Universitat Autònoma de Barcelona

Departament d'Enginyeria de la Informació i de les Comunicacions

Hadamard full propelinear codes of type Q; rank and kernel [1]

Submitted to Universitat Autònoma de Barcelona in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science

by Emilio J. Suárez Canedo

Cerdanyola del Vallès, January 2018

Advisor: Dr. Josep Rifà i Coma

Professor at Universitat Autònoma de Barcelona

I certify that I have read this thesis entitled "Hadamard full propelinear codes of type Q; rank and kernel." and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

Cerdanyola del Vallès, January 2018

Dr. Josep Rifà i Coma
(Advisor)

Committee:

Dr. Cristina Fernández Córdoba
Dr. José Andrés Armario Sampalo
Dr. Victor Aleksandrovich Zinoviev
Dr. Joaquim Borges Ayats (substitute)
Dr. Faina Ivanovna Solov'eva (substitute)
Dr. Víctor Álvarez Solano (substitute)

Amor est vitae essentia

Abstract

Communication systems need algebraic and combinatorial techniques to recover information in the presence of noise and interference. Hadamard codes constitute an important family of error correcting codes and they have been studied, since 20th century, by authors like Turyn. Although this codes are nonlinear, in general, they possess optimal algebraic and combinatorial properties which allow to encode, transmit and decode a message through a noisy channel. The most powerful mechanisms to construct Hadamard codes with a subjacent group structure are cocyclic Hadamard matrices, relative difference sets, Hadamard groups and Hadamard propelinear codes.

The aim of this thesis is to explore the algebraic and combinatorial properties of a subfamily of the Hadamard propelinear codes which we term Hadamard full propelinear codes. Firstly, we study the connections between Hadamard groups and Hadamard full propelinear codes. Inside the class of Hadamard full propelinear codes we find several group structures with nonsymmetric Hadamard matrices. This is the case of the families with a subjacent dicyclic group Q_{8n} and a $C_n \times Q_8$ group which belong to the class of Ito Hadamard matrices and the classs of Williamson Hadamard matrices, respectively. To help deciding whether two binary codes are nonequivalent we make use of two invariants: the rank and the dimension of the kernel. These parameters provide additional information about the code; for instance, they measure how far is the code from being linear. Specifically, we study the rank and the dimension of the kernel of the aforementioned families of Hadamard full propelinear codes and we also give iterative techniques which allow us to construct Hadamard full propelinear codes of higher orders.

Resumen

Los sistemas de comunicación se nutren de técnicas algebraicas y combinatóricas para recuperar la información en presencia de ruído e interferencias. Los códigos Hadamard constituyen una familia relevante en la teoría de códigos y ellos han sido objeto de estudio desde el siglo XX, por científicos como Turyn. Aunque estos códigos no son lineales en general, ellos poseen propiedades algebraicas y combinatóricas que permiten codificar, transmitir y decodificar un mensaje a través de un canal ruidoso. Los mecanismos más potentes para construír códigos de Hadamard con una estructura de grupo algebraico subyacente son: las matrices de Hadamard cocíclicias, los conjuntos de diferencias relativas, los grupos de Hadamard y los códigos Hadamard properlineales.

El propósito de esta tesis es explorar las propiedades algebraicas y combinatóricas de una subfamilia de los códigos Hadamard properlineales, que denominamos *códigos Hadamard full properlineales*. Nuestro primer objetivo es estudiar las relaciones existentes y las conexiones entre los grupos de Hadamard y los códigos Hadamard full properlineales. Además, en esta nueva subfamilia de códigos encontramos estructuras full properlineales que generan ciertas matrices de Hadamard no simétricas; en concreto, estamos hablando de las familias que tienen asociado el grupo dicíclico Q_{8n} y el grupo $C_n \times Q_8$. Estas matrices de Hadamard son conocidas como las matrices de Williamson y las matrices de Ito. Para ayudar a decidir cuando dos códigos son equivalentes usaremos dos invariantes de los códigos: el rango y la dimensión del núcleo. Estos parámetros nos aportan información sobre los códigos no lineales; a modo de ejemplo, son un indicador para ver cuánto dista un código binario de ser lineal. Concretamente, estudiaremos el rango y la dimensión del kernel de ambas familias y utilizaremos técnicas iteradas que permiten crear códigos Hadamard full properlineales de mayor orden.

Acknowledgements

En primer lugar me gustaría expresar mis más sinceros agradecimientos a mi director Josep Rifà i Coma por todos sus consejos y por su ayuda a lo largo de la realización de esta tesis doctoral.

I would like to express my gratitude to Prof. Leo Storme for his hospitality, unconditional care and for all valuable talks and helpful advices that he gave me during my internship at Ghent University.

Quiero agradecer de manera especial a Edgar Martínez Moro por confiar en mí como persona y estudiante. Por su asesoramiento y por el cariño que me ha dado en todo momento. Agradecer también a Alejandro y a Irene Márquez por su ayuda durante mi estancia en Soria.

Agradecer a mis "hermanos" del dEIC. De hecho, esta etapa no hubiese sido igual sin el resto de los doctorandos del departamento. Roger, Pablo, Roland, Naoufal, mi primera familia en Barcelona. También a Iván Bailera, Carlos, Jorge Bellón, Alex Chao.

A mis amigos sorianos Carlos, Pedro Alarcia, Cristina, "Burri"...

Al genio pucelano y gran matemático Miguel Fernández Duque.

Agradecer a mis amigos gaditanos: Luis Arellano, Esther Chinchilla, Gabriel (grupo fundamental), Ales (sirio), Natalia, Borja, Claudia, Carlos y Paula.

Agradecer o apoio á miña familia do Colexio Fogar de Santa Margarida.

A Santiago Montero, Matías Pérez, Eduardo Dorrego, David Saavedra, Pablo Rey, Quique Vázquez, César de la Fuente, Alejandro Bardanca e Christian Beade. Gracias por apoiarme e facerme a vida máis alegre en todo momento. Gracias tamén a Borja, "Iver", "Pibe", Paula Freixeiro, Lidia Robleda e Belén Otero.

Á xente de Fracasados de Antemano: Brais López, Javier e Bernardo Tejera, Bernardo Pita e Alba Clemente.

A Alba Rodríguez Orrego. No hubiese podido terminar este trabajo sin su amor, su apoyo incondicional y su paciencia. Gracias por tu cariño, comprensión y por irradiar felicidad en esos momentos tan complicados para mí.

A su familia Carlos, Sandra, Adrián, Conchi y Martín por hacerme sentir una persona especial en todo momento.

Á miña familia Marcos, Carlos e Marilé, Ángeles e Carlos, Damián e Iria, Emilia, Carlos e Yolanda, Alberto e Belén, Olalla e Amelia, Marichelo e José, Tania e Belén, Claudia e Ainhoa polo voso apoio e cariño.

Non atopo palabras para agradecer ao meu irmán **Román** e aos meus pais **Olga e Luis** e á miña cuñada Iria. Por todo o amor, apoio e por axudarme a manterme firme nos momentos máis difíciles. Gracias.

Á miña avoa Pilar e á memoria do meu avó Eladio Suárez Pereira polo cariño que me deron.

Contents

Chapter 1

Introduction

Information is known as any message which involves a certain degree of uncertainty. A communication system can be modelled by a scheme consisting of a message source which transmits information to a receiver through a channel. Coding theory is the discipline which studies optimal encoding and decoding schemes for reliable error detection and/or correction of data sent through a noisy transmission channel. A channel is said to be *noisy* if the received information is not necessary equal to the information that was sent. Figure 1.1 provides an idea about the configuration in any general communication channel.

In 1948, Claude Shannon [S48] gave birth to a new subject called "Information Theory", part of which is coding theory. Nowadays, we find that the theory of error correcting codes has been developed for diverse applications, intersecting mathematics and engineering, such as to minimise the noise from compact disc recordings, the transmission across telephone and satellite lines, data storage and information transmission from a distant source.

A finite alphabet coming from a finite field $\mathbb{F}_q$ of q elements, q a prime power, is the common alphabet used in Coding Theory. Codewords are n-tuples over the field $\mathbb{F}_q$ and consider a code as a subset of $\mathbb{F}_q^n$ that contains all codewords. According to scheme 1.1, the message m generated by the source is first encoded. This process results in a codeword x, which is sent over the channel, where noise in the form of vector e distorts it and produces a new message y. The received vector y is then decoded, obtaining an estimate $\hat{m}$ of the message m that hopefully agree. The process of correcting errors and retrieving the message is called decoding. Since there is a one-to-one correspondence between codewords and messages, decoding for us is to obtain an estimate $\hat{y}$ of the received vector y for which $\hat{y} = x$ is expected. The key

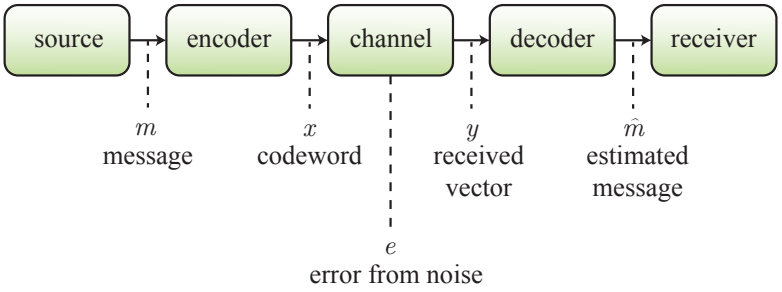

Figure 1.1: Communication channel

of this scheme is the noise, for without it there would be no need for the development of coding theory. The idea of error correcting codes is to add redundant information to enable the detection and correction of errors after transmission.

Hadamard codes are a subfamily of binary codes with good properties. In advance, through the Hadamard codes the **Mariner 9** was a space probe whose mission was to fly by Mars and transmit pictures back to Earth. Hadamard matrices, introduced by J. Hadamard [H83], were used in that mission for two reasons: first, error correction codes based on Hadamard matrices have maximal error correction capability for a given length of codeword and, second, the Hadamard matrices allow computer processing to be accomplished using additions (which are very fast and easy to implement in computer hardware) rather than multiplications (which are far slower). However, these family of codes are not linear codes, in general.

Historically, the most important codes were linear codes but it does not mean that they are the most appropriate. For instance, we find several binary nonlinear codes having twice as many codewords as any linear code with the same length and minimum distance which is, for example, the case of the Preparata and Kerdock codes [N91, HK$^+$94]. In the case of binary nonlinear codes we are interested in those which have an algebraic or combinatorial structure in order to encode, transmit and decode messages efficiently.

Hadamard codes with a subjacent algebraic structure have been deeply studied as well as the links with other topics in algebraic combinatorics

[B62, I94, BH95, F97]. It is well-known that the problem of finding Hadamard codes is equivalent to the problem of finding Hadamard matrices. Nowadays, the most powerful techniques to construct Hadamard codes with a subjacent group structure are cocyles, relative difference sets and Hadamard groups. Horadam and de Launey [HL93a] conjectured that there are cocyclic Hadamard matrices of length $4n$, for every natural n. Throughout computation of cocyclic Hadamard matrices over dihedral groups and over the $\mathbb{Z}_2 \times \mathbb{Z}_n$ (n odd) group, they were able to construct most of Hadamard matrices up to the length 252 [BH95, HL94b, AA$^+$16, AR$^+$15]. Ito [I81] defined the concept of a Hadamard group through relative difference sets and, in 1994 Ito [I94] conjectured that there are Hadamard groups of order $8n$ for every natural n. Schmidt [S99] verifies Ito's conjecture by constructing Hadamard matrices up to the length 184. Flannery et al [F97, LF$^+$00] proved the equivalence between Hadamard groups, cocyclic Hadamard matrices and relative difference sets.

On the other hand, one subfamily of Hadamard codes with a subjacent group structure are Hadamard propelinear codes [RB$^+$89]. Propelinear codes emerged from the idea of dealing with the relationship between completely regular codes and regular graphs and they become more interesting due to their associated group structure. Hadamard propelinear codes are nonlinear in general and, whenever a code is nonlinear, there are two invariants which provide information about the code: the rank and dimension of the kernel. For instance, in [RR13, MR15, BF$^+$14] Hadamard propelinear codes with the translation invariant condition (meaning Hadamard propelinear codes preservering the Hamming metric up to translation) have 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; the rank and the dimension of the kernel are also studied.

In this dissertation we introduce a subclass of the Hadamard propelinear codes that we term *Hadamard full propelinear codes*, or, HFP-codes for short. We study their algebraic and combinatorial properties and we compute the rank and dimension of the kernel for those families of HFP-codes with a subjacent dicyclic group structure Q_{8n} and with a $C_n \times Q_8$ (n odd) group structure, where C_n and Q_8 are the cyclic group of order n and the quaternion group, respectively.

The overview of the dissertation is the following:

- Chapter 2 depicts an introduction to coding theory which helps this dissertation to be as self contained as possible. Firstly, we review basic definitions and results related to binary propelinear codes as well

as the concept of isomorphic and equivalent binary codes. As an exemplification we discuss about $\mathbb{Z}_2$-linear, $\mathbb{Z}_4$-linear, $\mathbb{Z}_2\mathbb{Z}_4$-linear and $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes [BF$^+$14, RR13, MR15]. Furthermore, we review the theory of Hadamard matrices starting from the classical constructions and concluding with cocycles, relative difference sets and Hadamard groups. Finally, we show the main results on the equivalences between Hadamard groups, relative different sets and cocyclic Hadamard matrices [LF$^+$00, I94, F97, H00].

- Chapter 3 aims to introduce HFP-codes. Starting from Hadamard propelinear codes we define the class of HFP-codes and we study their general algebraic and combinatorial properties. At the same time, we define the transpose code of any Hadamard code and we prove that the transpose code C^T of any HFP-code C is HFP; moreover, we show that C and C^T are isomorphic as groups. Furthermore, we study the equivalences between HFP-codes and Hadamard groups, which also allow to connect them with cocyclic Hadamard matrices and relative difference sets. Lastly, we deal with the available groups realising HFP-codes and we show some examples in which we compare the family of HFP-codes with the family of Hadamard translation invariant propelinear codes.

- Chapter 4 is devoted to study the algebraic and combinatorial properties of HFP-codes of type Q (meaning those HFP-codes with a subjacent dicyclic group structure of $8n$ elements) and length $4n$. Ito [I97] studied Hadamard groups of type Q and we focused on classifying them attending to the rank and dimension of the kernel. Furthermore, we deal with the transpose code of a HFP-code of type Q and we also provide an iterative construction that enables to duplicate some HFP-code of type Q preserving its full propelinearity. The transpose HFP-structure and the iterative constructions help to determine HFP-codes of type Q with optimal parameters. Finally, we discuss about the computational results on HFP-codes of type Q.

- Chapter 5 is dedicated to study the algebraic and combinatorial properties of HFP-codes of type CQ (meaning those HFP-codes with a subjacent $C_n \times Q_8$ group structure of $8n$ elements) and length $4n$, n odd. Additionally, based on Kronecker tensor products, we present an equivalent concept for HFP-codes that we call *Kronecker sums*. As last result of this dissertation, using Kronecker sums, we show how to duplicate and quadruplicate HFP-codes of type CQ, preserving its full

propelinear structure, for which we compute the rank and the dimension of the kernel. Finally, we comment on the computational results on HFP-codes of type CQ.

- Chapter 6 presents our conclusions and proposes future lines of research on this topic.

We must mention that part of the research included in this dissertation was presented at several conferences and published in their proceedings [RS14, RS15]:

[RS14] J. Rifà and E. Suárez-Canedo, "About a class of Hadamard propelinear codes" *Electron. Note Discr. Math.*, vol. 46, pp. 289-296, 2014. Proc. of the *IX Jornadas de Matemática Discreta y Algorítmica*, Tarragona, 7-9 July 2014.

[RS15] J. Rifà and E. Suárez-Canedo, "Kronecker sums to construct Hadamard full propelinear codes" *in Proc. of the 21-st Conference on applications of Computer Algebra (ACA15)*, Kalamata, Greece, pp. 135-139, 20-23 July 2015.

The results included in Chapter 3 and in Chapters 4 have already been submitted to a journal [RS17] and they have been accepted:

[RS17] J. Rifà and E. Suárez-Canedo, "Hadamard full propelinear codes of type Q; rank and kernel", *Designs, Codes and Cryptography.* arXiv:1709.02465v2, 2017.

This work was partially supported by the Spanish MINECO under Grant TIN2013-40524-P, and by the Catalan AGAUR under Grant 2014SGR-691.

In the course of this doctoral thesis, I visited the Department of Mathematics at Ghent University in Ghent, Belgium, from 1 September to 30 November 2014 with the objective of learning the main topics of the COST Action IC1104 project titled *Random Network Coding and Designs over* $\mathbb{F}_q$. An introduction on Random Network Coding can be seen in [L82]. Most recent advances in the area of Network Coding are based on codes whose codewords are vector subspaces of a given vector space $\mathbb{F}_q^n$. Hence, random network coding changes the conception of codes based on classical coding theory in which codewords are vectors.

Firstly, we deliberate about new geometric properties for the family of constant dimension codes. *A constant dimension code* is a code fulfilling that

each codeword has the same dimension k. Among constant dimension codes, we focused on those subfamilies in which all codewords intersect pairwise in a subspace of dimension $k-t$. We found an upper bound for which we could find families of nontrivial constant dimension codes ([BE$^+$99, E02, ER14]) of this type, avoiding those which are known as *sunflowers*. Furthermore, we give a characterization of the families of maximal nontrivial constant dimension codes. On the other hand, some iterative constructions were provided on nontrivial constant dimension codes intersecting in a $(k-t)$-dimensional subspace, for all $t \geq 3$. The work done during this stay has been presented at several international conferences [BB$^+$15, BB$^+$16] and has been already submitted to a journal [BS$^+$16], and it has been accepted after minor revisions:

[BB$^+$15] R. D. Barrolleta, M. De Boeck, L. Storme, E. Suárez Canedo, and P. Vandendriessche, "A geometrical bound for the sunflower property," in Proc. of *Design and Application of Random Network Codes (DARNEC '15)*, Istanbul, Turkey, pp. 39, 4–6 November 2015.

[BB$^+$16] R. D. Barrolleta, M. De Boeck, L. Storme, E. Suárez Canedo, and P. Vandendriessche, "On constant distance random network codes," in Proc. of *Network Coding and Designs*, Dubrovnik, Croatia, pp. 48–49, 4–8 April 2016.

[BS$^+$16] R. D. Barrolleta, L. Storme, E. Suárez Canedo, and P. Vandendriessche, "On primitive constant dimension codes and a geometrical sunflower bound," submitted to *Adv. in Math. of Commun.*, 2016.

Chapter 2

Preliminaries

The aim of Chapter 2 is to provide an introduction on some topics of Coding Theory from the different mathematical disciplines which will be helpful along the whole dissertation. We review the state of the art on combinatorial and algebraic Coding Theory and thus, definitions and basic results are gradually presented. Section 2.1 and Section 2.2 consist of a survey on binary linear and nonlinear codes; we introduce propelinear codes and we deal with the classical Hadamard codes; examples of propelinear codes and classical Hadamard constructions are presented. Section 2.3 is dedicated to exhibit relative difference sets and designs as efficent combinatorial methods for constructing Hadamard matrices. Constructions of Hadamard matrices from cocycles are studied in Section 2.4. Section 2.5 is devoted to Hadamard groups; Hadamard groups are presented as a mechanism to construct Hadamard matrices from difference sets. In Section 2.6 we show the results about the equivalences between cocyclic Hadamard matrices, Hadamard groups and relative difference sets.

For an in-depth introduction to binary codes, propelinear codes and Hadamard matrices, presented in Section 2.1 and Section 2.2, the reader is referred to [RB+89, RP97, BM+12, L82, MS77, H98, HP03]; on designs and relative difference sets, concerning to Section 2.3, to [LH93, S03, W88, BJ+99]; on cocyclic Hadamard matrices, of Section 2.4, to [H00, H07, LH93, HL93a] and, on Hadamard groups, concerning to Section 2.5, to [I94, I95a, I97].

2.1 Propelinear codes

Let $\mathbb{Z}$ be the ring of integers, $\mathbb{Z}_s$ the ring of integers modulo s and $\mathbb{F}_q$ the finite field of q elements, with q a power prime. Let $\mathbb{Z}_2^n$ the n-dimensional vector

space over $\mathbb{Z}_2$. Any nonempty subset C of $\mathbb{F}_q^n$ is a *q-ary code* of length n and, in the case of $q = 2$ then $\mathbb{F}_q = \mathbb{Z}_2$ and C is called a *binary code*. Computers store all characters as numbers stored as binary data. Binary code uses the digits 0 and 1 (binary numbers) to represent computer instructions or text. From now on, denote by $\mathbf{0}$ or $\mathbf{e}$ the all-zero vector and denote by $\mathbf{1}$ or $\mathbf{u}$ the all-one vector. The elements of a code are called codewords.

The *Hamming weight* of a vector $v \in \mathbb{Z}_2^n$, $\mathrm{wt}(v)$, is defined as the number of nonzero coordinates in v, while the *Hamming distance* $d(u, v)$ between two vectors $u, v \in \mathbb{Z}_2^n$, is the number of coordinates in which u and v differ. The *minimum Hamming weight* $\mathrm{wt}(C)$, of a binary code C, is the minimum value of $\mathrm{wt}(v)$ for all $v \in C \backslash \{\mathbf{0}\}$. The *minimum Hamming distance* $d = d(C)$ of a binary code C, is the minimum value of $d(u, v)$, for all $u, v \in C$, $u \neq v$. The minimum Hamming distance d determines the number of errors that the code can correct. The code C is said to be a *t-error-correcting code*, where $t = \lfloor (d-1)/2 \rfloor$ is the *error-correcting capability*. Hence, the higher the minimum distance, the more errors the code can correct.

A binary code C of length n is said to be *a linear code* if C is a linear subspace of $\mathbb{Z}_2^n$. When C is a linear code, then it is known that $d(C) = \mathrm{wt}(C)$.

A binary (n, M, d)-code is a code with length n, M codewords and minimum distance d. A *coset* of a binary code C by $v \in \mathbb{Z}_2^n$ is the set $v + C = \{v + u | u \in C\}$. The covering radius ρ of a binary code C is the smallest integer such that $\mathbb{Z}_2^n$ is the union of the spheres of radius ρ centered at the codewords of C. When C is linear the covering radius ρ coincides with the weight of the coset of largest weight. A binary code C satisfying that for some integer t, $t \geq 0$, every $v \in \mathbb{Z}_2^n$ is within distance t from exactly one codeword of C, is called a t-perfect code. Any binary $(2^m - 1, 2^{2^m - m - 1}, 3)$-code, for a given integer m, is called binary 1-perfect code. Moreover, if perfect codes are linear then they are termed *Hamming codes*.

A classical form to describe a linear code is through generator and parity check matrices. *A generator matrix* of a linear code C is a matrix G whose rows form a basis of C. To define the parity check matrix is necessary to define, firstly, the inner product. The *inner product* of two vectors $u, v \in \mathbb{Z}_2^n$ is the bilinear form defined as

$$\langle u, v \rangle = \sum_{i=1}^{n} u_i v_i \in \mathbb{Z}_2.$$

Two vectors u and v are said to be *orthogonal* if $\langle u, v \rangle = 0$. The set of vectors which are orthogonal to all codewords of C, denoted by $C^\perp$, is

$$C^\perp = \{x \in \mathbb{Z}_2^n : \langle x, u \rangle = 0, \text{ for all } u \in C\}.$$

If C is a binary linear code then $C^\perp$ is called the *dual code* of C and, if $C = C^\perp$ then C is called *self-dual*. Otherwise, $C^\perp$ is said to be *orthogonal* to C. Any binary code C with $C^\perp \subset C$ is called *self-orthogonal*.

A *parity check matrix* H, for a binary linear code C, is a generator matrix of $C^\perp$. Parity check matrices are used to determine whether a vector belongs to the code; hence, $v \in C$ if and only if $Hv^T = 0$, where $(\cdot)^T$ denotes the transpose. The expression Hv^T computes the *syndrome* of a vector $v \in \mathbb{Z}_2^n$, and the codewords are characterized by having syndrome $\mathbf{0}$. All vectors lying in the same coset $v+C$ have the same syndrome. The minimum weight vector of a coset is said to be the *coset leader*.

Example 1. *The* $(7, 16, 3)$ *Hamming code has the following generator matrix and parity check matrix, respectively*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The dual code of a Hamming code of length 2^{m-1} *is called binary simplex code of length* 2^{m-1} *and is denoted by* S_m. *The matrix* H *is the generator matrix of the binary simplex code of length* 7.

It is possible to create larger codes by adding a coordinate. One and the most common way to do it consists of choosing the appropriate extension, it means that it must satisfy that the sum of all coordinates is 0. Let C be a binary linear code of length n and minimum distance d. The *extended code* $\widehat{C}$, is defined as

$$\widehat{C} = \{(x_1, \ldots, x_{n+1}) \in \mathbb{Z}_2^{n+1} \ : \ (x_2, \ldots, x_{n+1}) \in C \text{ with } \sum_{i=1}^{n+1} x_i = 0\}.$$

The extended code $\widehat{C}$ is also linear; furthermore, it is of length $n+1$ and minimum distance $\widehat{d}$, where $\widehat{d} = d$ or $d+1$. Let G and H be generator and parity check matrices for C, respectively. A generator matrix $\widehat{G}$ for $\widehat{C}$ can be obtained from G by adding an extra column to G so that the sum of the coordinates of each row of $\widehat{G}$ is 0. Moreover, a parity check matrix $\widehat{H}$ for $\widehat{C}$ is

$$\widehat{H} = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{0} & H \end{pmatrix}. \tag{2.1}$$

For example, extending a binary 1-perfect code of length $2^m - 1$ by (2.1), an 1-perfect code of length 2^m and minimum distance 4 is obtained.

Now we establish a criterion to decide whether two binary codes are equal. In the case of binary linear codes they are said to be equivalent if there is an isomorphism of vector spaces. However, the concept of the weight is lost, meaning, codewords of a fixed weight are sent to codewords of different weight by the isomorphism of vector spaces. Since we are interested in the equivalences preserving Hamming distances through isomorphism then the concepts of *isomorphism* (or, *permutation equivalent*) and *equivalence* appears as follows. Firstly, denote by $\mathcal{S}_n$ the symmetric group of permutations of the set $\{1, 2, \ldots, n\}$. For any $\pi \in \mathcal{S}_n$ and $v \in \mathbb{F}_2^n$, the image $\pi(v)$ of the vector $v = (v_1, v_2, \ldots, v_n)$ via permutation π is denoted by $(v_{\pi^{-1}(1)}, v_{\pi^{-1}(2)}, \ldots, v_{\pi^{-1}(n)})$. Two binary codes C_1 and C_2, of the same length n, are said to be *isomorphic* (or *permutation equivalent*) if one can be obtained from the other by permuting the coordinates. The set of all permutations keeping the code invariant is called the *automorphism group* of C, $\mathrm{Aut}\,(C) = \{\pi \in \mathcal{S}_n : \pi(C) = C\}$. Two binary codes C_1 and C_2, of the same length n, are said to be *equivalent* if there is a permutation $\sigma \in \mathcal{S}_n$ and a vector $v \in \mathbb{Z}_2^n$ such that $C_2 = \{v + \sigma(c) : c \in C_1\}$. We denote by $\mathrm{Iso}\,(C)$ the set of all isometries in $\mathbb{Z}_2^n$ which keeps the code C set-wise invariant.

The weight distribution of a binary code allows to determine the probability of a receiver vector to be decoded. Moreover, this distribution describes the codes through the Hamming weight of its codewords. The *weight distribution* of binary code is a set $\{A_0, \ldots, A_n\}$ where A_i is the number of codeword of Hamming weight i.

Definition 2. *[MS77] The weight enumerator of C is given by the homogeneous polynomial $W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$.*

Given a binary linear code MacWilliams [MS77] was able to write the enumerator polynomial of the corresponding binary dual linear code.

Theorem 3. *[MS77, MacWilliams identity, Ch.5] Let C be a linear code and $W_C(x, y)$ its weight enumerator polynomial. Then the enumerator polynomial of C^T is*

$$W_C(x, y) = \frac{1}{|C|} W_C(x + y, x - y)$$

Dealing with binary nonlinear codes requires accuracy techniques since they lose the algebraic structure and, as a consequence, they can rarely be

represented by generator matrices or/and parity check matrices. For instance, the dual concept on the nonlinear case is understood as follows; any two binary nonlinear codes satisfying the MacWilliams identity are said to be *formally dual* codes. In order to deal with binary nonlinear codes we make use of two structural invariants: the rank and the dimension of the kernel.

Definition 4. *The rank $r = r(C)$ of a binary code C is the dimension of the span $\langle C \rangle$ of C.*

Definition 5. *The kernel $K(C)$ of a binary code C, is the set of vectors that leave C invariant under translation, $K(C) = \{x \in \mathbb{Z}_2^n : x + C = C\}$. We denote by k the dimension of the kernel.*

If C contains the $\mathbf{0}$ vector, then $K(C)$ is a linear subspace of $\mathbb{Z}_2^n$. Furthermore, it is well-known that any binary linear code C satisfies $r = k$. In case of nonlinear codes, the rank and the dimension of the kernel measure how far is the code from being linear. Ranks and kernels are also used to determine whether two binary codes are not equivalent.

Coding theorists are interested on finding families of binary nonlinear codes with algebraic and combinatorial structures enabling information to be coded, transmitted, and decoded through a noisy channel.

One interesting family of binary codes with a subjacent group structure is termed *propelinear codes*. The starting point on propelinear codes was the study about the relationship of completely regular codes and distance regular graphs [BC$^+$89]. Further, completely regular codes in Hamming metric have been introduced in [D73a] and they have been of interest to coding theorists and also to graph theorists [SZ$^+$71, GT, N92]. These substructures were defined as a generalisation of perfect codes [D73b], and they include many codes having small minimum distance which were fundamental on the study of distance-regular graphs [RB$^+$89]. For instance, Hamming, Golay and some Hadamard codes belong to this family. In addition, their structures allow to establish relations between completely regular codes and other combinatorial structures like the distance regular graph [BC$^+$89]. From the distance regular graph theory in [BM$^+$12] is introduced the class of propelinear codes.

Definition 6. *[RB$^+$89] A binary code C of length n has a* ***propelinear*** *structure if for each codeword $x \in C$ there exists a subset $\Pi = \{\pi_x : x \in C\} \subset \mathcal{S}_n$ satisfying the following conditions:*

1. *For all $x, y \in C$*

$$x + \pi_x(y) \in C, \tag{2.2}$$

2. For all $x, y \in C$,

$$\pi_x \pi_y = \pi_z, \text{ where } \quad z = x + \pi_x(y). \tag{2.3}$$

For all $x \in C$ and for all $y \in \mathbb{Z}_2^n$, denote by $\cdot$ the binary operation such that $x \cdot y = x + \pi_x(y)$. Assume that the zero-vector $\mathbf{e}$ is always a codeword and $\pi_{\mathbf{e}}$ is the identity permutation. In [RB+89] is proved that $x^{-1} = \pi_x^{-1}(x)$, for all $x \in C$, and that $\mathbf{e}$ is the identity element in C. This fact implies that $(C, \cdot)$ is a group and that Π is a subgroup of $\mathcal{S}_n$. In [RR13] it was proved that propelinear codes preserve the Hamming distance by the left multiplication. This means,

$$d(u, v) = d(x \cdot u, x \cdot v), \quad \forall x \in C \text{ and } \forall u, v \in \mathbb{Z}_2^n.$$

Not all propelinear codes preserve the right multiplication, but there is a subfamily of propelinear codes satisfying this condition. They are termed *translation invariant propelinear codes.*

Definition 7. *[RP97] Let $(C, \cdot)$ be a propelinear code. The code C is said to be translation invariant if for all $u, v \in C$ and, for all $x \in \mathbb{Z}_2^n$*

$$d(u, v) = d(u \cdot x, v \cdot x).$$

It is not easy, in general, to decide whether a given binary code is propelinear or not. There is a characterization to decide whether any binary code can be provided with a propelinear structure.

Proposition 8. *[PR02] Let C be a binary code. Then C is a propelinear code if and only if* $\mathrm{Iso}(C)$ *contains a regular subgroup acting transitively on C.*

For instance, a binary 1-perfect code is propelinear if and only if the minimal distance graph (the graph with vertices the codewords and edges given by vertices at distance three) is a Cayley graph. On the other hand, a close related family to propelinear codes is the family of *transitive codes.*

Definition 9. *[BM+12] A binary code C is said to be transitive if for every $x \in C$ there exists a permutation π_x such that $x + \pi_x(C) = C$.*

In other words, a binary code C is said to be transitive if $\mathrm{Iso}\,(C)$ acts transitively in C. Let Φ be the set $\{\phi_x = (x, \pi) : x \in C\}$ that defines the operation $x \star y = x + \pi_x(y) \in C$, for all $x, y \in C$. The main difference between

transitive and propelinear codes is that Φ is not a group in general; more concretely, they may not satisfy the associative property (2.3). In [BM+12] it was proved that they are equivalent if and only if the set Φ is a subgroup of $\mathrm{Iso}\,(C)$.

The class of translation invariant propelinear codes contains families of binary codes with optimal parameters. As an example, in the family of translation invariant propelinear codes we find the families of $\mathbb{Z}_2\mathbb{Z}_4$-linear, $\mathbb{Z}_4$-linear and the $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes.

2.1.1 $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

The additive $\mathbb{Z}_2\mathbb{Z}_4$-code spring as a generalisation of linear codes over a finite field alphabet in a Hamming scheme. Delsarte [D73a] defined these codes as a subgroups of the underlying abelian group in a translation association scheme. In the special case of the binary Hamming scheme, the underlying abelian group is of size 2^n. In [RP97] it can be seen that the unique structures for abelian groups in any Hamming translation association scheme are of the form $\mathbb{Z}_2^\alpha + \mathbb{Z}_4^\beta$, with $\alpha + 2\beta = n$. A subgroup $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is called $\mathbb{Z}_2\mathbb{Z}_4$-*additive code*.

The *Lee weight function* over the elements of $\mathbb{Z}_4$ is defined as the shortest path on the cycle from an arbitrary element to 0. Hence, the elements $0, 1, 2, 3$ in $\mathbb{Z}_4$ have the following Lee weights: $\mathrm{wt}_L(0) = 0, \mathrm{wt}_L(1) = \mathrm{wt}_L(3) = 1$ and $\mathrm{wt}_L(2) = 2$. Furthermore, the Lee weight of any element in $\mathbb{Z}_4^n$ is the sum of the Lee weights in each coordinate meanwhile the *Lee distance* of a pair of vectors $u, v \in \mathbb{Z}_4^n$ is defined as $d_L(u, v) = \mathrm{wt}_L(u + v)$.

The *Gray map* over $\mathbb{Z}_4$ is a map $\Phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ where $\Phi(0) = 00, \Phi(1) = 01, \Phi(2) = 11, \Phi(3) = 10$ and, note that Φ can be extended coordinate-wise to $\mathbb{Z}_4^n$. Hence, some binary codes can be constructed from the quaternary coordinates. The Gray map is nonlinear but it is an isometry which transforms Lee distances in $\mathbb{Z}_4^n$ into Hamming distances in $\mathbb{Z}_2^{2n}$.

Any binary code C is called a $\mathbb{Z}_2\mathbb{Z}_4$-linear code if C is the image $\Phi(\mathcal{C})$ through the Gray map, where $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. The extended Gray map is the map which acts over the binary coordinates as the identity, concatenated with the Gray map acting over the quaternary coordinates. The generator and parity check matrices, the dual codes and the automorphism group of a $\mathbb{Z}_2\mathbb{Z}_4$-additive codes can be found in [BF+10, BF+14, KV15]; the rank and the dimension of the kernel of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes can be found in [FP+10].

$\mathbb{Z}_4$-linear codes

A code $\mathcal{C}$ is said to be a *quaternary code* of length n if $\mathcal{C}$ is a nonempty set of $\mathbb{Z}_4^n$, while $\mathcal{C}$ is said to be quaternary linear if $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$. If $\mathcal{C}$ is a quaternary linear code then $C = \Phi(\mathcal{C})$ is said to be $\mathbb{Z}_4$-*linear code*. The usual inner product for any two words $u, v \in \mathbb{Z}_4^n$ is $\langle u, v\rangle = u \cdot I_n \cdot v^T$, where I_n is the identity matrix of length n and v^T is the transpose vector of v. The *quaternary dual code* of $\mathcal{C}$ is defined as $\mathcal{C}^\perp = \{u \in \mathbb{Z}_4^n : \langle u, v\rangle = 0, v \in \mathcal{C}\}$ while $C_\perp = \Phi(\mathcal{C}^\perp)$ is called the $\mathbb{Z}_4$-dual code of C. In [N91, HK$^+$94, BP$^+$03b] it was proved that there exists an important family of $\mathbb{Z}_4$-linear codes with better parameters that any linear code of the same length. Two of the most important families of $\mathbb{Z}_4$-linear codes are the *Preparata and Kerdock* codes, [K72]. Preparata and Kerdock codes were proved to be formally dual to each other; their parameters and some constructions are studied in [BP$^+$03b, Z00]. Other families of $\mathbb{Z}_4$-linear codes can be found in [K01, FP$^+$08]. In [KW$^+$16, KZ13] a list of optimal $\mathbb{Z}_4$-linear codes with their associated parameters can be found. Furhtermore, in [BP$^+$03a] it is given a classification attending to the rank and the dimension of the kernel of the extended 1-perfect $\mathbb{Z}_4$-linear codes, that consists of a subfamily of the $\mathbb{Z}_4$-linear codes, termed $\mathbb{Z}_4$-linear Hadamard codes. Note that the family of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes generalised the $\mathbb{Z}_4$-linear and binary linear codes by considering $\alpha = 0$ or $\beta = 0$, respectively.

Every $\mathbb{Z}_4$-linear code C has a propelinear structure. If $0, 1, 2, 3$ are the elements in $\mathbb{Z}_4$, we can make the following assignation, $\pi_1 = \pi_2 = (1, 2)$ and $\pi_2 = \pi_0 = Id$. In $\mathbb{Z}_4$ we have that $1 + 3 = 0$ and in its binary propelinear representation it would be $1 \cdot 3 = (0, 1) + \pi_1(1, 0) = (0, 0)$. As well as the Gray map is extended coordinate wise to $\mathbb{Z}_4^n$ the propelinear structure can be extended to $\mathbb{Z}_2^{2n}$ by concatenating the associated permutations in each quaternary coordinate.

Remark 10. *Furthermore, every codeword in a $\mathbb{Z}_2\mathbb{Z}_4$-linear code have associated the identity permutation on the binary coordinates and the concatenation of the permutations assigned to each quaternary coordinate.*

2.1.2 $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes

Let Q_8 be the quaternion group of eight elements, presented by $Q_8 = \langle a, b : a^4 = e, a^2 = b^2, ab = ba^{-1}\rangle$, where e is the identity element.

Definition 11. *[RR13] A quaternionic code is defined as any subgroup of Q_8^n.*

Likewise in $\mathbb{Z}_4$-linear and $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, it is defined a suitable Gray map for the quaternion group. Quaternionic codes can be seen as binary codes through the Gray map $\varphi : Q_8 \to \mathbb{Z}_2^4$, defined by

$$\begin{array}{ll} \varphi(e) = (0,0,0,0), & \varphi(b) = (0,1,1,0), \\ \varphi(a) = (0,1,0,1), & \varphi(ab) = (1,1,0,0), \\ \varphi(a^2) = (1,1,1,1), & \varphi(a^2b) = (1,0,0,1), \\ \varphi(a^3) = (1,0,1,0), & \varphi(a^3b) = (0,0,1,1). \end{array}$$

The map φ can be extended coordinate-wise to Q_8^n. If $\mathcal{C}$ is a quaternionic code, then we will say that $C = \varphi(\mathcal{C})$ is a Q_8-code of binary length $4n$. In [RR13] it is proved a quaternionic code can be provided with a propelinear structure by considering $\pi_a = (1,2)(3,4)$ and $\pi_b = (1,3)(2,4)$.

Denote by Φ the extended Gray map formed by the concatenation of the Gray maps on the binary, quaternary and quaternionic coordinates. Furthermore, if $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \times Q_8^\gamma$ then $C = \Phi(\mathcal{C})$ is called a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code. The propelinear structure of a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code is reached by concatenating the permutations associated to the binary, quaternary and quaternionic coordinates. Note that this family of codes generalises $\mathbb{Z}_2\mathbb{Z}_4$-linear codes by considering $\gamma = 0$, and therefore, the $\mathbb{Z}_4$-linear and the binary linear codes. The following result shows a characterization which decides whether a propelinear code is translation invariant.

Proposition 12. *[RP97] Let C be a binary propelinear code. Then C is a translation invariant code if and only if C is a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes.*

In [RR13] it is proved that the family of $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes enlarges the family of those $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. Although Hadamard codes are introduced in the following section, it is worth mentioning that Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes constitutes an important subfamily of the $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. In [RR13] Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes are described attending to five different shapes for which bounds on the rank and the dimension of the kernel are established. Furthermore, in [MR15] Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes are completely classified attending to the values of the rank and the dimension of the kernel.

2.2 Binary Hadamard matrices

The study of Hadamard matrices becomes an important target on several applied mathematical disciplines since the early 20th century. Through

Hadamard matrices, Hadamard codes come to life. These codes have optimal parameters in order to modulate and transmit information through a noisy channel. To emphasize their relevance, they were used in early satellite transmissions in the 1972 Mariner mission to Mars. Modern CDMA cellphones use Hadamard matrices (Walsh covers) to modulate transmission on the uplink and minimise interference with other transmissions to the base station. The Walsh-Hadamard Transform is in common use as a fast discrete transform. New applications are pattern recognition, neuroscience, optical communication, cryptography and stenography[H07].

Definition 13. *[H83] A Hadamard matrix H of order n is a matrix of size $n \times n$ with entries $\{\pm 1\}$, such that $HH^T = nI$.*

In other words, any Hadamard matrix is a square matrix of order n such any two different rows or columns agree in precisely $\frac{n}{2}$ entries. It is well known that if a Hadamard matrix exists then n is $1, 2$ or multiple of 4, [MS77, AK92]. The smallest trivial examples of Hadamard matrices

$$H_1 = \begin{pmatrix} 1 \end{pmatrix}, \qquad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$$

At the end of the 19th century, Jacques Hadamard [H83] enunciated several problems concerning Hadamard matrices, such as the general constructions for Hadamard matrices. Several decades later, Paley studied some of the Hadamard problems and conjectured the next statement known as the "Hadamard conjecture".

Conjecture 1. *[P33, Hadamard's conjecture] There are Hadamard matrices of length $4n$, for every natural number n.*

It is said that two Hadamard matrices H_1 and H_2 are *equivalent* if one can be obtained from the other by performing a finite sequence of:

1. permutations of the rows or/and columns,

2. multiplications by -1 rows or/and columns.

Optimal advances were reached since 1970 and lots of inequivalent Hadamard matrices have been constructed; a complete list of nonequivalent Hadamard matrices for small orders can be seen in [GK05].

From the operations of equivalence, the first row and column of H can be changed into $+1$'s and then we say that H is *normalized*. Any Hadamard matrix H is a *Hadamard binary matrix* if $+1$'s are replaced by 0's and -1's by 1's.

A Hadamard code C consists of the rows of a binary Hadamard matrix H and their complementaries. In other words, a binary Hadamard code is a binary $(4n, 8n, 2n)$-code. Hadamard codes are not linear in general, but it is well-known that there is a unique binary linear Hadamard code of length $n = 2^m$, for any $m \geq 2$. Further, this code is the dual of the extended Hamming code of length 2^m [MS77, Chapter 2].

Example 14. *[MS77] The binary linear Hadamard code of length* 16 *with generator matrix*

$$G_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

is constructed as in (2.1). Hence, G_4 *is the generator matrix for the simplex code* S_4*, of length* 15.

Several constructions of binary Hadamard codes attending to the values of the rank and dimension of the kernel can be found in [PR+05a, PR+06c].

Remark 15. *Further than the lineal Hamming code, the dual of the* $\mathbb{Z}_4$*-Hamming code and the* $\mathbb{Z}_2\mathbb{Z}_4$*-Hamming code are the Hadamard* $\mathbb{Z}_4$*-code and Hadamard* $\mathbb{Z}_2\mathbb{Z}_4$*-code, respectively.*

The recent advances on combinatorics, complex analysis and algebra made easier to determine new tools for constructing Hadamard matrices of higher orders. In order to develop a broad perspective on Hadamard matrices it is convenient to present an overview on classical and modern constructions.

Classical and modern constructions

Since the beginning of the 20th century, various mathematicians have been trying to give a solution to the *Hadamard's conjecture*. While a general proof for the Hadamard conjecture seems unreachable, some mathematicians deal with methods for constructing Hadamard matrices of high orders.

