



Self-dual bent sequences for complex Hadamard matrices

Minjia Shi¹ · Yaya Li¹ · Wei Cheng² · Dean Crnković³ · Denis Krotov⁴ · Patrick Solé⁵

Received: 25 April 2022 / Revised: 31 August 2022 / Accepted: 9 November 2022 /

Published online: 15 December 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

A new notion of bent sequence related to Hadamard matrices was introduced recently, motivated by a security application (Solé et al. 2021). In this paper we introduce the analogous notion for complex Hadamard matrices, and we study the self-dual class in length at most 90. We use three competing methods of generation: Brute force, Linear Algebra and Groebner bases. Regular complex Hadamard matrices and Bush-type complex Hadamard matrices provide many examples. We introduce the strong automorphism group of complex Hadamard matrices, which acts on their associated self-dual bent sequences. We give an efficient algorithm to compute that group. We also answer the question which complex Hadamard matrices can be uniquely reconstructed from the off-diagonal elements, define a related concept of mixed-skew Hadamard matrix, and show the existence of mixed-skew Hadamard matrices of small orders.

Keywords Bent sequences · Complex Hadamard matrices · Regular complex Hadamard matrices · Bush-type complex Hadamard matrices · Mixed-skew Hadamard matrices

Mathematics Subject Classification Primary 94D10; Secondary 15B34

Communicated by Y. Zhou.

This work is supported in part by the National Natural Science Foundation of China (Grant No. 12071001). The work of Dean Crnković is supported by Croatian Science Foundation under the project 6732. The work of Denis Krotov is supported within the framework of the state contract of the Sobolev Institute of Mathematics (Project FWNF-2022-0017).

✉ Minjia Shi
smjwcl.good@163.com

Extended author information available on the last page of the article

1 Introduction

Complex Hadamard matrices are matrices C of order v with entries in the fourth roots of unity $\Omega_4 = \{\pm 1, \pm i\}$ satisfying

$$CC^* = vI,$$

where $*$ denotes the transpose conjugate, and I is the identity matrix of order v . They were introduced by Turyn and studied by Seberry [25], and Kharaghani [13, 14], among others. A more general notion of complex Hadamard matrices where Ω_4 is replaced by the set of complex numbers of modulus one exists, but will not be considered in this paper. A survey of that more general notion is [22]. A related webpage is [3]. Complex Hadamard matrices are conjectured to exist for all even v [25]. This is the complex analogue of the celebrated Hadamard conjecture.

Recently, a notion of bent sequences attached to Hadamard matrices was introduced in [21] from a motivation of security. In a companion paper [18] the self-dual subclass of bent sequences for Hadamard matrices is studied. Three competing methods are used to construct such sequences: Brute force, Linear Algebra and Groebner bases. The first and the last are easier to program but only work for matrices of small orders (resp. medium orders). The Linear Algebra method requires some complex programming, but performs well even in large orders if the dimension of the relevant eigenspace is small enough.

In the present paper we conduct the analogous study by the same methods for complex Hadamard matrices. The main hurdle in this generalization was in the definition, as explained in the Preliminaries section, Sect. 2. A self-dual bent sequence is defined here as an eigenvector of a complex Hadamard matrix with values in the complex fourth roots of unity. This can exist only if the related eigenvalue is a Gaussian integer, which implies in turn that v is either a perfect square or the sum of two squares (Proposition 1).

We have a hierarchy of definitions of bent sequences from the special to the general

- (1) classical bent sequences and Sylvester type Hadamard matrices [4],
- (2) bent sequences attached to general Hadamard matrices [18, 21],
- (3) complex bent sequences attached to Sylvester type Hadamard matrices [20],
- (4) complex bent sequences attached to complex Hadamard matrices: the present paper.

Like in [18], the regular complex Hadamard matrices [13] and the Bush-type complex Hadamard matrices have proved especially useful. As is known since the seminal paper of Turyn [23], conference matrices can be used in the creation of complex Hadamard matrices. Their spectrum can be determined exactly (Proposition 9). Williamson type constructions are also very useful and lead to concomitant constructions of self-dual bent sequences (Theorem 3). In general, equivalent Hadamard matrices do not have corresponding sets of self-dual bent sequences. The notion of strong equivalence of Hadamard matrices remedies to this problem at the price of smaller groups. An effective algorithm for computing the strong automorphism group of complex Hadamard matrices based on graphical interpretation, is derived.

The material is organized as follows. The next section collects basic facts and definitions needed for the other sections. In Sect. 3, we discuss how to compute the automorphism group of a complex Hadamard matrix and which complex Hadamard matrices can be uniquely reconstructed from the off-diagonal part. Section 4 documents the constructions of complex Hadamard matrices we have used to construct self-dual bent sequences. Section 5 develops an interesting connection with \mathbb{Z}_4 -codes [8]. Section 6 contains the search methods employed

to obtain the numerical results of 7. Sections 8 concludes the article. An appendix contains detailed information on some complex Hadamard matrices of various orders.

2 Preliminaries

Definition 1 If C is a complex Hadamard matrix of order v a *bent sequence* of length v attached to C is any vector $X \in \Omega_4^v$, such that

$$CX = \lambda Y,$$

where λ is an eigenvalue of C and $Y \in \Omega_4^v$. We will say that X is a *self-dual bent sequence* attached to C if $Y = X$.

Proposition 1 *If there exists at least one self-dual bent sequence of length v , then v is a square or the sum of two squares.*

Proof By the Hadamard property we see that $|\lambda|^2 = v$. By eigenvalue definition, we see that

$$\lambda = \left(\sum_{j=1}^v c_{1j} x_j \right) x_1^{-1} = a + ib \in \mathbb{Z}[i].$$

Taking squared norms we get $v = a^2 + b^2$. If one of a, b is zero then v is a square. If both are non zero then v is a sum of two squares. □

An equivalent definition is thus: let $v = a^2 + b^2$, with $a, b \geq 0$. A self-dual bent sequence attached to C is defined as $X \in \Omega_4^v$ such that

$$CX = (\pm a + \pm ib)X,$$

where $(\pm a + \pm ib)$ are eigenvalues of C . Note that $b + ia = i(a - bi) = i(a + bi)^*$, so that swapping a and b amounts to simple changes in C and X .

In the case $v = 2^{2m} = (2^m)^2$, and H the Sylvester Hadamard matrix of order v such sequences were studied in [20]. The case of v a square and H an arbitrary real Hadamard matrix is treated in [18].

The even integers ≤ 90 and sum of at most two squares are

$$\{2, 4, 8, 10, 16, 18, 20, 26, 32, 34, 36, 40, 50, 52, 58, 64, 68, 72, 74, 80, 82, 90\}.$$

3 Finding automorphism groups and reconstructing the matrix from its off-diagonal elements

The class of complex Hadamard matrices of order v is preserved by the three following operations:

- row permutation,
- column permutation,
- multiplication of a row or column by an element of Ω_4 ,

which form a group $G(v)$ with structure $(S_v \wr C_4)^2$, where S_m denotes the symmetric group on m letters, and C_m the cyclic group of order m . We denote by $S(v)$ the group of diagonal

matrices of order v with diagonal elements in Ω_4 , and by $M(v)$ the matrix group generated by $P(v)$, the group of permutation matrices of order v , and $S(v)$. Note that $M(v)$ consists of unitary matrices so that $QQ^* = I$ for every Q in $M(v)$. The action of $G(v)$ on a complex Hadamard matrix C is of the form

$$C \mapsto PCQ,$$

with $P, Q \in M(v)$. The cases when this action is 2-transitive are classified in [17]. To work on the symmetries of bent sequences we will require the notion of strong automorphism group $\text{SAut}(C)$ of C defined as the set of $P \in M(v)$ such that $PC = CP$. Then we can state the following result.

