J Syst Sci Complex (2023) 36: 894–908

Self-Dual Hadamard Bent Sequences*

SHI Minjia · LI Yaya · CHENG Wei · CRNKOVIĆ Dean · KROTOV Denis · SOLÉ Patrick

DOI: 10.1007/s11424-023-2276-8
Received: 26 June 2022 / Revised: 5 September 2022

Abstract A new notion of bent sequence related to Hadamard matrices was introduced recently, motivated by a security application (Solé, et al., 2021). The authors study the self-dual class in length at most 196. The authors use three competing methods of generation: Exhaustion, Linear Algebra and Gröbner bases. Regular Hadamard matrices and Bush-type Hadamard matrices provide many examples. The authors conjecture that if v is an even perfect square, a self-dual bent sequence of length v always exists. The authors introduce the strong automorphism group of Hadamard matrices, which acts on their associated self-dual bent sequences. The authors give an efficient algorithm to compute that group.

Keywords Bent sequences, bush-type Hadamard matrices, Hadamard matrices, PUF functions, regular Hadamard matrices.

1 Introduction

Bent functions and bent sequences are classical objects in algebraic combinatorics with sundry connections to design theory, distance regular graphs, and symmetric cryptography[1, 2].

SHI Minjia · LI Yaya
Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei 230601*, China; State Key Laboratory of Information Security (Institute of Information Engineering), Chinese Academy of Sciences, Beijing* 100093*, China.*
Email: smjwcl.good@163.com; yayali187125@163.com.
CHENG Wei
LTCI, Télécom Paris, 91120 *Palaiseau, France; Secure-IC S.A.S.,* 104 *Bd du Montparnasse,* 75014 *Paris, France.* Email: wei.cheng@telecom-paris.fr.
CRNKOVIĆ Dean
Faculty of Mathematics, University of Rijeka, Croatia. Email: deanc@math.uniri.hr.
KROTOV Denis
Sobolev Institute of Mathematics, Novosibirsk 630090*, Russia.* Email: krotov@math.nsc.ru.
SOLÉ Patrick
Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France. Email: sole@enst.fr.
*This work is supported in part by the National Natural Science Foundation of China under Grant No. 12071001. The work of Dean Crnković is supported by Croatian Science Foundation under the project 6732.
◇ *This paper was recommended for publication by Editor DENG Yingpu.*

In [3] a new notion of bent sequence was introduced as a solution in X, Y to the system

$$\mathcal{H}X = Y,$$

where H is a Hadamard matrix of order v, normalized to $\mathcal{H} = H/\sqrt{v}$ and $X, Y \in \{\pm 1\}^v$. Given H the vector X defines a *Hadamard bent* (binary) sequence by the correspondence

$$x \mapsto (X_x + 1)/2.$$

When v is a power of 2 and H is the Hadamard matrix of Sylvester type, we recover the classical notion of bent sequence[1, 2]. They meet the covering radius of Hadamard codes (see §2, Lemma 2.1) in the same way that classical bent functions meet the covering radius of the first order Reed-Muller code [4, Chap.14, Th.6]. Beyond generalization for the sake of generalization, this notion was introduced in [3] from a cryptographic perspective (see §6 for details). We believe this concept has a combinatorial interest of its own, as it pertains to the fine print of Hadamard matrix theory: Regular matrices, and automorphism groups.

It is proved in [3] that this kind of bent sequence can only exist if v is a perfect square. As is well-known, Hadamard matrices of order $v > 2$ only exist for v a multiple of 4. Thus we reduce to $v = 4m^2 = (2m)^2$ with m an integer (in practice $1 \leq m \leq 7$).

In [5], when H is of Sylvester type, a linear algebra technique is used to find **self-dual** bent sequences, a situation which corresponds to the case $X = Y$ in the above equation. Namely X is, in particular, an eigenvector associated to the eigenvalue 1 of $\mathcal{H}$. The condition $X \in \{\pm 1\}^v$ has to be checked independently, using a basis of the eigenspace.

In order for the approach of [5] to work for more general Hadamard matrices than Sylvester type, we need to assume that $\mathcal{H}$ has the eigenvalue 1 in its spectrum, and that the dimension of the associated eigenspace is not too large, as this parameter controls the complexity of the search. Another algebraic technique consists in reducing the existence of a sequence of length v to a quadratic system in v variables, which can be solved by using Gröbner bases. This second method works well as long as the number of variables is less than one hundred. The brute force approach which consists in checking all 2^v possible X's is not feasible for $v > 30$, say.

A connection with regular Hadamard matrices is pointed out. Every regular Hadamard matrix admits the all-one vector as a self-dual bent sequence. In particular, Bush-type Hadamard matrices of order $v = 4u^2$ afford at least 2^{2u} self-dual bent sequences. The Karaghani conjecture[6] on the existence of regular Hadamard matrices suggests then that self-dual bent sequences exist for all even perfect square orders (Conjecture 3.10). This conjecture is satisfied for all even square orders where a regular Hadamard matrix exists. The first unknown order seems to be $v = 4u^2$ for $u = 47$.

We introduce the notion of strong automorphism group of a Hadamard matrix. This group acts on the associated self-dual bent sequences. We give an efficient algorithm to compute it, based on a digraph defined from the matrix. We also connect this group to the group of polarities of the Menon design defined by the matrix.

