Determinants of Binary Circulant Matrices

Gérard Maze
gerard.maze@epfl.ch

ISIT 2004

June 28, 2004.

Joint work with H. Parlier

Outline of Talk:

1. Known conjectures
2. J.Cohn's result
3. The case of $\{0, 1\}$-matrices
4. The case of $\{-1, 1\}$-matrices
5. Conclusion

1. Known conjectures

This talk presents a connection between the Hadamard matrix conjecture, the circulant Hadamard matrix conjecture (which if proved true would imply the Barker conjecture) and the AG inequality.

Conjecture 1 (Hadamard Conjecture) *If n is a multiple of 4, then there exists a Hadamard matrix H_n, i.e, there exists $H_n \in \{-1, 1\}^{n\times n}$ such that*

$$H_n H_n^t = H_n^t H_n = n \cdot I_n.$$

Remark: H_n Hadamard $\Longleftrightarrow \det H_n = n^{n/2}$

Conjecture 2 (Circulant Hadamard Conjecture)
If $n > 4$ then there does not exist a circulant Hadamard matrix in dimension n, i.e, a Hadamard matrix of the form

$$\mathrm{Circ}_n[a_0, ..., a_{n-1}] = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \dots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{bmatrix}.$$

Conjecture 3 (Barker conjecture) *There is no Barker sequence of even length $n > 13$, i.e., there is no $a \in \{-1, 1\}^n$ with*

$$\left| \sum_{k=1}^{n-j} a_k a_{k+j} \right| \leq 1,\ j = 1, ..., n-1$$

Barker sequences are sequences with optimal energy configuration. It is known that no such sequence exists of odd length.

The Circulant Hadamard Conjecture implies the Barker Conjecture.

2. J.Cohn's result

J.Cohn (1963) has shown that the following equality holds:

$$2^{n-1} \cdot \max\{\text{determinant of } \{0,1\}\text{-matrix of size } n-1\}$$

$$=$$

$$\max\{\text{determinant of } \{-1,1\}\text{-matrix of size } n\} \leqslant n^{n/2}$$

Moreover his proof leads to a method that produces a $n \times n$ Hadamard matrix from a $n-1 \times n-1$ $\{0,1\}$-matrix with maximal determinant, i.e., when $\det = 2 \cdot (n/4)^{n/2}$.

Strategy for building Hadamard matrices?

Based on J.Cohn's equality, we would like to construct $n-1 \times n-1$ $\{0,1\}$-matrices with maximal determinant to produce Hadamard matrices. We focus on circulant matrices and use the classical identity

$$\det \mathrm{Circ}_{n-1}[b_0, ..., b_{n-2}] = \prod_{j=0}^{n-2} p(\zeta_{n-1}^j),$$

where $p(x) = \sum_{k=0}^{n-2} b_k x^k$ and $\zeta_{n-1} = \exp(2\pi i/(n-1))$.

3. The case of $\{0,1\}$-matrices

Theorem 4 *Let M be a circulant matrix with first line $[b_0, \ldots, b_{n-2}]$, $b_i \in \{0,1\}$, and $p(x) = \sum_{j=0}^{n-2} b_j x^j$. The following conditions are equivalent:*

1. $\det M$ *is maximal, i.e., equal to* $2 \cdot (n/4)^{n/2}$.

2. *The polynomial p satisfies the following equalities:*

$$|p(\zeta_{n-1}^j)| = \begin{cases} \frac{(n-1)+1}{2} & \text{if } j = 0, \\ \sqrt{\frac{(n-1)+1}{4}} & \text{otherwise,} \end{cases}$$

   and $n \equiv 0 \mod 4$.

Proof:

$$(\det M)^2 = \prod_{j=0}^{n-2} p(\zeta_{n-1}^j)^2 = p(1)^2 \prod_{j=1}^{n-2} |p(\zeta_{n-1}^j)|^2.$$

Let $k := p(1)$. Using the AG inequality, we have

$$\begin{aligned}(\det M)^2 &\leqslant p(1)^2 \left(\frac{1}{n-2} \sum_{j=1}^{n-2} |p(\zeta_{n-2}^j)|^2 \right)^{n-2} \\ &= k^2 \left(\frac{n-1}{n-2} \cdot \frac{\sum_{j=0}^{n-2} |p(\zeta_{n-1}^j)|^2 - k^2}{n-1} \right)^{n-2}\end{aligned}$$

