On the matrix equation $MX = \overline{X}$ and self-dual Butson bent sequences

J. A. Armario[1], R. Egan[2], and P. Ó Catháin[3]

[1]Departamento de Matemática Aplicada I, Universidad de Sevilla, Avda. Reina Mercedes s/n, 41012 Sevilla, Spain

[2]School of Mathematical Sciences, Dublin City University, Ireland

[3]Fiontar & Scoil na Gaeilge, Dublin City University, Ireland

Abstract

Let M be a square matrix of order n and X a vector of n components, each with complex entries. We are interested in studying $MX = \overline{X}$ for some particular M where $\overline{X}$ denotes the image of X under complex conjugation. If $X \in \mathbb{R}^n$, X is an eigenvector for M associated to the eigenvalue 1. Here we reduce our study to $M = \frac{1}{\sqrt{n}}H$ where $HH^* = nI$ and the entries of H and X are in set of the complex k^{th} roots of unity (i.e., H is a Butson Hadamard matrix). Connections to generalized bent functions are studied.

1 Introduction

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

$$\frac{1}{\sqrt{n}}HX = Y,$$

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. If H is the Sylvester Hadamard matrix of order $n = 2^m$ then any bent Boolean function $f\colon \mathbb{Z}_2^m \to \mathbb{Z}_2$ determines a bent sequence for H by the rule $X = (-1)^f$ (and vice versa).

Clearly, the vector Y can also be shown to be a bent sequence attached to H^T, called the dual of X. When $X = Y$ the sequence X is said to be *self-dual*. In [4] this notion of self-dual bent sequence for a real Hadamard matrix was further generalized to a $n \times n$ Butson-Hadamard matrix with entries in the set of complex 4-*th* roots of unity as a solution in X to the system

$$HX = \lambda X \tag{1}$$

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

Bent functions are equivalent to certain Hadamard matrices and difference sets. The concept has been generalized, yielding equivalences between various associated objects. In Schmidt's survey [1] equivalences between generalized bent functions $f\colon \mathbb{Z}_k^m \to \mathbb{Z}_h$, group invariant Butson Hadamard matrices, and splitting relative difference sets are described.

In this paper, we extend the definition of self-dual bent sequence X for H to any Butson Hadamard matrix (not only for the 4-*th* roots of unity) which is "complementary" to the

definition given in [4]. That consists of considering, instead of (1), the system

$$\frac{1}{\sqrt{n}}HX = \overline{X} \quad \text{(or more generally, } HX = \lambda\overline{X}\text{)} \tag{2}$$

where the overline denotes complex conjugation, the entries of H and X belong to the set of complex k^{th} roots of unity. A solution X of the system (2) is what we understand in this paper for a self-dual bent sequence for H. We believe that it is a more natural extension from the real to the complex case. Furthermore, when H and X take values in the set $\{\pm 1\}$, we recover the definition of [3]. Some motivation for the study of this self-duality concept can also be found in this reference. Finally, it is easy to realize that if H is the complex conjugation of the m^{th} Kronecker power of the $q \times q$ Fourier matrix then any self-dual bent sequence for H determines a self-dual generalized bent function $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_q$ by the rule $X = [\zeta_q^{f(\mathbf{a})}]_{\mathbf{a}\in\mathbb{Z}_q^m}^{\top}$ which we denote by $X = \zeta_q^f$ for convenience.

2 Preliminaries

Let m and k be positive integers, and $\zeta_k = \exp(2\pi\sqrt{-1}/k)$ be a complex k^{th} root of unity. We write $\langle\zeta_k\rangle = \{\zeta_k^j\}_{0\le j\le k-1}$. Let $\mathbb{Z}_k$ be the ring of integers modulo k with $k > 1$, and denote by $\mathbb{Z}_k^m$ the set of m-tuples over $\mathbb{Z}_k$. If k is a prime, then $\mathbb{Z}_k$ is the finite field of k elements. We use bold notation $\mathbf{x} = [x_1, \ldots, x_m] \in \mathbb{Z}_k^m$ to denote vectors (or codewords) in $\mathbb{Z}_k^m$. We denote the set of $n \times n$ matrices with entries in a set S by $\mathcal{M}_n(S)$ (and in general, the set of $m \times n$ matrices $\mathcal{M}_{m,n}(S)$). Finally, overline $\overline{a}$ denotes complex conjugation of the complex number a.