Proposition 2 *If X is a self-dual bent sequence for C , and if $P \in M(v)$ is a strong automorphism of C , then PX is also a self-dual bent sequence for C .*

Proof By hypothesis $CX = \lambda X$. Multiplying the left hand side of this equation by P we get

$$\lambda PX = PCX = CPX.$$

Letting $Y = PX$, we see that $CY = \lambda Y$. The result follows upon noticing that $Y \in \Omega_4^n$. \square

3.1 Finding Aut and SAut

There are six kinds of natural transformations that send a complex Hadamard matrix to a complex Hadamard matrix:

- (I) permuting rows,
- (II) permuting columns,
- (III) multiplying rows by constants from Ω_4 ,
- (IV) multiplying columns by constants from Ω_4 ,
- (V) transposition,
- (VI) conjugation, applied to all elements of the matrix.

A combination of (I)–(IV) (of (I)–(VI)) is called an automorphism (semi-automorphism) of a complex Hadamard matrix C if it sends C to itself. The group of all automorphisms of a complex Hadamard matrix is denoted $\text{Aut}(C)$.

Let C be a complex Hadamard matrix of order n . Define the di-graph $G(C)$ of order $8n$ in the following way:

- for each $t \in \{0, \dots, n - 1\}$, the t th row corresponds to 4 row vertices $r_{t,x}$ and 4 row arcs $(r_{t,x}, r_{t,ix}), x \in \Omega_4$;
- for each $s \in \{0, \dots, n - 1\}$, the s th column corresponds to 4 column vertices $c_{s,x}$ and 4 column arcs $(c_{s,x}, c_{s,ix}), x \in \Omega_4$;
- each cell (t, s) corresponds to four cell arcs $(r_{t,x}, c_{s,C_{t,sx}}), x \in \Omega_4$.

The following four lemmas are straightforward.

Lemma 1 *If the matrix C' is obtained from C by multiplying the t th row by $y, y \in \Omega_4$, then $G(C')$ is obtained from $G(C)$ by the following permutation of four row vertices: $r_{t,x} \rightarrow r_{t,y^{-1}x}, x \in \Omega_4$.*

Lemma 2 *If the matrix C' is obtained from C by multiplying the s th column by $y, y \in \Omega_4$, then $G(C')$ is obtained from $G(C)$ by the following permutation of four column vertices: $c_{s,x} \rightarrow c_{s,yx}, x \in \Omega_4$.*

Lemma 3 *If the matrix C' is obtained from C by permuting the rows with a permutation π , $\pi \in \text{Sym}(n)$:*

$$C'_{\pi(t),s} = C_{t,s},$$

then $G(C')$ is obtained from $G(C)$ by the following permutation of four row vertices: $r_{t,x} \rightarrow r_{\pi(t),x}$, $t \in \{0, \dots, n - 1\}$, $x \in \Omega_4$.

Lemma 4 *If the matrix C' is obtained from C by permuting the columns with a permutation π , $\pi \in \text{Sym}(n)$:*

$$C'_{t,\pi(s)} = C_{t,\pi(s)},$$

then $G(C')$ is obtained from $G(C)$ by the following permutation of four column vertices: $c_{s,x} \rightarrow c_{\pi(s),x}$, $s \in \{0, \dots, n - 1\}$, $x \in \Omega_4$.

Proposition 3 *Every automorphism of $G(C)$ is the composition of transformations considered in the four lemmas above.*

Proof We first note that the in-degree and the out-degree of a row vertex are 1 and $n + 1$, respectively, while for a column vertex these values are $n + 1$ and 1. So, any automorphism stabilizes the set of row (column) vertices.

Next, the arcs between the row vertices form n vertex-disjoint directed cycles of length four, and every automorphism permutes the cycles (corresponding transformations are considered in Lemma 3) and cyclically permutes the vertices in each cycle (corresponding transformations are considered in Lemma 1). Similarly, for the column vertices. \square

Corollary 1 *The automorphism group of the graph $G(C)$ is isomorphic to the automorphism group of C .*

Remark 1 Similarly, to check if two complex Hadamard matrices are isomorphic, one can check the isomorphism between the corresponding graphs. In particular, to find the group of semi-automorphisms of C , one can extend $\text{Aut}(C)$ by isomorphisms (if any) between C and C^t , C and \bar{C} , between C and C^* .

3.2 SAut

An automorphism is *strong* if the columns and the rows are permuted by the same permutation and multiplied by conjugate constants. In other words, the action of a strong automorphism corresponds to the following action of a complex-signed permutation matrix S : $C \rightarrow SC S^*$. Strong automorphisms of a complex Hadamard matrix C correspond to automorphisms of the graph $G(C)$ that do not break the pairs $\{r_{s,x}, c_{s,x}\}$. To avoid the other automorphisms we can connect the paired vertices $r_{s,x}$ and $c_{s,x}$ of $G(C)$ by a length-2 path, say $r_{s,x}l_{s,x}c_{s,x}$ where $l_{s,x}$ are some additional vertices. Denote the new graph by $\tilde{G}(C)$. From Corollary 1, we have

Corollary 2 *The automorphism group of the graph $\tilde{G}(C)$ is isomorphic to the automorphism group of C .*

Another way is to identify the vertices $r_{s,x}$ and $c_{s,x}$ (we call the merged vertex $m_{s,x}$) $s \in \{0, \dots, n - 1\}$, $x \in \Omega_4$. In this way, we should resolve one problem: there is no way to distinguish the row-column arcs between the vertices $m_{s,1}, m_{s,i}, m_{s,-1}, m_{s,-i}$ and the

cell arcs between the same four vertices (i.e., corresponding to the diagonal cell $C_{s,s}$ of the matrix). To resolve this, we, at first, delete the diagonal cell arcs, and, at second, add *special* vertices m_s with four arcs $(m_s, m_{s,1}), (m_s, m_{s,i}), (m_s, m_{s,-1}), (m_s, m_{s,-i})$ for each s . We denote the new digraph by $\hat{G}(C)$. Deleting the diagonal cell arcs can be regarded as replacing the diagonal elements of the matrix by zeros. If the diagonal of the matrix is uniquely reconstructed from its off-diagonal elements, then the strong automorphism group of the matrix does not change after such replacement.

Corollary 3 *If the diagonal of a complex Hadamard matrix C is uniquely reconstructed from its off-diagonal elements, then the strong automorphism group of the graph $\hat{G}(C)$ is isomorphic to the automorphism group of C .*

Of course, such a statement is not useful without saying for which matrices it is applicable. In Sect. 3.5, we characterize the matrices whose diagonal is not uniquely reconstructed. The interesting theory related with these matrices is actually one of motivations for us to consider the second way of finding the strong automorphism group of a complex Hadamard matrix.

