Determinants of Binary Circulant Matrices *

Gérard Maze
e-mail: gerard.maze@epfl.ch
Laboratoire de Mathématiques Algorithmiques
Ecole Polytechnique Fédérale de Lausanne
1015 Lausanne, Switzerland

Hugo Parlier
e-mail: hugo.parlier@epfl.ch
Section de Mathématiques, IGAT,
Ecole Polytechnique Fédérale de Lausanne
1015 Lausanne, Switzerland

November 27, 2003

Abstract

Using new methods, we investigate in this paper the problem of deciding whether or not determinants of binary matrices (i.e. matrices with entries in either $\{0,1\}$ or $\{-1,1\}$) can reach Hadamard's bound. Several results are presented using new tools, such as the AG inequality. A direct consequence of this study can be applied to the existence of Barker sequences. The general point of view is to find conditions so that a binary circulant matrix can reach the maximum value given by the Hadamard inequality.

1 Introduction

This paper 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. The circulant Hadamard matrix conjecture was first stated in 1963 in Ryser's book "Combinatorical Mathematics" [11]. It states that there are no circulant Hadamard matrices of order n for $n > 4$. Turyn [13] was the first to show that if such a matrix exists then its order n verifies $n = 4m^2$ with $m \geq 55$ odd . 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 and some of them were found incorrect (see [8] for details). The methods used are either elementary or make use of the theory of difference sets. Among the existing results, the most interesting come from Bernhard Schmidt who proved that given any finite set of primes p_i the conjecture is true for all but finitely many n which are products of powers of the p_i [12]. The ideas given in the present article are self-contained and do not use the notion of difference sets.

The general approach is to find necessary and sufficient conditions for the determinant of binary circulant matrices to reach the maximum value given by the Hadamard inequality. This general approach, when applied to matrices with $\{0,1\}$ entries, leads to the following result:

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

1. *The determinant of M is maximum, i.e., $\det M = 2\left(\frac{m+1}{4}\right)^{(m+1)/2}$.*

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

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

[*] The first author was supported in part by NSF grant DMS-00-72383, the second author was supported by the Swiss National Science Foundation grants 21 - 57251.99 and 20 - 68181.02.

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

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

When applied to matrices with $\{-1,1\}$ entries, this method leads to the following theorem:

Theorem 2 *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. *The determinant of* N *is maximum, i.e.,* $\det N = n^{n/2}$.
2. *The polynomial* p *satisfies* $|p(\zeta_n^j)| = \sqrt{n}$ *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.*

2 The Maximum Determinant Problem

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 dimension n let $f(n)$ be the maximum determinant of $\{0,1\}$-matrices and $g(n)$ be the maximum determinant of $\{-1,1\}$-matrices (for a $n \times n$ matrix by dimension we mean n). J.Cohn [2] has shown that the following equality and inequalities hold:

$$2^{n-1} f(n-1) = g(n) \ , \ \ g(n) \leqslant n^{n/2} \ , \ \ f(n) \leqslant 2\left(\frac{n+1}{4}\right)^{(n+1)/2} . \tag{2.1}$$

The equality comes from a standard constructive manipulation between $\{0,1\}$-matrices of dimension $n-1$ and $\{-1,1\}$-matrices of dimension n [2, 3]. Consequently, the existence of a $\{0,1\}$-matrix of dimension $n-1$ with determinant equal to $2(n/4)^{n/2}$ implies the existence of a $\{-1,1\}$-matrix of dimension n with maximum determinant. The first inequality comes from the Hadamard Inequality (see Proposition 6) and the second inequality is a consequence of the previous two relations.

Let A be a circulant $n \times n$ matrix, i.e., a matrix of the form

$$\mathrm{Circ}_n[a_0, a_1, ..., a_{n-1}] = (A_{ij})_{i,j=1..n} \quad \text{with } A_{ij} = a_{i-j \bmod n}.$$

From classical theory of such matrices, e.g. [4], it is known that for a given primitive n-th root of unity, say ζ, one has

$$\det \mathrm{Circ}_n[a_0, a_1, ..., a_{n-1}] = \prod_{j=0}^{n-1} p(\zeta^j) \quad \text{where} \quad p(x) = \sum_{k=0}^{n-1} a_k x^k. \tag{2.2}$$

Note that any primitive n-th root of unity can be considered in the product. In the sequel, we will write ζ_n for $\exp(\frac{2\pi i}{n})$ and call $p(x)$ the *associated polynomial* to A.

