Self-dual Butson bent sequences

J.A. Armario*, R. Egan†, P. Ó Catháin‡

*Depart. Matemática Aplicada I, Universidad de Sevilla, Spain
†School of Mathematical Sciences, Dublin City University, Ireland
‡Fiontar & Scoil na Gaeilge, Dublin City University, Ireland

3 –7 July, 2023

RICCOTA 2023, Rijeka, Croatia

*Spanish Strategic R+D Project **TED2021-130566B-I00**

Outline

Index

Definitions

A Boolean function

$$f : \mathbb{Z}_2^m \to \mathbb{Z}_2$$

is called a bent function if

$$\Big| \sum_{x \in \mathbb{Z}_2^m} (-1)^{f(x)} (-1)^{vx^\top} \Big|^2 = 2^m \text{ for all } v \in \mathbb{Z}_2^m,$$

consequently, m should be even.

Example of bent function

$$
\begin{array}{rccc}
f: & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2 \\
 & (x_1, x_2) & \mapsto & x_1 \cdot x_2
\end{array}
$$

v	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$\sum_{x\in\mathbb{Z}_q^m} (-1)^{f(x)}(-1)^{vx^\top}$	2	2	2	-2

Bent functions are of interest in cryptography, coding theory,...

Example of bent function (nonlinearity of Boolean functions)

$$\begin{array}{rccc} f: & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2 \\ & (x_1, x_2) & \mapsto & x_1 \cdot x_2 \end{array}$$

(x_1, x_2)	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$f(x_1, x_2)$	0	0	0	1
x_2	0	1	0	1
$x_1 + x_2$	0	1	0	0

The Hamming distance of f to the 8 affine Boolean functions is either 1, 2 or 3. Therefore the nonlinearity of f is 1.

Example of bent function (Cryptography)

Boolean functions with large nonlinearity are difficult to approximate by linear functions and so provide resistance against linear cryptanalysis.

Result

The largest nonlinearity of a Boolean function on $\mathbb{Z}_2^n$ is $2^{n-1} - 2^{n/2-1}$ for n even. The functions attaining this bound, are called bent functions.

Hadamard matrices

Let H be a square matrix of order n with entries in $\{\pm 1\}$. We say that H is a Hadamard matrix if

$$HH^* = nI_n$$

where I_n is the $n \times n$ identity matrix and H^T is the transpose of H.

Example

A Sylvester Hadamard matrix of order 2^n, denoted by S_n, is generated by

$$S_0 = 1, \qquad S_n = \begin{bmatrix} S_{n-1} & S_{n-1} \\ S_{n-1} & -S_{n-1} \end{bmatrix}, \qquad n = 1, 2, \ldots$$

or

Example of bent function: Hadamard matrix

$$\begin{array}{rccc} f: & \mathbb{Z}_2^2 & \rightarrow & \mathbb{Z}_2 \\ & (x_1, x_2) & \mapsto & x_1 \cdot x_2 \end{array}$$

$$H = [\zeta_2^{f(x-y)}]_{x,y\in\mathbb{Z}_2^2} = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix}$$

$$HH^T = 4I_4$$

$h_{x,y} = \zeta_2^{f(x-y)} = \zeta_2^{f(xz-yz)} = h_{xz,yz} \quad x, y, z \in \mathbb{Z}_2^2$ Group Invariant

Sylvester Hadamard matrices

Property

Let S_n be the Sylvester Hadamard matrix of order 2^n. Then

$$[S_n]_{i,j} = (-1)^{\alpha_{i-1}\alpha_{j-1}^T}$$

where $\alpha_0 = (0,\ldots,0), \alpha_1 = (0,0,\ldots,1), \ldots, \alpha_{2^m-1} = (1,\ldots,1)$ with $\alpha_i \in \mathbb{Z}_2^m$.