2.2.1 Hadamard matrices of Sylvester Type

One of the forefathers on Hadamard matrices was James Joseph Sylvester, [S67]. Around 1860, Sylvester had realised that given a Hadamard matrix H, then the expanded matrix

$$\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

is a Hadamard matrix. Let us go over the general case. Let A and B, respectively, be $m \times n$ and $p \times q$ matrices with $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ and $B = (b_{ij})_{1 \leq i \leq p, 1 \leq j \leq q}$.

Definition 16. *The Kronecker product (or tensor product) $A \otimes B$ of two matrices A and B is the resultant matrix obtained by replacing each $a_{i,j}$ in A by $a_{i,j}B$.*

Now, let H_n and H_m be Hadamard matrices of orders n and m, respectively. Then the Kronecker product $H_n \otimes H_m$ is a Hadamard matrix of order nm. Hence, any Hadamard matrix H is said to be of *Sylvester type*, if H consists of n iterated tensor products of the matrix $S = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

2.2.2 Hadamard matrices of Paley type

Paley [P33] showed the existence of a new family of Hadamard matrices for which he gave several constructions. It is necessary to introduce the quadratic residues over finite fields $\mathbb{F}_q$ of q elements, with q a prime power, to understand the Hadamard matrices of Paley type. For more details, the reader is referred to [RM+99].

An element $g_i \in \mathbb{F}_q$ is a *quadratic residue* if $g_i = g_j^2$ has a solution in $\mathbb{F}_q$. The *Legendre character* is the map

$$\chi : \mathbb{F}_q \to \{-1, 0, 1\},$$

where $\chi(0) = 0$, $\chi(x) = -1$ if x is a nonsquare, and $\chi = 1$ otherwise.

For any $g_i, g_j \in \mathbb{F}_q$ we denote by Q the *Jacobsthal matrix* defined by χ, $Q_{ij} = \chi(g_i - g_j)$, $0 \leq i, j < q$. When $q \equiv 3 \pmod 4$, since $Q_{ij} = \chi(g_i - g_j) = \chi(-1)\chi(g_j - g_i) = -Q_{ji}$, then the matrix Q is *skew-symmetric* ($-Q = Q^T$). Furthermore, if $q \equiv 1 \pmod 4$ then -1 is a square in $\mathbb{F}_q$ and then Q is symmetric ($Q = Q^T$).

Definition 17. *[H00] Let I_{q+1} be the identity matrix of order $q+1$ and let Q be the matrix defined by the Legendre character over $\mathbb{F}_q$, $\chi(g_i - g_j)_{0\leq i,j<q}$. Consider* $S = \begin{pmatrix} 0 & \mathbf{1} \\ \mathbf{1}^T & Q \end{pmatrix}_{(q+1)\times(q+1)}$

1. *If $q \equiv 3 \pmod 4$ then the $\mathcal{P}_1$ is said to be of* type Paley I, *where*

$$\mathcal{P}_1 = \begin{pmatrix} 1 & -\mathbf{1} \\ \mathbf{1}^T & Q + I_q \end{pmatrix}$$

2. *If $q \equiv 1 \pmod 4$ then the matrix $\mathcal{P}_2$ is said to be of* type Paley II, *where*

$$\mathcal{P}_2 = \begin{pmatrix} S + I_{q+1} & S - I_{q+1} \\ S - I_{q+1} & -S - I_{q+1} \end{pmatrix}$$

The matrices $\mathcal{P}_1$ and $\mathcal{P}_2$ are Hadamard matrices [MS77, Chapter2, Lemma 7][H07]. Combining these constructions with the Sylvester expanded matrices yields a large number of Hadamard matrices. To illustrate the above theory, we show an example of a Paley type I Hadamard matrix.

Example 18. *[H00] Let $\mathcal{P}_1$ be the matrix defined from the set $\{1, 2, 4\}$ of quadratic residues* $\pmod 7$. *Then,*

$$\mathcal{P}_1 = \begin{pmatrix} 1 & -\mathbf{1} \\ \mathbf{1}^T & Q \end{pmatrix} = \begin{pmatrix} 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{pmatrix}.$$

Paley [P33] provided the following results on the existence of Hadamard matrices.

Theorem 19. *[P33]*

1. *Let n be divisible by 4, with $n = 2^k(p^h+1)$, where p is an odd prime and natural numbers k and h. Then we can construct a Hadamard matrix of order n.*

2. *Let n be divisible by 4, with $n = 2^k p(p+1)$, where $p \equiv 3 \pmod 4$, p an odd prime and natural number k. Then we can construct a Hadamard matrix of order n.*

These methods enabled Paley to find Hadamard matrices of small orders. However, there exists some orders n, $n \leq 200$, for which Paley constructions could not provide Hadamard matrices; in particular, these gaps are $n \in \{92, 116, 156, 172, 184, 188\}$.

2.2.3 Williamson Matrices

Williamson [W84] gave another method to construct Hadamard matrices. This method generalises the Paley type I construction and complete some of the aforementioned gaps, like $n = 172$. Afterwards, more developed techniques allow researchers to compute Williamson matrices more efficiently but, even nowadays, it is still a hard problem. Likewise in Paley constructions, Williamson matrices have a specific internal structure; this structure has different block circulant matrices satisfying the following conditions.

Definition 20. *[R52] Any square matrix M of length n is said to be a circulant matrix if M can be written as,*

$$M = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_n & v_1 & \dots & v_{n-1} \\ \vdots & \vdots & & \vdots \\ v_2 & v_3 & \dots & v_1 \end{pmatrix}$$

Definition 21. *[W84] A Hadamard matrix H is of* Williamson type *if H can be written up to equivalence as*

$$H = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

where A, B, C, D are circulant and symmetric matrices such that

$$AA^T + BB^T + CC^T + DD^T = 4nI \tag{2.4}$$

The most difficult step on the construction of Williamson matrices, relies in finding those circulant matrices satisfying condition (2.4).

Example 22. *Consider the matrices*

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, B = C = D = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}.$$

Since A, B are symmetric matrices then it is clear that $A^2 + B^2 + C^2 + D^2 = 12 \cdot I_{12}$.

Thus, combining appropriate circulant matrices, the Williamson method produces Hadamard matrices of higher orders. One can think that if there were additional Hadamard circulant matrices, then the Williamson construction would produce new Hadamard matrices. Nevertheless, this problem is one of the classical conjectures in the area of Hadamard matrices.

Conjecture 2. *[R63] There is no Hadamard circulant matrix of order n, unless $n = 1$ and $n = 4$.*

Example 23. *The unique nontrivial circulant Hadamard matrix is*

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix},$$

Williamson matrices are introduced in [W84] quite early in the development of the theory of orthogonal matrices; most of Williamson matrices are those of order $(q+1)/2$, where $q \equiv 1 \pmod 4$ is a prime power, [W84].

The most significant advancements on the Williamson method were principally conducted by Baumert, Golomb and Hall (1962), [BG+62] which constructed Hadamard matrices of order 92, 116 and 156 and, from Sylvester method, the Hadamard matrix of order 184, [BG+65, B66]. Around 1970 the main contributions were essentially done by Turyn [T69, T72]; Turyn proved that a matrix of Paley Type II is equivalent to a Williamson Hadamard matrix with symmetric circulant components. Concurrently in 1970, Cooper and J. Wallis were be able to construct Hadamard matrices of new orders, such as the case of a Hadamard matrix of order 836 [CW72].

2.2.4 Ito Hadamard matrices

Alternatively to the Turyn's construction, Goethal and Seidel [GS67, GS70] provided Hadamard matrices related to the Williamson type although the

conditions that they require for the circulant matrices are less restrictive than on the Williamson case. Around 1990, Ito [I94] proposed a general construction for Hadamard matrices employing circulant matrices which is not as restrictive as Williamson's but more restrictive than Goethals and Seidel's matrices. In [I81] these matrices are termed *Hadamard matrices of type Q*.

Definition 24. *[I81] A matrix H is said to be of type Q if it can be written as*

$$H = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C^T & D^T & A^T & -B^T \\ -D^T & -C^T & B^T & A^T \end{pmatrix} \tag{2.5}$$

where A, B, C, D and are circulant matrices satisfying condition (2.4) and

$$AB^T + CD^T = BA^T + DC^T$$

Schmidt [S99] realised that Williamson type matrices are included in the Hadamard matrices of type Q, and this fact brought Williamson matrices back to light. Ito designed an algebraic structure for these matrices that he called *Hadamard groups* but, it will not be until Section 2.5 where we give an explanation on Hadamard groups.

2.2.5 Generalised quaternion Hadamard matrices

Yamada [Y91] generalised Ito Hadamard matrices by introducing $2^t \times 2^t$ block back negacyclic (2.6) matrices (t possitive integer) with circulant components of order n, instead of 2×2 back negacyclic matrices (2.7)). These new matrices are termed *generalised quaternion Hadamard matrices.*

Definition 25. *[Y91] A matrix M is said to be back negacyclic if M can be written as*

$$M = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ -v_n & v_1 & \cdots & v_{n-1} \\ -v_{n-1} & -v_n & \cdots & v_{n-2} \\ \vdots & \vdots & & \vdots \\ -v_2 & -v_3 & \cdots & v_1 \end{pmatrix}, \tag{2.6}$$

Definition 26. *[Y91] A Hadamard matrix H of order $4nN$ is said to be a generalised quaternion matrix of order $4nN$ if H can be written as*

$$H = \begin{pmatrix} \mathcal{A} & \mathcal{B} \\ -\mathcal{B}^T & \mathcal{A}^T \end{pmatrix}, \tag{2.7}$$

where $\mathcal{A}$ and $\mathcal{B}$ are the following back negacyclic matrices

$$\mathcal{A} = \begin{pmatrix} A_1 & A_2 & \cdots & A_{2N} \\ -A_{2N} & A_1 & \cdots & A_{2N-1} \\ -A_{2N-1} & -A_n & \cdots & A_{2N-2} \\ \vdots & \vdots & & \vdots \\ -A_2 & -A_3 & \cdots & A_1 \end{pmatrix}, \mathcal{B} = \begin{pmatrix} B_1 & B_2 & \cdots & B_{2N} \\ -B_{2N} & B_1 & \cdots & B_{2N-1} \\ -B_{2N-1} & -B_n & \cdots & B_{2N-2} \\ \vdots & \vdots & & \vdots \\ -B_2 & -B_3 & \cdots & B_1 \end{pmatrix},$$

and, where A_i and B_i are $n \times n$ circulant matrices, $i \in \{1, 2, \ldots, 2N\}$.

2.3 Relative difference sets

Design theory evolved in the last century as an important mathematical discipline with diverse applications in computer sciences. Design theory produces useful combinatorial devices for constructing Hadamard matrices. It was realised very early that some Hadamard matrices are equivalent to certain block designs; as an example, Paley type I Hadamard matrices can be constructed directly from square block designs [BJ+99]. Hence, it is reasonable and convenient to introduce the available combinatorial structures that are used to construct Hadamard matrices. The following definitions are fairly standard and, for more information, the reader is referred to [AK92, S03, RM+99, W88, BJ+99].

Definition 27. *[S03] Let v, k, λ and t be positive integers such that $v > k \geq t$. A t-(v, k, λ) design is pair $\mathcal{D} = (P, B)$, where $P := \{p_1, p_2, \ldots, p_v\}$ is a set of points and $B := \{B_1, B_2, \ldots, B_b\}$ is a set of blocks, such that the following properties are satisfied:*

1. *$|P| = v$, $|B| = b$*
2. *each block contains exactly k points, and*
3. *every set of t distinct points is contained in exactly λ blocks.*

Every element of P is incident with exactly $r = \frac{\lambda(v-1)}{k-1}$ elements of B. We say that a t-(v, k, λ) design is nontrivial when $v - 1 > k > \lambda > t \geq 0$. The term t-design is used to indicate any t-(v, k, λ) design.

Note that any t-design might contain repeated blocks. If $\lambda = 1$, then the correspondent design is called a *simple design* and it can not contain any repeated block. Finding tools to construct t-designs becomes more difficult when $\lambda > 1$.

Example 28. *[MS77, AK92] Let* $B := \{123, 145, 167, 246, 257, 347, 356\}$ *and suppose that* $P := \{1, 2, 3, 4, 5, 6, 7\}$. *Then* $\mathcal{D} = (P, B)$ *is a* $2-(7, 3, 1)$ *design. This design is a projective plane, known as Fano plane, satisfies that for any two distinct points there exists exactly one line such that both points belong to the line, and that any two lines intersect in exactly one point. Any projective plane* $\mathcal{P}$ *of order* n *generates a* $2\text{-}(n^2 + n + 1, n, 1)$ *design, [AK92].*

Definition 29. *[S03] An incidence matrix* $A = (a_{ij})$ *of a* t*-design* $\mathcal{D} = (P, B)$, *where* $|P| = v$ *and* $|B| = b$, *is a* $v \times b$ *matrix with entries in* $\{\pm 1\}$, *where* $a_{ij} = -1$ *if and only if* $p_j \in B_i$. *If we replace* -1 *by* 1 *and* 1 *by* 0 *we obtain a binary incidence matrix.*

The $2\text{-}(7, 3, 1)$ design of Example 28 has the following incidence matrix,

$$H' = \left(\begin{array}{ccccccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right)$$

and it is clear that $H = \left(\begin{array}{c|c} 1 & \mathbf{1} \\ \hline \mathbf{1} & H' \end{array}\right)$ is a Hadamard matrix.

Assume that (P, B) and (P', B') are two designs. They are said to be *isomorphic* if there exists a bijection map $\alpha : P \to P'$ satisfying

$$B' = \{\{\alpha(p) : p \in B_i\} : B_i \in B\}$$

and the bijection α is called *isomorphism*. Two designs are said to be *equivalent* if there exists an isomorphism between them. An *automorphism* of $\mathcal{D}$ is an isomorphism $\alpha : (P, B) \to (P, B)$ preserving points and blocks. The set of all bijections is the *full automorphism group*, $\mathrm{Aut}(\mathcal{D})$, while any subgroup G of $\mathrm{Aut}(\mathcal{D})$ is said to be a *automorphism group*. If G is a subgroup $\mathrm{Aut}(\mathcal{D})$ such that for any pair of points p, p' there is a unique $\alpha \in G$ such $\alpha(p) = p'$, then G is said to be *regular*.

Remark 30. *[BJ+99] These automorphisms can also be described in terms of incidence matrices. Indeed, in [BJ+99] it proved that if the rows or columns of an incidence matrix are permuted, then the resultant matrix is an incidence matrix of an equivalent design.*

The following theorem gives a characterization which decides whether any binary matrix can be realised by a t-design. Denote by I_v the identity matrix of order v and J_v the square all-one matrix of length v.

Theorem 31. *[W88, Theorem 2.9]. Let A be a $v \times b$ binary matrix. The matrix A is an incidence matrix for a t-(v, k, λ) design if and only if*

$$AA^T = (k - \lambda)I_v + \lambda J \quad \textit{and} \quad AJ_V = kJ_v.$$

Definition 32. *[S03] A t-design $\mathcal{D} = (P, B)$ is said to be symmetric if $|P| = |B|$. Hence, the incidence matrix of a symmetric design is square.*

The incidence matrices of t-designs are not square, in general. In fact, there is no square incidence matrices in t-designs for which $t > 2$ because the number of blocks is larger than the number of points. In other words, a design is symmetric if and only if the intersection of any two blocks has fixed size λ. In [MS77, Chap.2 Corollary 9] it is proved that any 2-(v, k, λ) has the following parameters:

$$k = r, \quad \lambda(v - 1) = k(k - 1).$$

Furthermore, if $\mathcal{D}$ is a symmetric design from a projective plane then $\mathcal{D}$ is said to be of order n and [AK92, Theorem 4.2.1]

$$n = k - \lambda$$

The dual concept also holds in designs. Given a design $\mathcal{D}$ with an incident matrix A, then we understand the concept of *the dual design* $\mathcal{D}^*$ of $\mathcal{D}$, such design with A^T as its incident matrix.

Definition 33. *[S03] Let $\mathcal{D} = (P, B)$ be a design, where $|P| = v$ and $|B| = b$. A dual design $\mathcal{D}^* = (P', B')$ of $\mathcal{D}$ satisfies the following properties:*

1. *$|P'| = |B| = b$, $|B'| = |P| = v$.*
2. *Every point in P' occurs in exactly k blocks in B' and any two distinct blocks $B'_i, B'_j \in B'$ intersect in exactly λ points.*

The first link between Hadamard matrices and designs appeared in 1933 when Todd [T33] showed an equivalence between a subfamily of Hadamard matrices of Paley type I and a symmetric design.

Lemma 34. *[BJ+99, Lemma I.9.3] There is a Hadamard matrix of order $4n$ if and only if there is a 2-$(4n - 1, 2n - 1, n - 1)$ design.*

A Hadamard matrix associated to a $(4n-1, 2n-1, n-1)$-design is

$$H = \left(\begin{array}{c|c} 1 & \mathbf{1} \\ \hline \mathbf{1}^T & H' \end{array}\right)$$

where H' is the incidence matrix of such design and $\mathbf{1}$ is the all-one vector. Hence, the term *Hadamard designs* is referred to those designs whose associated incidence matrix is a Paley type I matrix.

Remark 35. *[AK92] Starting from a square $(4n-1, 2n-1, n-1)$-design, the number of points can be extended to $4n$ and the blocks can be redefined in such a way that every block is incident with $2n$ points, and that every 3 distinct points, are together incident with exactly $n-1$ blocks. The resultant design is called a Hadamard 3-$(4n, 2n, n-1)$-design and it is the unique extension (up to isomorphism) of a Hadamard design [AK92, Theorem 7.2.1].*

Several constructions of Hadamard matrices from designs can be found in [L90, LS98]. Nowadays, it becomes harder to construct Hadamard designs and difference sets constitutes a mechanism to do it.

Definition 36. *[EB66] Let G be a multiplicative group such $|G| = v$, and let D be a subset of G such that $|D| = k$. We say that D is a (v, k, λ)-difference set in G if, for each $g \in G$, there are precisely λ pairs $d_i, d_j \in D$ such that $d_i d_j^{-1} = g$. We say that D is nontrivial if $v - 1 > k > \lambda > 0$.*

In [R52] it was proved that $k(k-1) = \lambda(v-1)$. Note that this equality corresponds to a necessary condition stated for symmetric designs. Difference sets were originally defined for additive groups and after finding the relations between finite fields and difference sets, this definition was extended to multiplicative groups. The following theorem shows a strong equivalence between Paley type I matrices (Hadamard designs) and some subclasses of difference sets.

Theorem 37. *[B71] If there is a group G containing a (v, k, λ)-difference set D, then there exists a symmetric design on which G acts regularly. Conversely, a symmetric design on which G acts regularly corresponds to a difference set in G.*

The group ring is the most usual set for studying difference sets. Let G be a finite multiplicative group and $\mathbb{Z}[G]$ the group ring. Each element of $\mathbb{Z}[G]$ is of the form $\sum_{g \in G} a_g g$, where the coefficients $a_g \in \mathbb{Z}$, while a subset $D \subset G$ can be identified with the element $D = \sum_{g \in G} a_g g$ in $\mathbb{Z}[G]$ that has

coefficients 1 when $g \in G$ belongs to D and 0 otherwise. Moreover, each integer n is identified with the element $n \cdot 1_G$ in $\mathbb{Z}[G]$. For an arbitrary $D \subset G$ it is defined $D^{-1} = \sum_{g \in G} a_g g^{-1}$. The set D is a (v, k, λ)-difference set if and only if we have the following property (in the group ring)

$$DD^{-1} = (k-1)e + \lambda G. \tag{2.8}$$

The parameter $n = k - \lambda$ is called the order of D. If $g \in G$, the set $Dg := \sum_{d_i \in D} d_i g$ is also a difference set with the same parameters as D and every Dg is called a *translate* of D. Two difference sets D_1 and D_2 in G are *equivalent* if one can be mapped onto the other by either an automorphism group or a translation.

Example 38. *[S03] Let $G = \langle c : c^7 = 1 \rangle$ and let the subset $D = \{c, c^2, c^4\}$. Then each element of $G \setminus \{1\}$ appears once in DD^{-1}. Indeed,*

$$DD^{-1} = (c + c^2 + c^4)(c^6 + c^5 + c^3) = 2 + G$$

and D is a $(7, 3, 1)$-difference set whose associated incidence matrix is the incidence matrix of the Fano Plane.

Remark 39. *Let D_1 and D_2 be equivalent difference sets in G. If G acts regularly on D_1, then G acts regularly on D_2. In addition, let $\mathcal{D}_1, \mathcal{D}_2$ equivalent designs and G a group acting regularly on $\mathcal{D}_1$; then G acts regularly in $\mathcal{D}_2$. Conversely, equivalent symmetric designs give rise to equivalent difference sets.*

Difference sets over abelain groups were relatively well studied in [B71, K78, JP96]. In [B62] it was also discovered that not only Paley difference set generates Hadamard matrices. Indeed, there is a family of Hadamard matrices of orders n ($n = 4u^2$ and u prime power) that spring from a class of $(4u^2, 2u^2 \pm u, u^2 \pm u)$-difference sets, called regular Hadamard matrices, meaning, Hadamard matrices with constant row and column sums. For the sake of clarity, the reader is referred to [H07].

The first notion of relative difference sets was introduced by Bose [B42] and it was deeply studied by Eliot and Butson [EB66, B63].

Definition 40. *[S03] Let G be a group, $|G| = v$, N a normal subgroup of G and D a subset of G, $|D| = k$. It is said that D is a relative (v, m, k, λ) difference set in G relative to N, if the multiset of values $d_i d_j^{-1}$ of distinct elements $d_i, d_j \in D$ contains each element of $G \setminus N$ exactly λ times, and does not contain elements of N.*

The set of quotients $d_i d_j^{-1} \in G$ allow to write any relative difference set D as $D = \sum_{g_i, g_j \in G} g_i g_j^{-1}$. Consequently, the condition (2.8) also holds for relative difference set. Hence,

$$DD^{-1} = ke + \lambda(G - N). \tag{2.9}$$

Furthermore, the existence of a relative difference set is related to the existence of a difference set. More concretely, the existence of a relative (m, n, k, λ) difference set implies the existence of a $(m, k, n\lambda)$ difference set. As an explanation, let G be a group containing a relative difference set D relative to a normal subgroup N. If a normal subgroup H of G is contained in N, then there exists a relative difference set in G/H relative to N/H. Now, if D is a (m, n, k, λ)-difference set then the correspondent structure in the quotient G/H is a $(m, nh, k, \lambda h)$-relative difference set where $|H| = h$. Hence, G/N will contain an $(m, k, n\lambda)$-difference set which is said to be a contraction of D. In other words, difference sets are the images via an homomorphism of relative difference sets.

Example 41. *[S03] Let Q_8 be the quaternion group presented by $\langle a, b : a^4 = y^4 = 1, a^2 = b^2, ab = ba^{-1}\rangle$ and assume $N = \langle b^2\rangle$. The set $D = \{1, a, b, ab\}$, is a relative $(4, 2, 4, 2)$ difference set of Q_8 relative to N and, from (2.9)*

$$DD^{-1} = (1 + a + b + ab)(1 + a^{-1} + b^{-1} + (ab)^{-1}) = 4 + 2(Q_8 - N).$$

In [LS98, P95] the relations between relative difference sets and *divisible designs* are studied.

Definition 42. *[S03] An (m, n, k, λ)-divisible design is an incidence structure with mn points and the same number of blocks such that every block has k points and every point is on k blocks. A square divisible (v, m, v, λ)-design is class regular with respect to N if it admits an automorphism group N that stabilises each point class and acts regularly on each of them.*

Jungnickel, Seberry et. al [S78, J82, JP96] provide constructions on the class regular divisible designs and relative difference sets.

Definition 43. *[H07] A GH matrix $H(v, \lambda) = (h_{ij})$ over a group G, $|G| = v$ for a, is a $v\lambda \times v\lambda$ matrix with entries from in G with the property that, for every i and j, the set $\{h_{is}h_{js}^{-1} : 1 \leq s \leq v\lambda\}$ contains every element of G exactly λ times.*

Example 44. *[H07] Let $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{00, 10, 01, 11\}$ be the cyclic group of four elements. Then the generalised Hadamard matrix $GH(4,1)$ is*

$$GH(4,1) = \begin{pmatrix} 00 & 00 & 00 & 00 \\ 00 & 01 & 10 & 11 \\ 00 & 10 & 11 & 01 \\ 00 & 11 & 01 & 10 \end{pmatrix}$$

Theorem 45. *[JP96] Let G a group of order v and N a normal subgroup of G with w elements. The existence of the following items is equivalent*

1. *A relative $(v, w, v, v/w)$-difference set in $N \times G$, relative to $N \times \{1\}$.*
2. *A divisible $(v, w, v, v/w)$-design, class regular with respect to $N \times \{1\}$, with regular group $N \times G$.*
3. *A $GH(w, v/w)$ over N.*

2.4 Cocyclic Hadamard matrices

In spite of the important role played by cocycles in the representation group theory, cocyclic Hadamard matrices were not studied until the last twenty years. Cohomological techniques, from character theory, were used in to describe the internal structures of the component circulant matrices in a Hadamard matrix. Although this thesis is more closely related to Hadamard groups, it is convenient to give an overview on cocycles because it is one of the most efficient tools on the computation of Hadamard matrices. In the beginning, *group developement* was one of the first theories on dealing with the algebraic structure in matrices.

Let M be an $n \times n$ matrix with entries in a commutative ring R, then M is said to be *group developed* over a finite group G if there exists a function $\mu : G \to R$ such that $M = [\mu(gh^{-1})]_{g,h \in G}$ for an arbitrary labelling of the rows and columns of M by the elements of G. In the case of Hadamard matrices R is replaced by $\mathbb{Z}_2 = \{\pm 1\}$.

Definition 46. *A matrix $M \in \mathbb{F}_q^{n \times n}$ is said to be a monomial if each row and column has exactly one nonzero entry.*

Definition 47. *[H00] Let R be a ring with a unit group U and let M be a square matrix of order n with coefficients in R. The full automorphism group $\mathrm{Aut}\,(M)$ is defined as the set of all pairs (V, W), where U and W are $n \times n$ monomial matrices with coefficients in U satisfying $VMW^T = H$.*

The following result gives us a criterion to decide whether a $\{\pm 1\}$-matrix M is a group developed over G.

Theorem 48. *[H00] An $\{\pm 1\}$-matrix M is group developed over the group G if and only if* $\mathrm{Aut}\,(M)$ *contains a subgroup isomorphic to G, acting regularly on the rows and columns of M.*

Horadam, de Launey, et al. dealt with the group developemnt theory in [LH93, HL94b, HP97] and elaborate the theory of *cocyclic Hadamard matrices*. In the early 1990's connections between combinatorial design theory and 2−cocycles are studied as well as the connections with coding theory [HL93a].

Definition 49. *[H00] Let G be a finite group of order v and N be a finite abelian group. A cocycle is a map $\psi : G \times G \to N$ such that*

$$\psi(g,h)\psi(gh,k) = \psi(g,hk)\psi(h,k), \forall g,h,k \in G.$$

The cocycle is said to be normalised if $\psi(e,e) = 1$. A cocycle is said to be symmetric if $\psi(g,h) = \psi(h,g)$.

In [H07] it is proved that the set of cocycles, denoted by $Z_2(G,N)$ or Z_2 forms an abelian group under the pointwise multiplication $\odot$, defined by $(\phi \odot \psi)(g,h) = \phi(g,h)\psi(g,h)$, for every $\psi, \phi \in Z_2$, $g,h \in G$.

Definition 50. *[H07] A cocycle ψ can be represented by a square matrix whose rows and columns are indexed by the elements of G under some fixed ordering, and whose entry in position (g,h) is $\psi(g,h)$, and the matrix is represented as $M_\psi = [\psi(g,h)]_{g,h\in G}$. The matrix M is called G-cocyclic matrix.*

Definition 51. *[H00] A (2)-coboundary, $\partial\phi$, is a map $\phi : G \times G \to N$ satisfying*

$$\partial\phi(g,h) = \phi(g)^{-1}\phi(h)^{-1}\phi(gh).$$

The set of coboundaries forms a group denoted by $B_2(G,N)$ or B_2. Every coboundary is a cocycle and as a consequence B_2 is a subgroup of Z_2, [H07]. The quotient group Z_2/B_2 is *the second cohomology group* of G and it is denoted by $H_2(G,N)$ or H_2. The equivalence class of ψ in $Z_2(G,N)$ is denoted by $[\psi]$. Two cocycles ψ_1 and ψ_2 are *cohomologically equivalent* if there exists a coboundary $\partial\phi$ such that $\psi_2 = \psi_1\partial\phi$.

Now, we show some examples for the sake of clarity.

Example 52. *[H07] Let $G = \langle c : c^3 = e\rangle$ and let ω be a cube primitive complex root. Let $\mu : G \to N$, $N = \langle\omega\rangle$ be the function defined by $\mu(e) = 1$ and $\mu(c) = \mu(c^2) = \omega$. We can define the cocycle $\psi : G \times G \to \langle\omega\rangle$, where $\psi(c^i, c^h) = \mu(c^i)\mu(c^j)\mu(c^{i+j})^{-1}$ and it is represented by indexing the row and column i by c^{i-1} as*

$$M_\psi = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

Example 53. *[H07] Let $G = \mathbb{Z}_2^n$ and $N = \{\pm 1\}$. The usual inner product $\langle\cdot,\cdot\rangle$ determines a cocycle ψ, where $\psi(u, v) = (-1)^{\langle u,v\rangle}$, for all $u, v \in G$, and M_ψ is the Sylvester Hadamard matrix of order 2^n. Specifically, in a binary representation with $n = 2$, we have*

$$M_\psi = \begin{pmatrix} (-1)^{\langle 00,00\rangle} & (-1)^{\langle 00,01\rangle} & (-1)^{\langle 00,10\rangle} & (-1)^{\langle 00,11\rangle} \\ (-1)^{\langle 00,01\rangle} & (-1)^{\langle 01,01\rangle} & (-1)^{\langle 01,10\rangle} & (-1)^{\langle 01,11\rangle} \\ (-1)^{\langle 10,00\rangle} & (-1)^{\langle 10,01\rangle} & (-1)^{\langle 10,10\rangle} & (-1)^{\langle 10,11\rangle} \\ (-1)^{\langle 11,00\rangle} & (-1)^{\langle 11,01\rangle} & (-1)^{\langle 11,10\rangle} & (-1)^{\langle 11,11\rangle} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Definition 54. *[H00] Any group E is an extension of N by G if there exists an injective map $\imath : N \to E$ and a surjective map $\pi : E \to G$ such that the next sequence is exact*

$$1 \to N \xrightarrow{\imath} E \xrightarrow{\pi} G \to 1.$$

The extension is said to be central if $\imath(N)$ is a subgroup of $Z(E)$. The set $T(\psi) = \{(1, g) : g \in G\}$ is called a normalised transversal of $N \times \{1\}$ in E.

To construct Hadamard matrices only central extensions are considered.

Definition 55. *[H00] Two extensions E_1, E_2 of N by G are said to be equivalent if the following diagram is commutative, and therefore γ is an isomorphism*

$$\begin{array}{ccccccccc} e & \to & N & \xrightarrow{\imath} & E_1 & \xrightarrow{\pi} & G & \to & e \\ & & \downarrow Id & & \downarrow \gamma & & \downarrow Id & & \\ e & \to & N & \xrightarrow{\imath'} & E_2 & \xrightarrow{\pi'} & G & \to & e \end{array}.$$

In [H00] it is proved that any equivalence class of an extension E of $\mathbb{Z}_2$ by a finite group G corresponds uniquely to a 2-cocycle class in the second cohomology group $H^2(G, \mathbb{Z}_2)$. Let us introduce the following argument to clarify the aforementioned correspondence. Each cocycle ψ determines an

extension group E_ψ consisting of the set of ordered pairs $\{(a,g) : a \in N; g \in G\}$ with multiplication $(a,g)(b,h) = (ab\psi(g,h), gh)$. In the binary case, $N = \mathbb{Z}_2$ and each cocycle $\psi : G \times G \to \{\pm 1\}$ determines a central extension E_ψ of $\mathbb{Z}_2$ by G: E_ψ is the group with elements $\{(\pm 1, g) : g \in G\}$ and $(u,g)(w,h) = (uw\psi(g,h), gh)$. Conversely, each extension E in N, determines cocycles. Indeed, each normalised transversal T of $\imath(N)$ in E determines a transversal function, $\tau_T : G \to E$, that means, $\pi\tau_T = Id$ and $\tau_T(1_G) = 1_G$, where Id is the identity map. Furthermore, $\tau_T(G)$ is a complete set of representatives of the elements of the quotient group $E/\imath(N)$. In the binary case, the cocycle map is $\psi : G \times G \to \mathbb{Z}_2$, where

$$\psi_{\tau_T}(a,g) = \imath^{-1}(\tau(g)\tau(h)\tau(gh)^{-1})$$

Definition 56. *[H00] A cocycle ψ is said to be orthogonal if the cocyclic matrix M_ψ is Hadamard.*

Lemma 57. *[BH95, Lemma 2.6] Let G be a group with $4n$ element, $n \geq 1$. Then a cocycle $\psi : G \times G \to \{\pm 1\}$ is orthogonal if and only if for each $h \in H$, the number of $g \in G$ such that $\psi(g,h) = 1$ is $2n$.*

Cocycles have been one of the main sources in the recent advances on the computation of Hadamard matrices. Further than the cohomological structures, the computation of field extensions and cocycles requires efficent algorithms. Essentially, there are three algorithms for computing these cocycles. The importance of these algorithms in comparison with those used in group develop theory relies on the decomposition of the second cohomology group into the direct sum of two summands [HL94b, Theorem 11.1],

$$H_2(G, \mathbb{Z}_2) \cong Ext(\frac{G}{[G,G]}, \mathbb{Z}_2) \oplus Hom(H_2(G, \mathbb{Z}_2), \mathbb{Z}_2).$$

Furthermore, in [LF$^+$00, F97] it is showed that all the classical Hadamard matrices we saw in Section 2.2 are cocyclic Hadamard matrices. Two of the most important families of coyclic Hadamard matrices are those which are cocyclic over $\mathbb{Z}_n \times \mathbb{Z}_2^2$ and over the dihedral group D_{4n}.

In the first case, in [LH93, BH95] it is showed that the group extensions over $\mathbb{Z}_2$ realising it are:

- $Q_8 \times \mathbb{Z}_n$, when n odd.
- $Q_8 \times \mathbb{Z}_n$, $D_8 \times \mathbb{Z}_n$, $\mathbb{Z}_2^2 \times \mathbb{Z}_{2n}$, $\mathbb{Z}_2^3 \times \mathbb{Z}_n$, $\mathbb{Z}_4 \times \mathbb{Z}_{2n}$ and $\mathbb{Z}_2 \times \mathbb{Z}_{4n}$, when n is even.

In [LF+00] is proved that this family of matrices are equivalent to the matrices of Paley type II.

In [LH93, AA+01, AA+16] it is showed that the group extensions (over $\mathbb{Z}_2$) of the cocyclic Hadamard matrices over the dihedral group D_{4n} are

- $D_{4n} \times \mathbb{Z}_2, \mathbb{Z}_{2n} \rtimes \mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4 (n = 1)$,

In [F97] is showed that this family of matrices are equivalent to the matrices of type Ito.

2.5 Hadamard groups

Let H be a Hadamard matrix. In order to investigate the structure of Aut (H) (see Definition 47) meaning the groups acting regularly on the set of rows and columns of H, Ito introduces the concept of Hadamard groups. This concept is used to construct theoretically Hadamard matrices with an algebraic subjacent group structure. A first approach to Hadamard groups can be seen in [I81], where Ito describes Hadamard groups of type Q and the form of its component submatrices (2.5).

Definition 58. *[I94] Let G be a finite group of order $8n$. The group G is said to be a Hadamard group if G contains a subset D of G with $|D| = 4n$ and an element e^* such that:*

1. $|D \cap Da| = 4n$ *if* $a = e$, *where e denotes de identity element of G.*
2. $|D \cap Da| = 0$ *if* $a = e^*$, *where e^* denotes the central involution of G.*
3. $|D \cap Da| = 2n$, $a \in G$ *and* $a \notin \{e, e^*\}$
4. $|Da \cap \{b, be^*\}| = 1$ *for any* $a, b \in G$.

The set D is called a Hadamard subset.

Remark 59. *Ito [IS00, I00] said that a set T (see Section 2.4) is a a transversal set of a group G if T satisfies $|T \cap Tx| = 2n$ or $|T \cap xT| = 2n$; if T satisfies the first (respectively, the second) equality then T is said to be a right Hadamard subset (respectively, a left Hadamard subset). In other words, a group G is said to be a left Hadamard group if G contains a subset D satisfying, for any $a, b \in G$,*

1. $|D \cap aD| = 4n$ *if* $a = e$, *where e denotes de identity element of G.*

2. $|D \cap aD| = 0$ *if* $a = e^*$, *where* e^* *denotes the central involution of* G.

3. $|D \cap aD| = 2n$, $a \in G$ *and* $a \notin \{e, e^*\}$

4. $|aD \cap \{b, e^*b\}| = 1$ *for any* $a, b \in G$.

In [LF+00, Remark 2.2], right and left transversal structures are also considered to construct cocyclic Hadamard matrices. In [I96] it was proved that if G *is a left Hadamard group with a Hadamard subset* D *then* G *is also a left Hadamard group with the Hadamard subset* D^{-1}.

Ito [I94] proved that the element e^* in a Hadamard group G of order $8n$ is a central involution. The existence of a central involution in a group G plays an important role for G to be a Hadamard group. Let $N = \langle e^* \rangle$ be the central subgroup of G. Likewise in relative difference sets, any Hadamard groups G can be represented over the group ring $\mathbb{Z}[G]$ as

$$G = \sum_{i=1}^{8n} g_i.$$

From the definition of Hadamard group, any Hadamard subset D and its correspondent D^{-1}, represented by $D = \sum_{d \in D} d_i$ and $D^{-1} = \sum_{d \in D} d_i^{-1}$, satisfies

$$DD^{-1} = 4ne + 2n(G - N).$$

Remark 60. *Note that the equality (2.9) also holds for Hadamard groups.*

Ito [I94] defines an incidence matrix for any Hadamard group G as follows. Let G be a Hadamard group of $8n$ elements and let D be a Hadamard subset for G with respect to the central involution e^*. The Hadamard group G can be decomposed in $4n$ pairs of 2 elements in such a way that $G = \{a_i, a_i e^* : a_i \in D, 1 \leq i \leq 4n\}$, where $a_1 = e$. Further, from every pair $(a_i, a_i e^*)$ write

$$Da_i = \{a_j g_j(i) : g_j(i) = e, \text{ or } g_j(i) = e^*, 1 \leq j \leq 4n\}, \ \ 1 \leq i \leq 4n.$$

Ito [I94] claims that the $\{\pm 1\}$-matrix $H = (h_{i,j})$, defined by

$$h_{i,j} = \begin{cases} 1, & \text{if} \quad g_j(i) = e, \\ -1, & \text{if} \quad g_j(i) = e^*, \end{cases}$$

is a Hadamard matrix.

Example 61. *[I94] Let $C_2 = \langle a : a^2 = e\rangle$ be a cyclic group of order two. If D is chosen as $D = \{a\}$ then C_2 is a Hadamard group whereas the cyclic group $C_4 = \langle a : a^4 = e, a^2 = e^*\rangle$ is a Hadamard group by considering $D = \{a, a^2\}$ as its Hadamard subset.*

Example 62. *[I94] Let Q_8 be a quaternion group presented by $Q_8 = \langle a, b : a^4 = e, a^2 = b^2 = e^*, ab = ba^{-1}\rangle$. If we consider the set $D = \{a, e^*, ab, e^*b\}$ then it is easy to see that D is a Hadamard subset for Q_8 and, as a consequence, Q_8 is a Hadamard group.*

Definition 63. *[F97] Two Hadamard groups are said to be isomorphic if there is an isomorphism of groups between them that respects the distinguished central subgroups of order 2.*

Proposition 64. *[I94, Prop.6, Coro.1] Let G be a Hadamard group of order $2n = 2^t n'$, $t \geq 3$ and n' odd. Then Sylow 2-subgroups can neither be realised by a dihedral group nor a cyclic group, but by a generalised quaternion group.*

Remark 65. *In [H07, S03] is proved that the Proposition 64 also holds for Hadamard difference sets and cocyclic Hadamard matrices.*

In [I95a] Ito shows that the concept of equivalence for Hadamard designs is less restrictive than the concept of equivalence for Hadamard designs. To illustrate the theory of Hadamard groups, Ito [I95b] constructs Hadamard groups of Paley type such as *tetrahedral, octahedral,* and *icosahedral* groups.

Wallis [W76] conjectured the existence of matrices of type Ito for every order $4n$, but it seems difficult to be proved, at least, from the point of view of Hadamard groups. The first advances on the existence of Hadamard groups of high orders can be seen in [I97], where Ito deal with the family of generalised quaternion Hadamard groups, meaning Hadamard groups with a subjancet Q_{2^n} group structure. To "complete" the generalised quaternion case, Ito introduces the concept of Hadamard groups of type Q.

Definition 66. *[I97] Let G be a Hadamard group of $8n$ elements. The group G is said to be of type Q if G can be presented*

$$G(n) = \langle a, b : a^{4n} = e, a^{2n} = b^2 = e^*, ab = ba^{-1}\rangle.$$

The Hadamard group $G(n)$ contains an unique central involution e^* which generates the central subgroup $N = \langle e^*\rangle$ of G. List the Hadamard subset D as

$$ee_0, ae_1, a^2e_2, \ldots, a^{2n-1}e_{2n-1}, bf_0, abf_1, \ldots, a^{2n-1}bf_{2n-1}$$

where $e_i, f_i \in \{e, e^*\}$, $0 \leq i \leq 2n-1$. Consider the associated polynomials to D, $c(x), d(x) \in \mathbb{Z}_2[x]/x^{2n}-1$ defined by

$$c(x) = c_0 + c_1 x + \ldots + c_{2n-1}x^{2n-1},$$
$$d(x) = d_0 + d_1 x + \ldots + d_{2n-1}x^{2n-1},$$

where c_i (respectively, d_i) is 0 if $e_i = e$ (respectively, $f_i = e$), otherwise, $c_i = 1$ (respectively, $d_i = 1$). Ito [I95b] proved that $c(x)$ and $d(x)$ are polynomials which define a Hadamard group if and only if

$$c(x^{-1})c(x) + d(x^{-1})d(x) = 4n.$$

The following result [I97] states that starting from a Hadamard group $G(n)$ we can construct another Hadamard group $G(2n)$.

Proposition 67. *[I97] Let $G(n)$ be a Hadamard group of order $8n$ and associated polynomials $c(x), d(x) \in \mathbb{Z}_2[x]/(x^{2n}+1)$. Then the polynomials $c'(x), d'(x) \in \mathbb{Z}_2[x]/(x^{4n}+1)$,*

$$c'(x) = c(x^2) + xd(x^2), \quad \textit{and} \quad d'(x) = d(x^2) - x^{-1}c(x^2)$$

are the polynomials associated to a Hadamard group $G(2n)$ of $16n$ elements.

Note that Proposition 67 proves the existence of Hadamard groups of generalised quaternion type Q_{2^n}, for every natural n. Further, in [I97, I93] it is showed a characterization which decides whether a Hadamard group G is Williamson type, quadratic residue type and Paley type.

Schmidt [S99] studied the problem of the existence of generalised Hadamard matrices from relative difference set perspective, using alternative proofs of Ito's results and incorporating Williamson Hadamard matrices with circulant (but not necessarily symmetric) components. In concrete, Schmidt was able to prove the existence of Hadamard groups of type Q and order $8n$, $1 \leq n \leq 23$.

2.6 On some equivalent Hadamard structures

We finish the current chapter by seeing some of the equivalences between relative difference sets, cocyclic Hadamard matrices and Hadamard groups.

According to Ito, a group G containing a $(4n, 2, 2n, n)$-difference set is called a Hadamard group. Thus, the Hadamard subset D is a relative $(4n, 2, 4n, n)$-difference set in which G acts regularly. Attending to the equivalences between relative difference sets, class regular designs and cocyclic Hadamard matrices we find the following results

Theorem 68. *[LF$^+$00, LS98] The following statements are equivalent.*

1. *There is a cocyclic Hadamard matrix of length $4n$ over G.*
2. *There is a normal $(4n, 2, 4n, 2n)$-relative difference set in a central extension of $\langle -1 \rangle$.*
3. *There is a divisible regular $(4n, 2, 4n, 2n)$-design with respect to $\langle -1 \rangle$; and with a central extension of $\langle -1 \rangle$ by G as a regular group of automorphisms.*

Finally, Flannery [F97] proved the equivalence between Hadamard groups and cocyclic Hadamard matrices.

