A generalization of circulant Hadamard and conference matrices

Ondřej Turek

(Joint work with D. Goyeneche)

6 March 2018

Introduction

Circulant matrix

$$C = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & c_1 & & c_{n-2} \\ \vdots & c_{n-1} & c_0 & \ddots & \vdots \\ c_2 & & \ddots & \ddots & c_1 \\ c_1 & c_2 & \cdots & c_{n-1} & c_0 \end{pmatrix}$$

Circulant matrix

$$C = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & c_1 & & c_{n-2} \\ \vdots & c_{n-1} & c_0 & \ddots & \vdots \\ c_2 & & \ddots & \ddots & c_1 \\ c_1 & c_2 & \cdots & c_{n-1} & c_0 \end{pmatrix}$$

$g = (c_0, c_1, \ldots, c_{n-1})$ ... **generator** of C

Circulant matrix

$$C = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & c_1 & & c_{n-2} \\ \vdots & c_{n-1} & c_0 & \ddots & \vdots \\ c_2 & & \ddots & \ddots & c_1 \\ c_1 & c_2 & \cdots & c_{n-1} & c_0 \end{pmatrix}$$

$g = (c_0, c_1, \ldots, c_{n-1})$ ... **generator** of C

Examples:

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2\pi & \mathrm{e} \\ \mathrm{e} & 1 & 2\pi \\ 2\pi & \mathrm{e} & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 2 & -4 & 1 \\ 1 & 0 & 2 & -4 \\ -4 & 1 & 0 & 2 \\ 2 & -4 & 1 & 0 \end{pmatrix}$$

Hadamard matrix

Hadamard matrix is a square matrix with entries ± 1 and mutually orthogonal rows.

Examples:

$$\begin{pmatrix} 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Hadamard matrix

Hadamard matrix is a square matrix with entries ± 1 and mutually orthogonal rows.

Examples:

$$\begin{pmatrix}1\end{pmatrix}, \qquad \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \qquad \begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}$$

Theorem

The order of any Hadamard matrix is 1, 2, or a multiple of 4.

Hadamard matrix

Hadamard matrix is a square matrix with entries ± 1 and mutually orthogonal rows.

Examples:

$$\begin{pmatrix} 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Theorem

The order of any Hadamard matrix is 1, 2, or a multiple of 4.

Hadamard conjecture (before 1933)

There exists an Hadamard matrix of order $4k$ for every $k \in \mathbb{N}$.

Hadamard matrices and the determinant

Theorem (Hadamard 1893)

If all the entries of an $M \in \mathbb{C}^{n,n}$ satisfy $|m_{ij}| \leq 1$, then

$$|\det(M)| \leq n^{n/2}\,,$$

and equality is achieved if and only if $|m_{ij}| = 1$ for all i, j and the rows of M are orthogonal.

Corollary

Hadamard matrices have maximal $|\det(M)|$ among all matrices of order n with entries $m_{ij} \in \{-1, 1\}$.

Hadamard circulant matrices

$$\begin{pmatrix}1\end{pmatrix}, \qquad \begin{pmatrix}-1\end{pmatrix}$$

$$\pm\begin{pmatrix}-1 & 1 & 1 & 1\\ 1 & -1 & 1 & 1\\ 1 & 1 & -1 & 1\\ 1 & 1 & 1 & -1\end{pmatrix}, \qquad \pm\begin{pmatrix}1 & -1 & 1 & 1\\ 1 & 1 & -1 & 1\\ 1 & 1 & 1 & -1\\ -1 & 1 & 1 & 1\end{pmatrix},$$

$$\pm\begin{pmatrix}1 & 1 & -1 & 1\\ 1 & 1 & 1 & -1\\ -1 & 1 & 1 & 1\\ 1 & -1 & 1 & 1\end{pmatrix}, \qquad \pm\begin{pmatrix}1 & 1 & 1 & -1\\ -1 & 1 & 1 & 1\\ 1 & -1 & 1 & 1\\ 1 & 1 & -1 & 1\end{pmatrix}$$

Hadamard circulant matrices

$$(1)\ , \qquad (-1)$$

$$\pm\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}, \qquad \pm\begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \end{pmatrix},$$

$$\pm\begin{pmatrix} 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \end{pmatrix}, \qquad \pm\begin{pmatrix} 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{pmatrix}$$

Hadamard circulant conjecture (Ryser 1963):

Hadamard circulant matrices exist only of orders $n = 1$ and $n = 4$.

