About a class of Hadamard Propelinear Codes. *

Josep Rifà Coma and Emilio Suárez Canedo

Departament d'Enginyeria de la Informació i de les Comunicacions,
Universitat Autònoma de Barcelona
josep.rifa@deic.uab.cat,emilio.suarez@deic.uab.cat

Abstract. This article aims to explore the algebraic structure of Hadamard propelinear codes, which are not abelian in general but they have good algebraic and combinatorial properties. Concretely, we construct a subclass of Hadamard propelinear codes which enlarges the Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. Several papers have been devoted to the relations between difference sets, t-designs, cocyclic-matrices and Hadamard groups, and we present a link between them and a class of Hadamard propelinear codes, which will be called full propelinear. Finally, as an exemplification, we go over Hadamard codes of length sixteen giving a propelinear structure for all of them.

Key words: Hadamard group, propelinear code, full propelinear codes.

1 Introduction

The discovery of the existence of a quaternary structure in some relevant families of codes with better parameters than any linear code [9] has raised the interest in the study of these codes and more generally on codes with a group structure. Propelinear codes issued from the idea of study the relationship between completely regular codes and regular graphs. Any propelinear code is associated to a group structure, for instance $\mathbb{Z}_2\mathbb{Z}_4$-linear codes ([6,9]) are propelinear codes. An important subclass of propelinear codes are those which are translation invariant, which were charaterized as $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code in [14]. The goal of this article is to study the algebraic properties of a kind of propelinear, which we call full propelinear.

In Section 2, we present the preliminaries of propelinear codes and the connections between the difference sets, t-designs, Hadamard groups, and cocyclic matrices. In Section 3, we construct the subclass of Hadamard full propelinear codes and anaylize some of the algebraic properties of these codes, while concluding that all Hadamard codes of length sixteen are Hadamard propelinear codes.

* This work has been partially supported by the Spanish MICINN under Grants TIN2010-17358 and TIN2013-40524-P, and by the Catalan AGAUR under Grant 2009SGR1224.

2 Preliminaries

We denote by $\mathbb{Z}$, $\mathbb{Z}_r$, $\mathbb{F}_q$, the ring of integers, the ring of integers modulo r and any representation of a finite field with q elements, respectively. Any subset C of $\mathbb{F}_2^n$ is called a binary code. It is denoted by $d_H(\cdot,\cdot)$ and $\mathrm{wt}_H(\cdot)$ the *Hamming distance* and the *Hamming weight* on $\mathbb{F}_q^n$, respectively. We write $d_H(C)$ for the minimum distance of a linear code C, which is equal to its minimum weight, for C a linear subspace. A $[n,k,d]$ linear code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The elements of C are called *codewords*. If the code is not linear we will call (n,M,d) a code of length n, cardinality M and minimum distance equal to d. The parameter d determine the error-correcting capability of C which is given by $e=\left\lfloor \frac{d-1}{2} \right\rfloor$. For a word v in $\mathbb{F}_q^n$, the support of v, denoted by $\mathrm{Supp}(v)$, is defined as the set of its nonzero positions.
Let S_n denote the symmetric group of permutations of the set $\{1,\ldots,n\}$. For any $\pi \in S_n$ and any vector $v \in \mathbb{F}_2^n$, $v=(v_1,v_2,\ldots,v_n)$, we write $\pi(v)$ to denote $(v_{\pi^{-1}(1)},v_{\pi^{-1}(2)},\ldots,v_{\pi^{-1}(n)})$. The isometries of a code C (distance preserving bijective mappings from C to C) form a group, $\mathrm{Iso}(C)$. We will call $\mathrm{Perm}(C)$ the group of coordinate permutations stabilizing C. 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 $y \in \mathbb{F}_2^n$ and a $\pi \in S_n$ such $C_2=\{y+\pi(x) : x \in C_1\}$.
The *rank* of a binary code C is the dimension of the linear span of the codewords of C. The *kernel* K of a binary code C is the set of words which keeps the code invariant by translation, so $K(C)=\{z \in \mathbb{F}_2^n : C+z=C\}$. Assuming the all zero vector is in C we have that the kernel is a linear subspace and the dimension of $K(C)$ will be denoted by by $k(C)$ or simply k.

