Self-dual bent sequences for complex Hadamard matrices

Minjia Shi, Yaya Li, Wei Cheng, Dean Crnković, Denis Krotov, Patrick Solé

Self-dual bent sequences for complex Hadamard matrices

Minjia Shi, Yaya Li[*], Wei Cheng[†], Dean Crnković[‡], Denis Krotov[§], Patrick Solé[¶]

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 98. We use three competing methods of generation: Brute force, Linear Algebra and Groebner bases. Regular Hadamard matrices and Bush-type 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.

Keywords: PUF functions, Bent sequences, Hadamard matrices, regular Hadamard matrices, Bush-type Hadamard matrices

AMS Classification (MSC 2010): Primary 94D10, Secondary 15B34

[*]Minjia Shi and Yaya Li, School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China, smjwcl.good@163.com, yayali187125@163.com

[†]Télécom Paris; Secure-IC S.A.S., 104 Boulevard du Montparnasse, 75014 Paris, France, wei.cheng@telecom-paris.fr

[‡]Department of Mathematics, University of Rijeka, Croatia, deanc@math.uniri.hr

[§]Sobolev Institute of Mathematics,Novosibirsk 630090, Russia, krotov@math.nsc.ru

[¶]CNRS, University of Aix Marseille, Centrale Marseille, I2M, Marseille, France, sole@enst.fr

1 Introduction

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

$$CC^* = nI,$$

where * denotes the transpose conjugate, and I is the identity matrix of order n. They were introduced by Turyn and studied by Seberry [10], and Kharaghani [4, 5], among others. A survey is [9]. A webpage is [14]. Complex Hadamard matrices are conjectured to exist for all even n [10].

If n is even and the sum of two squares $n = a^2 + b^2$, then at least one **regular** C is conjectured to exist.

Recently, a notion of bent sequences attached to Hadamard matrices was introduced in [8] from a motivation of security. In a companion paper [11] the self-dual subclass bent sequences for Hadamard matrices is studied. In the present paper we conduct the analogous study for complex Hadamard matrices. The main hurdle in this generalization was in the definition, as explained in the Preliminaries section.

2 Preliminaries

A self-dual bent sequence attached to the complex Hadamard matrix C is defined as $X \in \Omega_4^n$ such that

$$CX = \lambda X,$$

where λ is an eigenvalue of C.

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

Proof. By the Hadamard property we see that $|\lambda|^2 = n$. By eigenvalue definition, we see that $\lambda = a + ib \in \mathbb{Z}[i]$. Taking squared norms we get $n = a^2 + b^2$. If one of a, b is zero then n is a square. If both are non zero then n is a sum of two squares. □

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

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

where $(\pm a + \pm ib)$ is an eigenvalue 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 $n = 2^{2m} = (2^m)^2$, and C the Sylvester Hadamard matrix of order n such sequences were studied in [12]. The case of n a square and C an arbitrary real Hadamard matrix is treated in [11].

The even integers ≤ 98 and sum of at most two squares are

$$\{2, 4, 8, 10, 16, 18, 20, 26, 32, 34, 36, 40, 50, 52, 58, 64, 68, 72, 74, 80, 82, 90, 98\}.$$

3 Constructions of Complex Hadamard matrices

3.1 Kronecker products

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

Proposition 2 *If there exists a Hadamard matrix H of order n, then there exists a complex Hadamard matrix C of order $2n$. 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 $CC^* = 2nI$ 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: The matrix C in this Theorem has an order 4 or a multiple of 8. This is a special case of Theorem 1 of [10]: The Kronecker product of a Hadamard matrix of order n by a complex 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: 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.

3.2 Bush type

A complex analogue of the Bush-type Hadamard matrix is the following result, inspired by [3, Th. 1]. Similar constructions appear in [4, §5].

