Communications in Mathematics

Daniel Uzcátegui Contreras; Dardo Goyeneche; Ondřej Turek; Zuzana Václavíková
Circulant matrices with orthogonal rows and off-diagonal entries of absolute value 1

Communications in Mathematics, Vol. 29 (2021), No. 1, 15–34

Persistent URL: http://dml.cz/dmlcz/148989

Terms of use:

© University of Ostrava, 2021

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

sciendo

Communications in Mathematics 29 (2021) 15–34
DOI: 10.2478/cm-2021-0005

©2021 D. Uzcátegui Contreras, D. Goyeneche, O. Turek, Z. Václavíková
This is an open access article licensed
under the CC BY-NC-ND 3.0

Circulant matrices with orthogonal rows and off-diagonal entries of absolute value 1

Daniel Uzcátegui Contreras, Dardo Goyeneche, Ondřej Turek, Zuzana Václavíková

Abstract. It is known that a real symmetric circulant matrix with diagonal entries $d \geq 0$, off-diagonal entries ± 1 and orthogonal rows exists only of order $2d+2$ (and trivially of order 1) [Turek and Goyeneche 2019]. In this paper we consider a complex Hermitian analogy of those matrices. That is, we study the existence and construction of Hermitian circulant matrices having orthogonal rows, diagonal entries $d \geq 0$ and any complex entries of absolute value 1 off the diagonal. As a particular case, we consider matrices whose off-diagonal entries are 4th roots of unity; we prove that the order of any such matrix with d different from an odd integer is $n = 2d+2$. We also discuss a similar problem for symmetric circulant matrices defined over finite rings $\mathbb{Z}_m$. As an application of our results, we show a close connection to mutually unbiased bases, an important open problem in quantum information theory.

2020 MSC: 15B10, 15B36, 15B05
Key words: Circulant matrix, orthogonal matrix, Hadamard matrix, mutually unbiased base
Affiliation:
Daniel Uzcátegui Contreras – Departamento de Física, Facultad de Ciencias Básicas, Universidad de Antofagasta, Casilla 170, Antofagasta, Chile
E-mail: danuzco@gmail.com
Dardo Goyeneche – Departamento de Física, Facultad de Ciencias Básicas, Universidad de Antofagasta, Casilla 170, Antofagasta, Chile
E-mail: dardo.goyeneche@uantof.cl
Ondřej Turek – Nuclear Physics Institute, Czech Academy of Sciences, 250 68 Řež, Czech Republic & Department of Mathematics, University of Ostrava, Ostrava, Czech Republic
E-mail: ondrej.turek@osu.cz
Zuzana Václavíková – Department of Mathematics, University of Ostrava, Ostrava, Czech Republic
E-mail: zuzana.vaclavikova@osu.cz

1 Introduction

A *circulant matrix* is a square matrix of order $n \in \mathbb{N}$ of the form

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

The first row, $(c_0, c_1, \ldots, c_{n-1})$, is called the *generator* of C. In this work we will denote a circulant matrix of order n having generator $(c_0, c_1, \ldots, c_{n-1})$ by $\mathrm{circ}_n(c_0, c_1, \ldots, c_{n-1})$.

Let $C = \mathrm{circ}_n(c_0, c_1, \ldots, c_{n-1})$ be a complex circulant matrix of order $n \geq 2$ satisfying the following conditions:

$$\begin{cases} c_0 = d \geq 0; \\ |c_j| = 1 \quad \text{for all } j = 1, \ldots, n-1; \\ CC^* = (d^2 + n - 1)I. \end{cases} \tag{2}$$

The aim of this paper is to examine possible orders of a matrix C obeying the above conditions for a given d. In other words, we shall examine values of d that are allowed on the main diagonal of matrices C of a given order n.

In paper [18], real matrices satisfying (2) were studied. In particular, a complete solution was obtained for the case of *symmetric* matrices. It was proved that the order of a symmetric matrix C is related with the diagonal value d by the formula $n = 2d+2$. In the present work we discuss extensions of the results in two directions:

- complex Hermitian matrices;
- symmetric matrices with entries defined over finite rings $\mathbb{Z}_m$.

Note that a complex *non-Hermitian* matrix C satisfying (2) with a given $d \geq 0$ trivially exists for every $n \leq 2d + 2$. Indeed, consider

$$C = \mathrm{circ}_n(d, -\mathrm{e}^{\mathrm{i}\alpha}, -\mathrm{e}^{\mathrm{i}\alpha}, \ldots, -\mathrm{e}^{\mathrm{i}\alpha}).$$

Then CC^* is a circulant matrix with generator

$$(d^2 + n - 1, n - 2 - 2d\cos\alpha, n - 2 - 2d\cos\alpha, \ldots, n - 2 - 2d\cos\alpha);$$

so every $n \leq 2d+2$ allows to set $\alpha = \arccos\frac{n-2}{2d}$ to obtain a matrix C satisfying (2). On the other hand, the question becomes hard for orders $n > 2d + 2$.

Our object of study has a close relation with *polyphase sequences* [10], [15], that is, n-tuple sequences of complex numbers having the form ω^k, where $\omega = \exp\left(\frac{2\pi\mathrm{i}}{n}\right)$ is the main nth root of the unity. Among the entire set of polyphase sequences there is a relevant subset given by *perfect autocorrelation sequences*, which are characterized by having zero autocorrelation function [10]. Let us recall

that for a sequence $\mathbf{a} = (a_0, a_1, ..., a_{n-1})$, whose elements satisfy $a_i = a_{i+\nu}$, the autocorrelation function $\theta_{\mathbf{a}}(\nu)$ is defined as

$$\theta_{\mathbf{a}}(\nu) = \sum_{i=0}^{n-1} a_i a_{i+\nu}^* \,, \tag{3}$$

where ν is called the shift or period and $i + \nu$ is computed modulo n [3]. In a sense, the autocorrelation function quantifies how much a sequence differs from its cyclic shifts of entries. Polyphase sequences having perfect autocorrelation are one-to-one connected with generators g of matrices C having order n satisfying conditions (2) for the special case of $d = 1$ and nth roots of the unity in its entries. These sequences have practical applications in several fields, for example in communication and radar systems [8], [12], [14], [20]. Therefore, construction of perfect sequences of length n has been extensively studied (cf. [4], [10], [13], [14] and references therein).

2 Preliminaries

A circulant matrix C of order n has normalized eigenvectors $v_0, v_1, \ldots, v_{n-1}$ given as

$$v_k = \frac{1}{\sqrt{n}} \left(1, \omega^k, \omega^{2k}, \ldots, \omega^{(n-1)k}\right)^T \,,$$

where $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$. The associated eigenvalues are

$$\lambda_k = c_0 + c_1\omega^k + c_2\omega^{2k} + \cdots + c_{n-1}\omega^{(n-1)k} \,, \tag{4}$$

where $(c_0, c_1, \ldots, c_{n-1})$ is the generator of C.

The vectors $(c_0, c_1, \ldots, c_{n-1})^T$ and $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})^T$ are related by the discrete Fourier transform; the inverse transform gives the generator in terms of the eigenvalues as follows:

$$c_j = \frac{1}{n} \left(\lambda_0 + \lambda_1\omega^{-j} + \lambda_2\omega^{-2j} + \cdots + \lambda_{n-1}\omega^{-(n-1)j}\right). \tag{5}$$

Throughout the paper, we will index the rows and columns of the matrix C by integers from 0 to $n - 1$ (instead of from 1 to n).