3.3 Equivalent self-dual bent sequences

Two self-dual bent sequences f and g with respect to a complex Hadamard matrix C are *equivalent* if there is a complex-signed permutation matrix S such that $SCS^* = C$ (i.e., $SCS^* \rightarrow C$ is a strong automorphism of C) and $Sf = Sg$. To recognise the equivalence of self-dual bent sequences, one can, for each such sequence f , color the graph $\hat{G}(C)$ in the following way: the vertices $m_{s,x}$ such that $f(s) = x$ are black, and the other vertices (including m_s) are white. Such colored graphs will be denoted $\hat{G}_f(C)$.

Corollary 4 *Assume that the diagonal of a complex Hadamard matrix C is uniquely reconstructed from its off-diagonal elements. Two self-dual bent sequences f and g are equivalent if and only if there is an automorphism of $\hat{G}(C)$ that sends the black vertices of $\hat{G}_f(C)$ to the black vertices of $\hat{G}_g(C)$.*

If C does not satisfy the hypothesis of Corollary 4 (see Theorem 1 for the characterization of such matrices), then we can similarly color the graph $\tilde{G}(C)$. To find the automorphism group of a self-dual bent sequence, it is sufficient to find the group of the automorphisms of the graph that preserve the corresponding coloring. Note that the modern graph-isomorphism software can deal with colored graphs as well.

3.4 Regular matrices

A complex Hadamard matrix C of order v is *regular* if it has constant row and column sum. Let us denote this constant by σ . Regular complex Hadamard matrices are studied in [13], where it is observed that $|\sigma|^2 = v$, which in turn implies that v is the sum of two squares. A direct connection between self-dual bent sequences and regular complex Hadamard matrices is as follows.

Proposition 4 *If C is a regular complex Hadamard matrix of order v , then j the all-one vector of length v , is a self-dual bent sequence for C .*

Proof Denote by σ the sum of elements of any row. By definition of regular complex Hadamard matrices $Cj = \sigma j$. □

Example 1 Some regular complex Hadamard matrices are as follows:

- (1) For order $v = 2$ we have the matrix $\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$ where $\sigma = 1 + i$,
- (2) For orders $v = 18$ and $v = 34$ we have $\sigma = 3 + 3i$ and $\sigma = 5 + 3i$, respectively, both from Lemma 6 of [13],
- (3) For order $v = 90$, we have $\sigma = 9 + 3i$ by Corollary 9 (ii) of [13].

3.5 Reconstructing diagonal

Definition 2 Let A be a square matrix with $\text{diag}(A) = I$ (the identity matrix), and let $U := A - I$, then A is called *skew* if $U^* = -U$. We will say that a matrix A is *i -skew* (*$-i$ -skew*) if $U^* = iU$ (respectively, $U^* = -iU$).

We will say that a matrix A is *mixed-skew* if there is a subset J of indices such that

- (a) the submatrix of A restricted by the elements with both indices in J is $-i$ -skew,
- (b) the submatrix of A restricted by the elements with indices not in J is i -skew,
- (c) $A_{s,t} = -\overline{A_{t,s}}$ for every s in J and t not in J .

In other words, A is mixed-skew if for some complex-signed permutation matrix P the matrix PAP^* has the form

$$\begin{pmatrix} A' & U \\ -U^* & A'' \end{pmatrix},$$

where A' is $-i$ -skew and A'' is i -skew. Note that i -skew and $-i$ -skew matrices are special cases of mixed-skew matrices, where A' or A'' has size 0.

Theorem 1 Assume that two different complex Hadamard matrices C and C' of order n coincide in all off-diagonal elements. Then for the complex sign matrix $D := \text{diag}(C)$, the matrices $G := CD^*$ and $G' := C'D^*$ satisfy one of the following:

- (i) G is skew and $G' = G - 2I$;
- (ii) there is a subset J of indices from $\{0, \dots, n - 1\}$ such that
 - (ii.a) the submatrix of G restricted by the elements with both indices in J is $-i$ -skew,
 - (ii.b) the submatrix of G restricted by the elements with indices not in J is i -skew,
 - (ii.c) $G_{s,t} = -\overline{G_{t,s}}$ for every s in J and t not in J ,
 - (ii.d) $G'_{s,s} = i$ for every s in J ,
 - (ii.e) $G'_{t,t} = -i$ for every t not in J .

Proof Given C and C' as in the theorem, we choose a complex sign matrix $D := \text{diag}(C)$ such that the diagonal elements of CD^* are all equal to 1. Denote $G := CD^*$ and $G' := C'D^*$. So, G and G' are two different complex Hadamard matrices coinciding in the off-diagonal elements, and $G_{s,s} = 1, s = 0, \dots, n - 1$.

Since for different s and t the t th and s th rows of a complex Hadamard matrix are orthogonal and the t th (s th) row of G coincides with the t th (s th) row of G' in all positions except the t th (s th) one, we find

$$G'_{s,s} \overline{G'_{t,t}} + \overline{G'_{t,t}} G'_{s,t} = G_{s,s} \overline{G_{t,t}} + \overline{G_{t,t}} G_{s,t} = \overline{G'_{t,t}} + G'_{s,t}. \tag{1}$$

In particular, $G'_{s,s}$ and $G'_{t,t}$ are either both real or both imaginary. We conclude that the diagonal elements of G' are either all real or all imaginary. Consider these two cases.

- (i) If all diagonal elements of G' are real, then at least one of them, say $G'_{s,s}$, equals -1 . From (1), we see that for every t different from s , $G'_{t,t}$ cannot be 1. Hence, all diagonal elements equal -1 . For arbitrary different s and t , substituting $G'_{s,s} = -1$, $\overline{G'_{s,s}} = -1$ to (1), we find $G'_{s,t} = -\overline{G'_{t,s}}$. Hence, G is skew, and assertion (i) of the theorem takes place.
- (ii) Assume that all diagonal elements of G' are imaginary. Denote $J := \{s \in \{0, \dots, n-1\} : G'_{s,s} = i\}$. Consider different s and t from J . With $G'_{s,s} = G'_{t,t} = i$, Eq. (1) turns to $iG'_{t,s} - iG'_{s,t} = \overline{G'_{t,s}} + G'_{s,t}$, which implies $(i-1)\overline{G'_{t,s}} = (i+1)G'_{s,t}$, and $\overline{G'_{t,s}} = -iG'_{s,t}$. This proves assertion (ii.a) in the claim of the theorem. Assertions (ii.b) and (ii.c) are proved similarly, while (ii.d) and (ii.e) hold by the definition of J .

□

It is easy to see that for $n > 2$, the same matrix G cannot satisfy both (i) and (ii.a–c). So, we can conclude the following:

Corollary 5 *For every complex Hadamard matrix C of order at least 4, there is at most one other complex Hadamard matrix C' coinciding with C in all off-diagonal elements. Moreover, the existence of such C' implies that CD^* is skew or mixed-skew, where $D := \text{diag}(C)$.*

Example 2 Case (i) of Theorem 1 is illustrated by the following matrices:

$$\begin{aligned}
 C &= \begin{pmatrix} 1 & i & i & 1 \\ -1 & i & i & -1 \\ -i & 1 & -1 & i \\ -1 & i & -i & 1 \end{pmatrix}, & C' &= \begin{pmatrix} -1 & i & i & 1 \\ -1 & -i & i & -1 \\ -i & 1 & 1 & i \\ -1 & i & -i & -1 \end{pmatrix}, \\
 D &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \\
 G &= \begin{pmatrix} 1 & 1 & -i & 1 \\ -1 & 1 & -i & -1 \\ -i & -i & 1 & i \\ -1 & 1 & i & 1 \end{pmatrix}, & G' &= \begin{pmatrix} -1 & 1 & -i & 1 \\ -1 & -1 & -i & -1 \\ -i & -i & -1 & i \\ -1 & 1 & i & -1 \end{pmatrix}.
 \end{aligned}$$

Example 3 Case (ii) of Theorem 1 is illustrated by the matrices C and C' below:

$$C = \left(\begin{array}{cc|cc} 1 & i & -i & -i \\ 1 & 1 & i & 1 \\ \hline 1 & -1 & i & -1 \\ 1 & -i & -i & i \end{array} \right), \quad C' = \left(\begin{array}{cc|cc} i & i & -i & -i \\ 1 & i & i & 1 \\ \hline 1 & -1 & 1 & -1 \\ 1 & -i & -i & 1 \end{array} \right).$$

Multiplying the last two columns of C by $-i$ makes it mixed-skew. It can be checked that $C' = PCP^*$, where

$$P = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ i & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

which shows that the strong automorphism groups of C and of the off-diagonal part of C do not coincide.