Conference matrix

Conference matrix is an $n \times n$ matrix $(n > 1)$ such that

$$m_{ij} = \begin{cases} \pm 1 & \text{for } i \neq j \\ 0 & \text{for } i = j \end{cases}$$

and its rows are mutually orthogonal.

Examples:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & -1 & 1 \\ 1 & 1 & 0 & -1 \\ 1 & -1 & 1 & 0 \end{pmatrix}$$

The name "conference matrix"

V. Belevitch (*Electrical Communication*, vol. 27, 1950):

An n-port ideal conference network exists if and only if there exists an $n \times n$ orthogonal matrix

$$S = \frac{1}{(n-1)^{1/2}} \begin{pmatrix} 0 & \pm 1 & \pm 1 & \cdots & \pm 1 \\ \pm 1 & 0 & \pm 1 & \cdots & \pm 1 \\ \pm 1 & \pm 1 & 0 & & \pm 1 \\ \vdots & \vdots & & \ddots & \pm 1 \\ \pm 1 & \pm 1 & \cdots & \pm 1 & 0 \end{pmatrix}.$$

(ideal = constructed without resistances)

... Hence the name "conference matrix".

Circulant conference matrices

Examples: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$

Circulant conference matrices

Examples: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$

Theorem (Stanton and Mullin 1976)

A circulant conference matrix, i.e.,

$$\begin{pmatrix} 0 & c_1 & \cdots & c_{n-2} & c_{n-1} \\ c_{n-1} & 0 & c_1 & & c_{n-2} \\ \vdots & c_{n-1} & 0 & \ddots & \vdots \\ c_2 & & \ddots & \ddots & c_1 \\ c_1 & c_2 & \cdots & c_{n-1} & 0 \end{pmatrix}$$

with

$$c_j \in \{1, -1\} \qquad \forall j = 1, \ldots, n-1$$

and mutually orthogonal rows, exists only for $n = 2$.

Generalized problem

$$C = \begin{pmatrix} d & c_1 & \cdots & c_{n-2} & c_{n-1} \\ c_{n-1} & d & c_1 & & c_{n-2} \\ \vdots & c_{n-1} & d & \ddots & \vdots \\ c_2 & & \ddots & \ddots & c_1 \\ c_1 & c_2 & \cdots & c_{n-1} & d \end{pmatrix}$$

with entries

$$d \geq 0\,, \quad c_j \in \{1, -1\} \qquad \forall j = 1, \ldots, n-1$$

and mutually orthogonal rows.

Problem: Determine possible orders $n > 1$ for a given value of d.

Generalized problem

$$C = \begin{pmatrix} d & c_1 & \cdots & c_{n-2} & c_{n-1} \\ c_{n-1} & d & c_1 & & c_{n-2} \\ \vdots & c_{n-1} & d & \ddots & \vdots \\ c_2 & & \ddots & \ddots & c_1 \\ c_1 & c_2 & \cdots & c_{n-1} & d \end{pmatrix}$$

with entries

$$d \geq 0\,, \quad c_j \in \{1, -1\} \qquad \forall j = 1, \ldots, n-1$$

and mutually orthogonal rows.

Problem: Determine possible orders $n > 1$ for a given value of d.

Remark. $d = 0 \;\Rightarrow\; n = 2$ *(Stanton and Mullin)*

$d = 1 \;\overset{?}{\Rightarrow}\; n = 4$ *(Hadamard circulant conjecture)*

Conditions on n

The problem

Let

$$C = \begin{pmatrix} d & \pm 1 & \pm 1 & \cdots & \pm 1 \\ \pm 1 & d & \pm 1 & \cdots & \pm 1 \\ \pm 1 & \pm 1 & d & & \pm 1 \\ \vdots & \vdots & & \ddots & \pm 1 \\ \pm 1 & \pm 1 & \cdots & \pm 1 & d \end{pmatrix} \in \mathbb{R}^{n,n}$$

be

- circulant,
- having mutually orthogonal rows.

Question: For a given d, what are possible sizes of C?

Convention.
We assume $n \geq 2$ and $d \geq 0$ without loss of generality.