Definition 1. *[15] 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:*

1. *For all $x,y \in C$, $x+\pi_x(y) \in C$,*
2. *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 $y \in \mathbb{F}_2^n$, denote by $*$ the binary operation such that $x*y=x+\pi_x(y)$. Then, $(C,*)$ acts over $\mathbb{F}_2^n$ and, specifically, it is a group, which is not abelian in general. The vector $\mathbf{0}$ is always a codeword and $\pi_{\mathbf{0}}$ is the identity permutation. Hence, $\mathbf{0}$ is the identity element in C and $x^{-1}=\pi_x^{-1}(x)$, for all $x \in C$ [15]. We call $(C,*)$ a **propelinear code** if it can be provided with a propelinear structure.

Definition 2. *The action of a group, G on a set X is regular if it is both transitive and semiregular. Transitivity requires that for all $x,y \in X$, there is some $g \in G$ such that $gx=y$. Semiregularity requires that the stabilizers of all points be trivial. Obviously, if G acts regularly on X then $|G|=|X|$.*

Proposition 1. *[11] Let $(C, *)$ be a group. C is a propelinear code if and only if* $\mathrm{Iso}(C)$ *contains a regular subgroup acting transitively on C.*

Definition 3. *A Hadamard matrix is an $4n \times 4n$ matrix H containing entries from the set $\{1, -1\}$, with the property that:*

$$HH^T = 4nI,$$

where I means the identity matrix.

Let H be a normalized Hadamard matrix of order $4n$, so a matrix with all the entries in the first row and first column equal to $+1$. let H' be the matrix H after removing the first row and the first column. Let $B = \frac{1}{2}(H' + J)$, where J is the all one matrix. Hadamard matrices of order $4n$ $(n > 1)$, can be used to create an special family of 2-designs.
A set T of vectors $v \in \mathbb{F}^n$ of weight w is a *t-design*, t-(n, w, λ), if for any vector $z \in \mathbb{F}_2^n$ of weight t, $1 \leq t \leq w$, there are precisely λ vectors $v_i,\ i = 1, \ldots, \lambda$ from T, each of them covering z. A square divisible (n, m, w, λ)-design consists of a set of nm points and a set of nm blocks, where each point is in w blocks and each block consists of w points. Further, the point set is partitioned into n point classes of m points each, such that two points in distinct classes are both contained in precisely λ blocks, and no block contains distinct points in the same class. A 2-(n, w, λ)-design is just a divisible $(n, 1, w, \lambda)$-design.
Thus, note that the before defined matrix B is the incidence matrix of a 2-$(4n - 1, 2n - 1, n - 1)$ design, and we can take it as an alternative definition for a Hadamard matrix [1]. Let H be a $4n \times 4n$ Hadamard matrix, and A the incidence matrix defined by $A = \frac{1}{2}(H + J)$. Write $\bar{A}$ for the complement of A. Then

$$\Phi = \begin{pmatrix} A & \bar{A} \\ \bar{A} & A \end{pmatrix}$$

is the incidence matrix of a divisible $(4n, 2, 4n, 2n)$-design.

Elliott and Butson [5] define a **relative (v, m, k, λ)-difference set in a group** G relative to a normal subgroup N, where $|G| = vm$ and $|N| = m$. This 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. Thus $k(k-1) = \lambda m(v-1)$ and $v \neq 2k$. Equivalently, $|D \cap xD| = \lambda$, for all $x \in G \backslash N$. Let R be a relative $(4n, 2, 4n, 2n)$-difference set in a group G of order $8n$ relative to a normal subgroup $N \simeq \mathbb{Z}_2$ of G. Such a group is called a **Hadamard group** of order $8n$ [8]. In other words, G is a Hadamard group of order $8n$ and identity element $\mathbf{e}$, if it is a finite group containing a $4n$-subset D and an element $\mathbf{u}$ (called Hadamard subset corresponding to $\mathbf{u}$), such that

- D and $\mathbf{u}D$ are disjoints,
- aD and D intersect exactly in $2n$ elements, for any $a \in G$, $a \neq \mathbf{u}$, $a \neq \mathbf{e}$.

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

Let G be a finite group of order $4n$ and let $\langle -1 \rangle \simeq \mathbb{Z}_2$. A (normalized, binary, two-dimensional) cocycle is a set map $\psi\colon G \times G \to \mathbb{Z}_2$ satisfying $\psi(\mathbf{e}, \mathbf{e}) = 1$ and

$$\psi(g, h)\psi(gh, k) = \psi(g, hk)\psi(h, k), \text{for all } g, h, k \in G.$$

A cocycle over G is naturally displayed as a **cocyclic matrix** M; that is, under some fixed ordering of the elements of G which indexes rows, and some (possibly different) fixed ordering of the elements of G which indexes columns, the entry in the (g, h)th position of the cocyclic matrix is $\psi(g, h)$, for all $g, h \in G$.
The connection between cohomology theory and Hadamard matrices afforded by cocyclic matrices was introduced by de Launey and Horadam. Furthermore, in [3] it is stated that the existence of a normal relative $(4n, 2, 4n, 2n)$ difference set is equivalent to the existence of a cocyclic Hadamard matrix of order $4n$. In [7], Flannery proved that the concepts of Hadamard group and cocyclic Hadamard matrix are equivalent.

