Hadamard, quasi-Hadamard, and generalized Hadamard full propelinear codes

Ivan Bailera

Universitat Autònoma de Barcelona

Departament d'Enginyeria de la Informació i de les Comunicacions

Hadamard, quasi-Hadamard, and generalized Hadamard full propelinear codes

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

by Ivan Bailera

Cerdanyola del Vallès, July 2020

Advisor: Dr. Joaquim Borges i Ayats

Professor at Universitat Autònoma de Barcelona

I certify that I have read this thesis entitled "Hadamard, quasi-Hadamard, and generalized Hadamard full propelinear codes" 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, July 2020

Dr. Joaquim Borges i Ayats
(Advisor)

It gets easier. Every day it
gets a little easier. But you
gotta do it every day.
That's the hard part.
But it does get easier.

Abstract

This thesis belongs to the fields of algebraic combinatorics and mathematical information theory. Motivated by the computational advantage of the full propelinear structure, we study different kinds of error-correcting codes endowed with this structure. Since a full propelinear code is also a group, it is possible to generate the code from the codewords associated to the generators as a group, even if the code is nonlinear. This offers the data storage benefits of a linear code. Rifà and Suárez introduced full propelinear codes based on binary Hadamard matrices (HFP-codes) and they proved an equivalence with Hadamard groups. The existence of Hadamard matrices of orders a multiple of four remains an open problem. Therefore, the study of new Hadamard codes may contribute to address the Hadamard conjecture. A code with a full propelinear structure is composed of two sets, i.e., codewords and permutations. We define the associated group of an HFP-code as the group comprised of the permutations. Firstly, we study the HFP-codes with a fixed associated group. The next step is to generalize the binary HFP-codes to finite fields. Subsequently, we prove that the existence of generalized Hadamard full propelinear codes is equivalent to the existence of central relative $(v, w, v, v/w)$-difference sets. Furthermore, we build infinite families of nonlinear generalized Hadamard full propelinear codes. Finally, we introduce the concept of quasi-Hadamard full propelinear code. We also give an equivalence between quasi-Hadamard groups and quasi-Hadamard full propelinear codes. In all codes studied, we analyze the rank and the dimension of the kernel. Two parameters that provide information about the linearity of a code, and also about the nonequivalence of codes.

Resum

Aquesta tesi pertany als camps de la combinatòria algebraica i de la teoria matemàtica de la informació. Motivada per l'avantatge computacional de l'estructura *full propelinear*, estudiem diferents tipus de codis correctors d'errors dotats d'aquesta estructura. Com que un codi *full propelinear* és també un grup, és possible generar el codi a partir de les paraules associades als generadors com a grup, fins i tot si el codi és no lineal. Això ofereix els beneficis d'emmagatzematge d'un codi lineal. Rifà i Suárez van definir els codis *full propelinear* sobre matrius Hadamard binàries (HFP-codis) i van provar una equivalència amb els grups Hadamard. L'existència de matrius Hadamard d'ordres múltiple de quatre segueix sent un problema obert. Per tant, l'estudi de nous codis Hadamard pot contribuir a abordar la conjectura de Hadamard. Un codi amb una estructura *full propelinear* està compost per dos conjunts; paraules i permutacions. Definim el grup associat d'un HFP-codi com el grup format per les permutacions. Primerament, estudiem els HFP-codis amb un grup associat fixat. El següent pas és generalitzar a cossos finits els HFP-codis binaris. Després vam provar que l'existència de codis Hadamard *full propelinear* generalitzats és equivalent a l'existència de conjunts de diferències relatius amb paràmetres $(v, w, v, v/w)$. A més, construïm famílies infinites de codis Hadamard *full propelinear* generalitzats no lineals. Finalment, definim el concepte de codi quasi-Hadamard *full propelinear*. També donem una equivalència entre els grups quasi-Hadamard i els codis quasi-Hadamard *full propelinear*. En tots els codis estudiats, analitzem el rang i la dimensió del nucli. Dos paràmetres que proporcionen informació sobre la linealitat d'un codi i sobre la no equivalència de codis.

Resumen

Esta tesis pertenece a los campos de la combinatoria algebraica y de la teoría matemática de la información. Motivada por la ventaja computacional de la estructura *full propelinear*, estudiamos diferentes tipos de códigos correctores de errores dotados de dicha estructura. Como un código *full propelinear* es también un grupo, es posible generar el código a partir de las palabras asociadas a los generadores como grupo, incluso si el código es no lineal. Esto ofrece los beneficios de almacenamiento de un código lineal. Rifà y Suárez definieron los códigos *full propelinear* sobre matrices Hadamard binarias (HFP-códigos) y probaron una equivalencia con los grupos Hadamard. La existencia de matrices Hadamard de órdenes múltiplo de cuatro sigue siendo un problema abierto. Por tanto, el estudio de nuevos códigos Hadamard puede contribuir a abordar la conjetura de Hadamard. Un código con una estructura *full propelinear* está compuesto por dos conjuntos; palabras y permutaciones. Definimos el grupo asociado de un HFP-código como el grupo formado por las permutaciones. Primeramente, estudiamos los HFP-códigos con un grupo asociado fijado. El siguiente paso es generalizar a cuerpos finitos los HFP-códigos binarios. Después probamos que la existencia de códigos Hadamard *full propelinear* generalizados es equivalente a la existencia de conjuntos de diferencias relativos con parámetros $(v, w, v, v/w)$. Además, construimos familias infinitas de códigos Hadamard *full propelinear* generalizados no lineales. Finalmente, definimos el concepto de código quasi-Hadamard *full propelinear*. También damos una equivalencia entre los grupos quasi-Hadamard y los códigos quasi-Hadamard *full propelinear*. En todos los códigos estudiados, analizamos el rango y la dimensión del núcleo. Dos parámetros que proporcionan información sobre la linealidad de un código y sobre la no equivalencia de códigos.

Acknowledgements

Primerament vull agrair als meus directors de tesi, Joaquim Borges i Josep Rifà, per la seva disposició i consells en qualsevol moment que els he necessitat. La confiança i llibertat que m'han donat des d'un principi ha estat molt important perquè hagi pogut desenvolupar aquesta tesi. També a la Mercè i la Cristina, especialment per la seva ajuda amb el MAGMA. Així mateix, vull estendre aquest agraïment a tots els membres i exmembres del *Departament d'Enginyeria de la Informació i de les Comunicacions* que he conegut al llarg d'aquests més de quatre anys.

En segundo lugar doy las gracias a José Andrés Armario por su inestimable ayuda a la hora de ampliar mi visión en la investigación. Primero colaborando conmigo en un artículo (y los que vendrán) y posteriormente supervisando mi estancia de investigación en la Universidad de Sevilla. De aquella estancia no puedo dejar de agradecer a Víctor, Raúl, Félix, Belén y Loli, su hospitalidad en todo momento, lo que siempre contribuye a que el trabajo sea más eficaz.

Treće, ali ne nužno manje važno od gore navedenog, zahvaljujem Deanu Crnkoviću što mi je pružio priliku da sam napravio dva istraživačka boravka u Rijeci. Zahvaljujem i Sanji, Andrei i Matteu na gostoprimstvu.

Lastly, I would also like thank to Ronan Egan for his willingness to collaborate with me in research papers.

En el plano personal, agradezco a mi familia su alta tasa de actividad en *WhatsApp*, lo cual viene bien cuando estás lejos o incluso en el mismo sofá. A mi novia Virginia, por muchas cosas que no caben en estas líneas, pero sobre todo por su comprensión y apoyo, mejorando mi calidad de vida desde que la conozco. A Morer, por todas las charlas que hemos compartido y hacerme *aprovechar* la vida de doctorando. A Carlos Vela, por no perder nunca los nervios teniéndome en el mismo despacho durante unos largos años; gracias

también por acogerme en tu casa en Sevilla. Al resto de *pifos*, especialmente a Roland, Sara, Sergi y Carlos de Cea por su ayuda para desconectar en el día a día. A Melody, por entenderme y apoyarme. No puedo cerrar los agradecimientos sin mencionar a los *Onanes* y a los *frikis*, por todo lo que hemos compartido, ayudándome siempre a sentir la realidad más allá de la *Academia*.

Contents

Chapter 1

Introduction

"It's always best to start at the beginning."

Glinda the Good Witch. The Wizard of Oz.

With the purpose of making the information flow reliable, coding theory was born. When a message is sent from a source to a receiver, the information travels through a channel. There does not exist a perfect channel. The information could be corrupted due to noise produced in the channel. Therefore, the receiver obtain a message which differs from the initial one. In order to detect and correct channel errors, the communication scheme is performed as shows Figure 1.1. Firstly, the message is encoded obtaining codewords. The codewords are sent across the channel. Again the channel is noisy and the codeword suffers errors, but then this information is decoded. Finally, the receiver get an estimated message which is 'quite' similar to the sent one by the source.

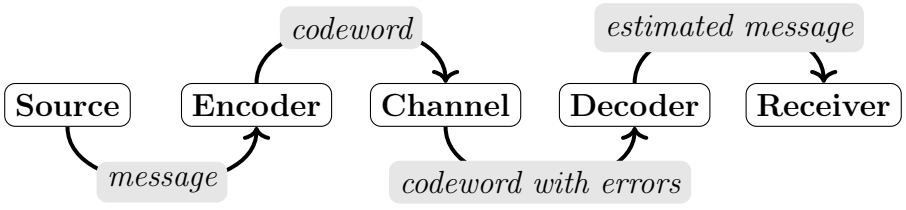

Figure 1.1: Communication scheme.

The engineering problem of noisy channels is addressed by means of mathematics. Coding theory, sometimes called algebraic coding theory, was created

under the influence of the theory of information transmission developed by Claude Shannon in 1948 [72]. Coding theory is linked with several areas of discrete mathematics such as combinatorics, graph theory, experimental designs, and number theory. Moreover, finite fields and group theory are also essential tools involved in coding theory. The usual way to represent, manipulate and transmit information is to use bit strings, i.e., n-tuples over the finite field $\mathbb{F}_2$ called codewords. Therefore, we say that a code is a subset of $\mathbb{F}_2^n$ that contains all codewords. A code is said to be linear if also is a subspace. Classically, linear codes have been studied and developed more than nonlinear codes due to their nice properties in the process of coding and decoding messages. Nevertheless, there exist nonlinear codes that are capable of detecting and correcting more errors than linear codes. For instance, there are nonlinear codes having twice as many codewords as any linear code with the same length and minimum distance, e.g., Preparata and Kerdock codes [42, 57]. In this dissertation, we focus on Hadamard codes, which are codes based on Hadamard matrices [40]. These matrices have several applications in engineering and computer science, as signal transforms, spreading sequences, error-correcting codes, and cryptographic primitives. The existence of Hadamard matrices for any order multiple of four is an open problem called the Hadamard conjecture [59]. This conjecture has stimulated advances in design theory and combinatorics. Terms such as Hadamard groups, relative difference sets, cocyclic Hadamard matrices, and Hadamard full propelinear codes are related in different ways [28, 37, 48, 66]. These concepts involve the main techniques to generate new Hadamard matrices.

1.1 Objectives

The core objective of this dissertation is to deepen into the study of error-correcting codes endowed with a propelinear structure. These codes are called propelinear codes. They have an underlying group structure. In general, all codewords of nonlinear codes have to be stored due to there does not exist a generator matrix of the code. One of the benefits of the propelinear codes is to exploit their group structure in order to generate the code from a subset of codewords even if the code is nonlinear. The concept of generator matrix

of a code is replaced by two sets. The set of generators as a group of the propelinear code and a set of associated permutations to each generator. When the nontrivial permutations of the previous set have no fixed coordinates, then the structure is called full propelinear. Along this dissertation, we endow different kind of codes with a full propelinear structure. The principal tasks that we have followed to achieve the main objective are:

1. Study binary Hadamard full propelinear codes with a fixed associated group.

2. Generalize the full propelinear structure to finite fields.

3. Endow a subclass of generalized Hadamard codes with a full propelinear structure.

4. Study the values of the rank and the dimension of the kernel of all codes introduced since they give us information about the linerarity of the code.

1.2 Outline

A summary of each chapter follows.

Chapter 2 covers basic definitions and properties of coding theory, Hadamard matrices, Hadamard groups, relative diference sets, cocyclic Hadamard matrices, and propelinear codes.

In *Chapter 3* we introduce the Hadamard full propelinear codes that factorize as direct product of groups such that their associated group is $C_{2t} \times C_2$ or $C_t \times C_2 \times C_2$. We study the rank, the dimension of the kernel, and the structure of these codes. For several specific parameters we establish some links from circulant Hadamard matrices and the nonexistence of the codes we study. We also get an equivalence between circulant complex Hadamard matrix and a type of Hadamard full propelinear code, and we find a new example of circulant complex Hadamard matrix of order 16.

In *Chapter 4* we present codes from generalized Hadamard matrices. Here we deal with these codes when the generalized Hadamard matrices are cocyclic. As a consequence, a new class of codes that we call generalized Hadamard full propelinear codes turns out. We prove that their existence is equivalent to

the existence of central relative $(v, w, v, v/w)$-difference sets. Moreover, some structural properties of these codes are studied and examples are provided.

In *Chapter 5* we give a characterization of quasi-Hadamard groups in terms of full propelinear codes. We define a new class of codes that we call quasi-Hadamard full propelinear codes. Some structural properties of these codes are studied and examples are provided.

Chapter 6 recaps the main results of the rest of chapters, and proposes future lines of research on this topic.

1.3 Contributions

Part of the results presented in Chapter 3 has been published in [11, 12]:

- 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).

- Bailera I., Borges J., Rifà J.: On Hadamard full propelinear codes with associated group $C_{2t} \times C_2$. To appear in Adv. Math. Commun. (2020).

The results of Chapter 4 has been submitted to the international journal *Designs, Codes and Cryptography*. A preprint is available in [8]:

- Armario J.A., Bailera I., Egan R.: Generalized Hadamard full propelinear codes. arXiv:1906.06220 [math.CO].

The results of Chapter 5 has been published in [6]:

- Armario J.A., Bailera I., Borges J., Rifà, J.: Quasi-Hadamard Full Propelinear Codes. Math. Comput. Sci. **12**(4), 419–428 (2018).

Moreover, several results of this dissertation has been presented in national and international workshops and conferences:

- *About some Hadamard full propelinear* $(2t, 2, 2)$*-codes. Rank and Kernel.* Discrete Mathematics Days (JMDA16). Barcelona, Spain. July 6–8th, 2016.

- *Hadamard full propelinear codes of type CQ.* 5th Workshop on Real and Complex Hadamard Matrices and Applications. Budapest, Hungary. July 10–14th, 2017.

- *Hadamard full propelinear codes of type $C_{4t} \times C_2$ and $C_{2t} \times C_2$. Rank and kernel.* IV Congreso de Jóvenes Investigadores de la Real Sociedad Matemática Española. València, Spain. September 4–8th, 2017.

- *Existence of Hadamard full propelinear codes which are extensions of $C_t \times C_2^2$ by C_2.* Escuela de Doctorandos de la Red de Matemáticas en la Sociedad de la Información. Tenerife, Spain. November 27–28th, 2017.

- *Códigos de Hadamard full propelinear.* Seminario Rubio de Francia. University of Zaragoza, Spain. May 3rd, 2018.

- *On Hadamard full propelinear codes with associated group $C_{2t} \times C_2$.* Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2018). Svetlogorsk (Kaliningrad region), Russia. September 2–8th, 2018.

- *Hadamard and quasi-Hadamard full propelinear codes.* Seminar za konačnu matematiku, Department of mathematics, University of Rijeka, Croatia. October 4th, 2018.

- *Códigos Hadamard full propelinear.* IMUS Seminar. Seville, Spain. June 25th, 2019.

- *Generalized Hadamard full propelinear codes.* Seminar za konačnu matematiku, Department of mathematics, University of Rijeka, Croatia. September 19th, 2019.

- *Códigos Hadamard generalizados full-propelineales.* V Congreso de Jóvenes Investigadores de la Real Sociedad Matemática Española. Castelló, Spain. January 27–31th, 2020.

During the academic years of this thesis, I was granted with three competitive research fellowships that allowed me collaborating with distinct researchers:

- Erasmus+ scholarship. From September to December, 2018. I visited the Department of Mathematics at the University of Rijeka, Croatia. Prof. Dean Crnković was the supervisor.

- Borsa Ferran Sunyer i Balaguer. From June to July, 2019. I visited the Department of Applied Mathematics at the University of Seville, Spain. Prof. José Andrés Armario was the supervisor.

- UAB stay grant. From September to October, 2019. I visited the Department of Mathematics at the University of Rijeka, Croatia. Prof. Dean Crnković was the supervisor.

Along the first research stay in Rijeka, we studied the orbit matrices of Hadamard matrices associated to Hadamard full propelinear codes. For more information about orbit matrices, we refer to [25]. In the second stay in Rijeka, we proposed a new model for network coding based in propelinear codes, and a generalization of subspace codes. This work is in preparation. For more information about linear network coding and subspace codes, we refer to [1, 54, 56]. In the research stay in Seville, we studied generalized Hadamard full propelinear codes (see Chapter 4). The results were submitted to the journal *Designs, Codes and Cryptography*.

This Thesis has been partially supported by the Spanish grants TIN2013-40524-P, TIN2016-77918-P (AEI/FEDER, UE) and MTM2015-69138-REDT, and by the Catalan AGAUR grant 2014SGR-691.

Chapter 2

Preliminaries

"Remember, all I'm offering is the truth, nothing more."

Morpheus. The Matrix.

This chapter presents some background necessary to follow the results presented throughout the thesis. Along this chapter we establish the notation that will be used across the dissertation. Any other background material required will be referenced just before it is used.