The material is organized as follows. The next section collects notions and notations needed in the following sections. Section 3 investigates interesting properties of self-dual bent sequences,

and Section 4 develops three search methods. Section 5 displays the numerical results we found. Section 6 introduces the application of Hadamard bent sequences. Section 7 concludes the article. An appendix develops the construction techniques of Hadamard matrices of order 16, 36, 64, 100, 144 and 196.

2 Background Material

2.1 Hadamard Matrices

A **Hadamard matrix** H of order v is a v by v real matrix with entries ± 1 satisfying $HH^t = vI_v$, where H^t is the transpose of H and I_v is the identity matrix of order v. If $v > 2$, it is well-known that v must be a multiple of 4[4]. An important construction of Hadamard matrices, due to **Sylvester** is obtained for $v = 2^h$, when H is indexed by binary vectors of length h and $H_{xy} = (-1)^{\langle x,y\rangle}$, where $\langle x, y\rangle = \sum_{i=1}^{h} x_i y_i$. We denote henceforth this matrix by S_v. For more general constructions, properties and applications of Hadamard matrices we refer the reader to [7]. A Hadamard matrix of order v is **normalized** if both first row and first column are equal to the all-one vector. A Hadamard matrix of order v is **regular** if its v row and column sums are all equal to a constant σ. In that case, it is known that $v = 4u^2$ with u a positive integer and that $\sigma = 2u$ or $-2u$[8]. A special class is that of **Bush-type** Hadamard matrices[9]. A Hadamard matrix of order $v = 4u^2$ is said to be Bush-type if it is blocked into $2u$ blocks of side $2u$, denoted by H_{ij}, such that the diagonal blocks H_{ii} are all-ones, and that the off-diagonal blocks have row and column sums zero.

2.2 Bent Boolean Functions

A Boolean function f of arity h is any map from $\mathbb{F}_2^h$ to $\mathbb{F}_2$. The sign function of f is defined by $F(x) = (-1)^{f(x)}$. The Walsh-Hadamard transform of f is defined as

$$\widehat{f}(y) = \sum_{x \in \mathbb{F}_2^h} (-1)^{\langle x,y\rangle + f(x)}.$$

Thus in term of vectors

$$\widehat{f} = S_v F.$$

A Boolean function f is said to be **bent** iff its Walsh-Hadamard transform takes its values in $\{\pm 2^{h/2}\}$. Such functions can only exist if h is even. The dual of a bent function f is defined by its sign function $\widehat{f}/2^{h/2}$[5]. A bent function is said to be **self-dual** if it equals its dual. In terms of the Sylvester matrix the sign function F of a self-dual bent function satisfies $\mathcal{S}_v F = F$ where $\mathcal{S}_v = \frac{S_v}{2^{h/2}}$ and $v = 2^h$.

2.3 Hadamard Bent Sequences

If H is a Hadamard matrix of order v a **bent sequence** of length v attached to H is any vector $X \in \{\pm 1\}^v$, such that

$$\mathcal{H}X = Y,$$

where $\mathcal{H} = H/\sqrt{v}$ and $Y \in \{\pm 1\}^v$.

The **dual** sequence of X is defined by $Y = \mathcal{H}X$. If $Y = X$, then X is a **self-dual** bent sequence attached to H. It is easy to see that the vector Y is itself a bent sequence attached to H^t. When $H = S_v$ we recover the definitions of the preceding subsection.

2.4 Hadamard Codes

We consider codes over the alphabet $A = \{\pm 1\}$. If H is a Hadamard matrix of order v, we construct a code C of length v and size $2v$ by taking the columns of H and their opposites. Let $d(\cdot, \cdot)$ denote the Hamming distance on A. The **covering radius** of a code C of length v over A is defined by the formula

$$r(C) = \max_{y \in A^v} \min_{x \in C} d(x, y).$$

The following lemma is immediate by Theorems 1 and 2 of [3].

Lemma 2.1 *Let v be an even perfect square, and let H be a Hadamard matrix of order v, with the associated Hadamard code C. The vector $X \in A^v$ is a bent sequence attached to H iff*

$$\min_{Y \in C} d(X, Y) = r(C) = \frac{v - \sqrt{v}}{2}.$$

Remark 2.2 This lemma generalizes nicely Theorem 6 of [4, Chap. 14].

2.5 Graphs

A directed graph (**digraph** for short) on a set V of vertices is determined by a set of arcs $E \subseteq V \times V$. Declare two vertices x, y adjacent and write $x \sim y$ iff $(x, y) \in E$. The **adjacency matrix** A is then defined by

$$A_{xy} = \begin{cases} 1 & \text{if } x \sim y, \\ 0 & \text{if } x \nsim y. \end{cases}$$

The **automorphism group** of such a digraph is the group of permutations on V that preserve incidence.