3 Hermitian solutions over $\mathbb{C}$

First of all, let us observe that for each $n \geq 2$ there exists a Hermitian circulant matrix satisfying (2) with main diagonal $d = \frac{n}{2} - 1$.

Proposition 1. *A Hermitian circulant matrix*

$$C = \mathrm{circ}_n \left(\frac{n}{2} - 1, -\omega^{\nu}, -\omega^{2\nu}, \ldots, -\omega^{(n-1)\nu}\right)$$

where $\omega = \mathrm{e}^{2\pi \mathrm{i}/n}$ *satisfies conditions* (2) *for every* $n \geq 2$ *and every* $\nu \in \mathbb{Z}_n$. *In particular, the choice* $\nu = 0$ *gives a real symmetric solution*

$$C = \mathrm{circ}_n \left(\frac{n}{2} - 1, -1, -1, \ldots, -1\right) .$$

Proof. From equation (4), eigenvalues of C can be written in term of entries c_j as follows:

$$\lambda_k = \sum_{j=0}^{n-1} c_j \omega^{jk} = \frac{n}{2} - 1 + \sum_{j=1}^{n-1} (-\omega^{j\nu})\omega^{jk} = \frac{n}{2} - 1 - \sum_{j=0}^{n-1} \omega^{j(\nu+k)} + 1$$
$$= \frac{n}{2} - n\,\delta_{\nu+k,0}\,. \quad (6)$$

This equation becomes either $\lambda_k = \frac{n}{2}$ or $\lambda_k = \frac{n}{2} - n = -\frac{n}{2}$ for $\nu + k \neq 0$ or $\nu + k = 0$, respectively. Thus $CC^* = \left(\frac{n}{2}\right)^2 I = \left(\left(\frac{n}{2} - 1\right)^2 + n - 1\right)^2 I$, so C satisfies conditions (2) for every $\nu \in \mathbb{Z}_n$. □

Let us now examine the situation of a general $d \geq 0$. We will distinguish matrices of even and odd orders.

3.1 Matrices C of even orders

Proposition 2. *If a Hermitian circulant matrix C of an even order n satisfies* (2)*, then*

(i) there exists a positive integer $k \leq \frac{n}{2\sqrt{n-1}}$ such that

$$\sqrt{d^2 + n - 1} = \frac{n}{2k}\,; \quad (7)$$

(ii) d is rational;

(iii) $d \leq \frac{n}{2} - 1$.

Proof. Since C is Hermitian and satisfies $C^2 = (d^2 + n - 1)I$, the eigenvalues of C are $\sqrt{d^2 + n - 1}$ and $-\sqrt{d^2 + n - 1}$. Let us denote their multiplicities by ν and $n - \nu$, respectively. The sum of eigenvalues is equal to the trace of C, i.e.,

$$\nu\sqrt{d^2 + n - 1} - (n - \nu)\sqrt{d^2 + n - 1} = nd\,. \quad (8)$$

Hence

$$\left(\nu - \frac{n}{2}\right)\sqrt{d^2 + n - 1} = \frac{n}{2}d\,. \quad (9)$$

Now we will use an idea from [6, proof of Theorem 8]. Since C is Hermitian, its generator has the form $(d, c_1, \ldots, c_{\frac{n}{2}-1}, c_{\frac{n}{2}}, \overline{c_{\frac{n}{2}-1}}, \ldots, \overline{c_1})$, where $c_{\frac{n}{2}} \in \mathbb{R}$. Let M be a circulant matrix with the generator

$$(c_{\frac{n}{2}}, \overline{c_{\frac{n}{2}-1}}, \ldots, \overline{c_1}, d, c_1, \ldots, c_{\frac{n}{2}-1})\,.$$

Note that M is Hermitian and satisfies $M = CP$, where $P = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$ is a permutation matrix. Therefore,

$$M^2 = MM^* = (CP)(CP)^* = CPP^*C^* = CC^* = (d^2 + n - 1)I\,.$$

Consequently, M has eigenvalues $\sqrt{d^2+n-1}$ and $-\sqrt{d^2+n-1}$; we denote their multiplicities by μ and $n-\mu$, respectively. The sum of eigenvalues of M must be equal to the trace of M, so

$$\mu\sqrt{d^2+n-1} - (n-\mu)\sqrt{d^2+n-1} = nc_{\frac{n}{2}}\,. \tag{10}$$

Recall that $c_{\frac{n}{2}}$ is real due to the hermiticity of M. At the same time $|c_{\frac{n}{2}}| = 1$ by (2). Hence $c_{\frac{n}{2}} = \pm 1$, and equation (10) implies

$$\left|\mu - \frac{n}{2}\right| \sqrt{d^2+n-1} = \frac{n}{2}\,. \tag{11}$$

We denote $k := \left|\mu - \frac{n}{2}\right|$. By definition of μ, k is an integer from $\left[0, \frac{n}{2}\right]$. The value $k=0$ is forbidden by (11). Values $k > \frac{n}{2\sqrt{n-1}}$ would imply $\sqrt{d^2+n-1} < \sqrt{n-1}$, which is impossible. So $1 \le k \le \frac{n}{2\sqrt{n-1}}$.

(ii) Since $\sqrt{d^2+n-1} = \frac{n}{2k} \in \mathbb{Q}$, equation (9) gives $d \in \mathbb{Q}$.

(iii) Applying statement (i), one gets

$$d = \sqrt{\left(\frac{n}{2k}\right)^2 - n + 1} \le \sqrt{\left(\frac{n}{2}\right)^2 - n + 1} = \frac{n}{2} - 1\,. \qquad \square$$

Note that the value $k=1$ in Proposition 2(i) corresponds to $d = \frac{n}{2} - 1$, for which a Hermitian circulant matrix C always exists – see Proposition 1.

The statement of Proposition 2 can be strengthened in the special case when d is integer:

Proposition 3. *Let a Hermitian circulant matrix C of an even order n satisfy* (2) *with an integer d. Let us denote*

$$\ell := \sqrt{d^2+n-1}\,. \tag{12}$$

Then we have:

(i) ℓ is integer (in other words, d^2+n-1 is a perfect square).

(ii) $\ell \mid \frac{n}{2}$.

(iii) $\ell \mid (d^2-1)$. In particular, if d is odd, then $\ell \mid \frac{d^2-1}{2}$.

(iv) If $n-1$ is prime, then $d = \frac{n}{2} - 1$.

Proof. (i) If d is integer, then $\ell = \sqrt{d^2+n-1}$ is obviously either integer or irrational. But ℓ cannot be irrational by Proposition 2(i); so ℓ is integer.

(ii) Since ℓ is integer by (i), the statement $\ell \mid \frac{n}{2}$ immediately follows from Proposition 2(i).

(iii) Equation (12) implies $d^2 - 1 = \ell^2 - n$. Since $\ell \mid n$ by (ii) and obviously $\ell \mid \ell^2$, we have $\ell \mid (d^2-1)$. In particular, if d is odd, then d^2+n-1 is even, so ℓ is even. Thus $2\ell \mid \ell^2$. At the same time $2\ell \mid n$ by (ii), so $2\ell \mid (\ell^2 - n)$. Hence $2\ell \mid (d^2-1)$ due to $d^2 - 1 = \ell^2 - n$.