Theorem 69. *[F97, theorem 3.2] Let ψ be a cocycle. If ψ is orthogonal then the extension E_ψ is a Hadamard group with $\{(1, g) : g \in G\}$ as a Hadamard subset. If E is a Hadamard group with a Hadamard subset T containing 1 and such $G = E/\langle -1 \rangle$, then define $\sigma : G \to T$ by $\psi : g\langle -1 \rangle \to g$, for every $g \in T$. Hence, the following map is an orthogonal cocycle $\psi : G \times G \to \langle -1 \rangle$*

$$\psi(g, h) = \sigma(gh)^{-1}\sigma(g)\sigma(h).$$

Chapter 3

Hadamard full propelinear codes

In the current chapter, we introduce HFP-codes and we analyse some of their algebraic and combinatorial properties. Furthermore, we deal with the connections between Hadamard groups and HFP-codes which also allow to link them with relative difference sets, Hadamard designs, cocyclic Hadamard matrices and class regular divisible designs. We also define the transpose code of a Hadamard code and we prove that the transpose code C^T of a HFP-code C is also a HFP-code; further, we prove that C and C^T are isomorphic as groups. On the other hand, we present some results concerning the available algebraic group structures realizing HFP-codes generalising Ito [I94] and we also review the available HFP-codes of order eight for which we compute the rank and the dimension of the kernel. Finally, to corroborate that the HFP-codes are a proper subfamily of the Hadamard propelinear codes, we present examples of propelinear codes with a specific group structure forbidden for the HFP-case.

The introduction and the first advances on HFP-codes that we show in the current chapter constitute the first contribution of this dissertation which was presented at "IX Jornadas de Matemática Discreta y Algorítmica" and which was published in *Electronic Notes in Discrete Mathematics* as "About a class of Hadamard propelinear codes" [RS14], in Tarragona, Spain, 2014.

3.1 HFP-codes

We found out that there is a subfamily of Hadamard propelinear codes with interesting properties. We termed this family, *Hadamard full propelinear codes*, or, HFP-*codes* for short.

Remind that we denote by $\mathcal{S}_n$ the group of permutations over the set

$\{1, 2, \ldots, n\}$ and we also denoted by $(C, \cdot)$ a binary propelinear code whose associated permutation group is $\Pi = \{\pi_x : x \in C\} \subseteq \mathcal{S}_n$. The binary code C with the operation $x \cdot y = x + \pi_x(y)$, for all $x, y \in C$, where $\pi_{x\cdot y} = \pi_x \pi_y$ forms a group structure $(C, \cdot)$ and $x^{-1} = \pi_x^{-1}(x)$, [RP97].

Definition 70. *[RS14] A binary code C has a full propelinear structure if C has a propelinear structure satisfying that the permutation associated to any element different from $\boldsymbol{e}$ and $\boldsymbol{u}$ has no fixed points. Moreover, $\pi_{\boldsymbol{e}} = \pi_{\boldsymbol{u}} = Id$. A* HFP*-code is a binary Hadamard code with a full propelinear structure.*

The condition which states that $\pi_{\mathbf{e}}, \pi_{\mathbf{u}}$ are the unique permutations fixing points makes HFP-codes special with respect to the family of Hadamard propelinear codes. At the end of the current chapter we show that the family of Hadamard propelinear codes is larger than the family of HFP-codes. Now, we present examples of small orders.

Example 71. *Let $C = \langle a \rangle$ be a Hadamard propelinear where $a = (1, 0)$ and $\pi_a = (1, 2)$. If we compute C then we have that $a^2 = a \cdot a = a + \pi_a(a) = (1, 0) + \pi_a((1, 0)) = (1, 1) = \boldsymbol{u}$ and $a^3 = a \cdot a^2 = a + \pi_a(\boldsymbol{u}) = (1, 0) + \pi_a((1, 1)) = (0, 1)$; hence, $C = \{(0, 0), (1, 0), (1, 1), (0, 1)\}$. The code $(C, \cdot)$ is a* HFP*-code with a subjacent $\mathbb{Z}_4$ group structure and $\Pi = \mathbb{Z}_2$. Furthermore, the rank is $r = 2$ and the dimension of the kernel is $k = 2$.*

Example 72. *Let $C = \langle a, b \rangle$ be a Hadamard propelinear code $C = \langle a, b \rangle$, where $a = (1, 0, 1, 0)$, $b = (1, 0, 0, 1)$ and $\pi_a = (1, 2)(3, 4), \pi_b = (1, 3)(2, 4)$. If we compute all elements in $(C, \cdot)$ then we have*

$$
\begin{array}{llll}
\boldsymbol{e} = (0,0,0,0), & \pi_{\boldsymbol{e}} = Id, & a = (1,0,1,0), & \pi_a = (1,2)(3,4), \\
a^2 = (1,1,1,1), & \pi_{a^2} = Id, & a^3 = (0,1,0,1), & \pi_{a^3} = (1,2)(2,4), \\
b = (1,0,0,1), & \pi_b = (1,3)(2,4), & ab = (1,1,0,0), & \pi_{ab} = (1,4)(2,3), \\
a^2b = (0,1,1,0), & \pi_{a^2b} = (1,3)(2,4), & a^3b = (0,0,1,1), & \pi_{a^3b} = (1,4)(2,3).
\end{array}
$$

Hence, C is a HFP*-code with a subjacent quaternion group structure Q_8. Indeed, C is presented by $\langle a, b : a^4 = b^2 = \boldsymbol{u}, ab = ba^{-1} \rangle = Q_8$ and $\Pi = \langle \pi_a, \pi_b \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. The rank is $r = 3$ and the dimension of the kernel is $k = 3$. Furthermore, this code is translation invariant because for any $x \in \mathbb{Z}_2^4$ and $u, v \in C$ we have that*

$$d(u, v) = d(u \cdot x, v \cdot x)$$

Example 73. *Let $C = \langle a, b\rangle$ be a Hadamard propelinear code, where $a = (1,0,1,0), b = (1,1,0,0)$ and $\pi_a = (1,2)(3,4), \pi_b = (1,3)(2,4)$. If we compute $(C,\cdot)$ we have*

$$\begin{array}{llll} \boldsymbol{e} = (0,0,0,0), & \pi_{\boldsymbol{e}} = Id, & a = (1,0,1,0), & \pi_a = (1,2)(3,4), \\ a^2 = (1,1,1,1), & \pi_{a^2} = Id, & a^3 = (0,1,0,1), & \pi_{a^3} = (1,2)(3,4), \\ b = (1,1,0,0), & \pi_b = (1,3)(2,4), & ab = (0,1,1,0), & \pi_{ab} = (1,4)(2,3), \\ a^2b = (0,0,1,1), & \pi_{a^2b} = (1,3)(2,4), & a^3b = (1,0,0,1), & \pi_{a^3b} = (1,4)(2,3). \end{array}$$

Hence, C is an abelian propelinear code of eight elements realizing a $\mathbb{Z}_2 \times \mathbb{Z}_4$ group. In fact, C is presented by $\langle a, b : a^4 = \boldsymbol{e}, a^2 = b^2, ab = ba^{-1}\rangle = \mathbb{Z}_2 \times \mathbb{Z}_4$; the group $\Pi = \langle \pi_a, \pi_b\rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. The rank is $r = 3$ and the dimension of the kernel is $k = 3$. This is an example of an abelian HFP*-code but nontranslation invariant. In fact,*

$$d(ab, \boldsymbol{e}) = \mathrm{wt}(ab) = \mathrm{wt}(0,1,1,0) = 2, \qquad \text{and}$$
$$d(ab \cdot (0,1,0,0), \boldsymbol{e} \cdot (0,1,0,0)) = d((0,1,0,0),(0,1,0,0)) = 0.$$

Furthermore, in [DL98, RP97] it was proved that any abelian propelinear translation invariant has a group structure $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, for which $\alpha + 2\beta = 4n$. In this example, $\alpha = \beta = 1$.

Definition 74. *Let C_1 and C_2 be two binary codes of length n. It is said that C_1 is isomorphic to C_2 if there exists a permutation $\pi \in \mathcal{S}_n$ such that*

$$C_2 = \{\pi(c) : c \in C_1\}.$$

Definition 75. *Let C_1 and C_2 two binary codes of length n. It is said that C_1 and C_2 are equivalent if there exists a permutation in $\pi \in \mathcal{S}_n$, and a vector $y \in \mathbb{Z}_2^n$ such*

$$C_2 = \{y + \pi(c) : c \in C_1\}.$$

Isomorphic and equivalent concepts are, in general, different but they coincide in the case of binary linear codes.

Remark 76. *It is well-known that there is a unique binary linear Hadamard code of length 2^n, for any n, which is the dual of the extended Hamming code of length 2^n.*

It is easy to see that HFP-codes of Example 72 and Example 73 are equal, as binary codes. Furthermore, due to the fact that the rank and the dimension of the kernel coincide, the binary code is linear. Hence, we appreciate that different full propelinear structures not necessarily generate different binary Hadamard codes.

Proposition 77. *Let $(C,\cdot)$ be a full propelinear code. Then, if any binary code C' is isomorphic, as a binary code, to C then C' is a full propelinear code and C and C' are isomorphic as groups.*

Proof. Let $(C,\cdot)$ be a full propelinear code of length n and let C' be a isomorphic code to C. Hence, there exists $\pi \in \mathcal{S}_n$ with $C' = \{c' = \pi(c) : c \in C\}$. Thus, if for any $x, y, z \in C$ we have $z = x \cdot y = x + \pi_x(y)$ with $\pi_z = \pi_x\pi_y$ then $\pi(x) + \pi\pi_x\pi^{-1}(\pi(y)) = \pi(x) + \pi\pi_x(y) = \pi(x + \pi_x(y)) = \pi(z)$. Thus, if we consider $\Pi' = \{\pi_{c'} = \pi\pi_c\pi^{-1} : \pi_c \in \Pi\}$ to be the associated group of permutations of C' then $(C',\cdot)$ is a propelinear code, where $x' \cdot y' = x' + \pi_{x'}(y')$. If there is an element $z' \in C' \setminus \{\mathbf{e}, \mathbf{u}\}$ in such a way that $\pi_{z'} = \pi\pi_z\pi^{-1}$ fixes a coordinate, for instance $\pi\pi_z\pi^{-1}(1) = 1$, then $\pi_z(\pi^{-1}(1)) = \pi^{-1}(1)$ contradicting the full propelinearity of C.

Finally, define the morphism $\phi : (C,\cdot) \to (C',\cdot)$ such that $\phi(c) = c'$. It is clear that ϕ is well defined and, from the previous paragraph, it follows straightforward that ϕ is an isomorphism. □

In Definiton 70 we impose that the element $\mathbf{u}$ must belong to HFP-codes. In the following result it is proved that this element is central.

Lemma 78. *[RS14] Let $(C,\cdot)$ be a* HFP*-code and let $\boldsymbol{u}$ be the all-one vector. Then vector $\boldsymbol{u}$ is central.*

Proof. The fact that $\pi_{\mathbf{u}} = Id$ comes from the definition of full propelinearity. For any vector $\mathbf{a} \in C$ we have $\mathbf{a}\cdot\mathbf{u} = \mathbf{a} + \pi_{\mathbf{a}}(\mathbf{u}) = \mathbf{a} + \mathbf{u} = \mathbf{u} + \pi_{\mathbf{u}}(\mathbf{a}) = \mathbf{u}\cdot\mathbf{a}$, so vector $\mathbf{u}$ is central in C. □

3.2 Properties of HFP-codes

The aim of the current section is to show the equivalences between HFP-codes and Hadamard groups, to deal with the transpose code of any HFP-code and to study the subjacent algebraic structures in HFP-codes.

Let C be a Hadamard propelinear code of length $4n$. From now on, we denote by D_j the set of codewords of C with a zero on the jth coordinate and by $e_j \in \mathbb{Z}_2^{4n}$ the unitary vector with only one nonzero coordinate at the position j^{th}, for $j \in \{1, 2, \ldots, 4n\}$.

Lemma 79. *Let $(C,\cdot)$ be a Hadamard propelinear code of length $4n$ and consider the set D_1. Then, for any $a \in C$ we have that $|D_1 \cap a \cdot D_1| \in \{0, 2n, 4n\}$.*

Proof. Let $(C, \cdot)$ be a Hadamard propelinear code of length $4n$ and take D_1 the set of codewords of C with a zero in the first position.

1) Let a be an element in C such that $\pi_a(e_1) = e_1$. If $a \in D_1$ then $a \cdot D_1 = D_1$ and $|a \cdot D_1 \cap D_1| = 4n$, otherwise $a \cdot D_1 = \mathbf{u} + D_1 = \mathbf{u} \cdot D_1$ and $|a \cdot D_1 \cap D_1| = 0$.

2) Let a be an element in C such that $\pi_a(e_1) = e_k$, for some $k \neq 1$. Hence, $a \cdot D_1 = D_k$ if and only if $a \in D_k$, otherwise $a \cdot D_1 = \mathbf{u} \cdot D_k$. Since C is a Hadamard code, in both cases we have $|D_1 \cap a \cdot D_1| = 2n$.

□

Proposition 80. *Let $(C, \cdot)$ be a* HFP*-code of length $4n$ and let D_1 be the set of codewords of C which have the value zero in their first position. We can order the set $D_1 = \{a_1, a_2, \ldots, a_{4n}\}$ in such a way that $\pi_{a_i}(e_i) = e_1$. Consider the matrix H, whose rows are the elements of D_1. Then H is the matrix whose row $a_i \in D_1$, in the j^{th} position has the value*

$$\begin{cases} 0, & \text{if and only if } \ a_j \cdot a_i \in D_1. \\ 1, & \text{if and only if } \ a_j \cdot a_i \notin D_1. \end{cases} \tag{3.1}$$

Furthermore, H is a normalised Hadamard matrix associated to C, whose columns are indexed by the elements of D_1.

Proof. Consider the set $D_1 = \{a_1, a_2, \ldots, a_{4n}\}$ of all codewords of C with the first coordinate equal to zero. The order defined in D_1 is well defined; it means that, for any two different $a_i, a_j \in D_1$ we have $\pi_{a_i^{-1}}(e_1) \neq \pi_{a_j^{-1}}(e_1)$. Indeed, if $\pi_{a_i^{-1}}(e_1) = \pi_{a_j^{-1}}(e_1)$ then $\pi_{a_i \cdot a_j^{-1}}(e_1) = e_1$ since $\pi_{a_i \cdot a_j^{-1}} = \pi_{a_i}\pi_{a_j^{-1}} = \pi_{a_i}\pi_{a_j}^{-1}$ contradicting Definition 70.

On the other hand, let $a_i \in D_1$ and let D_j be the set of codewords with a zero in the j^{th} position. Let $a_j \in D_1$; since $\pi_{a_j}(e_j) = e_1$ then the vectors in $\pi_{a_j}(D_j)$ have the first coordinate equal to zero. Now, from the fact that $a_j \in D_1$ then the vectors in $a_j \cdot D_j = a_j + \pi_{a_j}(D_j)$ and, so, $D_1 = a_j \cdot D_j$. □

We choose the Hadamard subset D_1 for convenience and because it provides a normalised Hadamard matrix H of C; but we could have selected another Hadamard subset instead of D_1.

Remark 81. *The order we give in Propositon 80 for $D_1 = \{a_1, a_2, \ldots, a_{4n}\}$ is understood as the order in which we index the columns of the matrix H by the elements of D_1. This order depends, exclusively, on the permutations π_{a_i},*

with $\pi_{a_i}(e_i) = e_1$ we fixed in Proposition 80. Nevertheless, the order in D_1 does not put any restriction on the rows of H, meaning that, if we permute the rows of H then the codewords of C keep invariant.

For every $a_i \in C$, π_{a_i} acts as a permutation over the coordinates of C and, since the coordinates of C are indexed by the elements of D_1 then, one can think that π_{a_i} acts as a permutation over the set D_1. The following result shows this statement in more detail.

Lemma 82. *Let $(C, \cdot)$ be a* HFP*-code of length $4n$ and let D_1 the set of codewords with the first position equal to zero. For every $x \in C$, define δ_x as the element in $\{\boldsymbol{e}, \boldsymbol{u}\}$ such that $\delta_x \cdot x \in D_1$. Then the map $\pi_{a_i}(a_j) = a_i + a_i \cdot a_j$ acts as a permutation over the set D_1 by sending*

$$\begin{array}{rccc} \pi_{a_i}: & D_1 & \to & D_1 \\ & a_j & \to & \delta_{(a_j \cdot a_i^{-1})} \cdot a_j \cdot a_i^{-1}. \end{array}$$

Proof. First of all we are going to prove that π_{a_i} is injective. If we have $\pi_{a_i}(a_j) = \pi_{a_i}(a_k)$, for any two different $a_j, a_k \in D_1$, then we can write $\delta_{(a_j \cdot a_i^{-1})} \cdot a_j \cdot a_i^{-1} = \delta_{(a_k \cdot a_i^{-1})} \cdot a_k \cdot a_i^{-1}$ which turns to $\delta_{(a_j \cdot a_i^{-1})} \cdot a_j = \delta_{(a_k \cdot a_i^{-1})} \cdot a_k$. Since $a_k, a_j \in D_1$ then $\delta_{(a_j \cdot a_i^{-1})} = \delta_{(a_k \cdot a_i^{-1})}$ and, so $a_j = a_k$. On the other hand, we prove that π_{a_i} is a surjective map by seeing that the image of $a_k \in D_1$, through π_{a_i}, is the element $\delta_{(a_k \cdot a_i)} \cdot a_k \cdot a_i \in D_1$. From the definition of π_{a_i} we can write $\pi_{a_i}(\delta_{(a_k \cdot a_i)} \cdot a_k \cdot a_i) = \delta_{(\delta_{(a_k \cdot a_i)} \cdot a_k)} \cdot \delta_{a_k \cdot a_i} \cdot a_k$ and, since $a_k \in D_1$, then it follows straightforward that $\delta_{(\delta_{(a_k \cdot a_i)} \cdot a_k)} = \delta_{(a_k \cdot a_i)}$. Hence, π_{a_i} is a bijection and, as a consequence, π_{a_i} acts as a permutation on the set D_1.

Finally, we are going to prove that the map π_{a_i}, which takes the position $a_j \in D_1$ to the position $\delta_{(a_j \cdot a_i^{-1})} \cdot a_j \cdot a_i^{-1} \in D_1$, can be written as $\pi_{a_i}(a_j) = a_i + a_i \cdot a_j$, for every $a_j \in C$. To see this property, take two vectors $x, y \in C$ with the same value on a position, for instance in $a_j \in D_1$; thus, $a_j \cdot x$ and $a_j \cdot y$ simultaneously belong (respectively, do not belong) to D_1. The pair of vectors $a_i + a_i \cdot x$ and $a_i + a_i \cdot y$ mutually agree (respectively, mutually disagree) like the pair $a_i \cdot x$ and $a_i \cdot y$ on any coordinate. And, the values of $a_i \cdot x$ and $a_i \cdot y$ in the position $\delta_{(a_j \cdot a_i^{-1})} \cdot a_j \cdot a_i^{-1}$ agree or disagree depending on whether $\delta_{(a_j \cdot a_i^{-1})} \cdot a_j \cdot a_i^{-1} \cdot a_i \cdot x = \delta_{(a_j \cdot a_i^{-1})} \cdot a_j \cdot x$ and $\delta_{(a_j \cdot a_i^{-1})} \cdot a_j \cdot a_i^{-1} \cdot a_i \cdot y = \delta_{(a_i^{-1} \cdot a_j)} \cdot a_j \cdot y$ belong (respectively, do not belong) simultaneously to D_1. □

Definition 83. *From a Hadamard matrix H we define a Hadamard code $C = H \cup H + \boldsymbol{u}$. We denote by C^T the Hadamard code $C^T = H^T \cup H^T + \boldsymbol{u}$ and we call C^T the transpose code of C.*

The following result shows that the transpose code C^T of any HFP-code C is a HFP-code. As a previous idea, we are going to see that HFP-structure in C^T is induced by the HFP-structure of C; more concretely, we prove that C^T is *opposite group* C^{op} of C.

Definition 84. *[B90, Definition 2.1.1] If $(G,\cdot)$ is a group, denoted by $(G^{op},\diamond)$ the opposite group: the underlying set of G^{op} is G and in the group law G^{op} satisfies, for any $g,h\in G$, that*

$$g\cdot h = h\diamond g.$$

Proposition 85. *Let $(C,\cdot)$ be a* HFP*-code of length $4n$. Then C^T is a* HFP*-code. Moreover, C and C^T are isomorphic as groups.*

Proof. Consider the ordered set $D_1=\{a_1,a_2,\ldots,a_{4n}\}$ and the Hadamard matrix H defined in Proposition 80. Let $(C^{op},\diamond)$ be the opposite group and take the isomorphism $\phi: C\to C^{op}$, where $\phi(c)=c^{-1}$. We define the binary representation of a vector $a_i\in C^{op}$ as follows; the vector $a_i\in C^{op}$ has the value 0 in the position $a_j\in D_1$ if and only if $a_j\diamond a_i\in D_1$. Since $a_j\diamond a_i = a_i\cdot a_j$ then the matrix given by the elements in $C^{op}\cap D_1$ is the transpose matrix of H and, therefore, $C^{op}=C^T$. As a result, C^{op} is a Hadamard code.

We are going to prove that the code $(C^{op},\diamond)$ is full propelinear. The full propelinear structure requires to define a permutation τ_{a_i}, for each vector $a_i\in C^{op}$. Hence, for any two $a_i,a_j\in C^{op}$ define the map $\tau_{a_i}(a_j)=a_i+a_i\diamond a_j$. From Lemma 82 we know that the map τ_{a_i} acts as a permutation over D_1 by taking the position $a_j\in D_1$ to the position $\delta_{(a_j\diamond a_i^{-1})}\diamond a_j\diamond a_i^{-1}\in D_1$, which is, $\delta_{(a_i^{-1}\cdot a_j)}\cdot a_i^{-1}\cdot a_j\in D_1$. Now, we need to check that $(C^{op},\diamond)$ satisfies the propelinear conditions. The first item (2.2) follows straightforward and the second item (2.3) follows from

$$\begin{aligned}\tau_{a_i}\tau_{a_j}(a_k) &= \tau_{a_i}(\tau_{a_j}(a_k)) = \tau_{a_i}(a_j+a_j\diamond a_k)\\ &= \tau_{a_i}(a_j)+\tau_{a_i}(a_j\diamond a_k) = a_i\diamond a_j + a_i\diamond a_j\diamond a_k\\ &= \tau_{(a_i\diamond a_j)}(a_k),\end{aligned}$$

and, from $\tau_{a_i}(\mathbf{e})=a_i+a_i\diamond\mathbf{e}=\mathbf{e}$ and $\tau_{a_i}(\mathbf{u})=a_i+a_i\diamond\mathbf{u}=\mathbf{u}$. Finally, to verify that $(C^{op},\diamond)$ is a full propelinear code, assume that there is a permutation τ_{a_i}, $a_i\in C\setminus\{\mathbf{e},\mathbf{u}\}$ fixing a position, for instance the position correspondent to $a_j\in D_1$. If $\tau_{a_i}(a_j)=a_j$ then $a_j=\delta_{(a_i^{-1}\cdot a_j)}\cdot a_i^{-1}\cdot a_j$ but it implies that a_i^{-1} and a_i coincide with $\delta_{(a_i^{-1}\cdot a_j)}\in\{\mathbf{e},\mathbf{u}\}$. Consequently, $(C^{op},\diamond)$ is a HFP-code and, C and C^{op} are isomorphic as groups. □

Remark 86. *Likewise in Proposition 80, permutations $\pi_{a_i}(e_i) = e_1$, $a_i \in C$, define an order for D_1, it is clear that permutations τ_{a_i}, defined in Proposition 85, depend on the order in which we take the rows of the matrix H. In other words, the elements in $C \cap D_1$ and in $C^{op} \cap D_1$ (the rows of H and H^T) might not be equally ordered.*

Now, we present the first goal in this thesis by studying the equivalences between Hadamard groups and HFP-codes. Let us introduce the following notation for the sake of clarity. We denote by $([G, D, \mathbf{u}], *)$ the Hadamard group $(G, *)$ which contains a Hadamard subset D with respect to the central involution $\mathbf{u}$. We shall begin by seeing that any HFP-code $(C, \cdot)$ determines a left Hadamard group $([C, D_1, \mathbf{u}], \cdot)$.

Proposition 87. *Let $(C, \cdot)$ be a* HFP*-code of length $4n$. Then $([C, D_1, \boldsymbol{u}], \cdot)$ is a left Hadamard group with respect to the central element $\boldsymbol{u}$.*

Proof. We are going to prove that C contains a subset D with respect to the central involution $\mathbf{u}$ satisfying the four properties of Definition 58. Let $D_1 = \{a_1, a_2, \ldots, a_{4n}\}$ be the ordered set of Proposition 80, formed by all codewords of C with the first coordinate equal to zero with $\pi_{a_i}(e_i) = e_1$. Firstly, we have $|D_1| = 4n$ and $C = D_1 \cup \mathbf{u} + D_1$. Note that, if $a_j \in D_1$ then it follows that $a_j \cdot D_j = D_1$ and $D_j = a_j^{-1} \cdot D_1$, where D_j is the set of all codewords with the j^{th} coordinate equal to zero. Hence, for any $a_j \in D_1$ we have that $|D_1 \cap a_j^{-1} \cdot D_1| = |D_1 \cap D_j|$ which is $2n$, since C is a Hadamard code. Otherwise, if $a_j \in \mathbf{u} + D_1$ then $|D_1 \cap a_j^{-1} \cdot D_1| = |D_1 \cap \mathbf{u} + D_j|$ which is $2n$, since C is a Hadamard code. Finally, the value of $|D_1 \cap a_j^{-1} \cdot D_1|$ is 0 or $4n$ if and only if a_j^{-1} is $\mathbf{u}$ or $\mathbf{e}$, respectively. As a result, D_1 is a left Hadamard subset and, so, $([C, D_1, \mathbf{u}], \cdot)$ is a left Hadamard group. □

Vice versa, the following result shows that any left Hadamard group determines a HFP-code. A first version of this result can be seen in [RS14] but now, we show a new version in which we go deeper into detail.

Proposition 88. *Let $([G, D, \boldsymbol{u}], *)$ be a left Hadamard group of order $8n$. Then G determines a* HFP*-code $(C, \cdot)$.*

Proof. Write the Hadamard subset $D = \{a_1, a_2, \ldots, a_{4n}\}$ where $a_1 = \mathbf{e}$. Define $\gamma_{(a_i, a_j)}$ as the element in $\{\mathbf{e}, \mathbf{u}\}$ satisfying $\gamma_{(a_i, a_j)} * a_j * a_i \in D$. We are going to define a matrix indexed by the elements in D. Let H be the matrix in which the entry (a_i, a_j) has the value 0 if and only if $\gamma_{a_i, a_j} = \mathbf{e}$ and, otherwise has a 1. It is obvious that the first row and column are all-zero

vectors. We claim that H^T is a Hadamard matrix. Firstly, any column a_p has $|\mathbf{u} * D \cap a_p * D|$ positions with 1's and $|D \cap a_p * D|$ position with 0's. Since $([G, D, \mathbf{u}, *)$ is a left Hadamard group then $\mathrm{wt}(a_p)$ is 0 or $4n$ if and only if a_p is $\mathbf{u}$ or $\mathbf{e}$, respectively, and, otherwise $\mathrm{wt}(a_p) = 2n$. Concerning the Hamming distance, take two columns a_p and a_q, $a_p \notin \{a_q, a_q * \mathbf{u}\}$, and compute the number of positions in which they disagree. By definition, a_p and a_q disagree in $a_i \in D$ if and only if one of the following conditions is satisfied: $a_i \in (a_p^{-1} * \mathbf{u} * D) \cap (a_q^{-1} * D)$ or $a_i \in (a_p^{-1} * D) \cap (a_q^{-1} * \mathbf{u} * D)$. To compute the Hamming distance, firstly, take into account that $|D \cap \{a_p, a_p * \mathbf{u}\}| = 1$ and $|a_p^{-1} * D \cap a_q^{-1} * \mathbf{u} * D| = 2n$ since $([G, D, \mathbf{u}], *)$ is a left Hadamard group. Now, the key is based on $(a_p^{-1} * \mathbf{u} * D) \cap (a_q^{-1} * D) = \mathbf{u} * ((a_p^{-1} * D) \cap (a_q^{-1} * \mathbf{u} * D))$ because it rises to $d(a_p, a_q) = |a_p^{-1} * D \cap a_q^{-1} * \mathbf{u} * D| = 2n$. Thus, H^T is a Hadamard matrix and so does H.

Now, we are going to define a Hadamard code C' as follows. For each $a_i \in D$, define the vector v_{a_i}, where its j^{th} position coincides with the value in the entry (a_i, a_j). Hence, $v_{a_1} = \mathbf{e} \in \mathbb{Z}_2^{4n}$, $v_{a_{4n+1}} = \mathbf{u} \in \mathbb{Z}_2^{4n}$ and $v_{a_{4n+i}} = v_{a_i} + \mathbf{u}$, $1 \leq i \leq 4n$. Define the sets $C' = \{v_{a_i} : 1 \leq i \leq 8n\}$ and $D' = \{v_{a_i} : a_i \in D\}$.

To provide C' with a propelinear structure we should associate a permutation to each vector in C' and to define the correspondent operation.

It might be noted that the coordinates of the vectors in C' are indexed by the elements of D. For this reason, associate to each $v_{a_i} \in C'$ the map $\pi_{v_{a_i}} : D \to D$, defined by $\pi_{v_{a_i}}(a_j) = \gamma_{(a_i^{-1}, a_j)} * a_j * a_i^{-1}$. We need to prove that $\pi_{v_{a_i}}$ is a permutation and we begin by seeing that it is injective. If $\pi_{v_{a_i}}(a_j) = \pi_{v_{a_i}}(a_k)$, for any two different $a_j, a_k \in D$, then the equality $\gamma_{(a_i^{-1}, a_j)} * a_j * a_i^{-1} = \gamma_{(a_i^{-1}, a_k)} * a_k * a_i^{-1}$ turns to $\gamma_{(a_i^{-1}, a_j)} * a_j = \gamma_{(a_i^{-1}, a_k)} * a_k$; it is clear that the values of both gamma's coincide since $a_j, a_k \in D$ and so $a_j = a_k$. To see that $\pi_{v_{a_i}}$ is surjective we prove that a_k is the image of $\gamma_{(a_i, a_k)} * a_k * a_i$ through $\pi_{v_{a_i}}$. Indeed, the element $\pi_{v_{a_i}}(\gamma_{(a_i, a_k)} * a_k * a_i)$ is $\gamma_{(a_i^{-1}, \gamma_{(a_i, a_k)} * a_k * a_i)} * \gamma_{(a_i, a_k)} * a_k$ and, both gamma's coincide since $a_k \in D$.

We claim that $\pi_{v_{a_i}}$ can be written as $\pi_{v_{a_i}}(v_{a_j}) = v_{a_i} + v_{a_i * a_j}$, for any $v_{a_j} \in C'$. To see this property, take two vectors $v_{a_p}, v_{a_q} \in C'$ with the same value in a position, for instance in $a_k \in D$. Hence, $a_k * a_p$ and $a_k * a_q$ simultaneously belong (respectively, do not belong) to D. Note that the pair of vectors $v_{a_i} + v_{a_i * a_p}$ and $v_{a_i} + v_{a_i * a_q}$ agrees or disagrees like the pair $v_{a_i * a_p}$ and $v_{a_i * a_q}$ on any coordinate. Now, the values of the pair $v_{a_i * a_p}$ and $v_{a_i * a_q}$ on the position $\gamma_{(a_i^{-1}, a_k)} * a_k * a_i^{-1} \in D$ agree or do not agree depending on whether $\gamma_{(a_i^{-1}, a_k)} * a_k * a_p$ and $\gamma_{(a_i^{-1}, a_k)} * a_k * a_q$ belong (respectively, do not belong) simultaneously to D.

Define the operation $\cdot$ in C' by $v_{a_i} \cdot v_{a_j} = v_{a_i} + \pi_{v_{a_i}}(v_{a_j})$, for every $v_{a_i}, v_{a_j} \in C'$. We claim $(C', \cdot)$ is a HFP-code. We are going to verify the propelinear condition. Item (2.2) follows straightforward and, item (2.3) follows from

$$\begin{aligned} \pi_{v_{a_i}}\pi_{v_{a_j}}(v_{a_k}) &= \pi_{v_{a_i}}(v_{a_j} + v_{(a_j * a_k)}) = v_{(a_i * a_j)} + v_{(a_i * a_j * a_k)} \\ &= \pi_{v_{(a_i * a_j)}}(v_{a_k}) = \pi_{(v_{a_i} \cdot v_{a_j})}(v_{a_k}), \end{aligned}$$

and, from $\pi_{v_{a_i}}(\mathbf{e}) = v_{a_i} + v_{a_i} \cdot \mathbf{e} = \mathbf{e}$ and $\pi_{v_{a_i}}(\mathbf{u}) = v_{a_i} + v_{a_i} \cdot \mathbf{u} = \mathbf{u}$. To prove the full propelinearity of $(C', \cdot)$ assume that there is an element $a_i \notin \{\mathbf{e}, \mathbf{u}\}$ whose map $\pi_{v_{a_i}}$ fixes a position, for instance $a_j \in D$. The equality $v_{a_j} = v_{(\gamma_{(a_i^{-1}, a_j)} * a_j * a_i^{-1})}$ provides the equality $a_j = \gamma_{(a_i^{-1}, a_j)} * a_j * a_i^{-1}$. Hence, $a_i^{-1} = \gamma_{(a_i^{-1}, a_j)} \in \{\mathbf{e}, \mathbf{u}\}$ and, so does $a_i \in \{\mathbf{e}, \mathbf{u}\}$. The result is proved $\square$

Corollary 89. *There is a one-to-one correspondence between left Hadamard groups and* HFP*-codes.*

Proof. Let Ψ be the map which takes any HFP-code $(C, \cdot)$ to the left Hadamard group $([C, D_1, \mathbf{u}], \cdot)$ developed in Proposition 87. Let θ be the map which takes any left Hadamard group $([G, D, \mathbf{u}], *)$ to the HFP-code $(C', \star)$ by Proposition 88. To prove that there is a one-to-one correspondence between HFP-codes and left Hadamard groups we should see that $\Psi \circ \theta$ and $\theta \circ \Psi$ coincide with the identity map, where $\circ$ denotes the composition.

On one hand, consider the map

$$\Phi : (C, \cdot) \xrightarrow{\Psi} ([C, D_1, \mathbf{u}], \cdot) \xrightarrow{\theta} (C', \star).$$

Let D_1 and H be the ordered set and the Hadamard matrix of Proposition 80. Hence, any vector $a_i \in C$ has a 0 in its j^{th} position, indexed by $a_j \in D_1$, if and only if $a_j \cdot a_i \in D_1$, otherwise has a 1. Now, the left hadamard group $\Psi((C, \cdot)) = ([C, D_1, \mathbf{u}], \cdot)$ defines a matrix H', indexed by the elements of D_1, whose entry (a_i, a_j) has the value 0 if and only if $a_j \cdot a_i$, otherwise a 1. Now, consider $\theta(([C, D_1, \mathbf{u}], \cdot)) = (C', \star)$ and $D' = \{v_{a_1}, v_{a_2}, \ldots, v_{a_{4n}}\}$. Hence, any v_{a_i} has a 0 in its j^{th} position, indexed by a_j, if and only if $a_j \cdot a_i \in D_1$, otherwise has a 1. Consequently, for every $a_i \in D_1$, the binary vectors v_{a_i} and a_i coincide and so do $a_i + a_i \cdot a_j$ and $v_{a_i} + v_{a_i \cdot a_j}$. In addition, since $v_{a_i \cdot a_j} = v_{a_i} \star v_{a_j}$ then $v_{a_i} + v_{a_i \cdot a_j} = v_{a_i} + v_{a_i} \star v_{a_j}$, meaning, $\pi_{a_i}(a_j) = \pi_{v_{a_i}}(v_{a_j})$. Finally, $(C, \cdot) = (C', \star)$ and, therefore, Φ is the identity map.

On the other hand, consider the map $\Phi' : \Psi \circ \theta$,

$$\Phi' : ([G, D, \mathbf{u}], *) \xrightarrow{\theta} (C', \star) \xrightarrow{\Psi} ([C', D', \mathbf{u}], \star).$$

Write $D = \{a_1, a_2, \ldots, a_{4n}\}$ and let H' be the Hadamard matrix, indexed by the elements of D, whose the entry (a_i, a_j) has the value 0 if and only if $a_j * a_i \in D$, otherwise has a 1. Consider the HFP-code $\theta(([G, D, \mathbf{u}], *)) = (C, \star)$ and its subset set $D' = \{v_{a_1}, v_{a_2}, \ldots, v_{a_{4n}}\}$. The vectors v_{a_i}, $a_i \in D$, have the value 0 in its j^{th} position, indexed by $a_j \in D$, if and only if $v_{a_j * a_i} \in D'$, otherwise, have a 1. Furthermore, the operation $\star$ satisfies $v_{a_i} \star v_{a_j} = v_{a_i * a_j}$. Thus, the matrix $\hat{H}$, formed by the elements of D', coincide with H'. Finally, the left Hadamard groups $\Psi((C, \star)) = ([C', D', \mathbf{u}], \star)$ and $([G, D, \mathbf{u}], *)$ coincide. Indeed, since $v_{a_j} \star v_{a_i} = v_{a_j * a_i}$ then it follows straightforward that, for every $a_i, a_j \in D$, $v_{a_j} \star v_{a_i} \in D'$ if and only if $a_j * a_i \in D$. □

At this point we have seen that left Hadamard groups are in one-to-one correspondence with HFP-codes. The following result shows that the correspondence also holds for right Hadamard groups.

Proposition 90. *Let C be a* HFP*-code of length $4n$ and let D_1 be the set of codewords with a zero in the first coordinate. Then $([C, D_1, \boldsymbol{u}], \cdot)$ is a right Hadamard group.*

Proof. Write $D_1 = \{a_1, a_2, \ldots, a_{4n}\}$. We shall prove that $([C, D_1, \mathbf{u}], \cdot)$ satisfies the properties of Remark 59. The first, second, and fourth properties follow straightforward from the fact that $([C, D_1, \mathbf{u}], \cdot)$ is a left Hadamard group (see Proposition 87).

The elements in $D_1 \cap D_1 \cdot x$ are those of the form $\{a_i + \pi_{a_i}(x) : a_i \in D_1\}$ with the first coordinate equal to zero. Now, for every $a_i \in D_1$, the first coordinate of the elements of the form $a_i + \pi_{a_i}(x)$ has the same value than the first coordinate of the elements of the form $\pi_{a_i}(x)$. Remind from Proposition 80 that $\pi_{a_i}(e_i) = e_1$ and, therefore we have that $\pi_{a_i}^{-1}(e_1) = e_i$, for every i. Thus, the first coordinate of the vectors in $\{\pi_{a_i}(x) : a_i \in D_1\}$ are exactly the values of every coordinate of the vector x. Hence, if $x \notin \{\mathbf{e}, \mathbf{u}\}$ then $|D_1 \cap D_1 \cdot x| = 2n$ since x has half zeros and half ones. □

Corollary 91. *If $([G, D, \boldsymbol{u}], *)$ is a left Hadamard group then $([G, D, \boldsymbol{u}], *)$ is a right Hadamard group. Furthermore, $([G, D^{-1}, \boldsymbol{u}], *)$ and $([G^{op}, D, \boldsymbol{u}], *)$ are left and right Hadamard groups.*

Proof. If $([G, D, \mathbf{u}], *)$ is a left Hadamard group then it follows from Proposition 88 and Proposition 90 that $([G, D, \mathbf{u}], *)$ is a right Hadamard group.

Now, since $([G, D, \mathbf{u}], *)$ is a right Hadamard group then $([G^{op}, D, \mathbf{u}], \diamond)$ is a left Hadamard group. Now, $([G^{op}, D, \mathbf{u}], *)$ is a left Hadamard group and using the isomorphism $\phi : G^{op} \to G$ such that $\phi(g) = g^{-1}$ we obtain that $([G, D^{-1}, \mathbf{u}], *)$ is a left Hadamard group. □

Remark 92. *Let $(C,\cdot)$ be a* HFP*-code. It is worth mentioning that the Hadamard groups $([C^{op}, D_1, \boldsymbol{u}], \diamond)$ and $([C, D_1^{-1}, \boldsymbol{u}], \cdot)$ provide the same binary code.*

Further than the connections between Hadamard groups and HFP-codes, we want to show two important properties concerning the algebraic group structure of the HFP-codes. Firstly, Ito [I94, Prop. 7] showed that no Hadamard group G of order $2^s n'$, n' odd and $s > 3$, contains a 2-Sylow cyclic group. We generalise this result by seeing that there is no HFP-code with a subjacent cyclic group structure.

Proposition 93. *Let C be a* HFP*-code of length $4n$. Then C can not be a cyclic group.*

Proof. Let C be a HFP-code of order of length $4n$ and $8n$ elements. Deny the proposal, so there exists an element $a \in C$ satisfying $C = \langle a \rangle$ and therefore $\Pi = \langle \pi_a \rangle$. Since $\mathbf{u} \in C$ and $\mathbf{u}$ is the unique element of order two, then $a^{4n} = \mathbf{u}$.

Let D_1 be the set of elements in C with a zero in the first position. Write $D_1 = \{a \cdot g_1, a^2 \cdot g_2, \ldots, a^{4n} \cdot g_{4n}\}$, where $g_i = \mathbf{e}$ or $g_j = \mathbf{u}$. Consider the ordered sequence $\{g_1, g_2, \ldots, g_{4n}\}$. Note that if $g_1 = g_{4n}$ (respectively $g_1 \neq g_{4n}$), then the changes in the sequence, form one to other value in $\{\mathbf{e}, \mathbf{u}\}$, occur an even (respectively, an odd) numbers of times. When a change occurs between g_i and g_{i+1} then $a \cdot a^i \cdot g_i$ does not belong to D_1. Moreover, since a^{4n} is of order at most two and $a^{4n} \in \{\mathbf{e}, \mathbf{u}\}$, we have $a^{4n} = g_{4n}$ and therefore, $a \cdot a^{4n} \cdot g_{4n} = a \in D_1$ if and only if $g_1 = \mathbf{e}$. Hence, $|D_1 \cap a \cdot D_1|$ is odd, which contradicts the fact that, from Proposition 79, $|D_1 \cap a \cdot D_1|$ should be even. □

Ito [I94, Coro. 1] proved that any Hadamard group contains a 2-Sylow subgroup which is a generalised quaternion group. Although we saw the correspondences between HFP-codes and Hadamard groups we think that we can present an alternative prove for HFP-codes.

Lemma 94. *[B55] Any 2-group (group whose order is a power of two) with only one involution must be cyclic or generalised quaternion group.*

Proposition 95. *Let C be a* HFP*-code of length $4n$, such that $\boldsymbol{u} \in C$ is the only involution in C. Then a Sylow 2-subgroup of C is a generalized quaternion group for $n \geq 2$.*

Proof. Denote by N be the subgroup generated by $\mathbf{u}$. N is of order two and it is a normal subgroup of $(C, \cdot)$; further, N is central. Let H be the quotient C/N. Since C has a unique involution, from Proposition 95 the Sylow 2-subgroup of C must be cyclic or generalised quaternion groups. Denote by P the Sylow 2-subgroup of C, and we see that the group P/N is a Sylow 2-subgroup of H, is cyclic or generalised quaternion. The statement follows from Proposition 93. □

In Section 2.1, we claim that it is difficult to decide whether a code is propelinear or not; it is also hard to decide whether a binary Hadamard code has a full propelinear structure. To analyse the existence of HFP-codes of high orders it is important, firstly, to review if there is cocyclic Hadamard matrices for such orders. In [H07] it can be found that every Hadamard matrix of order $4n \leq 20$ is cocyclic. Furthermore, when $4n \leq 200$, it is known that there is a cocyclic construction for every order except for $4 \cdot 47 = 188$. Section 3.3 born as a justification of Chapter 4 and Chapter 5 and, in which we show several examples of HFP-codes and we also compare the family of Hadamard propelinear codes with the family of HFP-codes.

3.3 Examples

We divided the current section in two different subsections. In the first one, we deal with the HFP-codes with a subjacent group structure of eight elements. In the last one, we show some examples of HFP-codes with a subjacent nonabelian group structure of higher order.

3.3.1 Trivial examples

Concerning the abelian group structures of eight elements we finnd the C_8, $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ groups, where C_8 is the cyclic group of 8 elements. Firstly, from Proposition 93 we know that there is no HFP-codes with a subjacent C_8 group structure. Furthermore, in Example 73 we show an example of a non translation invariant HFP-code with a subjacent $\mathbb{Z}_2 \times \mathbb{Z}_4$ group structure. The following example consists of a HFP-code with a subjacent $\mathbb{Z}_2^3$ group structure.