2.1 Propelinear codes

Let $\mathbb{F}_q$ denote the finite field of order $q = p^r$, where p is prime. In particular, $\mathbb{F}_q$ is an additive elementary abelian group of order q. For $q = 2$, we denote by $\mathbb{F}$ the binary field $\mathbb{F}_2$. Let $\mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$. The *Hamming distance* between two vectors $x, y \in \mathbb{F}_q^n$, denoted by $d(x, y)$, is the number of coordinates in which x and y differ. The *Hamming weight* of x is given by $\mathrm{wt}_H(x) = d(x, \mathbf{0})$, where $\mathbf{0}$ is the all-zero vector. Throughout this dissertation, the all-one vector of length n is denoted by $\mathbf{1}_n$, and the vector $(1, 0, \ldots, 1, 0)$ of length $2n$ by $\boldsymbol{\omega}_{2n}$, but we will write $\mathbf{1}$ and $\boldsymbol{\omega}$ when the length is clear from the context.. The *support* of $x \in \mathbb{F}_q^n$, denoted by $\mathrm{Supp}(x)$, is defined as the set of its nonzero positions. The *complement* of $x \in \mathbb{F}^n$, denoted by $\bar{x}$, is defined as $\bar{x} = x + \mathbf{1}$.

Any nonempty subset C of $\mathbb{F}_q^n$ is a *code* over $\mathbb{F}_q$ (or a q-ary code) of length n. Usually, a code C is presented by the triple $(n, M, d)_q$ where n is the length,

$M = |C|$ is the size of the code, and d is the greatest value such that $d(x, y) \geq d$ for all $x, y \in C$ with $x \neq y$. The elements of a code are called *codewords* and d is called *minimum distance*. The parameter d determines the error-correcting capability of C which is given by

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

and C is said to be a *t-error-correcting* code.

Throughout this dissertation, when a codeword v will appear as $v = (\alpha, \beta, \gamma, \delta, \ldots)$, assume $\alpha, \beta, \gamma, \delta$ have the same length. For example, if C is a code of length n and $v = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in C$, then the length of each α_i is n/m.

A q-ary code C of length n is *linear* if any linear combination of codewords is also a codeword, i.e., C is a subspace of $\mathbb{F}_q^n$. The *dimension* of a q-ary linear code is its dimension as a subspace. A q-ary linear code of length n and dimension k is presented by the triple $(n, k, d)_q$. Note that the size of C is $|C| = q^k$.

Let $\mathcal{S}_n$ be the symmetric group of permutations of the set $\{1, \ldots, n\}$. For any $\pi \in \mathcal{S}_n$ and $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, we write $\pi(x)$ to denote $(x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$. Two codes C_1, C_2 of length n are said to be *isomorphic* if there is a coordinate permutation $\pi \in \mathcal{S}_n$ such that $C_2 = \{\pi(x) \mid x \in C_1\}$. They are said to be *equivalent* if there is a vector $y \in \mathbb{F}_q^n$ and a coordinate permutation $\pi \in \mathcal{S}_n$ such that $C_2 = \{y + \pi(x) \mid x \in C_1\}$.

In order to study the linearity of a code, we introduce two structural parameters. The *rank* of a q-ary code C, denoted by $\mathrm{rank}(C)$ or r, is the dimension of the linear span of C. The *kernel* of a q-ary code, denoted by $\mathcal{K}(C)$, is defined as

$$\mathcal{K}(C) = \{x \in \mathbb{F}_q^n \mid C + \alpha\, x = C \text{ for all } \alpha \in \mathbb{F}_q\}.$$

The p-kernel of C is defined as the set of vectors which keeps the code invariant by translation, $\mathcal{K}_p(C) = \{x \in \mathbb{F}_q^n \mid C + x = C\}$, where q is a power of a prime p. Note that $\mathcal{K}(C)$ is a subspace of $\mathbb{F}_q^n$ and $\mathcal{K}_p(C)$ is $\mathbb{F}_p$-additive. If C is binary, then $\mathcal{K}(C) = \mathcal{K}_p(C)$. Assuming the all-zero vector is in C, $\mathcal{K}(C) \subseteq C$. The dimension k of the kernel of C is denoted by $\ker(C)$. The rank r and the dimension of the kernel k do not always give a full classification of codes, since two nonisomorphic codes could have the same rank and dimension of the

kernel. In spite of that, they can help in classification, since if two codes have different rank or dimension of the kernel, they are nonisomorphic. In some sense, these two parameters give information about the linearity of a code.

Remark 2.1. *A code is linear if and only if its rank and the dimension of its kernel are equal to the dimension of the code.*

From now on, assume $\mathbf{0} \in C$ for every code C. The following result shows a bound for the rank of a code in terms of the length and the dimension of the kernel.

Lemma 2.2 ([67, Lemma 6])**.** *Let C be a code of length n. The rank r of C fulfils*

$$r \leq \frac{2n}{2^k} + k - 1,$$

where k is the dimension of the kernel of C.

For $q = 2$, Rifà, Basart, and Huguet [64] introduced a concept which is useful to study nonlinear codes, since it permits endow with an algebraic structure to certain codes.

Definition 2.3 ([64])**.** *A binary code C of length n has a propelinear structure if for each codeword $x \in C$ there exists $\pi_x \in \mathcal{S}_n$ satisfying the following conditions for all $y \in C$:*

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

(ii) $\pi_x \pi_y = \pi_z$, *where* $z = x + \pi_x(y)$.

Assuming C has a propelinear structure, for all $x, y \in C$, we denote by $\star$ the binary operation such that

$$x \star y = x + \pi_x(y).$$

Then, $(C, \star)$ is a group, which is not abelian in general. The vector $\mathbf{0}$ is always a codeword and $\pi_{\mathbf{0}} = Id$ is the identity permutation. Hence, $\mathbf{0}$ is the identity element in C and $x^{-1} = \pi_x^{-1}(x)$, for all $x \in C$. We call $(C, \star)$ a *propelinear code*. Note that the binary operation $\star$ can be extended to $\mathbb{F}^n$ as an action of C over $\mathbb{F}^n$. Therefore, for all $x \in C$ and for all $y \in \mathbb{F}^n$, $x \star y = x + \pi_x(y) \in \mathbb{F}^n$. Henceforth we use xy instead of $x \star y$ if there is no confusion. Binary propelinear

codes were introduced by Rifà et al. in [64]. They have been deeply studied in the literature, see [15, 61, 65] among other references. These codes have a group structure that allows them to be studied from an algebraic point of view. As a propelinear code is also a group, it is possible to define a kind of generator matrix even if the code is nonlinear. The rows of the generator matrix are the codewords that are associated with the generators of the group. Thus, the code can be built from a few codewords using the propelinear operation associated to the propelinear code.

Remark 2.4. *Let $\mathcal{G}$ be the wreath product $(\mathbb{F}^n, +) \wr \mathcal{S}_n$, i.e., an n-dimensional vector space over $\mathbb{F}$ with the natural action of $\mathcal{S}_n$ on coordinates. A propelinear code is a subgroup of $\mathcal{G}$.*

An automorphism of a binary code C is a permutation on the set of coordinates leaving the code invariant. We denote by $\mathrm{Aut}(C)$ the set of all automorphisms of C. We call it the *automorphism group* of the code C. A code C is called *transitive* if $\mathrm{Aut}(C)$ acts transitively on its codewords, i.e., the code satisfies the property *(i)* of Definition 2.3. The following result is a characterization of propelinear codes in terms of the automorphism group.

Proposition 2.5 ([61, Proposition III.1])**.** *Let $(C, \star) \subset \mathbb{F}_2^n$ be a group. C is a propelinear code if and only if $\mathrm{Aut}(C)$ contains a regular subgroup acting transitively on C.*

Example 2.6. *Every binary linear code has a propelinear structure. Let C be a linear code over $\mathbb{F}$. For any $x \in C$, set $\pi_x = Id$. Then $C \simeq \mathbb{Z}_2^{\log_2 |C|}$.*

Let x be in a propelinear code, we denote the element $x \star x^{i-1}$ by x^i, with $x^1 = x$, for any $i > 1$.

Lemma 2.7. *Let C be a propelinear code. Then $x^i = x + \pi_x(x) + \ldots + \pi_x^{i-1}(x)$, for all $x \in C$.*

Proof. We proceed by induction on i. The base case is $x^2 = x + \pi_x(x)$. Let us see the inductive step, $x^i = x \star x^{i-1} = x + \pi_x(x^{i-1}) = x + \pi_x(x + \pi_x(x) + \ldots + \pi_x^{i-2}(x)) = x + \pi_x(x) + \ldots + \pi_x^{i-1}(x)$. $\mathcal{QED}$

Lemma 2.8 ([15, Lemma 5.1])**.** *Let C be a propelinear code. Then:*

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

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

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

2.2 Hadamard matrices

In 1893 Jacques Hadamard raised the following problem: *Let A be a square matrix of order n with entries in the closed unit disk. How large can the absolute value of the determinant of A be?* This is known as the Hadamard maximum determinant problem. Hadamard proved in [40] that if all elements of the matrix A are complex numbers, then

$$|\det A| \leq n^{n/2}.$$

The matrices that achieve the equality are called *Hadamard matrices*. A square matrix $H = (z_{ij})$ of order n is a *complex Hadamard matrix*, if $\|z_{ij}\| = 1$ and $HH^* = nI_n$, where I_n is the identity matrix of order n and H^* is the conjugate transpose of H. It is known that there exist complex Hadamard matrices of order n for each positive integer n.

Example 2.9. *Let n be positive a integer and $\zeta_n = \mathrm{e}^{\frac{2\pi i}{n}}$ be the complex n^{th} root unity .The Fourier matrices*

$$F_n = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_n & \zeta_n^2 & \zeta_n^3 & \cdots & \zeta_n^{n-1} \\ 1 & \zeta_n^2 & \zeta_n^4 & \zeta_n^6 & \cdots & \zeta_n^{2(n-1)} \\ 1 & \zeta_n^3 & \zeta_n^6 & \zeta_n^9 & \cdots & \zeta_n^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_n^{n-1} & \zeta_n^{2(n-1)} & \zeta_n^{3(n-1)} & \cdots & \zeta_n^{(n-1)(n-1)} \end{pmatrix}$$

are complex Hadamard matrices.

Usually, the term Hadamard matrix refers to Hadamard matrices with entries in $\{1, -1\}$.

Definition 2.10. *A Hadamard matrix of order n is a $n \times n$ matrix H containing entries from the set $\{1, -1\}$, with the property that*

$$HH^T = nI_n,$$

where I_n is the identity matrix of order n.

Example 2.11. *The Hadamard matrices of order $1, 2, 4$ are*

$$H_1 = (1)\,, \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

For $n > 2$, any three rows (columns) agree in precisely $n/4$ coordinates. Thus, if there is a Hadamard matrix of order n, with $n > 2$, then n is multiple of 4. The existence of real Hadamard matrices is a question that remains still open. In 1933 Paley [59] formulated a conjecture that now is known as Hadamard's conjecture.

Conjecture 2.12 (**Hadamard's conjecture**)**.** *There exists real Hadamard matrices of order $4n$ for every positive integer n.*

The smallest order, for which no Hadamard matrix is yet known, is 668. Other orders smaller than 1000, for which Hadamard matrices have not been found yet, are 716 and 892.

Several constructions of Hadamard matrices have been developed (Paley [59], Williamson [78], Goethals and Seidel [38, 39], Ito [47]). Here is presented one due to James Joseph Sylvester which realized that if H is a Hadamard matrix, then so is

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

Let $A = (a_{ij})$ and B be $m \times n$ and $s \times t$ matrices, respectively. The *Kronecker*

product $A \otimes B$ is a $ms \times nt$ matrix given by

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2} & \cdots & a_{mn}B \end{pmatrix}.$$

The Kronecker product of two Hadamard matrices is a Hadamard matrix (Ryser [68]). In Example 2.11, clearly $H_4 = H_2 \otimes H_2$. The *Sylvester construction* [76] is the iterated Kronecker product of the Hadamard matrix H_2 from Example 2.11. Let S be the matrix H_2, the Sylvester construction define the matrices

$$S^t = S \otimes S^{t-1}$$

for $t \in \{2, 3, \ldots\}$, which form an infinity family of Hadamard matrices of orders 2^t. S^t is called the *Sylvester matrix* of order 2^t.

Two Hadamard matrices are *Hadamard-equivalent* (or just *equivalent*) if one can be obtained from the other by permuting rows and/or columns and multiplying them by -1. Determine the number of equivalence classes of Hadamard matrices for each order is also an open problem. For orders $2, 4, 8, 12, 16, 20, 24$, 28 the number of nonequivalent Hadamard matrices are $1, 1, 1, 1, 5, 3, 60, 487$ (see Sloane's A007299).

A $n \times n$ matrix of the form

$$\begin{pmatrix} c_1 & c_2 & c_3 & \ldots & c_n \\ c_n & c_1 & c_2 & \ldots & c_{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ c_2 & c_3 & c_4 & \ldots & c_1 \end{pmatrix}$$

is called *circulant matrix*. No circulant Hadamard matrices of order larger than 4 has ever been found, but the nonexistence is still a non proven result (Ryser, [68]).

Conjecture 2.13 (**Circulant Hadamard conjecture**). *There do not exist circulant Hadamard matrices of order $n > 4$.*

The main work on circulant Hadamard conjecture seems to be due to Turyn [77]. He proved that a circulant Hadamard matrix of order n fulfils that $n =$

$4u^2$ with u odd or $n = 1$. Schmidt [69, 71] showed that there is no Hadamard circulant matrix of order n with $4 < n \leq 10^{11}$ with three possible exceptions.

Any Hadamard matrix is equivalent to a Hadamard matrix whose first row and columns is the all-one vector. This matrix is called *normalized*. The matrix obtained from a normalized Hadamard matrix, by replacing all 1's by 0's and all -1's by 1's, is called *binary normalized Hadamard matrix*. A (binary) *Hadamard code* is a binary code consisting of the rows of a binary Hadamard matrix and their complements, which is of length n, with $2n$ codewords, and minimum distance $n/2$, i.e., a Hadamard code is a $(n, 2n, n/2)_2$-code. A *binary normalized circulant matrix* is a binary normalized matrix which is equivalent to a binary circulant matrix. The binary code consisting of the rows of a binary normalized circulant Hadamard matrix and their complements is called a *circulant Hadamard code*.

Example 2.14. *Let H_4 be the Hadamard matrix from Example 2.11. The binary Hadamard matrix H associated to H_4 and the corresponding $(4, 8, 4)_2$-Hadamard code C_H are*

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

2.3 Hadamard full propelinear codes

Rifà and Suárez [66, 67] introduced a subclass of propelinear codes based on Hadamard matrices. These codes are called Hadamard full propelinear codes.

Definition 2.15 ([66])**.** *A Hadamard full propelinear code (HFP-code) is a Hadamard propelinear code C such that $\pi_a(i) \neq i$ for any i, where $a \in C \setminus \{\mathbf{0}, \mathbf{1}\}$, and $\pi_{\mathbf{0}} = \pi_{\mathbf{1}} = Id$.*

Definition 2.16. *The associated group* Π *of a propelinear code* C *is the set of permutations of all elements of* C, $\Pi = \{\pi_x \in \mathcal{S}_n \mid x \in C\}$, *which is a subgroup of* $\mathcal{S}_n$.

Example 2.17. *Let* H *be the binary Hadamard matrix of order* 2, *and* C_H *be the corresponding Hadamard code. That is,*

$$H = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \; C_H = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let a *be the codeword* $(0,1)$. *Thus,* $C_H = \{\mathbf{0}, a, \mathbf{1}, \bar{a}\}$. *Set* $\pi_{\mathbf{0}} = \pi_{\mathbf{1}} = Id \in \mathcal{S}_2$, $\pi_a = \pi_{\bar{a}} = (1,2) \in \mathcal{S}_2$. *Let* $\star$ *be the propelinear operation. Computing* a^i *we obtain:*

$$\begin{aligned} a^1 &= a = (0,1) \in C_H, \\ a^2 &= a \star a = a + \pi_a(a) = (0,1) + (1,0) = \mathbf{1} \in C_H, \\ a^3 &= a \star a^2 = a + \pi_a(a^2) = (0,1) + (1,1) = (1,0) = \bar{a} \in C_H, \\ a^4 &= a \star a^3 = a + \pi_a(a^3) = (1,0) + (1,0) = \mathbf{0} \in C_H. \end{aligned}$$

Therefore, $(C_H, \star)$ *is an HFP-code of length* 2 *with a group structure* $C_4 \simeq \langle a \rangle$ *and associated group* $\Pi \simeq C_2 \simeq \langle \pi_a \rangle$, *where* C_i *is the cyclic group of order* i.

Remark 2.18. *The HFP-code* C_H *from previous example is also a linear code. A linear code could have a full propelinear structure but there is not a characterization about that.*

Proposition 2.19 ([11, Proposition 2.8])**.** *Let* C *be a Hadamard full propelinear code. Then* $\mathbf{1} \in \mathcal{K}(C)$ *and the associated group of* C *is isomorphic to* $C/\langle \mathbf{1} \rangle$.

Proof. Let $x \in C$. Since $x + \mathbf{1} = x + \pi_x(\mathbf{1}) = x \star \mathbf{1} \in C$, we have $\mathbf{1} \in \mathcal{K}(C)$. Let $\varphi : C \to \Pi$ be the mapping given by $\varphi(x) = \pi_x$ for all $x \in C$. As $\pi_{x \star y} = \pi_x \pi_y$ for all $x, y \in C$, the mapping φ is a group homomorphism. Since C is full propelinear, the kernel of this homomorphism is $\langle \mathbf{1} \rangle$. Thus, $C/\langle \mathbf{1} \rangle \simeq \varphi(C) = \Pi$. $\mathcal{QED}$

Note that a code could have different group structures depending on the permutation associated to each codeword. The following example illustrates this fact.