(iv) Statement (i) implies that $n-1 = \ell^2 - d^2 = (\ell-d)(\ell+d)$ for some integer $\ell \ge 0$. If $n-1$ is prime, then necessarily $\ell - d = 1$; hence $\ell + d = \ell - d + 2d = 1 + 2d$, and so $n - 1 = 1 \cdot (1+2d)$. Consequently, $n = 2 + 2d$, thus $d = \frac{n}{2} - 1$. $\square$

Proposition 3 has a series of consequences, which will be formulated below as Corollaries 1, 2 and 3.

Definition 1. A complex square matrix C of order n is called a complex *conference matrix* if all its diagonal entries are 0, its off-diagonal entries are of absolute value 1, and $CC^* = (n-1)I$.

Corollary 1. *A Hermitian circulant conference matrix of an even order $n \geq 2$ exists only for $n = 2$.*

Proof. Let a conference matrix C satisfy the assumptions, i.e., C is a Hermitian circulant matrix obeying (2) with $d = 0$ and an even $n \geq 2$. Then Proposition 3(iii) implies $\ell \mid -1$; so $|\ell| = 1$. Hence, by (12), we have $\sqrt{n-1} = 1$; thus $n = 2$. □

Definition 2. A complex square matrix H of order n is called a complex *Hadamard matrix* if all its entries are of absolute value 1 and $HH^* = nI$.

Corollary 2. *A Hermitian circulant Hadamard matrix of an even order $n \geq 2$ exists only if n is a square of an even integer.*

Proof. The statement follows immediately from Proposition 3(i) with $d = 1$. □

Remark 1. Corollary 2 concerns Hermitian circulant complex Hadamard matrices with off-diagonal entries being any complex units (i.e., $|c_j| = 1$ for all $j = 1, \ldots, n-1$). Let us note that if the off-diagonal entries are restricted to 4th roots of unity, i.e., $c_j \in \{1, -1, \mathrm{i}, -\mathrm{i}\}$ for all $j = 1, \ldots, n$, it is known that no such matrix of order $n > 4$ exists (see Craigen and Kharaghani [5]). Matrices C with off-diagonal entries from $\{1, -1, \mathrm{i}, -\mathrm{i}\}$ and general diagonal values $d \geq 0$ will be further discussed in Section 3.3.

Corollary 3. *Consider a Hermitian circulant matrix C satisfying (2) with an integer d. If $n/2$ is prime, then $n = 2d + 2$.*

Proof. If d is integer and $n/2 = p$ is a prime number, then from Proposition 3(ii) we have $\ell = 1$ or $\ell = p$, where $\ell = \sqrt{d^2 + 2p - 1}$. The case $\ell = 1$ cannot occur, as it leads to $1 = \sqrt{d^2 + 2p - 1}$, which is impossible for any prime p. So $\ell = p = n/2$, which implies $d^2 = \left(\frac{n}{2} - 1\right)^2$; hence $d = \frac{n}{2} - 1$. □

Now we will extend the result of Corollary 3 in two ways (Propositions 4 and 5).

Proposition 4. *Let C be a Hermitian circulant matrix satisfying (2) with an integer d. If $n/2$ is a product of two primes, then $n = 2d + 2$.*

Proof. Let $n/2 = pq$ for p, q being primes. Then (12) gives

$$\ell = \sqrt{d^2 + 2pq - 1}\,. \tag{13}$$

We may assume $p \leq q$ without loss of generality. Proposition 3(ii) gives $\ell \mid pq$; hence $\ell \in \{1, p, q, pq\}$. If $\ell = pq$, equation (13) leads to $d = pq - 1 = \frac{n}{2} - 1$, i.e.,

$n = 2d+2$. Case $\ell = 1$ cannot occur, because the right hand side of (13) is greater than 1 for any two primes p, q. Similarly, $\ell = q$ is not possible, because (13) gives $d = \sqrt{q^2 - 2pq + 1}$, where $q^2 - 2pq + 1 \leq 1 - q^2 < 0$ due to the assumption $p \leq q$. In the following we demonstrate that the case $\ell = p$ is impossible as well. If $\ell = p$, equation (13) implies $p^2 = d^2 + 2pq - 1$, so

$$d^2 = (p-q)^2 - q^2 + 1\,.$$

Hence $p - q > d$. Denoting the difference $p - q - d$ by an integer variable $k > 0$, one can rewrite the last equation as follows:

$$(q+k+1)(q+k-1) = 2kp\,.$$

Thus $2k \mid (q+k+1)(q+k-1)$. Let $2k = a \cdot b$ for $a \mid (q+k+1)$ and $b \mid (q+k-1)$. Then

$$p = \frac{q+k+1}{a} \cdot \frac{q+k-1}{b}\,.$$

Since p is prime, necessarily $\frac{q+k+1}{a} = 1$ or $\frac{q+k-1}{b} = 1$.

- If $\frac{q+k+1}{a} = 1$, we have $b = \frac{2k}{a} = \frac{2k}{q+k+1} < 2$; thus $b = 1$. Therefore, $q+k-1 = 1$, which can never be true for an integer $k > 0$ and prime q.
- If $\frac{q+k-1}{b} = 1$, we have $a = \frac{2k}{b} = \frac{2k}{q+k-1} \leq \frac{2k}{1+k} < 2$; hence $a = 1$. Thus $q+k+1 = 1$, which is again false for any positive integer $k > 0$ and prime q.

□

In the following proposition, we omit the cases $d = 0$ and $d = 1$ that were treated generally in Corollaries 1 and 2.

Proposition 5. *Let C be a Hermitian circulant matrix satisfying* (2) *with an integer $d \geq 2$. If $n/2$ is a power of a prime, then $n = 2d + 2$.*

Proof. Let $n/2 = p^m$ for p being prime and m being a non-negative integer. Proposition 3(ii) implies that $\ell \mid p^m$; hence $\ell = p^j$ for $0 \leq j \leq m$. By (12) we have $\ell = \sqrt{d^2 + 2p^m - 1}$; i.e., $p^{2j} = d^2 + 2p^m - 1$. Consequently,

$$p^{2j} - 2p^m = d^2 - 1\,. \tag{14}$$

Note that $d^2 - 1 > 0$ because of the assumption $d \geq 2$. Now we distinguish $p = 2$ and $p \geq 3$.

- If $p = 2$, the left hand side of equation (14) takes the form

$$2^{2j} - 2 \cdot 2^m = 2^{2j} - 2^{m+1} = 2^{m+1}(2^{2j-m-1} - 1)\,; \tag{15}$$

  so (14) with its right hand side $d^2 - 1 > 0$ can be satisfied only if $2j - m - 1 > 0$ and $2^{m+1} \mid (d-1)(d+1)$. Thus both $d-1$ and $d+1$ are even. Since one of any two consecutive even numbers must be oddly even, we have two possibilities:

$$(d - 1 = 2a \ \wedge\ d + 1 = 2^m b) \quad \text{or} \quad (d - 1 = 2^m a \ \wedge\ d + 1 = 2b)\,,$$

  where both a, b are odd. So $2^m \mid (d+1)$ or $2^m \mid (d-1)$. Thus in either case we have $2^m \leq d + 1$. Recalling that $2^m = \frac{n}{2}$, we obtain $\frac{n}{2} \leq d + 1$. This inequality together with Proposition 2(iii) gives $n = 2d + 2$.