3 Properties of Self-Dual Bent Sequences

3.1 Automorphism Groups

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

- row permutation,
- column permutation,
- row or column negation,

which form a group $G(v)$ with structure $\{\mathrm{Sym}(v) \wr \mathrm{Sym}(2)\}^2$, where $\mathrm{Sym}(n)$ denotes the symmetric group on n letters, and $\wr$ denotes the wreath product. We denote by $S(v)$ the group of diagonal matrices of order v with diagonal elements in $\{\pm 1\}$, and by $M(v)$ the matrix group

generated by $P(v)$, the group of **permutation matrices** of order v, and $S(v)$. The action of $G(v)$ on a Hadamard matrix H is of the form

$$H \mapsto PHQ,$$

with $P, Q \in M(v)$. The **automorphism group** $\mathrm{Aut}(H)$ of a Hadamard matrix H is defined classically as the set of all pairs $(P, Q) \in G(v)$ such that $PHQ = H$[10]. Some information on this group in the case of Paley matrices can be found in [11–13]. The cases of type I and type II (i.e., $q \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$ where q is the prime power in the definition of Paley matrix) were exactly determined in [13] and [14], respectively. The automorphism group of (a generalization of) the Sylvester matrix can be found in [12, p. 101–103]. We give a characterization of $\mathrm{Aut}(H)$ for the Sylvester matrix S_v.

Consider the action of an **extended affine transform** $T_{A,b,d,c}$ on a Boolean function f, i.e.,

$$f(x) \mapsto f(A^{-1}x + A^{-1}b) \cdot (-1)^{\langle d,x\rangle} \cdot c,$$

where A is an m-by-m invertible matrix over $\mathbb{F}_2$, $b \in \mathbb{F}_2^m$, $d \in \mathbb{F}_2^m$, $c \in \{1, -1\}$.

Theorem 3.1 *The pair* $(T_{A,b,d,c}, T_{(A^{-1})^t,d,b,c(-1)^{\langle b,d\rangle}})$ *is in* $\mathrm{Aut}(S_v)$.

Proof By definition of S_v, where $v = 2^m$, we have $g = S_v f$ iff $g(y) = \sum_{x\in\mathbb{F}_2^m} f \cdot (-1)^{\langle x,y\rangle}$. We compute $S_v T_{A,b,d,c}(f)$ by the same formula

$$\begin{aligned}
\sum_{x\in\mathbb{F}_2^m} T_{A,b,d,c}f(x) \cdot (-1)^{\langle x,y\rangle} &= \sum_{x\in\mathbb{F}_2^m} f(A^{-1}x + A^{-1}b) \cdot (-1)^{\langle d,x\rangle} \cdot c \cdot (-1)^{\langle x,y\rangle} \\
&= c \cdot \sum_{x'\in\mathbb{F}_2^m} f(x') \cdot (-1)^{\langle Ax'+b,y+d\rangle} \quad \textit{//By taking } x = Ax' + b \\
&= c \cdot (-1)^{\langle b,y+d\rangle} \cdot \sum_{x'\in\mathbb{F}_2^m} f(x') \cdot (-1)^{\langle Ax',y+d\rangle} \\
&= c(-1)^{\langle b,d\rangle} \cdot (-1)^{\langle b,y\rangle} \cdot \sum_{x'\in\mathbb{F}_2^m} f(x') \cdot (-1)^{\langle x',A^ty+A^td\rangle} \\
&= T_{(A^{-1})^t,d,b,c(-1)^{\langle b,d\rangle}} g(y).
\end{aligned}$$

Thus $S_v T_{A,b,d,c} f = T_{(A^{-1})^t,d,b,c(-1)^{\langle b,d\rangle}} g$ and the pair $(T_{A,b,d,c}, T_{(A^{-1})^t,d,b,c(-1)^{\langle b,d\rangle}})$ is in $\mathrm{Aut}(S_v)$. ∎

To work on the symmetries of bent sequences we will require the notion of **strong automorphism group** $\mathrm{SAut}(H)$ of H defined as the set of $P \in M(v)$ such that $PH = HP$. Then we can state the following result.

Proposition 3.2 *If X is a self-dual bent sequence for H, and if $P \in M(v)$ is a strong automorphism of H, then PX is also a self-dual bent sequence for H.*

Proof By hypothesis $\mathcal{H}X = X$. Multiplying on left this equation by P we get

$$PX = P\mathcal{H}X = \mathcal{H}PX.$$

Letting $Y = PX$, we see that $\mathcal{H}Y = Y$. ∎

A partial characterization in the case of $\mathrm{SAut}(S_v)$ is as follows. It is an immediate corollary of the preceding theorem and its proof is omitted.

Corollary 3.3 *An extended affine transform $T_{A,b,d,c}$ is in* $\mathrm{SAut}(S_v)$ *iff* $A^t = A^{-1}$, $b = d$ *and* $\mathrm{wt}_H(b)$ *is even.*

Remark 3.4 In particular, the number of such transforms is $|\mathcal{O}_m|2^m$ where $\mathcal{O}_m = \{A \in \mathrm{GL}(m, \mathbb{F}_2) \mid AA^t = I_m\}$. By [15, Theorem 4], we know that

- $|\mathcal{O}_m| = 2^{k^2} \prod_{i=1}^{k-1}(2^{2i} - 1)$ if $m = 2k$,
- $|\mathcal{O}_m| = 2^{k^2} \prod_{i=1}^{k}(2^{2i} - 1)$ if $m = 2k + 1$.