Example 2.20. *Let C_H be the code from Example 2.14. Let*

$$\Pi = \{Id, (1,3)(2,4), (1,2)(3,4), (1,4)(2,3)\} \simeq C_2 \times C_2$$

be the associated group, where C_2 is the cyclic group of order 2. If we assign to each codeword the elements of Π in the following three ways:

$\pi_{\mathbf{0}} = Id$	$\pi_{\mathbf{0}} = Id$	$\pi_{\mathbf{0}} = Id$
$\pi_{(0101)} = (1,3)(2,4)$	$\pi_{(0101)} = (1,3)(2,4)$	$\pi_{(0101)} = (1,2)(3,4)$
$\pi_{(0011)} = (1,2)(3,4)$	$\pi_{(0011)} = (1,4)(2,3)$	$\pi_{(0011)} = (1,4)(2,3)$
$\pi_{(0110)} = (1,4)(2,3)$	$\pi_{(0110)} = (1,2)(3,4)$	$\pi_{(0110)} = (1,3)(2,4)$
$\pi_{\mathbf{1}} = Id$	$\pi_{\mathbf{1}} = Id$	$\pi_{\mathbf{1}} = Id$
$\pi_{(1010)} = (1,3)(2,4)$	$\pi_{(1010)} = (1,3)(2,4)$	$\pi_{(1010)} = (1,2)(3,4)$
$\pi_{(1100)} = (1,2)(3,4)$	$\pi_{(1100)} = (1,4)(2,3)$	$\pi_{(1100)} = (1,4)(2,3)$
$\pi_{(1001)} = (1,4)(2,3)$	$\pi_{(1001)} = (1,2)(3,4)$	$\pi_{(1001)} = (1,3)(2,4)$

Then we obtain three Hadamard full propelinear codes with group structures $C_2 \times C_2 \times C_2$, $C_4 \times C_2$, Q, respectively, where Q is the quaternion group of eight elements. Note that

$$(C_2 \times C_2 \times C_2)/\langle \mathbf{1} \rangle \simeq (C_4 \times C_2)/\langle \mathbf{1} \rangle \simeq Q/\langle \mathbf{1} \rangle \simeq C_2 \times C_2.$$

Definition 2.21. *An extension of a group H by a group N is a group G with a normal subgroup M such that $M \simeq N$ and $G/M \simeq H$. This information can be encoded into a short exact sequence of groups*

$$1 \to N \to G \to H \to 1.$$

Let C be a Hadamard full propelinear code with associated group Π. Thus, from Proposition 2.19 we have $C/\langle \mathbf{1} \rangle \simeq \Pi$. Hence, a Hadamard full propelinear code is a central extension of the associated group by the cyclic group of order 2. The search for Hadamard full propelinear codes is an extension problem

with the following short exact sequence

$$1 \to \langle \mathbf{1} \rangle \to C \to \Pi \to 1.$$

Next lemmas are well known. We omit the proofs.

Lemma 2.22 ([66, Lemma 3.3]). *Let $(C, \star)$ be a Hadamard propelinear code of length $4t$. Then C is not a cyclic group of order $8t$.*

Lemma 2.23 ([63, Prop. 2.2 and Prop. 2.3]). *Let C be a circulant Hadamard code of length $4t$, then C is an HFP-code with a cyclic associated group Π of order $4t$. Vice versa, an HFP-code C with a cyclic associated group Π of order $4t$ is a circulant Hadamard code of length $4t$.*

Lemma 2.24 ([63, Proposition 2.5]). *Let C be a nonlinear circulant Hadamard code of length $4t$. Then the dimension of the kernel is $k = 1$.*

Lemma 2.25 ([62, Theorem 1]). *Let C be a nonlinear Hadamard code of length $2^s t'$, where t' is odd. The dimension of the kernel k fulfils $1 \leq k \leq s - 1$.*

Lemma 2.26 ([10, Thm. 2.4.1 and Thm. 7.4.1]). *Let C be a Hadamard code of length $4t = 2^s t'$, where t' is odd.*

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

(ii) If $s = 2$ then $r = 4t - 1$.

To finish this subsection, we recall a notation introduced in [11] to denote the Hadamard full propelinear codes that we will use in the next chapters. An $\mathrm{HFP}(t, 2, 2, 2_{\mathbf{1}})$ code means a Hadamard full propelinear code of type $C_t \times C_2 \times C_2 \times C_2$ where the codeword $\mathbf{1}$ is the generator of the last C_2. So the numbers in parentheses mean the orders of the cyclic groups. If the parameter in the parentheses is Q, then it means the quaternion group of eight elements.

2.4 Relative difference sets

In 1938, Singer [74] introduced the concept of difference set. Later Hall [41] and Bruck [19] laid down the first stone in the systematic study of difference sets. Hall studied cyclic planar difference sets, and Bruck started the investigation of difference sets in arbitrary groups.

Definition 2.27. *A (v, k, λ)-difference set is a k-subset D of a group G of order v for which the multiset $\{d_1 d_2^{-1} \mid d_1, d_2 \in D, d_1 \neq d_2\}$ contains each nonidentity element of G exactly λ times.*

A difference set is called abelian, nonabelian or cyclic according to the properties of the underlying group. A difference set with parameters $(4m^2, 2m^2 - m, m^2 - m)$ is called *Hadamard difference set*. Hadamard difference sets have been deeply studied, see [30, 50] and their references. The *exponent* of a group G, $\exp(G)$, is the smallest positive integer n such that $g^n = 1$ for all $g \in G$.

Proposition 2.28 (Kraemer [55, Theorem 3])**.** *There exists a Hadamard difference set in an abelian group G of order 2^{2s+2} if and only if $\exp(G) \leq 2^{s+2}$.*

Proposition 2.29 ([12])**.** *Let C be a Hadamard full propelinear code of length $4t$. If $C \simeq G \times \langle \mathbf{1} \rangle$, then there exists a Hadamard difference set in G.*

Proof. From [48, Proposition 1], if $C = G \times \langle \mathbf{1} \rangle$ is a Hadamard group of order $8t$, then there exists a Hadamard difference set in G. From [66, Proposition 3.2, Proposition 3.5], C is a Hadamard full propelinear code if and only if C is a Hadamard group. $\mathcal{QED}$

Conjecture 2.30 (**Ryser's conjecture**)**.** *There is no cyclic (v, k, λ)-difference set with $\gcd(v, k - \lambda) > 1$.*

Remark 2.31. *Ryser's conjecture implies the circulant Hadamard conjecture.*

Bose [17] presented the first examples of relative difference set in 1942. Butson and Elliot [21, 36] studied more deeply this concept.

Definition 2.32 (Butson [21])**.** *Let G be a group of order mn with a normal subgroup N of order n. A relative (m, n, k, λ)-difference set in a group G with forbidden subgroup N is a k-subset D of G such that the multiset of quotients $d_1 d_2^{-1}$ of distinct elements $d_1, d_2 \in D$ contains each element of $G \setminus N$ exactly λ times, and contains no elements of N.*

Let D be a relative difference set in a group G with forbidden subgroup N. If N is a central subgroup of G, then we call D a *central relative difference set*. Note that a (v, k, λ)-difference set in G is a relative $(v, 1, k, \lambda)$-difference set in G with trivial forbidden subgroup. The existence of a relative

(m, n, k, λ)-difference set implies the existence of an $(m, k, n\lambda)$-difference set. Let D be a relative difference set in a group G with forbidden subgroup N. If H is a normal subgroup of G contained in N, then there exists a relative difference set in G/H with forbidden subgroup N/H. Moreover, if D has parameters (m, n, k, λ), then the corresponding relative difference set in G/H has parameters $(m, n/h, k, \lambda h)$, where $h = |H|$. Therefore, D is an extension of an $(m, k, n\lambda)$-difference set in G/N. Hence, difference sets are the images of relative difference sets via an homomorphism.

The existence of relative difference sets with parameters $(4t, 2, 4t, 2t)$ implies the existence of binary Hadamard matrices of order $4t$. Relative difference sets with the parameters $k = n\lambda$ have been constructed in many ways (Elliot and Butson [36], Jungnickel [51], Davis [26]).

2.5 Hadamard groups

In 1994, Ito [47, 48] introduced the concept of Hadamard groups and he showed a relation between Hadamard difference sets and Hadamard groups. Later in 1997, Ito [49] conjectured that the dicyclic group $Q_{8t} = \langle a, b \mid a^{4t} = 1, a^{2t} = b^2, b^{-1}ab = a^{-1} \rangle$ is always a Hadamard group. Schmidt [70] verified Ito's conjecture for all $t \leq 46$.

Definition 2.33 (Ito [47])**.** *A Hadamard group G of order $8t$ is a group containing a $4t$-subset D and a central involution u such that:*

(i) D and Da intersect exactly in $2t$ elements, for any $a \notin \langle u \rangle \subset G$.

(ii) Da and $\{b, bu\}$ intersect exactly in one element, for any $a, b \in G$.

The subset D is called *Hadamard subset* corresponding to u. From the previous definition, it follows that $G = D \cup Du$, and $D \cap Du = \emptyset$.

Remark 2.34. *Let D be a central relative $(4t, 2, 4t, 2t)$-difference set in a group G with forbidden subgroup $N \simeq \mathbb{F}_2$. The group G is a Hadamard group of order $8t$.*

Conjecture 2.35 (**Ito's conjecture**)**.** *The dicyclic group Q_{8t} is always a Hadamard group.*

Lemma 2.36 (Ito [47, Proposition 5]). *Let G be a Hadamard group of order $8t$ such that $G = N \times \langle u \rangle$, where N is a normal subgroup of G of index 2. Then the order of N is a square.*

Proposition 2.37 (Dillon [30, Theorem 3.1]). *Let C be a Hadamard group of order 2^{2s+2} and suppose that C has a normal subgroup G such that C/G is cyclic. Then C/G has order at most 2^{s+2}.*

Rifà and Suárez [66] showed that the concept of Hadamard group is equivalent to Hadamard full propelinear code.

Proposition 2.38 ([66, Prop. 3.2, Prop. 3.5]). *If $(C, \star)$ is an HFP-code of length $4t$, then C is an Hadamard group with a Hadamard difference subset D_1 corresponding to $\mathbf{1}$, where D_1 is the set of codewords with a zero in the first coordinate. Conversely, if G is Hadamard group of order $8t$ 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 $\theta : G \to C$ is such that $\theta(D) = D_1$ and $\theta(u) = \mathbf{1}$.*

2.6 Cocyclic Hadamard matrices

Flannery [37] proved that the concepts of cocyclic Hadamard matrix and Hadamard group are equivalent. De Launey, Flannery and Horadam [28] proved that the existence of a cocyclic Hadamard matrix of order $4t$ is equivalent to the existence of a normal relative difference set with parameters $(4t, 2, 4t, 2t)$.

Conjecture 2.39 (**Cocyclic Hadamard conjecture**). *There is a cocyclic Hadamard matrix of order $4t$ for every positive integer t.*

The cocyclic Hadamard conjecture (de Launey and Horadam [29]) implies Ito's conjecture, but not conversely.

Let G and U be finite groups, with U abelian, of orders v and w, respectively. A map $\psi : G \times G \to U$ such that

$$\psi(g,h)\psi(gh,k) = \psi(g,hk)\psi(h,k) \quad \forall\, g,h,k \in G \tag{2.1}$$

is a *cocycle* over G with coefficients in U. We may assume that ψ is *normalized*, i.e., $\psi(g,1) = \psi(1,g) = 1$ for all $g \in G$. For any (normalized) map $\phi : G \to U$,

the cocycle $\partial\phi$ defined by

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

is a *coboundary*. The set of all cocycles $\psi : G \times G \to U$ forms an abelian group $Z^2(G,U)$ under pointwise multiplication. Factoring out the subgroup of coboundaries gives $H^2(G,U)$, the *second cohomology group of G with coefficients in U*.

Given a group G and $\psi \in Z^2(G,U)$, denote by E_ψ the canonical central extension of U by G; this has elements $\{(u,g) \mid u \in U,\ g \in G\}$ and multiplication $(u,g)\ (v,h) = (uv\psi(g,h), gh)$. The image $U \times \{1\}$ of U lies in the centre of E_ψ and the set $T(\psi) = \{(1,g) :\ g \in G\}$ is a normalized transversal of $U \times \{1\}$ in E_ψ. In the other direction, suppose that E is a finite group with normalized transversal T for a central subgroup U. Put $G = E/U$ and $\sigma(tU) = t$ for $t \in T$. The map $\psi_T : G \times G \to U$ defined by $\psi_T(g,h) = \sigma(g)\sigma(h)\sigma(gh)^{-1}$ is a cocycle; furthermore, $E_{\psi_T} \cong E$.

Each cocycle $\psi \in Z^2(G,U)$ is displayed as a square matrix M_ψ whose rows and columns are indexed by the elements of G under some fixed ordering, and whose entry in position (g,h) is $\psi(g,h)$. The matrix

$$M_\psi = [\psi(g,h)]_{g,h\in G}$$

is called *G-cocyclic matrix*. To check if a cocyclic matrix is Hadamard, it can be applied the *cocyclic Hadamard test* [45]. It claims that it suffices to check whether the summation of every row but the first is zero. This test runs in $\mathcal{O}(t^2)$ time instead of $\mathcal{O}(t^3)$ which is the time for the algorithm for usual Hadamard matrices.

A cocycle $\psi \in Z^2(G,U)$ is called *orthogonal* if, for each $g \neq 1 \in G$ and each $u \in U$, $|\{h \in G : \psi(g,h) = u\}| = v/w$. This definition arose as an equivalent formulation of the condition that the G-cocyclic matrix M_ψ be a generalized Hadamard matrix $\mathrm{GH}(w, v/w)$ over U.

Definition 2.40. *A $v \times v$ matrix $H = (h_{ij})$ with entries in a finite abelian group U of order w, where w divides v, is a generalized Hadamard matrix* $\mathrm{GH}(w, v/w)$ *if, for every $i, j,\ 1 \leq i < j \leq v$, each of the multisets $\{h_{ik}h_{jk}^{-1} \mid 1 \leq k \leq v\}$ contains every element of U exactly v/w times.*

A GH$(w, v/w)$ is *normalized* if the first row and first column consist entirely of the identity element of U. We can always assume that our GH matrices are normalized.

For certain parameters, the existence of relative difference sets is equivalent to the existence of Hadamard matrices. The following result addresses this situation.

Theorem 2.41 (Perera and Horadam [60, Theorem 4.1])**.** *The following statements are equivalent.*

(i) $\psi \in Z^2(G, U)$ *is orthogonal.*

(ii) M_ψ *is a (normalized)* GH$(w, v/w)$*.*

(iii) $T(\psi) = \{(1, g) \mid g \in G\}$ *is a (central) relative* $(v, w, v, v/w)$*-difference set in the central extension* E_ψ *of* U *by* G *with forbidden subgroup* $U \times \{1\}$*.*

Chapter 3

HFP-codes with a fixed associated group

"Structures are the weapons of the mathematician."

Bourbaki.

The goal of this chapter is to study the rank and dimension of the kernel of the Hadamard full propelinear codes whose group structure consists of a nontrivial direct product of groups such that their associated group is $C_{2t} \times C_2$ (see Section 3.1) or $C_t \times C_2 \times C_2$ (see Section 3.2). In Section 3.1, we introduce Hadamard full propelinear codes with associated group $C_{2t} \times C_2$ obtaining four kinds of codes that are studied in Subsections 3.1.1–3.1.4. In each subsection, we study the rank and the dimension of the kernel of every kind of code that we have introduced. Also, we prove that the parameter t is even if the Hadamard full propelinear code has an abelian group structure, and the parameter t is odd if the code has a non-abelian group structure. In Subsections 3.1.1 and 3.1.4, we prove that the dimension of the kernel is equal to 1. In Subsection 3.1.2, we prove that if the dimension of the kernel is greater than 1, then either there exists a circulant Hadamard matrix or there exist a code of Subsection 3.1.1. In Subsection 3.1.3, we present a conjecture about the nonexistence of a kind of Hadamard full propelinear code that is equivalent to Arasu et al. conjecture [5] about the nonexistence of circulant complex Hadamard matrices. Also, we show that the circulant complex Hadamard matrix of order $2t = 16$, introduced by Arasu et al. in [5], corresponds to a Hadamard full propelinear code with a

group structure isomorphic to $C_{2t} \times C_4$ with rank equal to 11 and dimension of the kernel equal to 2. Moreover, we have found another nonequivalent Hadamard full propelinear code with a group structure isomorphic to $C_{2t} \times C_4$ of length $4t = 32$ with rank equal to 13 and dimension of the kernel equal to 1 which corresponds to a circulant complex Hadamard matrix of order 16.

In Section 3.2, we introduce Hadamard full propelinear codes with associated group $C_t \times C_2 \times C_2$ obtaining five kinds of codes that are studied in Subsections 3.2.1–3.2.5. In Subsection 3.2.1, we prove that if the length of the code is a power of two, then the length is bounded by 64. In Subsection 3.2.2, we present two constructions to obtain codes from the codes of Subsections 3.1.2 and 3.1.3. In Subsection 3.2.3, we prove that the dimension of the kernel is bounded by 3, and we explicit the codewords of the kernel.