- If $p \geq 3$, we rewrite (14) as follows:

$$p^m(p^{2j-m} - 2) = (d-1)(d+1)\,. \tag{16}$$

Since $d-1$ and $d+1$ obviously cannot be both divisible by $p \geq 3$, we infer that

$$p^m \mid (d-1) \quad \text{or} \quad p^m \mid (d+1)\,.$$

Therefore, in either case we have $p^m \leq d+1$. Since $p^m = \frac{n}{2}$, we have $\frac{n}{2} \leq d+1$. Together with Proposition 2(iii), we get $n = 2d+2$. □

Remark 2. Let us emphasize that Proposition 3, Corollary 3 and Propositions 4 and 5 concern circulant matrices C obeying (2) with an *integer* on the main diagonal. They have no implications on matrices C with non-integer values d.

Example 1. Let us consider various integer values of $d \geq 2$, for which we will find necessary conditions on n using Proposition 3.

- $d = 2$: $n+3$ must be a square and $\sqrt{n+3} \mid 3$. The only even solution is $n = 6$.
- $d = 3$: $n+8$ must be a square and $\sqrt{n+8} \mid 4$. The only even solution is $n = 8$.
- $d = 4$: $n+15$ must be a square and $\sqrt{n+15} \mid 15$. The only even solutions are $n = 10$ and $n = 210$.
- $d = 5$: $n+24$ must be a square and $\sqrt{n+24} \mid 12$. The only even solutions are $n = 12$ and $n = 120$.

Proposition 1 implies that the matrices C of orders $n = 2d+2$ (i.e., those with $(d,n) \in \{(2,6),(3,8),(4,10),(5,12)\}$) exist. Recall that a matrix

$$C = \mathrm{circ}_{2d+2}(d,-1,-1,\ldots,-1)$$

obeys (2). On the other hand, the existence of matrices C with $(d,n) \in \{(4,210),(5,120)\}$ is open.

Example 2. In this example we shall consider various even values of n, for which we will find necessary conditions on d using Proposition 2.

- $n \leq 14$: The condition $k \leq \frac{n}{2\sqrt{n-1}}$ from Proposition 2(i) gives $k < 2$. Hence $k = 1$, so $d = \frac{n}{2} - 1$ is the only possible value of d.
- $n = 16$: The condition $k \leq \frac{n}{2\sqrt{n-1}} = \frac{16}{2\sqrt{15}}$ implies $k = 1$ or $k = 2$. The value $k = 1$ gives the trivial solution $d = \frac{n}{2} - 1 = 7$. Equation (7) with the value $k = 2$ leads to $d = 1$; this case is disproved by numerical simulations (see Appendix A where all possible diagonal values $d < \frac{n}{2} - 1$ for matrices C of orders n up to $n = 22$ are listed).

- $n = 18$: $k \leq \frac{n}{2\sqrt{n-1}} = \frac{18}{2\sqrt{17}}$ implies $k = 1$ or $k = 2$. The value $k = 1$ gives the trivial solution $d = \frac{n}{2} - 1 = 8$. Equation (7) with the value $k = 2$ leads to $d = \frac{\sqrt{13}}{2} \notin \mathbb{Q}$, which is impossible by Proposition 2(ii).
- $n = 20$: $k \leq \frac{n}{2\sqrt{n-1}} = \frac{20}{2\sqrt{19}}$ implies $k = 1$ or $k = 2$. The value $k = 1$ gives $d = \frac{n}{2} - 1 = 9$, $k = 2$ leads to $d = \sqrt{6} \notin \mathbb{Q}$. So the only possible value of d is $d = 9$.
- $n \in \{22, 24, \ldots, 100\}$: Similarly as above, one obtains mostly either trivial solutions $d = \frac{n}{2} - 1$ or forbidden values $d \notin \mathbb{Q}$, with the following 9 exceptions:

n	d	n	d	n	d
36	1	64	1	78	17/4
40	7/3	66	7/4	96	7
56	17/3	70	11/4	100	1

The existence of matrices C for the 9 combinations of n and d in the above table is open.

3.2 Matrices C of odd orders

In case of odd n, as well as in case of those even n that cannot be completely resolved using tools from Section 3.1, we searched for allowed values of d numerically using the following idea. Since C is Hermitian and satisfies $C^2 = (d^2 + n - 1)I$, the eigenvalues of C are $\pm\sqrt{d^2 + n - 1}$. Taking vectors $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ with entries $\pm\sqrt{d^2 + n - 1}$, we calculated the terms of the corresponding generator $(c_0, c_1, \ldots, c_{n-1})$ using formula (5). Then we checked whether the values c_j obey conditions (2), i.e., $|c_j| = 1$ for all $j = 1, \ldots, n-1$. In this way we found all allowed values of d that satisfy conditions (2) up to $n = 22$. The results for odd orders n are summarized in Table 1.

n	d	n	d
3	$\frac{1}{2}$	13	$\frac{11}{2}$, $\frac{5}{2\sqrt{3}}$
5	$\frac{3}{2}$	15	$\frac{13}{2}$, $\frac{1}{4}$
7	$\frac{5}{2}$, $\frac{1}{2\sqrt{2}}$	17	$\frac{15}{2}$
9	$\frac{7}{2}$	19	$\frac{17}{2}$, $\frac{1}{2\sqrt{5}}$
11	$\frac{9}{2}$, $\frac{1}{2\sqrt{3}}$	21	$\frac{19}{2}$, $\frac{11}{4}$

Table 1: Numerical results for odd order n.

The main difference between the even and odd order n is that for even n diagonal values d have to be rational, whereas they can be irrational for odd n. In

Appendix A we present examples of the generators associated to values n from 2 to 22 with the main diagonal d different from $\frac{n}{2}-1$ which were found by the method described above. (Recall that a solution with $d=\frac{n}{2}-1$ always exists – see Proposition 1.)

3.3 Matrices C with off-diagonal entries from $\{1,-1,\mathrm{i},-\mathrm{i}\}$

Let us now discuss a special case of complex circulant matrices satisfying (2) with off-diagonal entries being 4th roots of unity, i.e., $c_j \in \{1,-1,\mathrm{i},-\mathrm{i}\}$ for all $j=1,\dots,n-1$. As recalled in Remark 1, Craigen and Kharaghani proved that Hadamard matrices (satisfying (2) for $d=1$) of this type exist only of order $n=4$ (and trivially $n=1$). In this section we extend their result to any d that is not an odd integer, showing that the order of such matrix C is necessarily $n=2d+2$. Furthermore, if a generalization of the circulant Hadamard conjecture proposed in [18] is true, the necessary condition $n=2d+2$ applies on matrices C with odd diagonal values $d\geq 0$ as well.