Lemma. The order n satisfies

$$n \equiv 2d + 2 \pmod 4 \qquad \text{and} \qquad n \geq 2d + 2\,.$$

Lemma. The order n satisfies

$$n \equiv 2d + 2 \pmod 4 \qquad \text{and} \qquad n \geq 2d + 2\,.$$

Proof. Generator: $g = (d, c_1, c_2, \ldots, c_{n-1})$, $\quad c_j = \pm 1$

- <u>if n is *even*</u>: scalar product of the 0th and the $\frac{n}{2}$-th row

$$2dc_{\frac{n}{2}} + 2\sum_{j=1}^{\frac{n}{2}-1} c_j c_{\frac{n}{2}+j} = 0$$

$$d = \left| \sum_{j=1}^{\frac{n}{2}-1} c_j c_{\frac{n}{2}+j} \right|$$

$$\Rightarrow \quad d \equiv \frac{n}{2} - 1 \pmod 2 \qquad \text{and} \qquad d \leq \frac{n}{2} - 1$$

Lemma. The order n satisfies

$$n \equiv 2d + 2 \pmod 4 \qquad \text{and} \qquad n \geq 2d + 2\,.$$

Proof. Generator: $g = (d, c_1, c_2, \ldots, c_{n-1}), \quad c_j = \pm 1$

- <u>if *n* is *even*</u>: scalar product of the 0th and the $\frac{n}{2}$-th row

$$2dc_{\frac{n}{2}} + 2\sum_{j=1}^{\frac{n}{2}-1} c_j c_{\frac{n}{2}+j} = 0$$

$$d = \left|\sum_{j=1}^{\frac{n}{2}-1} c_j c_{\frac{n}{2}+j}\right|$$

$$\Rightarrow \quad d \equiv \frac{n}{2} - 1 \pmod 2 \qquad \text{and} \qquad d \leq \frac{n}{2} - 1$$

- <u>if *n* is *odd*</u>: using the orthogonality of the 0th and the 1st row.

Possible orders of C

We distinguish 4 cases:

I. d is even integer
II. d is odd integer
III. d is half-integer: $\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2}, \ldots$
IV. $2d$ is non-integer

Possible orders of C

We distinguish 4 cases:

I. d is even integer
II. d is odd integer
III. d is half-integer: $\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2}, \ldots$
IV. $2d$ is non-integer

Case IV.

Proposition. If $2d \notin \mathbb{Z}$, then C does not exist.

Proof. We use Lemma:

$$n \equiv 2d + 2 \pmod 4 \quad \ldots \text{no } n \in \mathbb{N} \text{ exists for } 2d \notin \mathbb{Z}$$

Case III.

Proposition. If d is half-integer ($d \in \{\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2}, \ldots\}$), then C exists only of order $n = 2d + 2$.

Proof. 4 steps:

1. Apply Lemma:

$$n \equiv 2d + 2 \pmod 4 \quad \Rightarrow \quad n \text{ is odd}$$

2. Orthogonality $\Rightarrow$ C is symmetric and $\exists k : c_k = c_{n-k} = -1$.
3. Prove that $\neg\exists j : c_j = c_{n-j} = 1$; hence

$$g = (d, -1, -1, \ldots, -1)\,.$$

4. Orthogonality $\Rightarrow$ $-2d + n - 2 = 0$ $\Rightarrow$ $n = 2d + 2$.

Case I.

Theorem. If d is even integer, then $n = 2d + 2$.

Proof. 4 steps:

1. Apply Lemma: $n \equiv 2d + 2 \pmod 4 \quad \Rightarrow \quad n \equiv 2 \pmod 4$.
2. Prove that $n \equiv 2 \pmod 4 \quad \Rightarrow \quad C$ is symmetric.
3. Use the symmetry of C to prove $d \equiv \frac{n}{2} - 1 \pmod 4$.
4. $d \equiv \frac{n}{2} - 1 \pmod 4$ and C is symmetric $\quad \Rightarrow \quad d = \frac{n}{2} - 1$

Case I.

Theorem. If d is even integer, then $n = 2d + 2$.

Proof. 4 steps:

1. Apply Lemma: $n \equiv 2d + 2 \pmod 4 \quad \Rightarrow \quad n \equiv 2 \pmod 4$.
2. Prove that $n \equiv 2 \pmod 4 \quad \Rightarrow \quad C$ is symmetric.
3. Use the symmetry of C to prove $d \equiv \frac{n}{2} - 1 \pmod 4$.
4. $d \equiv \frac{n}{2} - 1 \pmod 4$ and C is symmetric $\quad \Rightarrow \quad d = \frac{n}{2} - 1$

Example.

