About some Hadamard full propelinear $(2t, 2, 2)$-codes. Rank and Kernel

I. Bailera, [1,2] J. Borges, [1,3] and J. Rifà [1,4]

Department of Information and Communications Engineering
Universitat Autònoma de Barcelona
08193 - Cerdanyola del Vallès, Spain

Abstract

A new subclass of Hadamard full propelinear codes is introduced in this article. We define the HFP$(2t, 2, 2)$-codes as codes with a group structure isomorphic to $C_{2t} \times C_2^2$. Concepts such as rank and dimension of the kernel are studied, and bounds for them are established. For t odd, $r = 4t-1$ and $k = 1$. For t even, $r \leq 2t$ and $k \neq 2$, and $r = 2t$ if and only if $t \not\equiv 0 \pmod 4$.

Keywords: Hadamard codes, dimension of the kernel, full propelinear codes, rank.

1 Introduction

The Hadamard conjecture proposes that an Hadamard matrix of order $4t$ exists for every positive integer t. The search for a proof of the Hadamard conjecture has stimulated several advances in the fields of design theory and

[1] This work has been partially supported by the Spanish MINECO grant TIN2013-40524-P and the Catalan grant 2014SGR-691.

[2] Email: ivan.bailera@uab.cat

[3] Email: joaquim.borges@uab.cat

[4] Email: josep.rifa@uab.cat

combinatorics. Concepts such as Hadamard groups, difference sets, cocyclic Hadamard matrices and Hadamard full propelinear codes are related in different ways.

Ito [5], [6], [7] introduced the concept of Hadamard groups, he showed a relation between Hadamard difference sets and Hadamard groups and he conjectured that the dicyclic group Q_{8t} is always a Hadamard group. Schmidt [11] has verified Ito's conjecture for $1 \leq t \leq 46$. Rifà and Suárez [10] showed that the concept of Hadamard group is equivalent to Hadamard full propelinear codes. Flannery [4] proved that the concepts of cocyclic Hadamard matrix and Hadamard groups are equivalent. De Launey, Flannery and Horadam [3] proved that the existence of a cocyclic Hadamard matrix of order $4t$ is equivalent to the existence of a normal relative difference set with parameters $(4t, 2, 4t, 2t)$. The above equivalences give us different paths to approach to the proof of Ito's conjecture. For example, the cocyclic Hadamard conjecture (de Launey and Horadam) states that there is a cocyclic Hadamard matrix of order $4t$ for all $t \in \mathbb{N}$, that is equivalent to Ito's conjecture. The cocycles over the groups $C_t \times C_2^2$, for t odd, were studied in [1] by Baliga and Horadam. The solution set includes all Williamson Hadamard matrices, so this set of groups is potentially a uniform source for generation of Hadamard matrices. Every Hadamard matrix of length ≤ 20 is cocyclic. For lengths ≤ 200, only length $4t = 188 = 4 \cdot 47$ is not yet known to have a cocyclic construction. The goal of this article is to study the algebraic properties of a kind of Hadamard full propelinear codes, which we call HFP$(2t, 2, 2)$-codes, because they have a group structure isomorphic to $C_{2t} \times C_2^2$. Our work can be related with Baliga and Horadam [1] since the permutation group of the proposed group is the same which they used to approach cocyclic Hadamard matrices. Baliga and Horadam [1] studied the t odd case and in this paper we deal with the even case. In Section 2, we present the preliminaries about Hadamard full propelinear codes. In Section 3, we define the HFP$(2t, 2, 2)$-codes and we establish bounds for the rank and dimension of the kernel.