The main subject of study of this article is to decide whether equality in (2.1) can be reached by circulant matrices, both in the case where entries lie in $\{0,1\}$ and in $\{-1,1\}$. By *maximal determinant* we will always mean a determinant that reaches equality in Inequlity 2.1. This study has two faces each connected to well-known conjectures. In order to state them, recall that a Hadamard matrix H_n is a $\{-1,1\}$-matrix of dimension n such that $H_n H_n^t = nI_n$ and a circulant Hadamard matrix is a Hadamard matrix which is circulant. It is well known, e.g. [7], that Hadamard matrices exist in dimension $n > 2$ only when n is a multiple of 4. In the sequel we will always assume $n > 2$. Let us also recall that a Barker sequence $\{a_k\}_{k=1}^n$ is a real sequence that satisfies $|\sum_{k=1}^{n-j} a_k a_{k+j}| \leq 1$, $j = 1, ..., n-1$ and $|a_k| = 1$.

Conjecture 3 (Hadamard Conjecture) *If* n *is a multiple of 4, then there exists a Hadamard matrix* H_n.

Conjecture 4 (Circulant Hadamard Conjecture) *If $n > 4$ then there does not exist a circulant Hadamard matrix of dimension n.*

Conjecture 5 (Barker conjecture) *There is no Barker sequence of length > 13.*

The following result establishes the connection between these conjectures and our study.

Proposition 6 (Hadamard's Inequality) *For any real $n \times n$ matrix A, one has*

$$|\det A| \leqslant \prod_{j=1}^{n} \left(\sum_{i=1}^{n} a_{ij}^2 \right)^{1/2}$$

with equality if and only if a column is the zero vector or AA^t is diagonal. A $\{-1,1\}$-matrix N of dimension n is a Hadamard matrix if and only if $\det N$ is maximal, i.e., if and only if $\det N = n^{n/2}$.

The proof is in essence already contained in Hadamard's original paper on the subject [6] and a complete proof can be found in [5], p.153. Proposition 6 shows that Conjecture 4 is true if and only if there does not exist a circulant $\{-1,1\}$-matrix with maximal determinant in any dimension strictly bigger than 4. It also shows that if one can find a $n-1$ dimensional circulant $\{0,1\}$-matrix with maximal determinant, then there exists a Hadamard matrix of dimension n. One of the tools we use is the well-known arithmetico-geometric inequality:

Proposition 7 (Arithmetico-Geometric Inequality) *For any set of non-negative numbers $x_0, ..., x_{n-1}$ one has*

$$\left(\prod_{j=0}^{n-1} x_j \right)^{\frac{1}{n}} \leqslant \frac{1}{n} \sum_{j=0}^{n-1} x_j. \tag{2.3}$$

Equality holds if and only if $x_i = x_j$ for all i and j.

For a proof, see e.g. [9], p. 15. We will also use the following version of the Plancherel equality:

Proposition 8 *Let $p(x) = \sum_{j=0}^{n-1} a_j x^j$ be a polynomial with complex coefficients. Then*

$$\frac{1}{n} \sum_{j=0}^{n-1} |p(\zeta_n^j)|^2 = \sum_{j=0}^{n-1} |a_j|^2.$$

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

Let M be a circulant $\{0,1\}$-matrix of dimension m. This matrix is then of the form $M = \mathrm{Circ}_n[b_0, b_1, ..., b_{m-1}]$ where $b_i \in \{0,1\}$. Let $p(x) := \sum_{j=0}^{n-1} b_j x^j$ be its associated polynomial. This section provides necessary and sufficient conditions on p for $\det M$ to be maximal. First, we have from Equality (2.2):

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

Let k be the number of 1s among the b_i, i.e., $k := p(1)$. Using Proposition 8 and Inequality (2.3), we have

$$(\det M)^2 \quad \leqslant \quad p(1)^2 \left(\frac{1}{m-1} \sum_{j=1}^{m-1} |p(\zeta_m^j)|^2 \right)^{m-1}$$

$$
\begin{aligned}
&= k^2 \left(\frac{m}{m-1} \cdot \frac{\sum_{j=0}^{m-1} |p(\zeta_m^j)|^2 - k^2}{m} \right)^{m-1} \\
&= k^2 \left(\frac{m}{m-1} \cdot \left(\sum_{j=0}^{m-1} b_j^2 - \frac{k^2}{m} \right) \right)^{m-1} \\
&= k^{m+1} \cdot (m-k)^{m-1} \cdot \frac{1}{(m-1)^{m-1}}.
\end{aligned}
$$

Since $x^{m+1} \cdot (m-x)^{m-1}$ is maximum in $[0,m]$ if and only if $x = \frac{m+1}{2}$, we have

$$
(\det M)^2 \leqslant \left(\frac{m+1}{2} \right)^{m+1} \cdot \left(\frac{m-1}{2} \right)^{m-1} \cdot \frac{1}{(m-1)^{m-1}} = 4 \left(\frac{m+1}{4} \right)^{m+1}. \tag{3.1}
$$

Finally, we have

$$
\det M \leqslant 2 \left(\frac{m+1}{4} \right)^{(m+1)/2}, \text{ with equality if and only if } k = \frac{m+1}{2}.
$$

We have found Inequality 2.1 using Inequality 2.3. This comes with the proof of Theorem 1 and an extra condition connecting our problem to cyclic difference sets. The equivalence of points 1. and 3. below is not new but we were not able to find it stated in the litterature.