Theorem 1 *Let there exists a complex Hadamard matrix of order* $2n$*. Then there exists a Bush-type complex Hadamard matrix of order* $4n^2$*. This matrix is regular of row sum* $2n$*.*

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

1. $C_i^t = C_i$, for $i = 1, 2, \ldots, 2n$.
2. $C_1 = J_{2n}$, $C_i J_{2n} = J_{2n} C_i = 0$, for $i = 2, 3, \ldots, 2n$.
3. $C_i C_j^* = 0$, for $i \neq j, 1 \leq i, j \leq 2n$.
4. $C_1 C_1^* + C_2 C_2^* + \cdots + C_{2n} C_{2n}^* = 4n^2 I_{2n}$.

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

□

Example: 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

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

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

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

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

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

Proposition 3 *Let there exist a Bush-type Hadamard matrix of order n^2. Then there exists a Bush-type complex Hadamard matrix of order n^2 having the entries belonging to the set Ω_4.*

Proof.

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

□

3.3 Conference matrices

A construction indicated in [2, p.67] and in [10, Theorem 3] is connected to Paley II. The Jacobsthal matrix is the matrix C_q defined in [7, chap. 2, §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:

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

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 [6, 8].

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

with $\mathbf{j}$ being an all one row vector of length q.

Proposition 4 *If q is a prime power $\equiv 1 \pmod 4$, and S_q denotes the extended Jacobstahl 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 [7, 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

$$\{10, 18, 26, 50, 58, 74, 82, 90, 98\}.$$

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

Proposition 5 *Let q be a prime power $\equiv 1 \pmod 4$, and with S denoting the extended Jacobstahl matrix, write $C = iI + S_q$. The minimal polynomial of C is*

$$x^2 - 2ix - (q+1).$$

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

$$\{10, 26, 50, 82\}.$$

3.4 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

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

where i, j, k are quaternionic units given by

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

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 [5], 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 [4] exploits this correspondance to construct regular complex Hadamard matrices. In the next result, we use a similar construction.

Theorem 2 *If there is a Hadamard matrix H of order $4t^2$ with structure $H = \begin{pmatrix} R & S \\ -S & R \end{pmatrix}$ 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 [4]. 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: By [13], we know that the matrix H in this theorem can be constructed in relation with Williamson matrices.

4 Coding theoretic interpretation

Let C be a quaternary code of length n over the alphabet Ω_4. Let Z be the $\mathbb{Z}_4$ code determined by $i^Z = C$. The distance properties of C for the squared Euclidean distance d_E are equivalent to the distance properties of 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* H is a code of length n over Ω_4 with $|H| = n$ codewords that are pairwise orthogonal for the standard hermitian inner product $<,>$ in dimension n. Thus we can think of its codewords as the rows of a complex Hadamard matrix of size n. The *deviation* $\theta(C, x)$ of an arbitrary vector $x \in \Omega_4^n$ from C is defined as

$$\theta(C, x) = \max\{| < x, y > | \mid y \in C\}.$$

It can be seen by expanding $< x-y, x-y >$ that $\Re(< x, y >) = n - d_L(u, v)$, for all $x, y \in \Omega_4^n$. The *total deviation* of the code C is then

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

Proposition 6 *If there is a bent sequence for a complex Hadamard matrix H of order n, then its corresponding Hadamard code C has deviation $\theta(C) = \sqrt{n}$.*

Proof. See [8, Th. 1] for a euclidean inner product version. □

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

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

The simple inequality $\Re(< x, y >) \leq | < x, y > |$ shows that

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

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

Corollary 1 *If there is a bent sequence for a complex Hadamard matrix H of order n, then the covering radius of its attached $\mathbb{Z}_4$ code is bounded below as*

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

This is less satisfying that [11, Lemma 1].

5 Search methods

5.1 Brute force

This method is only applicable for small v's.

1. Construct C a Hadamard matrix of order v like in [8] by using Magma database.
2. For all $X \in \Omega_4^v$ compute $Y = HX$. If $Y = (a+ib)X$, then X is self-dual bent for C.

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

5.2 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.

5.3 Linear Algebra

1. Construct C a complex Hadamard matrix of order v by the Appendix, Section 7, or the database [14].

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.

