This is the accepted versión of: Rifà, J. and Suárez Canedo, E. "Kronecker sums to construct Hadamard full propelinear codes of type Cn Q8" in Springer Proceedings in Mathematics & Statistics, 2016 (Proceedings of the 21st Conference on applications of computer algebra, July 20-23, 2015, Kalamata, Greece)

Kronecker sums to construct Hadamard full propelinear codes of type C_nQ_8

J. Rifà[1], E. Suárez Canedo[1]

[1] *Universitat Autònoma de Barcelona, Catalunya, Spain, {josep.rifa,emilio.suarez}@uab.cat*

Hadamard matrices with a subjacent algebraic structure have been deeply studied as well as the links with other topics in algebraic combinatorics [1]. An important and pioneering paper about this subject is [5], where it is introduced the concept of Hadamard group. In addition, we find beautiful equivalences between Hadamard groups, 2-cocyclic matrices and relative difference sets [4], [7]. From the side of coding theory, it is desirable that the algebraic structures we are dealing with preserves the Hamming distance. This is the case of the propelinear codes and specially those which are translation invariant which has been characterized as the image, by a suitable Gray map, of a subgroup of a direct product of $\mathbb{Z}_2$, $\mathbb{Z}_4$ and Q_8 (see [8] and references there).

As for the 2-cocyclic matrices and relative difference sets it was shown in [10] that the concept of Hadamard group is equivalent to Hadamard full propelinear codes (HFP for short). This new equivalence provides a good place to study the rank and the dimension of the kernel of the Hadamard codes we construct. These are important steps trying to solve several conjectures involving Hadamard matrices. In [6] it was introduced a special Hadamard group, called type Q and it was conjectured that Hadamard matrices of this type exists for all possible lengths.

In this paper we are studying Hadamard codes of type C_nQ_8, which are full propelinear and the subjacent group structure is isomorphic to a direct sum of the cyclic group C_n and the quaternion group Q_8. The main results we present are about the links with the Hadamard codes of type Q and the construction of Kronecker sums allowing to duplicate or quadruplicate the length of the code. With the current results we conjecture that it is not possible to go deeper with the Kronecker construction than duplicate or quadruplicate the initial HFP-code, otherwise we contradicts the Ryse conjecture [11] about circulant Hadamard matrices.

1 Introduction

We denote by $\mathbb{Z}_q$, the ring of integers modulo q and by $\mathbb{F}_q$ a finite field with q elements. The Hamming distance between two vectors $x, y \in \mathbb{F}_2$, denoted by $d_H(x,y)$, is the number of coordinates in which they differ, and $wt_H(x)$ is the Hamming weight. We write d for the minimum distance of a code which is equal to its mini-

mum weight when C is linear. A $[n,k,d]$-code C over $\mathbb{F}_q$ is a k-dimensional vector subspace of $\mathbb{F}_q^n$ with minimum distance d. Any subset C of $\mathbb{F}_2^n$ is called a binary code. If the code is not linear we say that a (n,M,d)-code has length n, cardinal M and minimum Hamming distance d. For a vector v in $\mathbb{F}_q^n$, the support of v, denoted by $\mathrm{Supp}(v)$, is defined as the set of its nonzero positions. The *rank* of a binary code C is the dimension of the linear span of C. The *kernel* of a binary code is the set of words which keeps the code invariant by translation, $K(C) : \{z \in \mathbb{Z}_2^n : z+C = C\}$. Assuming that the zero vector is in C, the kernel is a linear subspace and we denote by k its dimension.

An Hadamard matrix of order $4n$ is a matrix of size $4n \times 4n$ with entries ± 1, such that $HH^T = 4nI$. Any two rows (columns) of an Hadamard matrix agree in precisely $2n$ components. Two Hadamard matrices are equivalent if one can be obtained from the other by permuting rows and/or columns and multiplying rows and/or columns by -1. With the last operations we can change the first row and column of H into $+1$'s and we obtain an equivalent Hadamard matrix which is called normalized. If $+1$'s are replaced by 0's and -1's by 1's, the initial Hadamard matrix is changed into an (binary) Hadamard matrix and, from now on, we will refer to it when we deal with Hadamard matrices. The binary code consisting of the rows of an (binary) Hadamard matrix and their complements is called an (binary) Hadamard code C_H, which is of length $4n$, with $8n$ codewords, and minimum distance $2n$.

In Section 1 we introduce some basics about the subject. In Section 2, we define the concept of Hadamard full propelinear code and we describe the motivation to work using $C_n \times Q_8$ group structures. In Section 3, we focus our attention to the case of n odd, we compute the rank and the dimension of the kernel and we provide an example of this kind of codes. In Section 4, we use the Kronecker sum construction to duplicate and quadruplicate the length of the initial HFP-code of type C_nQ_8, with n odd, obtaining new HFP-codes of type $C_{2n}Q_8$ and $C_{4n}Q_8$.