For the first few values of m, we get $1, 2, 8, 48, 768, 23040, 1474560, 185794560$.

A stronger characterization of the automorphism group of the set of self-dual bent functions within all Hamming isometric maps is in [16]. A weaker form of our corollary appears in [17, Theorem 1] where the group of invertible matrices A satisfying $A^t = A^{-1}$ is called the orthogonal group. An algorithm to compute the strong automorphism group is given at the end of the section.

Two Hadamard matrices H and K are **strongly equivalent** if there is $P \in M(v)$ such that $PHP^t = K$ (This relation is an equivalence relation on the set of Hadamard matrices). Then they share the same self-dual bent sequences, up to a monomial transform, as the next result, the main motivation for this new concept, shows.

Proposition 3.5 *If H and K are strongly equivalent Hadamard matrices, satisfying $K = PHP^t$, with $P \in M(v)$ then their respective sets of self-dual bent sequences, say $S(H)$ and $S(K)$, satisfy $S(H) = P^t S(K)$.*

Proof If $KX = \sqrt{v}X$ for some $X \in \{\pm 1\}^v$, then let $Y = P^t X$. We see that $HY = \sqrt{v}Y$ and that $Y \in \{\pm 1\}^v$. The result follows. ∎

The database of Magma collects the orbits of Hadamard matrices under $G(v)$ by their normalized representative. It is plain to see that the action of $G(v)$ does not preserve the self-dual bentness property. A simple example is given by the pair of equivalent matrices H and $-H$ who cannot allow a common nonzero self-dual bent sequence. In fact, the action of $G(v)$ can produce self-dual bent sequences as the next result shows.

Proposition 3.6 *If X is a bent sequence for H, then there is an equivalent Hadamard matrix H' such that X is a self-dual bent sequence for H'.*

Proof By hypothesis $\mathcal{H}X = Y$. There is a matrix $S \in S(v)$ such that $Y = SX$. Since S is an involution we have

$$X = S\mathcal{H}X = \mathcal{H}'X,$$

where $H' = SH$. ∎

3.2 Regular Hadamard Matrices

A direct connection between Hadamard bent sequences and regular Hadamard matrices is as follows.

Proposition 3.7 *If H is a regular Hadamard matrix of order $v = 4u^2$, with $\sigma = 2u$, then j is a self-dual bent sequence for H where j is the all-one vector of length v.*

Proof By definition of regular Hadamard matrices $Hj = \sigma j = \sqrt{v}j$, yielding $\mathcal{H}j = j$. ∎

Any construction of regular Hadamard matrices implies the existence of self-dual Hadamard bent sequences. The reference [18] yields the following result.

Corollary 3.8 *Let p and $2p-1$ be prime powers and $p \equiv 3 \pmod 4$, then there exists a self-dual Hadamard bent sequence of length $4p^2$. In particular $p = 3$ yields a self-dual Hadamard bent sequence of length 36, and $p = 7$ yields a self-dual Hadamard bent sequence of length 196.*

Another construction, valid for some primes $\equiv 7 \pmod{16}$ can be found in [19].

In fact each Bush-type Hadamard matrix implies the existence of many self-dual bent sequences.

Proposition 3.9 *If H is a Bush-type Hadamard matrix of order $v = 4u^2$, then there are at least 2^{2u} self-dual bent sequences for H.*

Proof From the definition, we see that the sequence X defined by

$$X^t = (\pm j, \cdots, \pm j),$$

where j is the all-one vector of length $2u$, and the $2u$ signs ± 1 are arbitrary, is a self-dual bent sequence. ∎

In view of Kharagani's conjecture that Bush-type Hadamard matrices exist for all even perfect square orders[6], the two previous propositions suggest the following.

Conjecture 3.10 *If v is an even perfect square, then there exists a self-dual Hadamard bent sequence for some Hadamard matrix of order v.*

We show that the Kronecker product of two self-dual bent sequences is also a self-dual bent sequence. Recall that the **Kronecker product** $K = X \otimes Y$ of two sequences X and Y of respective lengths v and w is defined by $K_{(i,j)} = X_i Y_j$. Similarly, the **Kronecker product** of two Hadamard matrices U and V of respective orders v and w can be defined as

$$(U \otimes V)_{(i,j),(k,\ell)} = U_{ij} V_{k\ell}.$$

Proposition 3.11 *If X and Y are two self-dual bent sequences with respective Hadamard matrices U and V, then $X \otimes Y$ is a self-dual bent sequence attached to $U \otimes V$.*

Proof As is well-known[8], if both U and V are Hadamard matrices then so is $(U \otimes V)$. Now the relations $X\sqrt{v} = UX$ and $Y\sqrt{w} = VY$ entail

$$(U \otimes V)(X \otimes Y) = \sqrt{vw}(X \otimes Y).$$

This completes the proof. ∎

This implies for instance, the existence of self-dual bent sequences of length $64 = 4 \times 16$, from the existence of self-dual bent sequences in lengths 4 and 16.

3.3 Computing the Strong Automorphism Group

3.3.1 The Strong Automorphism Group

Define a digraph $G(H)$ by its adjacency matrix $A(H)$ as follows. This matrix is obtained by replacing in H

- the 1's by $\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$,
- the -1's by $\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$.