Theorem 1 *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:*

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

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

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

Proof: If $\det M$ is maximum, then using Inequality (3.1) and the previous discussion, we see that $m \equiv -1 \mod 4$ as well as $p(1) = (m+1)/2$. Because of the property of Inequality (2.3), we also have $|p(\zeta_m^j)| = |p(\zeta_m^k)|$ for all j and k different from 0. This shows that 1. implies 2.. Reciprocally, if the conditions of 2. are fullfilled then clearly 1. holds. Next, we show that 2. is equivalent to 3. by considering the polynomials

$$
g(x) := p(x) \cdot \left(x^m p\left(\frac{1}{x} \right) \right) \mod x^m - 1 \text{ and } f(x) := \frac{m+1}{4} + \frac{m+1}{4}(1 + x + \ldots + x^{m-1}).
$$

Note that $g(\zeta_m^j) = |p(\zeta_m^j)|^2$, $\forall j$. Classical theory in difference sets, see, e.g., [1], shows that D is a difference set if and only if $f = g$. If 2. is fullfiled, we have

$$
f(1) = \frac{m+1}{4} + \frac{m+1}{4} m = \frac{(m+1)^2}{4} = g(1),
$$

and if $j \neq 0$

$$
f(\zeta_m^j) = \frac{m+1}{4} + 0 = |p(\zeta_m^j)|^2 = p(\zeta_m^j) p(\zeta_m^{-j}) = g(\zeta_m^j).
$$

Since both g and f have degree less or equal to $m-1$ and have the same value on m points, $f = g$ and 3. is proven. If 3. is fullfiled, then $f = g$ and 2. is clearly satisfied. □

Remark 9 As stated in Section 2, there is a standard manipulation that will create a $\{-1,1\}$-matrix N from any $\{0,1\}$-matrix M with the property that $\det N$ is maximal among all $\{-1,1\}$-matrices if and only if $\det M$ is maximal among all $\{0,1\}$-matrices. Therefore, in order to build a Hadamard matrix of order n, one could try to find a circulant $\{0,1\}$-matrix with maximal determinant. The previous theorem shows that this procedure will succeed if only if there exists a Hadamard difference set in $\mathbb{Z}/(n-1)\mathbb{Z}$, i.e., a difference set with the parameters described in point 3. of the theorem. However, it is known that there does not exist a Hadamard difference set when $n-1=55$ (c.f. [1]) but a Hadamard matrix of order 56 does exist. Hence this strategy in building Hadamard matrices is not complete.

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

Let N be a circulant $\{-1,1\}$-matrix of dimension n. This matrix is then of the form

$$N = \mathrm{Circ}_n[a_0, a_1, ..., a_{n-1}] \quad \text{where} \quad a_i \in \{-1,1\}.$$

Let $p(x) := \sum_{j=0}^{n-1} a_j x^j$ be its associated polynomial. This section provides necessary and sufficient conditions on p for $\det N$ to be maximal. The developpment is the same as in the previous section but the details are different. First,

$$n = \sum_{j=0}^{n-1} |a_j|^2 = \frac{1}{n} \sum_{j=0}^{n-1} |p(\zeta_n^j)|^2$$

due to Proposition 8. Then using 2.3, one has

$$n \geqslant \left(\prod_{j=0}^{n-1} |p(\zeta_n^j)|^2 \right)^{\frac{1}{n}} = \left(\left| \prod_{j=0}^{n-1} p(\zeta_n^j) \right| \right)^{\frac{2}{n}}$$

and since we have the expression of $\det N$ given by 2.2, we can write

$$n \geqslant (\det N)^{\frac{2}{n}} \quad \text{i.e.} \quad \det N \leqslant n^{n/2}. \tag{4.1}$$

Once again we have found the bound stated in (2.1) via Inequality (2.3). In addition this brings Theorem 2 below.

Theorem 2 *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.

Proof: From inequality 4.1, the determinant of N is maximum if and only if the inequality that comes from (2.3) is an equality. This is the case if and only if all the $|p(\zeta_n^j)|$ are equal, i.e., if and only if $|p(\zeta_n^j)| = \sqrt{n}$ for all j. This proves the equivalence. The last point comes from Turyn's work [13] and Proposition 6. □

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 $p(\zeta_n) = \sqrt{n} \cdot \zeta_n^k$. We prove now that such a situation is not possible. First, for such a k, consider the polynomial $\tilde{p}(x) := x^{n-k}p(x) \mod x^n - 1$ and the circulant matrix $\tilde{N}$ associated to it. Note that $\tilde{p}(x)$ is obtain from $p(x)$ by a cyclic permutation of its coefficient and that $\tilde{N}$ is still a circulant Hadamard matrix. But now $\tilde{p}(\zeta_n) = \sqrt{n}$. Therefore, without loss of generality, we can assume that $p(\zeta_n) = \sqrt{n}$.