2.1 Butson Hadamard matrices

Let H be a matrix of order n with complex entries of modulus 1. If the rows of H are pairwise orthogonal under the Hermitian inner product, then H is a *Hadamard matrix*. The term Hadamard matrix is more commonly used in the literature to refer to the special case with entries in $\{\pm 1\}$. In this paper, such a matrix will be call a *real Hadamard matrix*. A *Butson Hadamard (or simply Butson) matrix of order n and phase k* is a matrix $H \in \mathcal{M}_n(\langle\zeta_k\rangle)$ such that $HH^* = nI_n$, where I_n denotes the identity matrix of order n and H^* denotes the conjugate transpose of H. We write $\mathrm{BH}(n,k)$ for the set of such matrices. The simplest examples of Butson matrices are the Fourier matrices $F_n = [\zeta_n^{(i-1)(j-1)}]_{i,j=1}^n \in \mathrm{BH}(n,n)$. Real Hadamard matrices of order n, as they are usually defined, are the elements of $\mathrm{BH}(n,2)$. Denote the set of monomial matrices in $\mathcal{M}_n(\langle\zeta_k\rangle)$ by $\mathrm{Mon}_n(\langle\zeta_k\rangle)$. The phase and orthogonality of a matrix $H \in \mathrm{BH}(n,k)$ is preserved by multiplication on the left or right by an element of $\mathrm{Mon}_n(\langle\zeta_k\rangle)$ as well as by complex conjugation, i.e., $\overline{H} \in \mathrm{BH}(n,k)$. 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 induces an equivalence relation on $\mathrm{BH}(n,k)$. If $H(P,Q) = H'$, then H and H' are said to be *equivalent*.

A matrix is said to be in *dephased form* if every entry in its first row and first column is equal to 1. Every matrix can be dephased by using equivalence operations. Throughout this paper all matrices are assumed to be dephased.

Example 2.1 Let $D_{q,m}$ be the m^{th} Kronecker power of the $q\times q$ Fourier matrix, i.e., $(D_{q,m})_{i,j} = \zeta_q^{\alpha_{i-1}\cdot\alpha_{j-1}}$, where $\alpha_0 = (0,\ldots,0), \alpha_1 = (0,0,\ldots,1), \ldots, \alpha_{q^m-1} = (q-1,\ldots,q-1)$ with $\alpha_i \in \mathbb{Z}_q^m$. $D_{q,m} \in \mathrm{BH}(q^m, q)$. When $q = 2$ this is the well known Sylvester Hadamard matrix of order 2^n.

Let us mention that when q is a prime number, $D_{q,m}$ is related to the generalized first order Reed-Muller code $R_q(1,m)$.

2.2 Bent functions and generalizations

The notion of bentness admits various generalizations. We use the one in Schmidt's survey [1]. For positive integers q, m, h, a map $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_h$ is a *generalized bent function (GBF)* if

$$\Big|\mathcal{W}_f(w)\Big|^2 = q^m \quad \forall\, w \in \mathbb{Z}_q^m,$$

where $|z|$ as usual denotes the modulus of $z \in \mathbb{C}$ and $\mathcal{W}_f(w) = \sum_{x\in\mathbb{Z}_q^m} \zeta_h^{f(x)}\zeta_q^{-w\cdot x}$ (the so-called *the Walsh-Hadamard transform* of f) where $w \cdot x$ is the inner product $wx^\top$ of w and x. Thus, a GBF for $q = h = 2$ and even m is a (Boolean) bent function. For $h = q$, GBFs exist if m is even or $q \not\equiv 2 \mod 4$. However, no GBF with $h = q$, m odd, and $q \equiv 2 \mod 4$ is known.

Remark 2.2 The map $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_h$ is a GBF if, and only if, there exists $X \in \mathcal{M}_{q^m,1}(\langle\zeta_h\rangle)$ with $X_i = \zeta_h^{f(\alpha_i)}$ is a solution of the system $\frac{1}{q^{m/2}}\overline{D}_{q,m}\, X = Y$ for some $Y \in \mathcal{M}_{q^m,1}(\{y \in \mathbb{C}\colon |y| = 1\})$ (the α_i's and $D_{q,m}$ are defined in Example 2.1).