Theorem 3.12 *The group* $\mathrm{SAut}(H)$ *is isomorphic to the automorphism group of* $G(H)$.

Proof First, we note that any automorphism of $G(H)$ do not break the *blocks* $\{0,1\}$, $\{1,2\},\cdots,\{2n-2,2n-1\}$ (we assume that the vertices of $G(H)$ are the indices of the corresponding columns/rows in $A(H)$). Indeed, two vertices are in the same block if and only if their neighborhoods do not intersect.

The rest is straightforward. Permuting blocks of vertices in $G(H)$ corresponds to permuting the column/row indices of H, while swapping two vertices in the same block corresponds to the negation of the corresponding row and column in H. ∎

Remark 3.13 This graphical method can also be used to check if two Hadamard matrices are strongly equivalent.

3.3.2 The Permutation Part

The permutation part $C(H)$ of the strong automorphism group $\mathrm{SAut}(H)$ defined by

$$C(H) = \{P \in P(v) \mid PH = HP\}$$

admits an intuitive interpretation in terms of directed graphs (**digraphs**). Let $\Gamma(H)$ denote the digraph with adjacency matrix A where $H = J - 2A$, and J denote the v by v all-one matrix.

Theorem 3.14 *The group* $C(H)$ *is the group of isomorphisms of* $\Gamma(H)$.

Proof Since $P \in P(v)$, we have $PJ = JP = J$. Thus $HP = PH$ iff $PA = AP$. Assume now that i, j have respective preimages h and k under P. Computing matrix products we get

$$(PA)_{hj} = a_{ij} = (AP)_{hj} = a_{hk}.$$

Thus $i \sim j$ iff $h \sim k$ which shows that P preserves adjacency in $\Gamma(H)$. ∎

Remark 3.15 The above proof is a direct extension of the proof of [20, Prop. 15.2] from graphs to digraphs.

Example 3.16 Let H be the Paley type II Hadamard matrix of order 36. Then Magma[21] commands `HadamardAutomorphismGroup` and `AutomorphismGroup` allow us to compute

- $|\mathrm{Aut}(H)| = 2^7 \times 3^2 \times 17$,
- $|\mathrm{SAut}(H)| = 2^5 \times 3^2 \times 17$,
- $|C(H)| = 2^3 \times 17$.

Note that the latter number divides the former, as it should, since $C(H)$ can be embedded in a subgroup of $\mathrm{Aut}(H)$ by writing $PHP^t = H$. More generally $|C(H)|$ divides $|\mathrm{SAut}(H)|$ which divides $|\mathrm{Aut}(H)|$. In table 1 we give the same information for the 5 matrices of order 16 in Magma database. The first row is the index j of H in the Magma database.

Table 1

j	1	2	3	4	5
$\lvert\mathrm{Aut}(H)\rvert$	$2^{15}\times 3^2\times 5\times 7$	$2^{12}\times 3\times 7$	$2^{12}\times 3\times 7$	$2^{15}\times 3^2$	$2^{14}\times 3$
$\lvert\mathrm{SAut}(H)\rvert$	$2^9\times 3^2\times 5$	2^2	2	2	2
$\lvert C(H)\rvert$	$2^4\times 3^2\times 5$	1	1	1	1

3.3.3 Involutions

Define further the group $C_2(H)=\{P\in C(H)\mid P^2=I\}$, consisting of the identity and of the involutions in $C(H)$. This can be interpreted in terms of **combinatorial designs**. Consider the incidence system $(\mathcal{V},\mathcal{B},\mathcal{I})$ defined by the following three rules:

- $\mathcal{V}$ is the set of rows of H,
- $\mathcal{B}$ is the set of columns of H,
- $i\,\mathcal{I}\,j$ iff $H_{ij}=-1$.

A **duality** π of this incidence system on its dual $(\mathcal{B},\mathcal{V},\mathcal{I})$ is then defined as a bijection π between $\mathcal{V}$ and $\mathcal{B}$ that preserves incidence: $\mathcal{B}$ and $\mathcal{V}$ are swapped by π and $i\mathcal{I}j$ iff $\pi(i)\mathcal{I}\pi(j)$ (Cf [22, (4.1.b) p. 34, Def. 4.9]). The set of all dualities form a group for map composition. Furthermore if a duality is an involution, it is called a **polarity**. In terms of the incidence matrix A of $\mathcal{I}$, a permutation matrix P is a polarity if $PA=A^tP^t$ and $P^t=P$, or, equivalently, if $PA=A^tP$ and $P^t=P$.

Theorem 3.17 *If H is symmetric, then the group $C_2(H)$ coincides with the group of polarities of the above incidence structure.*

Proof The incidence matrix A of $(\mathcal{V},\mathcal{B},\mathcal{I})$ satisfies by definition $H=J-2A$, where J denotes the v by v all-one matrix. If H is symmetric, then $H=H^t$, and, since $J=J^t$, we have $A=A^t$. Since $P\in P(v)$, we have $PJ=JP=J$. Thus $HP=PH$ iff $PA=AP$, or, equivalently, iff $PA=A^tP$. The result follows.

4 Search Methods

4.1 Exhaustion

This method is only applicable for small v's.

