Hadamard matrices and spherical designs

Patrick Solé
joint work with D. Lu, M.Shi, A. Armario, R. Egan, F. Özbudak

CNRS/I2M, Marseilles

Seville, Spain

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.
Given a bent sequence X for some Hadamard matrix H this matrix can be tweaked to make X self-dual bent.

Hadamard Matrices: History

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

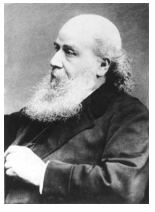
(Hadamard $\longrightarrow$ Fréchet $\longrightarrow$ Fortet $\longrightarrow$Cohen $\longrightarrow$ S.)

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 $H_{m+1} = \begin{pmatrix} H_m & H_m \\ H_m & -H_m \end{pmatrix}$ is a Hadamard matrix.

Note that $H_h = S$, as defined before.

This construction is due to Sylvester  a british algebraist

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

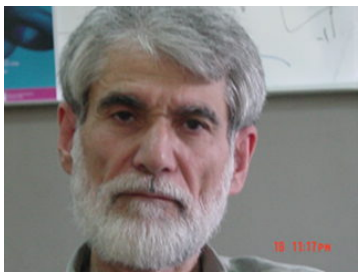
Hadamard Matrices: Bush-type II

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, $i = 1, \ldots v$.

(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 $PH = HP$.

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 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 $\mathcal{O}_m = \{A \in GL(m, \mathbb{F}_2) \mid AA^t = I\}$ 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
$1, 2, 8, 48, 768, 23040, 1474560, 185794560$.

Butson Hadamard matrices: definition

A complex **Hadamard** matrix of order n is an $n \times n$ matrix H with entries in the complex unit satisfying the equation

$$HH^* = nI,$$

where the $*$ denotes the transpose conjugate. If all of its elements are in

$$\Omega_q = \{z \in \mathbb{C} \mid z^q = 1\},$$

for some integer q, then H is said to be **Butson** type, and we write $H \in BH(n, q)$.

A matrix $H \in BH(n, q)$ is in **dephased** form when both first row and first columns only contain ones.(Cf. normalized for $BH(n, 2)$)

A. T. Butson, Generalized Hadamard matrices, Proc. Am. Math. Soc. 13, 894-898 (1962).

Butson Hadamard matrices: bent sequences

Given $H \in BH(n,q)$ the sequence $X \in \Omega_q^n$ is a **bent sequence** if there is $Y \in \Omega_q^n$ such that $HX = \lambda Y$ for some $\lambda \in \mathbb{Z}[\zeta_q]$.

The notion of self-dual bent sequence can be extended to that setting: $Y = X$

Further extension:

For any k coprime with q we define the multiplier $\mu_k : \Omega_q \longrightarrow \Omega_q$ by the rule $\mu_k(z) = z^k$.

A self-dual bent sequence attached to $H \in BH(n,q)$ is $X \in \Omega_q^n$ such that $HX = \lambda\mu_k(X)$.

When $k = 1$, this is the definition of self-dual bent sequence in Shi et al. DCC 2023.

When $k = q - 1$, this is the definition of self-dual bent sequence in Armario et al. Riccota conference 2023.

Existence conditions for bent sequences

If H in $BH(n,q)$, such that $HX = \lambda X$ with $\lambda \in \mathbb{Z}[\zeta_q]$, with $X \in \Omega_q^n$,

$$\Rightarrow$$

there are q integers $0 \leq y_r \leq n$ such that $n = \sum_{r=0}^{q-1} y_r$ (a "composition" of n) and such that

$$n = \left(\sum_{r=0}^{q-1} y_r c_r\right)^2 + \left(\sum_{r=0}^{q-1} y_r s_r\right)^2$$

where $\zeta_q^r = c_r + i s_r$ and $i = \zeta_4$.

Example: If $n = 6, q = 3$ there are 28 compositions. None of them satisfy this equation. $\Rightarrow$ no matrix in $BH(6,3)$ has such a λ.

General construction I: Kronecker product

It is well-known that the Kronecker product preserves the Hadamard property.

This carries over to Hadamard bent sequences.

Let $H \in BH(n, q)$ (resp. $K \in BH(m, q)$) affording a self dual bent sequence X (resp. Y) for the multiplier μ_k.
Then $X \otimes Y$ is a self-dual bent sequence with multiplier μ_k, for $H \otimes K \in BH(mn, q)$.