Bent functions and bent sequences

$$\begin{array}{rccc} f: & \mathbb{Z}_2^2 & \rightarrow & \mathbb{Z}_2 \\ & (x_1, x_2) & \mapsto & x_1 \cdot x_2 \end{array}$$

v	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$X = (-1)^{f(v)}$	1	1	1	-1
$\sum_{x\in\mathbb{Z}_2^m} (-1)^{f(x)}(-1)^{vx^\top}$	2	2	2	-2

$$\sum_{x\in\mathbb{Z}_2^m} (-1)^{f(x)}(-1)^{vx^\top} = [S_2]_{v,x} X$$

Bent functions and bent sequences

Property

Let $f\colon \mathbb{Z}_2^m \to \mathbb{Z}_2$ be a Boolean bent function. The bent sequence $X = (-1)^f$ satisfy

$$\frac{1}{\sqrt{2^m}} S_m\, X = Y,$$

for some $Y \in \{\pm 1\}^{2^m}$ where S_m is the Sylvester Hadamard matrix of order 2^m.

If $X = Y$ then the sequence X is said to be self-dual.

New notion of bent sequences

[1] P. Solé, W. Cheng, S. Guilley and O. Rioul. Bent Sequences over Hadamard Codes ... *IEEE Inter. Symposion on Inf. Theory*, 801–806, (2021).

Definition

A new notion of bent sequences was introduced in [1] as a solution in X, Y to the system

$$\frac{1}{\sqrt{n}} H\, X = Y,$$

where H is a real Hadamard matrix of order n and $X, Y \in \{\pm 1\}^n$. X is called a bent sequence for H. When $X = Y$ then is said to be self-dual.

New notion of (self-dual) bent sequences

[2] M. Shi, Y. Li, W. Cheng, D. Crnkovic, D. Krotov and P. Solé. Self-dual bent sequences for complex Hadamard matrices. *Des. Codes Cryptogr.* 91, 1453 - 1474 (2023).

Definition

In [2] this notion of self-dual bent sequence for a (real) Hadamard matrix was further generalized to (complex) Hadamard matrix with entries in the set of the complex 4-*th* roots of unity as a solution in X to the system

$$HX = \lambda X \qquad (1)$$

where λ is an eigenvalue of H and $X \in \{\pm 1, \pm\sqrt{-1}\}^n$.

Our motivation

[1] P. Solé, W. Cheng, S. Guilley and O. Rioul. Bent Sequences over Hadamard Codes ... *IEEE Inter. Symposion on Inf. Theory*, 801–806, (2021).

[2] M. Shi, Y. Li, W. Cheng, D. Crnkovic, D. Krotov and P. Solé. Self-dual bent sequences for complex Hadamard matrices. *Des. Codes Cryptogr.* 91, 1453â-1474 (2023).

Question

How to extend the “notion” of self-dual bent sequence X for any Butson Hadamard matrix H (not only for the 4-*th* roots of unity).

Real	*Complex*
$\frac{1}{\sqrt{n}} H\, X = X$	????

Butson Hadamard matrices

Let ζ_k be the complex k^{th} root of unity $\exp(2\pi\sqrt{-1}/k)$.

Let H be a square matrix of order n with entries in $\langle\zeta_k\rangle = \{\zeta_k^l : l = 0, \ldots, k-1\}$. We say that H is a Butson Hadamard matrix if

$$HH^* = nI_n$$

where I_n is the $n \times n$ identity matrix and H^* is the complex conjugate transpose of H. We denote by $H \in \mathrm{BH}(n, k)$.

Example: the m^{th} Kronecker power of the $q \times q$ Fourier matrix

$(D_{q,m})_{i,j} = \zeta_q^{\alpha_{i-1}\cdot\alpha_{j-1}^{\top}} \in \mathrm{BH}(q^m, q)$, where
$\alpha_0 = (0, \ldots, 0), \alpha_1 = (0, 0, \ldots, 1), \ldots, \alpha_{q^m-1} = (q-1, \ldots, q-1)$.