2 Preliminaries

Let $\mathbb{F}$ be the binary field. The *Hamming distance* between two vectors $u, v \in \mathbb{F}^n$, denoted by $d_H(u, v)$, is the number of the coordinates in which u and v differ. The *Hamming weight* of u is given by $\mathrm{wt}_H(u) = d_H(u, \mathbf{e})$, where $\mathbf{e}$ is the all-zero vector. A (n, M, d)-code is a subset, C, of $\mathbb{F}^n$ such that $|C| = M$ and $d_H(u, v) \geq d$ for all $u, v \in C$ with $u \neq v$. The elements of a code are called *codewords* and d is called *minimum distance*. The parameter d determines the error-correcting capability of C which is given by $e = \lfloor \frac{d-1}{2} \rfloor$. For a vector v in $\mathbb{F}^n$, the support of v, denoted by Supp(v), is defined as the set of its nonzero positions. The *rank* of a binary code C, $r = rank(C)$, is the dimension of the linear span of C. The binary orthogonal code of the code C is the set $C^\perp = \{v \in \mathbb{F}^n : v \cdot c = 0\ \forall c \in C\}$, where $v \cdot c$ is the inner product on $\mathbb{F}$. The *kernel* of a binary code is the set of words which keeps the code invariant by translation, $K(C) := \{z \in \mathbb{F}^n : C + z = C\}$. Assuming the zero vector is in C we have that $K(C)$ is a linear subspace. We will denote the dimension of the kernel of C by $k = ker(C)$.

Definition 2.1 A $t-(v,k,\lambda)$-design is an incidence structure $(\mathcal{P},\mathcal{B})$, where $\mathcal{P}$ is a v-set of elements (called points) and $\mathcal{B}$ is a collection of k-subsets of points (called blocks) such that every t-subset of points is contained in exactly $\lambda > 0$ blocks $(0 < t \leq k \leq v)$.

Definition 2.2 A relative (v,m,k,λ)-difference set in a group G relative to a normal subgroup N, where $|G| = vm$ and $|N| = m$, is a subset D of G such that $|D| = k$ and the multiset of quotients $d_1 d_2^{-1}$ of distinct elements $d_1, d_2 \in D$ contains each element of $G \backslash N$ exactly λ times, and contains no elements of N.

Let D a relative $(4t, 2, 4t, 2t)$-difference set in a group G of order $8t$ relative to a normal subgroup $N \simeq \mathbb{F}$ of G. Thus G is called an *Hadamard group* of order $8t$.

Definition 2.3 G is an Hadamard group of order $8t$, if it is a finite group containing a $4t$-subset D and a central involution $\mathbf{u}$ (D is called Hadamard subset corresponding to $\mathbf{u}$), such that

i) D and $\mathbf{u}D$ are disjoint and $D \cup \mathbf{u}D = G$,

ii) aD and D intersect exactly in $2t$ elements, for any $a \notin \langle \mathbf{u} \rangle \subset G$,

iii) aD and $\{b, b\mathbf{u}\}$ intersect exactly in one element, for any $a, b \in G$.

Definition 2.4 An Hadamard matrix is a $n \times n$ matrix H containing entries from the set $\{1, -1\}$, with the property that:

$$HH^T = nI,$$

where I is the identity matrix.

If $n > 2$ it is easy to proof that any three rows (columns) agree in precisely $n/4$ coordinates. Thus, if $n > 2$ and there is an Hadamard matrix of order n, then n is multiple of 4. We will say $n = 4t$. The matrix obtained from an Hadamard matrix, by replacing all 1's by 0's and all -1's by 1's, is called *binary Hadamard matrix*. The binary code consisting of the rows of a binary Hadamard matrix and their complements is called a (binary) *Hadamard code*, which is of length n, with $2n$ codewords, and minimum distance $n/2$.

Let S_n be the symmetric group of permutations of the set $\{1, \ldots, n\}$. For any $\pi \in S_n$ and $v \in \mathbb{F}^n$, $v = (v_1, \ldots, v_n)$, we write $\pi(v)$ to denote $(v_{\pi^{-1}(1)}, \ldots, v_{\pi^{-1}(n)})$. Two binary codes C_1, C_2 of length n are said to be *isomorphic* if there is a coordinate permutation $\pi \in S_n$ such that $C_2 = \{\pi(x) : x \in C_1\}$. They are said to be *equivalent* if there is a vector $y \in \mathbb{F}^n$ and a coordinate permutation $\pi \in S_n$ such that $C_2 = \{y + \pi(x) : x \in C_1\}$.