General construction II: Fourier transforms

Define a "Sylvester-like" Butson Hadamard matrix H by the rule

$$H_{xy} = \zeta_q^{x \cdot y}.$$

Application of orthogonality of group characters for $(\mathbb{Z}_q, +)$.
Write $X = (\zeta_q^{f(x)})_{x \in \mathbb{Z}_q^n}$. X is self-dual bent for H iff f is a generalized bent function à la Kumar-Scholtz-Welch.
Consider the generalized Maiorana-McFarland f of the kind $f(x, y) = x \cdot \phi(y)$, where ϕ is a permutation of $\mathbb{Z}_q^{n/2}$.
We give some conditions on k for f to be self-dual bent wrt H^*.
Generalizations to more complicated matrices with

$$H_{(x_1,x_2),(y_1,y_2)} = \zeta_q^{(x_1-y_1)\cdot(x_2-y_2)}$$

Butson Hadamard matrices: codes over rings

A Butson matrix $H \in BH(n, q)$ is conveniently represented in logarithmic form.
If $H = \left[\zeta_q^{\varphi_{i,j}}\right]_{i,j=1}^{n}$ define $L(H) = [\varphi_{i,j} \bmod q]_{i,j=1}^{n}$.
Denote by F_H the $\mathbb{Z}_q$-code of length n consisting of the rows of $L(H)$, and by

$$C_H = \cup_{\alpha \in \mathbb{Z}_q}(F_H + \alpha \mathbf{1})$$

where $\mathbf{1}$ denotes the all-one vector.
The code $C_H \subseteq \mathbb{Z}_q^n$ is called a **Butson Hadamard** code, and was introduced in

J. A. Armario, I. Bailera, R. Egan, Butson full propelinear codes, Designs, Codes and Cryptography, 2023, **91***(2): 333–351.*

Butson Hadamard codes: chinese Euclidean distance

The **Chinese Euclidean weight** $w_{CE}(x)$ of a vector $x \in \mathbb{Z}_q^n$ is

$$\sum_{i=1}^{n} \left[2 - 2\cos\left(\frac{2\pi x_i}{q}\right) \right],$$

and the **Chinese Euclidean distance** between the codewords u and $v \in \mathbb{Z}_q^n$ is defined as

$$d_{CE}(u, v) = w_{CE}(u - v).$$

This distance coincide with the Lee distance for $q = 4$, but not in general.

P. Chella Pandian, On the covering radius of codes over $\mathbb{Z}_6$, International Journal on Information Theory, 2016, **5***(2): 01–09.*

Butson Hadamard codes: covering radius

If there is a bent sequence X for $H \in BH(n, q)$, then the covering radius for the chinese Euclidean distance of its attached $\mathbb{Z}_q$-code C_H is bounded below as

$$r_{CE}(C_H) \geq 2n - 2\sqrt{n}.$$

This bound is tight for many values of n when $q = 4, 6, 8$.

Butson Hadamard codes: Euclidean distance distribution

The Chinese Euclidean distances of C_H are

$$\left\{ d_E(x,y) \mid x \neq y, x, y \in w^{C_H} \right\} =$$

$$\{2n\} \cup \left\{ 2n(1 - \cos \frac{2\pi t}{q}) \mid t = 1, 2, \ldots, \left\lfloor \frac{q}{2} \right\rfloor \right\}.$$

The proof follows simply by the Hadamard property and properties of roots of unity

Spherical codes: general

The **unit sphere** Υ_d in Euclidean d-space $\mathbb{R}^d$ is the set of all unit norm vectors:

$$\Upsilon_d \triangleq \left\{ x = (x_1, x_2, \ldots, x_d) \in \mathbb{R}^d : \|x\| = 1 \right\}$$

A **spherical code** in dimension d is a finite set $X \subseteq \Upsilon_d$. Its minimum distance for the squared Euclidean distance is denoted by ρ. Its parameters are denoted compactly by $(d, \rho, |X|)$. The function $A_d(\rho)$ can then be defined as

$$A_d(\rho) = \max\{|X| \mid X \text{ spherical code of parameters } (d, \rho, |X|)\}.$$

T. Ericson, V. Zinoviev, Codes on Euclidean spheres, North Holland, 2001.

Spherical codes: getting real

The map $\psi : \mathbb{C} \longrightarrow \mathbb{R}^2, x + iy \longmapsto (x, y)$ is an isometry from $(\mathbb{C}^n, d_E)$ to $\left(\mathbb{R}^{2n}, \delta\right)$, where

$$\delta(U, V) = \|U - V\|^2,$$

for all $U, V \in \mathbb{R}^{2n}$. Note that

$$(\psi(a), \psi(b)) = \Re\big(\langle a, b\rangle\big),$$

where a and $b \in \mathbb{C}^n$, and $(,)$ denotes the standard inner product in $\mathbb{R}^{2n}$.

For normalization purposes, we will let $\phi(z) = \frac{\psi(z)}{\sqrt{n}}$, for all $z \in \mathbb{C}^n$.

Spherical codes: Hadamard matrices I

The spherical code $\phi(\zeta_q^{C_H}) \subseteq \Upsilon_{2n} \subseteq \mathbb{R}^{2n}$ has a size of nq and a distance of

$$\rho = \frac{d_{CE}}{n} = 2(1 - \cos\frac{2\pi}{q}).$$

This is an easy consequence of the Hadamard property.