Example 96. *Let C be a* HFP*-code with a subjacent group structure* $\mathbb{Z}_2 \times$

$\mathbb{Z}_2 \times \mathbb{Z}_2$, *where* $C = \langle a, b, \boldsymbol{u} \rangle$ *with*

$$\begin{array}{l} a = (1,1,0,0), \pi_a = (1,2)(3,4), \\ b = (0,1,1,0), \pi_b = (1,4)(2,3), \\ \boldsymbol{u} = (1,1,1,1), \pi_{\boldsymbol{u}} = Id. \end{array}$$

The Hadamard code generated by a, b *and* $\boldsymbol{u}$ *is the binary linear Hadamard code of eight elements so* $r = k = 3$. *Further, if we take* $e_1 = (1,0,0,0) \in \mathbb{Z}_2^4$ *then we have*

$$d(a, \boldsymbol{e}) = 2, \text{ but } d(a \cdot e_1, \boldsymbol{e} \cdot e_1) = d((1,0,0,0),(1,0,0,0)) = 0, \tag{3.2}$$

and, consequently, C *is not translation invariant.*

On the nonabelian groups of eight elements we find the dihedral group and the quaternion group. Ito [I94] showed that there is no Hadamard group with a subjacent dihedral group structure, so there is no HFP-code with a subjacent dihedral group. Now, we analyse the case of the Q_8-code. Remind that the quaternion group is presented by

$$Q_8 = \langle a, b : a^4 = \mathbf{e}, a^2 = b^2 = \mathbf{u}, ab = ba^{-1} \rangle. \tag{3.3}$$

Lemma 97. *Let* $(C, \cdot)$ *be a* HFP*-code of order* 8. *If* C *is presented by* $\langle a, b : a^4 = \boldsymbol{e}, a^2 = b^2 = \boldsymbol{u}, ab = ba^{-1} \rangle$ *then the unique quaternion* HFP*-structure for* C *is given by*

$$\begin{array}{ll} a = (0,1,0,1), & \pi_a = (1,2)(3,4), \\ b = (0,1,1,0), & \pi_b = (1,3)(2,4). \end{array} \tag{3.4}$$

Furthermore, this presentation has the minimum value γ *for which it is possible the representation of a quaternion code in* $\mathbb{Z}_2^\gamma$. *This structure is unique (up to isomorphism in* Q_8*).*

Proof. Let C be a HFP-code with a subjacent $Q_8 = \langle a, b \rangle$ group structure in terms of (3.3). Consider the map $Q_8 \to \mathbb{Z}_2^4 \times \mathcal{S}_4$ which sends an element $a \in Q_8$ to (v_a, π_a) where v_a is the representing vector of a in $\mathbb{Z}_2^4$ and π_a its associated permutation. Let us denote by x, further than an element of Q_8, its correspondent vector in $\mathbb{Z}_2^4$. First of all, if we want C to be a propelinear code then, for any $x, y, z \in C$ it follows that $d(x, y) = d(x \cdot z, y \cdot z)$, so the elements in each pair $(a, a^3), (b, a^2b), (ab, a^3b)$ have the same weight. Since $d(a^3b, \mathbf{e}) = d(a, b) = d(a, \mathbf{e}) + d(b, \mathbf{e}) - 2i(a, b)$, where $i(z, y)$ means the number of binary nonzero coordinates in the intersection of the supports of z and y,

then the weight values of the three pairs are all even or two odd and one even. Assume $d(a, \mathbf{e}) = d(a^3, \mathbf{e}) = 2$. Furthermore, from $a^2 = a + \pi_a(a)$ then $d(a^2, \mathbf{e})$ is even; moreover $d(a^2, \mathbf{e}) = 4$. Indeed, if the three pairs have even weight then it follows straightforward; in the case of two of these three pairs have odd weight, if we take the pair with the weight value one, for instance (b, b^3), then $\mathrm{Supp}\,(b) \subset \mathrm{Supp}\,(a)$ or $\mathrm{Supp}\,(b) \subset \mathrm{Supp}\,(a^3)$ so π_{ab} or π_{a^3b} is the identity permutation contradicting that ab or a^3b are of order four. Now, if we take the pair of odd weight, for instance (b, b^3) then $4 = d(b^2, \mathbf{e}) = d(b^3, b) = d(b^3, \mathbf{e}) + d(b, \mathbf{e}) - 2i(b^3, b) = d(b^3, \mathbf{e}) + d(b, \mathbf{e}) - 2\mathrm{wt}(\mathbf{u} + b + b^3) \leq 2$, and hence, for any $x \in Q_8 \setminus \{\mathbf{e}, a^2\}$ we have $d(x, \mathbf{e}) = 2$.

Let $\Pi = \{\pi_x : x \in Q_8\}$ and let $\{i, j, k, l\}$ be the set of positions corresponding to each coordinate in the vector space $\mathbb{Z}_2^4$. Firstly, $\mathbf{e} = (0, 0, 0, 0)$, $a^2 = \mathbf{u} = (1, 1, 1, 1)$ and $\pi_{\mathbf{e}} = \pi_{\mathbf{u}} = I$. Assume $\mathrm{Supp}(a) = \{i, j\}$ and $\pi_a = (i, l)(j, k)$. Since $\pi_{x^2} = Id$, for any $x \in Q_8$, Π is a commutative group of order four. The permutation π_b can be either $(i, k)(j, l)$ or $(i, j), (k, l)$, otherwise, ab is not of order four. Assume $\pi_b = (i, k)(j, l)$ and $\mathrm{Supp}\,(b) = \{i, l\}$, otherwise, consider the automorphism in Q_8 which takes b to a^2b. Finally, $\pi_b = \pi_{a^2b}$, and we can compute $\mathrm{Supp}\,(ab) = \{j, l\}$ with $\pi_{ab} = (i, j)(k, l)$ and $a^3b = ab + \mathbf{u}$ with $\pi_{ab} = \pi_{a^3b}$. Finally, for any two possible propelinear presentations C_1 and C_2 for Q_8, there is a $\pi \in \mathcal{S}_4$ such $\pi(C_1) = C_2$. □

Although Proposition 64 ensures that there is no dihedral HFP-code, it does not mean that there is no Hadamard propelinear codes with a subjacent dihedral group. In fact, if we consider the code $(C, \cdot)$ with the elements

$$\begin{array}{llll} \mathbf{e} = (0,0,0,0), & \pi_{\mathbf{e}} = Id, & a = (1,1,0,0), & \pi_a = (14)(23), \\ a^2 = (1,1,1,1), & \pi_{a^2} = Id, & a^3 = (0,0,1,1), & \pi_{a^3} = (14)(23), \\ b = (0,1,1,0), & \pi_b = (14)(23), & ab = (1,0,1,0), & \pi_{ab} = Id, \\ a^2b = (1,0,0,1), & \pi_{a^2b} = (14)(23), & a^3b = (0,1,0,1), & \pi_{a^3b} = Id, \end{array}$$

then $(C, \cdot)$ is a dihedral Hadamard propelinear code with eight elements. Since $\pi_{ab} = I$ then C is not full propelinear. Moreover, C is neither translation invariant; indeed, if consider the vector $e_2 = (0, 1, 0, 0) \in \mathbb{Z}_2^4$, then we have $d(b, \mathbf{e}) = 2$ but $d(b \cdot e_2, \mathbf{e} \cdot e_2) = d((0, 1, 0, 0), (0, 1, 0, 0)) = 0$.

3.3.2 Non trivial examples

It is well-known that there are five nonequivalent Hadamard matrices of length 16 which can be described attending to the rank, r, and dimension of the kernel, k, $(r, k) \in \{(5, 5), (6, 3), (7, 2), (8, 1), (8, 2)\}$. The $(5, 5)$ Hadamard

matrix corresponds to a linear code while the $(6,3)$ Hadamard matrix can be regarded as a $\mathbb{Z}_2\mathbb{Z}_4$-linear code and the other three cannot be realised as $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, [FP$^+$10]. However, the $(7,2)$ can be realized as a $\mathbb{Z}_2\mathbb{Z}_4Q_8$-code, more specifically, as a pure Q_8-code [RR13]. The last two Hadamard codes $(8,2),(8,1)$ justify the study of HFP-codes, and more concretely, of those which have a generalised quaternion as a subjancent group structure.

Example 98. *Let Q_{32} be the group of 32 elements presented by $\langle a,b : a^{16} = \boldsymbol{e}, a^8 = b^2 = \boldsymbol{u}, ab = ba^{-1}\rangle$. Consider the elements $a,b \in Q_{32}$ and their corresponding permutations $\pi_a, \pi_b \in \mathcal{S}_{16}$.*
The code $(C_1,\cdot)$ with $(r,k) = (8,2)$ can be computed from $\langle a,b\rangle$, where :

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

The code $(C_2,\cdot)$ with $(r,k) = (8,1)$ can be computed from $\langle a,b\rangle$, where:

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

The previous codes C_1 and C_2 are not translation invariant. In fact, take the vector $e_{14} = (0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0)$ and for both vectors $a_{C_1} = a \in C_1$ and $a_{C_2} = a \in C_2$ we have that

$$d(\boldsymbol{e}, a_{C_1}) = d(\boldsymbol{e}, a_{C_2}) = 8, \text{ but } d(\boldsymbol{e}\cdot e_{14}, a_{C_1}\cdot e_{14}) = d(\boldsymbol{e}\cdot e_{14}, a_{C_2}\cdot e_{14}) = 10.$$

Further than HFP-codes with a subjacent generalized quaternion group structure, in Chapter 4 we deal with those HFP-codes with a subjacent group structure presented by $Q_{8n} = \langle a,b : a^{4n} = b^2 = \mathbf{u}, ab = ba^{-1}\rangle$, for any natural n. This family of codes will be termed HFP-*codes of type Q*.

Example 99. *Let C be the* HFP-*code with a subjacent Q_{24} group structure where*

$$\begin{aligned}
a &= (1,1,0,1,0,0,1,1,1,0,0,0),\\
b &= (1,1,0,1,0,0,1,1,1,0,0,0),\\
\pi_a &= (1,2,\ldots,6)(7,8,\ldots,12),\\
\pi_b &= (1,12)(2,11)\ldots(6,7).
\end{aligned}$$

The code C has rank $r = 11$ and dimension of the kernel $k = 1$. Now, if we take the vector $e_3 = (0,0,1,0,0,0,0,0,0,0,0,0) \in \mathbb{Z}_2^{12}$ then we see that

$$d(b, \boldsymbol{e}) = 6, \text{ but } d(b \cdot e_3, \boldsymbol{e} \cdot e_3) = 8,$$

so C is not a translation invariant code.

Another interesting family of HFP-codes with a subjacent nonabelian structure is the family which can be realised by a $C_n \times Q_8$ group structure, where C_n is the cyclic group of n elements, n odd. This family of codes will be studied on Chapter 5 and they will be termed HFP-*codes of type CQ*. The following example shows the existence of this family of HFP-codes.

Example 100. *Let C be a* HFP-*code with a subjacent $C_3 \times Q_8$ presented by $C = \langle a, b, c : a^4 = e, a^2 = b^2, ab = ba^{-1}, c^3 = e, ac = ca, bc = cb \rangle$ where*

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

Then the code C has rank $r = 11$, $k = 1$ and $\Pi = \langle \pi_a, \pi_b, \pi_c \rangle \simeq C_2^2 \times C_3$. This code is not a translation invariant propelinear code. In fact, take c and the vector $e_1 = (1,0,0,0,0,0,0,0,0,0,0,0)$ and observe that

$$d(\boldsymbol{e}, c) = 6, \quad \text{but} \quad d(\boldsymbol{e} \cdot e_1, c \cdot e_1) = 8$$

Flannery [F97] showed that any Williamson type Hadamard matrix of order $4n$, for any n positive odd integer, belongs to one of the following classes.

- Cocyclic over $C_2^2 \times C_n$ with Hadamard group $C_n \times Q_8$.
- Cocyclic over D_{4n} with Hadamard group Q_{8n}.

It is worth mentioning that in [F97, BH95, I94] it is proved that most of Williamson Hadamard matrices of orders $2^s n$, n odd and $s \geq 3$, are cocyclic over $D_{2^s n}$ with Hadamard group $Q_{2^{s+1} n}$. Additional constructions can be seen in [AA$^+$16, AR$^+$15]. Recall that Schmidt [S99] verified the Ito's conjecture of the existence of Hadamard groups of type Q, throughout relative $(4n, 2, 4n, 2n)$-difference sets, $n \leq 46$ odd, such that $2n - 1$ or $4n - 1$ is a prime power.

Chapter 4

HFP-codes of type Q

In Section 2.5 we introduced Hadamard groups and we focused, in particular, on those Hadamard groups of type Q [I97]. In Chapter 3 we deal with the equivalences between Hadamard groups and HFP-codes. The aim of the current chapter is to describe the combinatorial properties of the HFP-codes of type Q and length $4n = 2^s n'$, n' odd, for which we compute the values of the rank and the dimension of the kernel. More specifically, when $s = 2$ we prove that the the values of the rank r and the dimension of the kernel k are $4n - 1$ and 1, respectively. When $s > 2$ we show that k can be either 1 or 2; concerning the rank, we show that $r \leq 2n$ and, in addition, we prove that we can compute explicitly the rank of those HFP-codes of type Q whose dimension of the kernel is $k = 2$. We also contribute with an iterative construction which allows to duplicate any HFP-code of type Q and length $4n$ with $k = 2$ preserving its HFP-structure and the dimension of the kernel. In particular, we prove that if we duplicate any HFP-code of type Q with rank $r = 2n$ and $k = 2$ then we obtain a HFP-code of type with rank $4n$. We also deal with the transpose code C^T of any HFP-code C of type Q and we prove that, if C has $k = 2$ then C^T has dimension of the kernel equal to 1. This work enables to reinforce the Ito's conjecture about the existence of Hadamard groups of type Q and length $4n$, for any natural n [I97]. Finally, we comment on the computational results on HFP-codes of type Q in MAGMA and we compare them with those which have been obtained from relative difference sets and cocyclic Hadamard matrices.

The compendium of the results appearing in Chapter 3 and in Chapter 4 constitutes the article "Hadamard full propelinear codes of type Q; rank and kernel" which was published in *Designs, Codes and Cryptography* [RS17].

4.1 Properties of HFP-codes of type Q

In the current section, we deal with HFP-codes of type Q and length $4n = 2^s n'$, n' odd. More concretely, we study their HFP-structure and we state general bounds for the values of the rank and dimension of the kernel for general Hadamard codes. We also deal with submatrices in a Hadamard matrix of any HFP-code of type Q.

Definition 101. *Let C be a* HFP*-code of length $4n = 2^s n'$, n' odd. We say that C is a* HFP*-code of type Q when C can be presented as*

$$\langle a, b : a^{4n} = \boldsymbol{e}, a^{2n} = b^2 = \boldsymbol{u}, b^{-1}ab = a^{-1} \rangle, \tag{4.1}$$

where $\boldsymbol{e}$ and $\boldsymbol{u}$ are, respectively, the all-zero vector and the all-one vector.

Take into account that if $n' = 1$ then $4n = 2^s$ and C would be a generalised quaternion group. Hence, HFP-codes of type Q generalises the case of HFP-codes with a subjacent generalised quaternion group, which were previously studied by Ito [I94, I97]. The set of $8n$ elements of any HFP-code C of type Q with length $4n$ is

$$C = \{\mathbf{e}, a, a^2, \ldots, a^{4n-1}, b, ab, a^2b, \ldots, a^{4n-1}b\}. \tag{4.2}$$

The following result indicates the full propelinear sturcture that we will consider, from now on, on any HFP-code of type Q. Firstly, let us denote by $\{1, 2, \ldots, 4n\}$ the set of coordinates of the vectors in $\mathbb{Z}_2^{4n}$.

Proposition 102. *Let C be a* HFP*-code of type Q and length $4n = 2^s n'$. If $C = \langle a, b \rangle$, then, up to isomorphism, we can assume*

i) $\pi_a = (1, 2, \ldots, 2n)(2n+1, 2n+2, \ldots, 4n)$.

ii) $\pi_b = (1, 4n)(2, 4n-1)\ldots(2n, 2n+1)$.

Proof. Let $C = \langle a, b \rangle$ be a HFP-code of type Q and length $4n = 2^s n'$ with n' odd and let $\Pi = \{\pi_x : x \in C\}$ be the associated permutation group of C.

Since the element a is of order $4n$ then we have $a^{2n} = \mathbf{u}$ which implies that π_a is of order $2n$. Otherwise, if there exists a natural j with $j < 2n$, such that π_a^j is the identity permutation then $a^{2j} = a^j + \pi_{a^j}(a^j) = a^j + \pi_a^j(a^j) = \mathbf{e}$ which contradicts that a has order $4n$. The full propelinear condition requires π_x to not fix any coordinate when $x \in C \setminus \{\mathbf{e}, \mathbf{u}\}$. Hence, π_a which has order $2n$, consists of two disjoint cycles of length $2n$ and therefore, we can assume $\pi_a = (1, 2, \ldots, 2n)(2n+1, \ldots, 4n)$, up to isomorphism.

On the other hand, since $b^2 = \mathbf{u}$ then the permutation π_b is of order 2. From the full propelinearity π_b consists of a composition of $2n$ disjoint transpositions. If $\pi_a = (1, 2, \ldots, 2n)(2n+1, 2n+2, \ldots, 4n)$ then each transposition of π_b sends a coordinate in the first cycle of π_a to a coordinate in the second cycle of π_a. Indeed, if π_b moved the position 1 to the position i, $1 \leq i \leq 2n$, then $\pi_{a^{2n-i}b}(1) = \pi_{a^{2n-i}}\pi_b(1) = \pi_{a^{2n-i}}(i) = 1$ against the full propelinear condition. Now, if we assume that π_b moves the position 1 to any position i, $i \geq 2n+1$, then π_b is uniquely determined. In fact, since $\pi_b\pi_a = \pi_a^{-1}\pi_b$ then $\pi_a\pi_b\pi_a = \pi_b$ and $\pi_b(2n) = \pi_a\pi_b\pi_a(2n) = \pi_a\pi_b(1) = \pi_a(i) = i+1$ and so on. Hence, $\pi_b = (1, i)(2n, i+1)(2n-1, i+2)\ldots(2, i-1)$. We can assume $\pi_b = (1, 4n)(2, 4n-1)\ldots(2n, 2n+1)$, up to isomorphism. □

Lemma 103. *Let $(C, \cdot)$ be a propelinear code of length $4n$. For any $a \in C$, we can write*

$$a^i = \sum_{j=0}^{i-1} \pi_{a^j}(a), \text{ for every } i. \tag{4.3}$$

Furthermore, if $C = \langle a, b\rangle$ is a HFP*-code of type Q then $\Pi = C/\langle \mathbf{u}\rangle$ is the dihedral group $\mathcal{D}_{2n}$.*

Proof. Firstly, $a = \pi_{a^0}(a)$, $a^2 = a \cdot a = a + \pi_a(a)$ and, since π_a is a permutation, $a^3 = a \cdot a \cdot a = a + \pi_a(a + \pi_a(a)) = a + \pi_a(a) + \pi_{a^2}(a)$. By induction, assume that $a^i = \sum_{j=0}^{i-1} \pi_{a^j}(a)$ and then $a^{i+1} = a \cdot a^i = a + \pi_a(\sum_{j=0}^{i-1} \pi_{a^j}(a)) = \sum_{j=0}^{i} \pi_{a^j}(a)$.

On the other hand, for any $i \in \{1, 2, \ldots, 4n\}$ we have that $a^{2n} = (a^i b)^2 = \mathbf{u}$. This implies that π_a and $\pi_{a^i b}$ have orders $2n$ and 2, respectively. Furthermore, from the equalities $\pi_{ab} = \pi_a\pi_b = \pi_b\pi_a^{-1} = \pi_b\pi_{a^{-1}} = \pi_{ba^{-1}}$ and from the fact that $|\Pi| = 4n$ it follows that $\Pi \simeq \mathcal{D}_{2n}$. □

Now, we introduce the polynomial notation which will be helpful during the current chapter. Let $\mathbb{Z}_2[x]$ be the polynomial ring with coefficients over $\mathbb{Z}_2$ and consider the $\mathbb{Z}_2[x]$-module $\mathbb{Z}_2[x]/(1+x^{2n}) \times \mathbb{Z}_2[x]/(1+x^{2n})$. The elements in $\mathbb{Z}_2[x]/(1+x^{2n}) \times \mathbb{Z}_2[x]/(1+x^{2n})$ can be written as $v(x) = (v_1(x), v_2(x))$, where $v_1(x), v_2(x) \in \mathbb{Z}_2[x]/(1+x^{2n})$. Hence, there is correspondence between the elements of $\mathbb{Z}_2^{2n} \times \mathbb{Z}_2^{2n}$ and the elements of $\mathbb{Z}_2[x]/(1+x^{2n}) \times \mathbb{Z}_2[x]/(1+x^{2n})$. In fact, we can associate the vector $(v_1, v_2, \ldots, v_{2n} | v_{2n+1}, v_{2n+2}, \ldots, v_{4n}) \in \mathbb{Z}_2^{2n} \times \mathbb{Z}_2^{2n}$ to the polynomial

$$(v_1 + v_2 x + v_3 x^2 + \ldots + v_{2n} x^{2n-1}, v_{2n+1} + v_{2n+1} x \ldots + v_{4n} x^{2n-1})$$

Now, let C be a HFP-code of type Q of length $4n$ generated by a and b in terms of Proposition 102. Let v be a vector in $\mathbb{Z}_2^{2n} \times \mathbb{Z}_2^{2n}$, where $v =$

$v(x) = (v_1(x), v_2(x))$. The action of the permutation π_a, corresponding to the generator a, over v, denoted by $\pi_a(v)$, is in correspondence with

$$xv(x) = (xv_1(x) \pmod{x^{2n}+1}, xv_2(x) \pmod{x^{2n}+1}). \tag{4.4}$$

For any $i < 2n$ we have that the polynomial $1+x+\ldots+x^{i-1}$ in $\mathbb{Z}_2[x]/(1+x^{2n})$ corresponds to the polynomial $\frac{1+x^i}{1+x}$. Write the generator a as $a(x) = (a_1(x), a_2(x))$. We know, from Lemma 103, that $a^i = \sum_{j=0}^{i-1} \pi_{a^j}(a)$ and, it is in correspondence with

$$(\tfrac{1+x^i}{1+x}a_1(x) \pmod{x^{2n}+1}, \tfrac{1+x^i}{1+x}a_2(x) \pmod{x^{2n}+1}). \tag{4.5}$$

On the other hand, let $p(x) \in \mathbb{Z}_2[x]$ with degree at most $2n-1$. We call $p(x)^* = x^{2n}p(\frac{1}{x})$. The polynomial $p(x)^*$ is not exactly the reciprocal polynomial of $p(x)$ but coincides with it when $p(x)$ has maximum degree $2n-1$. The action of π_b, corresponding to the generator b, over a vector $v \in \mathbb{Z}_2^{2n} \times \mathbb{Z}_2^{2n}$, where $v = v(x) = (v_1(x), v_2(x))$, can be thought as

$$\pi_b(v) = v^*(x) = (v_2^*(x), v_1^*(x)). \tag{4.6}$$

Proposition 104. *Let $C = \langle a, b\rangle$ be a* HFP*-code of type Q and length $4n = 2^s n'$ with n' odd. Then, up to equivalence, knowing the value of a is enough to define b uniquely, up to complementary.*

Proof. Let $C = \langle a, b\rangle$ be a HFP-code of type Q in terms of Proposition 102. From $ab = ba^{-1}$ we can write $a + \pi_a(b) = b + \pi_b(a^{-1})$ and from the equalities $\pi_b(a^{-1}) = \pi_b\pi_a^{-1}(a) = \pi_b\pi_{a^{-1}}(a) = \pi_a\pi_b(a)$ it follows that $b + \pi_a(b) = a + \pi_{ab}(a)$. Using polynomials, from (4.4) and (4.6), we can write $(1+x)b_i(x) = a_i(x) + xa_{i'}^*(x) \pmod{x^{2n}-1}$, for $i, i' \in \{1,2\}$, $i \neq i'$. Polynomials $a_i(x) + xa_{i'}^*(x) \pmod{x^{2n}-1}$, $i, i' \in \{1,2\}$ and $i \neq i'$ are multiples of $(1+x)$, so $b_i(x) = \frac{a_i(x)+xa_{i'}^*(x) \pmod{x^{2n-1}}}{1+x}$ for $i, i' \in \{1,2\}$ and $i \neq i'$, and $b(x) = (b_1(x), b_2(x))$. Finally, $(1+x)b(x) = (1+x)(b(x)+\mathbf{u}(x))$ and since $\pi_b(b) = b+\mathbf{u}$ it follows that $b_2(x) = b_1^*(x) + \mathbf{u}(x)$ and the statement is proved. □

Remark 105. *By fixing the permutations π_a and π_b, as well as in Proposition 102, any* HFP*-code of type Q can be computed by knowing only the generator a.*

The following properties, concerning the rank and dimension of the kernel, are valid for general Hadamard codes. Remind that the kernel $K(C)$ of a binary code C of length n, consists of the vectors in $\mathbb{Z}_2^n$ which keeps the code invariant under translation; hence, $K(C) = \{x \in \mathbb{Z}_2^n : x + C = C\}$. Furthermore, if $\mathbf{e} \in K(C)$ then $K(C)$ is a vector space. On the other hand, the rank of a binary code C is defined as the dimension of the span $\langle C\rangle$.

Lemma 106. *[PR+06c] Let C be a Hadamard code of length $2^s n'$, where n' is odd and $n' \neq 1$. If the dimension of the kernel is $k \geq 1$ then $s \geq k+1$.*

Lemma 107. *[AK92, Th. 2.4.1 and Th. 7.4.1] Let C be a Hadamard code of length $4n = 2^s n'$, where n' is odd.*

(i) If $s \geq 3$ then the rank of C is $r \leq 2n$, with equality if $s = 3$.

(ii) If $s = 2$ then $r \geq 4n - 1$.

Lemma 108. *Let C be an Hadamard code of length $2^s n'$. The rank r of C fulfills $r \leq \frac{2^{s+1}n'}{2^k} + k - 1$, where k is the dimension of the kernel.*

Proof. Let k be the dimension of the the kernel $K(C)$, then we can see C as a disjoint union of, at the most, $\frac{2^{s+1}n'}{2^k}$ cosets of $K(C)$. Hence, the rank of C will be at the most $r \leq \frac{2^{s+1}n'}{2^k} - 1 + k$. □

Proposition 109. *Let C be a* HFP*-code of type Q and length $4n = 2^s n'$ with n' odd. Then*

1. *Code C is linear if and only if the following equalities are true*

$$4n = 2^s, \text{ and } r = k = s + 1.$$

2. *If C is not linear then $a \notin K(C)$.*

3. *If C is not linear then the dimension of the kernel is $k \in \{1, \ldots, s\}$. If $n' \neq 1$ then $k \leq s - 1$.*

4. *If C is not linear and $s = 2$ then $r = 4n - 1$ and $k = 1$.*

Proof. First item is straightforward.

For the second item, deny the statement, so assume that $a \in K(C)$. Then $\langle a \rangle \subset K(C)$ and so $|C/K(C)| \leq 2$. When $|C/K(C)| = 1$ it follows that $C = K(C)$. In the case of $|C/K(C)| = 2$ then there exists an element $c \in C$ such that $C = K(C) \cup (c + K(C))$. Now, we have that $c + x' \in C$, for every $x' \in C$, which implies that $c \in K(C)$ and, therefore, that $C = K(C)$ contradicting the condition of nonlinearity of C. Indeed, if $x' = y + c$, with $y \in K(C)$, then $c + x' = y \in C$ and, if $x' = y \in K(C)$, with $y \in K(C)$, then $c + x' = c + y \in C$.

For the third item, we have that kernel $K(C)$ is a subgroup of C and also a binary linear space, so $k = |K(C)|$ is a power of two and a divisor of $8n = 2^{s+1}n'$. The maximal case, so when $k = 2^{s+1}$ is unreachable. Otherwise,

all elements of even order will be into de kernel, for instance $b, ba \in K(C)$ which leads to $a \in K(C)$ contradicting the nonlinearity of C. When $n' \neq 1$ then, from Lemma 107, the case b $k = s$ is also unreachable. Hence, the item follows straightforward.

For the fourth item we know from Lemma 107 that $r \geq 4n-1$. Assuming that $r = 4n$ we will have that all elements $\{a^i, a^i b\}$, for $i \in \{1, \ldots, 2n\}$, are linearly independent, which is impossible since $\sum_i (a^i + a^i b) \in \{\mathbf{e}, \mathbf{u}\}$. Indeed, $\sum_{i=1}^{2n} \pi_{a^i}(\mathbf{e}_j) = \mathbf{u}'$, where $\mathbf{u}'$ is the vector with ones in all the first $2n$ coordinates and zeros elsewhere if the unit elements $\mathbf{e}_j$ has the support into the first $2n$ coordinates, otherwise $\mathbf{u}'$ is the vector with ones in all the last $2n$ coordinates and zeros elsewhere. Hence, $\sum_i (a^i + a^i b) = \sum_i a^i + \sum_i a^i b = \sum_i \pi_{a^i}(b) \in \{\mathbf{e}, \mathbf{u}\}$. Thus, $r \leq 4n-1$ and therefore $r = 4n-1$. Finally, since $\mathbf{u} \in K(C)$ and, from Lemma 108, it follows that $k = 1$. The fourth item is proven. □

Let $C = \langle a, b \rangle$ be a HFP-code of type Q and length $4n$ and, let H and D_1 be the Hadamard matrix and the ordered set of Proposition 80, respectively. According to Proposition 80 we give a suitable order for D_1 in order to analyse some component submatrices in H.

On one hand, $C = D_1 \cup D_1 + \mathbf{u}$ and, for every $x \in C$, we have that $\pi_x = \pi_{x+\mathbf{u}}$. Now, let us we denote by $x \in C$ the representative element in $\{x, x+\mathbf{u}\}$ lying into D_1. In other words, we denote by x the element in $\{x, x+\mathbf{u}\} \cap D_1$. Now, from Proposition 102 we have, for every $i \in \{0, 1, \ldots, 2n-1\}$,

- $\pi_b(e_{4n-i}) = e_{1+i}$.
- $\pi_{a^i}(e_1) = e_{1+i}$ and $\pi_{a^i}(e_{4n-i}) = e_{4n}$.
- $\pi_{ba^i}(e_{4n-i}) = \pi_b \pi_{a^i}(e_{4n-i}) = \pi_b(e_{4n}) = e_1$.

Hence, since $\pi_b \pi_{a^i} = \pi_{a^{-i}} \pi_b$ we can write D_1, based on Proposition 80, as

$$D_1 = \{\mathbf{e}, a^{2n-1}, a^{2n-2}, \ldots a^2, a, ab, a^2 b, \ldots, a^{2n-1} b, b\}. \tag{4.7}$$

On the other hand, we know from Proposition 102, that any element $x \in C$ can be written as $x = (x_1, x_2)$, where x_1 and x_2 correspond to the first and to the last $2n$-coordinates of the vector x, respectively. Hence, the Hadamard matrix H of any HFP-code of type Q, defined in Proposition 80, can be written as

$$H = \left(\begin{array}{c|c} H_1 & H_2 \\ \hline H_3 & H_4 \end{array} \right) \tag{4.8}$$

where H_1 and H_2 are $2n \times 2n$ matrices whose rows are the first $2n$ elements of D_1 (4.7) and whose columns are those which are indexed by the first $2n$ and the last $2n$ elements of D_1, respectively. H_3 and H_4 are the matrices whose rows are the elements in last $2n$ elements of D_1 and whose columns are indexed by the first and the last $2n$ elements of D_1, respectively.

Remark 110. *The component submatrices H_1, H_2 of (4.8) are not Hadamard. To see this, write $a = (a_1, a_2)$ and consider the full propelinear codes $C_1 = \langle a_1 \rangle$ and $C_2 = \langle a_2 \rangle$ with $\pi_{a_1} = \pi_{a_2} = (1, 2, \ldots, 2n)$. If H_1 and H_2 were Hadamard matrices then $C_1 = H_1 \cup H_1 + \boldsymbol{u}$ and $C_2 = H_2 \cup H_2 + \boldsymbol{u}$ would be cyclic* HFP*-codes contradicting Proposition 93. The matrix H_3 is neither Hadamard since H_3^T could be provided with a cyclic* HFP*-structure.*

Now we present different examples of HFP-codes of type Q attending to the values of the rank and the dimension of the kernel.

Example 111. *Take the vectors $a, b \in \mathbb{Z}_2^{20}$ and $\pi_a, \pi_b \in \mathcal{S}_{20}$ where*

$$\begin{aligned} a &= (1,1,1,1,0,1,1,1,0,0,1,0,1,0,1,0,0,0,0,0), \\ b &= (0,1,0,1,1,0,0,1,0,0,1,1,0,1,1,0,0,1,0,1), \\ \pi_a &= (1,2,\ldots,10)(11,12,\ldots,20), \\ \pi_b &= (1,20)(2,19)\ldots(10,11). \end{aligned}$$

If we compute $(C, \cdot)$, where $C = \langle a, b \rangle$, then C is a HFP*-code is of type Q and length 20. Moreover, the rank is $r = 19$ and the dimension of the kernel is $k = 1$.*

Example 112. *Take the vectors $a, b \in \mathbb{Z}_2^{24}$ and $\pi_a, \pi_b \in \mathcal{S}_{24}$ where*

$$\begin{aligned} a &= (1,1,1,1,1,1,0,1,1,0,1,0||1,0,1,0,0,1,0,0,0,0,0,0) \\ b &= (0,1,0,1,0,1,1,1,0,0,0,0||1,1,1,1,0,0,0,1,0,1,0,1), \\ \pi_a &= (1,2,\ldots,12)(13,14,\ldots,24), \\ \pi_b &= (1,24)(2,23)\ldots(12,13). \end{aligned} \tag{4.9}$$

If we compute $(C, \cdot)$, where $C = \langle a, b \rangle$, then C is a HFP*-code of type Q and length 24. Furthermore, the rank is $r = 12$ and the dimension of the kernel is $k = 2$, where $K(C) = \langle a^{23} b \rangle$ with*

$$a^{23}b = (0,1,0,1,0,1,0,1,0,1,0,1||1,0,1,0,1,0,1,0,1,0,1,0).$$

4.2 On the kernel of HFP-codes of type Q

In this section we prove that the dimension of the kernel k, of any HFP-code of type Q and length $4n = 2^s n'$ ($s > 3$ and n' odd), can be either 1 or 2. Further, we study the generator candidates of the kernel on those HFP-codes of type Q with $k = 2$. To conclude this section, we prove that the transpose code of any HFP-code of type Q with $k = 2$ has dimension of the kernel 1.

In order to reach the previous objectives, we need some properties. The following result, given in [BM$^+$12], proves that Π is a subgroup of Aut $(K(C))$.

Lemma 113. *[BM$^+$12, Lemma 5.1] Let C be a propelinear code and $K(C)$ be its kernel. Then $\pi_c(K(C)) = K(C)$, for all $c \in C$.*

Lemma 114. *Let C be a propelinear code of length $4n$. The kernel $K(C)$ is a subgroup of C and also a binary linear space.*

Proof. Since $\pi_{xy} = \pi_x \pi_y$, for any $x, y \in C$, we have $\pi_{xy} \in \mathrm{Aut}(C)$ when $\pi_x, \pi_y \in \mathrm{Aut}(C)$. Further, if $x, y \in K(C)$ then $x + y + C = x + C = C$. □

Lemma 115. *Let $C = \langle a, b \rangle$ be a* HFP*-code of type Q and length $4n = 2^s n'$, n' odd. We have $\pi_{a^i}(a^n) \neq \pi_{a^n}(a^n)$, for those a^i whose orders are different from $2^2 j$, $j > 1$ odd.*

Proof. Firstly, remind that $a^{2n} = a^n + \pi_{a^n}(a^n) = \mathbf{u}$ which implies that $\pi_{a^n}(a^n) = a^n \mathbf{u}$. Note that we can write $a^n \mathbf{u} = a^n + \mathbf{u}$. Assume j odd with $j > 1$.

Let a^i of order j (respectively, of order $2j$). If $\pi_{a^i}(a^n) = a^n + \mathbf{u}$ then we would have that $\pi_{(a^i)^j}(a^n) = \pi^j_{a^i}(a^n) = a^n + \mathbf{u}^j$ and, since j is odd, then $\pi_{(a^i)^j}(a^n) = a^n + \mathbf{u}$. But, since $(a^i)^j = \mathbf{e}$ (respectively, $(a^i)^j = \mathbf{u}$) then $\pi_{(a^i)^j} = \pi_{\mathbf{e}}$ (respectively, $\pi_{(a^i)^j} = \pi_{\mathbf{u}}$) and $\pi_{\mathbf{e}}$ (respectively, $\pi_{\mathbf{u}}$) is the identity permutation lying into a contradiction.

Let a^i is of order $2^l j$, with $l \geq 3$ and assume $\pi_{a^i}(a^n) = a^n + \mathbf{u}$. We have that $\pi_{(a^i)^{2^{l-2}j}}(a^n) = \pi^{2^{l-2}j}_{a_i}(a^n) = a^n + \mathbf{u}^{2^{l-2}j}$ and, since $2^{l-2}j$ is even then $\pi_{(a^i)^{2^{l-2}j}}(a^n) = a^n$. But, since $(a^i)^{2^{l-2}j}$ is either a^n or $a^n \mathbf{u}$ and $\pi_{a^n} = \pi_{a^n \mathbf{u}}$, then $\pi_{(a^i)^{2^{l-2}j}} = \pi_{a^n}$ which is a contradiction. □

Lemma 116. *Let $C = \langle a, b \rangle$ be a* HFP*-code of type Q and length $4n = 2^s n'$, n' odd. Then $\pi_{a^i}(a^n) \neq a^n$, for those a^i, $1 \leq i \leq 2n-1$, with orders different from $2^l j$, $l \geq 2$ and $j > 1$ odd.*

Proof. Let a^i be an element of order order $2^l j$, with j odd and $l \geq 2$. If $\pi_{a^i}(a^n) = a^n$ then $(\pi_{a^i})^{2^{(l-2)}j}(a^n) = a^n$. Further, $\pi_{(a^i)^{2^{l-2}j}} = (\pi_{a^i})^{2^{(l-2)}j}$ and

$(a^i)^{2^{(l-2)}j} \in \{a^n, a^n\mathbf{u}\}$ but, since $\pi_{a^n} = \pi_{a^n\mathbf{u}}$ we would have $\pi_{a^n}(a^n) = a^n$ which is a contradiction. □

The following result shows that the element a^n does not belong to $K(C)$ in any HFP-code $C = \langle a, b\rangle$ of type Q. This fact will be the key to determine the maximum dimension of the kernel of this family of codes.

Proposition 117. *Let $C = \langle a, b\rangle$ be a* HFP*-code of type Q and length $4n = 2^s n'$, n' odd. Then $a^n \notin K(C)$.*

Proof. Let C be a HFP-code of type Q and length $4n = 2^s n'$, n' odd. Assume the contrary, so $a^n \in K(C)$. Thus, from Lemma 106, $s > 2$.

Consider the sets $S = \{\mathbf{e}, \mathbf{u}, \pi_{a^i}(a^n) : i \in \{1, 2, \ldots, 2n\}\}$ and $M = \{a, a^2, \ldots, a^{2n}\}$. Firstly, from Lemma 113 we know that $S \subseteq K(C)$ and, therefore, $|S| \leq |K(C)|$. Since $s > 2$ then we count in M, at most $\frac{n'-1}{2}$, elements of order j, $\frac{n'-1}{2}$ elements of order $2j$ and $\frac{n'-1}{2}$ elements of order $2^2 j$, with $j > 1$ odd. Hence, from Lemma 115 and Lemma 116, we have $|S| > 2^{s-1}n' - 2(n'-1) + 2$. Further, since C is nonlinear then $k \leq s-1$ and

$$|S| > (2^{s-1} - 2)n' + 4 > 2^k = |K(C)|.$$

□

Corollary 118. *Let $C = \langle a, b\rangle$ be a* HFP*-code of type Q and length $4n = 2^s n'$, n' odd. Then the dimension of the kernel is $k \leq 2$. Moreover, if $k = 2$ then $K(C) = \langle a^\kappa b\rangle$, for some $\kappa \in \{1, 2, \ldots, 4n\}$.*

Proof. Assume the contrary, meaning that $k > 2$. We know, from Lemma 115 that $K(C)$ is a group and, since $K(C)$ is a vector space then $|K(C)| = 2^k$. Therefore, $K(C)$ can be decomposed into a direct product of 2-subgroups. Since $k \geq 3$ then there exists an element of the form a^i, $a^i \notin \{\mathbf{e}, \mathbf{u}\}$ lying into $K(C)$ and, $|\langle a^i\rangle| > 2$ due to the fact that $\mathbf{u}$ is the unique element in C of order 2. Since $\langle a^i\rangle$ can be decomposed into a direct product of 2-subgroups then it follows straightforward that $a^n \in \langle a^i\rangle$ contradicting Proposition 117.

If we assume that $k = 2$ then the generator of the kernel must be of order 4 due to the fact that the unique element in C of order two is $a^{2n} = \mathbf{u}$. The unique elements of order 4 in C are $a^n, a^n + \mathbf{u}$ and those of the form $a^i b$ but, from Proposition 117, neither a^n nor $a^n + \mathbf{u}$ belong to $K(C)$. Therefore, $K(C) = \langle a^\kappa b\rangle$, for some $\kappa \in \{1, 2, \ldots, 4n\}$. □

At this point, we have determined the available candidates lying into the kernel of any HFP-code of type Q with $k = 2$. Let us study the the binary representation of these candidates, which depends on the HFP-structure

fixed in Proposition 102. The following result helps to determine this binary representation.

Lemma 119. *Let C be a Hadamard code of length $4n$ with $\beta \in K(C)\setminus\{\boldsymbol{e}, \boldsymbol{u}\}$. Then, the projection of C onto* Supp (β) *consists of a Hadamard code of length $2n$.*

Proof. Let $C = H \cup H + \mathbf{u}$ where H is a normalised Hadamard matrix. Denote $\mathbf{e} = (\mathbf{e}_1, \mathbf{e}_2)$ and $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2)$. As an isomorphism of binary codes, we can permuting the columns of C to obtain $\beta = (\mathbf{e}_1, \mathbf{u}_2)$. Since $\beta \in K(C)$ then $\beta + x \in C$, for every $x \in C$. Thus, we can write

$$H = \left(\begin{array}{c|c} H_1 & H_2 \\ \hline H_1 & H_2 + \mathbf{u}_2 \end{array}\right) \tag{4.10}$$

where H_1 and H_2 are $2n \times 2n$ binary matrices. Let $x = (x_1, x_2) \in C$ such that x is a row in $\left(\begin{array}{c|c} H_1 & H_2 \end{array}\right)$. Since C is a Hadamard code then $\mathrm{wt}(x_1)+\mathrm{wt}(x_2) = d(x, \mathbf{e}) = 2n = d(x+\beta, \mathbf{e}) = \mathrm{wt}(x_1)+\mathrm{wt}(x_2 + \mathbf{u}_2) = \mathrm{wt}(x_1)+2n-\mathrm{wt}(x_2)$ and, therefore, $\mathrm{wt}(x_1) = \mathrm{wt}(x_2) = n$. Two elements $x, y \in C\setminus\{\mathbf{e}, \mathbf{u}\}$ such that $y \notin \{x, x+\mathbf{u}\}$ satisfy $d(x, y) = d((x_1, x_2), (y_1, y_2)) = 2n$. Now, from the equalities $d(x_1, y_1)+d(x_2, y_2) = d(x, y) = 2n = d(x+\beta, y) = d((x_1, x_2+\mathbf{u}_2), (y_1, y_2)) = d(x_1, y_1) + d(x_2 + \mathbf{u}_2, y_2)$ we have that $d(x_1, y_1) = d(x_2, y_2) = n$. Thus, H_1 and H_2 are Hadamard matrices and the projections $C_\beta = H_2 \cup H_2 + \mathbf{u}$ and $C_{\beta+\mathbf{u}} = H_1 \cup H_1 + \mathbf{u}$ are Hadamard codes. □

Proposition 120. *Let $C = \langle a, b\rangle$ be a* HFP*-code of type Q with length $4n = 2^s n'$, n' odd and $k = 2$. If $K(C) = \langle a^\kappa b\rangle$ then the vector $a^\kappa b$ is, up to complementary,*

- $(0, 1, 0, 1, \ldots, 0, 1||0, 1, 0, 1, \ldots, 0, 1) \in \mathbb{Z}_2^{4n}$*, when κ is even.*
- $(\underbrace{0, 1, 0, 1, \ldots, 0, 1}_{2n} || \underbrace{1, 0, 1, 0, \ldots, 1, 0}_{2n}) \in \mathbb{Z}_2^{4n}$*, when κ is odd.*

Proof. Firstly, from Corollary 118 we can assume that $K(C) = \langle a^\kappa b\rangle$, for some $\kappa \in \{1, 2, \ldots, 4n\}$. Now, from Lemma 113 $\pi_a(a^\kappa b) \in K(C)$ and, for obvious reasons, $\pi_a(a^\kappa b) \notin \{\mathbf{e}, \mathbf{u}\}$. Now, we claim that $\pi_a(a^\kappa b) = a^\kappa b\mathbf{u}$. Indeed, if $\pi_a(a^\kappa b) = a^\kappa b$ then the element $a^\kappa b$ would be, up to complementary, $a^\kappa b = (\mathbf{u}_1, \mathbf{e}_2)$. Now, if we project C onto the support of $a^\kappa b$ then $C_{a^\kappa b} = \langle a_1\rangle$ with $\pi_{a_1} = (1, 2, \ldots, 2n)$ and, from Lemma 119 $C_{a^\kappa b}$ is a Hadamard code contradicting Proposition 93. Finally, from the equalities $\pi_a(a^\kappa b) = a^\kappa b + \mathbf{u}$ and $\pi_{a^\kappa b}(a^\kappa b) = a^\kappa b + \mathbf{u}$ the result follows straightforward. □

Let C be a HFP-code of type Q and length $4n = 2^s n'$, n' odd. From Proposition 85 we know that C^T is a HFP-code of type Q. Concerning the dimension of the kernel, when $s = 2$ we know, from Lemma 106, that the dimension of the kernel of C and C^T both, is 1. When $s > 2$, Corollary 118 shows that k can be either 1 or 2. The following result shows that the transpose code C^T of any HFP-code C of type Q with $k = 2$ has dimension of the kernel 1. Because of the proof of the following result, we need to show the following lemma and to introduce additional notation.