Definition 4. *Any binary $(2n, 4n, n)$-code is called a Hadamard code. Furhter, C is said to be a Hadamard propelinear code if it is a Hadamard code and also a propelinear code.*

In [12] it was computed all possible values for two structural parameters (rank and dimension of the kernel) of a binary Hadamard code of length a power of two. Our interest is to deal with Hadamard codes with some kind of algebraic structure. The most basic structure is coming from groups of order 8 which, apart from those composed by $\mathbb{Z}_2$ and $\mathbb{Z}_4$, are the cyclic $\mathbb{Z}_8$, the dihedral D_8 and the quaternionic Q_8. The next proposition summarizes the results we obtained.

Proposition 2. *(The propelinear structures for Q_8, D_8, $\mathbb{Z}_8$)*

1. *The minimum lenght n for which a Hadamard propelinear structure exists for $Q_8 = \langle \mathbf{a}, \mathbf{b} : \mathbf{a}^4 = \mathbf{e}, \mathbf{a}^2 = \mathbf{b}^2, \mathbf{a}^{\mathbf{b}} = \mathbf{bab}^{-1} = \mathbf{a}^{-1} \rangle$ is $n = 4$. Furthermore, this structure is unique (up to isomorphism) and is given by:*

$$\mathbf{a} = (0, 1, 0, 1), \mathbf{b} = (0, 1, 1, 0), \pi_{\mathbf{a}} = (1, 2)(3, 4), \pi_{\mathbf{b}} = (1, 3)(2, 4).$$

2. *The unique Hadamard propelinear structure of length n for the dihedral $D_8 = \langle a, b : a^4 = \mathbf{e}, b^2 = \mathbf{e}, a^b = bab^{-1} = a^{-1} \rangle$ is given by:*

$$a = (1, 1, 0, 0), b = (0, 1, 1, 0), \pi_a = (1, 4)(2, 3), \pi_b = (1, 4)(2, 3).$$

Furthermore, there are only two propelinear structures of length 3 (up to isomorphism) given by:

$$a = (1, 1, 0), b = (1, 0, 0), \pi_a = (23), \pi_b = (23).$$
$$a = (1, 0, 0), b = (0, 0, 1), \pi_a = (12), \pi_b = (12).$$

3. *There is no any Hadamard propelinear structure for the cyclic group* $\mathbb{Z}_8 = \langle a : a^8 = \mathbf{e} \rangle$. *Although, there is a unique propelinear structure (up to isomorphism) of length 4 given by:*

$$a = (1, 1, 1, 0), \pi_a = (1, 2, 3, 4).$$

3 Hadamard Full Propelinear Codes

In this section we introduce the concept of Hadamard full propelinear code C. These codes have the property that the associated permutation π_x to each $x \in C$ do not have any fix point, except for $x \in \{\mathbf{e}, \mathbf{u}\}$. We show that the above definition is equivalent to the well known concepts of Hadamard group, 2-cocyclic matrices and relative difference sets. The section concludes showing that all binary Hadamard codes of length 16 are full propelinear.

Definition 5. *A Hadamard full propelinear code is a Hadamard propelinear code* C *such that for every* $a \in C$, $a \neq \mathbf{e}, a \neq \mathbf{u}$ *the permutation* π_a *has not any fixed coordinate and* $\pi_{\mathbf{e}} = \pi_{\mathbf{u}} = I$.

Lemma 1. *In a Hadamard full propelinear code* $(C, *)$ *let* $\mathbf{u}$ *be the all one vector. Then vector* $\mathbf{u}$ *is central in* C *and* $\pi_{\mathbf{u}} = I$.

