Self-dual Hadamard bent sequences

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

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*.
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 $X, Y \in \{\pm 1\}^v$.
A matrix H with entries $\in \{\pm 1\}$ is a Hadamard matrix of order v if

$$HH^t = vI_v.$$

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 $\longrightarrow$ Fréchet $\longrightarrow$ Fortet $\longrightarrow$Cohen $\longrightarrow$ 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

Announcement

CONFERENCE ALCOCRYPT

ALgebraic and combinatorial methods

for

COding and CRYPTography

CIRM, Luminy, France

20 - 24 February 2023

Special issue of the journal

Advances in Mathematics of Communication

Deadline: September 1st, 2022

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, $i = 1, \ldots v$.

(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.

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 $PH = HP$.

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

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.

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

The last slide

Thanks for your attention!

Viel dank!!!!

Grazie Mille!!!!