1) Construct H a Hadamard matrix of order v. Compute $\mathcal{H}=\frac{1}{\sqrt{v}}H$.

2) For all $X\in\{\pm1\}^v$ compute $Y=\mathcal{H}X$. If $Y=X$, then X is a self-dual bent sequence attached to H.

Complexity: Exponential in v since $|\{\pm1\}^v|=2^v$.

4.2 Linear Algebra

This method is more complex to program than the others but allow to reach higher v's.

1) Construct H a Hadamard matrix of order v. Compute $\mathcal{H}=\frac{1}{\sqrt{v}}H$.

2) Compute a basis of the eigenspace associated to the eigenvalue 1 of $\mathcal{H}$.

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 $Z \in \{\pm 1\}^k$ solve the system in C given by $Z = CB_k$.

5) Compute the remaining $v - k$ entries of CB.

6) If these entries are in $\{\pm 1\}$ declare CB a self-dual bent sequence attached to H.

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 r and r' of the submatrices of B with k rows and columns defined by the respective lists J and $J' = \mathit{Append}(J, \ell)$.

(iii) If $r < r'$ then update $J := J'$.

(iv) Repeat until $|J| = \mathrm{rank}(B)$.

Remark 4.1 The matrix in Step (1) can be constructed by using Magma database[21] or by the techniques in the Appendix.

Remark 4.2 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. This happens for the unique circulant core Hadamard matrix of order 36[23].

Complexity: Roughly of order $v^3 2^k$. In this count v^3 is the complexity of computing an echelonized basis of $H - \sqrt{v}I$. The complexity of the invertible minor finding algorithm is of the same order or less.

4.3 Gröbner Bases

The system $\mathcal{H}X = X$ with $X \in \{\pm 1\}^v$ can be thought of as the real quadratic system $\mathcal{H}X = X$, $\forall i \in [1, v]$, $X_i^2 = 1$. For background material on Gröbner bases we refer the reader to [24].

More concretely, we can consider the following steps.

(i) Construct the ring P of polynomial functions in v variables X_i, $i = 1, \cdots, v$.

(ii) Construct the linear constraints $\mathcal{H}X = X$.

(iii) Construct the quadratic constraints $\forall i \in [1, v]$, $X_i^2 = 1$.

(iv) Compute a Gröbner basis for the ideal I of P determined by constraints (ii) and (iii).

(v) Compute the solutions as the zeros determined by I.

With a tip from Delphine Boucher we produced the following program in Magma[21] in the case $v = 4$. This program is easy to adapt for higher v's. We give it here for exposition purpose only.

```
F:=RationalField();
//Polynomial ring defining the variables
var := 4;
P⟨w,x,y,z⟩ := PolynomialRing(F,var);
```

//The equations of the system one wants to solve over F

$$sys := [w+x+y+z-2*w, w-x+y-z-2*x, w+x-y-z-2*y, w-x-y+z-2*z,$$
$$w^2-1, x^2-1, y^2-1, z^2-1];$$

//The ideal of the relations

`I := ideal`$\langle P|sys\rangle$;

//Computation of a Gröbner basis (for the lexicographical order if no other order is specified)

```
Gröbner(I:Faugere:=true);
```

//The set of solutions, S

```
S:=Variety(I); S;
```

Complexity: In general the complexity of computing a Gröbner basis in v variables can be doubly exponential in v[24]. However, for the systems at hand the complexity is at most singly exponential (see [25, Th.10]). The authors are grateful to Elisa Gorla for pointing this out.

5 Numerics

The following Table 2 gives an upper bound on the dimension of the eigenspace attached to the eigenvalue 1 of $\mathcal{H}$. The row # gives the number of non-Sylvester Hadamard matrices of given order in the Magma database[21].

Table 2 Hadamard matrices with different orders in Magma database

v	4	16	36	64	100	144	196
#	0	4	219	394	1	1	1
dim $\leq$	–	7	4	3	2	1	2

Given how small these upper bounds are, the method of Subsection 4.2 is very successful. By using linear algebra method, we verify that there is no self-dual bent sequence in above (non-Sylvester) Hadamard matrices. In particular, the Magma database contains only one matrix for $v \in \{100, 144, 196\}$, respectively. We thus have to construct extra matrices as explained in the Appendix. In Table 3, each column corresponds to one type of matrix from the Appendix†

†For the sake of computational complexity, in Table 3, we focus on Hadamard matrices with dimensions of the eigenspace attached to the eigenvalue 1 of $\mathcal{H}$ smaller than 30.