Let C be a Hadamard full propelinear code of length $4n$. Define $D_j \subset C$ the subset of all vectors in C such that the jth coordinate is zero. Vectors in C have $4n$ coordinates and we can associate each one of them to a vector in D_j. Let $x \in D_j$ such that $\pi_x(e_j) = e_x$, where, for $i \in \{1, \ldots, 4n\}$, e_i means the unitary vector with only one nonzero coordinate at the position ith. The position where e_x is nonzero is the associated coordinate to vector x. This association is well defined, for a vector $y \neq x$ the associated coordinate is $e_y \neq e_x$. Let k the position where e_x has the nonzero coordinate. Note that either $D_k = x * D_j$ or $D_k = \mathbf{u} * x * D_j$ depending on the value of the kth coordinate of vector x. Calling $\delta_{x,j} = \mathbf{e}$ when the value of the kth coordinate of vector x is zero and $\delta_{x,j} = \mathbf{u}$ when the value of the kth coordinate of vector x is one, we have $D_k = \delta_{x,j} * x * D_j$, for $x \in D_j$.

Let H be the normalized Hadamard matrix corresponding to C and assume that the columns and the rows of H are indexed by the elements in D_1. The (y, x)-entry of H is zero if vector y belongs to D_k, where $\pi_x(e_1) = e_k$, so

$$(y, x)\text{-entry of } H \text{ is zero if and only if } y * x^{-1} * \delta_{x,1} \in D_1. \tag{1}$$

Proposition 3. *Let $(C, *)$ be a Hadamard propelinear code of length $4n$. Let D_1 the set of codewords with a zero in the first coordinate. Then for any $a \in C$ we have $|D_1 \cap a * D_1| \in \{0, 4n, 2n\}$.*

If C is a Hadamard full propelinear code of length $4n$ then C is a Hadamard group in the sense of [8] and D_1 is a Hadamard set corresponding to $\mathbf{u}$.

Proof.

1. If $a \in D_1$ and π_a does not include the first position then $a * D_1 = D_1$ and $|D_1 \cap a * D_1| = 4n$.
2. If $a \notin D_1$ and π_a does not include the first position then $a * D_1 = \mathbf{u} * D_1$ and $|D_1 \cap a * D_1| = 0$.
3. If π_a includes the first position, say that $\pi_a(e_1) = e_k$ then $D_k = \delta_{a,1} * a * D_1$ and $|D_1 \cap a * D_1| = 2n$.

If C is a full propelinear code the previous first two items show that $|D_1 \cap a * D_1| = 4n$ if and only if $a = \mathbf{e}$ and $|D_1 \cap a * D_1| = 0$ if and only if $a = \mathbf{u}$. Hence, in this case, C is a Hadamard group.

Proposition 4. *Let G be a Hadamard group with D as a Hadamard subset. Then G is a Hadamard full propelinear code.*

Proof. Let G a Hadamard group of order $8n$ with Hadamard subset D. We can construct an $4n \times 4n$ matrix H, where the rows and columns are indexed by the elements in D. The entry (a, b) of H is 0 or 1, depending on whether $ab^{-1}\delta_{b,1} \in D$, where $\delta_{b,1}$ was defined in (1). Matrix H is a Hadamard matrix and G can be equipped with a full propelinear structure. For any $a \in G$ define $\pi_a(x) = a + xa$, where $x \in G$. The map π_a acts as a permutation on the coordinates. Specifically, coordinate given by b is moved to coordinate ba after π_a. To show this, take two vectors x, y with the same value on the coordinate given by b, so xb^{-1} and yb^{-1} simultaneously belong (respectively, does not belong) to D. Consider the values of $(a + xa)$ and $(a + ya)$ on the coordinate given by ba. This pair of values agrees or does not agree like the values of xa and ya on the same coordinate and these last ones agree or do not agree depending on whether $xa(ba)^{-1}$ and $ya(ba)^{-1}$ simultaneously belong (respectively, do not belong) to D. Thus, we reached the same condition that the starting one. Also we see that $\pi_a(\mathbf{e}) = a + \mathbf{e}a = \mathbf{e}$. Finally, we can define the propelinear structure on G given by $a * b = a + \pi_a(b) = ba$. This proves the statement.