The study of HFP-codes depending on its associated group Π is related with the study of cocycles over the group Π. Let H be a cocyclic Hadamard matrix over a finite group Π. We call associated group to this group Π in the context of Hadamard full propelinear codes. A Hadamard full propelinear code, as a group, is a central group extension of Π by C_2. In order to study Hadamard full propelinear codes with a determined associated group, it seems that the easiest way to start is to set the cyclic group as associated group. If the associated group is the cyclic group C_{4t} of order $4t$ then the corresponding Hadamard full propelinear code has one of the two following group structures, C_{8t} or $C_{4t} \times C_2$. Rifà and Suárez [66] proved that a Hadamard full propelinear code cannot be a cyclic group and Rifà [63] showed that a Hadamard full propelinear code of type $C_{4t} \times C_2$ is equivalent to a circulant Hadamard code. Remind that circulant Hadamard conjecture states that there are no circulant Hadamard matrices for orders greater than 4. Therefore, the next natural step is to study Hadamard full propelinear codes with associated group whose structure is a product of two cyclic groups, $C_{2t} \times C_2$, which are equivalent to the cocyclic Hadamard matrices over $C_{2t} \times C_2$. Baliga and Horadam [13] studied this class of cocyclic Hadamard matrices for the case t odd, i.e., the cocycles over the groups $C_t \times C_2^2$ for t odd. The solution set includes all Williamson Hadamard matrices, so this family of groups is potentially a uniform source for generation of Hadamard matrices. Any Hadamard matrix of order less than or equal to 20 is cocyclic. For orders less than or equal to 200, only order $4t = 188 = 4 \cdot 47$

is not yet known to have a cocyclic construction.

3.1 Associated group $C_{2t} \times C_2$

Now, we introduce a subclass of Hadamard full propelinear codes whose group structure consists of direct product of groups, fulfilling that its associated group Π is $C_{2t} \times C_2$. In other words, we study the short exact sequence

$$1 \to C_2 \to C \to C_{2t} \times C_2 \to 1,$$

where C is a nontrivial direct product of groups.

Proposition 3.1. *Let C be a Hadamard full propelinear code of length $4t$ with associated group $C_{2t} \times C_2$. If C as a group is a nontrivial direct product, then C is some of the following HFP-codes:*

(i) $\mathrm{HFP}(4t_{\mathbf{1}}, 2) \simeq C_{4t} \times C_2 = \langle a, b \mid a^{4t} = b^2 = \mathbf{0}, a^{2t} = \mathbf{1} \rangle$.

(ii) $\mathrm{HFP}(2t, 2, 2_{\mathbf{1}}) \simeq C_{2t} \times C_2 \times C_2 = \langle a, b, \mathbf{1} \mid a^{2t} = b^2 = \mathbf{0} \rangle$.

(iii) $\mathrm{HFP}(2t, 4_{\mathbf{1}}) \simeq C_{2t} \times C_4 = \langle a, b \mid a^{2t} = b^4 = \mathbf{0}, b^2 = \mathbf{1} \rangle$.

(iv) $\mathrm{HFP}(t, Q_{\mathbf{1}}) \simeq C_t \times Q = \langle d, a, b \mid d^t = \mathbf{0}, a^2 = b^2 = \mathbf{1}, aba = b \rangle$, *where Q is the quaternion group of eight elements.*

Proof. Note that there are two different cases depending on the parity of the value of t. Firstly, we suppose that t is odd, so $C_{2t} \times C_2 \simeq C_t \times C_2^2$. Let E be an HFP-code with $\Pi = C_t \times C_2^2$. From Proposition 2.19, $\Pi = E/\langle \mathbf{1} \rangle$. Thus, the code E is an extension of $C_t \times C_2^2$ by $\langle \mathbf{1} \rangle \simeq C_2$. From [37, Table 2], we have that the central extensions of $C_t \times C_2^2$ by C_2 with t odd are $C_t \times C_2^3$, $C_t \times C_4 \times C_2$, $C_t \times Q$ and $C_t \times D$ (where D is the dihedral group of order 8). Furthermore, as t is odd we have that $C_t \times D$ cannot be a Hadamard group by [47, Proposition 6]. Hence, from Proposition 2.38 there are no HFP-codes of type $C_t \times D$.

Now, we suppose that t is even. Let E be an HFP-code with associated group $\Pi = C_{2t} \times C_2$. From Proposition 2.19, $\Pi = E/\langle \mathbf{1} \rangle$. Thus, the code E is an extension of $C_{2t} \times C_2$ by $\langle \mathbf{1} \rangle \simeq C_2$. The extensions of C_2 by C_2 are C_4 and $C_2 \times C_2$. We denote by E_1 any of these extensions. Making the direct product

$E_1 \times C_{2t}$ we get two extensions of $C_{2t} \times C_2$ by C_2. Thus, we obtain $\mathrm{HFP}(2t, 4_{\mathbf{1}})$ and $\mathrm{HFP}(2t, 2, 2_{\mathbf{1}})$.

Let $t = 2^s t'$ with t' odd, so $C_{2t} \times C_2$ is isomorphic to $C_{2^{s+1}} \times C_{t'} \times C_2$. Let E_2 be the extensions of $C_{2^{s+1}}$ by C_2. As E_2/C_2 is cyclic, E_2 is abelian. Thus, E_2 is $C_{2^{s+2}}$ or $C_{2^{s+1}} \times C_2$. Making the direct product $E_2 \times C_{t'} \times C_2$ we get two extensions of $C_{2t} \times C_2$ by C_2. Thus, we obtain $\mathrm{HFP}(4t_{\mathbf{1}}, 2)$ and $\mathrm{HFP}(2t, 2, 2_{\mathbf{1}})$. Let E_3 be the extension of $C_{t'}$ by C_2, which is abelian since E_3/C_2 is cyclic. Hence, E_3 is $C_{2t'}$. Therefore, the direct product $C_{2t'} \times C_{2^{s+1}} \times C_2 \simeq C_{2t} \times C_2^2$ is an extension of $C_{2t} \times C_2$ by C_2, which corresponds with an $\mathrm{HFP}(2t, 2, 2_{\mathbf{1}})$-code. $\mathcal{QED}$

Remark 3.2. *In the conditions of Proposition 3.1, if t is even, then C cannot be an $\mathrm{HFP}(t, Q_{\mathbf{1}})$-code because its associated group is $C_t \times C_2^2$. If the value of t is odd, then $\mathrm{HFP}(t, 2, 2, 2_{\mathbf{1}}) \simeq \mathrm{HFP}(2t, 2, 2_{\mathbf{1}})$ and $\mathrm{HFP}(t, 4_{\mathbf{1}}, 2) \simeq \mathrm{HFP}(2t, 4_{\mathbf{1}}) \simeq \mathrm{HFP}(4t_{\mathbf{1}}, 2)$.*

Proposition 3.3. *Let C be a nonlinear Hadamard full propelinear code of length $4t$ with associated group $C_{2t} \times C_2$. Then:*

(i) If t is odd, then $r = 4t - 1$ and $k = 1$.

(ii) If t is even, then $r \leq 2t$, and $r = 2t$ if $t \equiv 2 \bmod 4$.

Proof. (i) and *(ii)* follow from Lemma 2.26 and [67, Lemma 4]. $\mathcal{QED}$

Proposition 3.4. *Let $C = \langle a, b, \mathbf{1} \rangle$ be an HFP-code of type $\mathrm{HFP}(4t_{\mathbf{1}}, 2)$ or $\mathrm{HFP}(2t, 2, 2_{\mathbf{1}})$ or $\mathrm{HFP}(2t, 4_{\mathbf{1}})$. Then, up to equivalence, we have:*

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

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

(iii) Knowing the value of a is enough to define b.

(iv) $\Pi = C_{2t} \times C_2$.

Proof. In any case, we have that $a^{2t}, b^2 \in \{\mathbf{0}, \mathbf{1}\}$, so π_a has order $2t$ and π_b has order 2. As π_a has order $2t$, π_a is the product of two cycles of length $2t$. Indeed, if we have a cycle of length $j < 2t$ then $\pi_{a^j} = \pi_a^j$ has a fixed point, which contradicts that C is full propelinear. Without loss of generality, we can

set $\pi_a = (1, 2, \ldots, 2t)(2t+1, 2t+2, \ldots, 4t)$, which shows *(i)*. As π_b has order 2, π_b is a product of disjoint transpositions. Each one of the transpositions sends an element of the first half of $\{1, 2, \ldots, 4t\}$ to the second half and vice versa. Indeed, assume $\pi_b(1) = i$ for $i \leq 2t$. We also have $\pi_{a^{i-1}}(1) = i$, so $\pi_{b^{-1}a^{i-1}}$ has a fixed point which contradicts that C is full propelinear. Furthermore, if $\pi_b(1) = i$ for $i \geq 2t+1$ then π_b is uniquely determined. Indeed, as $\pi_a\pi_b = \pi_b\pi_a$, we have that $\pi_{a^{-1}}(2) = 1$, $\pi_b(1) = i$, and $\pi_a(i) = i + 1$. Hence, $\pi_b(2) = i + 1$, and so on. Thus, we can assume $\pi_b = (1, 2t + 1)(2, 2t + 2) \ldots (2t, 4t)$, which shows *(ii)*.

Since $ab = ba$, we have $b = \pi_a(b) + a + \pi_b(a) = \pi_a(b) + \widehat{a}$, where $\widehat{a} = a + \pi_b(a) = (\widehat{a}_1, \ldots, \widehat{a}_{2t}, \widehat{a}_1, \ldots, \widehat{a}_{2t})$, then $b_i = \sum_{j=i+1}^{2t} \widehat{a}_j$ for $i \in \{1, \ldots, 2t-1\}$ and $b_{2t} \in \{0, 1\}$. We know that $b^2 \in \{\mathbf{0}, \mathbf{1}\}$.
If $b^2 = \mathbf{0}$, then $b = \pi_b(b)$, and $b_i = b_{2t+i}$ for $i \in \{1, \ldots, 2t\}$. Thus

$$\begin{aligned} b \;=\; \Bigg(& b_{2t} + \sum_{j=2}^{2t} \widehat{a}_j, b_{2t} + \sum_{j=3}^{2t} \widehat{a}_j, \ldots, b_{2t} + \widehat{a}_{2t}, b_{2t}, \\ & b_{2t} + \sum_{j=2}^{2t} \widehat{a}_j, b_{2t} + \sum_{j=3}^{2t} \widehat{a}_j, \ldots, b_{2t} + \widehat{a}_{2t}, b_{2t} \Bigg). \end{aligned}$$

If $b^2 = \mathbf{1}$, then $b = \pi_b(b) + \mathbf{1}$, so $b_i = b_{2t+i} + 1$ for $i \in \{1, \ldots, 2t\}$. Thus

$$\begin{aligned} b \;=\; \Bigg(& b_{2t} + \sum_{j=2}^{2t} \widehat{a}_j, b_{2t} + \sum_{j=3}^{2t} \widehat{a}_j, \ldots, b_{2t} + \widehat{a}_{2t}, b_{2t}, \\ & 1 + b_{2t} + \sum_{j=2}^{2t} \widehat{a}_j, 1 + b_{2t} + \sum_{j=3}^{2t} \widehat{a}_j, \ldots, 1 + b_{2t} + \widehat{a}_{2t}, 1 + b_{2t} \Bigg). \end{aligned}$$

(iv) follows from Proposition 2.19. $\mathcal{QED}$

Note that item *(iii)* saves us computing time because, by brute-force search, we only need to check different values of a.
In Subsections 3.1.1–3.1.3 we will use the permutations associated to the generators as in Proposition 3.4.

The following lemma will be useful in some proofs in the next sections. It is an stronger version of [67, Proposition 6].

Lemma 3.5. *Let C be a Hadamard code of length $4t$ with dimension of the kernel k, and $s \in \mathcal{K}(C) \setminus \langle \mathbf{1} \rangle$. Then $C|_s$ consists of two copies of a Hadamard*

code of length $2t$ *and dimension of the kernel equal to* $k-1$*, where* $C|_s$ *is the projection from* C *onto* $\mathrm{Supp}(s)$.

Proof. In [67, Proposition 6], it is proved that $C|_s$ consists of two copies of a Hadamard code of length $2t$. As we project the code C over the support of s, we have that $s|_s = \mathbf{1}_{2t}$. Thus, the kernel of $C|_s$ decreases in one unit. $\mathcal{QED}$

3.1.1 HFP$(4t_{\mathbf{1}}, 2)$-codes

In this subsection we assume that $C = \langle a, b \mid a^{4t} = b^2 = \mathbf{0}, a^{2t} = \mathbf{1} \rangle$.

Proposition 3.6. *Let* C *be an* $\mathrm{HFP}(4t_{\mathbf{1}}, 2)$*-code of length* $4t$ *with* $t > 1$*. Then* t *is even.*

Proof. Suppose that t is odd. Thus, $C_{4t} \times C_2 \simeq C_{2t} \times C_4$ and an $\mathrm{HFP}(4t_{\mathbf{1}}, 2)$-code is equivalent to an $\mathrm{HFP}(2t, 4_{\mathbf{1}})$-code. Without loss of generality, we can assume that $C = \langle a, b \mid a^{2t} = b^4 = \mathbf{0}, b^2 = \mathbf{1} \rangle$. From Proposition 3.3, $r = 4t-1$. We know that the rank of C is $r \leq \mathrm{rank}(H) + 1$ (due to the vector $\mathbf{1}$) but $r \leq \mathrm{rank}(H)$ if $\mathbf{1}$ is a combination of rows of H, where

$$H = \begin{pmatrix} a \\ a^2 \\ \vdots \\ a^{2t-1} \\ \mathbf{0} \\ b \\ ba \\ ba^2 \\ \vdots \\ ba^{2t-1} \end{pmatrix} = \begin{pmatrix} a \\ a + \pi_a(a) \\ \vdots \\ a + \pi_a(a^{2t-2}) \\ a + \pi_a(a^{2t-1}) \\ b \\ b + \pi_b(a) \\ b + \pi_b(a^2) \\ \vdots \\ b + \pi_b(a^{2t-1}) \end{pmatrix}.$$

If we sum the first half of rows, then we obtain $a + a^2 + \ldots + a^{2t-1} = \pi_a(a) + \ldots + \pi_a(a^{2t-1}) = \pi_a(a + \ldots + a^{2t-1})$. Thus, $a + a^2 + \ldots + a^{2t-1} = w$, such that $w = \pi_a(w)$. Therefore $w \in \{\mathbf{0}_{4t}, \mathbf{1}_{4t}, (\mathbf{0}_{2t}, \mathbf{1}_{2t}), (\mathbf{1}_{2t}, \mathbf{0}_{2t})\}$. If $w = \mathbf{0}_{4t}$, then in the first half of rows there is at most $2t-2$ independent rows, but if $w \in \{\mathbf{1}_{4t}, (\mathbf{0}_{2t}, \mathbf{1}_{2t}), (\mathbf{1}_{2t}, \mathbf{0}_{2t})\}$, then there is at most $2t-1$ independent rows. Making the sum of the second half of rows we obtain $\pi_b(a + a^2 + \ldots + a^{2t-1})$, so

the number of independent rows in the second half of rows is at most equal to the number of independent rows in the first half plus one, due to the vector b. Therefore, if $w = \mathbf{0}_{4t}$ then $\text{rank}(H) \leq 4t - 3$, and as a consequence $r \leq 4t - 2$. But if $w = \mathbf{1}_{4t}$, then $\mathbf{1}_{4t}$ appears as combination of the rows of the first half and also as combination of the rows of the second half. Hence, $\text{rank}(H) \leq 4t - 2$, and thus $r \leq 4t - 2$. If $w \in \{(\mathbf{0}_{2t}, \mathbf{1}_{2t}), (\mathbf{1}_{2t}, \mathbf{0}_{2t})\}$, then the sum of all rows of H is the vector $\mathbf{1}_{4t}$ and so in each column of H there is an odd number of ones, which contradicts that H is a Hadamard matrix for $t > 1$. Therefore, $r < 4t - 1$ which contradicts that t is odd by Proposition 3.3. $\mathcal{QED}$

Proposition 3.7. *Let C be a nonlinear* $\text{HFP}(4t_{\mathbf{1}}, 2)$*-code. If t is a power of two, then $r = 2t$.*

Proof. We suppose that t is a power of two, then $4t = 2^s$ for some integer $s \geq 2$. Let A be the matrix whose rows are $a, a^2, \ldots, a^{2t}$. Thus,

$$r \geq \text{rank}(A).$$

Vectors in $\mathbb{F}^{4t}$ can be written as polynomials in $\mathbb{F}[x]/(x^{4t} - 1)$, where the coordinates of the vector have been substituted by the coefficients of the polynomial. That is, $v = (v_0, v_1, \ldots, v_{4t-1}) \in \mathbb{F}^{4t}$ is represented by $v(x) = v_0 + v_1 x + \ldots + v_{4t-1} x^{4t-1}$.