For Boolean functions, $\mathcal{W}_f(w)$ is always an integer and if it is also bent then $\mathcal{W}_f(w) = 2^{m/2}(-1)^{f^\star(w)}$ for $f^\star\colon \mathbb{Z}_2^m \to \mathbb{Z}_2$ called the *dual* of f. As is well-known, the dual $f^\star$ is a bent function as well, and $(f^\star)^\star = f$. If $f = f^\star$, the bent function f is called *self-dual*.

For $q = h$ an odd prime and $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_q$ a GBF, the value of its Walsh-Hadamard transform satisfies

$$\mathcal{W}_f(w) = \begin{cases} \pm\zeta_q^{f^\star(w)} q^{m/2} & q^m = 1 \mod 4; \\ \pm\sqrt{-1}\,\zeta_q^{f^\star(w)} q^{m/2} & q^m = 3 \mod 4, \end{cases}$$

where $f^\star\colon \mathbb{Z}_q^m \to \mathbb{Z}_q$, which again is called the dual of f. A GBF f is said to be (γ, u)-*self dual* if for all $w \in \mathbb{Z}_q^m$, $\mathcal{W}_f(w) = \gamma q^{m/2}\zeta_q^{uf(w)}$ where $\gamma \in \langle\zeta_4\rangle$ and $u \in \mathbb{Z}_q^*$. Here we are interested in the case $\gamma = 1$ and $u = -1$.

Example 2.3 Let $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_q$ with $m = 2t$ be the map

$$f(x_1, \ldots, x_{2t}) = x_1x_{t+1} + \ldots + x_tx_{2t}$$

is a $(1, -1)$-self dual GBF.

Remark 2.4 If we consider $X = \zeta_q^f$ where f is the function defined in Example 2.3, then X is a solution of the system $\frac{1}{q^{m/2}}\overline{D}_{q,m}\, X = \overline{X}$. In other words, X is a self-dual bent sequence for $\overline{D}_{q,m}$.

The *nonlinearity* of a map $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_q$ is the Hamming distance between f and the set of the q^{m+1} affine functions from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$. When q is a prime, the largest possible nonlinearity, denoted by $\rho_q(m)$, is the covering radius of the (generalized) first order Reed-Muller code $R_q(1,m)$ over $\mathbb{Z}_q$. For m even and q a prime, we have (see [2])

$$\rho_q(m) = q^{m-1}(q-1) - q^{m/2-1}.$$

Boolean ($q = 2$) bent functions are characterized as the Boolean functions in even dimension with the largest possible nonlinearity. However, a similar characterization does not apply for GBF in general (even when $q = h$ an odd prime and m even). For $q = h$ an odd prime, the nonlinearity of a GBF is known. Here we only mention that the nonlinearity of a $(1, u)$-self dual GBF for m even is $(q-1)q^{m-1} - (q-1)q^{m/2-1}$ (different to $\rho_q(m)$). For m odd, the determination of $\rho_q(m)$ is an open problem in general.

3 Self-dual bent sequences for Butson matrices

In Remark 2.4, we have seen that for $n = q^m$ and $k = q$ there are self-dual bent sequences for $\overline{D}_{q,m}$ when m is even. In this Section, we show further progress on the study of self-dual bent sequences for Butson matrices.

Firstly, we study necessary conditions of existence for self-dual bent sequences over $\mathrm{BH}(n, k)$ for $k = 2, 3$ and 4.

Proposition 3.1 *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.*

We have checked by computer that there are self-dual bent sequences for, at least, one element of any of the three matrices in $\mathrm{BH}(9, 3)$ up to equivalence.

The necessary condition of existence for self-dual bent sequences for $\mathrm{BH}(n, 2)$ is also that $n = 4m^2$ (see [3]). Let us observe that our definition of self-dual in the real case and the one given in [3] are the same.

Proposition 3.2 *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* $-H$*.*

Secondly, we give more general results on the existence. The methods for obtaining them are based on some matrix analysis and the orthogonality relations in the matrices.