Butson Hadamard matrices: Equivalences

$P \in \mathrm{Mon}_n(\langle \zeta_k \rangle)$ means P is an $n \times n$ monomial matrix with non-zero entries in the set of k^{th} roots of unity,

The action of pairs $(P, Q) \in \mathrm{Mon}_n(\langle \zeta_k \rangle)^2$ is defined by

$$H(P, Q) = PHQ^*,$$

and this action is an equivalence operation on $\mathrm{BH}(n, k)$.

If $H(P, Q) = H'$, then H and H' are said to be equivalent.

If $H = H'$, then (P, Q) is an automorphism of H.

Generalized bent functions

A map

$$f : \mathbb{Z}_q^m \to \mathbb{Z}_q$$

is a generalized bent function (GBF) if

$$\Big| \sum_{x \in \mathbb{Z}_q^m} \zeta_q^{f(x)} \zeta_q^{-vx^\top} \Big|^2 = q^m \text{ for all } v \in \mathbb{Z}_q^m,$$

where $|z|$ as usual denotes the modulus of $z \in \mathbb{C}$

Remark

$$\overline{D}_m X = [\sum_{x \in \mathbb{Z}_q^m} \zeta_q^{f(x)} \zeta_q^{-vx^\top}]^\top_{\mathbf{v} \in \mathbb{Z}_q^m}$$

where $X = [\zeta_q^{f(\mathbf{a})}]^\top_{\mathbf{a} \in \mathbb{Z}_q^m}$ and $\overline{z}$ as usual denotes the complex conjugation.

Question

Question

If X is a GBF,

$$\frac{1}{q^{m/2}}\overline{D}_m X = \frac{1}{q^{m/2}}[\sum_{x\in\mathbb{Z}_q^m} \zeta_q^{f(x)}\zeta_q^{-vx^\top}]^\top_{\mathbf{v}\in\mathbb{Z}_q^m} \in \langle\zeta_q\rangle^{q^m} ????$$

where $X = [\zeta_q^{f(\mathbf{a})}]^\top_{\mathbf{a}\in\mathbb{Z}_q^m}$

Result: P.V. Kumar, R.A. Scholtz, L.R. Welch. Generalized bent functions and their properties. *J- Combin. Theory Ser. A*, 40 90–107, (1985)

Let q be a prime and $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_q$ a GBF,

$$\frac{1}{q^{m/2}} \sum_{x \in \mathbb{Z}_q^m} \zeta_q^{f(x)} \zeta_q^{-vx^\top} = \begin{cases} \pm\zeta_q^{f^\star(v)} & q^m = 1 \mod 4; \\ \pm\sqrt{-1}\,\zeta_q^{f^\star(v)} & q^m = 3 \mod 4, \end{cases}$$

where $f^\star\colon \mathbb{Z}_q^m \to \mathbb{Z}_q$, which is called the dual of f.

Example: $f\colon \mathbb{Z}_3^2 \to \mathbb{Z}_3$ so $m = 2$ and $q = 3$

$X = (\zeta_3)^{f(v)}$	$(\zeta_3^2, \zeta_3, \zeta_3, \zeta_3^2, \zeta_3, \zeta_3, \zeta_3, 1, 1)$
$\frac{1}{3}\overline{D_3}X$	$(\zeta_3, \zeta_3^2, \zeta_3^2, \zeta_3^2, \zeta_3^2, \zeta_3^2, \zeta_3^2, 1, 1)$

Computational facts for GBF $f\colon \mathbb{Z}_3^2 \to \mathbb{Z}_3$

There is no a solution $X \in \langle \zeta_3 \rangle^9$ to the system

$$\frac{1}{3}\overline{D}_{3,2}X = X.$$

But there are for

$$\frac{1}{3}\overline{D}_{3,2}X = \overline{X}.$$

This situation also happens for matrices in the other two classes of equivalences in $\mathrm{BH}(9,3)$.

Index

Self-dual bent (p-ary) sequences for Butson matrices

Question

How to extend the "notion" of self-dual bent sequence X for any Butson Hadamard matrix H (not only for the 4-*th* roots of unity).

