Self-dual Hadamard bent sequences
arxiv.org/abs/2203.16439,&
hal.science/hal-03870634

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

CNRS/I2M, Marseilles, France

Classical Bent Sequences

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

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

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. Then F is said to be a bent sequence.

Sylvester matrix

Thus in term of vectors the Walsh-Hadamard transform is

$$\widehat{f} = SF,$$

where $S_{xy} = (-1)^{<x,y>}$ is the Sylvester matrix of size 2^h by 2^h.

Here $x, y \in \mathbb{F}_2^h$ and $< x, y >= \sum_{i=1}^{h} x_i y_i$.

A recursive construction is possible.

Applications of Bent Sequences

- covering radius of first order Reed-Muller code
- building blocks of stream ciphers
- strongly regular graphs
- difference sets in elementary abelian groups

Self-dual Classical Bent Sequences

The dual of a bent function f is defined by its sequence $\widehat{f}/2^{h/2}$.
A bent function is said to be **self-dual** if it equals its dual.
Their sequences are eigenvectors for the Sylvester matrix attached to the eigenvalue $2^{h/2}$.

$$SF = 2^{h/2}F.$$

Self-dual bent functions for $h = 2, 4$ were classified under the action of the extended orthogonal group in
C. Carlet, L. E. Danielsen, M. G. Parker, and P. Solé, “Self-dual bent functions,” Int. J. Inf. Coding Theory , (2010), 384–399.

Hadamard Bent Sequences: Motivation

A new notion of bent sequence was introduced in
P. Solé, W. Cheng, S. Guilley, and O. Rioul, "Bent sequences over Hadamard codes for physically unclonable functions," in *IEEE International Symposium on Information Theory, Melbourne, Australia, July 12–20, 2021*.

PUF 's are fingerprint of a circuit reflecting the randomness of mass production.

The v rows of a Hadamard matrix maximize the entropy when using v bits to define the PUF.

What is the best entropy code of size v+1 and length v ?

Conjecture: add a vector at the covering radius of the Hadamard code.

Hadamard Bent Sequences: Definition

A matrix H with entries $\in \{\pm 1\}$ is a Hadamard matrix of order v if

$$HH^t = vI_v.$$

If there is 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 $X, Y \in \{\pm 1\}^v$ then X is a bent sequence attached to H.

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 $d(.,.)$ denote the Hamming distance on A. The **covering radius** of a code C of length v over A is defined by the formula

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

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

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

self-dual Hadamard Bent Sequences

The **dual** sequence of X is defined by $Y = \mathcal{H}X$.
Because $HH^t = vI_v$, we see that the vector Y is itself a bent sequence attached to H^t.
If $Y = X$, then X is a **self-dual** bent sequence attached to H.
For a given H, there are many bent sequences.
Self-dual bent sequences are fewer and easy to construct.

Hadamard Matrices: History

My grandgrandgrandadvisor invented Hadamard matrices in 1893 as a solution of an extremal problem for determinants.

(Hadamard ⟶ Fréchet ⟶ Fortet ⟶Cohen ⟶ S.)

Sylvester construction

The unique Hadamard matrix of order 2 is $H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

The Kronecker product preserves the Hadamard property. By induction the matrix $H_{m+1} = H_1 \otimes H_m$ is a Hadamard matrix. Note that $H_h = S$, as defined before.

This construction is due to Sylvester

J. J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers, Philosophical Magazine 34 (1867), 461–475.

Hadamard Matrices: normalization

A Hadamard matrix is normalized if its top row and its leftmost column consists only of ones.
Every Hadamard matrix can be cast in normalized form by a succession of the three following operations

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

Hadamard Matrices: regular

A Hadamard matrix of order v is regular if the sum of all its rows and all its columns is a constant σ.

In that case, it is known that $v = 4u^2$ with u a positive integer and that $\sigma = 2u$ or $-2u$

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

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.

Many constructions are known for $u = p$, a prime satisfying some extra arithmetic conditions.

Hadamard Matrices: Bush-type I

A regular 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.

Motivation: finite projective planes.
K. A. Bush, *Unbalanced Hadamard matrices and finite projective planes of even order*,J. Combin. Theory Ser. A11, (1971) 38–44

Hadamard Matrices: Bush-type II

Each Bush-type Hadamard matrix implies the existence of many self-dual bent sequences.

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.

The idea is to have a sequence equal to a constant on the blocks.

Existence conjecture

Hadhi Kharagani ’s conjecture:
Bush-type Hadamard matrices exist for all even perfect square orders

$\Longrightarrow$ We conjecture: if v is an even perfect square, then there exists a self-dual Hadamard bent sequence for some Hadamard matrix of order v

Search Methods:Exhaustion

This method is only applicable for small v's.

(1) Construct H a Hadamard matrix of order v.

(2) For all $X \in \{\pm 1\}^v$ compute $Y = \mathcal{H}X$. If $Y = X$, then X is self-dual bent sequence attached to H.

Complexity: Exponential in v since $|\{\pm 1\}^v| = 2^v$.

Search Methods:Groebner bases

The system $\mathcal{H}X = X$ with $X \in \{\pm 1\}^v$ can be thought of as the real quadratic system $\mathcal{H}X = X$, $\forall i \in [1, v]$, $X_i^2 = 1$.

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

(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 Groebner basis for the ideal I of P determined by constraints (ii) and (iii).

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

Complexity: As is well-known, the complexity of computing Groebner bases can be doubly exponential in the number of variables, that is v here. In our situation, it can be shown to be at most doubly exponential (Elisa Gorla).