Table 3 Number of self-dual bent sequences in various Hadamard matrices with dimensions of the eigenspace attached to the eigenvalue 1 of $\mathcal{H}$ smaller than 30

v	16	36		64		100			144	196
Types	Sylvester	Bush [26], [27]	Paley	Regular [28]	Regular by Switching	Regular [11]	Regular [29]	Regular Menon [11]	Bush [29], [30]	Regular [31]
# of H	1	29	1	16	1	115	1	4	4	4
# of X	140	64	204	2, 4, 6, 12, 620	2	1024, 1056, 1152, 1216, 2336, 3616, ... 5312, 6464	12	924	20, 924, 1052	6864, 12870

All detailed self-dual bent sequences for the above Hadamard matrices in Table 3 are publicly available on `Github`:

`https://github.com/Qomo-CHENG/Hadamard_bent.`

6 Application

A recent and original application of Hadamard bent sequences, first introduced in [3], lies in Physical Unclonable Functions (PUFs). PUFs can be viewed as the fingerprint of a circuit, which generate unique outputs because of uncontrollable technological dispersions during the manufacturing process of silicon chips. They are employed for many security purposes like authentications[32], cryptographic key generations[33], etc. A PUF usually generates a series of random bits (by feeding customized inputs) that uniquely depends on the corresponding circuit. Therefore, one of the metrics of the performance of a PUF is the entropy of the generated random bits[34]. For instance, we expect to generate cryptographic keys as randomly as possible in practice, leading to as high entropy as possible.

It is demonstrated in [34] that v inputs generated from a Hadamard matrix (e.g, v row vectors) can achieve the maximal entropy of v bits in PUFs. Later on, as demonstrated in [3], bent sequences maximize the entropy of outputs when adding one more sequence (then $v+1$ sequences in total) to the Hadamard code $(v, 2v)$. When they exist, bent sequences reach the covering radius of the Hadamard code constructed from a Hadamard matrix as in §2 (Cf. Lemma 2.1). The main conjecture of [3], checked numerically for small v (e.g., $v \leq 16$), is that maximizing the entropy of outputs is equivalent to adding a new codeword at distance the covering radius of the Hadamard code. In this respect, we construct various Hadamard matrices for different v up to 196 and verify the existence of self-dual bent sequences in this paper.

7 Conclusion

We have considered the self-dual bent sequences attached to Hadamard matrices from the viewpoints of generation and symmetry. Our generation method based on linear algebra works especially well when the eigenvalue 1 of the normalized Hadamard matrix has low geometric multiplicity. For some matrices of order 100 this method performs well, while the Gröbner basis method cannot finish. The lack of Hadamard matrices of order > 36 in Magma database[21] has led us to use the switching method of [35] to generate more matrices. In general, it would be a worthy research project to enrich the known databases, even in the cases where complete enumeration of equivalence classes is unfeasible. In the same vein, refining the classification of Hadamard matrices for $v \leq 28$ from equivalence to strong equivalence would be of interest.

We note that the concept of self-dual bent sequences being not invariant by Hadamard equivalence, classification of these become infeasible, even for matrices of small order. In general, classification at order v would require to consider $(v!2^v)^2$ matrices for each orbit representative. This makes already 147456 for $v = 4$.

References

[1] Mesnager S, *Bent Functions, Fundamentals and Results*, Springer, Cham, 2016.

[2] Tokareva N, *Bent Functions. Results and Applications to Cryptography*, Elsevier/Academic Press, Amsterdam, 2015.

[3] Solé P, Cheng W, Guilley S, et al., Bent sequences over Hadamard codes for physically unclonable functions, *IEEE International Symposium on Information Theory, Melbourne, Australia*, 2021, 801–806.

[4] MacWilliams F J and Sloane N J A, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, Netherlands, 1977.

[5] Carlet C, Danielsen L E, Parker M G, et al., Self-dual bent functions, *Int. J. Inf. Coding Theory*, 2010, **1**(4): 384–399.

[6] Kharaghani H, On the twin designs with the Ionin-type parameters, *Electr. J. Comb.*, 2000, **7**(#R1(1–11): 2000.

[7] Horadam K J, *Hadamard Matrices and Their Applications*, Princeton University Press, Princeton, NJ, 2007.

[8] Wallis W D, Street A P, and Wallis J S, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Ser. Lect. Notes Math. Springer-Verlag, Berlin, 1972, **292**.

[9] Bush K A, Unbalanced Hadamard matrices and finite projective planes of even order, *J. Comb. Theory, Ser. A*, 1971, **11**(1): 38–44.

[10] Hall M Jr, Note on the mathieu group M_{12}, *Arch. Math.*, 1962, **13**: 334–340.

[11] Crnković D, Egan R, and Švob A, Orbit matrices of Hadamard matrices and related codes, *Discrete Math.*, 2018, **341**(5): 1199–1209.

[12] de Launey W and Flannery D, *Algebraic Design Theory*, Ser. Math. Surv. Monogr., American Mathematical Society (AMS), Providence, RI, 2011.

[13] Kantor W M, Automorphism groups of Hadamard matrices, *J. Comb. Theory*, 1969, **6**(3): 279–281.

[14] de Launey W and Stafford R M, On the automorphisms of Paley's type II Hadamard matrix, *Discrete Math.*, 2008, **308**(13): 2910–2924.

[15] Janusz G J, Parametrization of self-dual codes by orthogonal matrices, *Finite Fields Appl.*, 2007, **13**(3): 450–491.

[16] Kutsenko A, The group of automorphisms of the set of self-dual bent functions, *Cryptogr. Commun.*, 2020, (5): 881–898.

[17] Feulner T, Sok L, Solé P, et al., Towards the classification of self-dual bent functions in eight variables, *Des. Codes Cryptography*, 2013, **68**(1–3): 395–406.

[18] Crnković D, A series of regular Hadamard matrices, *Des. Codes Cryptography*, 2006, **39**(2): 247–251.