Theorem 1. *If $d\geq 0$ is not an odd integer, then a Hermitian circulant matrix $C=\mathrm{circ}_n(c_0,c_1,\dots,c_{n-1})$ ($n\geq 2$) satisfying (2) with off-diagonal entries $c_j\in\{1,-1,\mathrm{i},-\mathrm{i}\}$ exists only of order $n=2d+2$. Moreover, C is real and takes the form*

- $C=\mathrm{circ}_{2d+2}(d,-1,-1,\dots,-1)$ *or* $C=\mathrm{circ}_{2d+2}(d,1,-1,1,-1,1,\dots,-1,1)$ *for even d;*
- $C=\mathrm{circ}_{2d+2}(d,-1,-1,\dots,-1)$ *for d being half-integer.*

Proof. We start the proof similarly as Craigen and Kharaghani in [5, Thm. 7]. Let us write the circulant matrix C satisfying the assumptions as $C=A+\mathrm{i}B$, where A,B are real matrices. Then both A and B are circulant matrices, A is symmetric, B is skew-symmetric. Let us denote $M=A+B$; then M is a circulant matrix satisfying

$$MM^T=(A+B)(A-B)=A^2-B^2$$

(recall that A,B are circulant matrices, so they commute). Since

$$CC^*=(A+\mathrm{i}B)(A+\mathrm{i}B)=A^2-B^2+2\mathrm{i}AB=(d^2+n-1)I\,,$$

we have $AB=0$ and $A^2-B^2=(d^2+n-1)I$. So $MM^T=(d^2+n-1)I$. To sum up, M is a real circulant matrix satisfying (2). Now, taking advantage of results of [18], we have:

- $2d$ must be integer; thus M exists only for d being half-integer or integer (and so does C) [18, Prop. 3.1];
- if d is half-integer, then $n=2d+2$ [18, Prop. 3.1] and

$$M=\mathrm{circ}_{2d+2}(d,-1,-1,\dots,-1)$$

[18, Rem. 3.2];

- if d is even integer, then $n = 2d + 2$ [18, Thm. 3.5] and M is symmetric [18, Prop. 3.4]. Moreover, the value n is oddly even, thus [18, Sect. 5] implies that M has one of the forms

$$M = \operatorname{circ}_n\left(\frac{n}{2} - 1, -1, -1, \ldots, -1\right) = \operatorname{circ}_{2d+2}(d, -1, -1, \ldots, -1),$$
$$M = \operatorname{circ}_n\left(\frac{n}{2} - 1, 1, -1, 1, -1, 1, \ldots, -1, 1\right)$$
$$= \operatorname{circ}_{2d+2}(d, 1, -1, 1, -1, 1, \ldots, -1, 1)\,.$$

Finally, since M is symmetric in all cases, we conclude that $B = 0$; hence $C = A = M$ is real. □

Remark 3. It was conjectured in [18, Conjecture 3.6] that real circulant matrices of order $n \geq 2$ satisfying (2) with odd values $d > 0$ exist only for $n = 2d + 2$ as well. This is a generalization of the *circulant Hadamard conjecture* stating that there a real circulant Hadamard matrix exists only of order $n = 4$ (and trivially of order $n = 1$). If the generalized conjecture is true, one can extend the argument in the proof of Theorem 1 to odd $d > 0$ as well, obtaining that a Hermitian circulant matrix C satisfying (2) with an odd $d > 0$ and off-diagonal entries $c_j \in \{1, -1, \mathrm{i}, -\mathrm{i}\}$ exists only of order $n = 2d + 2$. Moreover, we know from [18, Sect. 5] that any real circulant matrix M satisfying (2) with an odd d and $n = 2d + 2$ (so n is a multiple of 4) has one of the forms

$$\operatorname{circ}_{2d+2}(d, -1, -1, \ldots, -1)\,,$$
$$\operatorname{circ}_{2d+2}(d, 1, -1, 1, -1, 1, \ldots, -1, 1)\,,$$
$$\operatorname{circ}_{2d+2}(d, 1, 1, -1, -1, 1, 1, -1, -1, \ldots, 1, 1, -1)\,,$$
$$\operatorname{circ}_{2d+2}(d, -1, 1, 1, -1, -1, 1, 1, -1, \ldots, -1, 1, 1)\,.$$

Hence we obtain, similarly as in the proof of Theorem 1, that the matrix C can be either real, taking one of the forms

$$\operatorname{circ}_{2d+2}(d, -1, -1, \ldots, -1)\,,$$
$$\operatorname{circ}_{2d+2}(d, 1, -1, 1, -1, 1, \ldots, -1, 1)\,,$$

or complex taking one of the forms

$$\operatorname{circ}_{2d+2}(d, \mathrm{i}, 1, -\mathrm{i}, -1, \mathrm{i}, 1, -\mathrm{i}, -1, \ldots, \mathrm{i}, 1, -\mathrm{i})\,,$$
$$\operatorname{circ}_{2d+2}(d, -\mathrm{i}, 1, \mathrm{i}, -1, -\mathrm{i}, 1, \mathrm{i}, -1, \ldots, -\mathrm{i}, 1, \mathrm{i})$$

(notice that the last two matrices are conjugate transposes to each other).

4 Circulant matrices over $\mathbb{Z}_m$

In this section we will briefly consider circulant matrices C satifying conditions (2) with entries c_j being elements of the ring $\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$ for some m. In this particular case, the condition $|c_j| = 1$ is meant as $c_j \equiv 1 \pmod m$ or $c_j \equiv -1 \equiv m - 1 \pmod m$.

First of all, note the following fact:

Remark 4. For any $C = \mathrm{circ}_n(d, c_1, c_2, \ldots, c_{n-1})$ over $\mathbb{Z}_m$ such that

$$C \cdot C^T = (d^2 + n - 1)I\,,$$

the matrix $-C = \mathrm{circ}_n(m - d, -c_1, -c_2, \ldots, -c_{n-1})$ fulfills the same condition.

Proposition 6. *Let $C = \mathrm{circ}_n(d, c_1, c_2, \ldots, c_{n-1})$ be defined over $\mathbb{Z}_m$ with $c_i \equiv \pm 1 \pmod m$. If m is even, then n is also even.*

Proof. The dot product of any two distinct rows is sum of n terms, of which $n-2$ are equal to ± 1 and the other two are $\pm d$. Thus the sum is even if n is even and odd if n is odd. Hence if m is even, n must be too. □

Remark 5. The converse implication of Proposition 6 does not hold. For example, consider $C = \mathrm{circ}_4(2, 1, 1, 1)$ over $\mathbb{Z}_3$. In this case $n = 4$ is even and $m = 3$ is odd, and for this matrix $C \cdot C^T = I$.

4.1 Odd n

If a circulant matrix C is defined over $\mathbb{R}$, satisfies the conditions (2) and its order n is odd, then the generator of C is $(\frac{n}{2} - 1, -1, \ldots, -1)$, so the matrix C has to be symmetric. This follows from [18, Prop. 3.1 and Sect. 5].

If C of an odd order n is defined over $\mathbb{Z}_m$, the situation is different. There exist non-symmetric matrices C satisfying conditions (2). Consider for example the matrix $C = \mathrm{circ}_9(1, 1, 1, 1, 1, 1, 1, 1, -1)$ over $\mathbb{Z}_5$ is not symmetric and satisfies (2).

4.2 Symmetric matrices

If C is a symmetric matrix over $\mathbb{Z}_m$, i.e., $c_k = c_{n-k}$, where the subscripts are interpreted modulo n, the condition $C \cdot C^T = (d^2 + n - 1)I$ leads to

$$2c_0c_k + \sum_{\substack{j=1 \\ j\neq k}}^{n-1} c_j \cdot c_{n-k+j} \equiv 0 \pmod m$$

for all $k = 1, \ldots, n-1$ (subscripts are interpreted modulo n), i.e.,

$$2dc_k + \sum_{\substack{j=1 \\ j\neq k}}^{n-1} c_j \cdot c_{n-k+j} \equiv 0 \pmod m\,.$$

Note that due to the symmetry, it is sufficient to verify this condition for $k = 1, \ldots, \lceil \frac{n}{2} \rceil + 1$.