Definition 2.5 A binary code C of length n has a propelinear structure if for each codeword $x \in C$ there exists $\pi_x \in S_n$ satisfying the following conditions:

(i) For all $x, y \in C$, $x + \pi_x(y) \in C$.

(ii) For all $x, y \in C$, $\pi_x \pi_y = \pi_z$, where $z = x + \pi_x(y)$

For all $x \in C$ and for all $y \in \mathbb{F}^n$, denote by $*$ the binary operation such that $x * y = x + \pi_x(y)$. Then, $(C, *)$ is a group, which is not abelian in general. The vector $\mathbf{e}$ is always a codeword and $\pi_{\mathbf{e}}$ is the identity permutation. Hence, $\mathbf{e}$ is the identity element in C and $x^{-1} = \pi_x^{-1}(x)$, for all $x \in C$. We call $(C, *)$ a propelinear code.

Proposition 2.6 *[2] Let C be a propelinear code. Then:*

(i) For $x \in C$ we have $x \in K(C)$ if and only if $\pi_x \in Aut(C)$.

(ii) The kernel $K(C)$ is a subgroup of C and also a binary linear space.

(iii) If $c \in C$ then $\pi_c \in \mathrm{Aut}(K(C))$.

Definition 2.7 An Hadamard full propelinear code is an Hadamard propelinear code C such that for every $\mathbf{a} \in C$, $\mathbf{a} \neq \mathbf{e}$, $\mathbf{a} \neq \mathbf{u}$ the permutation $\pi_{\mathbf{a}}$ has not any fixed coordinate and $\pi_{\mathbf{e}} = \pi_{\mathbf{u}} = Id$.

An automorphism of an Hadamard code is a permutation on the set of coordinates leaving the code invariant. The *group* Π *of permutations* of a propelinear code C is defined by $\Pi = \{\pi_x \in S_n : x \in C\}$.

Proposition 2.8 *Let C be an Hadamard full propelinear code of length $4t$. Then $\mathbf{u} \in K(C)$ and the group of permutations of C is isomorphic to $C/\langle \mathbf{u} \rangle$.*

3 HFP$(2t, 2, 2)$-codes

Definition 3.1 Let C be an HFP code of length $4t$. We will say that C is an HFP$(2t, 2, 2)$-code when C is the direct product $C_{2t} \times C_2 \times C_2$, where C_i is a cyclic group of order i.

Let C be an HFP$(2t, 2, 2)$-code, there are two possibilities for the presentation of C:

(i) $C = \langle \mathbf{a}, \mathbf{b}, \mathbf{u} \rangle$, where $\mathbf{a}$ has order $2t$ and $\mathbf{b}$ has order 2.

(ii) $C = \langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle$, where $\mathbf{a}$ has order $2t$, $\mathbf{a}^t = \mathbf{u}$, $\mathbf{b}$ has order 2 and $\mathbf{c}$ has order 2.

Hereinafter, we assume that $C = \langle \mathbf{a}, \mathbf{b}, \mathbf{u} \rangle$.

Proposition 3.2 *Let C be an* HFP$(2t, 2, 2)$*-code. Then, up to equivalence, we can assume*

i) $\pi_{\mathbf{a}} = (1, 2, \ldots, 2t)(2t + 1, 2t + 2, \ldots, 4t)$,

ii) $\pi_{\mathbf{b}} = (1, 2t + 1)(2, 2t + 2) \ldots (2t, 4t)$,

iii) Knowing the value of $\mathbf{a}$ *is enough to define* $\mathbf{b}$.

Proposition 3.3 *Let C be an* HFP$(2t, 2, 2)$*-code which is not linear with t odd. Then $r = 4t - 1$ and $k = 1$.*

Proposition 3.4 *Let C be an* HFP$(2t, 2, 2)$*-code which is not linear with t even. Then $r \leq 2t$, and $r = 2t$ if and only if $t \not\equiv 0 \pmod 4$.*

The next lemma is a generalization to nonlinear Hadamard codes of a Parseval equation (see [8] Corollary 3, p. 416 for the linear case and [9] for length a power of two).