Real	*Complex*
$\frac{1}{\sqrt{n}} H\, X = X$	$\frac{1}{\sqrt{n}} H\, X = \overline{X}$

Existence results for $\frac{1}{\sqrt{n}}H\ X = \overline{X}$

Proposition

If $H \in \mathrm{BH}(n,q)$ is symmetric then the sequence $X_{(i-1)n+j} = \left(H\right)_{i,j}$ is a self-dual bent sequence for $H^* \otimes H^* \in \mathrm{BH}(n^2,q)$.

Corollary

- $X_{(i-1)n+j} = \left(D_{q,m}\right)_{i,j}$ is a self-dual bent sequence for $\overline{D}_{q,2m} \in \mathrm{BH}(q^{2m},q)$.
- In the 3 equivalence classes of $\mathrm{BH}(9,3)$ are symmetric matrices.

Existence results for $\frac{1}{\sqrt{n}} H\, X = \overline{X}$

Proposition

If $H \in \mathrm{BH}(4m^2, 4)$ is of Bush-type, then it has at least 2^{2m} self-dual bent sequences attached to $-H$.

Proposition

If X and Y are self-dual bent sequences for, respectively, $H \in \mathrm{BH}(n, k)$ and $K \in BH(m, k)$, then $X \otimes Y$ is a self-dual bent sequence for $H \otimes K \in \mathrm{BH}(n \cdot m, k)$.

Necessary conditions of existence for bent sequences for $\mathrm{BH}(n,k)$ for $k=2,3$ and 4

Proposition

If there exists at least one self-dual bent sequence for $\mathrm{BH}(n,3)$ *(resp.* $\mathrm{BH}(n,4)$*), then* $n=9m^2$ *(resp.* $n=4m^2$*) with* m *a positive integer.*

Remark

The definition of bent sequence reduces to the one in Solé's papers when $k=2$*. Therefore, the necessary condition of existence for self-dual bent sequences for* $\mathrm{BH}(n,2)$ *is also that* $n=4m^2$*.*

Equivalence relations between self-dual bent sequences

Proposition

Let $H \in \mathrm{BH}(n,k)$, $P \in \mathrm{Mon}_n(\langle \zeta_k \rangle)$ and $K = \overline{P} H P^*$.

- $K \in \mathrm{BH}(n,k)$ and H and K are said to be strongly conjugate equivalent. Moreover, PX is a self-dual bent sequence for K if, and only if, X is a self-dual for H.
- If $H = K$ and X is a self-dual bent sequence for H, then PX is a self-dual bent sequence for H as well and they are said to be equivalent.

Open problems

- Are there $H \in \mathrm{BH}(36,3)$ and $X \in \langle \zeta_3 \rangle^{36}$ satisfying

$$\frac{1}{6} HX = \overline{X}????$$

- It is known there is no solution $X \in \langle \zeta_6 \rangle^{216}$ to

$$\frac{1}{6\sqrt{6}} D_{6,3} X = \overline{X}.$$

Are there $H \in \mathrm{BH}(216,6)$ and $X \in \langle \zeta_3 \rangle^{216}$ satisfying

$$\frac{1}{6\sqrt{6}} HX = \overline{X}????$$

Thank you!!!

References

B. Schmidt, *A survey of group invariant Butson matrices and their relation to generalized bent functions and various other objects.* Radon Ser. Comput. Appl. Math. 23 (2019), 241–251.

K-U Schmidt, *Highly nonlinear functions over finite fields.* Finite Fields Appl. 63 (2020), 101640.

P. Solé, W. Cheng, S. Guilley, and O. Rioul, *Bent Sequences over Hadamard Codes for Physically Unclonable Functions.* IEEE International Symposion on Inf. Theory (2021), 801–806.

M. Shi, Y. Li, W. Cheng, D. Crnkovic, D. Krotov, and P. Solé, *Self-dual bent sequences for complex Hadamard matrices.* Des. Codes Cryptogr. (2022). https://doi.org/10.1007/s10623-022-01157-6