Let $a = (a_1, a_2)$, where a_1 and a_2 are the first and the second half of components of the generator a, respectively. Since $a^{2t} = \mathbf{1}$, we have that $\text{wt}(a_i)$ is odd, so $a_i(x)$ does not contain the factor $(x - 1)$, for $i \in \{1, 2\}$. Note that

$$\text{rank}(A) = 2t - \deg(\gcd(a_1(x), a_2(x), x^{2^{s-1}} - 1)).$$

Since $a_1(x)$ and $a_2(x)$ do not contain the factor $(x - 1)$, and $x^{2^{s-1}} - 1 = (x - 1)^{2^{s-1}}$, we have that $\deg(\gcd(a_1(x), a_2(x), x^{2^{s-1}} - 1)) = 0$. Thus,

$$r \geq \text{rank}(A) = 2t.$$

From Proposition 3.3, we have that $r \leq 2t$, so $r = 2t$. $\mathcal{QED}$

Proposition 3.8. *Let C be an* $\text{HFP}(4t_{\mathbf{1}}, 2)$*-code. Then $b \notin \mathcal{K}(C)$.*

Proof. We are going to show that $b \notin \mathcal{K}(C)$. Assume the contrary and take $a = (a_1, a_2)$. We know that $b = (\beta, \beta)$, where $\text{wt}(\beta) = t$. As $b \in \mathcal{K}(C)$,

we have $ba, b+a \in C$. Thus, $(\beta+a_2, \beta+a_1), (\beta+a_1, \beta+a_2) \in C$ and the first vector should be at distance $2t$ to the second vector, so $\mathrm{wt}(a_1+a_2) = t$. Indeed, if $d(ab, a+b) = 0$, then $b = \pi_a(b)$ so $b \in \{\mathbf{0}, \mathbf{1}\}$, which is impossible. If $d(ab, a+b) = 4t$, then $a = (a_1, \bar{a}_1)$ and $b \in \{\boldsymbol{\omega}_{4t}, \bar{\boldsymbol{\omega}}_{4t}\}$. We denote the first and the second half of a^j by a_1^j and a_2^j, respectively, for any j. We have that $a^{2i} = (a_1^{2i}, a_1^{2i})$ for $i \in \{1, \ldots, t\}$. Hence, the projection of the first half a_1^{2i} onto the support of β, $a_1^{2i}|_\beta$, conform a Hadamard matrix of order t, and $a_1^2|_\beta$ generates a cyclic group, which is impossible by Lemma 2.22. Note that this lemma is only applicable if $t \geq 4$, but if $t = 3$ it is clear that $k = 1$. Thus, $d(ab, a+b) = 2t$ and $\mathrm{wt}(a_1+a_2) = t$. Now, using the same argument for all elements a^i of C instead of a, we obtain $\mathrm{wt}(a_1^i + a_2^i) = t$ and also $d(a_1^i+a_2^i, a_1^j+a_2^j) = t$. Indeed, $d(a_1^i+a_2^i, a_1^j+a_2^j) = \mathrm{wt}(a_1^i+a_1^j+a_2^i+a_2^j)$, and using Lemma 2.7, $\mathrm{wt}(a_1^i+a_1^j+a_2^i+a_2^j) = \mathrm{wt}(\pi_{a^i}(a_1^{j-i}+a_2^{j-i})) = \mathrm{wt}(a_1^{j-i}+a_2^{j-i}) = t$. Hence, the elements $(a_1^i+a_2^i)$, for $i \in \{1, \ldots, 4t\}$, give a cyclic Hadamard code of length $2t$, which is impossible. Therefore, $b \notin \mathcal{K}(C)$. $\mathcal{QED}$

Proposition 3.9. *Let C be an $\mathrm{HFP}(4t\mathbf{1}, 2)$-code. The vectors $(\mathbf{0}_{2t}, \mathbf{1}_{2t})$, $\boldsymbol{\omega}_{4t}$, and $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t})$ are not in the kernel of C for $t \geq 4$.*

Proof. Firstly, suppose that $(\mathbf{0}_{2t}, \mathbf{1}_{2t}) \in \mathcal{K}(C)$. Note that $(\mathbf{0}_{2t}, \mathbf{1}_{2t}) = a^t b$. Indeed, if $(\mathbf{0}_{2t}, \mathbf{1}_{2t}) = a^i$ for some i, then $(\mathbf{0}_{2t}, \mathbf{1}_{2t})^2 = \mathbf{0}$ which is not possible. If $(\mathbf{0}_{2t}, \mathbf{1}_{2t}) = a^i b$ for some i, then $(\mathbf{0}_{2t}, \mathbf{1}_{2t})^2 = \mathbf{1}$, so $i = t$. From Lemma 3.5, the projection of C over the support of $(\mathbf{0}_{2t}, \mathbf{1}_{2t})$ consists of two copies of a Hadamard code. We denote by $x|_{(\mathbf{0}_{2t}, \mathbf{1}_{2t})}$ the projection of a vector x over the support of $(\mathbf{0}_{2t}, \mathbf{1}_{2t})$. As $b^2 = \mathbf{0}$ and $b\,a^t b = a^t b\, b$, we have that $b = (\beta, \bar{\beta}, \beta, \bar{\beta})$ for some β. Thus, $a^t = (\bar{\beta}, \beta, \beta, \bar{\beta})$ and $a^t|_{(\mathbf{0}_{2t}, \mathbf{1}_{2t})} = b|_{(\mathbf{0}_{2t}, \mathbf{1}_{2t})}$. As $a^i b\, a^t b = a^t b\, a^i b$, we have that $a^i b = (\bar{\alpha}_{i,1}, \bar{\alpha}_{i,2}, \alpha_{i,2}, \alpha_{i,1})$, for some $\alpha_{i,j}$ where $i \in \{1, \ldots, 2t\}$ and $j \in \{1, 2\}$. Therefore, $a^{t+i} = (\alpha_{i,1}, \alpha_{i,2}, \alpha_{i,2}, \alpha_{i,1})$ and $a^i b|_{(\mathbf{0}_{2t}, \mathbf{1}_{2t})} = a^{t+i}|_{(\mathbf{0}_{2t}, \mathbf{1}_{2t})}$. Let α be the vector $a|_{(\mathbf{0}_{2t}, \mathbf{1}_{2t})}$ of length $2t$, and let $\pi_\alpha = (1, \ldots, 2t)$. Note that $\alpha^{2t} = a^{2t}|_{(\mathbf{0}_{2t}, \mathbf{1}_{2t})} = \mathbf{1}_{2t}$. We have that $\langle \alpha \rangle$ is a cyclic HFP-code of length $2t$, which contradicts Lemma 2.22 when $t \geq 2$.

Secondly, we suppose that $\boldsymbol{\omega}_{4t} \in \mathcal{K}(C)$. We have that $\boldsymbol{\omega}_{4t} \in \{a^i, a^i b\}$ for some i. If i is even, then $\boldsymbol{\omega}_{4t}^2 = \mathbf{0}$, so $\boldsymbol{\omega}_{4t} \in \{b, \bar{b}\}$ which contradicts Proposition 3.8. If i is odd, then $\boldsymbol{\omega}_{4t}^2 = \mathbf{1}$, so $i = t$, which contradicts Proposition 3.6.

Finally, suppose $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t}) \in \mathcal{K}(C)$. We will see that $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t}) = a^t b$. Let

$(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t}) = a^i$ for some i. If i is even, then $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t})^2 = \mathbf{0}$, which is not possible. If i is odd, then $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t})^2 = \mathbf{1}$, so $i = t$ which contradicts Proposition 3.6. Now, let $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t}) = a^i b$ for some i. If i is odd, then $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t})^2 = \mathbf{0}$ which is not possible. If i is even, then $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t})^2 = \mathbf{1}$, so $i = t$. Hence, $a^t b = (\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t})$. As $a^{2i} a^t b = a^t b a^{2i}$, it derives that $a^{2i} = (\alpha_{2i,1}, \alpha_{2i,2}, \alpha_{2i,2}, \alpha_{2i,1})$ for some $\alpha_{2i,j}$, with $i \in \{1, \ldots, t\}$ and $j \in \{1, 2\}$. From Lemma 3.5, the projection of C over the support of $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t})$ has a Hadamard structure. Taking the first half of coordinates of a^{2i} and projecting it over the support of $\boldsymbol{\omega}_{2t}$ we obtain a cyclic Hadamard code of length t, which contradicts Lemma 2.22 when $t \geq 4$. $\mathcal{QED}$

Proposition 3.10. *Let C be an* HFP$(4t_{\mathbf{1}}, 2)$*-code. Then $k \neq 2$ for $t \geq 4$.*

Proof. Suppose $k = 2$. Hence, there exists a vector $v \in \mathcal{K}(C) \setminus \langle \mathbf{1} \rangle$. From Lemma 2.8, as $a \in C$, we have that $\pi_a(v) \in \mathcal{K}(C)$. If $\pi_a(v) \in \langle \mathbf{1} \rangle$, then it contradicts $v \notin \langle \mathbf{1} \rangle$. If $\pi_a(v) = v$, then $v = (\mathbf{0}_{2t}, \mathbf{1}_{2t})$, which contradicts Proposition 3.9. If $\pi_a(v) = \bar{v}$, then $v \in \{\boldsymbol{\omega}_{4t}, (\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t})\}$, which contradicts Proposition 3.9. $\mathcal{QED}$

Lemma 3.11. *Let C be an* HFP$(4t_{\mathbf{1}}, 2)$*-code. If $v \in \mathcal{K}(C) \setminus \langle \mathbf{1} \rangle$ and j_v is the smallest value such that $\pi_a^{j_v}(v) = v$, then j_v is even.*

Proof. Let $v \in \mathcal{K}(C) \setminus \langle \mathbf{1} \rangle$. As $a^i \in C$ for $i \in \{1, \ldots, 2t\}$, from Lemma 2.8 we have that $\pi_a^i \in \mathrm{Aut}(\mathcal{K}(C))$, so $\pi_a^i(v) \in \mathcal{K}(C)$. Therefore, there is some j such that $\pi_a^j(v) = v$. Note that $j \neq 1$. Indeed, $j = 1$ implies that $\pi_a(v) = v$, so $v \in \{\mathbf{0}, \mathbf{1}, (\mathbf{0}_{2t}, \mathbf{1}_{2t}), (\mathbf{1}_{2t}, \mathbf{0}_{2t})\}$, which is not possible by Proposition 3.9. As $\pi_a^j(v) = v$, it derives that $v = (v_1, \ldots, v_j, v_1, \ldots || v_{2t+1}, \ldots, v_{2t+j}, v_{2t+1}, \ldots)$, where $||$ separates the first half from the second. Since $\mathrm{wt}(v) = 2t$, we have $2t = (4t/2j)\mathrm{wt}(v_1, \ldots, v_j, v_{2t+1}, \ldots, v_{2t+j})$, so $\mathrm{wt}(v_1, \ldots, v_j, v_{2t+1}, \ldots, v_{2t+j}) = j$. Suppose that j is an odd number. Without loss of generality, we can assume that the first j coordinates of v have an odd weight, and the first j coordinates of the second half of v have an even weight. Note that $v + \pi_a(v) = (v_1 + v_j, \ldots, v_j + v_{j-1}, v_1 + v_j, \ldots || v_{2t+1} + v_{2t+j}, \ldots, v_{2t+j} + v_{2t+j-1}, v_{2t+1} + v_{2t+j}, \ldots) \in \mathcal{K}(C)$. Moreover, since $\mathrm{wt}(v + \pi_a(v)) = 2t$, we have $2t = (4t/2j)\mathrm{wt}(v_1 + v_j, \ldots, v_j + v_{j-1}, v_{2t+1} + v_{2t+j}, \ldots, v_{2t+j} + v_{2t+j-1})$, so $\mathrm{wt}(v_1 + v_j, \ldots, v_j + v_{j-1}, v_{2t+1} + v_{2t+j}, \ldots, v_{2t+j} + v_{2t+j-1}) = j$, but $\mathrm{wt}(v_1 + v_j, \ldots, v_j + v_{j-1}, v_{2t+1} + v_{2t+j}, \ldots, v_{2t+j} + v_{2t+j-1})$ is even, then we have a contradiction and therefore j cannot be odd. $\mathcal{QED}$

Proposition 3.12. *Let C be an* HFP$(4t_{\mathbf{1}}, 2)$*-code. If $k > 1$, then the length of C is a power of two.*

Proof. Let $4t = 2^s t'$, where t' is odd. For any binary vector x of even length we say that $x^{(1)}, x^{(2)}$ are the projections over the first and the second half part of x, respectively. Let $v \in \mathcal{K}(C) \setminus \langle \mathbf{1} \rangle$. From Lemma 2.8, as $b \in C$ we have that $\pi_b \in \mathrm{Aut}(\mathcal{K}(C))$. Hence, $\pi_b(v) \in \mathcal{K}(C)$, and $v + \pi_b(v) \in \mathcal{K}(C)$ since the kernel is a subspace. We denote $v + \pi_b(v)$ by v_1. Since $v + \pi_b(v) = (v^{(1)} + v^{(2)}, v^{(1)} + v^{(2)})$, we have $v_1^{(1)} = v_1^{(2)}$. As $a^t \in C$, $v_1 + \pi_{a^t}(v_1) \in \mathcal{K}(C)$. We denote $v_1 + \pi_{a^t}(v_1)$ by v_2. Note that $v_1^{(1)(1)} = v_1^{(1)(2)}$, since $v_1 + \pi_{a^t}(v_1) = (v^{(1)(1)} + v^{(1)(2)}, v^{(1)(1)} + v^{(1)(2)}, v^{(1)(1)} + v^{(1)(2)}, v^{(1)(1)} + v^{(1)(2)})$. If we repeat the same construction for v_2 using $\pi_{a^{t/2}}$, we obtain $v_3 = (\alpha_3, \ldots, \alpha_3) \in \mathcal{K}(C)$, where the length of α_3 is $t/2$. If we repeat this process until we can apply $\pi_{a^{t/2^s}}$, we obtain a vector w in the kernel which can be divided in 2^s parts of length t' which are exactly equal. Thus, we have $\pi_a^{t'}(w) = w$, and from Lemma 3.11, it is only possible if $t' = 1$ and $w \in \{\mathbf{0}, \mathbf{1}\}$.

In each iteration of the construction of v_i's it could happen two exceptions. We could get a vector v_j which is compounded by a combination of $\mathbf{0}_l$'s and $\mathbf{1}_l$'s. As $v_j + \pi_a(v_j) \in \mathcal{K}(C)$,$\mathrm{wt}(v_j + \pi_a(v_j)) \in \{0, 2t, 4t\}$, which is not possible by the shape of v_j, unless $v_j = (\mathbf{0}_l, \mathbf{1}_l, \ldots, \mathbf{0}_l, \mathbf{1}_l)$ with $l \in \{1, 2, 2t\}$ or $v_j = (\mathbf{0}_l, \mathbf{1}_l, \mathbf{1}_l, \mathbf{0}_l, \ldots, \mathbf{1}_l, \mathbf{0}_l)$ where only appear two consecutive equal parts with $l = 1$. Firstly, we suppose that $v_j = (\mathbf{0}_l, \mathbf{1}_l, \ldots, \mathbf{0}_l, \mathbf{1}_l)$ with $l \in \{1, 2, 2t\}$. If $l = 1$, then $\boldsymbol{\omega}_{4t} \in \mathcal{K}(C)$ which contradicts Proposition 3.9. If $l = 2t$, then $v_j = (\mathbf{0}_{2t}, \mathbf{1}_{2t})$, which contradicts Proposition 3.9. If $l = 2$, then $v_j + \pi_a(v_j) = \boldsymbol{\omega}_{4t} \in \mathcal{K}(C)$, which contradicts Proposition 3.9. Now, we suppose that $v_j = (\mathbf{0}_l, \mathbf{1}_l, \mathbf{1}_l, \mathbf{0}_l, \ldots, \mathbf{1}_l, \mathbf{0}_l)$ where only appear two consecutive equal parts with $l = 1$. It is clear that there exists a permutation π_{a^i} for some i such that $\pi_{a^i}(v_j) = (\mathbf{0}_l, \mathbf{0}_l, \mathbf{1}_l, \mathbf{1}_l, \ldots, \mathbf{0}_l, \mathbf{0}_l, \mathbf{1}_l, \mathbf{1}_l)$, which is the same case as before where $l = 2$.

The other exception is that we could obtain a vector $v_j \in \{\mathbf{0}, \mathbf{1}\}$ for some j. This means that $v_{j-1} = (\gamma, \ldots, \gamma)$ or $v_{j-1} = (\delta, \bar{\delta}, \ldots, \delta, \bar{\delta})$ with γ, δ of length i and $v_j = v_{j-1} + \pi_{a^i}(v_{j-1}) \in \{\mathbf{0}, \mathbf{1}\}$. Note that i is even. On the contrary, if $v_{j-1} = (\gamma, \ldots, \gamma)$, then $\pi_a^i(v_{j-1}) = v_{j-1}$ which is not possible by Lemma 3.11. If $v_{j-1} = (\delta, \bar{\delta}, \ldots, \delta, \bar{\delta})$, then $\mathrm{wt}(v_{j-1} + \pi_a(v_j)) \notin \{0, 2t, 4t\}$. Therefore, i is even. In order to try to solve this case, we have to take $v_j =$

$v_{j-1} + \pi_{a^{i/2}}(v_{j-1})$. Thus, we obtain $v_j = (\gamma^{(1)} + \gamma^{(2)}, \ldots, \gamma^{(1)} + \gamma^{(2)})$ or $v_j = (\delta^{(1)} + \delta^{(2)}, \ldots, \delta^{(1)} + \delta^{(2)})$. If we obtain $v_j \in \{\mathbf{0}, \mathbf{1}\}$ again, then we have to take $v_j = v_{j-1} + \pi_{a^{i/4}}(v_{j-1})$ and we can repeat this until we get $v_j \notin \{\mathbf{0}, \mathbf{1}\}$ unless $v_{j-1} \in \{\mathbf{0}, \mathbf{1}, (\mathbf{0}_l, \mathbf{1}_l, \ldots, \mathbf{0}_l, \mathbf{1}_l)\}$. But, if $v_{j-1} \in \{\mathbf{0}, \mathbf{1}\}$ then we can repeat an analogous argumentation as for v_j obtaining $v \in \{\mathbf{0}, \mathbf{1}\}$ which contradicts the hypotheses. If $v_{j-1} = (\mathbf{0}_l, \mathbf{1}_l, \ldots, \mathbf{0}_l, \mathbf{1}_l)$, then we obtain the first exception that we have treated in the previous paragraph. $\mathcal{QED}$

Theorem 3.13. *Let C be an* HFP$(4t_{\mathbf{1}}, 2)$*-code. Then $k = 1$ for $t \geq 4$.*

Proof. Suppose $k > 1$. From Proposition 3.10, we have $k \geq 3$. From Proposition 3.12 and Proposition 3.7, t is a power of two and $r = 2t$, which contradicts Lemma 2.2 for any $t \geq 3$. $\mathcal{QED}$

3.1.2 HFP$(2t, 2, 2_{\mathbf{1}})$-codes

In this subsection we assume that $C = \langle a, b, \mathbf{1} \mid a^{2t} = b^2 = \mathbf{1}^2 = \mathbf{0} \rangle$.