2 Hadamard full propelinear codes

Let S_n denote the symmetric group of permutations of the set $\{1,2,\ldots,n\}$. For any $\pi \in S_n$ and $v \in \mathbb{F}_2^n$, we denote by $(v_{\pi^{-1}(1)}, v_{\pi^{-1}(2)}, \ldots, v_{\pi^{-1}(n)})$ the image of the vector $v = (v_1, v_2, \ldots, v_n)$ by the permutation π.

Definition 1. *[2] 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:*

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

For all $x \in C$ and for all $y \in \mathbb{Z}_2^n$, 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 $\mathbf{0}$ 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 $x \in C$, [2]. We call C an Hadamard propelinear code if it has a propelinear structure and it is an Hadamard code.

As an example, let Q_8 be the group of quaternions which can be presented as $Q_8 = \{\mathbf{a}, \mathbf{b} : \mathbf{a}^4 = \mathbf{e}; \mathbf{a}^2 = \mathbf{b}^2 = \mathbf{u}, \mathbf{bab}^{-1} = \mathbf{a}^{-1}\} = \{\mathbf{e}, \mathbf{a}, \mathbf{a}^2, \mathbf{a}^3, \mathbf{b}, \mathbf{ab}, \mathbf{a}^2\mathbf{b}, \mathbf{a}^3\mathbf{b}\}$. We use the *Gray map* given by $\mathbf{e} \to (0,0,0,0)$, $\mathbf{b} \to (0,1,1,0)$, $\mathbf{a} \to (0,1,0,1)$, $\mathbf{ab} \to (1,1,0,0)$, $\mathbf{a}^2 \to (1,1,1,1)$, $\mathbf{a}^2\mathbf{b} \to (1,0,0,1)$, $\mathbf{a}^3 \to (1,0,1,0)$, $\mathbf{a}^3\mathbf{b} \to (0,0,1,1)$. As a propelinear code, the associated permutations to the generator elements of Q_8 are: $\pi_{\mathbf{a}} = (1,2)(3,4)$, $\pi_{\mathbf{b}} = (1,3)(2,4)$. From now on, we use $\mathbf{e}$ for the binary all-zero vector and $\mathbf{u}$ for the binary all-one vector.

Definition 2. *An Hadamard full propelinear code is an Hadamard propelinear code C such that for every $a \in C$, $a = \mathbf{e}$, $a = \mathbf{u}$, the permutation π_a has not any fixed coordinate and $\pi_{\mathbf{e}} = \pi_{\mathbf{u}} = I$. From now on, we denote by* HFP*-codes the Hadamard full propelinear codes.*

Ito proved in [6] that there is no Hadamard group realizing a dihedral group neither a cyclic group C_{8n}, and conjectured that for any length we can construct an Hadamard group of type Q, so a dicyclic group or a $C_n \rtimes Q_8$. Ryser [11] conjectured that there is no an Hadamard circulant matrix of length $8n$, which corresponds to a $C_{4n} \times C_2$ propelinear structure. Along the non-abelian groups of order $8n$, we focused our interest in Hadamard codes realizing a $C_n \times Q_8$ group structure.

3 HFP-codes of type C_nQ_8, n odd

Hadamard codes C of type C_nQ_8 were partially studied by Baliga and Horadam in [1]. In the current paper we study the minimum number of generators of C, we compute the rank and the dimension of the kernel and, finally, we give an example of such HFP-codes.

Definition 3. *Let C be an* HFP*-code of length $4n$. We say that C is a code of type C_nQ_8 when C is the direct product $C_n \times Q_8$.*

Lemma 4. *Let $C = \langle a,b,c \rangle$ be an* HFP*-code of type C_nQ_8, with n odd Then $C = \langle d,b \rangle$, where $d = ac$. Further, knowing d we can define b, uniquely (up to complementary).*

Proposition 5. *Let C be an* HFP*-code of type C_nQ_8 and length $4n$. Up to equivalence, we can fix the value of permutations associated to the elements of C. Further, the group generated by the associated permutations to each element of C is*

$$\Pi = C/\langle \mathbf{u} \rangle = C_2^2 \times C_n.$$

Proposition 6. *Let C be an* HFP*-code of type C_nQ_8 with n odd. Then, the rank of C is $r = 4n-1$ and the dimension of the kernel is $k = 1$.*

Now, we present an example of an HFP-code of type C_3Q_8.