Lemma 121. *Let $C = \langle a, b\rangle$ be a* HFP*-code of type Q and length $4n = 2^s n'$, n' odd, with $k = 2$. Let D_1 be the set of codewords with a zero in the first position. Let $a^\kappa b \in D_1$ such that $K(C) = \langle a^\kappa b\rangle$. Then, for every $a^j \in D_1$ we have that $a^j + a^\kappa b$ is $a^{j+\kappa}b$, up to complementary.*

Proof. For any $a^j \in D_1$, we have $a^j + a^\kappa b \in D_1$. In addition, from the equality $\pi_{a^j}(a^\kappa b) = a^\kappa b + \mathbf{u}^j$ then $a^{j+\kappa}b = a^j \cdot a^\kappa b = a^j + \pi_{a^j}(a^\kappa b) = a^j + a^\kappa b + \mathbf{u}^j$ and, we can write $a^{j+\kappa}b + \mathbf{u}^j = a^j + a^\kappa b$. Hence, $a^j + a^\kappa b$ is $a^{j+\kappa}b$, up to complementary. □

Let C be a Hadamard code of length $4n$, let $\beta \in K(C) \setminus \{\mathbf{u}, \mathbf{e}\}$, and let H the Hadamard matrix (4.10). Recall that, in Lemma 119, we denote by $C_\beta = H_2 \cup H_2 + \mathbf{u}$ and by $C_{\beta+\mathbf{u}} = H_1 \cup H_1$ the Hadamard projected codes. Now, denote by $H_{\beta+\mathbf{u}}$ and by H_β the correspondent projected matrices H_1 and H_2, and, for every $x \in C$, denote by x_β the projeciton of x onto Supp (β).

Proposition 122. *Let $(C, \cdot)$ be a* HFP*-code of type Q of length $4n = 2^s n'$, n' odd and $k = 2$, where $C = \langle a, b\rangle$. Then the transpose code C^T of C is a* HFP*-code of type Q with dimension of the kernel* 1.

Proof. Let D_1 and H be the ordered set and the normalised Hadamard matrix defined in Proposition 80, respectively. Since $k = 2$ then, from Corollary 118 we can assume $K(C) = \langle a^{\kappa_1} b\rangle$, for some $\kappa_1 \in \{1, 2, \ldots, 4n\}$. Now, let $(C^T, \diamond)$ be the transpose code of C defined in Proposition 85, and assume $K(C^T) = \langle a^{\kappa_2} \diamond b\rangle$, for some $\kappa_2 \in \{1, 2, \ldots, 4n\}$. Now, consider the $2n \times 2n$ matrices Λ and Λ^T

$$\Lambda = \begin{pmatrix} 0 & 1 & 0 & 1 & \ldots & 0 & 1 \\ 0 & 1 & 0 & 1 & \ldots & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & 0 & 1 & \ldots & 0 & 1 \end{pmatrix} \text{ and } \Lambda^T = \begin{pmatrix} 0 & 0 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 1 & 1 & \ldots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 1 & 1 & \ldots & 1 \end{pmatrix}.$$

Note that any row of Λ corresponds to the first half of coordinates of the vector $a^{\kappa_1}b \in K(C)$, up to complementary, and any column of Λ^T corresponds to the first half of coordinates of the vector $a^{\kappa_2} \diamond b \in K(C^T)$, up to complementary.

The proof follows by constructing a cyclic HFP-code and this goes against Proposition 93, meaning that it is imposible to have simultaneously $a^{\kappa_1}b \in K(C)$ and $a^{\kappa_2} \diamond b \in K(C^T)$.

First of all, assume that κ_1 and κ_2 have the same parity. From Proposition 120, we know that the entry $(a^{\kappa_1}b, a^{\kappa_2} \diamond b)$ in H is 1. Then, from Lemma 121 we can write H, up to isomorphism of binary codes, as

$$H = \left(\begin{array}{c|c} H_1 & H_1 + \Lambda^T \\ \hline H_1 + \Lambda & H_1 + \Lambda + \Lambda^T + \mathbf{u} \end{array} \right). \tag{4.11}$$

Write the element a ($a + \mathbf{u}$, in the case $a \notin D_1$) as $a = (a_1, a_1 + \mathbf{u})$. Furthermore, from Lemma 121 we have $a^{\kappa_1+1}b = a + a^{\kappa_1}b$ and, based on (4.11), we can write $a + a^{\kappa_1}b = (a_1 + (a^{\kappa_1}b)_1, a_1 + (a^{\kappa_1}b)_1))$. Thus, $\mathrm{wt}((a \cdot a^{\kappa_1}b)_1) = n$. Now, for every $i \in \{1, 2, \ldots, 4n\}$, define $v^{(i)}$ as the projection of the vector $a^i \cdot (a^{\kappa_1}b)^i$ over the first half of coordinates, denoted by $v^{(i)} = (a^i \cdot (a^{\kappa_1}b)^i)_1 \in \mathbb{Z}_2^{2n}$.

Let $\mathcal{V} = \{v^{(i)} : 1 \leq i \leq 4n\}$ and, to equip $\mathcal{V}$ with a propelinear structure we associate to v, $v = v^{(1)}$, the permutation $\pi = (1, 2, \ldots, 2n)$ and we are going to show that $v^{(i)} = v + \pi(v^{(i-1)})$, meaning $v^i = v^{(i)}$. Note that we can rewrite $(a^{\kappa_1}b)^i$ as $\sum_{j=0}^{i-1} \pi_a^j(a^{\kappa_1}b)$ and, from Proposition 120, $\pi_a^j(a^{\kappa_1}b)$ as $\pi_a^{-j}(a^{\kappa_1}b)$, for every j. Now, $v + \pi(v) = ((a \cdot a^{\kappa_1}b)_1 + \pi((a \cdot a^{\kappa_1}b)_1) = (a + \pi_a(a) + \pi_a^2((a_1^{\kappa}b) + \pi_a^{-1}(a^{\kappa_1}b)))_1 = (a^2 \cdot (a^{\kappa_1}b)^2)_1 = v^{(2)}$. Hence, we can assume by induction $v^{(i-1)} = v + \pi(v^{(i-2)})$, meaning $v^{i-1} = v^{(i-1)}$ and we see

$$\begin{aligned} v + \pi(v^{(i-1)}) &= v + \pi(v^{i-1}) = v + \pi(\textstyle\sum_{j=0}^{i-2} \pi^j(v)) = \sum_{j=0}^{i-1} \pi^j(v) \\ &= (\textstyle\sum_{j=0}^{i-1} \pi_a^j(a + \pi_a(a^{\kappa_1}b)))_1 = (\sum_{j=0}^{i-1} \pi_a^j(a) + \sum_{l=1}^{i} \pi_a^l(a^{\kappa_1}b))_1 \\ &= (a^i + \pi_a^i(\textstyle\sum_{l=0}^{i-1} \pi_a^l(a^{\kappa_1}b)))_1 = (a^i + \pi_{a^i}((a^{\kappa_1}b)^i))_1 = v^{(i)} \end{aligned}$$

We are going to prove that $\mathcal{V}$ is a Hadamard code. Firstly, since n is even then $v^{2n} = \mathbf{u}$ and $v^{4n} = \mathbf{e}$. Now, based on (4.11), $\mathrm{wt}(v^i) = \mathrm{wt}((a^i)_1) = 2n$, for every even number i, except for $a^i \in \{\mathbf{e}, \mathbf{u}\}$; otherwise, $\mathrm{wt}(v^i) = \mathrm{wt}((a^i \cdot (a^{\kappa_1}b)^i)_1) = \mathrm{wt}((a^i + a^{\kappa_1}b + \mathbf{u}^{\frac{(i+1)}{2}})_1) = 2n$. We shall compute $d(v^i, v^j)$, for every $v^i, v^j \in \mathcal{V}$ satisfying $v^i \notin \{v^j, v^j + \mathbf{u}\}$. We can assume $j > i$ and note that $d(v^i, v^j) = \mathrm{wt}(v^i + v^j) = \mathrm{wt}(\pi^i(v^{j-i})) = \mathrm{wt}(v^{j-i}) = 2n$. Finally, since π has order $2n$ then $\pi_{\mathbf{e}}$ and $\pi_{\mathbf{u}}$ are the unique permutations fixing coordinates and, therefore, it follows that $(\mathcal{V}, \cdot)$ is a cyclic HFP-code.

Without loss of generality consider the case in which κ_1 and κ_2 are odd and even natural numbers, respectively. From Lemma 121 we can write the

matrix H, up to isomorphism of binary codes, as

$$H = \left(\begin{array}{c|c} H_1 & H_1 + \Lambda^T \\ \hline H_1 + \Lambda & H_1 + \Lambda + \Lambda^T \end{array} \right).$$

Consider $(C^T)_{a^{\kappa_2} \diamond b + \mathbf{u}}$ and, call $C' = ((C^T)_{a^{\kappa_2} \diamond b + \mathbf{u}})^T$ and $H' = ((H^T)_{a^{\kappa_2} \diamond b + \mathbf{u}})^T$. From Lemma 119 we know that the rows of H' are, precisely, the subvectors

$$\{\mathbf{e}_1, (a^{2n-2})_1, (a^{2n-4})_1, \ldots, \ldots, (a^2)_1, (a^{\kappa_1} b)_1, (a^{\kappa_1 - 2} b)_1, \ldots, (a^{\kappa_1 + 2} b)_1\}.$$

We claim that the element $(a^{\kappa_1} b)_1$ belongs to $K(C')$. Indeed, from Lemma 121, we know that the element $(a^{2i} + a^{\kappa_1} b)_1$ is $(a^{2i + \kappa_1} b)_1$ (up to complementary) and, since $(a^{\kappa_1 + 2i} b)_1$ belongs to C', for every i, then $(a^{\kappa_1} b)_1 \in K(C')$.

From Lemma 119 we know that, if we project C' over the support of $(a^{\kappa_1} b + \mathbf{u})_1$ then we obtain a binary Hadamard code; call it $\mathcal{V}$. The elements in $\mathcal{V}$ are those which are obtained by projecting the elements a^{2i}, $1 \leq i \leq 2n$, onto the support of $(a^{\kappa_1} b + \mathbf{u})_1$. Hence, the binary code $\mathcal{V}$ has a propelinear structure induced by C; in other words, $(\mathcal{V}, \cdot)$ is generated by the element which is obtained from projecting a^2 onto the support of $(a^{\kappa_1} b + \mathbf{u})_1$ whose permutation is π_{a^2}. Finally, since $\pi_{\mathbf{e}}$ and $\pi_{\mathbf{u}}$ are the unique permutations fixing coordinates then $(\mathcal{V}, \cdot)$ is a cyclic HFP-code. □

Remark 123. *Proposition 124 claims that two* HFP*-codes with the property of being isomorphic as groups may not to be equivalent as binary codes.*

It is worth mentionioning that the recyprocal property of Proposition 122 is not always true. The following example is enough to corroborate this fact.

Example 124. *Let $(C, \cdot)$ be that* HFP*-code of type Q and length* 24*, where $C = \langle a, b \rangle$ and*

$$\begin{array}{l} a = (1,1,0,1,1,1,0,1,0,1,0,0,1,1,1,1,0,0,1,0,0,0,0,0), \\ \pi_a = (1,2,\ldots,12)(13,14,\ldots,24), \\ b = (0,1,1,0,1,0,1,0,0,0,1,0,1,0,1,1,1,0,1,0,1,0,0,1), \\ \pi_b = (1,24)(2,23)\ldots(12,13). \end{array} \tag{4.12}$$

This HFP*-code has $k = 1$ and $r = 12$. Furthermore, the transpose code $(C^T, \cdot)$ of (4.12) is presented by $C^T = \langle a, b \rangle$ where*

$$\begin{array}{l} a = (1,1,0,0,1,0,1,0,1,1,1,0,0,1,1,1,1,0,0,1,0,0,0,0), \\ \pi_a = (1,2,\ldots,12)(13,14,\ldots,24), \\ b = (1,0,0,0,1,0,1,1,1,1,1,0,1,0,0,0,0,0,1,0,1,1,1,0), \\ \pi_b = (1,24)(2,23)\ldots(12,13). \end{array} \tag{4.13}$$

Moreover, C^T is a HFP*-code of type Q and it has dimension of the kernel $k = 1$ and rank $r = 12$.*

4.3 On the rank of HFP-codes of type Q

In the current section we deal with the rank of HFP-codes of type Q and length $4n = 2^s n'$, n' odd. In the case of $s = 2$ we have seen that the rank is $4n - 1$. When $s > 2$, we stablish the upper bound $r \leq 2n$ for those HFP-codes of type Q with dimension of the kernel 1 whose transpose has dimension of the kernel $k = 1$. And, we compute explicitly the rank of those HFP-codes of type Q with $k = 2$. To conclude this section, we show an iterative construction that allows to duplicate any HFP-code of type Q and length $4n$ with $k = 2$ preserving its HFP-structure and the dimension of the kernel.

Definition 125. *Let R be a commutative ring. Any R-module M is said to be finitely generated if there exists a set $\{m_1, m_2, \ldots, m_n\}$ such $M = \sum_i Rm_i$.*

Definition 126. *[MS77] A code C is called quasicyclic if there is some integer i such that every cyclic shift of a codeword by i places, meaning $x^i c(x)$, is again a codeword. Of course a cyclic code is a quasicyclic code with $i = 1$. The integer i is called the index of the code C.*

Cyclic codes can be considered as ideals in the quotient ring $\mathbb{Z}_2[x]/(1 + x^{2n})$. In [MS77] it is showed that quasicyclic codes of index i of length $4n = i \cdot m$ can be represented by submodules of $(\mathbb{Z}_2[x]/(1 + x^m))^i$; In the case when $i = 2$ these quasicyclic codes can be represented by submodules of $\mathbb{Z}_2[x]/(1+x^{2n}) \times \mathbb{Z}_2[x]/(1+x^{2n})$. It is well known ([H98]) that the morphism

$$\begin{array}{rcl} \mathbb{Z}_2[x] & \to & \mathbb{Z}_2[x]/(1 + x^{2n}) \\ p(x) & \to & p(x) \pmod{1 + x^{2n}} \end{array}$$

gives a correspondence between the submodules of $\mathbb{Z}_2[x]$ containing $(x^{2n} + 1)$ and the submodules of $\mathbb{Z}_2[x]/(x^{2n} + 1)$. Note that, for every natural i, this morphism can be extended coordinate-wise to $(\mathbb{Z}_2[x])^i \to (\mathbb{Z}_2[x]/x^{2n} + 1)^i$.

We know, from Proposition 109, that the linear span of a HFP-code C of type Q can be written, in polynomial way, as

$$\langle C \rangle = \langle a(x), xa(x), \ldots, x^{2n-1}a(x), b(x), xb(x), \ldots, x^{2n-1}b(x) \rangle, \qquad (4.14)$$

where $a(x), b(x)$ are the polynomial expressions for a, b, respectively. Hence, $\langle C \rangle$ can be considered as a quasicyclic code of index 2 generated by

$$\begin{bmatrix} a_1(x) & a_2(x) \\ b_1(x) & b_2(x) \\ x^{2n} + 1 & 0 \\ 0 & x^{2n} + 1 \end{bmatrix}. \qquad (4.15)$$

Proposition 127. *[LF01, Cor. 2.14] Let $\mathcal{D}$ be 1-dimensional quasicyclic code $\mathcal{D} = \langle (a_1(x), a_2(x)) \rangle$ with $a_1(x), a_2(x) \in \mathbb{Z}_2[x]/(x^{2n}+1)$ whose generator matrix is*

$$\begin{bmatrix} a_1(x) & a_2(x) \\ x^{2n}+1 & 0 \\ 0 & x^{2n}+1 \end{bmatrix}. \tag{4.16}$$

The code $\mathcal{D}$ has rank $r(\mathcal{D}) = 2n - deg(gcd(a_1(x), a_2(x), x^{2n}+1))$.

Proposition 127 ensures that we can compute the rank of those 1-dimensional quasicyclic codes $\mathcal{D}$ for every $a_1(x), a_2(x) \in \mathbb{Z}_2[x]/(x^{2n}+1)$. In the case of HFP-codes of type Q, generated by $\langle a, b \rangle$, the vector $a = a(x) = (a_1(x), a_2(x))$ is not a general vector. In fact, polynomials $a_1(x), a_2(x)$ must satisfy some conditions in order that $\langle a, b \rangle$ computes a Hadamard code. The following result enables to compute the rank for those HFP-codes of type Q with $k = 2$.

Proposition 128. *Let $C = \langle a, b \rangle$ be a* HFP*-code of type Q and length $4n = 2^s n'$, n' odd. Denote by $a = (a_1(x), a_2(x))$, where $a_1(x), a_2(x) \in \mathbb{Z}_2[x]/(x^{2n}+1)$ and consider the 1-dimensional quasicyclic code $D = \langle (a_1(x), a_2(x)) \rangle$. If the dimension of the kernel of C is $k = 2$ then $r(D) = r(C)$.*

Proof. Since $k = 2$ then we know, from Lemma 107, that $s \geq 3$ and, we can assume, from Proposition 118, $K(C) = \langle a^\kappa b \rangle$ for some $\kappa \in \{1, 2, \ldots, 4n\}$. Further, based on Proposition 120 it follows straightforward that $a^\kappa b$ can be written as $a^\kappa b(x) = (\frac{x^{2n}+1}{(x+1)^2}, x^\kappa \frac{x^{2n}+1}{(x+1)^2})$.

It might be noted that, from the equality $x(a^\kappa b(x)) = a^i b(x) + \mathbf{u}(x)$ we know $r(C) \leq r(D) + 1$. In addition, since $a \cdot a^\kappa b = a^\kappa b \cdot a^{-1}$ then we can write $\mathbf{u} = a^\kappa b + \pi_a(a^\kappa b) = a + \pi_{a^{\kappa+1}b}(a)$. Thus, the component vectors are $a = (a_1, a_2) = (a_1, \pi_{a^{\kappa+1}}(a_1^*) + \mathbf{u}_1)$ and, we can write them in a polynomial way as $a(x) = (a_1(x), a_2(x)) = (a_1(x), (x^{\kappa+1}a_1^*(x) + \mathbf{u}_1(x)) \pmod{x^{2n}-1})$. Now, based on (4.5), $\mathbf{u}(x) = \frac{x^{2n}+1}{1+x}$ and, from the equality $\frac{x^{2n}+1}{x+1}a(x) = \mathbf{u}(x)$, we can write

$$\begin{aligned} \tfrac{x^{2n}+1}{(1+x)^2}a(x) &= (\tfrac{x^{2n}+1}{(x+1)^2}a_1(x), \tfrac{x^{2n}+1}{(x+1)^2}(x^{\kappa+1}a_1^*(x) + \mathbf{u}_1(x))) \\ &= (\tfrac{\mathbf{u}(x)}{(1+x)}, x^\kappa(\tfrac{x^{2n}+1}{(1+x)^2}(xa_1^*(x) + \mathbf{u}_1(x))) \\ &= (a^\kappa b_1(x), x^\kappa(a^\kappa b_1^*(x) + \mathbf{u}(x))) = (a^\kappa b_1(x), a^\kappa b_2(x)) = a^\kappa b(x). \end{aligned}$$

Hence, $a^\kappa b \in D$ and, therefore, $r(D) = r(C)$. □

Remark 129. *It is worth mentioning that, from Proposition 93, we know that there is no cyclic* HFP*-codes but, from Proposition 128, we conclude that the spanned codes of those* HFP*-codes of type Q with $k = 2$ belong to the family of 1-dimensional quasicyclic codes.*

Corollary 130. *Let $C = \langle a, b\rangle$ be a* HFP*-code of type Q and length $4n = 2^s n'$, where n' is odd. Denote by $a = a(x) = (a_1(x), a_2(x))$ where $a_1(x), a_2(x) \in \mathbb{Z}_2[x]/(x^{2n}+1)$. Let r, k be the rank and the dimension of the kernel of C, respectively.*

1. *If $s = 2$ then C is a full rank code, so $r = 4n-1$ and $k = 1$.*
2. *If $s = 3$ then we have that $k \in \{1, 2\}$ and $r = 2n$*
3. *If $s > 3$:*
   a) *If either $k = 2$ or $k = 1$ and C^T has dimension of the kernel 2, then*
   $$r(C) = 2n - deg(gcd(a_1(x), a_2(x), x^{2n}+1))$$
   b) *If $k = 1$ and C^T has $k = 1$ then $r \leq 2n$.*

Proof. The first item and second item, as far as the rank is concerned, comes from Lemma 107 and Proposition 109. For the dimension of the kernel we use Lemma 108, Proposition 109, and Proposition 118.

The third item follows from Lemma 107, Proposition 109, Proposition 118 and Corollary128. □

As last result of this section we show how to duplicate any HFP-code of type Q and length $4n = 2^s n'$, n' odd, with $k = 2$.

Proposition 131. *Let $C = \langle a, b\rangle$ be a* HFP*-code of type Q and length $4n = 2^s n'$, n' odd, and $k = 2$. Then we can duplicate C obtaining a* HFP*-code C' with the same* HFP*-structure and dimension of the kernel. Moreover, if $r(C) = 2n$ then $r(C') = 4n$.*

Proof. Consider π_a and π_b in terms of Proposition 102 and note, from Proposition 104, that the code C can be computed by knowing a, π_a and π_b. Further, from Corollary 118, we assume $K(C) = \langle a^\kappa b\rangle$, for some natural κ.

Now, we are going to define a new HFP-code C' of type Q of length $8n$, starting from C. Let $C' = \langle A, B\rangle$ be the propelinear code of type Q, where $A = (A_1(x), A_2(x))$ and $A_i(x) = a_i(x^2) + xa^\kappa b_i(x^2) \in \mathbb{Z}_2[x]/(x^{4n}+1)$, $i \in \{1, 2\}$. Consider $\pi_A = (1, 2, \ldots, 4n)(4n+1, 4n+2, \ldots, 8n)$ and $\pi_B = (1, 8n)(2, 8n-1)\ldots(4n, 4n+1)$. The code C' can also be generated by A and $A^{2\kappa}B$, where $\pi_{A^{2\kappa}B} = \pi_{A^{2\kappa}} \cdot \pi_B$. Now, we are going to compute the element $A^{2\kappa}B$. The equality $A \cdot A^{2\kappa}B = A^{2\kappa}B \cdot A^{-1}$ is written as $A(x) + xA^{2\kappa}B(x) =$

$A^{2\kappa}B(x) + x^{2\kappa+1}A^*(x)$ and, therefore, $(1+x)A^{2\kappa}B(x) = A(x) + x^{2\kappa+1}A^*(x)$. Hence, for any $i, i' \in \{1,2\}$, $i \neq i'$,

$$\begin{aligned} A^{2\kappa}B_i(x) &= \frac{A_i(x)+x^{2\kappa+1}A^*_{i'}(x)}{1+x} = \frac{(a_i(x^2)+xa^\kappa b_i(x^2))+x^{2\kappa+1}(a_{i'}(x^2)+xa^\kappa b_{i'}(x^2))^*}{(1+x)} \\ &= \frac{(a_i(x^2)+x^{2\kappa+2}a^*_{i'}(x^2)+x(a^\kappa b_i(x^2)+x^{2\kappa}a^\kappa b^*_{i'}(x^2))}{1+x} = \frac{\mathbf{u}(x^2)+x\mathbf{u}(x^2)}{(1+x)} \\ &= x\mathbf{u}(x^2). \end{aligned}$$

Let us study the polynomial representation of A^i and A^iB. The elements A^iB will be represented taking into account that$A^iB = A^{i-2\kappa} \cdot A^{2\kappa}B$.

$$\begin{aligned} A^i(x) = \; & (\textstyle\sum_{j=0}^{i-1} x^j(a_1(x^2) + xa^\kappa b_1(x^2)), \sum_{j=0}^{i-1} x^j(a_2(x^2) + xa^\kappa b_2(x^2))). \\ A^iB(x) = \; & ((\textstyle\sum_{j=0}^{i-2\kappa-1} x^j(a_1(x^2) + xa^\kappa b_1(x^2))) + x^{i-2\kappa}x\mathbf{u}(x^2), \\ & (\textstyle\sum_{j=0}^{i-2\kappa-1} x^j(a_2(x^2) + xa^\kappa b_2(x^2))) + x^{i-2\kappa}x\mathbf{u}(x^2)). \end{aligned}$$

Firstly, for every i, $(A^iB)^2 = A^{4n} = \mathbf{U}$, where $\mathbf{U}$ is the all-one vector in $\mathbb{Z}_2^{8n}$.

Secondly, we are going to prove that C' is a Hadamard code with dimension of the kernel 2. It follows straightforward that $\mathrm{wt}(A^i) = 4n$, for every i. From this condition we know that $d(A^i, A^j) = \mathrm{wt}(A^i + A^j) = \mathrm{wt}(\pi_{A^i}(A^{j-i})) = \mathrm{wt}(A^{j-i}) = 4n$ when $i < j$. Now, since $A^iB = A^{i-2\kappa} \cdot A^{2\kappa}B$ then it is easy to see that we have $\mathrm{wt}(A^iB) = 4n$, for every i. Further, from Lemma 121 the vector $A^i + A^{2\kappa}B$ coincides (up to complementary) with $A^{2\kappa+i}B$. The first consequence is that $d(A^iB, A^j) = 4n$ (for every i, j) and, the second consequence is that $A^{2\kappa}B \in K(C')$. The way we constructed C' guarantees that it is a HFP-code of type Q.

Now assume $r(C) = 2n$. Without loss of generality we can take $a_1(x)$ as a monic polynomial. From Corollary 130 we know that $\gcd(a_1(x), a_2(x), x^{2n} + 1) = 1$ and, therefore, it is obvious that $\gcd(a_1(x), x^i a_2(x), x^{2n} + 1) = \gcd(a_1(x), a_2(x), x^{2n}+1) = 1$ for every natural i. Consequently there are two polynomials $z_1(x), z_2(x) \in \mathbb{Z}_2[x]/(x^{2n}+1)$ satisfying $z_1(x)a_1(x)+z_2(x)a_2(x) = 1 \pmod{x^{2n}+1}$ and $z_1(x)a^\kappa b_1(x) + z_2(x)a^\kappa b_2(x) = 0 \pmod{x^{2n}+1}$. Now, if we consider $z_1(x^2), z_2(x^2) \in \mathbb{Z}_2[x]/(x^{4n}+1)$ then we have the equality

$$z_1(x^2)A_1(x^2) + z_2(x^2)A_2(x) = 1 \pmod{x^{4n}+1}$$

and, therefore, $r(C') = 4n$ by Corollary 130. □

Proposition 131 enables to duplicate any HFP-code C of type Q with $k = 2$ preserving its HFP-structure and the dimension of the kernel; however, this construction is more restrictive than Proposition 67. On the other hand, if we transpose C we know, from Proposition 124, that $(C')^T$ is a HFP-code of length $8n$ with dimension of the kernel 1.

4.4 On the computation of HFP-codes of type Q

Along this dissertation, what we essentially did with respect to the computation of HFP-codes was to design some tools and functions in MAGMA which allow us to compute different families of HFP-codes and their respective ranks and kernels. MAGMA (`http://magma.maths.usyd.edu.au/magma/`) is a software system designed to solve computationally hard problems in algebra, number theory, geometry and combinatorics. In general, MAGMA supports basic facilities for linear codes over finite fields, and linear codes over integer residue rings and Galois rings, including additional functionality for the special case of codes over $\mathbb{Z}_4$ [BC$^+$16].

Firstly, we study the available group structures which can be realised by a HFP-code. Since Hadamard $\mathbb{Z}_2\mathbb{Z}_4$ and Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes were previously studied in [RR13, MR15, BF$^+$12, BF$^+$14] we decided to analyse some propelinear codes with a nonabelian structure. In Section 3.3, we deal with propelinear codes with a subjacent Q_8, D_4, C_8, $Q_8 \times \mathbb{Z}_n$, Q_{8n} groups for small orders. In addition, from Proposition 93 and Proposition 64 we realise that there are neither HFP-codes with a subjacent cyclic nor a dihedral group structure. In the current chapter we have seen that HFP-codes of type Q are in correspondence with those Hadamard groups of type Q and we try to clasify them attending to the values of the rank and dimension of the kernel.

To compute HFP-codes of type Q, we only need to fix the full propelinear structure (Proposition 102) of a HFP-code of type Q, which is presented by $\langle a, b : a^{4n} = \mathbf{e}, a^{2n} = b^2, a \cdot b = b \cdot a^{-1} \rangle$ and, to find the appropiate generator a. Hence, the HFP-structure makes easier the computation in comparison with Hadamard groups in which it used to be by a brute-force algorithm.

We have computed most of HFP-codes of type Q, up to the length 120. More specifically, we can construct HFP-codes of type Q with length $4n = 2^s n'$, $s > 2$ until the length 120 with $k = 2$ and rank $r = 2n$. By transposing the HFP-codes of type Q with $k = 2$ we obtain HFP-codes of type Q with $k = 1$ and with the same rank. However, the computation of HFP-codes of type Q with $k = 1$ whose transpose code has dimension of the kernel 1, is a hard task and we only found a few examples. See Example 124.

Finally, the way we compute HFP-codes of type Q does not reach the improvements that were made on the field of cocyclic Hadamard matrices and relative difference sets over the dihedral group. Indeed, Álvarez et al [H07, AA$^+$01, AA$^+$06] computed cocyclic Hadamard matrices up to the length 188.

Chapter 5

HFP-codes of type CQ

There are several studies about cocyclic Hadamard matrices over abelian groups like the $C_n \times C_4$, $C_n \times C_4 \times C_2$, $C_n \times C_2^3$, where C_n is the cyclic group of order n, n odd. In Proposition 64 Ito discards the existence of cocyclic Hadamard matrix over $C_n \times C_8$. Additionally, the existence of the cocyclic Hadamard matrices over $C_n \times C_4 \times C_2$ satisfying $\mathbf{u} \in C_2$ is an open problem known as the *Hadamard circulant conjecture*, [R63]. Finally, the existence of cocyclic Hadamard matrices over $C_n \times C_2^3$ was studied by Horadam and Baliga in [BH95]. Flannery [F97] gave some constructions of cocyclic Hadamard matrices over $C_n \times C_2^2$ providing Hadamard groups with a subjacent $C_n \times Q_8$ group structure.

In the current chapter, we introduce a subclass of the HFP-codes with a subjacent nonabelian structure related to the quaternion group Q_8 and the cyclic group C_n of order n with n odd. This family of codes are different from the previous $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes and also from HFP-codes of type Q. The goal of the current chapter is to show the existence of HFP-codes with a subjacent $C_n \times Q_8$ structure, termed *of type* CQ, and to study their algebraic and combinatorial properties. Furthermore, based on Kronecker products we reach to duplicate and quadruple HFP-codes of type CQ and length $4n$, n odd, preserving its HFP-structure. Further, the resultant ranks are $4n$ and $4n+1$, respectively, and the dimension of the kernels are 2 and 3, respectively.

The results showed in Chapter 5 were presented at *21-st Conference on Applications of Computer Algebra* in Kalamata, Greece, 2015, [RS15].

5.1 Properties of HFP-codes of type CQ

The aim of the current section is to show the algebraic and combinatorial properties of HFP-codes of type CQ. We comment on the time complexity of the HFP-structure on computing HFP-codes of type CQ attending to the parity of the length. Finally, we show examples of HFP-codes of type CQ.

Definition 132. *Let C be a* HFP *code of length $4n$. We say that C is of type CQ when the code C is, as a group, the direct product $C_n \times Q_8$, where C_n is a cyclic group of order n and Q_8 is the quaternion group.*

Hence, any HFP-code C of type CQ and length $4n$ is generated, as a group, by d, g, c, where d and g are the generators of Q_8 and c the generator of the cyclic group C_n. Hence, C as a group is presented by

$$C = \langle d, g, c : c^n = d^4 = \mathbf{e}, d^2 = g^2, dg = gd^{-1} \rangle.$$

Lemma 133. *Any* HFP*-code $C = \langle d, g, c \rangle$ of type CQ and length $4n$, n odd, can be generated as $C = \langle f, g \rangle$, where $f = dc$.*

Proof. We should prove that d, c can be generated from f.

Firstly, if we assume $n \equiv 1 \bmod 4$ then there is a natural t such that $n = 4t + 1$. Thus, $f^n = d^{4t+1}c^n = d$ and $f^{3n+1} = d^{12t+4}c = c$.

Finally, if $n \equiv 3 \bmod 4$ then $n = 4t + 3$. It is enough too see that $f^{n+1} = d^{4t+4}(c)^{n+1} = c$ and $f^{3n} = d^{12t+9}c^n = d^9 = d$. □

When n is odd then it follows straightforward that the element $\mathbf{u} \in Q_8$. This implies that $d^2 = g^2 = \mathbf{u}$. When n is even then, by Lemma 97, we know that the unique HFP-structure over a quaternion group satisfies $\mathbf{u} \in Q_8$.

Proposition 134. *Let $C = \langle d, g, c \rangle$ be a* HFP *code of type CQ and length $4n$. Up to equivalence, we can assume that:*

i) The associated permutations of the generators d, g, c and f, when n is odd, are

$$\begin{aligned}
\pi_d = \;& (1, n+1)(2, n+2)\dots(n, 2n)(2n+1, 3n+1)\dots(3n, 4n).\\
\pi_g = \;& (1, 2n+1)(2, 2n+2)\dots(2n, 4n).\\
\pi_c = \;& (1, n+2, 3, n+4, n+4, \dots, 2n-1, n)\\
& (2, n+3, 4, n+5, \dots, 2n, n+1)\\
& (2n+1, 3n+2, 2n+3, \dots, 4n-1, 3n)\\
& (2n+2, 3n+3, 2n+4, \dots, 4n, 3n+1),\\
\pi_f = \;& (1, 2, \dots, 2n)(2n+1, 2n+2, \dots, 4n).
\end{aligned} \tag{5.1}$$

ii) The associated permutations of the generators d, g, c, when n is even, are

$$\begin{aligned}\pi_d = &\ (1, n+1)(2, n+2)\dots(n, 2n)(2n+1, 3n+1)\dots(3n, 4n),\\ \pi_g = &\ (1, 2n+1)(2, 2n+2)\dots(2n, 4n),\\ \pi_c = &\ (1, 2, \dots, n)(n+1, n+2, \dots, 2n)\dots(3n+1, \dots, 4n).\end{aligned} \tag{5.2}$$

Proof. We are going to represent the $4n$ coordinates of the vectors in any HFP-code of type CQ, in terms of the n-copies of the quaternionic group as

$$\underbrace{(1, n+1, 2n+1, 3n+1)}_{Q_8}, \underbrace{(2, n+2, 2n+2, 3n+2)}_{Q_8}, \dots, \underbrace{(n, 2n, 3n, 4n)}_{Q_8} \tag{5.3}$$

We know that the element $\mathbf{u} \in Q_8$ and that $g^2 = d^2 = \mathbf{u}$. Hence π_d and π_g are of order 2 and, from the full propelinear condition, they consist of a composition of $2n$ disjoint transpositions. From Lemma 97 we can assume that $\pi_d = (1, n+1)(2, n+2)\dots(n, 2n)(2n+1, 3n+1)\dots(3n, 4n)$ and $\pi_g = (1, 2n+1)(2, 2n+2)\dots(n, 3n)(n+1, 3n+1)\dots(2n, 4n)$.

The element c has order n and, since $\mathbf{u} \in Q_8$ then π_c has order n. From the full propelinearity property, π_c consists of four n-disjoint cycles. We claim that every single coordinate in each n-cycle of π_c lies precisely in one quaternion. Indeed, for instance, if there is an integer j, $1 < j < n$, such that $\pi_c^j(1) = n+1$ then $\pi_d\pi_c^j$, $\pi_d\pi_c^j(1) = \pi_d(n+1) = 1$ contradicting the full propelinear condition.

On the first item we take $\pi_c = (1, n+2, 3, n+4, n+4, \dots, 2n-1, n)(2, n+3, 4, n+5, \dots, 2n, n+1)(2n+1, 3n+2, 2n+3, \dots, 4n-1, 3n)(2n+2, 3n+3, 2n+4, \dots, 4n, 3n+1)$. This idea comes from the fact that $\pi_f = \pi_d\pi_c = (1, 2, \dots, 2n)(2n+1, 2n+2, \dots, 4n)$ which makes easier the computation of HFP-codes of type CQ, as we will see in Lemma 136.

On the second item we assume $\pi_c = (1, 2, \dots, 2n)(2n+1, 2n+2, \dots, 4n)$ also for convenience on the computation of HFP-codes of type CQ.

Finally, both items satisfy $\pi_d\pi_c = \pi_c\pi_d$ and $\pi_g\pi_c = \pi_c\pi_g$ which means that the HFP-structure is well defined. □

Corollary 135. *Let C be a* HFP*-code of type CQ and length $4n$. Then, $\Pi = C/\langle \boldsymbol{u} \rangle = C_2^2 \times C_n$.*

Proof. Firstly, from Proposition 134 we have that π_c is of order n and, π_d and π_g are both of order two. Furthermore, since π_c, π_d and π_g pairwise commute then it follows straightforward that $\Pi = C/\langle \mathbf{u} \rangle = C_2^2 \times C_n$. □

In order to compute the normalised Hadamard matrix H of Proposition 80 we need to study the ordered set D_1 attending to Proposition 134.

Firstly, we deal with those HFP-codes of type CQ and length $4n$ with n odd. Since $f^{2n} = \mathbf{u}$ then $f^{2n+i} = f^i + \mathbf{u}$ and $\pi_{f^i} = \pi_{f^i+\mathbf{u}}$, for every $i \in \{1, 2, \ldots, 2n\}$. Let us denote by $x \in C$ the representative element in $\{x, x + \mathbf{u}\}$ lying into D_1. Now, by Proposition 134 we have, for every $i \in \{0, 1, 2, \ldots, 4n-1\}$, that

- $\pi_{f^{2n-i}}(e_{1+i}) = e_1$ and $\pi_g(e_{2n+1}) = e_1$.
- $\pi_{gf^{2n-i}}(e_{2n+1+i}) = \pi_g\pi_{f^{2n-i}}(e_{2n+1+i})\pi_g(e_{2n+1}) = e_1$.

Consequently, when n is odd, the columns of the normalised Hadamard matrix H, defined in Proposition 80, are indexed by the ordered set

$$D_1 = \{\mathbf{e}, f^{2n-1}, f^{2n-2}, \ldots, f^{2n-1}, g, gf, gf^2, \ldots, gf^{2n-1}\} \tag{5.4}$$

From Proposition 134 and from the order we have taken in (5.1) and (5.4), we can think of the elements $x \in C$ to be written as $x = (x_1, x_2)$. Hence, $v = (v_1(x), v_2(x))$ where $v_1, v_2 \in \mathbb{Z}_2[x]/(x^{2n}+1)$. The action of the permutation π_f over any element $v \in C$ is in correspondence with

$$xv(x) = (v_1(x) \pmod{x^{2n}+1}, xv_2(x) \pmod{x^{2n}+1}). \tag{5.5}$$

Furthermore, the action of the permutation π_g over any element $v \in C$, we denote by $\pi_g(v)$, is in correspondence with

$$(v_2(x), v_1(x)). \tag{5.6}$$

Lemma 136. *Let $C = \langle f, g\rangle$ a* HFP*-code of type CQ and length $4n$, with n odd. Then, up to equivalence, knowing the value of f is enough to define g uniquely, up to complementary.*

Proof. Let C be a HFP-code of type CQ generated by f, g in terms of Proposition 134. From the equality $fg = gf\mathbf{u}$ we can write $f+\pi_f(g) = g+\pi_g(f)+\mathbf{u}$ and, so, $g + \pi_f(g) = f + \pi_g(f) + \mathbf{u}$. Using polynomials, from (5.5) and (5.6) we can write $(1+x)g_i(x) = f_i(x)+f_{i'}+\mathbf{u}_1(x) \pmod{x^{2n}-1}$, for $i, i' \in \{1, 2\}$, $i \neq i'$. Polynomials $f_i(x) + f_{i'}(x) \pmod{x^{2n}-1}$, $i, i' \in \{1, 2\}$ and $i \neq i'$ are multiples of $(1+x)$, so $g_i(x) = \frac{f_i(x)+f_{i'}(x)+\mathbf{u}_1(x) \pmod{x^{2n-1}}}{1+x}$ for $i, i' \in \{1, 2\}$ and $i \neq i'$, and $g(x) = (g_1(x), g_2(x))$. Finally, $(1 + x)g(x) = (1 + x)(g(x) + \mathbf{u}(x))$ and, since $\pi_g(g) = g+\mathbf{u}$ then it follows $g_2(x) = g_1(x)+\mathbf{u}(x)$ and the statement is proved. □

Now we deal with those HFP-codes of type CQ and length $4n$, n even. From Proposition 134, that for every $i \in \{1, 2, \ldots, n-1\}$

- $\pi_a(e_{n+1}) = e_1$, $\pi_b(e_{2n+1}) = e_1$, $\pi_{ab}(3n+1) = e_1$, and $\pi_{c^i}(e_{n-i+1}) = e_1$.
- $\pi_{ac^i}(e_{2n-i+1}) = e_1$, $\pi_{bc^i}(e_{3n-i+1}) = e_1$, and $\pi_{abc^i}(e_{4n-i+1}) = e_1$.

Consequently, the normalised Hadamard matrix H of C, defined in Proposition 80 is the matrix whose rows and columns are indexed by the elements in

$$\begin{aligned} D_1 \;=\; & \{\mathbf{e}, c^{n-1}, c^{n-2}, \ldots, c, a, ac^{n-1}, \ldots, ac, b, bc^{n-1}, \ldots, bc, \\ & ab, abc^{n-1}, \ldots, abc\} \end{aligned} \tag{5.7}$$

From (5.7) and (5.2) we can think any element $v \in C$ to be written in terms of polynomials as $v = (v_1(x), v_2(x), v_3(x), v_4(x))$ where $v_i \in \mathbb{Z}_2[x]/(x^n+1)$, for each $i \in \{1, 2, 3, 4\}$. The action of π_c over any element $v \in C$ is in correspondence with

$$xv(x) = (v_1'(x), v_2'(x), v_3'(x), v_4'(x)),$$

where $v_i'(x) = xv_i(x) \pmod{x^n+1}$, for every $i \in \{1, 2, 3, 4\}$. Furthermore, the actions of π_g and π_d over any element $v \in C$ are in correspondence with

$$\begin{aligned} \pi_d(v) &\to (v_2(x), v_1(x), v_4(x), v_3(x)) \\ \pi_g(v) &\to (v_3(x), v_4(x), v_1(x), v_2(x)) \end{aligned}$$

Note that, from the equalities $\pi_g(g) = g + \mathbf{u}$ and $\pi_d(d) = d + \mathbf{u}$ then $d = (d_1, d_1 + \mathbf{u}, d_3, d_3 + \mathbf{u})$ and, $g = (g_1, g_2, g_1 + \mathbf{u}, g_2 + \mathbf{u})$.

Proposition 137. *Let $C = \langle d, g, c\rangle$ be a* HFP*-code of type CQ and length $4n$, n even. Knowing the value of d and c is enough to define g, up to complementary.*

Proof. Write $g = (g_1(x), g_2(x), g_3(x), g_4(x))$. From the equality $cg = gc$, we can write that $g + \pi_c(g) = c + \pi_g(c)$ and in terms of polynomials, we have

$$g_1(x) = \frac{c_1(x) + c_3(x)}{1+x}, \text{ and } g_2(x) = \frac{c_2(x) + c_4(x)}{1+x}.$$

Since $\pi_g(g) = g + \mathbf{u}$ then $g_3(x) = g_1(x) + \mathbf{u}(x)$ and $g_4(x) = g_3(x) + \mathbf{u}(x)$. Now, the equality $dg = gd\mathbf{u}$ shows that $d_1(x) + d_3(x) = g_1(x) + g_2(x) + \mathbf{u}(x)$ and therefore, it follows straightforward that g is defined through d and g, up to complementary. □

At this point, we know that the time complexity on computing HFP-codes of type CQ and length $4n$, depends on the parity of n. Now, we show examples of HFP-codes of type CQ with different values for the rank and dimension of the kernel.