It is well known that there are five inequivalent Hadamard codes of length 16. One of them is linear, another is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code and the other three cannot be realized as $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, [6]. However, one of those can be realized as a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code, more specifically, as a pure Q_8-code [4]. As an exemplification of the concepts of the current paper we present the last two

as Hadamard full propelinear codes. The group structure of these two propelinear codes correspond to a generalized quaternion group of order 32. This generalized quaternion group is given by $Q_{32} = \langle \mathbf{a}, \mathbf{b} : \mathbf{a}^{16} = \mathbf{e}, \mathbf{a}^8 = \mathbf{b}^2, \mathbf{a}^{\mathbf{b}} = \mathbf{bab}^{-1} = \mathbf{a}^{-1} \rangle$. To construct these propelinear codes take $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^{16}$ and their corresponding permutations $\pi_{\mathbf{a}}, \pi_{\mathbf{b}} \in S_4$.
The code C with rank equal to 8 and dimension of the kernel 2 is given by:

$$\begin{aligned} \mathbf{a} &= (1,1,1,1,0,0,1,0,0,1,1,0,0,0,0,1), \\ \mathbf{b} &= (0,0,1,0,1,1,0,0,1,1,1,0,0,1,0,1), \\ \pi_{\mathbf{a}} &= (8,7,6,5,4,3,2,1)(16,15,14,13,12,11,10,9), \\ \pi_{\mathbf{b}} &= (1,9)(2,16)(3,15)(4,14)(5,13)(6,12)(7,11)(8,10). \end{aligned}$$

and the remainder elements are computed giving the code $C = \langle \mathbf{a}, \mathbf{b} \rangle$.
The code $D = \langle \mathbf{a}, \mathbf{b} \rangle$, with rank equal to 8 and dimension of the kernel 1, is computed taking:

$$\begin{aligned} \mathbf{a} &= (1,1,1,1,0,0,1,0,1,0,1,1,0,0,0,0), \\ \mathbf{b} &= (0,1,1,1,0,0,0,1,1,0,0,0,1,1,1,0), \\ \pi_{\mathbf{a}} &= (8,7,6,5,4,3,2,1)(9,10,11,12,13,14,15,16), \\ \pi_{\mathbf{b}} &= (1,9)(2,10)(3,11)(4,12)(5,13)(6,14)(7,15)(8,16). \end{aligned}$$

Note that in both cases, the group $\Pi = \{\pi_x : x \in G\}$, where G is either C or D, is the dihedral group of order 16.

References

[1] E. F. Assmus, Jr. and J. D. Key. *Designs and their Codes. Cambridge University Press,* 1992. Cambridge Tracts in Mathematics, Vol. 103.

[2] W. Burnside, *Theory of Groups of Finite Order, 2nd edition, Cambridge University Press,* 1911, reprinted Dover Publications, New York, 1955.

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

[4] Á. del Rio, J. Rifà, *Families of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-Codes, IEEE Trans. Inf. Theory,* Vol. 59, (8), August 2013. pp: 5140–5155.

[5] J.E.H. Elliott, A.T. Butson, *Relative difference sets, Illinois J. Math. 10* (1966) 517–531.

[6] C. Fernandez-Cordoba, J. Pujol and J.Rifà, M. Villanueva *$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: Rank and kernel Designs,Codes and Cryptography,* volume 54, number 2, p.167-179, August 2009

[7] D.L. Flannery, *Cocyclic Hadamard matrices and Hadamard groups are equivalent, J. Algebra*192 (1997) 749–779.

[8] N. Ito, *On Hadamard groups, J. Algebra 168* (1994) 981–987.

[9] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Transactions on Information Theory*, 40(2) (1994) 301–319.

[10] K. J. Haradam, *Hadamard matrices and their applications. Princeton University Press.* Princeton New Jersey. 2007.

[11] K. T. Phelps, J. Rifà, *On Binary* 1*-Perfect Additive Codes: Some Structural Properties, IEEE Trans. Inf. Theory,* Vol. 48, No. 9, September 2002. pp. 2587–2592.

[12] K. T. Phelps, J Rifà, M. Villanueva, *Rank and kernel of binary Hadamard codes, IEEE Trans. Inf. Theory,* Vol. 51 (11), pp: 3931–3937. 2005.

[13] K. T. Phelps, J Rifà, M. Villanueva, *On the Additive ($\mathbb{Z}_4$-Linear and Non-$\mathbb{Z}_4$-Linear) Hadamard Codes: Rank and Kernel. IEEE Trans. Inf. Theory,* Vol. 52 (1), pp: 316–324. 2006.

[14] J. Rifà, J. Pujol, *Translation invariant properlinear codes. IEEE Trans. Inform. Theory,* vol. 43, pp.590-598, 1997.

[15] J. Rifà, J. M. Basart, L. Huguet, *On completely regular propelinear codes, Lecture Notes in Computer Science.* Berlin, Germany: Springer-Verlag, vol. 357, pp. 341–355, 1989.