4.2.1 Matrices with the generator $(d, -1, -1, \ldots, -1)$

In analogy with Proposition 1, we can formulate the following statement:

Proposition 7. *A symmetric circulant matrix C over $\mathbb{Z}_m$ satisfying (2) exists for each n and d such that $n \equiv 2d + 2 \mod m$.*

Proof. Consider the matrix $C = \mathrm{circ}_n(d, -1, -1, \ldots, -1)$ over $\mathbb{Z}_m$. The condition $C \cdot C^T = (d^2 + n - 1)I$ leads to

$$2d - \sum_{j=1, j\neq k}^{n-1} 1 \equiv 0 \pmod{m},$$

i.e.,

$$2d - n + 2 \equiv 0 \pmod{m},$$

which is equivalent to $n \equiv 2d + 2 \pmod{m}$. □

Example 3. In the special case when $n = m + 2$ and m is odd, any matrix of the type

$$\mathrm{circ}_{m+2}(0, -1, \ldots, -1)$$

over $\mathbb{Z}_m$ fulfills the condition (2). If $n = m + 2$ and m is even, then any matrix of the type

$$\mathrm{circ}_{m+2}(0, -1, \ldots, -1),$$

$$\mathrm{circ}_{m+2}(\frac{m}{2}, -1, \ldots, -1)$$

over $\mathbb{Z}_m$ fulfills the condition (2).

Example 4. If $m = 2$, i.e., for C defined over $\mathbb{Z}_2$, the congruence

$$2d - n + 2 \equiv 0 \mod 2$$

is trivially fulfilled for any even n and any d. So both matrices

$$\mathrm{circ}_{2k}(0, -1, \ldots, -1),$$

$$\mathrm{circ}_{2k}(1, -1, \ldots, -1)$$

over $\mathbb{Z}_2$ fulfill the conditions (2). A matrix C over $\mathbb{Z}_2$ of an odd order n satisfying (2) does not exist, in keeping with Proposition 6.

Remark 6. Because $1 \equiv -1 \pmod 2$, for matrices over $\mathbb{Z}_2$ there is no difference between $c_i = 1$ and $c_i = -1$. Therefore, Example 4 implies that any circulant matrix C of an even order n over $\mathbb{Z}_2$ with off-diagonal entries ± 1 obeys conditions (2).

4.2.2 An example of a matrix C that does not fulfill the conditions over $\mathbb{R}$ but fulfills them over $\mathbb{Z}_m$

By [18], a symmetric circulant matrix C over $\mathbb{R}$ satisfies conditions (2) only if its generator is $(d, -1, -1, \ldots, -1)$ or $(d, -1, +1, -1, +1, \ldots, -1)$. Let us demonstrate that this necessary condition does not extend to matrices C defined over $\mathbb{Z}_m$. We will construct an example of a symmetric circulant matrix C that does not fulfills the conditions (2) over $\mathbb{R}$, but fulfills them over $\mathbb{Z}_m$.

Let $C = \mathrm{circ}_n(d, c_1, c_2, \ldots, c_{n-1})$ be defined over $\mathbb{Z}_m$, where n is even, $c_{\frac{n}{2}} = 1 \pmod m$ and $c_i = -1 \pmod m$ for all $i \neq \frac{n}{2}$. I.e., the generator of C is

$$(d, \underbrace{-1, \ldots, -1}_{\frac{n}{2}-1 \text{ terms}}, 1, \underbrace{-1, \ldots, -1}_{\frac{n}{2}-1 \text{ terms}}) . \tag{17}$$

The dot product of the 0-th row and the k-th row of C is

$$2dc_k + \sum_{\substack{j=1 \\ j \neq k}}^{n-1} c_j \cdot c_{n-k+j} \,, \tag{18}$$

where the subscripts are interpreted modulo n. So for $k \neq \frac{n}{2}$, (18) is equal to $2d - (n-4) + 2$, and for $k = \frac{n}{2}$, (18) gives $2d - (n-2)$.

Therefore, the condition $C \cdot C^T = (d^2 + n - 1)I$ requires the following two congruences to be fulfilled:

$$2d \equiv -n + 2 \pmod m \qquad \wedge \qquad 2d \equiv n - 6 \pmod m . \tag{19}$$

In examples below, we will consider explicit solutions.

Example 5. Let C of an even order n defined over $\mathbb{Z}_m$ satisfy (17) and $m \mid n$. Then from the congruences we have $0 \equiv 8 \mod m$, so $m = 2, 4$, or 8. We will describe each situation separately.

1. For $m = 2$, already examined in Section 4.2.1, any matrix C over $\mathbb{Z}_2$ with even n such that $(m \mid n)$ of the type

   $$\mathrm{circ}_{2k}(d, -1, \ldots, -1, 1, -1, \ldots, -1) = \mathrm{circ}_{2k}(d, 1, \ldots, 1, 1, 1, \ldots, 1)$$

   with $k \in \mathbb{N}$ fulfills the conditions (2).

2. For $m = 4$ we get $d = 1 \text{ or } 3$, so any matrix C over $\mathbb{Z}_4$ of the type

   $$\mathrm{circ}_{4k}(1, -1, \ldots, -1, 1, -1, \ldots, -1)$$

   $$\mathrm{circ}_{4k}(3, -1, \ldots, -1, 1, -1, \ldots, -1)$$

   with $k \in \mathbb{N}$ fulfills the conditions (2).

3. For $m = 8$ we have $d = 1 \text{ or } 5 \mod 8$, so any matrix C over $\mathbb{Z}_8$ of the type

   $$\mathrm{circ}_{8k}(1, -1, \ldots, -1, 1, -1, \ldots, -1)$$

   $$\mathrm{circ}_{8k}(5, -1, \ldots, -1, 1, -1, \ldots, -1)$$

   with $k \in \mathbb{N}$ fulfills the conditions (2).

Example 6. Let C of an even order $n = 2k$ defined over $\mathbb{Z}_m$ satisfy (17) and let m be odd. Then the congruences (19) lead to

$$2d \equiv -2k + 2 \pmod{m} \quad \wedge \quad 2d \equiv 2k - 6 \pmod{m}.$$

Dividing in both congruences by 2 (which is a correct step due to $\gcd(2, m) = 1$), we get

$$d \equiv -k + 1 \pmod{m} \quad \wedge \quad d \equiv -3 + k \pmod{m},$$

hence

$$2d \equiv -2 \pmod{m},$$

and so

$$d \equiv -1 \pmod{m}.$$

In this case we get the matrices C over $\mathbb{Z}_m$ of the type

$$\mathrm{circ}_{2m\ell+4}(m-1, -1, \ldots, -1, 1, -1, \ldots, -1),$$

where m is odd.

Example 7. Let C of an even order $n = 2k$ defined over $\mathbb{Z}_m$ satisfy (17) and let m be even. Then the congruences (19) lead to

$$\frac{n}{2} \equiv -d + 1 \pmod{\frac{m}{2}} \quad \wedge \quad \frac{n}{2} \equiv 3 + d \pmod{\frac{m}{2}}.$$

By adding/substracting these two congruences, we get

$$n \equiv 4 \pmod{\frac{m}{2}},$$

$$2d \equiv -2 \pmod{\frac{m}{2}}.$$

Hence, for odd $\frac{m}{2}$, we obtain the matrices of type

$$\mathrm{circ}_{m\ell+4}(d, -1, \ldots, -1, 1, -1, \ldots, -1),$$

where $\ell \in \{0, 1, 2, \ldots\}$ and $d \equiv -1 \pmod{\frac{m}{2}}$.