Example 138. *If we compute the propelinear code $(C, \cdot)$ of length 12 with $C = \langle d, g, c \rangle$ and*

$$\begin{array}{ll} d = (0,1,1,1,0,0,0,1,0,1,0,1), & \pi_d = (1,4)(2,5)(3,6)(7,10)(8,11)(9,12), \\ g = (0,1,1,1,0,1,1,0,0,0,1,0), & \pi_g = (1,7)(2,8)(3,9)(4,10)(5,11)(6,12), \\ c = (0,0,0,1,0,1,1,0,1,1,0,1), & \pi_c = (1,5,3)(2,6,4)(7,11,9)(8,12,10), \end{array}$$

then C is a HFP*-code of type CQ with $r = 11$ and $k = 1$.*

Example 139. *If we compute the propelinear code $(C, \cdot)$ of length 16 with $C = \langle d, g, c \rangle$ with*

$$\begin{array}{l} d = (0,1,1,0,1,0,0,1,0,0,1,1,1,1,0,0), \\ g = (0,1,1,0,1,1,0,0,1,0,0,1,0,0,1,1), \\ c = (1,1,1,1,1,0,1,0,1,0,1,0,0,0,0,0), \\ \pi_d = (1,5)(2,6)(3,7)(4,8)(9,13)(10,14)(11,15)(12,16)(\\ \pi_g = (1,9)(2,10)(3,11)(4,12)(5,13)(6,14)(7,15)(8,16) \\ \pi_c = (1,2,3,4)(5,6,7,8)(9,10,11,12)(13,14,15,16). \end{array}$$

then C is a HFP*-code of type CQ with $r = 7$ and $k = 2$.*

Example 140. *If we compute the propelinear code $(C, \cdot)$ of length 28 with $C = \langle f, g \rangle$ and*

$$\begin{array}{lcl} f & = & (1,0,0,1,0,0,1,0,1,1,0,1,1,0,1,1,1,1,1,1,0,1,0,0,0,0,0,0), \\ g & = & (1,1,1,0,0,0,0,0,0,0,1,1,1,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,1), \\ \pi_f & = & (1,2,3,4,5,6,7,8,9,10,11,12,13,14) \\ & & (15,16,17,18,19,20,21,22,23,24,25,26,27,28), \\ \pi_g & = & (1,15)(2,16)(3,17)(4,18)(5,19)(6,20)(7,21) \\ & & (8,22)(9,23)(10,24)(11,25)(12,26)(13,27)(14,28), \end{array}$$

then C is a HFP*-code of type CQ with $r = 27$ and $k = 1$.*

In Table 5.1 we list all HFP-codes of type CQ and length $4n$, $2 \leq n \leq 11$, attending to the admissible values of the rank and of the dimension of the kernel. Moreover, we show the time complexity of the HFP-structures in terms of computation.

n	r	k	**Time (sec.)**
2	4	4	2.8
3	11	1	16.4
4	5	5	105.7
4	7	2	105.7
5	19	1	633.8
6	12	2	1005.7
7	27	1	3818.9
8	8	3	15401.6
8	9	2	15401.6
8	11	2	15401.6
9	35	1	23186.9
10	20	2	30527.1
10	20	1	30527.1
11	43	1	43651.0

Table 5.1: HFP-codes of type CQ and length $4n$.

The following example corresponds to the first HFP-code of type CQ and length $4n$, n even, that we found with dimension of the kernel $k = 1$.

Example 141. *If we compute the propelinear code $(C, \cdot)$ of length 40 with $C = \langle d, g, c\rangle$ and*

$$\begin{aligned}
c &= (1,0,0,1,1,0,0,1,0,0,0,0,1,0,0,1,0,0,0,0,\\
&\quad 1,1,0,1,1,0,1,1,0,0,1,1,0,1,1,0,1,1,1,1),\\
d &= (1,1,0,1,0,1,1,0,0,0,0,0,1,0,1,0,0,1,1,1,\\
&\quad 1,1,1,1,1,1,1,1,0,1,0,0,0,0,0,0,0,0,1,0),\\
g &= (0,1,1,1,1,1,0,0,0,0,1,0,1,0,1,0,1,0,1,0,\\
&\quad 1,0,0,0,0,0,1,1,1,1,0,1,0,1,0,1,0,1,0,1),\\
\pi_c &= (1,2,\ldots,10)(11,12,\ldots,20)\ldots(31,32,\ldots,40),\\
\pi_d &= (1,11)(2,12)\ldots(10,20)(21,31)(22,32)\ldots(30,40),\\
\pi_g &= (1,21)(2,22)\ldots(20,40),
\end{aligned}$$

then C is a HFP*-code of type CQ with $r = 20$ and $k = 1$.*

In order to compute HFP-codes of type CQ generated by d, g, c but, of higher orders, we introduce some restrictions on the support of d, g. These restrictions permit us to fix the vectors d and g and thus, the time complexity of the HFP-structure decrease.

n	r	k	**Time (sec.)**
12	13	3	51047.2
13	51	1	37838.4
14	22	2	29930.1
15	59	1	43700.2
17	67	1	37223.5
18	36	2	41241.8
19	75	1	27113.5
20	21	3	18321.6
21	83	1	39911.4
22	44	2	21252.1
23	91	1	19785.0
25	99	1	54712.3
26	52	2	31088.3
27	107	1	50661.8
28	23	3	21713.0
29	115	1	116884.4

Table 5.2: HFP-codes of type CQ and length $4n$ with restrictions.

Remark 142. *Let $C = \langle d, g, c\rangle$ be a* HFP*-code of type CQ and length $4n$. From the quaternion representation (5.3) we have the following items.*

- *Since $\pi_d(d) = d + \boldsymbol{u}$, then the admissible values of the vector d in any quaternion Q_8 (5.3), are those in $\{(0,1,0,1),(0,1,1,0)\}$, up to complementary.*
- *Since $\pi_g(g) = g + \boldsymbol{u}$ then the admissible values of the vector g in any quaternion Q_8 (5.3), are those in $\{(0,1,1,0),(0,0,1,1)\}$, up to complementary.*
- *From Lemma 97 we know that, for each value d (first item) there is an unique value for g (on the second item), up to complementary, satisfying $dg = gd^{-1}$.*

In Table 5.2 we list all HFP-codes of type CQ and length $4n$, that we have computed attending to the restrictions of Remark 142. Take into account that Table 5.2 does not list all nonequivalent HFP-code of type CQ. Neither could we compute HFP-codes of type CQ and length $4n$ for which $n \in \{16, 24\}$.

5.2 Kronecker sums over HFP-codes of type CQ

In this section we translate the classical constructions of Hadamard codes, based on Kronecker products, to the case of HFP-codes. Based on *Kronecker sums* we show that, starting from a HFP-code we can construct new HFP-codes of higher orders. The last result of this section shows that we can duplicate and quadruplicate any HFP-code of type CQ and length $4n$, n odd, preserving its full propelinear structure. Finally, we compute the rank and the dimension of the kernel for the resultant codes.

In Section 2.2.1 we show the Kronecker construction. Given any Hadamard matrix H, the expanded matrix $\hat{H} = S \otimes H$ is,

$$\hat{H} = \begin{pmatrix} H & H \\ H & -H \end{pmatrix} \text{ where } S = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{5.8}$$

which is a Hadamard matrix. The following result translates the concept of the Kronecker products into the Kronecker sums.

Proposition 143. *Let $A = (a_{ij}), B = (b_{ij})$ be binary Hadamard matrices corresponding to* HFP*-codes of length m, n, respectively, then the code with corresponding matrix given by (5.9) is a* HFP*-code.*

$$A \oplus B = \begin{pmatrix} a_{11} + B & a_{12} + B & \cdots & a_{1m} + B \\ a_{21} + B & a_{22} + B & \cdots & a_{2m} + B \\ \vdots & \vdots & \vdots & \vdots \\ a_{2m,1} + B & a_{2m,2} + B & \cdots & a_{2m,m} + B \end{pmatrix} \tag{5.9}$$

Proof. Let A, B be binary Hadamard matrices corresponding to HFP-codes of length m, n, respectively. Let $a = (a_1, a_2, \ldots, a_m)$ and $b = (b_1, b_2, \ldots, b_n)$ represent two rows in A, B, respectively. Then, $a \oplus b = (a_1 + b_1, \ldots, a_1 + b_n, a_2 + b_1, \ldots, a_2 + b_n, \ldots, a_m + b_1, \ldots, a_m + b_n)$ is a row in $\in A \oplus B$.

If π_a, π_b are the associated permutations to a, b, respectively, then we define the associated permutation to $a \oplus b$ as $\pi_{a\oplus b}$ such that $\pi_{a\oplus b}(x \oplus y) = (\pi_a(x) \oplus \pi_b(y)$, for any $x \oplus y \in A \oplus B$. With this definition we have $(a \oplus b)(c \oplus d) = (a \oplus b) + \pi_{a\oplus b}(c \oplus d) = (a \oplus b) + (\pi_a(c) \oplus \pi_b(d)) = ac \oplus bd$.

To see that $A \oplus B$ is the matrix corresponding to a propelinear code we have to prove that for any pair $a \oplus b, c \oplus d \in A \oplus B$ we have $\pi_{(a\oplus b)(c\oplus d)} = \pi_{(a\oplus b)}\pi_{(c\oplus d)}$. Now, for any $(x \oplus y) \in A \oplus B$, let us to compute $\pi_{(a\oplus b)(c\oplus d)}(x \oplus y) = \pi_{ac\oplus bd}(x \oplus y) = \pi_{ac}(x) \oplus \pi_{bd}(y) = \pi_a\pi_c(x) \oplus \pi_b\pi_d(y) = \pi_{(a\oplus b)}(\pi_c(x) \oplus$

$\pi_d(y)) = \pi_{(a\oplus b)}\pi_{(c\oplus d)}(x \oplus y)$. Hence, $A \oplus B$ is the matrix of a propelinear code. Furthermore, it is known that $A \oplus B$ is a Hadamard matrix and, also, it is easy to see that the permutations associated to all elements have no fixed points (with the exception of $\mathbf{e} \oplus \mathbf{e}$ and $\mathbf{u} \oplus \mathbf{u}$), so the obtained code, corresponding to $A \oplus B$ is a HFP-code. □

The following result gives the values of the rank and the dimension of the kernel, of those Hadamard codes obtained from Kronecker products (5.8).

Lemma 144. *[PR$^+$06c, Lemma 1] Let H be a binary Hadamard matrix and, let $C = H \cup H + \boldsymbol{u}$ be a Hadamard code with rank r and dimension of the kernel k. Then the Hadamard code $\hat{C} = \hat{H} \cup \hat{H} + \boldsymbol{u}$, where*

$$\hat{H} = \left(\begin{array}{c|c} H & H \\ \hline H & H + \boldsymbol{u} \end{array}\right)$$

has rank $r + 1$ and dimension of the kernel $k + 1$.

Proposition 143 ensures that we can construct new HFP-codes from a given HFP-code; however, these new codes may not preserve the initial HFP-structure. For example, if we duplicate any HFP-code C of type Q with $k = 2$, based on Proposition 143, then $C \oplus S$ can not be a HFP-code of type Q since its dimension of the kernel is 3. Hence, Kronecker sums does not preserve, in general, the initial HFP-structure.

The last objective of this thesis is to refine Kronecker sums in order that they could duplicate and quadruplicate HFP-code of type CQ with length $4n$, n odd, preserving its HFP structure. Duplication and quadruplication recquires, firstly, to study the HFP-structure of the following codes.

We denote by C_A the Hadamard code corresponding to the Hadamard matrix A. Let S be the binary Hadamard matrix of (5.8) that we write as

$$S = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{5.10}$$

Hence, C_S is a cyclic HFP-code. Indeed, $C_S = \{(0,0),(0,1)),(1,0),(1,1)\}$ and consider the permutations $\pi_{\mathbf{e}} = \pi_{\mathbf{u}} = Id$ and $\pi_{(1,0)} = \pi_{(0,1)} = (1,2)$.

Now, let T be the Hadamard matrix of length 4

$$T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}. \tag{5.11}$$

The code C_T is a HFP-code with a subjacent $C_4 \times C_2$ structure. Indeed, to see that C_T is a HFP-code we associate to each element the permutations $\pi_{\mathbf{e}} = I$, $\pi_{(1,0,0,1)} = (1,2,3,4)$, $\pi_{(0,1,0,1)} = (1,3)(2,4)$, $\pi_{(0,0,1,1)} = (1,4,3,2)$. To see that the matrix T is equivalent to the circulant Hadamard matrix of order 4, write the binary Hadamard matrix T but with entries in $\{\pm 1\}$ and multiply the 4^{th} column by -1.

Proposition 145. *Let $C = \langle f, g\rangle$ be a* HFP*-code of type CQ 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 a HFP*-code of type CQ and length $8n$. The values of the rank and dimension of the kernel for this code are $4n, 2$, respectively.*

ii) $C_{T\oplus A}$ is a HFP*-code of type CQ and length $16n$. The values of the rank and dimension of the kernel for this code are $4n+1, 3$, respectively.*

Proof. Let S and T be the HFP-codes of (5.10) and (5.11). From Proposition 143 we know that $C_{S\oplus A}$ and $C_{T\oplus A}$ are HFP-codes. The proof follows by proving, firstly, that C_S and C_T are HFP-codes of type CQ and, finally, by seeing the values of the ranks and the dimension of the kernels.

For the first item, let us construct the HFP-code of type CQ and length $8n$. The code $C_{S\oplus A}$ generated by $d' = (d,d), g' = (g,g), c' = (c,c)$ and $y' = (\mathbf{e}, \mathbf{u})$ with associated permutations $\pi_{d'} = (\pi_d, \pi_d), \pi_{g'} = (\pi_g, \pi_g), \pi_{c'} = (\pi_c, \pi_c)$ and $\pi_{y'} = (1, 4n+1)(2, 4n+2)\ldots(4n, 8n)$ has the element $c'\cdot y'$ which has order $4t$ instead of $2n$. In order to preserve the HFP-structure we need to make a few modifications on the construction of Proposition 143. Hence, take a new structure, call it C', on $C_{S\oplus A}$ by defining the permutation associated to $g'' = (g,g)$ as $\pi_{g''} = \pi_{g'}\pi_{y'}$. It is clear that $(C', \cdot)$ with generators c' and d' and g'' is a HFP-code. Furthermore, for every $x \in C_{S\oplus A}$ we have that $\pi_{y'}(x) = y'x + y'$ so we have that $g''\cdot x = g'\cdot(y'x + y')$.

Now, consider the set $\{d', g'', d'c'y'\}$. Firstly, $(d')^2 = (g'')^2 = \mathbf{u}$. Furthermore, if $n \equiv 1 \pmod 4$ then $(d'c'y')^n = (d, d\mathbf{u})$ and if $n \equiv 3 \pmod 4$ then we have that $(d'c'y')^n = (d\mathbf{u}, d)$. In both cases, $\pi_{(c'd'y')^n} = \pi_{a'}\pi_{y'}$ and therefore $(d'c'y')^{2n} = (\mathbf{e}, \mathbf{e})$.

Let us prove the commutativity between $d'c'y'$ and d', g''. Firstly, it is trivial that $y'\cdot d' = d'\cdot y'$. However, $y'\cdot g'' = (g, g\mathbf{u})$ and $g''\cdot y' = g'(y' + \mathbf{u}) = (g + \mathbf{u}, g)$ so $y'\cdot g'' = g''\cdot y'$. It is easy to see that $d'c'y'\cdot d' = d'\cdot d'c'y'$. In addition, since $c'\cdot g'' = g''\cdot c'$ and since $d'\cdot g'' = g''\cdot d'\mathbf{u}$ we have that $d'c'y'\cdot g'' = d'\cdot c'\cdot g''\mathbf{u}\cdot y' = d'\cdot g''\mathbf{u}\cdot c'\cdot y' = g'd'c'y'$. This proves that

$\{d', g'', d'c'y'\}$ is a set of generators of $C_{S\oplus A}$ and, as a consequence, $(C', \cdot)$ is a HFP-code of type CQ, where $c'd'y'$ is the generator element of C_{2n} and d', g' are the generator elements of the quaternion group Q_8.

For the second item, we show that $C_{T\oplus A}$ is of type CQ and length $16n$. Code $C_{T\oplus A}$ is generated by $d' = (d, d, d, d), g' = (g, g, g, g), c' = (c, c, c, c)$ and $y' = (\mathbf{u}, \mathbf{e}, \mathbf{e}, \mathbf{u})$ with permutations $\pi_{d'} = (\pi_d, \pi_d, \pi_d, \pi_d), \pi_{g'} = (\pi_g, \pi_g, \pi_g, \pi_g), \pi_{c'} = (\pi_c, \pi_c, \pi_c, \pi_c)$ and $\pi_{y'} = (1, 4n{+}1, 8n{+}1, 12n{+}1)(2, 4n{+}2, 8n{+}2, 12n{+}2)\dots(4n, 8n, 12n, 16n)$, respectively, where $\langle d, g\rangle$ is the quaternion subgroup of C_A and $c \in C_A$ is the generator element of the cyclic group of order n.

To see that $C_{T\oplus A}$ is of type CQ and length $16n$, we take a system of generators $\{d', g', c'y'\}$ of $C_{T\oplus A}$, where $\langle d', g'\rangle$ is the quaternion subgroup of $C_{T\oplus A}$ and $c'y' \in C_{T\oplus A}$ is a cyclic element of order $4n$. Further, the element $c'y'$ should commute with all elements in $C_{T\oplus A}$. The element c' is of order n and y' of order 4. In addition, since $\gcd(4, n) = 1$ we have that $(c'y')^{4n} = (\mathbf{e}, \mathbf{e})$. Indeed, since $c' \cdot y' = y' \cdot c'$ then $(c'y')^{4n} = (c')^{4n}(y')^{4n} = \mathbf{e}$. Further, since $(d')^2 = (g')^2 = \mathbf{u}$ then g' and d' are of order 4. Hence $c'y'$ is the generator element of C_{4n} and g', d' are the generator elements of Q_8.

Finally, we are going to check the values of the rank and dimension of the kernel of $C_{S\oplus A}$ and $C_{T\oplus A}$. It is easy to see, by definition, that in $C_{S\oplus A}$ and in $C_{T\oplus A}$ we have $y'\langle d', g', c'\rangle = y' + \langle d', g', c'\rangle$ and $(y')^2 = \mathbf{u}$. Hence, $\langle \mathbf{u}, y'\rangle$ is in the kernel. In the code $C_{S\oplus A}$ the subgroup $\langle \mathbf{u}, y'\rangle$ has four elements and so the dimension of the kernel is at least 2. In the code $C_{T\oplus A}$ the subgroup $\langle \mathbf{u}, y'\rangle$ has eight elements and so the dimension of the kernel is at least 3. Since the length of the code is $2^3n, 2^4n$, respectively, in both cases from Proposition 107 and Proposition 144, the above lower bounds give the true dimensions of the kernel. For the rank, the dimension of the span of $\langle d', g', c'\rangle$ is the same as the rank of C which is $4n-1$. Moreover, it is needed to consider the new independent vectors $\langle y'\rangle$ added to $\langle d', g', c'\rangle$ to obtain the full code. Hence the rank is $4n, 4n+1$, respectively, for $C_{S\oplus A}$ and $C_{T\oplus A}$ and the result follows from Lemma 144. □

To corroborate Proposition 145 we show an example in which we duplicate and quadruplicate the HFP-code of type CQ appearing in Example 138.

Example 146. *Let C be the* HFP*-code of type CQ and length* 12 *of Example 138. Consider $y' = (\boldsymbol{e}, \boldsymbol{u}) \in \mathbb{Z}_2^{24}$ and $\pi_{y'} = (1, 13)(2, 14)\dots(12, 24)$. Now, duplicating C, based on Proposition 145, we obtain the code $(C', \cdot)$ with*

$C' = \langle d', g'', d'c'y' \rangle$ *where*

$$\begin{aligned}
d' &= (0,1,1,1,0,0,0,1,0,1,0,1||\\
&\quad 0,1,1,1,0,0,0,1,0,1,0,1),\\
g'' &= (0,1,1,1,0,1,1,0,0,0,1,0||\\
&\quad 0,1,1,1,0,1,1,0,0,0,1,0),\\
c' &= (0,0,0,1,0,1,1,0,1,1,0,1||\\
&\quad 0,0,0,1,0,1,1,0,1,1,0,1),\\
\pi_{d'} &= (\pi_d, \pi_d),\\
\pi_{g''} &= (\pi_g, \pi_g)\pi_{y'},\\
\pi_{c'} &= (\pi_c, \pi_c).
\end{aligned}$$

The HFP*-code* C' *has rank* $r = 12$ *and dimension of the kernel* $k = 2$. $K(C') = \langle y' \rangle$.

Example 147. *Let* C *be the* HFP*-code of type* CQ *and length* 12 *of Example 138. If we quadruplicate the code* C *in terms of Proposition 145, we obtain the code* $(C', \cdot)$ *with* $C' = \langle d', g', c'y' \rangle$ *where,* $y' = (\boldsymbol{e}, \boldsymbol{u}, \boldsymbol{u}, \boldsymbol{e})$ *and its associated permutation* $\pi_{y'} = (1,13,25,37)(2,14,26,37)\ldots(12,24,36,48)$, *and*

$$\begin{aligned}
d' &= (0,1,1,1,0,0,0,1,0,1,0,1||\\
&\quad 0,1,1,1,0,0,0,1,0,1,0,1||\\
&\quad 0,1,1,1,0,0,0,1,0,1,0,1||\\
&\quad 1,0,0,0,1,1,1,0,1,0,1,0),\\
g' &= (0,1,1,1,0,1,1,0,0,0,1,0||\\
&\quad 0,1,1,1,0,1,1,0,0,0,1,0||\\
&\quad 0,1,1,1,0,1,1,0,0,0,1,0||\\
&\quad 1,0,0,0,1,0,0,1,1,1,0,1)\\
c' &= (1,1,1,0,1,0,0,1,0,0,1,0||\\
&\quad 1,1,1,0,1,0,0,1,0,0,1,0||\\
&\quad 0,0,0,1,0,1,1,0,1,1,0,1,||\\
&\quad 0,0,0,1,0,1,1,0,1,1,0,1),\\
\pi_{d'} &= (\pi_d, \pi_d, \pi_d, \pi_d),\\
\pi_{g'} &= (\pi_g, \pi_g, \pi_g, \pi_g)\\
\pi_{c'} &= (\pi_c, \pi_c, \pi_c, \pi_c).
\end{aligned}$$

The HFP*-code* C' *has rank* $r = 13$ *and dimension of the kernel* $k = 3$. *Furthermore,* $K(C') = \langle y' \rangle$.

Note that we can not increase the length of C eight times based on the constructions of Proposition 145 because of the following reasons. In the first

case, although C_S is a cyclic HFP-code of order four, in Proposition 145, we redefine the HFP-structure of $C_{S\oplus A}$ in order that $C_{S\oplus A}$ becomes a HFP-code of type CQ. In the second case, quadruplication requires a circulant Hadamard matrix like T, but of order eight, and this goes against the circulant Hadamard conjecture [R52]. On both cases, we use the cyclic HFP-structure of the matrices S and T but, we know from Propostion 93, that there is no cyclic HFP-structure for Hadamard matrices of length $8n$. Thus, based on this condition and on Table 5.2, we consider the existence of HFP-codes of type CQ and length $16n$ as an open problem.

We did not further study the rank and dimension of the kernel of the transpose code of any HFP-codes of type CQ because of the lack of added value in the area of Kroneckers sums. Indeed, any HFP-code of type CQ and length $4n$, n odd, and its transposed code have the same rank $4n-1$ and dimension of the kernel 1. We conclude, from Lemma 144, that the rank and dimension of the kernel keep invariant through Kronecker constructions.

5.3 On the computation of HFP-codes of type CQ

The computation of HFP-codes of type CQ and length $4n$, highly differs from the computation of HFP-codes of type Q. When n is odd, we know, from Proposition 133, that any HFP-code $C = \langle f, g\rangle$ can be computed by knowing only the generator f. Otherwise, when n is even, we know, from Proposition 137, that any HFP-code $C = \langle d, g, c\rangle$ can be computed by knowing, at least, the generators d and c. It is obvious that the time complexity of the HFP-structure increases when n is even. Furthermore, when we increase the value of n, we need to introduce the restrictions of the Remark 142 to compute HFP-codes of type CQ of higher orders. Table 5.1 and Table 5.2 reflect that we are able to compute most of HFP-codes of type CQ, up to the length 116. However, the first gaps that we find on the computation of HFP-codes of type CQ and length $4n$, are those in which $4n \in \{64, 96\}$.

Based on Kronecker sums of Proposition 145 we can duplicate all those HFP-codes of type CQ and length $4n$, n odd, of Table 5.1 and Table 5.2 to obtain HFP-codes of type CQ of higher orders. It is worth mentioning that we verified in MAGMA that, starting from a HFP-code of type CQ and length $4n$, n odd and $n \leq 29$ odd, we can construct a HFP-code of type Q with the same length.

Finally, we did not reach the results that were made for cocyclic Hadamard

matrices over $\mathbb{Z}_2^2 \times \mathbb{Z}_n$ (n odd). Indeed, in [AR$^+$15] they compute cocyclic Hadamard matrices over $\mathbb{Z}_2^2 \times \mathbb{Z}_n$ (n odd) up to the length 252 except for the cases in which the length is in $\{140, 188, 212, 236\}$.

Chapter 6

Conclusions

6.1 Summary

The existence of Hadamard matrices (or, equivalently, Hadamard codes) of length $4n$, for every natural n, is an open problem [H83]. Around 1990, authors like Horadam, Flannery, de Launey and Ito dealt with this question [H00, LF$^+$00, HL93a, S99]. Since there are many nonequivalent Hadamard codes of the same length then we use the rank r and the dimension of the kernel k to help determining whether two Hadamard codes are equivalent or not.

In Section 3.3.2 we remind that there are five nonequivalent Hadamard codes of length 16 with pairs $(r, k) \in \{(5, 5), (6, 3), (7, 2), (8, 2), (8, 1)\}$ [MS77]. In [RR13, BF$^+$14] it was proved that $(5, 5)$, $(6, 3)$, and $(7, 2)$ can be realised by a linear code, by a propelinear $\mathbb{Z}_4$-linear and by a propelinear Q_8-code, respectively. In Chapter 3, we construct HFP-codes with a subjacent Q_{32} group structure (Example 98) with rank and dimension of the kernel $(8, 2)$ and $(8, 1)$. The existence of this family of codes underscore the importance of HFP-codes with respect to the linear, $\mathbb{Z}_2\mathbb{Z}_4$-linear, and $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. The first contribution on this dissertation is given in Chapter 3 where we reach the following conclusions.

- Equivalences. We prove the equivalence between Hadamard groups and HFP-codes which allows us to connect them also with cocyclic Hadamard matrices and relative difference sets.

- Transpose code. We define the transpose code of a Hadamard code and, we prove that the transpose code of any HFP-code is HFP. Further, we

prove that any HFP-code and its transpose are isomorphic as groups but not neccesarily isomorphic as binary codes.

- Algebraic properties. We prove that no HFP-codes can be realised by a cyclic group, generalising the result of Ito [I94] which states that no HFP-code contains a cyclic 2-Sylow subgroup.

In Chapter 4 we introduce HFP-codes of type Q, meaning HFP-codes with a subjacent dicyclic group of $8n$ elements. This family of HFP-codes is in correspondence with Hadamard groups of type Q [I94, I97], relative difference sets [S99] and cocyclic Hadamard matrices over the dihedral group D_{4n} [LH93, F97]. Specifically, we focused on the computation of the values of the rank and dimension of the kernel of any HFP-code $C = \langle a, b\rangle$ of type Q and length $4n = 2^s n'$, n' odd. In Chapter 4 we reach the following conclusions.

- Dimension of the kernel. If $s = 2$ then we show that $k = 1$. If $s > 2$, Corollary 118 states that the dimension of the kernel can be either 1 or 2. Taking advantadge of the HFP-structure of the transpose code, we prove that the transpose code of a HFP-code of type Q with $k = 2$, has dimension of the kernel 1. We show that the reciprocal is not necessarily true, see Example 124.

- Rank. When $s = 2$ then we show that $r = 4n - 1$. When $s > 2$ we distinguish two cases. If either C or C^T (they have the same rank) have dimension of the kernel $k = 2$ then we compute explicitly the rank in Corollary 130. Otherwise, for those HFP-codes of type Q with $k = 1$ whose tranpose codes have dimension of the kernel 1, we establish $r \leq 2n$.

- Quasicyclic codes. The family of the spanned codes of those HFP-codes of type Q with $k = 2$ belongs to the family of 1-dimensional quasicyclic codes [LF01]. It is worth to mention that there is no cyclic HFP-code, but quasicyclic HFP-codes.

- Iterative construction. Proposition 131 gives an iterative construction which allows to duplicate any HFP-code of type Q with $k = 2$ preserving the HFP-structure and the dimension of the kernel. Moreover, if we duplicate any HFP-code of type Q with $k = 2$ and $r = 2n$ then the resultant code has rank $4n$.

- Computation in MAGMA. Based on Proposition 104 we only need to compute the generator a, instead of the two generators like in the case of Hadamard groups of type Q. We compute most of HFP-codes of type Q, up to the length 120. However, we did not reach the results which were obtained in the field of cocyclic Hadamard matrices over D_{4n}. Indeed, in [AA+16] it is provided an algorithm which allows to construct cocyclic Hadamard matrices over the dihedral group, up to the length 188.

In Chapter 5 we introduce HFP-codes of type CQ, meaning HFP-codes realised by a $C_n \times Q_8$ group structure. This family of codes was previously studied by Horadam and Baliga [BH95]. Specifically, we try to classificate them attending to the values of the rank and dimension of the kernel. We reach the following conclusions.

- Rank and dimension of the kernel. If n is odd then $r = 4n - 1$ and $k = 1$.

- Kronecker sums. We translate the concept of Kronecker products in terms of HFP-codes and thus Proposition 143 enables to construct HFP-codes of higher orders. However, the initial HFP-structures may not be preserved.

- Duplication and quadruplication. Based on Kronecker sums, in Proposition 145 we duplicate and quadruplicate any HFP-code of type CQ and length $4n$, n odd, preserving its HFP-structure. The duplicated code has rank $4n$ and dimension of the kernel 2 and, the quadruplicated code has rank $4n + 1$ and dimension of the kernel 3.

- Computation in MAGMA. We compute most of HFP-codes of type CQ and length $4n$, $1 \leq n \leq 29$ ($4n \leq 116$) except for $n \in \{16, 24\}$. In [AR+15] all cocyclic Hadamard matrices over $\mathbb{Z}_2^2 \times \mathbb{Z}_n$ (with n odd) are computed, up to the length 252, with the exceptions of lengths in $\{140, 188, 212, 236\}$.

- We have verified in MAGMA that, starting from a HFP-code of type CQ and length $4n$, $n \leq 29$ odd, we can construct a HFP-code of type Q and of the same length.

6.2 Future research

In this section, we indicate some open problems that derive from this dissertation which may be considered for future research on this topic:

- In [AA$^+$16, AR$^+$15] most of cocyclic Hadamard matrices over the dihedral group D_{4n} and $\mathbb{Z}_2^2 \times \mathbb{Z}_n$ (n odd), are computed up to lengths 188 and 252, respectively. In terms of computational capability: is there any improvement for decreasing the time complexity of HFP-codes of type Q and of type CQ?

- In Proposition 122 we prove that the dimension of the kernel of the transpose code of any HFP-code of type Q with $k = 2$ is 1 and we show that the reciprocal is not always true. We propose to find a characterisation which decides whether the transpose code of a HFP-code of type Q with $k = 1$ has dimension of the kernel 1.

- In Proposition 131 we provide an iterative construction for duplicating HFP-codes of type Q with $k = 2$. The following question arises naturally. Is there any construction for duplicating any HFP-code C of type Q with $k = 1$ (whose C^T has dimension of the kernel 1) preserving the HFP-structure and the dimension of the kernel?

- In Corollary 130 we compute explicitly the rank of any HFP-code C of type Q with $k = 2$ (or, with $k = 1$ and whose C^T has dimension of the kernel is 2). Is there an explicit form to compute the rank of any HFP-code C of type Q with $k = 1$ whose C^T has dimension of the kernel 1?

- Can we find an explicit form to determine the rank and the dimension of the kernel of those HFP-codes of type CQ of length $4n$ with n even? I am well aware that this question is being studied by I. Bailera, J. Borges, and J. Rifà.

- Proposition 145 enables to duplicate any HFP-code of type CQ and length $4n$, n odd. We propose to find an iterative construction for duplicating and quadruplicating HFP-codes of type CQ with n even.

- To deal with HFP-codes with different subjacent group structures; for instance, $C_n \times C_2^3$, n odd. This question is also being studied by I. Bailera, J. Borges and J. Rifà.

Bibliography

[AA+01] V. Álvarez, J.A. Armario, M.D. Frau, and P. Real, *An algorithm for computing cocyclic matrices developed over some semidirect products,* AAECC-14 Proceedings, LNCS 2227, S. Boztas and I.E. Shparlinski (Editors), Springer-Verlag, Berlin Heidelberg, pp. 287–296, 2001.

[AA+06] V. Álvarez, J. A. Armario, M. D. Frau, P. Real *A Genetic Algorithm for Cocyclic Hadamard Matrices* Lecture Notes in Computer Science, v. 3857, pp. 144-153, 2006.

[AA+16] V. Álvarez, J. A. Armario, M. D. Frau, F. Gudiel, B. Güemes, and A. Osuna. *On $\mathcal{D}_{4t}$-Cocyclic Hadamard Matrices* Journal of Combinatorial Designs, Wiley Online Library, pp. 352-368, January 2016.

[AR+15] V. Álvarez, F. G. Rodríguez, and B. A. Güemes Alzaga, *On $\mathbb{Z}_t \times \mathbb{Z}_2^2$-Cocyclic Hadamard Matrices,* Journal Of Combinatorial Designs (online), vol. 23, n. 8, pp. 352-368, 2015.

[AK92] E. F. Assmus and J. D. Key, *Designs and Their Codes*, Cambridge University Press, Great Britain, 1992.

[BH95] A. Baliga and K. J. Horadam *Cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$* Australas. J Combin, vol. 11, pp. 123-134, 1995.

[BB+15] R. D. Barrolleta, M. De Boeck, L. Storme, E. Suárez-Canedo, and P. Vandendriessche, "A geometrical bound for the sunflower property," in Proc. of *Design and Application of Random Network Codes (DARNEC '15)*, Istanbul, Turkey, pp. 39, 4–6 November 2015.

[BB+16] R. D. Barrolleta, M. De Boeck, L. Storme, E. Suárez-Canedo, and P. Vandendriessche, "On constant distance random network

codes," in Proc. of *Network Coding and Designs*, Dubrovnik, Croatia, pp. 48–49, 4–8 April 2016.

[BP+16] R. D. Barrolleta, J. Pernas, J. Pujol, and M.Villanueva, "Codes over $\mathbb{Z}_4$. A MAGMA package," version 2.0, Universitat Autònoma de Barcelona, `http://ccsg/uab.cat`, Accessed 13-09-2017.

[BS+16] R. D. Barrolleta, L. Storme, E. Suárez-Canedo, and P. Vandendriessche, "On primitive constant dimension codes and a geometrical sunflower bound," submitted to *Adv. in Math. of Commun.*, 2016.

[B66] L. D. Baumert, *Hadamard Matrices of Orders 116 and 232.* Bull. Amer. Math. Soc., vol. 72, pp. 237, 1966.

[B71] L. D. Baumert, *Cyclic difference sets.* Lecture Notes in Mathematics, vol. 182, Springer-Verlag Berlin, 1971.

[BG+62] L. D. Baumert, S. W. Golomb, M. Hall, , *Discovery of an Hadamard Matrix of Order 92.* Bull. Amer. Math. Soc., vol. 68, pp. 237-238, 1962.

[BG+65] L. D. Baumert, S. W. Golomb, M. Hall, , *A New Construction for Hadamard Matrices.* Bull. Amer. Math. Soc., vol. 71, pp.169-170, 1965.

[BJ+99] T. Beth, D. Jungnickel and H. Lenz, *Design Theory* 2nd ed., CUP, Cambridge, 1999.

[BE+99] A. Beutelspacher, J. Eisfeld, and J. Müller, "On sets of planes in projective space intersecting mutually in one point," *Geometriae Dedicata*, vol. 78, pp. 143–159, 1999.

[BF+10] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, *$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality*, *Des. Codes and Cryptogr.*, vol. 54, no. 2, pp. 167–179, 2010.

[BF+12] J. Borges, C. Fernández, J. Pujol, J. Rifà, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes. A MAGMA package," version 3.5, Universitat Autònoma de Barcelona, `http://ccsg/uab.cat`, Accessed 13-09-2016, 2012.

[BF+14] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, "Survey on $\mathbb{Z}_2\mathbb{Z}_4$-additive codes," Proc. of the *contact forum Galois geometries and applications*, Royal Flemish Academy of Belgium for Science and the Arts (October 5, 2012), pp. 19–67, 2014.

[BM+12] J. Borges, I. Y. Mogilnykh, J. Rifà, and F. I. Solov'eva, *Structural properties of binary propelinear codes,* Advances in Mathematics of Communications 6, pp. 329-346, 2012.

[BP+03a] J. Borges, K. T. Phelps, and J. Rifà, "The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear and additive non-$\mathbb{Z}_4$-linear codes," *IEEE Trans. Inf. Theory*, vol, 49, no. 8, pp. 2028–2034, 2003.

[BP+03b] J. Borges, K. T. Phelps, J. Rifà, and V. Zinoviev, "On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like codes", *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2834–2843, 2003.

[BR99] J. Borges and J. Rifà, *A characterization of* 1*-perfect additive codes*, IEEE Trans. infor. Theory, 45(5):1688-1697, 1999.

[B42] R.C. Bose, *An affine analogue of Singer's theorem,* J. Indian Math. Soc. (N.S.) 6, pp. 1-15, 1942.

[BC+16] W. Bosma, J. J. Cannon, C. Fieker, and A. Steel (eds.), *Handbook of Magma functions*, Edition 2.22 (2016) 5669 pages. `http://magma.maths.usyd.edu.au/magma/`.

[B90] S. Bouc, *Biset Functors for Finite Groups* Lecture Notes in Mathematics, Springer, 1990.

[BC+89] A.E. Brouwer, A.M. Cohen, and A. Neumaier. Distance-Regular Graphs, Springer-Verlag, vol 2., 1989.

[B55] Burnside, W., *Theory of Groups of Finite Order*, 2nd edition, Cambridge University Press, 1911, reprinted Dover Publications, New York, 1955.

[B62] A.T Butson *Generalized Hadamard matrices* Proc. Amer. Math. Soc., vol. 13, pp. 894-898, 1962.

[B63] A. T Butson, *Relations among generalized Hadamard matrices,* Canad. J. Math., vol. 15, pp. 42-48, 1963.

[CW72] J. Cooper and J. S. Wallis. *A construction for Hadamard arrays* Bull. Austral. Math. Soc., vol.7, pp. 269-278, 1972.

[D73a] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Reports Supplements, 10, 1973.

[D73b] P. Delsarte, *Four fundamental parameters of a code and their combinatorial significance,* Information and Control, vol. 23, pp. 407-438, 1973.

[DL98] P. Delsarte, V. I. Levensthein, *Association schemes and coding theory* IEEE Transactions on Information Theory, vol. 44, pp. 247-2504, 1998.

[E02] J. Eisfeld, "On sets of n-dimensional subspaces of projective spaces intersecting mutually in an $(n-2)$-dimensional subspace," *Discrete Mathematics*, vol. 255, pp. 81–85, 2002.

[EB66] J.E.H. Elliot, A.T. Butson, *Relative difference sets* Illinois J. Math., vol. 10 , pp. 517-531, 1966.

[ER14] T. Etzion and N. Raviv, "Equidistant codes in the Grassmannian", D. Appl. Math., vol. 186, pp. 87-97, 2015.

[FP+08] C. Fernández-Córdoba, J. Pujol, and M. Villanueva, "On rank and kernel of $\mathbb{Z}_4$-linear codes," *Lect. Notes Comput. Sc.*, vol. 5228, pp. 46–55, 2008.

[FP+10] C. Fernández-Córdoba, J. Pujol, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel," *Des. Codes and Cryptogr.*, vol. 56, no. 1, pp. 43–59, 2010.

[F97] D. L. Flannery, *Cocyclic Hadamard Matrices and Hadamard Groups are equivalent* Journal of Algebra 192, pp. 749-779, 1997.

[GK05] S. Georgiou and C. Koukouvinos, *Some results on orthogonal designs and Hadamard matrices* Int. J. Appl. Math., vol. 17, pp. 433-443, 2005.

[GS67] M. Goethals and J.J. Seidel, *Orthogonal matrices with zero diagonal*, Canad. J. Math., vol 19, pp. 1001-1010, 1967.

[GS70] J. M. Goethals and J.J. Seidel, *A skew Hadamard matrix of order 36,* J. Austral. Math. Soc., vol 11, pp. 343-344, 1970.

[GT] J. M. Goethals and H. C. A. Van Tilborg, *Uniformly packed codes.* Philips Research Reports, vol. 30, pp. 9-36, 1975.

[H83] J. Hadamard, *Resolution d'une question relative, aux dèterminants*, Bulletin des Sciences Mathèmatiques, (2), vol. 17, Part 1, pp. 240-246, 1893.

[HK+94] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes,* IEEE Trans. Inf. Theory, vol. 40, no. 2, pp. 301-319, 1994.

[H70] Hartley B., Hawkes T. O., *Rings, modules and linear algebra*, Chapman Hall/CRC, 1970.

[H00] K. J. Horadam *An introduction to cocyclic generalised Hadamard matrices*, Discrete Applied Mathematics, vol. 102, p. 115-131, 2000.

[H07] K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, 2007.

[HL93a] K. J. Horadam and W. de Launey, *Generation of cocyclic Hadamard matrices,* Research Report No.2, Mathematics Department, RMIT, March 1993.

[HL94b] K. J. Horadam and W. de Launey, *Cocyclic development of designs*, J. Algebraic Combinatorics, pp. 267-290, 1994.

[HP97] K.J. Horadam and A. A. I. Perera *Codes from cocycles,* Lecture Notes in Computer Science, volume 1255, pp.151-163, Springer–Verlag, Berlin–Heidelberg–New York, 1997.

[HP03] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[H98] W. C. Huffman, *Codes and Groups,* Handbook of Coding Theory, (V. S. Pless and W. C. Huffman, eds.), Elsevier, 1998.

[I81] N. Ito, *Note on Hadamard matrices of type Q,* Studia Sci. Math. Hungar. 16, pp. 389-393, 1981.

[I93] N. Ito, *Notes on Hadamard groups of quadratic residue type,* Hokkaido Math. J. 22, pp. 373-378, 1993 .

[I94] N. Ito, *On Hadamard groups* J. Algebra 168, pp. 981-987, 1994.

[I95a] N. Ito, *On Hadamard groups II* J. Algebra 169, pp. 936-942, 1994.

[I95b] N. Ito, *Some results on Hadamard groups* Groups-Korea '94, de Gruyer, Berlin and New York, 1995

[I96] N. Ito, *Remarks on Hadamard groups* Kyushu J. Math., vol 50, pp. 83-91, 1996.

[I97] N. Ito, *On Hadamard groups III,* Kyushu J. Math., vol 51, pp. 1-11, 1997.

[I00] N. Ito *On Hadamard Groups IV* J. of Algebra 234, pp. 651-663, 2000.

[IS00] N. Ito, P. S. Kim, *On Generalized Hadamard Subsets*, J. of Algebra 223, pp. 601-609, 2000.

[J82] D. Jungnickel , On automorphism groups of divisible designs, Canadian J. Math. 34, pp.257-297, 1982.

[JP96] D. Jungnickel and A. Pott, *Difference sets: Abelian, The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, eds., CRC Press, Boca Raton, 1996.

[K95] W. H. Kantor, "Codes, quadratic forms and finite geometries. Different aspects of coding theory," in Proc. of *Symp. Appl. Math.*, San Francisco, pp. 153–177, 1995.

[K72] A. M. Kerdock, "A class of low-rate nonlinear binary codes," *Inf. and Control*, vol. 20, pp. 182–187, 1972.

[K78] R. E. Kibler, *Summary of Noncyclic Difference Sets, $k < 20$* Combinatorial theory J., Series A 25, pp. 62-67, 1978.

[KW+16] M. Kiermaier, A. Wassermann, and J. Zwanzger, "New upper bounds on binary linear codes and a $\mathbb{Z}_4$-code with a better-than-linear Gray image," IEEE Trans. of Inf., vol. 62, pp. 6768-6771, 2016.