[19] Leung K H, Ma S L, and Schmidt B, New Hadamard matrices of order $4p^2$ obtained from Jacobi sums of order 16, *J. Comb. Theory, Ser. A*, 2006, **113**(5): 822–838.

[20] Biggs N, *Algebraic Graph Theory*, Ser. Camb. Tracts Math., Cambridge University Press, Cambridge, 1974, Vol. 67.

[21] Bosma W, Cannon J J, Fieker C, et al., *Handbook of Magma functions, Edition* 2.16, 2010.

[22] Beth T, Jungnickel D, and Lenz H, *Design Theory. Vol. I.*, Ser. Encycl. Math. Appl., Cambridge University Press, Cambridge, 1999.

[23] Kotsireas I S, Koukouvinos C, and Seberry J, Hadamard ideals and Hadamard matrices with circulant core, *J. Comb. Math. Comb. Comput.*, 2006, **57**: 47–63.

[24] Adams W W and Loustaunau P, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, 1994.

[25] Caminata A and Gorla E, Solving multivariate polynomial systems and an invariant from commutative algebra, *International Workshop on the Arithmetic of Finite Fields*, Springer, Cham, 2020, **12542**: 3–36.

[26] 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*, 2001, **95**(2): 360–364.

[27] Janko Z and Kharaghani H, A block negacyclic Bush-type Hadamard matrix and two strongly regular graphs, *J. Comb. Theory, Ser. A*, 2002, **98**(1): 118–126.

[28] Crnković D and Pavčević M -O, Some new symmetric designs with parameters (64, 28, 12), *Discrete Math.*, 2001, **237**(1–3): 109–118.

[29] Pavčević M -O, Symmetric designs of Menon series admitting an action of Frobenius groups, *Glas. Mat., III. Ser.*, 1996, **31**(2): 209–223.

[30] Crnković D, A construction of some symmetric $(144, 66, 30)$ designs, *J. Appl. Algebra Discrete Struct*, 2007, **5**(1): 33–39.

[31] Crnković D, A construction of some symmetric designs with parameters $(196, 91, 42)$, *Int. Math. Forum*, 2007, **2**(61–64): 3021–3026.

[32] Delvaux J, Peeters R, and Gu D, Verbauwhede I, A survey on lightweight entity authentication with strong PUFs, *ACM Comput. Surv.*, 2015, **48**(2): 1–42.

[33] Shamsoshoara A, Korenda A, Afghah F, et al., A survey on physical unclonable function (PUF)-based security solutions for Internet of Things, *Computer Networks*, 2020, **183**: 107593.

[34] Rioul O, Solé P, Guilley S, et al., On the entropy of physically unclonable functions, *IEEE International Symposium on Information Theory*, Barcelona, Spain, 2016, 2928–2932.

[35] Crnković D and Švob A, Switching for 2-designs, *Des. Codes Cryptography*, 2022, **90**: 1585–1593.
[36] Janko Z, Kharaghani H, and Tonchev V D, Bush-type Hadamard matrices and symmetric designs, *J. Comb. Des.*, 2001, **9**(1): 72–78.
[37] Crnković D, Some new Menon designs with parameters $(196, 91, 42)$, *Math. Commun.*, 2005, **10**(2): 169–175.

A Appendix on Hadamard Matrices

In this section we indicate that how to construct Hadamard matrices of orders not sufficiently covered in Magma Hadamard database[21].

A.1 Order 16

There are five Hadamard matrices in Magma database and the first one is of the Sylvester type.

A.2 Order 36

Bush-type Hadamard matrices can be found in [26, 27]. More can be generated by switching[35].

A.3 Order 64

16 regular Hadamard matrices were obtained from the symmetric $(64, 28, 12)$ designs constructed in [28]. One regular Hadamard matrix was obtained by switching[35].

A.4 Order 100

Two Hadamard matrices can be obtained from symmetric designs $(100, 45, 20)$ constructed in [11]. One Hadamard matrix can be obtained from the symmetric design $(100, 45, 20)$ obtained in the reference [29].

The switching method described in [35] applied to the Janko-Kharaghani-Tonchev symmetric $(100, 45, 20)$ design of [36] corresponding to a Bush-type Hadamard matrix of order 100 gives 2^{10} designs (including the original one), 208 of them are pairwise non-isomorphic. These 208 symmetric $(100, 45, 20)$ designs give rise to 120 pairwise non-equivalent regular Hadamard matrices. In particular, 115 of them have dimensions of the eigenspace attached to the eigenvalue 1 of $\mathcal{H}$ smaller than 27.

A.5 Order 144

Four Bush-type Hadamard matrices can be constructed from the symmetric $(144, 66, 30)$ designs in [29], [30]. Note that one of them has dimensions of the eigenspace attached to the eigenvalue 1 of $\mathcal{H}$ equal to 28.

A.6 Order 196

Four regular Hadamard matrices were obtained from the symmetric $(196, 91, 42)$ designs built in [31], and additional two regular Hadamard matrices were obtained from the symmetric $(196, 91, 42)$ designs constructed in [37]. However, the latter two have dimensions of eigensapce attached to the eigenvalue 1 of $\mathcal{H}$ equal to 33, so we omit them in Table 3.