Thus

$$
\begin{aligned}
(\det M)^2 &\leqslant k^2 \left(\frac{n-1}{n-2} \cdot \left(\sum_{j=0}^{n-2} b_j^2 - \frac{k^2}{n-1} \right) \right)^{n-2} \\
&= k^n \cdot (n-1-k)^{n-2} \cdot \frac{1}{(n-2)^{n-2}} \\
&\leqslant \left(\frac{n}{2}\right)^n \cdot \left(\frac{n-2}{2}\right)^{n-2} \cdot \frac{1}{(n-2)^{n-2}} \\
&= 4\left(\frac{n}{4}\right)^n .
\end{aligned}
$$

Finally, we have found Cohn's inequality for circulant $\{0,1\}$-matrices

$$\det M \leqslant 2\left(\frac{n}{4}\right)^{n/2}$$

based on the AG inequality. Equality holds if and only if

1. $n \equiv 0 \mod 4.$
2. $k = p(1) = \frac{n}{2},$
3. $|p(\zeta_{n-2}^{j})| = \sqrt{\frac{n}{4}}\ , \quad j = 1, ..., n-1$

This finishes the proof.

Corollary 5 *Constructing an $n \times n$ Hadamard matrix from a circulant $\{0,1\}$-matrix of size $n-1$ based on Cohn's construction is possible if and only if*

- $n \equiv 0 \mod 4$,
- *the set* $D := \{j \mid b_j = 1\}$ *is a* $(n-1, n/2, n/4)$ *Hadamard difference set in* $\mathbb{Z}/(n-1)\mathbb{Z}$.

Remark: There does not exist a Hadamard difference set when $n-1 = 55$ but a Hadamard matrix of order 56 does exist. Hence this strategy is not complete.

4. The case of $\{-1, 1\}$-matrices

Theorem 6 *Let N be a circulant matrix with first line $[a_0, ..., a_{n-1}]$, $a_i \in \{-1, 1\}$, and $p(x) = \sum_{j=0}^{n-1} a_j x^j$. The following conditions are equivalent:*

1. *N is a Hadamard matrix,*
2. $|p(\zeta_n^j)| = \sqrt{n}$ *for all j.*

The proof of Theorem 6 follows the same line as in the case of $\{0, 1\}$-matrix.

Example: The case $n = 4$ is well known and a circulant Hadamard matrix is given by the polynomial $p(x) = 1 + x - x^2 + x^3$ and all polynomials obtained by a cyclic permutation of the coefficients. These polynomials give rise to the following equalities

$$p(\zeta_4) = 2 \cdot \zeta_4^k, \quad k \in \{0, 1, 2, 3\}.$$

This is clearly a sign that if a circulant Hadamard matrix N exists of degree > 4, then the associated polynomial p might satisfy $p(\zeta_n) = \sqrt{n} \cdot \zeta_n^k$.

It turns out that the dimension $n = 4$ is the only one with this property:

Corollary 7 *If a circulant Hadamard matrix of dimension $n > 1$ exists with associated polynomial p such that $p(\zeta_n) = \sqrt{n} \cdot \zeta_n^k$, then $n = 4$.*

Corollary 8 *The existence of a Barker sequence of length $n > 13$ implies the existence of a polynomial of degree > 4 with coefficients in $\{-1, 1\}$ that satifies the above conditions.*

Due to the recent work of B.Schmidt, it is known that there is no Barker sequence of length l with

$$13 < l < 2.5 \cdot 10^9$$

and the smallest open case is

$$l = 4 \cdot 5^2 \cdot 101^2 \cdot 157^2 = 25,144,444,900.$$

L_1-norm of $\{-1,1\}$-polynomials

In a 1960 paper, D.J. Newman considers polynomials of degree $n-1$ with coefficients in $\{-1,1\}$ and proves that any such polynomial P satisfies a stronger form of the Cauchy-Schwarz inequality:

$$\int_0^1 |P(e^{2\pi it})|dt = \frac{1}{2\pi}\int_0^{2\pi} |P(e^{it})|dt < \sqrt{n-0.03}\,,$$

although Cauchy-Schwarz would only give the inequality $\leqslant \sqrt{n}$.

The circulant Hadamard conjecture can be seen as a discrete version of this result since the conjecture is equivalent to the conjecture that for such polynomials, we have

$$\frac{1}{n}\sum_{j=0}^{n-1}|P(e^{2\pi ij/n})| < \sqrt{n}$$

for $n > 4$. Once again, Cauchy-Schwarz would only give $\leqslant n$.

Conclusion

- In this talk, we have described the use of the AG inequality in proving extremal properties of $\{0, 1\}$-polynomials and $\{-1, 1\}$-polynomials that lead to circulant Hadamard matrices.
- Necessary and sufficient conditions have been found for such matrices to exist.
- A connection with the L_1-norm of polynomials has been shown.

For references and details, please have a look at

http://algo.epfl.ch/~gerard/