Proposition 3.14. *Let C be an* HFP$(2t, 2, 2_{\mathbf{1}})$*-code of length $4t$ with $t > 1$. Then t is an even square number.*

Proof. We have that $C \simeq C_{2t} \times C_2 \times \langle \mathbf{1} \rangle = N \times \langle \mathbf{1} \rangle$, where $N = C_{2t} \times C_2$. From Lemma 2.36 we have that $|C_{2t} \times C_2|$ is a square, thus t is a square. The proof of Proposition 3.6 only depends on the associated permutations to the generators of the code, so we can use the same proof to get that t is even. $\mathcal{QED}$

Proposition 3.15. *Let C be an* HFP$(2t, 2, 2_{\mathbf{1}})$*-code of length $4t$. If t is a power of two, then $t \in \{1, 4\}$.*

Proof. From Proposition 2.29, as $C = C_{2t} \times C_2 \times \langle \mathbf{1} \rangle$, we have a Hadamard difference set in $C_{2t} \times C_2$. From Proposition 3.14, t is also a square, so $t = 2^{2s}$ for some s. Thus, the order and the exponent of $C_{2t} \times C_2$ are 2^{2s+2} and 2^{2s+1}, respectively. From Proposition 2.28, it derives that $s \leq 1$. $\mathcal{QED}$

The next lemmas will be helpful in some proofs.

Lemma 3.16. *Let C be an* HFP$(2t, 2, 2_{\mathbf{1}})$*-code. Then $(\mathbf{0}_{2t}, \mathbf{1}_{2t}) \notin \mathcal{K}(C)$.*

Proof. Firstly, we note that if $(\mathbf{0}_{2t}, \mathbf{1}_{2t}) \in C$, then $(\mathbf{0}_{2t}, \mathbf{1}_{2t}) = a^t$. Indeed, if $(\mathbf{0}_{2t}, \mathbf{1}_{2t}) = a^i b$ for some $i \in \{1, \ldots, 2t\}$, then $(\mathbf{0}_{2t}, \mathbf{1}_{2t})^2 = \mathbf{1}$, which is not possible. If $(\mathbf{0}_{2t}, \mathbf{1}_{2t}) = a^i$ for some $i \in \{1, \ldots, 2t\}$, then $(\mathbf{0}_{2t}, \mathbf{1}_{2t})^2 = \mathbf{0}$ and so $i = t$. Now we assume that $a^t = (\mathbf{0}_{2t}, \mathbf{1}_{2t}) \in \mathcal{K}(C)$. Let $a = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$. Since $aa^t = a^t a$, we have $\alpha_0 = \alpha_1$ and $\alpha_2 = \alpha_3$. From Lemma 2.7, it derives that $a^t = a + \pi_a(a) + \ldots + \pi_a^{t-1}(a) = (\mathbf{0}_{2t}, \mathbf{1}_{2t})$, so $\sum_{i=1}^{t} a_i = 0$ and $\sum_{i=2t+1}^{3t} a_i = 1$. From Lemma 3.5, the projection of C over $\mathrm{Supp}(a^t)$ has a Hadamard structure. Therefore, $\mathrm{wt}(\alpha_i) = t/2$, where $i \in \{0, 2\}$. As $\sum_{i=2t+1}^{3t} a_i = 1$, we have that $\mathrm{wt}(\alpha_2)$ is odd, which is not possible since t is an even square number, and so $(\mathbf{0}_{2t}, \mathbf{1}_{2t}) \notin \mathcal{K}(C)$. $\mathcal{QED}$

Lemma 3.17. *Let C be an $\mathrm{HFP}(2t, 2, 2_{\mathbf{1}})$-code. If $v \in \mathcal{K}(C) \setminus \langle \mathbf{1} \rangle$ and j_v is the smallest value such that $\pi_a^{j_v}(v) = v$, then j_v is even.*

Proof. The proof is analogous to the one in Lemma 3.11. $\mathcal{QED}$

Lemma 3.18. *Let C be an $\mathrm{HFP}(2t, 2, 2_{\mathbf{1}})$-code of length $4t$. Let v be the codeword $\boldsymbol{\omega}_{4t}$ or $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t})$ in the kernel of C. If $v \neq a^t$, then there exists a circulant Hadamard code of length t. If $v = a^t$, then there exists an $\mathrm{HFP}(t_{\mathbf{1}}, 2)$-code of length t. The vectors $\boldsymbol{\omega}_{4t}$ and $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t})$ are not simultaneously in $\mathcal{K}(C)$.*

Proof. Let $v = \boldsymbol{\omega}_{4t} \in \mathcal{K}(C)$. We suppose that $v \in \{a^i, a^i b\}$ for some i, then $v^2 = \mathbf{0}$ if i is even, and $v^2 = \mathbf{1}$ if i is odd. Due to the structure of the code, there are no elements whose square is the vector $\mathbf{1}$. Thus, we have $v^2 = \mathbf{0}$ implying that $i \in \{0, t\}$. Hence $v \in \{b, a^t b, a^t\}$.

Firstly, we suppose that $v = b$. From Lemma 3.5, the projection of the code onto $\mathrm{Supp}(b)$ should have a Hadamard structure, which is not necessarily full propelinear. However, from $a^2 b = b a^2$ we obtain $a^2 + \pi_b(a^2) = b + \pi_a^2(b) = \mathbf{0}$. Thus, a^2 has the same values in the first and in the second half part. The subgroup of C generated by a^2 projected over the first half part of $\mathrm{Supp}(b)$ is an $\mathrm{HFP}(t, 2_{\mathbf{1}})$-code, $\widehat{C}$, of length t. From Lemma 2.23, we know that $\widehat{C}$ is a circulant Hadamard code and the dimension of its kernel is $\widehat{k} = 1$.

Secondly, we suppose that $v = a^t b$. From Lemma 3.5, the projection of the code onto $\mathrm{Supp}(a^t b)$ should have a Hadamard structure, which is not necessarily full propelinear. However, from $a^2 a^t b = a^t b a^2$ we obtain $a^2 + \pi_{a^t b}(a^2) = a^t b + \pi_a^2(a^t b) = \mathbf{0}$. Hence, a^2 has the same values in the first and in the second

half part, but in different order. The subgroup of C generated by a^2 projected over the first half part of $\mathrm{Supp}(a^t b)$ is an $\mathrm{HFP}(t, 2_{\mathbf{1}})$-code. Thus, from Lemma 2.23 it is a circulant Hadamard code and the dimension of its kernel is 1.

Thirdly, we suppose that $v = a^t$. Since $a^j a^t = a^t a^j$, we have that $a^j = (\alpha_{j,1}, \alpha_{j,1}, \alpha_{j,2}, \alpha_{j,2})$ if j is even, and $a^j = (\gamma_{j,1}, \bar{\gamma}_{j,1}, \gamma_{j,2}, \bar{\gamma}_{j,2})$ if j is odd. Let $b = (\beta_1, \beta_2, \beta_1, \beta_2)$ for some β_1, β_2, since $b^2 = \mathbf{0}$. As $ba^t = a^t b$, $\beta_1 = \beta_2$. Hence, $b = (\beta_1, \beta_1, \beta_1, \beta_1)$. From Lemma 3.5, the projection of the code onto $\mathrm{Supp}(a^t)$ should have a Hadamard structure, which is not necessarily full propelinear. The subgroup $\langle(\alpha_{2,1}, \alpha_{2,2})\rangle \times \langle(\beta_1, \beta_1)\rangle$ projected onto $\mathrm{Supp}(a^t)$ is an $\mathrm{HFP}(t_{\mathbf{1}}, 2)$-code.

Now, let $v = (\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t}) \in \mathcal{K}(C)$. Therefore $v \notin \{b, a^i b\}$ for any i. If $v = b$, then $b^2 = \mathbf{1}$ which is not possible. If $v = a^i b$, then $v^2 = \mathbf{0}$ if i is odd, and $v^2 = \mathbf{1}$ if i is even, which is not possible since t is even. Thus, $v = a^t$, but if we apply an analogous argumentation as before we obtain an $\mathrm{HFP}(t_{\mathbf{1}}, 2)$-code.

To conclude, we suppose that $\boldsymbol{\omega}_{4t}$ and $(\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t})$ are in $\mathcal{K}(C)$. Since $\mathcal{K}(C)$ is a linear subspace, then $\boldsymbol{\omega}_{4t} + (\boldsymbol{\omega}_{2t}, \bar{\boldsymbol{\omega}}_{2t}) = (\mathbf{0}_{2t}, \mathbf{1}_{2t}) \in \mathcal{K}(C)$ which contradicts Lemma 3.16. $\mathcal{QED}$

Theorem 3.19. *Let C be an $\mathrm{HFP}(2t, 2, 2_{\mathbf{1}})$-code of length $4t$. If $k > 1$, then we have some of the following:*

(i) $k = 5$, $t = 4$, *and C is linear.*

(ii) $k = 3$, $t = 1$, *and C is linear.*

(iii) $k = 3$, $t = 4$, *and $r = 6$.*

(iv) $k = 2$, *and there exists a circulant Hadamard code of length $4t' = t$, where t' is an odd square.*

(v) $k = 2$, *and there exists an $\mathrm{HFP}(4t'_{\mathbf{1}}, 2)$-code of length $4t' = t$, where t' is even.*

Proof. Firstly, we see that t is a power of two except in two cases. We can use the same proof that in Proposition 3.12, since the associated permutations to the generators are the same. To approach the two exceptions that appears in the proof of Proposition 3.12, here we use Lemma 3.17 and Lemma 3.18

instead of Lemma 3.11 and Proposition 3.9. Therefore, there exists a circulant Hadamard code of length $4t'$ or an HFP$(4t'_{\mathbf{1}}, 2)$-code, where $4t' = t$. If there are any of these two exceptions, then from Lemma 2.24, Theorem 3.13 and Lemma 3.5, $k = 2$.

If t is a power of two, then $t \in \{1, 4\}$ by Proposition 3.15. Finally, making use of the software MAGMA [18], we compute all the possibilities for HFP$(2t, 2, 2_{\mathbf{1}})$-codes with $t \in \{1, 4\}$. For $t = 1$, there is a linear code with $r = k = 3$. For $t = 4$, there is a linear code with $r = k = 5$, and there is a nonlinear code with $r = 6$ and $k = 3$. $\mathcal{QED}$

3.1.3 HFP$(2t, 4_{\mathbf{1}})$-codes

In this subsection we assume that $C = \langle a, b \mid a^{2t} = b^4 = \mathbf{0}, b^2 = \mathbf{1} \rangle$.

Proposition 3.20. *Let C be an* HFP$(2t, 4_{\mathbf{1}})$*-code of length $4t$ with $t > 1$. Then t is even.*

Proof. Suppose that t is odd. From Remark 3.2, HFP$(2t, 4_{\mathbf{1}}) \simeq$ HFP$(4t_{\mathbf{1}}, 2)$. Thus, t cannot be odd by Proposition 3.6. $\mathcal{QED}$

Proposition 3.21. *Let C be an* HFP$(2t, 4_{\mathbf{1}})$*-code of length $4t$. If t is a power of two, then $t \leq 8$.*

Proof. Let $t = 2^s$ for some s. Thus, we have that C_4 is a normal subgroup of C and $C/C_4 \simeq C_{2^{s+1}}$. From Proposition 2.37, $|C/C_4| \leq (s + 5)/2$. Hence, $s \leq 3$. $\mathcal{QED}$

Proposition 3.22. *Let C be an* HFP$(2t, 4_{\mathbf{1}})$*-code. If $(\mathbf{0}_{2t}, \mathbf{1}_{2t}) \in \mathcal{K}(C)$, then $k = 2$ and there exists a circulant Hadamard code of length $2t$.*

Proof. Note that if $v = (\mathbf{0}_{2t}, \mathbf{1}_{2t}) \in C$, then $v \in \{a^t, b, a^t b\}$. Indeed, if $v = a^i b$ for some $i \in \{1, \ldots, 2t\}$, then $(\mathbf{0}_{2t}, \mathbf{1}_{2t})^2 = \mathbf{1}$, so $i \in \{t, 2t\}$. If $v = a^i$ for some $i \in \{1, \ldots, 2t\}$, then $(\mathbf{0}_{2t}, \mathbf{1}_{2t})^2 = \mathbf{0}$ and so $i = t$. Now, we suppose $v \in \mathcal{K}(C)$. From Lemma 3.5, the projection of C over the support of v has a Hadamard structure. Thus, the second half of coordinates of each codeword has weight 0 or t or $2t$. We denote the second half of coordinates of a vector x by $x^{(2)}$. If we set $\pi_{a^{(2)}} = (1, 2, \ldots, 2t)$, then $a^{(2)}$ generates a cyclic group or order $2t$.

Firstly, we suppose that $v = b$. Thus, $b^{(2)} = \mathbf{1}$ and we set $\pi_{b^{(2)}} = I$. Hence, $\langle a^{(2)}, b^{(2)} \rangle \simeq C_{2t} \times C_2$, which is an HFP$(2t, 2_{\mathbf{1}})$-code. Since t is even, we have an

$\mathrm{HFP}(4(t/2), 2_{\mathbf{1}})$-code, which is a circulant Hadamard code. From Lemma 2.24, circulant Hadamard codes have dimension of the kernel equal to 1. Therefore, $k = 2$ by Lemma 3.5.

Secondly, we suppose that $v = a^t b$. Thus, $(a^t b)^{(2)} = \mathbf{1}$, and let $\pi_{(a^t b)^{(2)}} = I$. We have that $\langle a^{(2)}, (a^t b)^{(2)} \rangle \simeq C_{2t} \times C_2$ which is an $\mathrm{HFP}(2t, 2_{\mathbf{1}})$-code. Since t is even, we have an $\mathrm{HFP}(4(t/2), 2_{\mathbf{1}})$-code. As before, it is a circulant Hadamard code. From Lemma 2.24 and Lemma 3.5, $k = 2$.

Finally, we suppose that $v = a^t$. Let $a^j = (\alpha_{j0}, \alpha_{j1}, \alpha_{j2}, \alpha_{j3})$. Since $a^j a^t = a^t a^j$, we have that $\alpha_{j0} = \alpha_{j1}$, and $\alpha_{j2} = \alpha_{j3}$. Since $b^2 = \mathbf{1}$ and $ba^t = a^t b$, we have that $b = (\beta_1, \bar{\beta}_1, \bar{\beta}_1, \beta_1)$. We have the following Hadamard matrix,

$$H = \begin{pmatrix} A_1 & A_1 & A_2 & A_2 \\ B_1 + A_2 & \bar{B}_1 + A_2 & \bar{B}_1 + A_1 & B_1 + A_1 \end{pmatrix},$$

where A_1, A_2 are matrices whose rows are α_{j0}, α_{j2}, respectively, for $j \in \{1, \ldots, 2t\}$, and B is the matrix whose rows are β_1. Since H is a Hadamard matrix, if we set the matrix

$$\widehat{H} = \begin{pmatrix} A_1 & A_2 \\ B_1 + A_2 & \bar{B}_1 + A_1 \end{pmatrix},$$

then $\widehat{H}$ is a matrix whose rows have weight t, except the last row of (A_1, A_2) which is $\mathbf{0}$, and the distance between any pair of rows is t. Note that (A_1, A_2) is a Hadamard matrix of order $2t$. Moreover, (α_0, α_2) generates a cyclic group of order $2t$. Thus, the rows of (A_1, A_2) and their complements are an $\mathrm{HFP}(2t, 2_{\mathbf{1}})$-code. As before, we have that $k = 2$. $\mathcal{QED}$

Proposition 3.23. *If there exists a circulant Hadamard code C of length $4t$, then there also exists an $\mathrm{HFP}(4t, 4_{\mathbf{1}})$-code of length $8t$ with kernel $\langle \mathbf{1}, (\mathbf{0}_{4t}, \mathbf{1}_{4t}) \rangle$.*

Proof. From [63, Proposition 2.2], as C is a circulant Hadamard code, we have that $C = \langle a, \mathbf{1} \rangle$ is an $\mathrm{HFP}(4t, 2_{\mathbf{1}})$-code. Let $b = (\mathbf{0}_{4t}, \mathbf{1}_{4t})$, and H be the Hadamard matrix whose rows are $a, a^2, \ldots, a^{4t}$. Let $\widehat{H}$ be the matrix obtained by Sylvester's construction,

$$\widehat{H} = \begin{pmatrix} H & H \\ H & \bar{H} \end{pmatrix} = \begin{pmatrix} a & a \\ a^2 & a^2 \\ \vdots & \vdots \\ a^{4t} & a^{4t} \\ a & a+\mathbf{1} \\ a^2 & a^2+\mathbf{1} \\ \vdots & \vdots \\ a^{4t} & a^{4t}+\mathbf{1} \end{pmatrix}.$$

We note that the rows of $\widehat{H}$ and its complements form an HFP$(4t, 4_{\mathbf{1}})$-code, $\widehat{C}$, of length $8t$ given by $\langle (a,a), b\rangle$. As $(\mathbf{0}_{4t}, \mathbf{1}_{4t}) + w \in \widehat{C}$ for every $w \in \widehat{C}$, we have that $(\mathbf{0}_{4t}, \mathbf{1}_{4t}) \in \mathcal{K}(\widehat{C})$. Since C is a circulant Hadamard code, $\dim(\mathcal{K}(C)) = 1$ by Lemma 2.24. Hence, $\mathcal{K}(\widehat{C}) = \langle \mathbf{1}, (\mathbf{0}_{4t}, \mathbf{1}_{4t})\rangle$. $\mathcal{QED}$

From Proposition 3.22 and Proposition 3.23, we have a link between the existence of HFP$(2t, 4_{\mathbf{1}})$-codes with $\mathcal{K}(C) = \langle \mathbf{1}, (\mathbf{0}_{2t}, \mathbf{1}_{2t})\rangle$ and the existence of circulant Hadamard matrices. Even if Conjecture 2.13 is true, there could exist HFP$(2t, 4_{\mathbf{1}})$-codes with a kernel different from $\langle \mathbf{1}, (\mathbf{0}_{2t}, \mathbf{1}_{2t})\rangle$.