Example 4 Some other examples of mixed-skew matrices are (of order 8 and of orders 6, 10, 14, 22, 26 in a special bi-cyclic form)

$$\left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ i & 1 & 1 & -i & i & -1 & -1 & -i \\ i & i & 1 & -1 & -i & 1 & -i & -1 \\ i & -1 & -i & 1 & 1 & -1 & -i & i \\ \hline -1 & i & -i & -1 & 1 & -i & i & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & -i & -i & -1 & i & 1 & i \\ -1 & -i & 1 & i & -i & i & -1 & 1 \end{array} \right),$$

$$\left(\begin{array}{c|c} A & B \\ \hline -B^* & A^* \end{array} \right), \quad A = \text{circ}(a), \quad B = \text{circ}(b); \tag{2}$$

- $a = (1, 1, i), b = (1, 1, -1)$, or
- $a = (1, 1, -1, -i, i), b = (1, i, i, -1, i)$, or
- $a = (1, -1, -1, -i, -1, -i, -i), b = (1, 1, -1, 1, -1, -1, i)$, or
- $a = (1, 1, -1, -i, -1, -1, -i, -i, -1, -i, i)$,
 $b = (1, 1, i, -1, -1, 1, -1, i, i, 1, -1)$, or
- $a = (1, -i, 1, -i, -1, 1, 1, i, i, -i, -1, i, -1)$,
 $b = (1, -i, -i, -1, -i, -i, -i, i, -1, 1, -1, -i, 1)$,

where $\text{circ}(\dots)$ is the matrix whose rows are all cyclic shifts of the corresponding sequence.

Remark 2 A matrix in the form (2) is complex Hadamard if and only if

$$\langle a, \sigma^s(a) \rangle + \langle b, \sigma^s(b) \rangle = 0, \quad s = 1, \dots, n - 1, \tag{3}$$

where σ is the cyclic shift: $\sigma((a_0, a_1, \dots, a_{n-1})) = (a_{n-1}, a_1, \dots, a_{n-2})$. Such pairs (a, b) are called complex periodic Golay pairs. Additionally, the matrix is mixed-skew if $a = (a_0, a_1, \dots, a_{n-1})$ satisfies $a_k = ia_{n-k}^{-1}, k = 1, \dots, n - 1$.

Remark 3 Pairs of sequences satisfying (3) for the non-cyclic shift

$$\sigma((a_0, a_1, \dots, a_{n-1})) = (0, a_1, \dots, a_{n-2})$$

are called (complex) Golay pairs. A Golay pair is obviously a periodic Golay pair, but the inverse is not true. Golay pairs were firstly introduced in [7]. Periodic correlation is considered in [2]. Complex Golay pairs were firstly considered in [6, 19].

Remark 4 The bi-cyclic matrices of orders 10 and 26 from Example 4 admit self-dual bent sequences $(1, \dots, 1, -1, \dots, -1)$ and $(1, \dots, 1, 1, \dots, 1)$. In particular, these two matrices are regular complex Hadamard matrices.

Problem 1 Is there an i -skew complex Hadamard matrix of order more than 1?

Problem 2 Is there an infinite series of mixed-skew complex Hadamard matrices?

4 Constructions of complex Hadamard matrices

4.1 Kronecker products

A very simple construction of complex Hadamard matrices from Hadamard matrices is as follows.

Proposition 5 *If there exists a Hadamard matrix H of order v , then there exists a complex Hadamard matrix C of order $2v$. In particular, if H is regular, so is C .*

Proof Taking the Kronecker product of H with $\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$, yields the block matrix

$$C = \begin{pmatrix} H & iH \\ iH & H \end{pmatrix},$$

which satisfies $CC^* = 2vI$ by taking block product of C with

$$C^* = \begin{pmatrix} H^t & -iH^t \\ -iH^t & H^t \end{pmatrix}.$$

If the row sum of H is σ , then C is regular of constant row sum $(1 + i)\sigma$. □

Remark 5 The matrix C in Proposition 5 has an order 4 or a multiple of 8. This is a special case of Theorem 1 of [25]: The Kronecker product of a Hadamard matrix of order n by a complex Hadamard matrix of order h is a complex Hadamard matrix of order hn . The Magma command is `KroneckerProduct(A, B)` for the Kronecker product of A by B .

Example 5 The following program constructs 5 complex Hadamard matrices of order 32 from the 5 non-equivalent Hadamard matrices of order 16.

```
R<i>:=CyclotomicField(4);
C2:=Matrix(R,2,2,[1,i,i,1]);
D:=HadamardDatabase();Q:=RationalField();
for j:=1 to 5 do
  H:=Matrix(D,16,j);H:=ChangeRing(H,R);
  C32:=KroneckerProduct(C2,H);
  Eigenvalues(C32);
end for;
```

Note that the eigenvalues of these matrices all have squared norm 32. So there are more eigenspaces to consider.

4.2 Bush type

A complex Hadamard matrix C of order $v = 4u^2$ is said to be Bush-type if it is blocked into $2u$ blocks of side $2u$ say C_{ij} such that the diagonal blocks C_{ii} are all-ones and that the off-diagonal blocks have row and column sums zero. They have many self-dual bent sequences attached to C as the next result shows.

Proposition 6 *If C is a Bush-type complex Hadamard matrix of order $4u^2$, then it has at least 4^{2u} self-dual bent sequences attached to C .*

Proof From the definition, we see that the sequence X defined by $X^t = (u_1 j, \dots, u_{2u} j)$, where j is the all-one vector of length $2u$, and the u_k 's are arbitrary in Ω_4 , is a self-dual bent sequence. □

A complex analogue of the Bush-type Hadamard matrix is the following result, inspired by [12, Theorem 1]. Similar constructions appear in [13, Sect. 5].

Theorem 2 *If there exists a complex Hadamard matrix of order $2v$. Then there exists a Bush-type complex Hadamard matrix of order $4v^2$. This matrix is regular of row sum $2v$.*

Proof Let K be a normalized complex Hadamard matrix of order $2v$ and J_{2v} be a all-one matrix of order $2v$, and let r_1, r_2, \dots, r_{2v} be the row vectors of K . Let $C_i = r_i^t r_i$, for $i = 1, 2, \dots, 2v$. Then the following properties are easy to check:

- (1) $C_i^t = C_i$, for $i = 1, 2, \dots, 2v$.
- (2) $C_1 = J_{2v}$, $C_i J_{2v} = J_{2v} C_i = 0$, for $i = 2, 3, \dots, 2v$.
- (3) $C_i C_j^* = 0$, for $i \neq j, 1 \leq i, j \leq 2v$.
- (4) $C_1 C_1^* + C_2 C_2^* + \dots + C_{2v} C_{2v}^* = 4v^2 I_{2v}$.