Spherical codes: Hadamard matrices II

If $H \in BH(n, 4)$, then the spherical code $\phi(\zeta_q^{C_H})$ is optimal in dimension $2n$.

This is a consequence of Levenshtein bound on spherical codes: Let X be a spherical code with parameters $(d, \rho, |X|)$ and let $s = 1 - \frac{\rho}{2}$. Then the size $|X|$ is bounded above for $s \in [0, \frac{1}{(\sqrt{d+3}+1)})$, as

$$|X| \leq L_3(s) = \frac{d(2 + (d+1)s)(1-s)}{1 - ds^2},$$

V. I. Levenshtein, Designs as maximum codes in polynomial metric spaces, Acta Appl. Math. 25, (1982): 1–82

Spherical designs: general

A spherical design of strength t, is a finite set X of N points on the d-dimensional unit d-sphere S_d such that for every polynomial of degree at most t we have

$$\frac{1}{N}\sum_{x\in X} f(x) = \int_{s\in S_d} f(s).$$

Introduced in *Delsarte, P.; Goethals, J. M.; Seidel, J. J. (1977), "Spherical codes and designs", Geometriae Dedicata, 6 (3): 363–388.* A picture of Jaap Seidel, the father of the "Benelux school of combinatorics."

Spherical designs: motivation

- Approximation of functions (cubature formulas)
- Statistics of experimental design
- Algebraic Combinatorics (eigenspaces of association schemes)
- Euclidean lattices (modular forms analogue of Assmus-Mattson theorem)

Spherical designs: covering radius

Let Υ_d denote the unit sphere of $\mathbb{R}^d$. The covering radius of a spherical code $X \in \Upsilon_d$ is

$$\rho = \max_{x \in \Omega_d} \min_{y \in X} d_E(x, y).$$

Upper bounds of increasing precision when the strength grows were derived using linear programming and orthogonal polynomials in

G. Fazekas, V. I. Levenshtein, On upper bounds for code distance and covering radius of designs in polynomial metric spaces, Journal of Combinatorial Theory, Series A, 1995, **70***(2): 267-288.*

Spherical designs: harmonic characterization

Let $P(\mathbb{R}^n)$=real polynomials in n variables.

$$Harm(\mathbb{R}^n) := \{f \in P(\mathbb{R}^n) \mid \Delta f = 0\},$$

where Δ is the Laplacian operator.
$Hom_l(\mathbb{R}^n) :=$ the subspace of spanned by all the homogeneous polynomials of degree l.
$Harm_l(\mathbb{R}^n) := Harm(\mathbb{R}^n) \cap Hom_l(\mathbb{R}^n)$.
The spherical code X is a t-designs iff $\forall \phi \in Harm_l$ for $l = 1, 2, \cdots, t$ we have

$$\sum_{x \in X} \phi(x) = 0$$

Eiichi Bannai, Etsuko Bannai / European Journal of Combinatorics 30 (2009) 1392–1425

Spherical designs: small strength

A spherical code X is a **1-design** if its center of mass is the origin or, more concretely, for all coordinate indices i satisfy $\sum_{x \in X} x_i = 0$. It is **antipodal** if $X = -X$.

A spherical code X is a **2-design** if it is a **1-design**, and if, furthermore, for all pairs $i \neq j$ of coordinate indices the following two relations hold.

$$\sum_{x \in X} (x_i^2 - x_j^2) = 0, \ \sum_{x \in X} x_i x_j = 0.$$

Spherical designs: Butson matrices

Using the Hadamard property of Butson matrices we prove the following two statements.

If H is dephased, then $\phi(\zeta_q^{C_H})$ is a **1-design** and its covering radius is at most $\sqrt{2}$.

If $H \in BH(n, q)$ is dephased, then $\phi(\zeta_q^{C_H})$ is a **2-design** and its covering radius is at most $\sqrt{2(1 - \frac{1}{2n})}$.
This implies that the chinese euclidean distance covering radius of C_H is

$$r_{CE}(C_H) \leq 2n - \sqrt{2n}$$

Conclusion and Open Problems

- Which bound is closer to the true value for $n \to \infty$?

$$2n - 2\sqrt{n} \leq r_{CE}(C_H) \leq 2n - \sqrt{2n}$$

- for $q = 4, 6, 8$ the lower bound is met for many matrices
- How to improve the upper bound?

Work in progress: weighing matrices:

- weighing matrices:

$$WW^* = kI_v$$

  with $k \leq v$.
- trouble with zero entries of W (phase $= -\infty$?)
- no connection with codes over a finite alphabet. :=((
- need to have nonzero bent sequences
- geometric algorithm to determine the covering radius (Delaunay diagram on the sphere, joint work with Mathieu Dutour)
- again the spherical design upper bound is not very tight

The last slide

Thanks for your attention!!!

Gracias por su atención !!!