$d = 0$: $\quad n = 2 \cdot 0 + 2 = 2 \quad$ (Stanton and Mullin 1976)

Case II.

Proposition. If d is odd integer, then

$$\exists k \in \mathbb{N} : \qquad n = k(2d + k) + 1 \,.$$

Proof. $(1, 1, \ldots, 1)^T$ is an eigenvector of C, corresponding to the eigenvalue

$$\lambda = c_0 + c_1 + c_2 + \cdots + c_{n-1}$$

Case II.

Proposition. If d is odd integer, then

$$\exists k \in \mathbb{N} : \qquad n = k(2d + k) + 1 \,.$$

Proof. $(1, 1, \ldots, 1)^T$ is an eigenvector of C, corresponding to the eigenvalue

$$\lambda = c_0 + c_1 + c_2 + \cdots + c_{n-1}$$

Orthogonality of rows: $\quad CC^T = (d^2 + n - 1)I$

$\Rightarrow \quad$ eigenvalues of C satisfy $\quad |\lambda| = \sqrt{d^2 + n - 1}$

Case II.

Proposition. If d is odd integer, then

$$\exists k \in \mathbb{N}: \qquad n = k(2d+k)+1\,.$$

Proof. $(1,1,\ldots,1)^T$ is an eigenvector of C, corresponding to the eigenvalue

$$\lambda = c_0 + c_1 + c_2 + \cdots + c_{n-1}$$

Orthogonality of rows: $\quad CC^T = (d^2+n-1)I$

$\Rightarrow$ eigenvalues of C satisfy $\quad |\lambda| = \sqrt{d^2+n-1}$

$$\underbrace{|d + c_1 + \cdots + c_{n-1}|}_{\in\mathbb{Z}} = \sqrt{d^2+n-1}$$

Case II.

Proposition. If d is odd integer, then

$$\exists k \in \mathbb{N} : \qquad n = k(2d+k)+1\,.$$

Proof. $(1,1,\ldots,1)^T$ is an eigenvector of C, corresponding to the eigenvalue

$$\lambda = c_0 + c_1 + c_2 + \cdots + c_{n-1}$$

Orthogonality of rows: $\quad CC^T = (d^2+n-1)I$

$\Rightarrow \quad$ eigenvalues of C satisfy $\quad |\lambda| = \sqrt{d^2+n-1}$

$$\underbrace{|d + c_1 + \cdots + c_{n-1}|}_{\in\mathbb{Z}} = \sqrt{d^2+n-1}$$

$$\Rightarrow$$

Case II.

Proposition. If d is odd integer, then

$$\exists k \in \mathbb{N}: \qquad n = k(2d + k) + 1\,.$$

Proof. $(1, 1, \ldots, 1)^T$ is an eigenvector of C, corresponding to the eigenvalue

$$\lambda = c_0 + c_1 + c_2 + \cdots + c_{n-1}$$

Orthogonality of rows: $\quad CC^T = (d^2 + n - 1)I$

$\Rightarrow \quad$ eigenvalues of C satisfy $\quad |\lambda| = \sqrt{d^2 + n - 1}$

$$\underbrace{|d + c_1 + \cdots + c_{n-1}|}_{\in \mathbb{Z}} = \sqrt{d^2 + n - 1}$$

$$\Rightarrow \quad \exists k \in \mathbb{N}: \; \sqrt{d^2 + n - 1} = d + k$$

Partial summary

Case	d	Possible orders n
I	even integer	$n = 2d + 2$
II	odd integer	$n = k(2d + k) + 1$
III	half-integer	$n = 2d + 2$
IV	$2d \notin \mathbb{Z}$	no $n \in \mathbb{N}$; equivalently: $n = 2d + 2 \quad (\notin \mathbb{N})$

Partial summary

Case	d	Possible orders n
I	even integer	$n = 2d + 2$
II	odd integer	$n = k(2d + k) + 1$
III	half-integer	$n = 2d + 2$
IV	$2d \notin \mathbb{Z}$	no $n \in \mathbb{N}$; equivalently: $n = 2d + 2$ $(\notin \mathbb{N})$

Partial summary

Case	d	Possible orders n
I	even integer	$n = 2d + 2$
II	odd integer	$n = k(2d + k) + 1$
III	half-integer	$n = 2d + 2$
IV	$2d \notin \mathbb{Z}$	no $n \in \mathbb{N}$; equivalently: $n = 2d + 2$ $(\notin \mathbb{N})$

Conjecture. If d is odd, then the order n can be only $n = 2d + 2$.