For even $\frac{m}{2}$, we obtain the matrices of type

$$\mathrm{circ}_{\frac{m\ell}{2}+4}(d, -1, \ldots, -1, 1, -1, \ldots, -1),$$

where $\ell \in \{0, 1, 2, \ldots\}$ and $d \equiv -1 \pmod{\frac{m}{4}}$.

5 Application: Mutually unbiased bases

In this section, we present an application for the particular case of circulant matrices C satisfying conditions (2) with $d = 1$. If $c_0 = d = 1$, then all the entries of the generator have absolute value 1, so $C = \mathrm{circ}_n(c_0, c_1, \ldots, c_{n-1})$ defines an unormalized circulant complex Hadamard matrix of order n. Here, the absence of normalization is in the sense that matrix C is proportional to unitary but not unitary, as stated in Conditions (2). From now on, we consider normalized circulant matrices C, which differ from those defined in (2) by a constant factor $1/\sqrt{n}$. The reason to introduce this normalization is because columns of the considered unitary matrices define mutually unbiased -orthonormal- bases of $\mathbb{C}^n$. Throughout this section, we assume that C is *not necessarily Hermitian*; non-Hermitian matrices C are allowed. The problem of the existence of matrices C having constant diagonal $d = 1$ is particularly hard to solve in its full generality for arbitrary large n, as it contains the long-standing *circulant Hadamard conjecture* [16].

Let $\lambda = (\lambda_0, \ldots, \lambda_{n-1})$ be the vector of the eigenvalues of C. From Eqs. (2) we know that $\lambda_j = \sqrt{d^2 + n - 1}\, e^{i\alpha_j}$, where $\alpha_j \in [0, 2\pi]$ are suitable phases, for every $j = 0, \ldots, n-1$. As a basic property of circulant matrices, the generator of C is given by $g = F\lambda$, where F is the discrete Fourier transform of order n.

In order to satisfy conditions (2) we should have $[g]_0 = d$ and $|[g]_j| = 1$, for every $j = 0, \ldots, n-1$, where $[g]_k$ denotes the kth entry of vector g. Let us now show that this particular problem for $d = 1$ is one-to-one related to a well-known problem in quantum information theory: the *mutually unbiased bases* problem.

Two orthonormal bases in $\mathbb{C}^n$, $\{\phi_j\}_{j=0,\ldots,n-1}$ and $\{\psi_k\}_{k=0,\ldots,n-1}$, are mutually unbiased (MU) if $|\langle\phi_j|\psi_k\rangle|^2 = \frac{1}{n}$, for every $j, k = 0, \ldots, n-1$. Two MU bases exist in every dimension $n \geq 2$. Indeed, the canonical basis in dimension n is MU to the basis defined by the columns of the discrete Fourier transform for any order $n \geq 2$.

Even more, three pairwise MU bases (MUB) exist in every dimension $n \geq 2$ [2]. They are given by the eigenvectors bases of the three unitary operators Z, X and XZ, where $Z = \sum_{j=0}^{n-1} \omega^j \langle e_j, \cdot\rangle\, e_j$, $X = \sum_{j=0}^{n-1} \langle e_j, \cdot\rangle\, e_{j+1 \pmod n}$. Here, $\{e_j\}_{j=0,\ldots,n-1}$ denotes the jth element of the canonical basis and $\omega = \mathrm{e}^{2\pi\mathrm{i}/n}$. Eigenvectors of Z are given by the canonical basis, whereas the colums (or rows) of the discrete Fourier transform of order n are eigenvectors of X. For prime values of n, the eigenvectors basis of the product operator XZ is given by

$$\varphi_j = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \omega^{-jk-s_k}\,, \tag{20}$$

where $s_k = k + \cdots + n - 1$, cf. Eq. (3) in Ref. [2] for the special case $k = 1$ (here k follows notation used in Ref. [2]).

In general, there are at most $n + 1$ MUB in dimension n, where the upper bound can be saturated for every prime [11] and prime power [19] dimension n. For any other composite dimension, e.g. $n = 6$, it is not known how many pairwise MU bases can be constructed; this question is one of the main open problems in quantum information theory. The importance of MU bases relies on the fact that two physical observables, represented by hermitian operators, are canonical (i.e. as different as possible) if and only if their eigenvectors bases are MU. So, translated to

physics, the open question is about how many mutually canonical observables exist in every finite dimension n. Furthermore, the existence of a maximal set of $n+1$ MUB in dimension n provides a protocol for quantum state reconstruction from experimental measurements [11], which maximizes the robustness of reconstruction under the presence of errors in both state preparation and measurement stages [17].

Before introducing the relation to our problem let us establish a standard notation. When refering to a set of m MU bases we will use the notation $\{M_1, \ldots, M_m\}$, where M_j, $j = 1, \ldots, m$, are unitary matrices containing the vectors forming the bases in its columns. According to this notation, note that $M_j^* M_k = nH^{(j,k)}$, where all matrices $H^{(j,k)}$ are unnormalized complex Hadamard matrix. For instance, $\{I, F\}$, i.e. identity and Fourier matrices, define a pair of MU bases for any order n.

Proposition 8. *The identity matrix I together with discrete Fourier transform F and any circulant matrix C satisfying conditions (2) with $d = 1$ define a set of three MUB in dimension $n \geq 2$.*

Proof. Identity matrix I is MUB to both matrices F and C of order n because every entry of these two matrices has the same amplitude $1/\sqrt{n}$. Also, eigenvalues of C obey Eq.(4), which immediately imply that F and C are MUB. This is so because C is a unitary matrix, so it has n unimodular complex eigenvalues. □

Let us illustrate the above result with the explicit solution for a maximal set of MUB in dimensions $d = 2$ and $d = 3$, where three and four MUB exist, respectively:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad F = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad C = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \tag{21}$$

and

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad F = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

$$C_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} \omega & 1 & 1 \\ 1 & \omega & 1 \\ 1 & 1 & \omega \end{pmatrix} \qquad C_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} \omega^2 & 1 & 1 \\ 1 & \omega^2 & 1 \\ 1 & 1 & \omega^2 \end{pmatrix}$$

Let us mention that the discrete Fourier transform F of prime order n is equivalent to a circulant matrix C satisfying conditions (2) with $d = 1$ [1], [7]. Here, we consider the following notion of equivalence: two matrices A and B are equivalent if there exists diagonal unitary matrices D_1, D_2 and permutation matrices P_1, P_2 such that $A = D_1 P_1 B P_2 D_2$. Furthermore, any circulant matrix C satisfying conditions (2), with $d = 1$ and prime order n, is equivalent to F (cf. Theorem 1.2 in Ref. [9]).

6 Acknowledgements

DG and DU kindly acknowledge support from Grant FONDECYT Iniciación number 11180474, Chile.

DU acknowledges support from the project ANT1856, Universidad de Antofagasta.

OT acknowledges support from the Czech Science Foundation (GAČR) within the project 17-01706S.

Appendix

A Computer simulations

In this section we present all combinations of n and d with $n = 2, \ldots, 22$ and $d \neq \frac{n}{2} - 1$ such that a circulant matrix C satisfying conditions (2) exists. They were obtained using the algorithm described in Section 3.2. Each such pair (n, d) is supplemented with an example of a generator of C. Notice that the results of the simulations disprove the existence of C with $d \neq \frac{n}{2} - 1$ for all even values $n \leq 22$, in particular for $n = 16$ (discussed in Example 2).

