Determinants of Binary Circulant Matrices

Gérard Maze (LMA) [1] and Hugo Parlier (IGAT) [2]
Section of Mathematics, EPFL
CH-1015 Lausanne, Switzerland
{gerard.maze, hugo.parlier}@epfl.ch

Abstract — **We investigate the problem of deciding whether or not determinants of binary circulant matrices (i.e. matrices with entries in either $\{0,1\}$ or $\{-1,1\}$) can reach Hadamard's bound. We find necessary and sufficient conditions for the existence of such matrices. A direct consequence of this study relates to the existence of Barker sequences.**

I. Introduction

The circulant Hadamard matrix conjecture states that there are no circulant Hadamard matrices of order n for $n > 4$. Turyn [3] was the first to show that if such a matrix exists then its size n verifies $n = 4m^2$. He also showed that the existence of a Barker sequence of order $n > 13$ implies the existence of a circulant Hadamard matrix of order $n > 4$. Since then many articles have been published on the subject, some of them were found incorrect, and no significant progress has been realized until very recently (see [2]). The ideas given in the present article are self-contained and do not use the notion of difference sets. The proof of our results are based essentially on the AG inequality.

Let M (resp. N) be a $\{0,1\}$-matrix (resp. $\{-1,1\}$-matrix), i.e., a square matrix with entries in $\{0,1\}$ (resp. in $\{-1,1\}$). For a fixed size n let $f(n)$ be the maximum determinant of $\{0,1\}$-matrices and $g(n)$ be the maximum determinant of $\{-1,1\}$-matrices. J.Cohn [1] has shown that the following equality and inequalities hold: $2^{n-1}f(n-1) = g(n)$, $g(n) \leq n^{n/2}$, $f(n) \leq 2\left(\frac{n+1}{4}\right)^{(n+1)/2}$. Consequently, the existence of a $\{0,1\}$-matrix of size $n-1$ with determinant equal to $2(n/4)^{n/2}$ implies the existence of a $\{-1,1\}$-matrix of size n with maximum determinant. This would imply the existence of a Hadamard matrix of size n. The main subject of study of this article is to decide whether equality in the above inequalities can be reached by circulant matrices, both in the case where entries lie in $\{0,1\}$ and in $\{-1,1\}$.

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

Let M be a circulant $\{0,1\}$-matrix of size m. This matrix is then of the form $M = (b_{ij})$ where $b_{ij} = b_{i-j \bmod n} \in \{0,1\}$. Let $p(x) := \sum_{j=0}^{n-1} b_j x^j$ and $\zeta_m = \exp(2\pi i/m)$.

Theorem I Let M and $p(x)$ be as above. The following conditions are equivalent:

1. The determinant of M is maximum.
2. The polynomial p satisfies the following equalities:

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

and $m \equiv -1 \bmod 4$.

3. $m \equiv -1 \bmod 4$ and the set $D := \{j \mid b_j = 1\}$ is a $(m, (m+1)/2, (m+1)/4)$ difference set in $\mathbb{Z}/m\mathbb{Z}$.

In order to build a Hadamard matrix of order n, one could try to find a circulant $\{0,1\}$-matrix with maximal determinant and then build a $\{-1,1\}$-matrix based on Cohn's construction [1]. The previous theorem shows that this procedure will succeed if and only if there exists a Hadamard difference set in $\mathbb{Z}/(n-1)\mathbb{Z}$ (point 3. of Theorem I). However, it is known that there does not exist a Hadamard difference set when $n - 1 = 55$ but a Hadamard matrix of order 56 does exist. Hence this strategy in building Hadamard matrices is not complete.

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

Let N be a circulant $\{-1,1\}$-matrix of size n. This matrix is then of the form $N = (a_{ij})$ where $a_{ij} == a_{i-j \bmod n} \in \{0,1\}$. Let $p(x) := \sum_{j=0}^{n-1} a_j x^j$ and $\zeta_n = \exp(2\pi i/n)$.

Theorem II Let N and $p(x)$ be as above. The following conditions are equivalent:

1. The determinant of N is maximum.
2. $|p(\zeta_n^j)| = \sqrt{n}$ for all j.

Moreover, 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.

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 verify the following equality:

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

This is clearly a sign that if a circulant Hadamard matrix N of size > 4 exists, then the polynomial p might satisfy $p(\zeta_n) = \sqrt{n} \cdot \zeta_n^k$. The following corollary shows that this is not possible.

Corollary If a circulant Hadamard matrix of size $n > 1$ exists with associated polynomial p such that $p(\zeta_n) = \sqrt{n} \cdot \zeta_n^k$, for some $k \in \mathbb{N}$, then $n = 4$.

The full version of this article, with proofs, is available. Feel free to contact us.

[1] The first author was supported in part by NSF Grant DMS-00-72383.

[2] This second author was supported the by Swiss National Science Foundation grants 21 - 57251.99 and 20 - 68181.02.

References

[1] John H.E. Cohn, "On the Value of Determinants", *Proc. Amer. Math. Soc.*, vol. 14, pp. 581-588, 1963.

[2] B.Schmidt, *Characters and cyclotomic fields in finite geometry*, Lecture Notes in Mathematics, 1797, Berlin, 2002.

[3] R.J. Turyn, "Character sums and difference sets," *Pacific J. Math.*, vol. 15, pp. 319-346, 1965.