Partial summary

Case	d	Possible orders n
I	even integer	$n = 2d + 2$
II	odd integer	$n = k(2d + k) + 1$
III	half-integer	$n = 2d + 2$
IV	$2d \notin \mathbb{Z}$	no $n \in \mathbb{N}$; equivalently: $n = 2d + 2$ $(\notin \mathbb{N})$

Conjecture. If d is odd, then the order n can be only $n = 2d + 2$.

Remark. The conjecture is consistent with the circulant Hadamard conjecture:

$$d = 1: \qquad n = 2 \cdot 1 + 2 = 4$$

Small orders

Observation. Every C up to order $n = 50$ satisfies $n = 2d + 2$.

Proof.

Lemma: $n \equiv 2d + 2 \pmod 4$

Small orders

Observation. Every C up to order $n = 50$ satisfies $n = 2d + 2$.

Proof.

Lemma: $n \equiv 2d + 2 \pmod 4$

- n is odd $\Rightarrow$ d is half-integer (Case III) $\Rightarrow$ $n = 2d + 2$

Small orders

Observation. Every C up to order $n = 50$ satisfies $n = 2d + 2$.

Proof.

Lemma: $n \equiv 2d + 2 \pmod 4$

- n is odd $\Rightarrow$ d is half-integer (Case III) $\Rightarrow$ $n = 2d + 2$
- $n \equiv 2 \pmod 4$ $\Rightarrow$ d is even (Case I) $\Rightarrow$ $n = 2d + 2$

Small orders

Observation. Every C up to order $n = 50$ satisfies $n = 2d + 2$.

Proof.

Lemma: $n \equiv 2d + 2 \pmod 4$

- n is odd $\quad\Rightarrow\quad$ d is half-integer (Case III) $\quad\Rightarrow\quad$ $n = 2d + 2$
- $n \equiv 2 \pmod 4$ $\quad\Rightarrow\quad$ d is even (Case I) $\quad\Rightarrow\quad$ $n = 2d + 2$
- n is a multiple of 4 $\quad\Rightarrow\quad$ d is odd integer (Case II)

  $\Rightarrow \quad n = k(2d + k) + 1$, hence

$$d = \frac{n-1}{2k} - \frac{k}{2} \qquad \text{for } k|(n-1), \quad k \leq \sqrt{n-1}$$

Small orders

Observation. Every C up to order $n = 50$ satisfies $n = 2d + 2$.

Proof.

Lemma: $n \equiv 2d + 2 \pmod 4$

- n is odd $\Rightarrow$ d is half-integer (Case III) $\Rightarrow$ $n = 2d + 2$
- $n \equiv 2 \pmod 4$ $\Rightarrow$ d is even (Case I) $\Rightarrow$ $n = 2d + 2$
- n is a multiple of 4 $\Rightarrow$ d is odd integer (Case II)

  $\Rightarrow$ $n = k(2d + k) + 1$, hence

$$d = \frac{n-1}{2k} - \frac{k}{2} \qquad \text{for } k|(n-1), \quad k \leq \sqrt{n-1}$$

  - $n - 1$ is a prime $\Rightarrow$ $k = 1$ $\Rightarrow$ $n = 2d + 2$
  - $\exists k > 1$, k is a divisor of $n - 1$: (see next slide)

n	(k,d) for $k>1$, $d=\frac{n-1}{2k}-\frac{k}{2}$	Remark
4	none	$n-1$ is a prime
8	none	$n-1$ is a prime
12	none	$n-1$ is a prime
16	$(3,1)$	eliminated by a computer calculation
20	none	$n-1$ is a prime
24	none	$n-1$ is a prime
28	$(3,3)$	eliminated by a computer calculation
32	none	$n-1$ is a prime
36	$(5,1)$	eliminated by a computer calculation
40	$(3,5)$	eliminated by a computer calculation
44	none	$n-1$ is a prime
48	none	$n-1$ is a prime

$\Rightarrow$ Up to order $n=50$, n and d are related by $n=2d+2$.