[KZ13] M. Kiermaier and J. Zwanzger, "New ring-linear codes from dualization in projective Hjelmslev geometries," *Des. Codes Cryptogr.*, vol. 66, nos. 1–3, pp. 39–55, 2013.

[K01] D. S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes," *Electron. Note Discr. Math.*, vol. 6, pp. 107-112, 2001.

[KV15] D. S. Krotov and M. Villanueva, "Classification of the $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes and their automorphism groups," *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 887-894, 2015.

[LF01] K. Lally, Fitzpatrick P. *Algebraic structure of quasicyclic codes* Discrete Applied Mathematics, vol. 111, pp. 157-175, 2001.

[L13] L. Lambert, *Random Network Coding and Designs over* $\mathbb{F}_q$, Master dissertation, Ghent University, 2013. `http://www.network-coding.eu/pubs/Thesis-Lien.pdf`.

[L90] W. de Launey, *On the construction of n-dimensional designs from 2-dimensional designs,* Australas. J. Combin. 1, pp. 67-81, 1990.

[LF+00] W. de Launey, D. L. Flannery, and K. J. Horadam *Cocyclic Hadamard matrices and diference sets* Discrete Applied Mathematics 102, 47-61, 2000.

[LH93] W. de Launey and K. J. Horadam, *A weak difference set construction for higher dimensional designs*, Designs, Codes and Cryptography, vol. 3, pp.75-87, 1993.

[LS98] W. de Launey, M.J. Smith, *Cocyclic orthogonal designs and the asymptotic existence of maximal size relative diference sets with forbidden subgroup of size 2,* J. of Combinatorial Theory, Series A 93, vol 1, pp. 37-92, 2001.

[L82] J. van Lint, *Introduction to Coding Theory,* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1982.

[LR+99] S. Litsyn, R. M. Rains, and N. J. A. Sloane, "Table of nonlinear binary codes," online available at `http://www.eng.tau.ac.il/ litsyn/tableand/`. Accessed 13-09-2015. http://www.win.tue.nl/ aeb/codes/binary.html, 99.

[MS77] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.

[MR15] P. Montolio and J. Rifà, "Construction of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes for each allowable value of the rank and dimension of the kernel," *IEEE Trans. Inf. Theory*, vol. 61, no. 4, pp. 1948–1958, 2015.

[N91] A. Nechaev, *Kerdock code in a cyclic form,* Dis. Math. and Applic., vol.1, n.4, pp. 365-384, 1991.

[N92] A. Neumaier, *Completely regular codes*, Disc. Math., vol. 106/107, pp. 335-360 , 1992.

[P33] R. E. A. C. Paley, *On orthogonal matrices,* J. Math. Phys., vol 12, pp. 311-320 , 1933

[PP+12] J. Pernas, J. Pujol, and M. Villanueva, "Codes over $\mathbb{Z}_4$. A MAGMA package," version 1.4, Universitat Autònoma de Barcelona, Accessed 13-09-2016, `http://ccsg/uab.cat`, 2012.

[PR02] K. T. Phelps and J. Rifà, "On binary 1-perfect additive codes: some structural properties," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2587–2592, 2002.

[PR+05a] K. T. Phelps, J. Rifà, and M. Villanueva, *Rank and Kernel of binary Hadamard codes*, IEEE Trans. Inf. Theory, vol. 51, pp.3931-3937, 2005.

[PR+06b] K. T. Phelps, J. Rifà, and 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, no. 1, pp. 316-319, 2006.

[PR+06c] K. T. Phelps, J. Rifà, and M. Villanueva, *Hadamard Codes of Length $2^t s$ (s Odd). Rank and Kernel* Ap. Alg. and Error-Correcting Codes, Springer-Verlag Berlin, vol 3875, pp.328-337, 2006.

[P95] A. Pott, *Finite Geometry and Character Theory,* Springer-Verlag, Berlin-Heidelberg 1995.

[PV14] J. Pujol and M. Villanueva, "Binary codes. A MAGMA package," version 2.0, Universitat Autònoma de Barcelona, Accessed 21-09-2016 `http://ccsg/uab.cat`, 2014.

[RB+89] J. Rifà, J. M.Basart, L. Huguet *On Completely regular propelinear codes* AAECC-6 Proceedings of the 6th International Conference, on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pp. 341-355, 1989.

[RP97] J. Rifà and Pujol, J. *Translation-invariant propelinear codes,* IEEE Trans. Inf. Theory 43(2), pp.590-598, 1997.

[RR13] A. del Rio and J. Rifà, "Families of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 5140–5151, 2013.

[RS14] J. Rifà and E. Suárez-Canedo, *About a class of Hadamard propelinear codes,* Electron. Note Discr. Math., vol. 46, pp. 289-296, 2014.

[RS15] J. Rifà and E. Suárez-Canedo, *Kronecker sums to construct Hadamard full propelinear codes* in Proc. of the 21-st Conference on applications of Computer Algebra (ACA15), Kalamata, Greece, pp. 135-139, 20-23 July 2015.

[RS17] J. Rifà and E. Suárez-Canedo, *Hadamard full propelinear codes of type Q; rank and kernel.* Submitted to *Des. Codes and Cryptography*, arXiv:1709.02465v2, 2017.

[RM+99] K. H. Rosen, J. G. Michaels, J. L. Gross, J. H. Grossman, D. R. Shier, *Handbook of discrete and combinatorial mathematics* CRC Press, 1999.

[R52] H. J. Ryser, *Matrices with integer elements in combinatorial investigations,* Amer. J. Math., vol. 74, pp. 769-773, 1952.

[R63] H. J. Ryser, *Combinatorial Mathematics* Carus Mathematical Monographs No. 14. Mathematical Association of America, Washington, DC, 1963.

[S99] B. Schmidt, *Williamson matrices and a conjecture of Ito's,* Des. Codes, Cryptogr. 17, pp. 61-68 1999.

[S78] Seberry, J. *A class of group divisible designs.* Ars Combinatoria, pp. 151-152, 1978.

[SZ+71] N. V. Semakov, V. A. Zinoviev, and G. V. Zaitsev. *Uniformly packed codes,* Problemy Peredachi Informatsii, 7.1 , pp. 38-50, 1971.

[S48] C.E. Shannon, *A mathematical theory of communication.* Bell system technical journal, 27, 1948.

[S03] D. R. Stinson, *Combinatorial designs: Construction and Analysis* Springer-Verlag New York, 2003.

[S67] J. J. Sylvester, *Thoughts on Orthogonal Matrices, Simultaneous Sign Successions, and Tessellated Pavements in Two or More Colours, with Applications to Newton's Rule, Ornamental Tile Work, and the Theory of Numbers,* Phil. Mag., vol 34, pp.461-475, 1867.

[T33] J. A. Todd, *A Combinatorial Problem,* J. Math. and Phys. , vol. 12, pp. 321-333, 1933.

[T69] R. J. Turyn, *Complex Hadamard Matrices,* Combinatorial Structures and Their Applications, Gordon and Breach, New York, 1969.

[T72] R. J. Turyn, *An infinite class of Williamson matrices,* J. Combinatorial Theory Sect., vol. 12, pp. 319-321, 1972.

[W76] J. Wallis, *On the existence of Hadamard matrices*, J. Combinatorial Theory Ser. A 21, pp.444-451, 1976.

[W88] W. D. Wallis, *Combinatorial Designs,* Marcel Dekker, New York, 1988.

[W84] J. Williamson *Hadamard's determinant theorem and the sum of four squares* Duke Math J., vol 11, pp. 65-81, 1944.

[Y91] M. Yamada, *Hadamard matrices of generalised quaternion type*, Discr. Math. 87, pp. 187-196, 1991.

[Z00] V. Zinoviev, *On Generalized Concatenated Constructions of Perfect Binary Nonlinear Codes* Probl. Peredachi Inf., vol. 6, pp. 59–73, 2000.

Appendix A

HFP-codes of type Q. Rank and Kernel.

Des. Codes Cryptogr.
DOI 10.1007/s10623-017-0429-2

Hadamard full propelinear codes of type Q; rank and kernel

J. Rifà[1] · **Emilio Suárez Canedo**[1]

Received: 3 October 2016 / Revised: 5 October 2017 / Accepted: 9 October 2017

Abstract Hadamard full propelinear codes (HFP-codes) are introduced and their equivalence with Hadamard groups is proven; on the other hand, the equivalence of Hadamard groups, relative $(4n, 2, 4n, 2n)$-difference sets in a group, and cocyclic Hadamard matrices, is already known. We compute the available values for the rank and dimension of the kernel of HFP-codes of type Q and we show that the dimension of the kernel is always 1 or 2. We also show that when the dimension of the kernel is 2 then the dimension of the kernel of the transposed code is 1 (so, both codes are not equivalent). Finally, we give a construction method such that from an HFP-code of length $4n$, dimension of the kernel $k = 2$, and maximum rank $r = 2n$, we obtain an HFP-code of double length $8n$, dimension of the kernel $k = 2$, and maximum rank $r = 4n$.

Keywords Cocyclic Hadamard matrix · Hadamard code · Hadamard group · Kernel · Propelinear code · Rank · Relative difference set

Mathematics Subject Classification 5B · 5E · 94B

1 Introduction

Let $\mathbb{F}$ be the binary field. For any $v \in \mathbb{F}^n$, we define the support of v as the set of nonzero positions of v and we denote it by $\mathrm{Supp}(v)$. Denote by $\mathrm{wt}(x)$ the *Hamming weight* of a vector $x \in \mathbb{F}^n$ (i.e. the number of its nonzero positions). Given two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ from $\mathbb{F}^n$ we denote by $d(x, y)$ the *Hamming distance* between x and y (i.e., the number of positions i, where $x_i \neq y_i$). Let us denote by $e_i \in \mathbb{F}^n$ the vector with the

Communicated by J. D. Key.

J. Rifà
josep.rifa@uab.cat

1 Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193 Bellaterra, Spain

value of all coordinates zero, except the ith which is one. A binary *code* C of length n is a nonempty subset of $\mathbb{F}^n$. The elements of C are called *codewords*. Two structural properties of (nonlinear) codes are the dimension of the linear span and kernel. The *rank* of a binary code C, $r = \text{rank}(C)$, is the dimension of the linear span of C. The *kernel* of a binary code C is the set of codewords 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 denote the dimension of the kernel of C by $k = \ker(C)$. For a binary code C, $\text{Aut}(C)$ denotes the group of automorphisms of C, i.e. the set of coordinate permutations that fixes C setwise.

An *Hadamard matrix* of order n is a matrix of size $n \times n$ with entries ± 1, such that $HH^T = nI$, where I is the identity matrix and H^T means the transpose matrix of H. When $n > 1$ we can easily see that any two different rows (columns) of an Hadamard matrix agree in precisely $n/2$ coordinates and when $n > 2$ any three different rows (columns) agree in precisely $n/4$ coordinates. Thus, for $n > 2$, the order of an Hadamard matrix is always a multiple of 4. It is conjectured that the converse holds, i.e., there are Hadamard matrices of order $4n$, for any positive integer n [1].

Two *Hadamard matrices* are *equivalent* if one can be obtained from the other by permuting rows (or columns) or multiplying rows (or columns) by -1. With these 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 a (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 a (binary) Hadamard matrix and their complements is called a (binary) *Hadamard code*, which has $8n$ codewords, length $4n$ and minimum distance $2n$.

Elliott and Butson [6] define a *relative* (v, m, k, λ)*-difference set in a group* G relative to a normal subgroup $N \lhd G$, where $|G| = vm$ and $|N| = m$, as a subset D of G with $|D| = k$ such that the multiset of values $d_1 d_2^{-1}$ 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 D 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 an *Hadamard group* of order $8n$, in fact, a *left Hadamard group* using the following fine-tuned definition from [10].

Definition 1 A triple (G, D, u) is a left Hadamard group of order $8n$ if G is a finite group containing a prescribed $4n$-subset D and a prescribed central involution u (D is called the Hadamard subset corresponding to u), such that

(i) aD and D intersect in exactly $2n$ elements, for any $a \notin \langle u \rangle \subset G$,
(ii) aD and $\{b, bu\}$ intersect in exactly one element, for any $a, b \in G$.

Note that taking a in (ii) as the identity element of G we obtain that D and uD are disjoints and $D \cup uD = G$.

A right Hadamard group (G, D, u) can be characterized as a left Hadamard group over the opposite group G^{op} of G (the opposite group G^{op} of G, has the same underlying set as G and its group operation $\diamond$ is defined by $a \diamond b = b * a$).

From now on, when we use the term Hadamard group without any specification, we are referring to a left Hadamard group.

Hadamard matrices corresponding to Hadamard groups can also be obtained from 2-cocycles [4,7]. The concept of cocyclic Hadamard matrix was introduced in [9] and in [7] it is proven that cocyclic Hadamard matrices are equivalent to Ito's Hadamard groups. In [12], a special Hadamard group was introduced, called type Q. In this case G is a group of order

$8n$, $G = \langle \mathbf{a}, \mathbf{b} : \mathbf{a}^{4n} = e, \mathbf{a}^{2n} = \mathbf{b}^2, \mathbf{b}^{-1}\mathbf{a}\mathbf{b} = \mathbf{a}^{-1} \rangle$ with only one involution $u = \mathbf{a}^{2n} = \mathbf{b}^2$ which is central in G and where $\mathbf{e}$ means the neutral element.

Hadamard conjecture asserts that an Hadamard matrix of order $4n$ exists for every positive integer n. The smallest order for which no Hadamard matrix is known is 668, and at the time of [8] the smallest order for which no cocyclic Hadamard matrix is known is 188. Also, in [12], Ito conjectured that relative $(4n, 2, 4n, 2n)$-difference sets in groups of type Q exists for all positive integers n and he shows it is true for $n \leq 11$. Later [18] Ito's conjecture was verified for $n \leq 46$.

Let $\mathcal{S}_n$ denote the symmetric group of permutations of the set $\{1, \ldots, n\}$. For any $\pi \in \mathcal{S}_n$ and $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}^n$ we write $\pi(v)$ to denote $(v_{\pi^{-1}(1)}, v_{\pi^{-1}(2)}, \ldots, v_{\pi^{-1}(n)})$.

When we talk about a Hadamard group G we use e, u to refer the neutral element and the central involution in G, respectively. When we talk about binary codes we denote $\mathbf{e}$, $\mathbf{u}$ the all zeros and the all ones vector, respectively.

Definition 2 ([17]) A binary code C of length n, such that $\mathbf{e} \in C$, has a **propelinear** structure if for each codeword $x \in C$ there exists $\pi_x \in \mathcal{S}_n$ 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 $y \in \mathbb{Z}_2^n$, denote by $\cdot$ the binary operation such that $x \cdot y = x + \pi_x(y)$. Then, $(C, \cdot)$ is a group, which is not abelian in general. The zero vector $\mathbf{e}$ is the identity element and $\pi_{\mathbf{e}} = I$ is the identity permutation. Moreover, $x^{-1} = \pi_x^{-1}(x)$, for all $x \in C$ [17]. We call C a propelinear code if it has a propelinear structure.

The current paper is focused on the study and computation of the available parameters for the values of the rank and the dimension of the kernel of Hadamard codes corresponding to Hadamard groups of type Q. In Sect. 2 we introduce the HFP-codes (Hadamard full propelinear codes) and we show they are equivalent to Hadamard groups. We also show some properties for the kernel of these codes. In Sect. 3 we introduce the concept of HFP-codes of type Q, which correspond to Hadamard groups of type Q. We study the available values for the rank and the dimension of the kernel of HFP-codes of type Q and we show that the dimension of the kernel is always 1 or 2. In Sect. 4 we characterize HFP-codes with dimension of the kernel $k = 2$ and we show that the transposed matrix of an Hadamard matrix of type Q with $k = 2$ has the dimension of the kernel equal to 1, so both Hadamard matrices are not equivalent. Finally, in Sect. 5, we give a construction such that from an HFP-code of type Q, $k = 2$ and length $4n$, we obtain a new HFP-code of type Q, $k = 2$ and length $8n$ and we show that when the former code has maximum rank $r = 2n$ then the constructed code of double length has also maximum rank.

2 Hadamard full propelinear codes

We call $(C, \cdot)$ a propelinear Hadamard code if C is both, a propelinear code and an Hadamard code. In this section we introduce the concept of Hadamard full propelinear code and we show that it is equivalent to the well known concepts of Hadamard group, 2-cocyclic matrix and relative difference set.

Definition 3 ([16]) An HFP-code (Hadamard full propelinear code) is an 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 an* HFP*-code* $(C, \cdot)$ *the vector* $\mathbf{u}$ *is a central involution in* C.

Proof For any vector $a \in C$ we have $a\mathbf{u} = a + \pi_a(\mathbf{u}) = a + \mathbf{u} = \mathbf{u} + \pi_{\mathbf{u}}(a) = \mathbf{u}a$, so vector $\mathbf{u}$ is central in C. Also $\mathbf{u}^2 = \mathbf{u} + \pi_{\mathbf{u}}(\mathbf{u}) = \mathbf{u} + \mathbf{u} = \mathbf{e}$. □

Remark 1 Let $(C, \cdot)$ be an HFP-code of length $4n$ and let D_1 be the set of codewords with a zero in the first coordinate. The cardinality of D_1 is $4n$ and we can use D_1 as an indexing set for the coordinates of the elements in C. We will say that $x \in D_1$ is indexing the ith coordinate when

$$e_1 = \pi_x(e_i), \tag{1}$$

where e_i is defined in Introduction. Note that for any $i \in \{1, \ldots, 4n\}$ there is one and only one element $x \in D_1$ such that $e_1 = \pi_x(e_i)$ (otherwise, code C would not be full propelinear).

The value of the coordinate indexed by $x \in D_1$ in a vector $a \in C$ is zero or one, depending on the value of the first coordinate of $\pi_x(a)$. As $x \in D_1$, the value of the first coordinate of $\pi_x(a)$ is the same as in $x + \pi_x(a) = xa$. Hence, let $\delta_{(xa)} \in \{\mathbf{e}, \mathbf{u}\}$ be such that $\delta_{(xa)}xa \in D_1$, then the value of the coordinate indexed by $x \in D_1$ in vector $a \in C$ is given by $\gamma_{(xa)} \in \mathbb{Z}_2$, where $\gamma_{(xa)} = 0$ if and only if $\delta_{(xa)} = \mathbf{e}$. □

A previous version of the next statement was proved in [16] but we include a new proof here.

Proposition 1 *Let* $(C, \cdot)$ *be an* HFP*-code of length* $4n$ *and let* D_1 *be the set of codewords with a zero in the first coordinate. Then the triple* $(C, D_1, \mathbf{u})$ *is a left Hadamard group.*

Proof Since C is an HFP-code $\pi_x(e_1) \neq e_1$, except for $x \in \{\mathbf{e}, \mathbf{u}\}$. We have that $|D_1 \cap xD_1| = 4n$ if and only if $x = \mathbf{e}$, and $|D_1 \cap xD_1| = 0$ if and only if $x = \mathbf{u}$. For the other cases $\pi_x(e_1) = e_k$, where $e_1 \neq e_k$ and xD_1 is either D_k or $\mathbf{u}D_k$, depending on $x \in D_k$ or $x \notin D_k$, respectively, where D_k is the set of codewords with a zero in the kth position. In any case $|D_1 \cap xD_1| = 2n$. This proves the conditions in Definition 1. □

Vice versa, after Proposition 1, the next proposition shows that starting from a left Hadamard group (G, D, u) we can construct an HFP-code, isomorphic to G as a group, with D corresponding to the set of codewords with a zero in the first position and u corresponding to the all ones vector. A previous version of this result could be seen in [16].

Proposition 2 *Let* $(G, *)$ *be an Hadamard group of order* $8n$ *with* D *as the prescribed Hadamard subset corresponding to a central involution* u*. Then we can construct an* HFP*-code* C*, isomorphic to* G *as a group. This group isomorphism* $\sigma : G \to C$ *is such that* $\sigma(D) = D_1$ *and* $\sigma(u) = \mathbf{u}$*, where* D_1 *is the set of codewords of* C *with a zero in the first position corresponds and* $\mathbf{u}$ *is the all ones vector.*

Proof We can assume the identity element e of G is in D, otherwise we take as D the set $u * D$. From G we can construct a $4n \times 4n$ Hadamard matrix H, where the columns are indexed by the elements of D. Order the columns in such a way that $e \in D$ is indexing the first column. For $a, b \in D$, the entry (a, b) of H is 0 if $b * a \in D$ and 1 if $b * a \notin D$. We will say that the entry (a, b) of H is $\gamma_{(b*a)} \in \mathbb{Z}_2$, where $\gamma_{(b*a)} = 0$ if and only if $\delta_{(b*a)} = e$. The value of $\delta_{(b*a)} \in \{e, u\}$ is such that $\delta_{(b*a)} * b * a \in D$. For a fixed $a \in D$, the vector with entries (a, b), for $b \in D$ will be the corresponding codeword $\sigma(a)$ in the code C we are constructing. The first coordinate of codeword $\sigma(a)$ is zero.

First of all we show that H^T is an Hadamard matrix and so H is an Hadamard matrix too. Take two columns of H, indexed by $b, c \in D$, respectively. These two columns have the same value in the row position corresponding to codeword $\sigma(a)$ if and only if $\delta_{(b*a)} = \delta_{(c*a)}$ or, the same, if and only if either $a \in b^{-1} * D \cap c^{-1} * D$ or $a * u \in b^{-1} * D \cap c^{-1} * D$. Hence, since D is an Hadamard subset, there are $|b^{-1} * D \cap c^{-1} * D| = |c * b^{-1} * D \cap D| = 2n$ positions where the two different columns indexed by $b, c \in D$ coincide. As $e \in D$ then H is a normalized Hadamard matrix.

Now, we construct a full propelinear code C. The codewords of C are the rows (and the complements) of matrix H. For any $a \in G$, $\sigma(a)$ will be the corresponding row (or the complement) of H constructed from a. Obviously, $\sigma(e) = \mathbf{e}$ and $\sigma(u) = \mathbf{u}$.

For any $\sigma(a) \in C$ its coordinates are indexed by the elements in D and we define a map $\pi_{\sigma(a)} : C \longrightarrow \mathbb{F}^n$ by

$$\pi_{\sigma(a)}(\sigma(x)) = \sigma(a) + \sigma(a * x), \text{ for any } \sigma(x) \in C,$$

where the operation $+$ is the componentwise addition in $\mathbb{F}^n$. The map $\pi_{\sigma(a)}$ acts as a permutation on D. Specifically, the coordinate given by $b \in D$ is moved to the coordinate given by $\delta_{(b*a^{-1})} * b * a^{-1} \in D$. Indeed, take the element $x \in D$ to show that the value of the coordinate indexed by $b \in D$ in $\sigma(x)$ coincides with the value of the coordinate indexed by $\delta_{(b*a^{-1})} * b * a^{-1} \in D$ in $\pi_{\sigma(a)}(\sigma(x))$. The value of the coordinate indexed by b in $\sigma(x)$ is $\gamma_{(b*x)}$. The value of the coordinate indexed by $\delta_{(b*a^{-1})} * b * a^{-1}$ in $\sigma(a)$ is $\gamma_{(b*a^{-1})} + \gamma_b = \gamma_{(b*a^{-1})}$ ($\gamma_b = 0$ since $b \in D$). On the other hand, the value of the coordinate indexed by $\delta_{(b*a^{-1})} * b * a^{-1}$ in $\sigma(a * x)$ is $\gamma_{(b*a^{-1})} + \gamma_{(b*x)}$. So, we should check that $\gamma_{(b*x)} = \gamma_{(b*a^{-1})} + \gamma_{(b*a^{-1})} + \gamma_{(b*x)}$, which is obvious. Therefore, $\pi_{\sigma(a)}$ acts as a permutation on the set of coordinates.

For any $\sigma(a), \sigma(b) \in C$ we define $\sigma(a)\sigma(b) = \sigma(a) + \pi_{\sigma(a)}(\sigma(b)) = \sigma(a*b)$ which gives a propelinear structure on C. Indeed, the conditions in Definition 2 are fulfilled. The first one is straightforward. For the second condition we want to prove that, for all $\sigma(x), \sigma(y) \in C$, we have $\pi_{\sigma(x)}\pi_{\sigma(y)} = \pi_{\sigma(x)\sigma(y)}$. Take any $\sigma(z) \in C$ and compute $\pi_{\sigma(x)\sigma(y)}(\sigma(z)) = \pi_{\sigma(x*y)}(\sigma(z)) = \sigma(x * y) + \sigma((x * y) * z) = \sigma(x * y) + \sigma(x * (y * z)) = \sigma(x) + \pi_{\sigma(x)}(\sigma(y)) + \sigma(x) + \pi_{\sigma(x)}(\sigma(y * z)) = \pi_{\sigma(x)}(\sigma(y) + \sigma(y * z)) = \pi_{\sigma(x)}(\pi_{\sigma(y)}(\sigma(z)))$. This proves the statement. □

Remark 2 These two last propositions prove the equivalence of both concepts, Hadamard groups (G, D, u) and HFP-codes. If we begin with an HFP-code $(C, \cdot)$ we can consider the Hadamard group that such code gives rise to (Proposition 1) and then, from the Hadamard group we can construct an HFP-code which coincides with the initial one (Proposition 2 and Remark 1). Vice versa, starting from an Hadamard group (G, D, u) we can construct an HFP-code (which is isomorphic to G as a group), with $D_1 = \sigma(D)$ as the set of codewords with a zero in the first position and $\mathbf{u} = \sigma(u)$ as the all ones vector. This HFP-code coincides with the Hadamard group (G, D, u) (Proposition 1). □

It would seem, on the surface, that only left Hadamard groups are in one-to-one correspondence with HFP-codes. Next proposition shows that the correspondence is also for right Hadamard groups.

Proposition 3 *Let $(C, \cdot)$ be an* HFP*-code of length $4n$ and let D_1 be the set of codewords with a zero in the first coordinate. Then the triple $(C, D_1, \mathbf{u})$ is a right Hadamard group.*

Proof To show that $(C, D_1, \mathbf{u})$ is a right Hadamard group note that using all $a \in D_1$ the value of $\pi_a^{-1}(e_1)$ gives all e_i, for $i \in \{1, \ldots, 4n\}$, otherwise the code would not be full

propelinear. Indeed, if $\pi_a^{-1}(e_1) = \pi_b^{-1}(e_1)$, for $a, b \in D_1$, with $a \neq b$ then $\pi_{ab^{-1}}(e_1) = e_1$ which contradicts that C is HFP. Vectors in $D_1 \cap D_1 x$ are those in $\{a + \pi_a(x) : a \in D_1\}$ with a zero in the first coordinate, which coincides with those in $\{\pi_a(x) : a \in D_1\}$ with a zero in the first coordinate. The value of the first position in $\pi_a(x)$ is the value on the ith position of vector x, knowing that $\pi_a^{-1}(e_1) = e_i$. When we take all $a \in D_1$ the value of the first position in $\pi_a(x)$ take all values given by all positions of vector $x \notin \{\mathbf{e}, \mathbf{u}\}$, so half zeros and half ones. Hence, for $x \notin \{\mathbf{e}, \mathbf{u}\}$ we have $|D_1 \cap D_1 x| = 2n$. This proves the first condition in Definition 1. The second condition is obvious. □

Corollary 1 *If (G, D, u) is a left Hadamard group then (G, D, u) is a right Hadamard group; (G, D^{-1}, u) is a left Hadamard group and (G^{op}, D, u) is a left Hadamard group.*

Proof Let (G, D, u) be a left Hadamard group. From Propositions 3 and 2 we have that (G, D, u) is also a right Hadamard group. Now, (G^{op}, D, u) is a left Hadamard group and using the isomorphism $\phi : G^{\mathrm{op}} \to G$ such that $\phi(g) = g^{-1}$ we obtain that (G, D^{-1}, u) is also a left Hadamard group. □

It is worth to mention that in [11] it was proved that if (G, D, u) is a left Hadamard group then (G, D^{-1}, u) is also a left Hadamard group, considering the group ring of G over the field of complex numbers.

Let (G, D, u) be an Hadamard group. Following Proposition 2 construct the associated HFP-codes C, E to (G, D, u) and (G^{op}, D, u), respectively. It is easy to see that the corresponding normalized Hadamard matrices of codes C, E are transpose with one another. We will say that the HFP-code E is the *transpose code* of C.

Corollary 2 *Let C be an* HFP*-code of length $4n$ and $(C, D_1, \mathbf{u})$ the corresponding Hadamard group (Proposition 1). The transpose* HFP*-code of C has $(C, D_1^{-1}, \mathbf{u})$ as Hadamard group.*

Proof Straightforward from the proof of Corollary 1. □

Proposition 4 ([2]) *Let C be an* HFP*-code of length $4n$. Set $\Pi = \{\pi_x : x \in C\}$. Then $\mathbf{u} \in K(C)$ and Π is isomorphic to $C/\langle \mathbf{u} \rangle$.*

Proof The fact that $\mathbf{u} \in K(C)$ is straightforward. The map $x \longrightarrow \pi_x$ is a group homomorphism from C to Π. Since C is full propelinear, the kernel of this homomorphism is $\langle \mathbf{u} \rangle$. The statement is proven. □

Next proposition, proved in [16], extends a previous result by Ito in [10] where it was proved for a Sylow subgroup of C.

Proposition 5 ([16]) *Let $(C, \cdot)$ be an Hadamard propelinear code of length $4n$. Then $|C| = 8n$, but it is not a cyclic group of order $8n$.*

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 [15], and the other three cannot be realized as $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. However, one of those can be realized as a $\mathbb{Z}_2\mathbb{Z}_4 Q_8$-code, more specifically, as a pure Q_8-code [5]. As an easy example of HFP-codes it was shown in [16] that the last two are full propelinear codes, which are not translation invariant. The group structure of these two propelinear codes correspond to a generalized quaternion group of order 32.

3 Rank and kernel of HFP-codes of type Q

In this section we study the allowable values for the rank and for the dimension of the kernel of an HFP-code of type Q. The main result is that for HFP-codes of type Q and length $4n = 2^s n'$, where n' is odd and $s = 2$, we have rank $r = 4n - 1$ and dimension of the kernel $k = 1$; and when $s > 2$ we have rank $r \leq 2n$ and dimension of the kernel 1 or 2.

Proposition 6 *Let C be an Hadamard code of length $4n$ and $s \in K(C)$, $s \notin \{\mathbf{e}, \mathbf{u}\}$. Then, the projection of C onto* Supp(s) *is an Hadamard code of length $2n$.*

Proof Without loss of generality we can write s in the form (s_1, s_2) where $s_1 = (1, \ldots, 1)$, $s_2 = (0, \ldots, 0)$. Let $v = (v_1, v_2)$, $w = (w_1, w_2)$ be any two vectors in C. After projecting the $8n$ vectors of C over Supp(s) we have $2n$ different vectors and their complements. Indeed, exactly the vectors $v = (v_1, v_2)$, $w = (v_1, v_2 + \mathbf{u})$ goes to the same vector in the projection over the support of s. Hence, we want to prove that if $v_1 \neq w_1$ and $v_1 \neq w_1 + \mathbf{u}$ then $d(v_1, w_1) = n$.

Since $s \in K(C)$, for any $v \in C$ we have $s + v \in C$, so $(\mathbf{u} + v_1, v_2) \in C$ and for any $w \in C$ such that $v \neq w$, $v \neq w + \mathbf{u}$, $s + v \neq w$, $s + v \neq w + \mathbf{u}$ we have $d(s + v, w) = 2n$ and also $d(v, w) = 2n$. Hence, $d(v_1 + \mathbf{u}, w_1) + d(v_2, w_2) = 2n$ and $d(v_1, w_1) + d(v_2, w_2) = 2n$. Therefore, $d(v_1 + \mathbf{u}, w_1) = d(v_1, w_1)$ and since $\mathbf{u} + v_1$ is the complementary vector of v_1 we have $d(\mathbf{u} + v_1, w_1) + d(v_1, w_1) = 2n$. Thus, $d(v_1 + \mathbf{u}, w_1) = d(v_1, w_1) = n$. This proves the statement. □

Next three lemmas are well known. We include them without proof.

Lemma 2 ([3]) *Let $(C, \cdot)$ be a propelinear code of length $4n$.*

(i) *For $x \in C$ we have $x \in K(C)$ if and only if $\pi_x \in \mathrm{Aut}(C)$.*
(ii) *The kernel $K(C)$ is a subgroup of C and also a binary linear space.*
(iii) *If $c \in C$ then $\pi_c \in Aut(K(C))$ and $c \cdot K(C) = c + K(C)$.*

Lemma 3 ([13,14]) *Let C be a non linear Hadamard code of length $2^s n'$, where n' is odd. The dimension of the kernel is $1 \leq k \leq s - 1$.*

Lemma 4 ([1, Theorems 2.4.1 and 7.4.1]) *Let C be an Hadamard code of length $4n = 2^s n'$, where n' is odd.*

(i) *If $s = 2$ then $r = 4n - 1$.*
(ii) *If $s \geq 3$ then the rank of C is $r \leq 2n$, with equality if $s = 3$.*

Definition 4 Let C be an HFP-code of length $4n = 2^s n'$ with n' odd. We will say that C is a code of type Q when it is a group of type Q [12]

$$C = \langle \mathbf{a}, \mathbf{b} : \mathbf{a}^{4n} = \mathbf{e}, \mathbf{a}^{2n} = \mathbf{b}^2, \mathbf{b}^{-1}\mathbf{a}\mathbf{b} = \mathbf{a}^{-1} \rangle.$$

An HFP-code C of type Q contains only one involution $\mathbf{a}^{2n} = \mathbf{b}^2 = \mathbf{u}$ which is central in C.

The interest of studying HFP-codes of type Q is given by a conjecture of Ito stated in [12] saying that for any length $4n$ it is possible to find an Hadamard group of type Q.

Proposition 7 *Let $C = \langle \mathbf{a}, \mathbf{b} \rangle$ be an* HFP*-code of type Q and length $4n = 2^s n'$ with n' odd. Then*

(i) *Code C is linear if and only if the two following conditions are satisfied:* $4n = 2^s$, $r = k = s + 1$.
(ii) *If C is not linear then* $\mathbf{a} \notin K(C)$.
(iii) *If $s = 2$ then $r = 4n - 1$ and $k = 1$.*

Proof First item is straightforward.

For the second item, deny the statement, so assume that $\mathbf{a} \in K(C)$. Then $\langle \mathbf{a} \rangle \subset K(C)$ and so $|C/K(C)| \leq 2$. We conclude that $C = K(C)$ and C is a linear code or else $|K(C)| = 2^s n'$, with $n' = 1$, which contradicts Lemma 3.

The third item is straightforward from Lemmas 3 and 4. □

Lemma 5 *Let $(C, \cdot)$ be a propelinear code of length $4n$. To check that C is an Hadamard code it is enough to check that $(C, \cdot)$ has $8n - 2$ codewords (different from $\mathbf{e}, \mathbf{u}$) and that the weight of all these codewords is $2n$.*

Proof Let $x, y \in C$ and set $z = x^{-1} \cdot y \in C$. We have $y = x \cdot z = x + \pi_x(z)$ and then $d(x, y) = \mathrm{wt}(x + y) = \mathrm{wt}(\pi_x(z)) = \mathrm{wt}(z)$. Hence, we see that the distance of any two codewords can be computed through the weight of a codeword. When $x \neq y$ or $x \neq y + \mathbf{u}$ then $z \notin \{\mathbf{e}, \mathbf{u}\}$ and so we only require that $\mathrm{wt}(z) = 2n$ for all $8n - 2$ codewords different from $\mathbf{e}, \mathbf{u}$. This proves the statement. □

Proposition 8 *Let $C = \langle \mathbf{a}, \mathbf{b} \rangle$ be an* HFP*-code of type Q and length $4n$. Then, up to equivalence, we can assume*

(i) $\pi_{\mathbf{a}} = (1, 2, \ldots, 2n)(2n + 1, 2n + 2, \ldots, 4n)$,
(ii) $\pi_{\mathbf{b}} = (1, 4n)(2, 4n - 1) \ldots (2n, 2n + 1)$,
(iii) $\Pi = C/\langle \mathbf{u} \rangle$ *is the dihedral group $\mathcal{D}_{2n}$ of order $4n$,*

Proof Take $\mathbf{a} \in C$ and see that since it is of order $4n$ then the associated permutation $\pi_{\mathbf{a}}$ is of order $2n$. Indeed, if for $r < 2n$ we have $\pi_{\mathbf{a}}^r = I$ then $\mathbf{a}^{2r} = \mathbf{a}^r + \pi_{\mathbf{a}^r}(\mathbf{a}^r) = \mathbf{a}^r + \pi_{\mathbf{a}}^r(\mathbf{a}^r) = \mathbf{e}$, which contradicts that $\mathbf{a}$ is of order $4n$. Therefore we can think of $\pi_{\mathbf{a}}$ as two disjoint cycles of length $2n$, say for instance $\pi_{\mathbf{a}} = (1, 2, \ldots, 2n)(2n + 1, \ldots, 4n)$. In the case of $\pi_{\mathbf{b}}$, with an analogous argumentation as before we can say that it is of order two and so $\pi_{\mathbf{b}}$ is a composition of $2n$ disjoint transpositions. Each one of the transpositions sends an element of the first part of $\{1, 2, \ldots, 4n\}$ to the second part and vice versa. Indeed, assume for instance that $\pi_{\mathbf{b}}$ moves the first position to the $(2n + i)$th, where $i \leq 2n$, which is the same position that we obtain using $\pi_{\mathbf{a}^{i-1}}$, so $\pi_{\mathbf{b}^{-1}\mathbf{a}^{i-1}}$ has a fixed point which contradicts that C is full propelinear. Furthermore, if we assume that $\pi_{\mathbf{b}}$ moves, for instance, the first position to the ith position in the second part of $\{1, 2, \ldots, 4n\}$ then $\pi_{\mathbf{b}}$ is uniquely determined. Indeed, as $\pi_{\mathbf{b}}\pi_{\mathbf{a}} = \pi_{\mathbf{a}}^{-1}\pi_{\mathbf{b}}$ we have that $2n$ is moved to 1 by $\pi_{\mathbf{a}}$, 1 is moved to $(2n + i)$ by $\pi_{\mathbf{b}}$ and $(2n + i)$ is moved to $(2n + i + 1)$ by $\pi_{\mathbf{a}}$. Hence, $2n$ is moved to $(2n + i + 1)$ by $\pi_{\mathbf{b}}$, and so on. Hence, $\pi_{\mathbf{b}} = (1, 2n + i)(2n, 2n + i + 1)(2n - 1, 2n + i + 2) \ldots (2, 2n + i - 1)$. Items $i)$ and $ii)$ are proven. Item $iii)$ is straightforward from the definition of $\pi_{\mathbf{a}}$ and $\pi_{\mathbf{b}}$. □

In Remark 1, for a generic HFP-code C, we showed that we can consider the coordinates of any vector indexed by the elements of D_1 (the set of codewords with a zero in the first coordinate) in such a way that for any $x \in D_1$ the indexed coordinate is the ith such that $e_1 = \pi_x(e_i)$.

The value of the ith coordinate (indexed by $x \in D_1$) of an element $y \in C$ is given by $\gamma_{(xy)} \in \mathbb{Z}_2$, where $\gamma_{(xy)} = 0$ if and only if $\delta_{(xy)} = \mathbf{e}$. The value of $\delta_{(xy)} \in \{\mathbf{e}, \mathbf{u}\}$ is such that $\delta_{(xy)}xy \in D_1$.

Now, after Proposition 8 it is important not only to have the coordinates indexed by the elements in D_1, but also to order the elements in D_1 in such a way that the permutations of elements of C be in the form given in that proposition. Hence, fix $\mathbf{e} \in D_1$ as the index for the first coordinate. From Proposition 8 the second coordinate should be indexed by x such that $e_2 = \pi_{\mathbf{a}}(e_1)$ and $e_1 = \pi_x(e_2)$ (see Eq. (1)). Hence, $e_1 = \pi_{x\mathbf{a}}(e_1)$ which means that either $x\mathbf{a} = \mathbf{e}$ or $x\mathbf{a} = \mathbf{u}$, so and $x = \mathbf{a}^{-1}$, up to complement. Again, the third coordinate should be indexed by y such that $e_3 = \pi_{\mathbf{a}^2}(e_1)$ and $e_1 = \pi_y(e_3)$ (see Eq. (1)). Hence, $e_1 = \pi_{y\mathbf{a}^2}(e_1)$ which means that either $y\mathbf{a}^2 = \mathbf{e}$ or $y\mathbf{a}^2 = \mathbf{u}$, so $y = \mathbf{a}^{-2}$, up to complement. Again and again we will obtain that the coordinates 1st, 2nd, ..., $2n$th are indexed by the elements in D_1 corresponding (up to complement) to $\mathbf{e}, \mathbf{a}^{-1}, \ldots, \mathbf{a}^{-2n+1} = \mathbf{au}$, respectively.

Now, considering permutation $\pi_{\mathbf{b}}$ in Proposition 8, the $2n+1$th coordinate is indexed by x such that $e_{2n+1} = \pi_{\mathbf{b}}(e_{2n})$ and $e_1 = \pi_x(e_{2n+1})$ (see Eq. (1)). Also $\pi_{\mathbf{a}}^{2n-1}(e_1) = e_{2n}$. Hence, $e_1 = \pi_x(e_{2n+1}) = \pi_{x\mathbf{b}}(e_{2n}) = \pi_{x\mathbf{b}\mathbf{a}^{2n-1}}(e_1)$ which means that $x\mathbf{b}\mathbf{a}^{2n-1} = \mathbf{e}$ and so $x = \mathbf{a}^{-(2n-1)}\mathbf{b}^{-1}$ or $x = \mathbf{ab}$, up to complement. And again, with the same argumentation, we obtain that the coordinates $(2n+1)$th, $(2n+2)$th, ..., $4n$th are indexed by the elements in D_1 corresponding (up to complement) to $\mathbf{ab}, \mathbf{a}^2\mathbf{b}, \ldots, \mathbf{b}$, respectively.

Summarizing, we have the following remark which will be used throughout the paper.

Remark 3 Let $C = \langle \mathbf{a}, \mathbf{b} \rangle$ be an HFP-code of type Q and length $4n$. The coordinates of the elements in C are indexed by the elements in D_1 (the set of vectors with a zero in the first coordinate) in such a way that the ith coordinate is indexed by $b \in D_1$ such that $e_1 = \pi_b(e_i)$. We have that the coordinates 1st, 2nd, ..., $2n$th, $(2n+1)$th, $(2n+2)$th, ..., $4n$th are indexed by the elements in D_1 corresponding (up to complement) to $\mathbf{e}, \mathbf{a}^{-1}$, ..., $\mathbf{a}$, $\mathbf{ab}$, $\mathbf{a}^2\mathbf{b}$, ..., $\mathbf{b}$, respectively.

Also, we have that the value of the coordinate indexed by $x \in D_1$ in vector $y \in D_1$ is given by $\gamma_{(xy)} \in \mathbb{Z}_2$, where $\gamma_{(xy)} = 0$ if and only if $\delta_{(xy)} = \mathbf{e}$. The value of $\delta_{(xy)} \in \{\mathbf{e}, \mathbf{u}\}$ is such that $\delta_{(xy)}xy \in D_1$. The Hadamard matrix H constructed using as rows the vectors $y \in D_1$ is a normalized Hadamard matrix. In general, for any $x, y \in C$ we can say that the value of the coordinate indexed by x (or the complement when $x \notin D_1$) in vector y is given by

$$\gamma_x + \gamma_y + \gamma_{(xy)} \in \mathbb{Z}_2. \tag{2}$$

Analogously, from Corollary 2 the code C^T is an HFP-code of type Q with corresponding Hadamard group $(C, D_1^{-1}, \mathbf{u})$. The coordinates of elements in C^T are indexed by the elements in D_1^{-1} and, with the same argumentation as for code C, we will take the coordinates ordered in such a way that the permutations associated to elements in C^T coincides with those Proposition 8. The order is given by: $\mathbf{e}, \mathbf{a}, \ldots, \mathbf{a}^{2n-1}, \mathbf{ab}, \mathbf{a}^2\mathbf{b}, \ldots, \mathbf{a}^{2n}\mathbf{b}$. □

Note that both Hadamard groups $(C, D_1, \mathbf{u})$ and $(C, D_1^{-1}, \mathbf{u})$ have the same elements and the same group structure. However, the binary representation of these elements, which depends on the Hadamard subset, could be different (in the first case we are talking about the rows of H and in the second case about the columns).

Before going to the next proposition we will take the elements of C in a polynomial way, so the nonzero coefficients of $(a_1(x), a_2(x))$ are those in $\mathrm{Supp}(\mathbf{a})$, where $a_1(x), a_2(x) \in \mathbb{F}[x]$ have degree at most $2n-1$. Permutation π_a corresponds to multiplying by x modulo $x^{2n}-1$ and so we have the correspondence $\mathbf{a}^i \leftrightarrow \big((1+x+x^2+\cdots+x^{i-1})a_1(x), (1+x+x^2+\cdots+x^{i-1})a_2(x)\big) = \big(\frac{x^i-1}{x-1}a_1(x), \frac{x^i-1}{x-1}a_2(x)\big)$. Analogously, the nonzero coefficients of $(b_1(x), b_2(x))$ are those in $\mathrm{Supp}(\mathbf{b})$, where $b_1(x), b_2(x) \in \mathbb{F}[x]$ have degree at most $2n-1$.