Example 7. *Let $Q_8 = \langle a,b \,|\, a^4 = \mathbf{e}, a^2 = b^2 = \mathbf{u}, ab = ba^{-1}\rangle$ and $C_3 = \langle c \,|\, c^3 = \mathbf{e}\rangle$. We can take $a,b,c \in \mathbb{Z}_2^{12}$ with associated permutations as*

$$\begin{array}{ll} a = & (0,1,1,1,0,0,0,1,0,1,0,1),\ \pi_a = (1,4)(2,5)(3,6)(7,10)(8,11)(9,12), \\ b = & (0,1,1,1,0,1,1,0,0,0,1,0),\ \pi_b = (1,7)(2,8)(3,9)(4,10)(5,11)(6,12), \\ c = & (0,0,0,1,0,1,1,0,1,1,0,1),\ \pi_c = (1,5,3)(2,6,4)(7,11,9)(8,12,10). \end{array}$$

Then $C = \langle a,b,c\rangle$ is an HFP*-code of type $C_3 \times Q_8$ and $\Pi = \langle \pi_a, \pi_b, \pi_c\rangle = C_2^2 \times C_3$.*

4 HFP-codes of type C_nQ_8, n even

A standard method to construct Hadamard matrices from other Hadamard matrices is given by the the Kronecker product construction, [9]. Here, we adapt the Kronecker product, that we call *Kronecker sum construction*, and starting from an HFP-code of type C_nQ_8, n odd, we obtain HFP-codes of type $C_{2n}Q_8$ and $C_{4n}Q_8$.

Proposition 8. *Let $A = (a_{ij}), B = (b_{ij})$ be Hadamard matrices corresponding to* HFP*-codes of length m,n, respectively, then the code with corresponding matrix given by (1) is an* HFP*-code.*

$$A \oplus B = \begin{pmatrix} a_{11}+B & a_{12}+B & \cdots & a_{1m}+B \\ a_{21}+B & a_{22}+B & \cdots & a_{2m}+B \\ \vdots & \vdots & \vdots & \vdots \\ a_{2m,1}+B & a_{2m,2}+B & \cdots & a_{2m,m}+B \end{pmatrix} \tag{1}$$

Let $S = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ be the Hadamard matrix of length 2, and C_S the corresponding Hadamard code, which is an HFP-code, $C_S = \{(0,0),(0,1)),(1,0),(1,1)\}$, with associated permutations $\pi_{(0,0)} = \pi_{(1,1)} = I$, $\pi_{(1,0)} = \pi_{(0,1)} = (1,2)$. Consider also, the propelinear Hadamard code C_T of length 4 with associated matrix given by

$$T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

and with associated permutations $\pi_{0000} = I$, $\pi_{1001} = (1234)$, $\pi_{0101} = (13)(24)$, $\pi_{0011} = (1432)$. Note that matrix T is equivalent to the unique circulant matrix of order 4 and code C_T is an HFP-code.

Proposition 9. *Let C be an* HFP*-code of type C_nQ_8 and length $4n$, n odd. Let A be the corresponding Hadamard matrix, so $C = C_A$. Then,*

i) We can define a propelinear structure in $C_{S\oplus A}$ resulting in an HFP*-code of type $C_{2n}Q_8$. The values of the rank and dimension of the kernel for this code are $4n$ and 2, respectively.*

ii) $C_{T\oplus A}$ is an HFP*-code of type $C_{4n}Q_8$. The values of the rank and dimension of the kernel for this code are $4n+1$ and 3, respectively.*

Note that we can not octuplicate C with the same technique as in Proposition 9. To do that we need an Hadamard matrix like T, but of order eight. This goes against the circulant Hadamard conjecture [11]. This consideration leads to consider the existence of HFP-codes of type $C_{2^sn}Q_8$ as an open problem, for $s \geq 3$ and n odd.

5 Acknowledgement

This work has been partially supported by the Spanish MICINN grant TIN2013-40524 and the Catalan AGAUR grant 2014SGR-691.

References

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

[2] J. Basart, L. Huguet and J. Rifà. *On completely regular propelinear codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pp. 341-355, 1989.

[3] A. del Río and J. Rifà. *Families of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-Codes,* IEEE Transactions on Information Theory, **59**, 8, pp. 5140-5151, 2013.

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

[5] N. Ito. *On Hadamard Groups,* Journal of Algebra, **3**, 168, pp. 981-987, 1994.

[6] N. Ito. *On Hadamard groups III*, Kyushu Journal of Mathematics, **51**, 2, pp. 369-379, 1997.

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

[8] P. Montolio, and J. Rifà. *Construction of Hadamard-Codes for Each Allowable Value of the Rank and Dimension of the Kernel.* Information Theory, IEEE Transactions, textbf61.4, pp. 1948-1958, 2015.

[9] K. Phelps, J. Rifà and M.Villanueva. *Hadamard Codes of Length 2^ts (s Odd). Rank and Kernel*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pp. 328-337, 2006.

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

[11] J. H. Ryser. *Combinatorial Mathematics, volume 14 of The Carus Mathematical Monographs*, The Mathematical Association of America, **342** , 1963.