Symmetric C

The goal of this section

We already know:

If d is even or non-integer, then

$$C = \begin{pmatrix} d & \pm 1 & \pm 1 & \cdots & \pm 1 \\ \pm 1 & d & \pm 1 & \cdots & \pm 1 \\ \pm 1 & \pm 1 & d & & \pm 1 \\ \vdots & \vdots & & \ddots & \pm 1 \\ \pm 1 & \pm 1 & \cdots & \pm 1 & d \end{pmatrix} \in \mathbb{R}^{n,n}$$

can be circulant with mutually orthogonal rows only for $n = 2d + 2$.

In this section:

We will prove the relation $n = 2d + 2$ for odd d as well, under some condition.

Result of Johnsen

Hadamard circulant conjecture

There is no circulant Hadamard matrix of order $n > 4$.

Result of Johnsen

Hadamard circulant conjecture

There is no circulant Hadamard matrix of order $n > 4$.

Theorem (Johnsen 1964)

There is no symmetric circulant Hadamard matrix of order $n > 4$.

(I.e., the Hadamard circulant conjecture is true for symmetric matrices.)

Proof. Several proofs exist:

- Johnsen 1964
- Brualdi and Newman 1965
- McKay and Wang 1987
- Craigen and Kharaghani 1993

Generalization for symmetric C with any d

Assumptions: C is circulant with generator $(d, \pm 1, \pm 1, \ldots, \pm 1)$,
C has mutually orthogonal rows, $\quad d \geq 0, \quad n > 1$.

Theorem. If C is symmetric, then $n = 2d + 2$.

Generalization for symmetric C with any d

Assumptions: C is circulant with generator $(d, \pm 1, \pm 1, \ldots, \pm 1)$,
C has mutually orthogonal rows, $\quad d \geq 0, \quad n > 1$.

Theorem. If C is symmetric, then $n = 2d + 2$.

Proof. It suffices to consider the case $d =$ odd integer.

d is odd $\quad \Rightarrow \quad n = k(2d + k) + 1$ for some $k \in \mathbb{N}$

Generalization for symmetric C with any d

Assumptions: C is circulant with generator $(d, \pm 1, \pm 1, \ldots, \pm 1)$,
C has mutually orthogonal rows, $\quad d \geq 0, \quad n > 1$.

Theorem. If C is symmetric, then $n = 2d + 2$.

Proof. It suffices to consider the case $d =$ odd integer.

d is odd $\quad \Rightarrow \quad n = k(2d+k) + 1$ for some $k \in \mathbb{N}$

1. We prove $\boxed{n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \;\Rightarrow\; k + 1 \leq 2^r}$.

Generalization for symmetric C with any d

Assumptions: C is circulant with generator $(d, \pm 1, \pm 1, \dots, \pm 1)$,
C has mutually orthogonal rows, $\quad d \geq 0, \quad n > 1$.

Theorem. If C is symmetric, then $n = 2d + 2$.

Proof. It suffices to consider the case $d =$ odd integer.

d is odd $\quad \Rightarrow \quad n = k(2d + k) + 1$ for some $k \in \mathbb{N}$

1. We prove $\boxed{n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \;\Rightarrow\; k + 1 \leq 2^r}$.
2. $k \geq 2^7 \quad \Rightarrow \quad k + 1 > 2^r \quad \Rightarrow \quad$ no solution for $k \geq 2^7$

Generalization for symmetric C with any d

Assumptions: C is circulant with generator $(d, \pm 1, \pm 1, \ldots, \pm 1)$,
C has mutually orthogonal rows, $\quad d \geq 0, \quad n > 1$.

Theorem. If C is symmetric, then $n = 2d + 2$.

Proof. It suffices to consider the case $d =$ odd integer.

d is odd $\quad \Rightarrow \quad n = k(2d + k) + 1$ for some $k \in \mathbb{N}$

1. We prove $\boxed{n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \;\Rightarrow\; k + 1 \leq 2^r}$.
2. $k \geq 2^7 \quad \Rightarrow \quad k + 1 > 2^r \quad \Rightarrow \quad$ no solution for $k \geq 2^7$
3. $k < 2^7$: $\quad k + 1 \leq 2^r$ is satisfied in only 2 cases:
   $k = 7, n = 120; \quad k = 13, n = 924$

Generalization for symmetric C with any d

Assumptions: C is circulant with generator $(d, \pm 1, \pm 1, \ldots, \pm 1)$,
C has mutually orthogonal rows, $\quad d \geq 0, \quad n > 1$.