Let $C = circ(C_1, C_2, \dots, C_{2v})$, the block circulant matrix with the first row C_1, C_2, \dots, C_{2v} . Then C is a Bush-type complex Hadamard matrix of order $4v^2$. The regularity follows by the property (2). □

Example 6 The following matrix K is a complex Hadamard matrix of order 4:

$$K = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix},$$

The matrix $C_1 = J_4$. The matrices C_2, C_3 and C_4 are

$$C_2 = \begin{pmatrix} 1 & i & -1 & -i \\ i & -1 & -i & 1 \\ -1 & -i & 1 & i \\ -i & 1 & i & -1 \end{pmatrix}, \quad C_3 = \begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{pmatrix},$$

$$C_4 = \begin{pmatrix} 1 & -i & -1 & i \\ -i & -1 & i & 1 \\ -1 & i & 1 & -i \\ i & 1 & -i & -1 \end{pmatrix}.$$

The matrix $C = circ(C_1, C_2, C_3, C_4)$ is a Bush-type complex Hadamard matrix of order 16.

Another construction of a Bush-type complex Hadamard matrix is as follows.

Proposition 7 *If there exists a Bush-type Hadamard matrix of order v^2 . Then there exists a Bush-type complex Hadamard matrix of order v^2 having the entries belonging to the set Ω_4 .*

Proof Let $H = [H_{ij}]$ be a Bush-type Hadamard matrix of order v^2 , where $H_{ij}, 1 \leq i, j \leq v$, are blocks of order v . By multiplying the off-diagonal blocks with i , we obtain a Bush-type complex Hadamard matrix. □

4.3 Conference matrices

A construction indicated in [9, p.67] and in [25, Theorem 3] is connected to Paley II. The Jacobsthal matrix is the matrix C_q defined in [16, Chap. 2, Sect. 3] by $C_q(x, y) = \chi(y - x)$, for $x, y \in \mathbb{F}_q$. Here χ denotes the quadratic character defined by the three following mutually exclusive cases:

$$\chi(z) = \begin{cases} 0 & \text{if } z = 0, \\ 1 & \text{if } z = \square, \\ -1 & \text{if } z \neq \square. \end{cases}$$

where \square denotes an arbitrary quadratic residue of \mathbb{F}_q . Note that C_q is symmetric if $q \equiv 1 \pmod{4}$, since then -1 is a quadratic residue. Its extended version S_q is obtained by adding a border of ones according to the rule in [21, 24].

$$S_q = \begin{pmatrix} 0 & j \\ j^t & C_q \end{pmatrix},$$

with j being an all-one row vector of length q .

Proposition 8 *If q is a prime power and $q \equiv 1 \pmod{4}$, and S_q denotes the extended Jacobsthal matrix, then $iI + S_q$ is a complex Hadamard matrix of order $q + 1$.*

Proof It is known that S_q is a so-called conference matrix [16, Chap. 2, (16)], and therefore satisfies $S_q S_q^t = qI$. Hence

$$(iI + S_q)(iI + S_q)^* = (iI + S_q)(-iI + S_q) = (q + 1)I,$$

where the second equality follows by $S_q = S_q^t = S_q^*$. □

The calculation in the proof extends to the situation when we replace S_q by conference matrices with zero diagonal [1]. In particular this constructs complex Hadamard matrices of orders $\{10, 18, 26, 50, 74, 82, 90\}$.

Unfortunately, the spectrum of a matrix in that family is not favorable to the existence of self-dual bent sequences.

Proposition 9 *Let q be a prime power and $q \equiv 1 \pmod{4}$, and with S_q denoting the extended Jacobsthal matrix, write $C = iI + S_q$. The minimal polynomial of C is $x^2 - 2ix - (q + 1)$.*

Proof Since S_q is real and symmetric, we get $C^* = -iI + S_q = C - 2iI$. The Hadamard relation entails then $C(C - 2iI) = (q + 1)I$, then the result follows. □

Given that the roots of the quadratic are $i \pm \sqrt{q}$, they belong to $\mathbb{Q}(i)$ iff q is a perfect square. That leaves the following orders to test for that construction: $\{10, 26, 50, 82\}$.

4.4 Williamson type

A Hadamard matrix H of order $4m$ is said to be quaternionic if there are four matrices A, B, C, D of order m such that

$$H = A \otimes I + B \otimes i + C \otimes j + D \otimes k,$$

where \otimes stands for the Kronecker product of matrices and i, j, k are quaternionic units given by

$$i = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad k = ij.$$

If, furthermore, we assume A, B, C, D to be symmetric and circulant, we shall say that H is Williamson type.

By Lemma 3 of [14], we know that the existence of such a matrix entails that of a complex Hadamard matrix of the form $\begin{pmatrix} S & T \\ -\overline{T} & \overline{S} \end{pmatrix}$ where the overline denotes complex conjugation.

One may take $S = X + iY$ and $T = V + iW$, where $X = (A + B)/2$, and $Y = (A - B)/2$. Similarly $V = (C - D)/2$, and $W = (C + D)/2$.

Lemma 6 of [13] exploits this correspondence to construct regular complex Hadamard matrices. In the next result, we use a similar construction.

Theorem 3 *If there is a Hadamard matrix H of order $4t^2$ with structure $\begin{pmatrix} R & S \\ -S & R \end{pmatrix}$ then the matrix E given by $2E = (R + S) - i(R - S)$ is a complex Hadamard matrix. If, furthermore, $\begin{pmatrix} X \\ Y \end{pmatrix}$ is a self-dual bent sequence for $H' = \begin{pmatrix} S & -R \\ R & S \end{pmatrix}$ then $U + iV$ is a self-dual bent sequence for E with $U = X + Y$ and $V = X - Y$.*

Proof The first assertion is Lemma 4 in [13]. The second assertion is a simple calculation starting from

$$E(U + iV) = (1 + i)t(U + iV),$$

and replacing E by its value. Separating real and imaginary parts we get the system

$$\begin{aligned} RX + SY &= 2tY, \\ SX - RY &= 2tX, \end{aligned}$$

upon letting $X = (U + V)/2$, $Y = (U - V)/2$. □

Remark 6 By [23], we know that the matrix H in Theorem 3 can be constructed in relation with Williamson matrices.

5 Coding theoretic interpretation

Let \mathcal{C} be a quaternary code of length n over the alphabet Ω_4 . Let \mathcal{Z} be the \mathbb{Z}_4 -code determined by $i^{\mathcal{Z}} = \mathcal{C}$. We need to recall some connections between \mathcal{C} and \mathcal{Z} already present in [8, Sect. II. C].