Search Methods:Linear Algebra

(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.

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.

Hadamard Matrices: standard automorphism group

The class of Hadamard matrix 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 $(S_v \wr S_2)^2$, where S_m denotes the symmetric group on m letters.
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 $PHQ = H$.

Hadamard Matrices: strong automorphism group I

The **strong automorphism group** $\mathrm{SAut}(H)$ of H defined as the set of $P \in M(v)$ such that $PH = HP$.

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

Given H the group $\mathrm{SAut}(H)$ can be determined by an efficient graph theoretic algorithm.

Hadamard Matrices: strong automorphism group II

A partial characterization in the case of $\mathrm{SAut}(S)$ is as follows.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 $\mathbb{F}_2$,
- $b, d \in \mathbb{F}_2^m$,
- $c \in \{1, -1\}$.

The strong automorphism group of Sylvester matrices

An extended affine transform $T_{A,b,d,c}$ is in $\mathrm{SAut}(S_v)$ iff $A^t = A^{-1}$, $b = d$ and $w_H(b)$ is even.
We call this subgroup of $\mathrm{SAut}(S_v)$ the extended orthogonal group
In particular, the number of such transforms is $|\mathcal{O}_m|2^m$ where $\mathcal{O}_m = \{A \in \mathrm{GL}(m, \mathbb{F}_2) \mid AA^t = I\}$ is the orthogonal group .

- $|\mathcal{O}_m| = 2^{k^2} \prod_{i=1}^{k-1} (2^{2i} - 1)$ 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
$1, 2, 8, 48, 768, 23040, 1474560, 185794560.$

Conclusion for real Hadamard matrices

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 Groebner basis method cannot finish.

Generalization

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

(1) classical bent sequences and Sylvester type Hadamard matrices, C. Carlet, L. E. Danielsen, M. G. Parker, and P. Solé. Self-dual bent functions. *Int. J. Inf. Coding Theory*, 1(4):384–399, 2010.

(2) bent sequences attached to classical Hadamard matrices, as just discussed

(3) complex bent sequences attached to Sylvester type Hadamard matrices L. Sok, M. J. Shi, and P. Solé. Classification and construction of quaternary self-dual bent functions. *Cryptogr. Commun.*, 10(2):277–289, 2018.

(4) complex bent sequences attached to complex Hadamard matrices in the sense of Turyn: $\{\pm 1\} \to \{\pm 1, \pm i\}$

Complex Hadamard matrices

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, and Kharaghani, and other authors.

J. Wallis. Complex Hadamard Matrices. *Linear Multilinear Algebra*, 1(3):257–272, 1973.

H. Kharaghani and J. Seberry. Regular complex Hadamard matrices. *Congr.Numer.*, 75: 187–201, 1990.

Complex Hadamard matrices are conjectured to exist for all even v.

First Definition of bent sequences

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 $Y = X$.

Necessary condition

The squared norm of an eigenvalue of a complex Hadamard matrix of order v is v.

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

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

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

Second Definition of bent sequences

Let $v = a^2 + b^2$, with $a, b \geq 0$.
A self-dual bent sequence attached to a complex Hadamard matrix C of order v 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.

Kronecker products

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.

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 $(1+i)\sigma$.

Conference matrices and Paley II

The Jacobsthal matrix is the matrix C_q of order q defined by $C_q(x,y) = \chi(y-x)$, for $x, y \in \mathbb{F}_q$. Here χ denotes the quadratic character. Its extension of order $q+1$ is

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

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

If q is a prime power and $q \equiv 1 \pmod 4$, and S_q denotes the extended Jacobsthal matrix, then $C = iI_q + S_q$ is a complex Hadamard matrix of order $q+1$.

The spectrum of C_q is very restricted :=((
The minimal polynomial of C is $x^2 - 2ix - (q+1)$.

Complex Bush-type I

Let there exist 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.

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.

Complex Bush-type II

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

(1) $C_i^t = C_i$, for $i = 1, 2, \ldots, 2v$.

(2) $C_1 = J_{2v},\ C_i J_{2v} = J_{2v} C_i = 0$, for $i = 2, 3, \ldots, 2v$.

(3) $C_i C_j^* = 0$, for $i \neq j, 1 \leq i, j \leq 2v$.

(4) $C_1 C_1^* + C_2 C_2^* + \cdots + C_{2v} C_{2v}^* = 4v^2 I_{2v}$.

Let $C = circ(C_1, C_2, \ldots, C_{2v})$, the block circulant matrix with the first row $C_1, C_2, \ldots, C_{2v}$. Then C is a Bush-type complex Hadamard matrix of order $4v^2$. This matrix is regular of row sum $2v$.

Quaternionic structure I

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 i, j, k are quaternionic units given by

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

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

Quaternionic structure II

Williamson type matrices yield complex Hadamard matrices as follows.

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 $V = X - Y$.

Coding connection I

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 $i^{\mathcal{Z}} = \mathcal{C}$. 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

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

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

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

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

Coding connection II

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 $\langle , \rangle$ 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

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

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

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

Property: the total deviation of an Hadamard code of length n is $\sqrt{n}$.

Covering radius of Hadamard codes

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

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

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 total deviation yields the following bound.

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

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

Open problems

- enrich the Magma database of Hadamard matrices
- classify Hadamard matrices under strong equivalence for small orders
- classify self-dual bent sequences under the action of the strong automorphism group
- Butson Hadamard matrices and their codes
- unit Hadamard matrices (in preparation)

The last slide

Thanks for your attention!

Hvala na pažnji!