Theorem. If C is symmetric, then $n = 2d + 2$.

Proof. It suffices to consider the case d = odd integer.

d is odd $\quad \Rightarrow \quad n = k(2d + k) + 1$ for some $k \in \mathbb{N}$

1. We prove $\boxed{n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \;\Rightarrow\; k + 1 \leq 2^r}$.
2. $k \geq 2^7 \quad \Rightarrow \quad k + 1 > 2^r \quad \Rightarrow \quad$ no solution for $k \geq 2^7$
3. $k < 2^7$: $\quad k + 1 \leq 2^r$ is satisfied in only 2 cases:
   $k = 7, n = 120; \quad k = 13, n = 924$
4. $k = 7, n = 120$: no solution
   $k = 13, n = 924$: no solution

Matrices C for $n = 2d + 2$

The goal of this section

We already know:

Matrix

$$C = \begin{pmatrix} d & \pm1 & \pm1 & \cdots & \pm1 \\ \pm1 & d & \pm1 & \cdots & \pm1 \\ \pm1 & \pm1 & d & & \pm1 \\ \vdots & \vdots & & \ddots & \pm1 \\ \pm1 & \pm1 & \cdots & \pm1 & d \end{pmatrix}$$

can be circulant with mutually orthogonal rows only for $\underline{n = 2d + 2}$, *except for* the unresolved case, when d is odd and C is not symmetric.

In this section:

For any given d, we will explicitly find **all** such matrices C of order $n = 2d + 2$.

Observation. Let $2d \in \mathbb{N}_0$ and $n = 2d + 2$. Then

$$C = \begin{pmatrix} d & -1 & \cdots & -1 \\ -1 & d & \cdots & -1 \\ \vdots & & \ddots & \vdots \\ -1 & -1 & \cdots & d \end{pmatrix} \quad \text{has orthogonal rows.}$$

Observation. Let $2d \in \mathbb{N}_0$ and $n = 2d + 2$. Then

$$C = \begin{pmatrix} d & -1 & \cdots & -1 \\ -1 & d & \cdots & -1 \\ \vdots & & \ddots & \vdots \\ -1 & -1 & \cdots & d \end{pmatrix} \quad \text{has orthogonal rows.}$$

Theorem. If $n = 2d + 2$, C has orthogonal rows if and only if its generator takes one of the forms below:

generator	condition on d
$(d, -1, -1, \ldots, -1)$	$2d \in \mathbb{N}_0$
$(d, 1, -1, 1, -1, \ldots, -1, 1)$	$d \in \mathbb{N}_0$
$(d, 1, 1, -1, -1, \ldots, 1, 1, -1)$	d odd
$(d, -1, 1, 1, -1, \ldots, -1, 1, 1)$	d odd

Proof. 2 steps:

1. Find all matrices C satisfying $n = 2d + 2$ and

$$c_j = 1 \quad \vee \quad c_{n-j} = 1 \qquad \text{for all } j = 1, \ldots, n-1.$$

   Only 3 solutions exist:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \begin{pmatrix} 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{pmatrix}; \quad \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

Proof. 2 steps:

1. Find all matrices C satisfying $n = 2d + 2$ and

$$c_j = 1 \quad \vee \quad c_{n-j} = 1 \qquad \text{for all } j = 1, \ldots, n-1.$$

   Only 3 solutions exist:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \begin{pmatrix} 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{pmatrix}; \quad \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

2. Show that matrices C satisfying $n = 2d + 2$ and

$$\exists m \in \{1, \ldots, n-1\} : \quad c_m = c_{n-m} = -1$$

   can be constructed from the blocks found in Step 1.

Summary

Problem: Let C be a circulant matrix of order $n > 1$ with generator

$$(d, \pm 1, \pm 1, \ldots, \pm 1), \quad d \geq 0.$$

If C has orthogonal rows, find a relation between d and n.

Problem: Let C be a circulant matrix of order $n > 1$ with generator

$$(d, \pm 1, \pm 1, \ldots, \pm 1), \quad d \geq 0.$$

If C has orthogonal rows, find a relation between d and n.