Proposition 3.3 *The map* $f\colon \mathbb{Z}_q^m \times \mathbb{Z}_q^m \to \mathbb{Z}_q$ *defined by* $\zeta_q^{f(\alpha_i,\alpha_j)} = \left(D_{q,m}\right)_{i,j}$ *is a* $(1, -1)$*-self dual GBF for any integer* $q > 1$*. In other words,* $X = \zeta_q^f$ *is a self-dual bent sequence for* $\overline{D}_{q,2m}$*.*

Remark 3.4 The GBF of Proposition 3.3 and Example 2.3 are the same.

Proposition 3.5 *If* $H \in \mathrm{BH}(n, k)$ *is symmetric then the sequence* $X_{(i-1)n+j} = (H)_{i,j}$ *is a self-dual bent sequence for* $H^* \otimes H^*$*.*

Example 3.6 Each of the representatives of the three classes of $\mathrm{BH}(9, 3)$ posted at `https://www.daneflannery.com/classifying-cocyclic-butson-hadamard-matrices` are symmetric. The Paley type II elements of $\mathrm{BH}(n, 2)$ are symmetric too.

Remark 3.7 The same argument of Proposition 3.5 runs for any symmetric Hadamard matrix. That is, if C is a Hadamard matrix of order n (i.e, the entries of C belong to the set of complex numbers of modulus 1 satisfying that $CC^* = nI$) which is symmetric, then $\frac{1}{n}\left(C^* \otimes C^*\right)X = \overline{X}$ where $X_{(i-1)n+j} = (C)_{i,j}$. Hence, X is a self-dual bent sequence for $C^* \otimes C^*$.

4 On the covering radius of Butson codes

For the remainder of this section we assume, for convenience, every Butson matrix is represented in logarithmic form and we are using the Hamming distance.

The *covering radius* of a $\mathbb{Z}_k$-code C of length n is defined by $r(C) = \max_{x\in\mathbb{Z}_k^n} \min_{y\in C} d(x,y)$. Let $H \in \mathrm{BH}(n,k)$. We denote by F_H the $\mathbb{Z}_k$-code of length n consisting of the rows of H, and we denote by C_H the $\mathbb{Z}_k$-code defined as $C_H = \cup_{\alpha\in\mathbb{Z}_k}(F_H + \alpha\mathbf{1})$ where $\mathbf{1}$ denotes the all-one vector (and $\alpha\mathbf{1}$ the all-α vector). The code C_H over $\mathbb{Z}_k$ is called a *Butson Hadamard code* (briefly, BH-code).

If $H \in \mathrm{BH}(n,k)$, then the *deviation* $\Theta(C_H,\mathbf{x})$ of an arbitrary vector $\mathbf{x} \in \mathbb{Z}_k^n$ from C_H is defined as

$$\Theta(C_H,\mathbf{x}) = \max\{|\langle \mathbf{x},\mathbf{y}\rangle| \colon \mathbf{y} \in C_H\},$$

where $\langle \mathbf{x},\mathbf{y}\rangle = (\zeta_k^{x_1},\ldots,\zeta_k^{x_n})(\zeta_k^{y_1},\ldots,\zeta_k^{y_n})^* = \sum_{i=1}^n \zeta_k^{x_i-y_i}$. Then the *total deviation* of C_H is

$$\Theta(C_H) = \min\{\Theta(C_H,\mathbf{x}) \colon \mathbf{x} \in \mathbb{Z}_k^n\}.$$

Proposition 4.1 *Let $H \in \mathrm{BH}(n,3)$. Then, C_H is a $(n,3n,2/3n)$ code and $r(C_H) \geq 2/3(n - \Theta(C_H))$. If there is a bent sequence for $H \in \mathrm{BH}(n,3)$, then $\Theta(C_H) = \sqrt{n}$.*

Example 4.2 We can always choose $H \in \mathrm{BH}(9,3)$ such that there is a self-dual bent sequence for H (this is always possible for the three equivalence classes). Then, $r(C_H) \geq 4$. On the other hand, the covering radius of the generalized Reed-Muller code $R_3(1,2)$ is 5. Let us point out that $R_3(1,2)$ and $C_{D_{3,2}}$ are equivalent.

Acknowledgement

The first author was supported by Spanish Strategic R+D project TED2021-130566B-I00.

References

[1] 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.

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

[3] 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.

[4] 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