- $n = 7$, $d = \frac{1}{2\sqrt{2}}$

$$\left(\frac{1}{2\sqrt{2}}, 0.833289 - 0.552838i, -0.724402 - 0.689378i, 0.951773 - 0.306802i, \right.$$
$$\left. 0.951773 + 0.306802i, -0.724402 + 0.689378i, 0.833289 + 0.552838i\right)$$

- $n = 11$, $d = \frac{1}{2\sqrt{3}}$

$$\left(\frac{1}{2\sqrt{3}}, -0.00724338 - 0.999974i, 0.760473 - 0.649369i, 0.534533 - 0.845148i, \right.$$
$$-0.750986 + 0.660318i, 0.906599 - 0.421993i, 0.906599 + 0.421993i,$$
$$\left. -0.750986 - 0.660318i, 0.534533 + 0.845148i, 0.760473 + 0.649369i, \right.$$
$$\left. -0.00724338 + 0.999974i\right)$$

- $n = 13$, $d = \frac{5}{2\sqrt{3}}$

$$\left(\frac{5}{2\sqrt{3}}, 0.153536 - 0.988143i, -0.704051 - 0.710149i, 0.595162 - 0.803606i, \right.$$
$$0.869485 - 0.493959i, 0.0560739 + 0.998427i, 0.184495 - 0.982834i,$$
$$0.184495 + 0.982834i, 0.0560739 - 0.998427i, 0.869485 + 0.493959i,$$
$$\left. 0.595162 + 0.803606i, -0.704051 + 0.710149i, 0.153536 + 0.988143i\right)$$

- $n = 15,\ d = \frac{1}{4}$

$$\Big(\frac{1}{4}, 0.989074 + 0.147421i, 0.0432273 - 0.999065i, -0.309017 - 0.951057i,$$
$$0.165435 + 0.986221i, -0.5 - 0.866025i, 0.809017 - 0.587785i,$$
$$0.552264 - 0.833669i, 0.552264 + 0.833669i, 0.809017 + 0.587785i,$$
$$-0.5 + 0.866025i, 0.165435 - 0.986221i, -0.309017 + 0.951057i,$$
$$0.0432273 + 0.999065i, 0.989074 - 0.147421i\Big)$$

- $n = 19,\ d = \frac{1}{2\sqrt{5}}$

$$\Big(\frac{1}{2\sqrt{5}}, 0.999747 - 0.0225052i, -0.660552 - 0.75078i, 0.56565 - 0.824645i,$$
$$-0.693668 - 0.720295i, 0.527969 - 0.849264i, 0.952885 + 0.303331i,$$
$$-0.0601301 + 0.998191i, 0.802764 - 0.596297i, -0.422203 - 0.906501i,$$
$$-0.422203 + 0.906501i, 0.802764 + 0.596297i, -0.0601301 - 0.998191i,$$
$$0.952885 - 0.303331i, 0.527969 + 0.849264i, -0.693668 + 0.720295i,$$
$$0.56565 + 0.824645i, -0.660552 + 0.75078i, 0.999747 + 0.0225052i\Big)$$

- $n = 21,\ d = \frac{11}{4}$

$$\Big(\frac{11}{4}, -0.643041 + 0.765832i, 0.521717 - 0.853118i, 0.38874 - 0.921348i,$$
$$0.247078 - 0.968996i, -0.999681 + 0.0252613i, 0.0495156 + 0.998773i,$$
$$0.5 - 0.866025i, -0.341709 - 0.939806i, 0.811745 - 0.584012i,$$
$$0.715636 - 0.698474i, 0.715636 + 0.698474i, 0.811745 + 0.584012i,$$
$$-0.341709 + 0.939806i, 0.5 + 0.866025i, 0.0495156 - 0.998773i,$$
$$-0.999681 - 0.0252613i, 0.247078 + 0.968996i, 0.38874 + 0.921348i,$$
$$0.521717 + 0.853118i, -0.643041 - 0.765832i\Big)$$

References

[1] J. Backelin: *Square multiples n give infinitely many cyclic n-roots*. Stockholms Universitet, Matematiska Institutionen (1989).

[2] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan: A new proof for the existence of mutually unbiased bases. *Algorithmica* 34 (4) (2002) 512–528.

[3] S.T. Blake and A.Z. Tirkel: A construction for perfect periodic autocorrelation sequences. In: *International Conference on Sequences and Their Applications*. Springer (2014) 104–108.

[4] D. Chu: Polyphase Codes With Good Periodic Correlation Properties. *IEEE Transactions on information theory* 18 (4) (1972) 531–532.

[5] R. Craigen, H. Kharaghani: On the nonexistence of Hermitian circulant complex Hadamard matrices. *Australasian Journal of Combi natorics* 7 (1993) 225–228.

[6] R. Craigen: Trace, symmetry and orthogonality. *Canadian Mathematical Bulletin* 37 (4) (1994) 461–467.

[7] J.-C. Faugère: Finding all the solutions of Cyclic 9 using Gröbner basis techniques. In: K. Shirayanagi, K. Yokoyama: *Lecture Notes Series on Computing – Computer Mathematics: Proceedings of the Fifth Asian Symposium (ASCM 2001)*. World Scientific (2001) 1–12.

[8] E.C. Farnett, G.H. Stevens: Pulse Compression Radar. In: *Radar Handbook, 2nd edition*. McGraw-Hill, New York (1990) 10.1–10.39.

[9] G. Hiranandani, J.-M. Schlenker: Small circulant complex Hadamard matrices of Butson type. *European Journal of Combinatorics* 51 (2016) 306–314.

[10] R. Heimiller: Phase shift pulse codes with good periodic correlation properties. *IRE Transactions on Information Theory* 7 (4) (1961) 254–257.

[11] I.D. Ivonovic: Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General* 14 (12) (1981) 3241–3245.

[12] V.P. Ipatov: *Spread Spectrum and CDMA: Principles and Applications*. John Wiley & Sons (2005).

[13] Y. Liu, P. Fan: Modified Chu sequences with smaller alphabet size. *Electronics Letters* 40 (10) (2004) 598–599.

[14] A. Milewski: Periodic sequences with optimal properties for channel estimation and fast start-up equalization. *IBM Journal of Research and Development* 27 (5) (1983) 426–431.

[15] W.H. Mow: A study of correlation of sequences. PhD Thesis, Department of Information Engineering, The Chinese University of Hong Kong (1993)

[16] H.J. Ryser: *Combinatorial mathematics*. The Mathematical Association of America, John Wiley and Sons, Inc., New York (1963).

[17] A.J. Scott: Tight informationally complete quantum measurements. *Journal of Physics A: Mathematical and General* 39 (43) (2006) 13507.

[18] O. Turek, D. Goyeneche: A generalization of circulant Hadamard and conference matrices. *Linear Algebra and its Applications* 569 (2019) 241–265.

[19] W.K. Wootters, B.D. Fields: Optimal state-determination by mutually unbiased measurements. *Annals of Physics* 191 (2) (1989) 363–381.

[20] L. Xu: Phase coded waveform design for Sonar Sensor Network. In: *Conference on Communications and Networking in China (CHINACOM), 2011 6th International ICST*. Springer (2011) 251–256.

Received: 30 September 2019
Accepted for publication: 21 December 2019
Communicated by: Pasha Zusmanovich