Results:

- We proved that

$$\boxed{n = 2d + 2} \tag{1}$$

in each of the following cases:

Problem: Let C be a circulant matrix of order $n > 1$ with generator

$$(d, \pm 1, \pm 1, \ldots, \pm 1), \quad d \geq 0.$$

If C has orthogonal rows, find a relation between d and n.

Results:

- We proved that

$$\boxed{n = 2d + 2} \tag{1}$$

  in each of the following cases:

  - d is even integer

Problem: Let C be a circulant matrix of order $n > 1$ with generator

$$(d, \pm 1, \pm 1, \dots, \pm 1), \quad d \geq 0.$$

If C has orthogonal rows, find a relation between d and n.

Results:

- We proved that

$$\boxed{n = 2d + 2} \tag{1}$$

in each of the following cases:

  - d is even integer
  - d is half-integer

Problem: Let C be a circulant matrix of order $n > 1$ with generator

$$(d, \pm 1, \pm 1, \ldots, \pm 1), \quad d \geq 0.$$

If C has orthogonal rows, find a relation between d and n.

Results:

- We proved that

$$\boxed{n = 2d + 2} \tag{1}$$

in each of the following cases:

$$\left.\begin{array}{l} \bullet \quad d \text{ is even integer} \\ \bullet \quad d \text{ is half-integer} \\ \bullet \quad 2d \notin \mathbb{N}_0 \end{array}\right\} \quad \text{whenever } d \text{ is not an odd integer;}$$

Problem: Let C be a circulant matrix of order $n > 1$ with generator

$$(d, \pm 1, \pm 1, \ldots, \pm 1), \quad d \geq 0.$$

If C has orthogonal rows, find a relation between d and n.

Results:

- We proved that

$$\boxed{n = 2d + 2} \tag{1}$$

in each of the following cases:

$$\left.\begin{array}{l} \bullet\ \ d \text{ is even integer} \\ \bullet\ \ d \text{ is half-integer} \\ \bullet\ \ 2d \notin \mathbb{N}_0 \end{array}\right\} \quad \text{whenever } d \text{ is not an odd integer;}$$

- $n - 1$ is prime;

Problem: Let C be a circulant matrix of order $n > 1$ with generator

$$(d, \pm 1, \pm 1, \dots, \pm 1), \quad d \geq 0.$$

If C has orthogonal rows, find a relation between d and n.

Results:

- We proved that

$$\boxed{n = 2d + 2} \tag{1}$$

  in each of the following cases:

$$\left.\begin{array}{l} \bullet \ \ d \text{ is even integer} \\ \bullet \ \ d \text{ is half-integer} \\ \bullet \ \ 2d \notin \mathbb{N}_0 \end{array}\right\} \quad \text{whenever } d \text{ is not an odd integer;}$$

  - $n - 1$ is prime;
  - C is symmetric.

Problem: Let C be a circulant matrix of order $n > 1$ with generator

$$(d, \pm 1, \pm 1, \ldots, \pm 1), \quad d \geq 0.$$

If C has orthogonal rows, find a relation between d and n.

Results:

- We proved that

$$\boxed{n = 2d + 2} \tag{1}$$

  in each of the following cases:

$$\left.\begin{array}{l} \bullet \ d \text{ is even integer} \\ \bullet \ d \text{ is half-integer} \\ \bullet \ 2d \notin \mathbb{N}_0 \end{array}\right\} \quad \text{whenever } d \text{ is not an odd integer;}$$

  - $n - 1$ is prime;
  - C is symmetric.

- Conjecture: Relation (1) is valid for any diagonal value $d \geq 0$.

Problem: Let C be a circulant matrix of order $n > 1$ with generator

$$(d, \pm 1, \pm 1, \ldots, \pm 1), \quad d \geq 0.$$

If C has orthogonal rows, find a relation between d and n.

Results:

- We proved that
$$\boxed{n = 2d + 2} \tag{1}$$
in each of the following cases:
  - $\left.\begin{array}{l} \bullet\ d \text{ is even integer} \\ \bullet\ d \text{ is half-integer} \\ \bullet\ 2d \notin \mathbb{N}_0 \end{array}\right\}$ whenever d is not an odd integer;
  - $n - 1$ is prime;
  - C is symmetric.
- Conjecture: Relation (1) is valid for any diagonal value $d \geq 0$.
- We found all matrices C satisfying (1).

Thank you for your attention!