Remark 3.24. *Arasu, de Launey and Ma [5] proved that a circulant complex Hadamard matrix of order* $2t$ *is equivalent to a relative* $(4t, 2, 4t, 2t)$*-difference set in the group* $C_4 \times C_{2t}$ *where the forbidden subgroup is the unique subgroup of order two which is contained in the* C_4 *component. Thus,* HFP$(2t, 4_{\mathbf{1}})$*-codes are equivalent to circulant complex Hadamard matrices of order* $2t$*. Arasu et al. [5] also conjectured that there is no circulant complex Hadamard matrix of order greater than* 16*, and they proved several non-existence results for circulant complex Hadamard matrices. The following orders up to* 1000 *have yet to be excluded:* $260, 340, 442, 468, 520, 580, 680, 754, 820, 884, 890$.

A complex Hadamard matrix of order $2t$ is a matrix H whose entries are in $\{1, i, -1, -i\}$ such that $HH^* = 2tI_{2t}$, where H^* denotes the conjugate transpose of H. Let H be a circulant complex Hadamard matrix with first row g. From [5, Theorem 1.2], a Hadamard difference set can be built from g. From Proposition 3.4, an HFP$(2t, 4_{\mathbf{1}})$-code can be built from only one generator a. Next, we will make explicit the relationship between the first row $g = (g_1, g_2, \ldots, g_{2t})$ of a circulant complex Hadamard matrix and a generator

a of an HFP$(2t, 4_{\mathbf{1}})$-code. Let ϕ be the isomorphism from the abelian multiplicative group of fourth roots of unity to the additive group $\mathbb{Z}_4$, whose elements $\{0, 1, 2, 3\}$ after a Gray map [22], are taken as $\{(0,0), (0,1), (1,1), (1,0)\}$. Hence, for each coordinate of g, we have

$$\begin{array}{rcl} & \phi & \\ 1 & \to & (0,0) \\ i & \to & (0,1) \\ -1 & \to & (1,1) \\ -i & \to & (1,0) \end{array}$$

Set $\phi(g) = (\phi(g_1), \ldots, \phi(g_{2t})) \in \mathbb{F}^{4t}$ and rearrange the coordinates of $\phi(g)$ putting the first coordinates $\phi(g_i)_1$ of each $\phi(g_i)$ in the first half, and the second coordinates $\phi(g_i)_2$ in the second half. Thus,

$$\phi(g) = (\phi(g_1)_1, \ldots, \phi(g_{2t})_1, \phi(g_1)_2, \ldots, \phi(g_{2t})_2).$$

Define $\pi_a = (1, 2, \ldots, 2t)(2t+1, \ldots, 4t)$ and take $a = \phi(g) + \pi_a^{-1}(\phi(g))$. It is straightforward to show that a is a generator of an HFP$(2t, 4_{\mathbf{1}})$-code.

Reciprocally, if we know a generator a of an HFP$(2t, 4_{\mathbf{1}})$-code, then we can obtain the first row g of a circulant complex Hadamard matrix. Set $\phi(g) = (\phi(g_1)_1, \ldots, \phi(g_{2t})_1, \phi(g_1)_2, \ldots, \phi(g_{2t})_2)$. There are 4 possibilities for the pair $(\phi(g_1)_1, \phi(g_1)_2)$, that is, there are 4 possibilities for the first coordinate of g, $g_1 \in \{1, i, -1, -i\}$. Thus, without loss of generality, we can assume $\phi(g_1)_1 = \phi(g_1)_2 = 0$. This assumption will make that the first coordinate of g will be $g_1 = 1$. Let $a = (a_1, a_2, \ldots, a_{4t})$. From $a = \phi(g) + \pi_a^{-1}(\phi(g))$, we have

$$\phi(g) = \left(0, a_1, a_1 + a_2, \ldots, \sum_{j=1}^{2t-1} a_j, 0, a_{2t+1}, a_{2t+1} + a_{2t+2}, \ldots, \sum_{j=2t+1}^{4t-1} a_j\right).$$

Rearrange $\phi(g) = ((\phi(g_1)_1, \phi(g_1)_2), \ldots, (\phi(g_{2t})_1, \phi(g_{2t})_2)$ and apply ϕ^{-1} to obtain g.

In [5, Example 1.1], for order $4t = 32$, the first row of a circulant complex Hadamard matrix is $(1, 1, i, -i, i, 1, 1, i, -1, 1, -i, -i, -i, 1, -1, i)$, which corresponds to the generator $a = (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$ of an HFP$(2t, 4_{\mathbf{1}})$-code with $r = 11$ and $k = 2$. We have

found another HFP$(2t, 4_{\mathbf{1}})$-code of length $4t = 32$ with $r = 13$ and $k = 1$ whose generator a is $(0,0,0,0,0,0,0,1,0,0,1,0,1,0,1,1,1,1,0,0,0,1,1,1,1,1,1,0,1,1,0,1,0)$ which corresponds to the first row of a circulant complex Hadamard matrix equal to $(1, i, i, i, 1, i, -i, -1, -i, i, i, -i, -1, i, -i)$. Now we state a conjecture about HFP-codes that is equivalent to the conjecture presented by Arasu et al. [5] about circulant complex Hadamard matrices.

Conjecture 3.25. *There do not exist* HFP$(2t, 4_{\mathbf{1}})$*-codes of length* $4t$ *for* $t > 8$.

3.1.4 HFP$(t, Q_{\mathbf{1}})$-codes

In this subsection we assume that $C = \langle d, a, b \mid d^t = a^4 = b^4 = \mathbf{0}, a^2 = b^2 = \mathbf{1}, aba = b\rangle$ and the value of t is odd. These codes are equivalent to cocyclic Hadamard matrices for which the Sylow 2-subgroup of the indexing group is Q, which have been considered by several authors. Baliga and Horadam [13] proved that the Williamson Hadamard matrix of order $4t$ is a cocyclic Hadamard matrix over $C_{2t} \times C_2$ with t odd. Álvarez, Gudiel and Güemes [4] established some bounds on the number and distribution of 2-coboundaries over $C_t \times C_2^2$ in order to obtain a $C_t \times C_2^2$-cocyclic Hadamard matrix. Also, they completed the computational results obtained by Baliga and Horadam. Barrera and Dietrich [14] proved that there is a 1-1 correspondence between the perfect sequences of length t over $Q \cap qQ$, with $q = (1 + i + j + k)/2$, and the $(4t, 2, 4t, 2t)$-relative difference sets in $C_t \times Q$ relative to C_2. They showed that if $t = p^a + 1$ for a prime p and integer $a \geq 0$ with $t \equiv 2 \bmod 4$, then there exists a $(4t, 2, 4t, 2t)$-relative difference set in $C_t \times Q$ with forbidden subgroup C_2. Suárez also studied HFP-codes with group structure $C_t \times Q$ in his PhD thesis [75].

Proposition 3.26. *Let* C *be an* HFP$(t, Q_{\mathbf{1}})$*-code. Then, up to equivalence, we have:*

(i) $\pi_d = (1, 5, \ldots, 4t-3)(2, 6, \ldots, 4t-2)(3, 7, \ldots, 4t-1)(4, 8, \ldots, 4t)$.

(ii) $\pi_a = (1, 2)(3, 4)\ldots(4t-1, 4t)$.

(iii) $\pi_b = (1, 3)(2, 4)\ldots(4t-3, 4t-1)(4t-2, 4t)$.

(iv) $a = (A_1, A_2, \ldots, A_t)$ *where*

$$A_i \in \{(0,1,0,1), (1,0,1,0), (0,1,1,0), (1,0,0,1)\}.$$

(v) Knowing the value of d is enough to define a.

(vi) Knowing the value of a is enough to define b.

(vii) $\Pi = C_{2t} \times C_2$.

Proof. (i), (ii) and *(iii)* are analogous to the proof of Proposition 3.4.

(iv) Let $a = (a_1, \ldots, a_{4t}) = (A_1, \ldots, A_t)$, where

$$A_i = (a_{4i-3}, a_{4i-2}, a_{4i-1}, a_{4i}) \quad \text{with } i \in \{1, \ldots, t\}.$$

Since $a^2 = a + \pi_a(a) = \mathbf{1}$, we have

$$A_i = (a_{4i-3}, \bar{a}_{4i-3}, a_{4i-1}, \bar{a}_{4i-1}).$$

(v) Since $ad = da$, we have $a = \pi_d(a) + d + \pi_a(d) = \pi_d(a) + \widehat{d}$, where $\widehat{d} = d + \pi_a(d)$. Thus, $a_{4i-3} = a_{4t-3} + \sum_{j=1}^{i} \widehat{d}_{4j-3}$, and $a_{4i-1} = a_{4t-1} + \sum_{j=1}^{i} \widehat{d}_{4j-1}$, for any $i \in \{1, \ldots, t\}$. Since $a^2 = \mathbf{1}$, we have $a_{4i-3} = \bar{a}_{4i-2}$ and $a_{4i-1} = \bar{a}_{4i}$.

(vi) From $aba = b$, $a + \pi_a(b) = b + \pi_b(a^{-1}) = b + \pi_b(a^3) = b + \pi_b(\bar{a})$. Thus, $a + \pi_b(\bar{a}) = b + \pi_a(b)$. Note that $a + \pi_b(\bar{a}) = (\widehat{A}_1, \ldots, \widehat{A}_t)$ where $\widehat{A}_i = (1,1,1,1)$ or $(0,0,0,0)$. Hence,

$$\widehat{A}_i = \begin{cases} (1,1,1,1) \text{ if } A_i \in \{(0,1,0,1), (1,0,1,0)\} \\ (0,0,0,0) \text{ if } A_i \in \{(0,1,1,0), (1,0,0,1)\} \end{cases}.$$

Let $b = (b_1, \ldots, b_{4t}) = (B_1, \ldots, B_t)$ where $B_i = (b_{4i-3}, b_{4i-2}, b_{4i-1}, b_{4i})$. Since $b^2 = \mathbf{1}$, we have $B_i = (b_{4i-3}, b_{4i-2}, \bar{b}_{4i-3}, \bar{b}_{4i-2})$. Thus,

$$B_i \in \begin{matrix} \{(0,1,1,0), (1,0,0,1)\} \text{ if } A_i \in \{(0,1,0,1), (1,0,1,0)\} \\ \{(0,0,1,1), (1,1,0,0)\} \text{ if } A_i \in \{(0,1,1,0), (1,0,0,1)\} \end{matrix}.$$

(vii) It follows from Proposition 2.19 and since t is odd. $\mathcal{QED}$

Proposition 3.27. *Let C be an $\mathrm{HFP}(t, Q_{\mathbf{1}})$-code, where t is odd. Then $r = 4t - 1$ and $k = 1$.*

Proof. It follows from Proposition 3.3 and since t is odd. $\mathcal{QED}$

3.1.5 Magma computations

In Table 3.1, we show the values of the rank and the dimension of the kernel of the HFP codes that we have computed with Magma [18], fulfilling the analytic results, for length $4t$. Ó Catháin and Röder [58] built the cocyclic Hadamard matrices for $t \leq 9$ that correspond to many of the HFP-codes in Table 3.1, but we have computed the rank and the dimension of the kernel.

t	$(4t_{\mathbf{1}}, 2)$		$(2t, 2, 2_{\mathbf{1}})$		$(2t, 4_{\mathbf{1}})$		$(t, Q_{\mathbf{1}})$	
	r	k	r	k	r	k	r	k
1	3	3	3	3	3	3	x	x
2	4	4	✓	✓	4	4	-	-
3	✓	✓	✓	✓	✓	✓	11	1
4	x	x	5	5	7	2	-	-
			6	3				
5	✓	✓	✓	✓	✓	✓	19	1
6	x	x	✓	✓	x	x	-	-
7	✓	✓	✓	✓	✓	✓	27	1
8	x	x	✓	✓	11	2	-	-
					13	1		
9	✓	✓	✓	✓	✓	✓	35	1
10	x	x	✓	✓	x	x	-	-

Table 3.1: Rank and dimension of the kernel of Hadamard full propelinear codes with associated group $C_{2t} \times C_2$. Symbol x means that the non-existence was checked with Magma by exhaustive search, symbol ✓means that the non-existence was proved analytically, and "-" means that the code does not have $C_{2t} \times C_2$ as associated group. When the values for the rank and the dimension of the kernel appears in a box it means that they are the only values for that box.

Remark 3.28. *In this section, all values for the dimension of the kernel are less than or equal to* 3 *when the code is nonlinear. Note that if* $k = 3$*, then* $r \leq t + 2$ *by Lemma 2.2.*

Now we present some examples of the Hadamard full propelinear codes introduced in this section.

Example 3.29. *Let a and b be the following vectors of $\mathbb{F}^{16}$*

$$a = (0,1,1,0,1,0,0,1,1,1,1,1,0,0,0,0),$$
$$b = (1,1,1,0,1,1,1,0,0,0,0,1,0,0,0,1)$$

with associated permutations

$$\pi_a = (1,2,3,4,5,6,7,8)(9,10,11,12,13,14,15,16),$$
$$\pi_b = (1,9)(2,10)(3,11)(4,12)(5,13)(6,14)(7,15)(8,16).$$

Computing the powers of a, b, ab, we obtain $a^8 = \mathbf{0}$, $b^2 = \mathbf{1}$ and $ab = ba$. Thus, the code $C = \{a, a^2, \ldots, a^8, ab, a^2b, \ldots, a^8b, ab^2, a^2, b^2, \ldots, a^8b^2,\ ab^3, a^2b^3, \ldots, a^8b^3\}$ is an $\mathrm{HFP}(8, 4_{\mathbf{1}})$-code of length 16, which is an $\mathrm{HFP}(2t, 4_{\mathbf{1}})$-code with $t = 4$. Computing with MAGMA *the rank and the dimension of the kernel of C we obtain $r = 7$ and $k = 2$. Moreover, $\mathcal{K}(C) = \langle \mathbf{1}, a^4 \rangle$. The Hadamard matrix of order 16 associated to C is*

$$\begin{pmatrix} a \\ a^2 \\ a^3 \\ a^4 \\ a^5 \\ a^6 \\ a^7 \\ a^8 \\ ab \\ a^2b \\ a^3b \\ a^4b \\ a^5b \\ a^6b \\ a^7b \\ a^8b \end{pmatrix} = \begin{pmatrix} 0&1&1&0&1&0&0&1&1&1&1&1&0&0&0&0 \\ 1&1&0&1&1&1&0&1&1&0&0&0&1&0&0&0 \\ 1&0&0&0&0&1&1&1&1&0&1&1&0&1&0&0 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0 \\ 0&0&1&1&1&1&0&0&1&0&1&0&0&1&0&1 \\ 0&1&1&1&0&1&1&1&0&0&1&0&0&0&1&0 \\ 1&1&0&1&0&0&1&0&1&1&1&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&1&1&1&0&0&1&1&1&1&0&0&0 \\ 0&1&1&0&0&1&1&0&1&1&0&0&1&1&0&0 \\ 0&1&0&1&1&0&1&0&1&0&0&1&0&1&1&0 \\ 0&1&0&0&0&1&0&0&1&0&1&1&1&0&1&1 \\ 0&1&0&0&1&0&1&1&0&0&1&0&1&1&0&1 \\ 1&1&0&0&1&1&0&0&0&1&1&0&0&1&1&0 \\ 0&0&0&0&1&1&1&1&1&1&0&0&0&0&1&1 \\ 1&1&1&0&1&1&1&0&0&0&0&1&0&0&0&1 \end{pmatrix}.$$

Example 3.30. *Let a and b be the following vectors of $\mathbb{F}^{16}$*

$$a = (1,1,1,1,0,1,0,1,1,0,1,0,0,0,0,0),$$
$$b = (0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0)$$

with associated permutations

$$\pi_a = (1,2,3,4,5,6,7,8)(9,10,11,12,13,14,15,16),$$
$$\pi_b = (1,9)(2,10)(3,11)(4,12)(5,13)(6,14)(7,15)(8,16).$$

Computing the powers of a, b, ab, we obtain $a^8 = b^2 = \mathbf{0}$ and $ab = ba$. Thus, the code $C = \{a, a^2, \ldots, a^8, ab, a^2b, \ldots, a^8b, a\mathbf{1}, a^2\mathbf{1}, \ldots, a^8\mathbf{1}, ab\mathbf{1}, a^2b\mathbf{1}, \ldots, a^8b\mathbf{1}\}$ is an $\mathrm{HFP}(8, 2, 2_{\mathbf{1}})$-code of length 16, which is an $\mathrm{HFP}(2t, 2, 2_{\mathbf{1}})$-code with $t = 4$. Computing with MAGMA *the rank and the dimension of the kernel of C we obtain $r = 6$ and $k = 3$. Moreover, $\mathcal{K}(C) = \langle \mathbf{1}, a^4, b \rangle$. The Hadamard matrix of order 16 associated to C is*

$$\begin{pmatrix} a \\ a^2 \\ a^3 \\ a^4 \\ a^5 \\ a^6 \\ a^7 \\ a^8 \\ ab \\ a^2b \\ a^3b \\ a^4b \\ a^5b \\ a^6b \\ a^7b \\ a^8b \end{pmatrix} = \begin{pmatrix} 1&1&1&1&0&1&0&1&1&0&1&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0 \\ 0&1&1&1&0&0&1&0&1&1&0&1&1&0&0&0 \\ 1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0 \\ 1&0&0&1&0&0&1&1&1&1&0&0&0&1&1&0 \\ 0&0&1&1&1&1&0&0&1&1&0&0&0&0&1&1 \\ 1&1&1&0&1&0&1&1&0&1&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&1&0&0&0&1&1&0&1&0&0&1&0&0&1&1 \\ 1&0&0&1&0&1&1&0&0&1&1&0&1&0&0&1 \\ 1&0&1&1&1&1&1&0&0&0&0&1&0&1&0&0 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0 \\ 1&0&1&0&0&0&0&0&1&1&1&1&0&1&0&1 \\ 1&0&1&0&0&1&0&1&0&1&0&1&1&0&1&0 \\ 0&0&1&0&0&1&1&1&1&0&0&0&1&1&0&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0 \end{pmatrix}.$$