Lemma 3.5 *Let C be an Hadamard code of length $4t$, $\mathbf{e} \neq s \in \mathbb{F}^{4t}$, and $S = \mathrm{Supp}(s)$. Then $|S|^2 - 4t|S| + 2\sum_c \delta_c^2 = 0$, where the sum is extended to all vectors $c \in C$ of weight $2t$ and δ_c is such that $|\mathrm{Supp}(s) \cap \mathrm{Supp}(c)| = |S|/2 \pm \delta_c$.*

Proposition 3.6 *Let C be an* HFP$(2t, 2, 2)$*-code* $= \langle \mathbf{a}, \mathbf{b}, \mathbf{u} \rangle$*, where* $\mathbf{a}$ *has order $2t$ and* $\mathbf{b}$ *has order 2. If* $\mathbf{b} \in K(C)$ *then $k \geq 3$.*

Proposition 3.7 *Let C be an* HFP$(2t, 2, 2)$*-code* $= \langle \mathbf{a}, \mathbf{b}, \mathbf{u} \rangle$*, where* $\mathbf{a}$ *has order $2t$ and* $\mathbf{b}$ *has order 2. If* $\mathbf{a}^t \in K(C)$ *then $k \geq 3$.*

Example 3.8 We have constructed all HFP$(2t, 2, 2)$-codes $= \langle \mathbf{a}, \mathbf{b}, \mathbf{u} \rangle$ of length 16, *i.e.* $t = 4$. There are two types of generated codes, one of them are linear codes with $r = 5$ and $k = 5$, and the other are nonlinear codes with $r = 6$ and

$k = 3$. The values for the generators $\mathbf{a}$ and $\mathbf{b}$ for an specific nonlinear case are the following:

$$\mathbf{a} = (0,1,1,1,0,0,1,0,1,1,0,1,1,0,0,0),$$

$$\mathbf{b} = (0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1),$$

$$\pi_{\mathbf{a}} = (1,2,3,4,5,6,7,8)(9,10,11,12,13,14,15,16),$$

$$\pi_{\mathbf{b}} = (1,9)(2,10)(3,11)(4,12)(5,13)(6,14)(7,15)(8,16).$$

References

[1] Baliga, A. and K. J. Horadam, *Cocyclic Hadamard matrices over* $\mathbb{Z}_n \times \mathbb{Z}_2^2$, Australasian Journal of Combinatorics **11** (1995), pp. 123–134.

[2] Borges, J., I. Y. Mogilnykh, J. Rifà and F. I. Solov'eva, *Structural properties of binary propelinear codes.*, Advances in Mathematics of Communications **6** (2012), pp. 329 – 346.

[3] de Launey, W., D. L. Flannery and K. J. Horadam, *Cocyclic Hadamard matrices and difference sets*, Discrete Applied Mathematics **102** (2000), pp. 47–61.

[4] Flannery, D., *Cocyclic Hadamard matrices and Hadamard groups are equivalent*, Journal of Algebra **192** (1997), pp. 749–779.

[5] Ito, N., *On Hadamard groups*, Journal of Algebra **168** (1994), pp. 981 – 987.

[6] Ito, N., *On Hadamard groups II*, Journal of Algebra **169** (1994), pp. 936 – 942.

[7] Ito, N., *On Hadamard groups III*, Kyushu Journal of Mathematics **51** (1997), pp. 369–379.

[8] MacWilliams, F. J. and N. J. A. Sloane, "The Theory of Error-Correcting Codes," Amsterdam: North-Holland, 1983.

[9] Phelps, K. T., J. Rifà and M. Villanueva, *Rank and kernel of binary Hadamard codes*, Information Theory, IEEE Transactions on **51** (2005), pp. 3931–3937.

[10] Rifà, J. and E. Suárez, *About a class of Hadamard propelinear codes*, Electronic Notes in Discrete Mathematics **46** (2014), pp. 289–296.

[11] Schmidt, B., *Williamson matrices and a conjecture of Ito's*, Designs, Codes and Cryptography **17** (1999), pp. 61–68.