The distance properties of \mathcal{C} for the squared Euclidean distance d_E are equivalent to the distance properties of \mathcal{Z} for the Lee distance d_L because of the following identity, easily verified by induction on n :

$$d_E(x, y) = 2d_L(u, v),$$

where $x = i^u$ and $y = i^v$ with $u, v \in \mathbb{Z}_4^n$. Thus $u \mapsto i^u$ is an isometry from \mathbb{Z}_4^n onto Ω_4^n . A *Hadamard code* \mathcal{H} is a code of length n over Ω_4 with $|\mathcal{H}| = n$ codewords that are pairwise orthogonal for the standard Hermitian inner product $\langle \cdot, \cdot \rangle$ in dimension n , given by $\langle x, y \rangle = xy^*$. Thus we can think of its codewords as the rows of a complex Hadamard matrix of size n . The *deviation* $\theta(\mathcal{C}, x)$ of an arbitrary vector $x \in \Omega_4^n$ from \mathcal{C} is defined as

$$\theta(\mathcal{C}, x) = \max\{|\langle x, y \rangle| \mid y \in \mathcal{C}\}.$$

It can be seen by expanding $\langle x - y, x - y \rangle$ that

$$\mathcal{R}(\langle x, y \rangle) = n - d_L(u, v), \tag{4}$$

for all $x, y \in \Omega_4^n$. This relation can be exploited to derive weight distributions of \mathcal{Z} .

Proposition 10 (1) *If \mathcal{C} consists of the n rows of a complex Hadamard matrix, then \mathcal{Z} is an equidistant code for the Lee metric of parameters (n, n, n) .*

(2) If \mathcal{C} consists of the n rows of a complex Hadamard matrix, multiplied by the four scalars of Ω_4 , then \mathcal{Z} is a code for the Lee metric of parameters $(n, 4n, n)$.

Proof (1) The possible values of $\langle x, y \rangle$ for x, y two rows of a complex Hadamard matrix are n if $x = y$ and 0 otherwise. The result follows by the above relation (4).

(2) The possible values of $\mathcal{R}(x, y)$ for x, y two proportional rows of a complex Hadamard matrix are n if $x = y$ and $-n$ if $x = -y$. The result follows by the above relation (4).

This completes the proof. □

Remark 7 A similar construction as (2) above is in [26, p.77] with real Hadamard matrices of order $2n$.

Remark 8 The Gray map image of \mathcal{Z} in \mathbb{F}_2^{2n} is an Hadamard code, that is to say a binary code of parameters $(2n, 4n, n)$. This gives a one to many correspondence between a complex Hadamard matrix of order n and a Hadamard code of order $2n$.

Problem 3 Is there any relation with the doubling process of Turyn [23]?

This doubling associates to a complex Hadamard matrix $X + iY$ with X, Y real matrices the Hadamard matrix $X \otimes S_2 + Y \otimes T_2$, where $S_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and $T_2 = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$.

The total deviation of the code \mathcal{C} is then

$$\theta(\mathcal{C}) = \min\{\theta(\mathcal{C}, x) \mid x \in \Omega_4^n\}.$$

Proposition 11 If there is a bent sequence for a complex Hadamard matrix C of order n , then its corresponding Hadamard code \mathcal{C} has deviation $\theta(\mathcal{C}) = \sqrt{n}$.

Proof See [21, Theorem 1] for Euclidean inner product version. □

Recall that the covering radius of a code $\mathcal{Z} \subseteq \mathbb{Z}_4^n$ is given by

$$r_L(\mathcal{Z}) = \max_{u \in \mathbb{Z}_4^n} \min_{v \in \mathcal{Z}} d_L(u, v).$$

The simple inequality $\mathcal{R}(\langle x, y \rangle) \leq |\langle x, y \rangle|$ shows that

$$r_L(\mathcal{Z}) \geq n - \theta(\mathcal{C}).$$

Combining this fact with the above proposition yields the following bound.

Corollary 6 If there is a bent sequence for a complex Hadamard matrix C of order n , then the covering radius of its attached \mathbb{Z}_4 -code is bounded below as

$$r_L(\mathcal{Z}) \geq n - \sqrt{n}.$$

Remark 9 This is less satisfying than that of [18, Lemma 1].

6 Search methods

6.1 Brute force

This method is only applicable for small v 's.

- (1) Construct C a complex Hadamard matrix of order v like in [21] by using Magma database.
- (2) For all $X \in \Omega_4^v$ compute $Y = CX$. If $Y = (a + ib)X$, then X is a self-dual bent sequence for C .

Complexity Exponential in v since $|\Omega_4^v| = 4^v$.

6.2 Groebner basis

```

R<i>:=CyclotomicField(4);
P<X>:=PolynomialRing(R, 4);
H:=Matrix(R,4,4,[1, 1, 1, 1,
 1, -1, 1, -1,
 1, 1, -1, -1,
 1, -1, -1, 1]);
sys:=[];
for j:=1 to 4 do
  R:=0;
  for k:=1 to 4 do
    R:=R+H[j,k]*X[k];
  end for;
  sys:=Append(sys, R-2*X[j]); sys:=Append(sys, X[j]^4-1);
end for;
//The ideal of the relations
I := ideal<P | sys>;
//Computation of a Groebner basis (for the
  lexicographical order if no other order is
  specified)
Groebner(I:Faugere:=true);
//The set of solutions, S
S:=Variety(I);
S;

```

Complexity As is well-known the complexity of computing Groebner bases can be doubly exponential in the number of variables, that is v here.

6.3 Linear algebra

- (1) Construct C a complex Hadamard matrix of order v by the Appendix, Section 9, or the database [3].
- (2) Compute a basis of the eigenspace associated to the eigenvalue $a + ib$.
- (3) Let B denote a matrix with rows such a basis of size $k \leq v$. Pick B_k a k -by- k submatrix of B that is invertible, by the algorithm given below.
- (4) For all $Z \in \Omega_4^k$ solve the system in Y given by $Z = YB_k$.
- (5) Compute the remaining $v - k$ entries of YB .
- (6) If these entries are in Ω_4 declare YB a self-dual bent sequence attached to C .

To construct B_k we apply a greedy algorithm. We construct the list J of the indices of the columns of B_k as follows.

- (i) Initialize J at $J = [1]$.
- (ii) Given a column of index ℓ we compute the ranks over the complex of r and r' of the submatrices of B with k rows and columns defined by the respective lists J and $J' = \text{Append}(J, \ell)$.
- (iii) If $r < r'$ then update $J := J'$.
- (iv) Repeat until $|J| = \text{rank}(B)$.

Remark 10 If the first column of B is zero, step (i) does not make sense, but then there is no self-dual bent sequence in that situation, as all eigenvectors have first coordinate zero.

Remark 11 If the eigenspace has a real-valued basis, then every solution is of the form $(R + S) + i(R - S)$, where R, S are real-valued self-dual bent sequences. So, the number

Table 1 Complex Hadamard matrices of different orders, along with the corresponding minimum dimensions

v	2	4	8	10	16	18	20	26	32	34	36	40
# of C	1	1	1	1	2	1003	1	1	1	1	3	1
min{dim}	1	2	2	5	{2, 6}	{1, 2}	5	13	6	1	{1, 3}	5
v	50		52	58	64		68	72	74	80	82	90
# of C	8		1	1	3		1	2	2	1	2	1
min{dim}	{1, 5, 25 }		13	1	{4, 8, 12}		1	2	1	5	{1, 41 }	4

of complex self-dual bent sequences is equal to the square of the number of real-valued self-dual bent sequences. For example, this is so for the matrix $S_q + iI$ where S_q is a conference matrix: the eigenvalues are $i + c$, where c is an eigenvalue of S_q , and the $(i + c)$ -eigenspace coincides with the c -eigenspace of S_q .

