2)$

Because $\mathbf{z}_k = \mathbf{y}_k + \sum_{i=1}^{k-1} \alpha_{ki}\mathbf{y}_i$, matrices B and A are related via a transition matrix T, which is upper triangular and has 1's on the diagonal.

$$B = TA, \text{ where } T = \begin{pmatrix} 1 & \alpha_{12} & ... & \alpha_{1n} \\ 0 & 1 & ... & \alpha_{2n} \\ . & . & ... & . \\ 0 & 0 & ... & 1 \end{pmatrix}$$

Thus, we have

$$det(B) = det(TA) = det(T)det(A) = det(A), \text{ so } |det(B)|^2 = |det(A)|^2.$$

$$\text{But} \quad |det(B)|^2 = det(\overline{B}^t B) = \prod_{k=1}^{n} \|\mathbf{y}_k\|^2.$$

Since $\mathbf{z}_k = \mathbf{y}_k + \sum_{i=1}^{k-1} \alpha_{ki}\mathbf{y}_i$, using the orthogonality of $\mathbf{y}_k$'s, we have

$$\langle \mathbf{z}_k|\mathbf{z}_k\rangle = \|\mathbf{z}_k\|^2 = \langle \mathbf{y}_k|\mathbf{y}_k\rangle + \sum_{i=1}^{k-1} |\alpha_{ki}|^2 \langle \mathbf{y}_i|\mathbf{y}_i\rangle = \|\mathbf{y}_k\|^2 + \sum_{i=1}^{k-1} |\alpha_{ki}|^2 \|\mathbf{y}_i\|^2.$$

In conclusion: $\|\mathbf{y}_k\|^2 \leq \|\mathbf{z}_k\|^2$ with equality if and only if $\mathbf{y}_k = \mathbf{z}_k$.
Thus

$$|det(A)|^2 = |det(B)|^2 = \prod_{k=1}^{n} \|\mathbf{y}_k\|^2 \leq \prod_{k=1}^{n} \|\mathbf{z}_k\|^2,$$

with equality if and only if $\mathbf{y}_k = \mathbf{z}_k$ for all k, i.e the matrix A had orthogonal columns to start with, i.e. $\overline{A}^t A$ is a diagonal matrix. □

The next Corollaries give upper estimates for the maximum determinant problem.

Corollary 1.2

Let $A = (z_{ij})$ be an $n \times n$ complex matrix with $|z_{ij}| \leq 1$, then $|det(A)| \leq n^{\frac{n}{2}}$ with equality iff $|z_{ij}| = 1$ for all $1 \leq i, j \leq n$ and $\overline{A}^t A = nI_n$.

Proof

Let $\mathbf{z}_k$ be the k-column of A. Assume that the columns of A are linearly independent, as otherwise $det(\overline{A}^t A) = 0$ and the inequality is obvious. Since the absolute value of every column element is at most 1, then: $\|\mathbf{z}_k\|^2 = |z_{1k}|^2 + \ldots + |z_{nk}|^2 \leq n$.

Thus

$$|det(A)|^2 \leq \prod_{k=1}^{n} \|\mathbf{z}_k\|^2 \leq n^n.$$

Equality holds if only if $|z_{ij}| = 1$ and $\overline{A}^t A = nI_n$. □

Corollary 1.3

Let $A = (z_{ij})$ be an $n \times n$ complex matrix with $|z_{ij}| \leq M$, then $|det(A)| \leq M^n n^{\frac{n}{2}}$ with equality iff $|z_{ij}| = M$ for all $1 \leq i, j \leq n$ and $\overline{A}^t A = M^2 n I_n$.

Proof - Exercise 1

Now the natural question is whether the upper bound given by these estimates can be always achieved. Hadamard shows that the answer is affirmative in the complex case.

Definition 1.1. A **complex** $n \times n$ matrix $A = (z_{ij})$ is said to be a Hadamard matrix of order n if $|z_{ij}| = 1$ and $\overline{A}^t A = nI_n$.

Theorem 1.4 (Hadamard) *For any natural number n, there exists a complex Hadamard matrix A of order n.*

Proof - Exercise 2

$$\text{Let} \quad A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \xi_1 & \dots & \xi_{n-1} \\ 1 & \xi_1^2 & \dots & \xi_{n-1}^2 \\ . & . & \dots & \dots \\ 1 & \xi_1^{n-1} & \dots & \xi_{n-1}^{n-1} \end{pmatrix},$$

where $\xi_k = e^{\frac{i(2k\pi)}{n}}$, $\quad 0 \leq k \leq n-1$ are the complex n^{th} roots of unity. Show that this choice of A satisfies, indeed, $\overline{A}^t A = nI_n$.

Definition 1.2 A **real** $n \times n$ matrix $A = (x_{ij})$ is said to be a Hadamard matrix of order n if $x_{ij} = \pm 1$ and $A^t A = nI_n$.

In view of the preceding Theorem, one asks if there exist real Hadamard matrices of any order n. For $n = 2$, one easily checks that

$$H(2) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is a Hadamard matrix. In higher dimensions however, it turns out that real Hadamard matrices will not always exist.

Theorem 1.5 (Hadamard)

Let $A = (\alpha_{ij})$ be a real Hadamard matrix of order $n > 2$. Then n is divisible by 4.

Proof

If j and k are two different columns of A, these are orthogonal, so

$$0 = \sum_{i=1}^{n} (\alpha_{ij}\alpha_{ik}) = \pm 1 \pm 1 \pm ... \pm 1 \ .$$

Thus, n must be even, and any two distinct columns have identical entries in exactly $n/2$ rows.

Consider now j, k, l three different columns of A. Then:

$$\sum_{i=1}^{n} (\alpha_{ij} + \alpha_{ik})(\alpha_{ij} + \alpha_{il}) =$$

$$= \sum_{i=1}^{n} (\alpha_{ij}^2) + \sum_{i=1}^{n} (\alpha_{ij}\alpha_{il}) + \sum_{i=1}^{n} (\alpha_{ik}\alpha_{ij}) + \sum_{i=1}^{n} (\alpha_{ik}\alpha_{il}) = n + 0 + 0 + 0 = n \ .$$

But $(\alpha_{ij} + \alpha_{ik})(\alpha_{ij} + \alpha_{il}) = 4$ if j^{th}, k^{th} and l^{th} columns all have the same entry in the i^{th} row. Otherwise, the product $(\alpha_{ij} + \alpha_{ik})(\alpha_{ij} + \alpha_{il})$ is 0. Hence $n = 4p$ where p is the number of rows in which all the three columns have the same entry. In particular, any 3 different columns have the same entry in $\frac{n}{4}$ rows. □

From Theorem 1.5, we conclude that in dimension $n > 2$ real Hadamard matrices may exist only when n is divisible by 4. It is still a conjecture to this date that this is the only restriction.

Hadamard Conjecture (1893)

There exist a real Hadamard matrix for every order n divisible by 4.