Lemma 11 *Let $n \in \mathbb{N}$ and d be any divisor of n with the property that if p is a prime divisor of n then p divides d. Then $\mathcal{B} = \{1, \zeta_n, \zeta_n^2, ..., \zeta_n^{n/d-1}\}$ is a basis of the $\mathbb{Q}(\zeta_d)$-vector space $\mathbb{Q}(\zeta_n)$.*

The proof is left to the reader.

Theorem 12 *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 $n = 4$.*

Proof: If $n = 4$ the case is clear. Let $n = l^2$, $l = p(\zeta_n) \in \mathbb{N}$ and consider the $\mathbb{Q}(\zeta_l)$-vector space $\mathbb{Q}(\zeta_n)$. Note that l is a divisor of n that satisfies the condition of Lemma 11. Let us define λ as

$$\lambda := \sum_{j=0}^{l-1} a_{jl}\zeta_n^{jl} = \sum_{j=0}^{l-1} a_{jl}\zeta_l^j \in \mathbb{Q}(\zeta_l).$$

Then

$$l - \lambda = \sum_{i=0}^{n-1} a_i\zeta_n^i - \sum_{j=0}^{l-1} a_{jl}\zeta_n^{jl} = \sum_{t=0}^{l-1}\sum_{j=0}^{l-1} a_{lj+t}\zeta_n^{lj+t} - \sum_{j=0}^{l-1} a_{jl}\zeta_n^{jl} = \sum_{t=1}^{l-1}\left(\sum_{j=0}^{l-1} a_{lj+t}\zeta_l^j\right)\zeta_n^t$$

and finally

$$\underbrace{(l-\lambda)}_{\in\mathbb{Q}(\zeta_l)} \cdot 1 - \sum_{t=1}^{l-1}\underbrace{\left(\sum_{j=0}^{l-1} a_{lj+t}\zeta_l^j\right)}_{\in\mathbb{Q}(\zeta_l)}\zeta_n^t = 0.$$

This is a $\mathbb{Q}(\zeta_l)$-linear combination of the elements of the basis $\mathcal{B}$ (see Lemma 11) which is equal to zero. Hence all the coefficients are zero and $\lambda = \sum_{j=0}^{l-1} a_{jl}\zeta_l^j = l$. Applying the Cauchy-Schwarz inequality, which is in that case an equality, we see that the sequences $\{a_{jl}\}$ and $\{\zeta_l^j\}$ must be proportional (e.g. [9], p. 84), which is possible if and only if $l = 1$ or $l = 2$. The case $l = 1$ was excluded, which proves the theorem. □

Remark 13 There is a surprising connection between Theorem 2 and D.J. Newman's article "Norms of Polynomials". In his paper, 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 $\leqslant n$. 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 $n > 4$.

References

[1] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Mathematics 182, Springer Verlag, 1971.

[2] John H.E. Cohn, On the Value of Determinants, Proc. Amer. Math. Soc. 14 (1963), 581-588.

[3] C.J. Colbourn and J.H. Dinitz (Ed.), The CRC Handbook of Combinatorial Designs, CRC Press, 1996.

[4] P.J. Davis, Circulant Matrices, Pure and Applied Mathematics, Wiley Interscience Publications, 1979.

[5] J.N. Franklin, Matrix Theory, Prentice-Hall Series in Applied Mathematics, 1986.

[6] J.Hadamard, Résolution d'une question relative aux déterminant, Bull. Sci. Math. 2 (1893), 240-248.

[7] M. Hall Combinatorial theory, Blaisdell Publishing Co. Ginn and Co., 1967.

[8] C. Lin, W.D. Wallis, On the Circulant Hadamard Conjecture, In: Coding theory, design theory, group theory. Eds. D. Jungnickel, S.A. Vanstone. Wiley, New York (1993), 213-217.

[9] D.S. Mitrinović, J.E. Pecarić and A.M. Fink, Classical and New Inequalties in Analysis, Kluwer Academic Publishers, 1993.

[10] D.J. Newman, Norms of Polynomials, The Amer. Math. Monthly 67, (1960), 778-779.

[11] H.J. Ryser, Combinatorial Mathematics, Published by The Mathematical Association of America, 1963.

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

[13] R.J. Turyn, Character sums and difference sets, Pacific J. Math. 15, (1965), 319-346.