Remark 12 A computational improvement is to look at columns of B_k with a small Hamming weight (much less than k) and determine first the values of X at the indices in the support of that column.

Complexity Roughly of order $v^3 + vk2^k$. In this count v^3 is the complexity of computing an echelonized basis of the eigenspace of C attached to $a + bi$. The complexity of the invertible minor finding algorithm is of the same order or less.

7 Numerical examples

The following Table 1 gives the minimum dimensions of the eigenspace attached to the eigenvalues of complex Hadamard matrices C .

Given how small these minimum dimensions are, the method of Sect. 6.3 is very successful. By using linear algebra method, we verify that there is no self-dual bent sequence in certain cases, e.g., for 1002 matrices when $v = 18$. In Table 2, we investigate the number of self-dual bent sequences for the above complex Hadamard matrices and their constructions are detailed in the Appendix.¹

8 Conclusion

We have considered self-dual bent sequences attached to complex Hadamard matrices from the standpoints of generation and symmetry. We considered three generation techniques: brute force, linear algebra, and Groebner bases. The method based on linear algebra works especially well when considering eigenvalues of low geometric multiplicity. For some matrices of order 52 this method performs well, while the Groebner basis method cannot finish. The lack of complex Hadamard matrices of order > 12 in the database [3] has led us to use the switching method of [5] to generate more matrices. In general, it would be a valuable

¹ In Table 2, “—” means that the number of all self-dual bent sequences is unknown, as the dimensions of the eigenspaces attached to the eigenvalues of C are greater than 16, we are not able to obtain all the self-dual bent sequences. In Table 2, the positive integer N in N^2 is the number of real-valued self-dual bent sequences.

Table 2 Number of self-dual bent sequences in various complex Hadamard matrices with dimensions of the eigenspace attached to the eigenvalues of C smaller than 16

v	2	4	8	10	16	18		
# of C	1	1	1	1	2	1002	1	
Eigenvalues and # of X	$i + 1 : 2^2$ $-i + 1 : 2^2$	$2 : 2^2$ $-2 : 2^2$	$2 * i + 2 : 2^2$ $2 * i - 2 : 2^2$ $-2 * i + 2 : 2^2$ $-2 * i - 2 : 2^2$	$i + 3 : 12^2$ $i - 3 : 12^2$	4 : 10128 -4 : 144	4 : 400 -4 : 16 4i : 8 ² -4i : 8 ²	$3 * i + 3 : 0$ $3 * i - 3 : 0$ $-3 * i + 3 : 0$ $-3 * i - 3 : 0$	$3 * i - 3 : 2^2$ $-3 * i - 3 : 2^2$
v	20	26	32	34	36	40		
# of C	1	1	1	1	3	1		
Eigenvalues and # of X	$4 * i + 2 : 12^2$ $4 * i - 2 : 12^2$ $-2 * i + 4 : 12^2$ $-2 * i - 4 : 12^2$	$i + 5 : 260^2$ $i - 5 : 260^2$	$4 * i + 4 : 140^2$ $4 * i - 4 : 12^2$ $-4 * i + 4 : 140^2$ $-4 * i - 4 : 12^2$	$3 * i + 5 : 2^2$ $-3 * i + 5 : 2^2$	6 : 66 ² 6 : 64 ²	6 : 4356 6 : 64 ²	$6 * i + 2 : 12^2$ $6 * i - 2 : 12^2$ $2 * i + 6 : 144^2$ $2 * i - 6 : 144^2$ $-6 * i + 2 : 12^2$ $-6 * i - 2 : 12^2$	
v	50							
# of C	8							
Eigenvalues and # of X	$i - 7 : 2^2$ $-i - 7 : 2^2$	$i - 7 : 2^2$ $-i - 7 : 2^2$	$5 * i + 5 : 104$ $-5 * i + 5 : 2^2$	$5 * i + 5 : 104$ $-5 * i + 5 : 2^2$	5 * i + 5 : 104 -5 * i + 5 : 104	5 * i + 5 : 2 ² -5 * i + 5 : 2 ²	$i + 7 : 11452^2$ $i - 7 : 11452^2$	
v	52	58	64	68	72			
# of C	1	1	3	1	2			
Eigenvalues and # of X	$6 * i + 4 : 260^2$ $6 * i - 4 : 260^2$ $-4 * i + 6 : 260^2$ $-4 * i - 6 : 260^2$	$3 * i + 7 : 0$ $-3 * i + 7 : 0$	8 : 165504 -8 : 16 ²	8 : - -8 : - 8 * i : 7424 -8 * i : 7424	8 : 171008 -8 : 1024 8 * i : 176 ² -8 * i : 112 ²	$2 * i + 8 : 2^2$ $-2 * i + 8 : 2^2$ 8 * i + 2 : 2 ² -8 * i + 2 : 2 ²	$6 * i + 6 : 0$ $6 * i - 6 : 0$ $-6 * i + 6 : 0$ $-6 * i - 6 : 0$	$6 * i + 6 : 60^2$ $6 * i - 6 : 0$ $-6 * i + 6 : 60^2$ $-6 * i - 6 : 0$

Table 2 continued

v # of C	74 2	80 1	82 2	90 1
Eigenvalues and # of X	$5 * i - 7 : 2^2$ $-5 * i - 7 : 2^2$	$5 * i - 7 : 2^2$ $-5 * i - 7 : 2^2$	$i + 9 : 2^2$ $-i + 9 : 2^2$	$9 * i + 3 : 0$ $-9 * i + 3 : 0$
		$4 * i + 8 : 12^2$ $4 * i - 8 : 12^2$ $-4 * i + 8 : 396^2$ $-4 * i - 8 : 396^2$ $8 * i + 4 : 396^2$ $8 * i - 4 : 396^2$ $-8 * i + 4 : 12^2$ $-8 * i - 4 : 12^2$		

research project to enrich the known databases, even in the cases where complete enumeration of equivalence classes is not feasible. In the same vein, refining the classification of complex Hadamard matrices of [3] for $v \leq 12$, from equivalence to strong equivalence would be of interest.

9 Appendix on complex Hadamard matrices

In this appendix, we indicate how we constructed the matrices used in our computer experiments. The corresponding complex Hadamard matrices are publicly available on [Github](#).²

9.1 Order 8

The matrix is obtained by applying our Proposition 5.

9.2 Order 10

The matrix is obtained by applying our Proposition 8.

9.3 Order 16

One matrix is obtained applying our Theorem 2. The other matrix is obtained from the real Bush-type Hadamard matrix from a matrix in [12], by multiplying all off-diagonal blocks by i .

9.4 Order 18

The matrix is constructed from four Williamson type matrices of order 9 obtained from the database [15] upon using Lemma 6 of [13].

9.5 Order 20

The matrix is obtained by applying our Proposition 5.

9.6 Order 26

The matrix is obtained by applying our Proposition 8.

9.7 Order 32

The matrix is obtained by applying our Proposition 5.

² https://github.com/Qomo-CHENG/Hadamard_bent_complex.

9.8 Order 34

The matrix is constructed from four Williamson type matrices of order 17 obtained from the database [15] upon using Lemma 6 of [13].

9.9 Order 36

One matrix is obtained from the complex Hadamard matrix of order 6 using our Theorem 2. Two matrices are obtained from the real Bush-type Hadamard matrices of order 36 given in [10, 11] by multiplying the off-diagonal blocks with i .