1. Initialize J at $J = [1]$

2. 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 $J' = Append(J, \ell)$

3. If $r < r'$ then update $J := J'$

4. Repeat until $|J| = rank(B)$

Remark: If the first column of B is zero, step 1 does not make sense, but then there is no self-dual bent sequence in that situation, as all eigenvectors have first coordinate zero.

Complexity: Roughly of order $v^3 2^k$. 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.

6 Numerical examples

7 Conclusion

8 Appendix on Hadamard matrices

In this appendix, we indicate how we constructed the matrices used in our computer experiments.

8.1 Order 16

One matrix is obtained applying our Theorem 1 . The other matrix is obtained from the real Bush-type Hadamard matrix from a matrix in [3], by multiplying all off-diagonal blocks by i.

8.2 Order 36

One matrix is obtained from the complex Hadamard matrix of order 6 using our Theorem 1. Two matrices are obtained from the real Bush-type Hadamard matrices of order 36 given in [15, 16].

9 Order 64

Two matrices were constructed from two complex Hadamard matrices of order 8 obtained from the database [14] upon using our Theorem 1. Another matrix was obtained from a real Hadamard matrix of order 8, using the proposition 3.

References

[1] N. A. Balonin, J. Seberry, A Review and New Symmetric Conference Matrices,Informatsionno-upravliaiushchie sistemy, 71 (4), 2-7. https://ro.uow.edu.au/cgi/viewcontent.cgi?referer=&httpsredir=1 &article=3757&context=eispapers.

[2] Horadam, K. J. *Hadamard matrices and their applications.* Princeton University Press, Princeton, NJ, (2007).

[3] H. Kharaghani, On the twin designs with the Ionin-type parameters, Electron. J. Comb. 7 (2000), Research paper R1, 11 p.

[4] H. Kharaghani, J. Seberry, Regular complex Hadamard matrices, Proceedings of the Nineteenth Manitoba Conference on Numerical Mathematics and Computing (Winnipeg, MB, 1989), Congr. Numer. 75 (1990), 187–201. (https://documents.uow.edu.au/~jennie/WEB/WEB69-93/max/s)

[5] H. Kharaghani, J. Seberry, The excess of complex Hadamard matrices, Graphs and Combinatorics (1993) 9: 47–56
https://ro.uow.edu.au/cgi/viewcontent.cgi?referer=&httpsredir=1
&article=2088&context=infopapers

[6] J.H. van Lint, R. Wilson, *A course in Combinatorics*, second edition, Cambridge University Press (2001), Cambridge.

[7] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes*. North-Holland , Amsterdam, (1977)

[8] P., Solé, W., Cheng, S., Guilley, O., Rioul, Bent Sequences over Hadamard Codes for Physically Unclonable Functions. ISIT 2021: 801–806 (2021). https://perso.telecom-paristech.fr/rioul/publis/202102solechengguilleyrioul.pd

[9] https://arxiv.org/pdf/quant-ph/0512154.pdf

[10] https://ro.uow.edu.au/cgi/viewcontent.cgi?article=1965&context=infopapers

[11] Minjia Shi, Yaya Li, Wei Cheng, Denis Krotov, Dean Crnković, Patrick Solé, Self-dual Hadamard bent sequences, submitted.

[12] Lin Sok, Minjia Shi, Patrick Solé Classification and Construction of quaternary self-dual bent functions. Cryptogr. Commun. 10(2): 277-289 (2018).

[13] RJ Turyn, An infinite class of Williamson matrices, J. of Combinatorial Th. A **12**, (1972), 319–321.

[14] W. Bruzda, W. Tadej, K. Zyczkowski, "Catalogue of Complex Hadamard Matrices", available online athttps://chaos.if.uj.edu.pl/k̃arol/hadamard/index.html

[15] Z. Janko, The existence of a Bush-type Hadamard matrix of order 36 and two new infi nite classes of symmetric designs, J. Comb. Theory, Ser. A 95, no. 2, pp. 360-364, 2001.

[16] Z. Janko and H. Kharaghani, A block negacyclic Bush-type Hadamard matrix and two strongly regular graphs, J. Comb. Theory, Ser. A. 98, no. 1, pp. 118-126, 2002,