Given a polynomial $p(x)$ of degree at the most $2n-1$, we will call $\varphi_1(p(x)) = x^{2n-1}p(\frac{1}{x})$ and note that $\varphi_1(p(x))$ is not exactly the reciprocal polynomial of $p(x)$ but coincides with it in the case the degree of $p(x)$ is $2n-1$.

Denote by $u(x)$ the polynomial with all the coefficients 1 and by $e(x)$ the zero polynomial.

Proposition 9 *Let $C = \langle \mathbf{a}, \mathbf{b} \rangle$ be an* HFP*-code of type Q and length $4n$. Then, if we know the value of $\mathbf{a}$ then we can compute $\mathbf{b}$ in a unique way, up to complement.*

Proof We will take the elements in C in a polynomial way, so $(a_1(x), a_2(x))$ is the polynomial representation of $\mathbf{a}$. Permutation $\pi_{\mathbf{b}}$ takes $(a_1(x), a_2(x))$ to $(\varphi_1(a_1(x)), \varphi_1(a_2(x)))$.

From $\mathbf{ab} = \mathbf{ba}^{-1}$ we can write $\mathbf{b} + \pi_{\mathbf{a}}(\mathbf{b}) = \mathbf{a} + \pi_{\mathbf{b}}(\mathbf{a}^{-1}) = \mathbf{a} + \pi_{\mathbf{ab}}(\mathbf{a})$ (indeed, $\mathbf{a}^{-1} = \pi_{\mathbf{a}^{-1}}(\mathbf{a})$). Vector $\mathbf{b}$ and $\pi_{\mathbf{a}}(\mathbf{b})$ have the same parity, so $\mathbf{a}+\pi_{\mathbf{ab}}(\mathbf{a})$ has even parity. Using polynomials we have $(x+1)b_i(x) = a_i(x) + x\varphi_1(a_{i'}(x)) \pmod{x^{2n}-1}$, for $i, i' \in \{1,2\}$, $i \neq i'$. Polynomials $a_i(x) + x\varphi_1(a_{i'}(x)) \pmod{x^{2n}-1}$ are multiples of $x+1$ (indeed, $\mathbf{a} + \pi_{\mathbf{ab}}(\mathbf{a})$ has even parity). Hence, $b_i(x) = \frac{a_i(x)+x\varphi_1(a_{i'}(x)) \pmod{x^{2n}-1}}{x-1}$ for $i, i' \in \{1,2\}$, $i \neq i'$. Note that, as $x-1$ divides $x^{2n}-1$, the solution of the equation giving $b_i(x)$ is unique up to complement. □

A rough bound for r, depending on k, is established in the following lemma.

Lemma 6 *Let C be an Hadamard code of length $2^s n'$, where n' is odd. The rank r of C fulfills $r \leq \frac{2^{s+1}n'}{2^k} + k - 1$, where k is the dimension of the kernel.*

Proof Let k be the dimension of the the kernel $K(C)$, then we can see C as a disjoin union of, at the most, $\frac{2^{s+1}n'}{2^k}$ cosets of $K(C)$. Hence, the rank of C will be, at the most, $r \leq \frac{2^{s+1}n'}{2^k} - 1 + k$. □

Lemma 7 *Let $C = \langle \mathbf{a}, \mathbf{b} \rangle$ be an* HFP*-code of type Q and length $4n$. Let h be a divisor of n. Then $\pi_{\mathbf{a}}^h(\mathbf{a}^n) \neq \mathbf{a}^n$.*

Proof Indeed, assume the contrary, so $\pi_{\mathbf{a}}^h(\mathbf{a}^n) = \mathbf{a}^n$, where $n = hh'$. Hence, $\mathbf{u} = \mathbf{a}^{2n} = \mathbf{a}^n + \pi_{\mathbf{a}}^n(\mathbf{a}^n) = \mathbf{a}^n + (\pi_{\mathbf{a}}^h)^{h'}(\mathbf{a}^n) = \mathbf{a}^n + \mathbf{a}^n = \mathbf{e}$, which is impossible. □

Next theorem is one of the main results in the paper. It summarizes the values of the rank and dimension of the kernel for HFP-codes of type Q.

Theorem 1 *Let $C = \langle \mathbf{a}, \mathbf{b} \rangle$ be a non linear* HFP*-code of type Q and length $4n = 2^s n'$, where n' is odd. Let r, k be the rank and the dimension of the kernel of C, respectively.*

1. *If $s = 2$ then C is a full rank code, so $r = 4n - 1$ and $k = 1$.*
2. *If $s = 3$ then $r = 2n$ and $k \in \{1, 2\}$.*
3. *If $s > 3$ then $r \leq 2n$ and $k \in \{1, 2\}$.*

Proof The first and second items, as far as the rank is concerned, comes from Proposition 7 and Lemma 4. For the dimension of the kernel in the second item we use Lemmas 6 and 3.

For the third item, we begin by showing that $\mathbf{a}^n \notin K(C)$. Assume the contrary. From Lemma 2, $\pi_{\mathbf{a}} \in \mathrm{Aut}(K(C))$ and also, since $K(C)$ is a linear space and $\pi_{\mathbf{a}}$ is a linear morphism, $\pi_{\mathbf{a}}$ is a linear isomorphism of $K(C)$. We have $|K(C)| = 2^k$. The amount of available values for $\pi_{\mathbf{a}}(\mathbf{a}^n)$ is upper bounded by $2^k - 2$ so, if i is the smallest index $i \leq 2n$ such that $\pi_{\mathbf{a}}^i(\mathbf{a}^n) = \mathbf{a}^n$ then (Lemma 3),

$$i \leq 2^k - 2 \leq 2^{s-1} - 2. \tag{3}$$

We know that $\mathbf{u} = \mathbf{a}^{2n} = \mathbf{a}^n + \pi_{\mathbf{a}^n}(\mathbf{a}^n)$. We have $\pi_{\mathbf{a}}^n(\mathbf{a}^n) = \mathbf{a}^n + \mathbf{u}$ and $\pi_{\mathbf{a}}^{2n}(\mathbf{a}^n) = \mathbf{a}^n$. Set $d = \gcd(i, n)$ with $d = \lambda i + \mu n$, for some integers λ, μ. Compute $\pi_{\mathbf{a}}^d(\mathbf{a}^n) = \mathbf{a}^n + \delta\mathbf{u}$, where δ has the value 0, 1, depending on the parity of μ is either even or odd, respectively. Hence, $2d \geq i$ and d is a proper divisor of i (otherwise, i would be a divisor of n, which is impossible from Lemma 7) and therefore $2d = i$.

Hence, d is a divisor of n and $2d = i$ is not a divisor of n. As $n = 2^{s-2}n'$ we have $d = 2^{s-2}n^*$, where $n^* \mid n'$. Finally, $i = 2d = 2^{s-1}n^* \geq 2^{s-1}$, which contradicts (3). This proves that $\mathbf{a}^n \notin K(C)$).

The order of elements in $K(C)$ has to be a power of two (indeed, the order of the group $K(C)$ is a power of two). Thus, if $\mathbf{a}^i \in K(C)$ then take $j = \gcd(i, 4n)$ and note that also $\mathbf{a}^j \in K(C)$, where j divides $4n$. Therefore, for some ν, $2^\nu j = 4n$. Hence, as $\mathbf{a}^n \notin K(C)$ we should have $j \in \{2n, 4n\}$ and also $i \in \{2n, 4n\}$. Therefore, the elements in $K(C)$ different from $\mathbf{e}, \mathbf{u}$ should be of the form $\mathbf{a}^i\mathbf{b}$. But if two of them, say $\mathbf{a}^i\mathbf{b}, \mathbf{a}^j\mathbf{b}$, with $i \neq j$ and $i \neq 2n + j$, are in $K(C)$ then also $\mathbf{a}^{i-j} \in K(C)$, which is impossible.

Finally, the kernel is generated, at the most, by only one element different from $\mathbf{u}$, say it is $\boldsymbol{\kappa} = \mathbf{a}^\iota\mathbf{b}$, for some $\iota \in \{0, 1, \ldots, 2n - 1\}$. The dimension of the kernel is 1 or 2. For the rank, the statement comes from Lemma 4. □

4 HFP-codes of type Q. The transpose

Next step is to go further with the specific HFP-codes of type Q and length $4n = 2^s n'$, where n' is odd. We show that the transpose of an HFP-code of type Q and dimension of the kernel $k = 2$ has always dimension of the kernel equal to 1.

Proposition 10 *Let $C = \langle \mathbf{a}, \mathbf{b} \rangle$ be an* HFP*-code of type Q and length $4n$. Assume that the permutations associated to the elements $\mathbf{a}, \mathbf{b}$ are those in Proposition 8. If the dimension of the kernel is $k = 2$ then the vector $\boldsymbol{\kappa}$ in the kernel, different from $\mathbf{e}, \mathbf{u}$, with a zero in the first coordinate is*

$$\boldsymbol{\kappa} = (\mathbf{v}||\mathbf{w}), \text{ where } \mathbf{v} = (0, 1, 0, 1, \ldots, 0, 1) \text{ and either } \mathbf{w} = \mathbf{v} \text{ or } \mathbf{w} = \mathbf{v} + \mathbf{u}.$$

Proof Since the dimension of the kernel is 2, there exists an element $\boldsymbol{\kappa} \in C$, different from $\mathbf{u}$, belonging to the kernel. Since $\boldsymbol{\kappa}^2$ is also in the kernel and it is different from $\boldsymbol{\kappa}$ or $\boldsymbol{\kappa}\mathbf{u}$ we have $\boldsymbol{\kappa}^2 = \mathbf{u}$ or $\boldsymbol{\kappa}^2 = \mathbf{e}$. Then, the associated permutation $\pi_{\boldsymbol{\kappa}}$ should be such that $\pi_{\boldsymbol{\kappa}}^2 = I$ and so either $\boldsymbol{\kappa} = \mathbf{a}^n$ or $\boldsymbol{\kappa} = \mathbf{a}^i\mathbf{b}$, for some $i \in \{0, \ldots, 2n - 1\}$.

From Lemma 2 we have $\pi_{\mathbf{a}} \in \mathrm{Aut}(K(C))$ and so $\pi_{\mathbf{a}}(\boldsymbol{\kappa}) \in \{\boldsymbol{\kappa}, \boldsymbol{\kappa}\mathbf{u}\}$. As n is even we have $\pi_{\mathbf{a}}^n(\boldsymbol{\kappa}) = \boldsymbol{\kappa}$ so, from Lemma 7, $\boldsymbol{\kappa} = \mathbf{a}^i\mathbf{b}$, for some $i \in \{0, 1, \ldots, 2n - 1\}$. Again, from Lemma 2, we have $\pi_{\mathbf{a}}(\boldsymbol{\kappa}) = \boldsymbol{\kappa} + \epsilon$, where $\epsilon \in \{\mathbf{e}, \mathbf{u}\}$. Hence, we are in one of the following cases:

(i) $\boldsymbol{\kappa} = (1, 1, \ldots, 1||0, 0, \ldots, 0) + \epsilon$,
(ii) $\boldsymbol{\kappa} = (\mathbf{v}||\mathbf{w})$, where $\mathbf{v}, \mathbf{w} \in \{(1, 0, 1, 0, \ldots, 1, 0), (0, 1, 0, 1, \ldots, 0, 1)\}$.

Note that the first item could not happen. Indeed, by projecting the vectors to the first $2n$ coordinates, we obtain an Hadamard code of length $2n$ (Proposition 6). This code is a cyclic group of order $4n$ generated by the projection of $\mathbf{a}$, which contradicts Proposition 5. This proves the statement. □

Summarizing the above results, we conclude with the following Proposition.

Proposition 11 *Let $C = \langle \mathbf{a}, \mathbf{b} \rangle$ be an* HFP*-code of type Q, length $4n$ and dimension of the kernel $k = 2$. Let $\boldsymbol{\kappa}$ be the vector in the kernel, different from e,u, with a zero in the first coordinate. Then, up to equivalence,*

(i) $\pi_{\mathbf{a}} = (1, 2, \ldots, 2n)(2n+1, 2n+2, \ldots, 4n)$,
(ii) $\pi_{\mathbf{b}} = (1, 4n)(2, 4n-1) \cdots (2n, 2n+1)$,
(iii) $\boldsymbol{\kappa} = \mathbf{a}^{\iota}\mathbf{b}$, *up to complement, for some* $\iota \in \{0, \ldots, 2n-1\}$ *and either* $\boldsymbol{\kappa} = (\mathbf{v}||\mathbf{v}) \in K(C)$, *when ι is even, or* $\boldsymbol{\kappa} = (\mathbf{v}||\mathbf{w}) \in K(C)$, *when ι is odd, where* $\mathbf{v} = (0, 1, \ldots, 0, 1)$, $\mathbf{w} = \mathbf{v} + \mathbf{u}$.
(iv) $\mathbf{a} = (\mathbf{a}_1||\mathbf{a}_2)$ *where, in polynomial way,* $a_2(x) = x^{\iota+1}\varphi_1(a_1(x)) + u(x)$, $u(x)$ *is the polynomial of degree* $2n-1$ *with all the coefficients 1, and ι is the exponent in the above item iii).*

Proof Items (i), (ii) are straightforward from the previous results.

For item *iii*), note that the two non trivial elements in the kernel are $\boldsymbol{\kappa} = \mathbf{a}^{\iota}\mathbf{b}$ and $\boldsymbol{\kappa}\mathbf{u}$, for some index $\iota \in \{0, \ldots, 2n-1\}$. Take the vector $\boldsymbol{\kappa} = \mathbf{a}^{\iota}\mathbf{b}$ (the first coordinate may be zero or one). We know that $\boldsymbol{\kappa}^2 = \mathbf{u}$ and so $\mathbf{u} = \boldsymbol{\kappa} + \pi_{\boldsymbol{\kappa}}(\boldsymbol{\kappa}) = \boldsymbol{\kappa} + \pi_{\mathbf{a}^{\iota}}\pi_{\mathbf{b}}(\boldsymbol{\kappa})$. Hence, if ι is even then, up to complement, $\kappa = (\mathbf{v}||\mathbf{v})$ and if ι is odd then $\kappa = (\mathbf{v}||\mathbf{w})$, where $\mathbf{v} = (0, 1, \ldots, 0, 1)$, $\mathbf{w} = (1, 0, \ldots, 1, 0)\}$.

Item *iv*) comes from the same argumentation as in Proposition 9, where instead of $\mathbf{b}$ we use $\mathbf{a}^{\iota}\mathbf{b}$. Indeed, from $\boldsymbol{\kappa}\mathbf{a}^{-1} = \mathbf{a}\boldsymbol{\kappa}$ we obtain $\boldsymbol{\kappa} + \pi_{\boldsymbol{\kappa}}(\mathbf{a}^{-1}) = \mathbf{a} + \pi_{\mathbf{a}}(\boldsymbol{\kappa})$, so $\boldsymbol{\kappa} + \pi_{\mathbf{a}}(\boldsymbol{\kappa}) = \mathbf{a} + \pi_{\boldsymbol{\kappa}}(\mathbf{a}^{-1}) = \mathbf{a} + \pi_{\mathbf{a}^{\iota}}\pi_{\mathbf{b}}(\mathbf{a}^{-1}) = \mathbf{a} + \pi_{\mathbf{a}^{\iota}}\pi_{\mathbf{b}}\pi_{\mathbf{a}^{-1}}(\mathbf{a}) = \mathbf{a} + \pi_{\mathbf{a}^{\iota+1}}\pi_{\mathbf{b}}(\mathbf{a})$. But, $\mathbf{u} = \boldsymbol{\kappa} + \pi_{\mathbf{a}}(\boldsymbol{\kappa})$ so, in a polynomial way, $u(x) = a_1(x) + x^{\iota+1}\varphi_1(a_2(x))$ and $a_1(x) = x^{\iota+1}\varphi_1(a_2(x)) + u(x)$.

Analogously, $a_2(x) = x^{\iota+1}\varphi_1(a_1(x)) + u(x)$. This proves the statement. □

Theorem 2 *Let $C = \langle \mathbf{a}, \mathbf{b} \rangle$ be an* HFP*-code of type Q and length $4n$ and dimension of the kernel $k = 2$. Then, the dimension of the kernel of the transpose* HFP*-code is 1.*

Proof Let H be a normalized Hadamard matrix where the rows are elements of C and, from Remark 3, the coordinates of these elements are indexed by the elements in D_1 (the set of vectors with a zero in the first coordinate) with the order given by: $\mathbf{e}$, $\mathbf{a}^{-1}$, …, $\mathbf{a}^{-(2n-1)}$, $\mathbf{ab}$, $\mathbf{a}^2\mathbf{b}$, …, $\mathbf{a}^{2n}\mathbf{b}$. The columns of H are elements of C^T (Corollary 2) and their coordinates are indexed by the elements in D_1^{-1} with the corresponding order: $\mathbf{e}$, $\mathbf{a}$, …, $\mathbf{a}^{(2n-1)}$, $\mathbf{ab}$, $\mathbf{a}^2\mathbf{b}$, …, $\mathbf{a}^{2n}\mathbf{b}$.

Now, we assume that the dimension of the kernel is 2 in both codes C and C^T so we can use the results in Proposition 11 for both codes. We prove that this assumption leads to us to a contradiction.

Let $\boldsymbol{\kappa}_1 = \mathbf{a}^{\iota}\mathbf{b} \in K(C)$ (respectively, $\boldsymbol{\kappa}_2 = \mathbf{a}^{\bar{\iota}}\mathbf{b} \in K(C^T)$) the vector in the kernel of C (respectively, C^T) different from $\mathbf{e}$, $\mathbf{u}$ and with a zero in the first coordinate.

First of all we are going to see that the parity of $\iota, \bar{\iota}$ is different from each other. Deny the proposal and assume that $\iota, \bar{\iota}$ have the same parity. So, the row indexed by $\mathbf{a}^{\iota}\mathbf{b}$ and the column indexed by $\mathbf{a}^{\bar{\iota}}\mathbf{b}$ are equal. Consider the row indexed by $\mathbf{a}^{\iota}\mathbf{b}$ and compute the value of its coordinates, indexed by all different $\mathbf{a}^j\mathbf{b}$, for $j \in \{0, \cdots, 2n-1\}$. From Eq. (2) these values are given by $\gamma_{\mathbf{a}^{\iota}\mathbf{b}} + \gamma_{\mathbf{a}^j\mathbf{b}} + \gamma_{(\mathbf{a}^j\mathbf{b})(\mathbf{a}^{\iota}\mathbf{b})} = \gamma_{\mathbf{a}^{\iota}\mathbf{b}} + \gamma_{\mathbf{a}^j\mathbf{b}} + \gamma_{\mathbf{a}^{j-\iota}} + \gamma_{\mathbf{u}}$. Row vectors $\mathbf{a}^j\mathbf{b}$, in the coordinate indexed by $\mathbf{a}^{\bar{\iota}}\mathbf{b}$, have the following value: $\gamma_{\mathbf{a}^{\bar{\iota}}\mathbf{b}} + \gamma_{\mathbf{a}^j\mathbf{b}} + \gamma_{(\mathbf{a}^{\bar{\iota}}\mathbf{b})(\mathbf{a}^j\mathbf{b})} = \gamma_{\mathbf{a}^{\bar{\iota}}\mathbf{b}} + \gamma_{\mathbf{a}^j\mathbf{b}} + \gamma_{\mathbf{a}^{\bar{\iota}-j}} + \gamma_{\mathbf{u}}$.

Assuming that the row indexed by $\mathbf{a}^{\iota}\mathbf{b}$ coincides with the column indexed by $\mathbf{a}^{\bar{\iota}}\mathbf{b}$ we would have that these two previous values coincides, so:

$$\gamma_{\mathbf{a}^{j-\iota}} + \gamma_{\mathbf{a}^{\bar{\iota}-j}} = \gamma_{\mathbf{a}^{\bar{\iota}}\mathbf{b}} + \gamma_{\mathbf{a}^{\iota}\mathbf{b}}, \quad \text{for all } j \in \{0, \ldots, 2n-1\}. \tag{4}$$

Now, as $\iota, \bar{\iota}$ have the same parity we can take $j = \frac{\iota+\bar{\iota}}{2}$ in Eq. (4) to obtain

$$\gamma_{\mathbf{a}^{\bar{\iota}}\mathbf{b}} + \gamma_{\mathbf{a}^{\iota}\mathbf{b}} = 0. \tag{5}$$

If $\iota + \bar{\iota} \leq 2n$ (respectively, $\iota + \bar{\iota} \geq 2n$) then taking $j = \frac{\iota+\bar{\iota}+2n}{2}$ in Eq. (4) (respectively, $j = \frac{\iota+\bar{\iota}-2n}{2}$) we obtain $\mathbf{a}^{j-\iota} = \mathbf{a}^{\bar{\iota}-j}\mathbf{a}^{2n}$ and so $\gamma_{\mathbf{a}^{\bar{\iota}}\mathbf{b}} + \gamma_{\mathbf{a}^{\iota}\mathbf{b}} = 1$, which contradicts Eq. (5). Hence, we conclude that it could not happen that the row indexed by $\mathbf{a}^{\iota}\mathbf{b}$ and the column indexed by $\mathbf{a}^{\bar{\iota}}\mathbf{b}$ coincides. Therefore, the parity of $\iota, \bar{\iota}$ is different from each other.

Since $\boldsymbol{\kappa}_1$ belongs to the kernel of C the vectors in C with a zero in the first coordinate can be separated into two disjoint classes, the class $A_1 = \{\gamma_{\mathbf{a}^j}\mathbf{a}^i \ : \ 0 \leq j \leq 2n-1\}$ and the class $A_2 = \mathbf{a}^{\iota}\mathbf{b} + A_1$. Both classes are defined up to complement. Analogously for C^T.

Without loss of generality, we can assume that ι is odd and $\bar{\iota}$ is even. From Proposition 11, in matrix H row vectors $\mathbf{a}^j$, for even j, have the same coordinates in both halves and also vectors $\mathbf{a}^j\mathbf{b}$, for odd j, have the same coordinates in both halves. Therefore, projecting each of these vectors over the first half part we obtain $2n$ vectors of length $2n$ and weight n. Furthermore, the distance between them is also n and so they form an Hadamard matrix E. One of the rows of E is $\boldsymbol{\kappa}_1^{(p)}$, the projection of vector $\boldsymbol{\kappa}_1 = \mathbf{a}^{\iota}\mathbf{b}$ over the first half of coordinates. Vector $\boldsymbol{\kappa}_1^{(p)}$ is in the kernel of the code given by E. Indeed, from Lemma 2 we have $\mathbf{a}^j + K(C) = \mathbf{a}^j \cdot K(C)$ and so $\mathbf{a}^j + \boldsymbol{\kappa}_1 = \mathbf{a}^j\mathbf{a}^{\iota}\mathbf{b}$ (up to complement). Hence, for even j, $(\mathbf{a}^j)^{(p)} + \boldsymbol{\kappa}_1^{(p)} = (\mathbf{a}^{j+\iota}\mathbf{b})^{(p)}$, which is a row of matrix E (up to complement).

Now, we repeat the operation using column vectors of E. Column vectors corresponding to odd columns have the same coordinates in both halves. Hence, projecting each of these vectors over the first half part we obtain n vectors of length n and weight $n/2$. The distance between them is also $n/2$ and so they form an Hadamard matrix F. The rows of F are the projections of $\mathbf{a}^j$, for even $j \in \{0, 2, \ldots, 2n-2\}$ over the coordinates indexed by $\mathbf{a}^j$, for even $j \in \{2, \ldots, 2n\}$. If $\mathbf{a}^j = (a_1^{(j)}, a_2^{(j)}, \ldots, a_{4n}^{(j)})$ is a row in H, then $\mathbf{a}_p^j = (a_1^{(j)}, a_3^{(j)}, \ldots, a_{2n-1}^{(j)})$ is the corresponding row in F.

The group structure of the given code HFP-code C is $\langle \mathbf{a}, \mathbf{b} \rangle$ from where $\langle \mathbf{a}^2 \rangle$ is a cyclic subgroup with $2n$ elements. The associated permutation to $\pi_{\mathbf{a}}$ is a cyclic shift to the right, so the associated permutations to elements $\mathbf{a}^2$ are well defined acting over the set of even coordinates. Hence, the projection of elements in $\langle \mathbf{a}^2 \rangle$ over the even coordinates is a cyclic propelinear code C' of length n and $|C'| = 2n$. Since the elements in C' are exactly those in F (up to complement) we conclude that C' is a cyclic HFP-code of length n and $|C'| = 2n$ which, from Proposition 5, does not exist. The statement is proven. □

5 HFP-codes. Constructions

In this section we start from an HFP-code of type Q, length $4n$ and dimension of the kernel 2 and we construct a new HFP-code with double length $8n$ and the same dimension of the kernel $k = 2$. We also show that when the initial code has maximum rank $r = 2n$ the obtained code of length $8n$ has also maximum rank $4n$.

Throughout the section we will take $C = \langle \mathbf{a}, \mathbf{b} \rangle$ as an HFP-code of type Q, length $4n = 2^s n'$, $s \geq 3$, n' odd and $k = 2$. The kernel is $K(C) = \langle \mathbf{u}, \boldsymbol{\kappa} \rangle$ where, up to complement, $\boldsymbol{\kappa} = \mathbf{a}^{\iota}\mathbf{b}$ for some $\iota \in \{0, \ldots, 2n-1\}$ (see Proposition 11).

As we already said, given a polynomial $p(x)$ of degree at most $2n-1$ the polynomial $x^{2n-1}p(1/x)$ will be denoted by $\varphi_1(p(x))$. Now, given a polynomial $p(x)$ of degree at most $4n-1$ the polynomial $x^{4n-1}p(1/x)$ will be denoted by $\varphi_2(p(x))$.

We begin with an example and two technical lemmas. The example is to show that there are HFP-codes of type Q, length $4n$ and dimension of the kernel 2. The lemmas are about the greatest common divisor of polynomials, which will help to compute some ranks.

Example 1 The code $C = \langle \mathbf{a}, \mathbf{b} \rangle$ is an HFP-code of type Q, length $4n = 2^s n' = 24$ (so $s = 3, n' = 3$). The rank is $r = 12$, and dimension of the kernel is $k = 2$ (the kernel is $K(C) = \langle \mathbf{u}, \boldsymbol{\kappa} \rangle$, where $\kappa = \mathbf{a}^{11}\mathbf{b}$). The generators are

$$\begin{aligned}\mathbf{a} =&(1,1,1,1,1,1,0,1,1,0,1,0\,||\,1,0,1,0,0,1,0,0,0,0,0,0);\\ \mathbf{b} =&(0,1,0,1,0,1,1,1,0,0,0,0\,||\,1,1,1,1,0,0,0,1,0,1,0,1),\end{aligned}$$

and the permutations associated to each codeword are given by Proposition 11.

The transpose of this code has the same rank, but dimension of the kernel equal to 1.

Lemma 8 *Let $C = \langle \mathbf{a}, \mathbf{b} \rangle$ be an* HFP*-code of type Q, length $4n$, $k = 2$ and set $K(C) = \langle \mathbf{u}, \boldsymbol{\kappa} \rangle$, where $\boldsymbol{\kappa} = \mathbf{a}^\iota \mathbf{b}$ (up to complement) for an specific $\iota \in \{0, \ldots, 2n-1\}$.*

If $\gcd(a_1(x) + x^{\iota+1}\varphi_1(a_1(x)), x^{2n} - 1) = x - 1$ *then* $\operatorname{rank}(C) = 2n$*, where $(a_1(x), a_2(x))$ is the polynomial representation for $\mathbf{a} \in C$.*

Proof From Proposition 11, the element $\mathbf{a} = (a_1, a_2) \in C$ could be written, in a polynomial way, as $(a_1(x), x^{\iota+1}\varphi_1(a_1(x)) + u(x))$. Since $\mathbf{a}^{2n} = \mathbf{u}$, the weight of a_1 is odd (indeed, $\mathbf{a}^{2n} = \mathbf{a} + \pi_{\mathbf{a}}(\mathbf{a}) + \pi_{\mathbf{a}^2}(\mathbf{a}) + \cdots \pi_{\mathbf{a}^{2n-1}}(\mathbf{a})$ and so this means that in each coordinate of $\mathbf{a}^{2n}$ there is the addition of all coordinates of $\mathbf{a}$) and so $a_1(x) + x^{\iota+1}\varphi_1(a_1(x)) + u(x)$ is a multiple of $x-1$ (the weight of $u(x)$ is $2n$). Therefore, if $\gcd(a_1(x) + x^{\iota+1}\varphi_1(a_1(x)) + u(x), x^{2n} - 1) = x - 1$ then $\gcd(a_1(x), a_1(x) + x^{\iota+1}\varphi_1(a_1(x)) + u(x), x^{2n} - 1) = 1$. Polynomial $u(x)$ divides $x^{2n} - 1$ and so $\gcd(a_1(x), a_1(x) + x^{\iota+1}\varphi_1(a_1(x)), x^{2n} - 1) = 1$. Now, the dicyclic code generated by $a(x) = (a_1(x), a_2(x))$ has rank $2n$.

On the other hand, the linear span of C, using polynomials, is linearly generated by

$$\{a(x), xa(x), \ldots, x^{2n-1}a(x), b(x), xb(x), \ldots, x^{2n-1}b(x)\}, \tag{6}$$

and, since the polynomials associated to $\boldsymbol{\kappa}$ are $(\kappa_1(x), \kappa_2(x))$, where $\kappa_i(x) = 1 + x^2 + \cdots + x^{2n-2}$, up to complement, and $x\kappa_i(x) = \kappa_i(x) + u(x)$ then Eq. (6) is simplified to

$$\{a(x), xa(x), \ldots, x^{2n-1}a(x), \kappa(x)\}. \tag{7}$$

So, the rank r of the code C is $2n \le r \le 2n + 1$ and, from Lemma 4 the rank is upper bounded by $2n$. Hence $\operatorname{rank}(C) = 2n$. The statement is proven. □

Lemma 9 *Let $C = \langle \mathbf{a}, \mathbf{b} \rangle$ be an* HFP*-code of type Q, length $4n$, $k = 2$ and set $K(C) = \langle \mathbf{u}, \boldsymbol{\kappa} \rangle$, where $\boldsymbol{\kappa} = \mathbf{a}^\iota \mathbf{b}$ for an specific $\iota \in \{0, \ldots, 2n-1\}$.*

If $\gcd(a_1(x^2) + x\kappa_1(x^2) + x^{2\iota+1}(a_1(x^2) + x\varphi_2(\kappa_1(x^2)), x^{4n} - 1) \neq x - 1$ *then* $\gcd(a_1(x) + x^{\iota+1}\varphi_1(a_1(x)), x^{2n} - 1) \neq x - 1$.

Proof If $p(x)$ is any polynomial of degree at the most $2n - 1$ then we have $\varphi_2(p(x^2)) = x(\varphi_1(p(x^2)))$.

Indeed, if $p(x) = \sum_{i=0}^{2n-1} p_i x^i$ then $p(x^2) = \sum_{i=0}^{2n-1} p_i x^{2i}$ and $\varphi_2(p(x^2)) = \sum_{i=0}^{2n-1} p_i x^{4n-1-2i}$. On the other hand, $\varphi_1(p(x)) = \sum_{i=0}^{2n-1} p_i x^{2n-1-i}$ and $x\varphi_1(p(x^2)) = \sum_{i=0}^{2n-1} p_i x^{4n-1-2i}$.

We have

$$\begin{aligned}
&a_1\left(x^2\right)+x\kappa_1\left(x^2\right)+x^{2\iota+1}\left(a_1\left(x^2\right)+x\varphi_2\left(\kappa_1\left(x^2\right)\right)\right)\\
&\quad=a_1\left(x^2\right)+x\kappa_1\left(x^2\right)+x^{2\iota+1}\varphi_2\left(a_1\left(x^2\right)\right)+x^{2\iota+1}x^{4n-1}\varphi_2\left(\kappa_1\left(x^2\right)\right)\\
&\quad=a_1\left(x^2\right)+x^{2\iota+1}\varphi_2\left(a_1\left(x^2\right)\right)+x\kappa_1\left(x^2\right)+x^{2\iota}\varphi_2\left(\kappa_1\left(x^2\right)\right) \qquad (8)\\
&\quad=a_1\left(x^2\right)+x^{2\iota+2}\varphi_1\left(a_1\left(x^2\right)\right)+x\kappa_1\left(x^2\right)+x^{2\iota+1}\varphi_1\left(\kappa_1\left(x^2\right)\right)\\
&\quad=\left(a_1(x)+x^{\iota+1}\varphi_1\left(a_1(x)\right)\right)^2+x\left(\kappa_1(x)+x^{\iota}\varphi_1\left(\kappa_1(x)\right)\right)^2.
\end{aligned}$$

From Proposition 11 the polynomial $\kappa_1(x)+x^{\iota}\varphi_1(\kappa_1(x))$ is either zero or $u(x)$, depending on the parity of ι, and $x=1$ is a root of $u(x)$.

If $\gcd(a_1(x^2)+x\kappa_1(x^2)+x^{2\iota+1}(a_1(x^2)+x\varphi_2(\kappa_1(x^2)),x^{4n}-1)\neq x-1$ then it could be that $x=1$ is not a root of $a_1(x^2)+x\kappa_1(x^2)+x^{2\iota+1}(a_1(x^2)+x\varphi_2(\kappa_1(x^2))$ and so neither is a root of $a_1(x)+x^{\iota+1}\varphi_1(a_1(x))$.

Hence, $\gcd(a_1(x)+x^{\iota+1}\varphi_1(a_1(x)),x^{2n}-1)\neq x-1$.

Also, it could be that $x-1$ is a root of $a_1(x^2)+x\kappa_1(x^2)+x^{2\iota+1}(a_1(x^2)+x\varphi_2(\kappa_1(x^2))$, but there are more roots in that polynomial, for instance $x=w$, where $w\neq 1$ is a root of $x^{4n}-1$. In this case, w is also a root of $\kappa_1(x)+x^{\iota}\varphi_1(\kappa_1(x))$ and so, from (8), a root of $(a_1(x)+x^{\iota+1}\varphi_1(a_1(x)))^2$. Since $x^{4n}-1=(x^{2n}-1)^2$, w is also a root of $x^{2n}-1$ and we obtain $\gcd(a_1(x)+x^{\iota+1}\varphi_1(a_1(x)),x^{2n}-1)\neq x-1$. The statement is proven. □

Proposition 12 *Let $C=\langle\mathbf{a},\mathbf{b}\rangle$ be an* HFP*-code of type Q, length $4n$ and $k=2$. Then, there exists two* HFP*-codes E of type Q, length $8n$, one with dimension of the kernel $k=2$ and another with dimension of the kernel $k=1$. In both cases, if* $\operatorname{rank}(C)=2n$ *then* $\operatorname{rank}(E)=4n$.

Proof Let $(a_1(x),a_2(x))$, $(b_1(x),b_2(x))$ and $(\kappa_1(x),\kappa_2(x))$ be the polynomial representation associated to $\mathbf{a},\mathbf{b},\boldsymbol{\kappa}=\mathbf{a}^{\iota}\mathbf{b}$, respectively, in code C. We will construct code E taking $\mathbf{A},\mathbf{K}=\mathbf{A}^{2\iota+1}\mathbf{B}$ as its generators, where the polynomial representations are $(A_1(x),A_2(x))$ and $(K_1(x),K_2(x))$ with

$$\begin{aligned}
A_i(x)&=a_i\left(x^2\right)+x\kappa_i\left(x^2\right)\in\mathbb{F}[x]/x^{4n}-1,\\
K_i(x)&=1+x^2+\cdots+x^{4n-2}\in\mathbb{F}[x]/x^{4n}-1,
\end{aligned}$$

respectively. We will also take $\pi_{\mathbf{A}}=(1,2,\ldots,4n)(4n+1,4n+2,\ldots,8n)$, $\pi_{\mathbf{B}}=(1,8n)(2,8n-1)\cdots(4n,4n+1)$ and $\pi_{\mathbf{K}}=\pi_{\mathbf{A}}^{2\iota+1}\pi_{\mathbf{B}}$.

It is easy to see that the full propelinear properties of C are maintained in E, so E is a full propelinear code.

To show that E is Hadamard, from Lemma 5, we need to show that $\operatorname{wt}(\mathbf{A}^i)=\operatorname{wt}(\mathbf{A}^i+\mathbf{K})=4n$, for $i\in\{1,\ldots,4n-1\}$ and $\operatorname{wt}(\mathbf{A}^{4n})=8n$, $\operatorname{wt}(\mathbf{A}^{4n}+\mathbf{K})=4n$. Let $A^{(i)}(x)$ be any of the two polynomials associated to the element $\mathbf{A}^i$, say the first one (for the other polynomial the argument will be the same). Also say $a(x)^{(i)}$ and $\kappa(x)^{(i)}$ the first of the two polynomials associated to $\mathbf{a}^i,\boldsymbol{\kappa}^i$, respectively. We have

$$\begin{aligned}
A^{(2i)}(x)&=\left(1+x+\cdots+x^{2i-1}\right)a\left(x^2\right)+x\left(1+x+\cdots+x^{2i-1}\right)\kappa\left(x^2\right)\\
&=\left(1+x^2+\cdots+x^{2i-2}\right)a\left(x^2\right)+x\left(1+x^2+\cdots+x^{2i}\right)\kappa\left(x^2\right)\\
&\quad+x\left(1+x^2+\cdots+x^{2i-2}\right)a\left(x^2\right)+x^2\left(1+x^2+\cdots+x^{2i}\right)\kappa\left(x^2\right)\\
&=a^{(i)}\left(x^2\right)+x\kappa^{(i)}\left(x^2\right)+xa^{(i)}\left(x^2\right)+x^2\kappa^{(i)}\left(x^2\right)
\end{aligned}$$

We have $x^2\kappa^{(i)}(x^2) = \kappa^{(i)}(x^2) + \xi_i u(x^2)$, where ξ_i is 0 or 1 depending on i is even or odd, respectively. Hence, $A^{(2i)}(x) = p_1(x^2) + xp_2(x^2)$, where $p_1(x^2) = a^{(i)}(x^2) + \kappa^{(i)}(x^2) + \xi_i u(x^2)$ and $p_2(x^2) = a^{(i)}(x^2) + \kappa^{(i)}(x^2)$. Since $\boldsymbol{\kappa}, \mathbf{u} \in K(C)$ we have that both, $p_1(x)$ and $p_2(x)$ are in C and so, $\mathrm{wt}(\mathbf{A}^i) = 4n$ and $\mathrm{wt}(\mathbf{A}^i + \mathbf{K}) = 4n$, for even exponents $i \in \{2, 4, \ldots, 4n\}$, except for $i = 4n$ in which case $\mathrm{wt}(\mathbf{A}^{4n}) = 8n$. For odd exponents $i \in \{1, 3, \ldots, 4n-1\}$, using the same decomposition as for the even case, we have

$$\begin{aligned} A^{(2i+1)}(x) =& a^{(i+1)}\left(x^2\right) + xa^{(i)}\left(x^2\right) + x\kappa^{(i+1)}\left(x^2\right) + x^2\kappa^{(i)}\left(x^2\right) \\ =& q_1\left(x^2\right) + xq_2\left(x^2\right), \end{aligned}$$

where

$$\begin{aligned} q_1\left(x^2\right) =& a^{(i+1)}\left(x^2\right) + \kappa^{(i)}\left(x^2\right) + \xi_i u\left(x^2\right) \\ p_2\left(x^2\right) =& a^{(i)}\left(x^2\right) + \kappa^{(i+1)}\left(x^2\right). \end{aligned}$$

Both, $q_1(x)$ and $q_2(x)$ are in C so, $\mathrm{wt}(\mathbf{A}^i) = 4n$ and $\mathrm{wt}(\mathbf{A}^i + \mathbf{K}) = 4n$.

Regarding the kernel of E, we show that $\mathbf{K} \in K(E)$. To do this, we prove that $\pi_{\mathbf{K}} \in \mathrm{Aut}(E)$. It is clear that $\pi_{\mathbf{K}}(\mathbf{K})$ is either $\mathbf{K}$ or $\mathbf{K}+\mathbf{u}$. In any case $\pi_{\mathbf{K}}(\mathbf{K}) \in E$. Also, $\pi_{\mathbf{K}}(\mathbf{A}^i) = \mathbf{K} + \mathbf{A}^i + \pi_{\mathbf{A}^i}(\mathbf{K})$. We have that $\mathbf{K} + \pi_{\mathbf{A}^i}(\mathbf{K})$ is either $\mathbf{e}$ or $\mathbf{u}$ so, in any case, $\pi_{\mathbf{K}}(\mathbf{A}^i) \in E$. Hence, the dimension of the kernel is $k \geq 2$ and from Theorem 1 we have $k = 2$.

For the rank, the result is clear from Lemmas 8 and 9.

Finally, note that the constructed code E has dimension of the kernel equal to 2. Now, from Theorem 2, we can construct the transposed code of E, which has dimension of the kernel equal to 1. The statement is proven. □

The construction in the above Proposition 12 is more specific than a previous construction in [12, Proposition 1]. There, it is shown that given an Hadamard group of type Q we can obtain an Hadamard group of type Q with double length. Here, in Proposition 12 we show that from an HFP-code of type Q with dimension of the kernel $k = 2$ and maximum rank, we obtain an HFP-code of type Q with double length, dimension of the kernel $k = 2$ and maximum rank. Moreover, if we are looking for HFP-codes of double length and dimension of the kernel $k = 1$, we can obtain them applying Theorem 2.

Acknowledgements The authors are grateful to the anonymous referees for their helpful comments, which have improved the presentation of the results of this paper. This work has been partially supported by the Spanish MICINN Grants TIN2016-77918-P, MTM2015-69138-REDT and the Catalan AGAUR Grant 2014SGR-691.

References

1. Assmus E., Key J.: Designs and Their Codes. Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge (1992).
2. Bailera I., Borges J., Rifà J.: About some Hadamard full propelinear (2t, 2, 2)-codes. Rank and kernel. Electron. Notes Discret. Math. **54**, 319–324 (2016).
3. Borges J., et al.: Structural properties of binary propelinear codes. Adv. Math. Commun. **6**(3), 329–346 (2012).
4. de Launey W., Flannery D.L., Horadam K.J.: Cocyclic Hadamard matrices and difference sets. Discret. Appl. Math. **102**(1–2), 47–61 (2000).
5. del Río Á., Rifà J.: Families of Hadamard $\mathbb{Z}_2\mathbb{Z}_4 Q_8$-codes. IEEE Trans. Inf. Theory **59**(8), 5140–5151 (2013).
6. Elliott J., Butson A., et al.: Relative difference sets. Ill. J. Math. **10**(3), 517-513 (1966).
7. Flannery D.: Cocyclic Hadamard matrices and Hadamard groups are equivalent. J. Algebra **192**(2), 749–779 (1997). ISSN: 0021-8693.

8. Horadam K.J.: Hadamard matrices and their applications: progress 2007–2010. Cryptogr. Commun. **2**(2), 129–154 (2010).
9. Horadam K., de Launey W.: Cocyclic development of designs. J. Algebraic Comb. **2**(3), 267–290 (1993).
10. Ito N.: On Hadamard groups. J. Algebra **168**(3), 981–987 (1994). ISSN: 0021-8693.
11. Ito N.: Remarks on Hadamard groups. Kyushu J. Math. **50**(1), 83–91 (1996).
12. Ito N.: On Hadamard groups III. Kyushu J. Math. **51**(2), 369–379 (1997).
13. Phelps K.T., Rifà J., Villanueva M.: Rank and kernel of binary Hadamard codes. IEEE Trans. Inf. Theory **51**(11), 3931–3937 (2005).
14. Phelps K.T., Rifà J., Villanueva M.: Hadamard codes of length $2^t s$ (s Odd). Rank and kernel. In: Lu H.F. (ed.) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. LNCS 3857, pp. 328–337. Springer, Berlin (2006).
15. Phelps K.T., Rifà J., Villanueva M.: On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: rank and kernel. IEEE Trans. Inf. Theory **52**(1), 316–319 (2006).
16. Rifà J., Suárez E.: About a class of Hadamard propelinear codes. Electron. Notes Discret. Math. **46**, 289–296 (2014).
17. Rifà J., Basart J.M., Huguet L.: On completely regular propelinear codes. In: Lu H.F. (ed.) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. LNCS 357, pp. 341–355. Springer, Berlin (1989).
18. Schmidt B.: Williamson matrices and a conjecture of Ito's. Des. Codes Cryptogr. **17**(1–3), 61–68 (1999).

Emilio J. Suárez Canedo
Cerdanyola del Vallès, January 2018