9.10 Order 40

The matrix is obtained by applying our Proposition 5.

9.11 Order 50

One matrix is obtained by applying our Proposition 8. The other matrices are constructed from four Williamson type matrices of order 25 obtained from the database [15] upon using Lemma 6 of [13].

9.12 Order 52

The matrix is obtained by applying our Proposition 5.

9.13 Order 58

The matrix is constructed from four Williamson type matrices of order 29 obtained from the database [15] upon using Lemma 6 of [13].

9.14 Order 64

Two matrices are constructed from two complex Hadamard matrices of order 8 obtained from the database [3] upon using our Theorem 2. Another matrix is obtained from a real Hadamard matrix of order 8, using the proposition 7.

9.15 Order 68

The matrix is obtained by applying our Proposition 5.

9.16 Order 72

Two matrices are obtained by applying our Proposition 5.

9.17 Order 74

Two matrices are constructed from four Williamson type matrices of order 37 obtained from the database [15] upon using Lemma 6 of [13].

9.18 Order 80

The matrix is obtained by applying our Proposition 5.

9.19 Order 82

One matrix is constructed from four Williamson type matrices of order 41 obtained from the database [15] upon using Lemma 6 of [13]. Another matrix is obtained by applying our Proposition 8.

9.20 Order 90

The matrix is constructed from four Williamson type matrices of order 45 obtained from the database [15] upon using Lemma 6 of [13].

References


1. Balonin N.A., Seberry J.: A review and new symmetric conference matrices. *Informatsionno-upravlyayushchie sistemy* **4**(71), 2–7 (2014).
2. Bömer L., Antweiler M.: Periodic complementary binary sequences. *IEEE Trans. Inf. Theory* **36**(6), 1487–1494 (1990). <https://doi.org/10.1109/18.59954>.
3. Bruzda W., Tadej W., Zyczkowski K.: Catalogue of Complex Hadamard Matrices. (2009). <https://chaos.if.uj.edu.pl/~karol/hadamard/index.html>
4. Carlet C., Danielsen L.E., Parker M.G., Solé P.: Self-dual bent functions. *Int. J. Inf. Coding Theory* **1**(4), 384–399 (2010). <https://doi.org/10.1504/IJICoT.2010.032864>.
5. Crnković D., Švob A.: Switching for 2-designs. *Des. Codes Cryptogr.* **90**, 1585–1593 (2022). <https://doi.org/10.1007/s10623-022-01059-7>.
6. Frank R.: Polyphase complementary codes. *IEEE Trans. Inf. Theory* **26**(6), 641–647 (1980). <https://doi.org/10.1109/TIT.1980.1056272>.
7. Golay M.J.E.: Multi-slit spectrometry. *J. Opt. Soc. Am.* **39**(6), 437–444 (1949). <https://doi.org/10.1364/JOSA.39.000437>.
8. Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.: The Z_4 -linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inf. Theory* **40**(2), 301–319 (1994). <https://doi.org/10.1109/18.312154>.
9. Horadam K.J.: *Hadamard Matrices and Their Applications*. Princeton University Press, Princeton (2007).
10. Janko Z.: The existence of a Bush-type Hadamard matrix of order 36 and two new infinite classes of symmetric designs. *J. Comb. Theory Ser. A* **95**(2), 360–364 (2001). <https://doi.org/10.1006/jcta.2000.3166>.
11. Janko Z., Kharaghani H.: A block negacyclic Bush-type Hadamard matrix and two strongly regular graphs. *J. Comb. Theory Ser. A* **98**(1), 118–126 (2002). <https://doi.org/10.1006/jcta.2001.3231>.
12. Kharaghani H.: On the twin designs with the ionin-type parameters. *Electron. J. Comb.* **7**(R1), 1–11 (2000). <https://doi.org/10.37236/1479>.
13. Kharaghani H., Seberry J.: Regular complex Hadamard matrices. *Congr. Numer.* **75**, 187–201 (1990).
14. Kharaghani H., Seberry J.: The excess of complex Hadamard matrices. *Graphs Comb.* **9**(1), 47–56 (1993). <https://doi.org/10.1007/BF01195326>.
15. Koukouvinos C.: Design Theory Directory. <http://www.math.ntua.gr/~ckoukou/>
16. MacWilliams F.J., Sloane N.J.A.: *The Theory of Error-Correcting Codes*. North Holland, Amsterdam (1977).

17. Moorhouse G.E.: The 2-transitive complex Hadamard matrices. <http://ericmoorhouse.org/pub/complex.pdf>
18. Shi M.J., Li Y.Y., Cheng W., Crnković D., Krotov D., Solé P.: Self-dual Hadamard bent sequences. *J. Syst. Sci. Complex.* (2022), to appear. [arXiv:2203.16439](https://arxiv.org/abs/2203.16439)
19. Sivaswamy R.: Multiphase complementary codes. *IEEE Trans. Inf. Theory* **24**(5), 546–552 (1978). <https://doi.org/10.1109/TIT.1978.1055936>.
20. Sok L., Shi M.J., Solé P.: Classification and construction of quaternary self-dual bent functions. *Cryptogr. Commun.* **10**(2), 277–289 (2018). <https://doi.org/10.1007/s12095-017-0216-y>.
21. Solé P., Cheng W., Guilley S., Rioul O.: Bent Sequences over Hadamard Codes for Physically Unclonable Functions. *IEEE International Symposium on Information Theory*, 801–806 (2021) <https://doi.org/10.1109/ISIT45174.2021.9517752>
22. Tadej W., Życzkowski K.: A concise guide to complex Hadamard matrices. <https://arxiv.org/pdf/quant-ph/0512154.pdf>
23. Turyn R.J.: An infinite class of Williamson matrices. *J. Comb. Theory Ser. A* **12**(3), 319–321 (1972). [https://doi.org/10.1016/0097-3165\(72\)90095-7](https://doi.org/10.1016/0097-3165(72)90095-7).
24. van Lint J.H., Wilson R.: *A Course in Combinatorics*, 2nd edn Cambridge University Press, Cambridge (2001).
25. Wallis J.: Complex hadamard matrices. *Linear Multilinear Algebra* **1**(3), 257–272 (1973). <https://doi.org/10.1080/03081087308817024>.
26. Zinoviev V.A., Zinoviev D.: On the generalized concatenated construction for the L_1 and Lee metrics. *Probl. Inf. Transm.* **57**(1), 70–83 (2021). <https://doi.org/10.1134/S003294602101004X>.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Authors and Affiliations

Minjia Shi¹  · Yaya Li¹ · Wei Cheng² · Dean Crnković³ · Denis Krotov⁴ · Patrick Solé⁵

Yaya Li
yayali187125@163.com

Wei Cheng
wei.cheng@telecom-paris.fr

Dean Crnković
deanc@math.uniri.hr

Denis Krotov
krotov@math.nsc.ru

Patrick Solé
sole@enst.fr

¹ Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei 230601, Anhui, China

² Télécom Paris, Secure-IC S.A.S., 104 Boulevard du Montparnasse, 75014 Paris, France

³ Faculty of Mathematics, University of Rijeka, Rijeka 51000, Croatia

⁴ Sobolev Institute of Mathematics, Novosibirsk, Russia 630090

⁵ CNRS, University of Aix Marseille, Centrale Marseille, I2M, Marseille, France