Example 3.31. *Let d, a, and b be the following vectors of $\mathbb{F}^{12}$*

$$\begin{aligned} d &= (1,1,1,0,1,1,1,0,0,0,0,0),\\ a &= (0,1,1,0,0,1,0,1,0,1,0,1),\\ b &= (0,0,1,1,0,1,1,0,0,1,1,0) \end{aligned}$$

with associated permutations

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

Computing the powers of d, a, b and their products, we obtain $d^3 = a^4 = b^4 = \mathbf{0}$, $a^2 = b^2 = \mathbf{1}$, $da = ad$, $db = bd$, and $aba = b$. Therefore, the code $C = \{d, d^2, d^3, da, d^2a, d^3a, db, d^2b, d^3b, dab, d^2ab, d^3ab, d\mathbf{1}, d^2\mathbf{1}, d^3\mathbf{1}, da\mathbf{1}, d^2a\mathbf{1}, d^3a\mathbf{1}, db\mathbf{1}, d^2b\mathbf{1}, d^3b\mathbf{1}, dab\mathbf{1}, d^2ab\mathbf{1}, d^3ab\mathbf{1}\}$ is an $\mathrm{HFP}(3, Q_{\mathbf{1}})$-code of length 12, which is an $\mathrm{HFP}(t, Q_{\mathbf{1}})$-code with $t = 3$. Computing with MAGMA *the rank and the dimension of the kernel of C we obtain $r = 11$ and $k = 1$. Moreover, $\mathcal{K}(C) = \langle \mathbf{1} \rangle$. The Hadamard matrix of order 12 associated to C is*

$$\begin{pmatrix} d \\ d^2 \\ d^3 \\ da \\ d^2a \\ d^3a \\ db \\ d^2b \\ d^3b \\ dab \\ d^2ab \\ d^3ab \end{pmatrix} = \begin{pmatrix} 1&1&1&0&1&1&1&0&0&0&0&0\\ 1&1&1&0&0&0&0&0&1&1&1&0\\ 0&0&0&0&0&0&0&0&0&0&0&0\\ 1&0&1&1&1&0&0&0&0&1&0&1\\ 1&0&1&1&0&1&0&1&1&0&0&0\\ 0&1&1&0&0&1&0&1&0&1&0&1\\ 1&0&0&0&1&1&0&1&0&1&1&0\\ 1&0&0&0&0&1&1&0&1&1&0&1\\ 0&0&1&1&0&1&1&0&0&1&1&0\\ 0&0&1&0&1&0&1&1&1&1&0&0\\ 0&0&1&0&1&1&0&0&1&0&1&1\\ 0&1&0&1&1&1&0&0&1&1&0&0 \end{pmatrix}$$

3.2 Associated group $C_t \times C_2 \times C_2$

Now we introduce a subclass of Hadamard full propelinear codes whose group structure consists of direct product of groups, fulfilling that its associated group Π is $C_t \times C_2 \times C_2$. In other words, we study the short exact sequence

$$1 \to C_2 \to C \to C_t \times C_2 \times C_2 \to 1,$$

where C is a nontrivial direct product of groups.

Proposition 3.32. *Let C be a Hadamard full propelinear code of length $4t$ with associated group $C_t \times C_2^2$. If C as a group is a nontrivial direct product, then C is some of the following HFP-codes:*

(i) $\mathrm{HFP}(t, 2, 2, 2_{\mathbf{1}}) = C_t \times C_2 \times C_2 \times C_2 = \langle a, b, c, \mathbf{1} \mid a^t = b^2 = c^2 = \mathbf{0} \rangle$.

(ii) $\mathrm{HFP}(t, 4_{\mathbf{1}}, 2) = C_t \times C_4 \times C_2 = \langle a, b, c \mid a^t = b^4 = c^2 = \mathbf{0}, b^2 = \mathbf{1} \rangle$.

(iii) $\mathrm{HFP}(t, Q_{\mathbf{1}}) = C_t \times Q = \langle d, a, b \mid d^t = \mathbf{0}, a^2 = b^2 = \mathbf{1}, aba = b \rangle$, *where Q is the quaternion group of eight elements.*

(iv) $\mathrm{HFP}(t, D_{\mathbf{1}}) = C_t \times D = \langle d, a, b \mid d^t = b^2 = \mathbf{0}, a^2 = \mathbf{1}, aba = b \rangle$, *where D is the dihedral group of eight elements.*

(v) $\mathrm{HFP}(2t_{\mathbf{1}}, 2, 2) = C_{2t} \times C_2 \times C_2 = \langle a, b, c \mid b^2 = c^2 = \mathbf{0}, a^t = \mathbf{1} \rangle$.

Proof. Note that there are two different cases depending on the parity of the value of t. Firstly, we suppose that t is odd, so $C_t \times C_2^2 \simeq C_{2t} \times C_2$. The HFP-codes with associated group $\Pi = C_{2t} \times C_2$ have been studied in Section 3.1. When t is odd, we have proved that the unique HFP-code whose group structure is isomorphic to a direct product that has associated $C_{2t} \times C_2$ is the $\mathrm{HFP}(t, Q_{\mathbf{1}})$-code.

Now, we suppose t is even. From [37, Table 1], the central extensions of $C_2 \times C_2$ by $\langle \mathbf{1} \rangle \simeq C_2$ are C_2^3, $C_4 \times C_2$, Q and D. Let E be one of this extensions. We have that $C_2 \trianglelefteq E$, so $C_2 \trianglelefteq E \times C_t$ and $(E \times C_t)/C_2 \simeq (E/C_2) \times C_t \simeq C_t \times C_2^2$. Therefore $C_t \times C_2^3$, $C_t \times C_4 \times C_2$, $C_t \times Q$ and $C_t \times D$ are extensions of $C_t \times C_2^2$ by C_2. Now, depending on where is the vector $\mathbf{1}$ we have different possibilities for the HFP-codes. For $C_t \times C_4 \times C_2$, the vector $\mathbf{1}$ can only be the element

of order 2 of C_4 because the quotient $(C_t \times C_4 \times C_2)/\langle \mathbf{1} \rangle$ must be $C_t \times C_2^2$ by Proposition 2.19. Thus we obtain the $\mathrm{HFP}(t, 4_{\mathbf{1}}, 2)$-code. For $C_t \times Q$ and $C_t \times D$, the vector $\mathbf{1}$ is the center of Q and D, respectively, and so we obtain the $\mathrm{HFP}(t, Q_{\mathbf{1}})$-code and the $\mathrm{HFP}(t, D_{\mathbf{1}})$-code. For $C_t \times C_2^3$, the vector $\mathbf{1}$ can be a generator of a cyclic group of order 2, obtaining the $\mathrm{HFP}(t, 2, 2, 2_{\mathbf{1}})$-code, or an element of C_t. If $\mathbf{1} \in C_t$, then $C_t/\langle \mathbf{1} \rangle = C_{t/2}$, thus $t/2$ must be odd (i.e., t is not a multiple of 4) to get $\Pi = C_t \times C_2^2$. But this is a particular case of the $\mathrm{HFP}(t, 2, 2, 2_{\mathbf{1}})$-code when $t = 2t'$ where t' is odd.

Note that we also can compute the central extensions, E_t, of C_t by $\langle \mathbf{1} \rangle \simeq C_2$, and later we can obtain the extensions of $C_t \times C_2^2$ making the product $E_t \times C_2^2$. Let E_t be an extension of C_t by C_2, then $C_2 \trianglelefteq C_t$ and $E_t/C_2 \simeq C_t$. E_t cannot be non-abelian because the quotient by a central subgroup is cyclic. As t is even, we have $E_t = C_t \times C_2$ or C_{2t}. If $E_t = C_t \times C_2$, the extension of $C_t \times C_2^2$ by C_2 is $C_t \times C_2^3$, obtaining the $\mathrm{HFP}(t, 2, 2, 2_{\mathbf{1}})$-code. If $E_t = C_{2t}$, the extension of $C_t \times C_2^2$ by C_2 is $C_{2t} \times C_2^2$, with $\mathbf{1} \in C_{2t}$, obtaining the $\mathrm{HFP}(2t_{\mathbf{1}}, 2, 2)$-code.

Note that there exist no more possibilities for central extensions. If we compute the extensions of C_2 by C_2, denoted by E_2, we obtain $E_2 = C_4$ or $C_2 \times C_2$, so the extensions of $C_t \times C_2^2$ are $E_2 \times C_t \times C_2$, which are contained in the set of extensions obtained by making the extensions of $C_2 \times C_2$. Similarly, if we compute the extensions of $C_t \times C_2$, we obtain extensions contained in the set of extensions obtained by making the extensions of C_t. $\mathcal{QED}$

Corollary 3.33. *Let C be an $\mathrm{HFP}(t, Q_{\mathbf{1}})$-code. If t is odd, then C is the unique Hadamard full propelinear code whose group structure consists of direct product of groups that has $\Pi = C_t \times C_2^2$ as associated group.*

Proof. It is proved in the first part of the previous proof. $\mathcal{QED}$

Proposition 3.34. *Let C be a nonlinear Hadamard full propelinear code of length $4t$ with associated group $C_t \times C_2^2$. Then:*

(i) If t is odd, then $r = 4t - 1$ and $k = 1$.

(ii) If t is even, then $r \leq 2t$, and $r = 2t$ if $t \equiv 2 \bmod 4$.

Proof. (i) and *(ii)* follow from Lemma 2.26 and [67, Lemma 4]. $\mathcal{QED}$

Proposition 3.35. *Let* $C = \langle a, b, \mathbf{1}\rangle$ *be a code of type* $\mathrm{HFP}(t, 2, 2, 2_{\mathbf{1}})$ *or* $\mathrm{HFP}(t, 4_{\mathbf{1}}, 2)$ *or* $\mathrm{HFP}(2t_{\mathbf{1}}, 2, 2)$*. Then, up to equivalence, we have*

(i) $\pi_a = (1, 2, \ldots, t)(t+1, \ldots, 2t)(2t+1, \ldots, 3t)(3t+1, \ldots, 4t)$,

(ii) $\pi_b = (1, 2t+1)(2, 2t+2)\ldots(2t, 4t)$,

(iii) $\pi_c = (1, 3t+1)(2, 3t+2)\ldots(t, 4t)(t+1, 2t+1)\ldots(2t, 3t)$,

(iv) Knowing the value of a *is enough to define* b *and* c,

(v) $\Pi = C_t \times C_2^2$.

Proof. In any case $a^t \in \{\mathbf{0}, \mathbf{1}\}$, so $\pi_{a^t} = \pi_{\mathbf{0}} = \pi_{\mathbf{1}} = Id$ and π_a has order t. Thus, π_a is the product of four cycles of length t. Indeed, if we have a cycle of length $j < t$ then $\pi_a^j = \pi_{a^j}$ has a fixed point, which contradicts that C is full propelinear. Without loss of generality, we can set $\pi_a = (1, 2, \ldots, t)(t+1, t+2, \ldots, 2t)(2t+1, 2t+2, \ldots, 3t)(3t+1, 3t+2, \ldots, 4t)$, which shows *(i)*.

As π_b and π_c have order 2, they are products of transpositions. The permutation π_a divides the set of coordinates $\{1, 2, \ldots, 4t\}$ in 4 blocks of t coordinates. Each one of the transpositions sends an element of one block to another block. Indeed, assume $\pi_b(1) = i$ for some $i \in \{1, \ldots, t\}$. We also have $\pi_{a^{i-1}}(1) = i$, so $\pi_{b^{-1}}\pi_{a^{i-1}}$ has a fixed point, which contradicts that C is full propelinear. The same argument is valid for π_c. Thus, π_b and π_c move coordinates from a block to another different block. Furthermore, if we assume that $\pi_b(1) = i$ with $i \in \{2t+1, \ldots, 3t\}$, i.e., i is in the third block, then π_b is uniquely determined. Indeed, as $\pi_a\pi_b = \pi_b\pi_a$, we have $\pi_{a^{-1}}(2) = 1$, $\pi_b(1) = i$, and $\pi_a(i) = i+1$. Hence, $\pi_b(2) = i+1$, and so on. Therefore, we can assume $\pi_b = (1, 2t+1)(2, 2t+2)\ldots(2t, 4t)$, which shows *(ii)*.

If we assume that $\pi_c(1) = i$ with $i \in \{3t+1, \ldots, 4t\}$, i.e., i is in the fourth block, then π_c is uniquely determined. Indeed, as $\pi_a\pi_c = \pi_c\pi_a$, we have $\pi_{a^{-1}}(2) = 1$, $\pi_c(1) = i$, and $\pi_a(i) = i+1$. Hence, $\pi_c(2) = i+1$, and so on. Therefore, we can assume $\pi_c = (1, 3t+1)(2, 3t+2)\ldots(t, 4t)(t+1, 2t+1)(t+2, 2t+2)\ldots(2t, 3t)$, which shows *(iii)*.

Since $ab = ba$, we have $b = \pi_a(b) + a + \pi_b(a) = \pi_a(b) + \widehat{a}$, where $\widehat{a} = a + \pi_b(a) = (\widehat{a}_1, \ldots, \widehat{a}_{2t}, \widehat{a}_1, \ldots, \widehat{a}_{2t})$. Then $b_i = b_t + \sum_{j=i+1}^{t} \widehat{a}_j$, $b_t \in \{0, 1\}$, $b_{t+i} = b_{2t} + \sum_{j=t+i+1}^{2t} \widehat{a}_j$, and $b_{2t} \in \{0, 1\}$ for $i \in \{1, \ldots, t-1\}$. If $b^2 = \mathbf{0}$, then

$b = \pi_b(b)$, and $b_i = b_{2t+i}$ for $i \in \{1, \ldots, 2t\}$. Thus

$$\begin{aligned} b = \Bigg(& b_t + \sum_{j=2}^{t} \widehat{a}_j, b_t + \sum_{j=3}^{t} \widehat{a}_j, \ldots, b_t + \widehat{a}_t, b_t, \\ & b_{2t} + \sum_{j=t+2}^{2t} \widehat{a}_j, b_{2t} + \sum_{j=t+3}^{2t} \widehat{a}_j, \ldots, b_{2t} + \widehat{a}_{2t}, b_{2t}, \\ & b_t + \sum_{j=2}^{t} \widehat{a}_j, b_t + \sum_{j=3}^{t} \widehat{a}_j, \ldots, b_t + \widehat{a}_t, b_t, \\ & b_{2t} + \sum_{j=t+2}^{2t} \widehat{a}_j, b_{2t} + \sum_{j=t+3}^{2t} \widehat{a}_j, \ldots, b_{2t} + \widehat{a}_{2t}, b_{2t} \Bigg). \end{aligned}$$

If $b^2 = \mathbf{1}$, then $b = \pi_b(b) + \mathbf{1}$, and $b_i = b_{2t+i} + 1$ for $i \in \{1, \ldots, 2t\}$. Thus

$$\begin{aligned} b = \Bigg(& b_t + \sum_{j=2}^{t} \widehat{a}_j, b_t + \sum_{j=3}^{t} \widehat{a}_j, \ldots, b_t + \widehat{a}_t, b_t, \\ & b_{2t} + \sum_{j=t+2}^{2t} \widehat{a}_j, b_{2t} + \sum_{j=t+3}^{2t} \widehat{a}_j, \ldots, b_{2t} + \widehat{a}_{2t}, b_{2t}, \\ & 1 + b_t + \sum_{j=2}^{t} \widehat{a}_j, 1 + b_t + \sum_{j=3}^{t} \widehat{a}_j, \ldots, 1 + b_t + \widehat{a}_t, 1 + b_t, \\ & 1 + b_{2t} + \sum_{j=t+2}^{2t} \widehat{a}_j, 1 + b_{2t} + \sum_{j=t+3}^{2t} \widehat{a}_j, \ldots, 1 + b_{2t} + \widehat{a}_{2t}, 1 + b_{2t} \Bigg). \end{aligned}$$

Since $ac = ca$, we have $c = \pi_a(c) + a + \pi_c(a) = \pi_a(c) + \widehat{a}$, where $\widehat{a} = a + \pi_c(a) = (\widehat{a}_1, \ldots, \widehat{a}_t, \widehat{a}_{t+1}, \ldots, \widehat{a}_{2t}, \widehat{a}_{t+1}, \ldots, \widehat{a}_{2t}, \widehat{a}_1, \ldots, \widehat{a}_t)$, then $c_i = c_t + \sum_{j=i+1}^{t} \widehat{a}_j$, $c_t \in \{0, 1\}$, $c_{t+i} = c_{2t} + \sum_{j=t+i+1}^{2t} \widehat{a}_j$, and $c_{2t} \in \{0, 1\}$ for $i \in \{1, \ldots, t-1\}$. As $c^2 = \mathbf{0}$, we have $c_i = c_{3t+i}$ and $c_{t+i} = c_{2t+i}$ for $i \in \{1, \ldots, t\}$. Thus

$$\begin{aligned} c = \Bigg(& c_t + \sum_{j=2}^{t} \widehat{a}_j, c_t + \sum_{j=3}^{t} \widehat{a}_j, \ldots, c_t + \widehat{a}_t, c_t, \\ & c_{2t} + \sum_{j=t+2}^{2t} \widehat{a}_j, c_{2t} + \sum_{j=t+3}^{2t} \widehat{a}_j, \ldots, c_{2t} + \widehat{a}_{2t}, c_{2t}, \\ & c_{2t} + \sum_{j=t+2}^{2t} \widehat{a}_j, c_{2t} + \sum_{j=t+3}^{2t} \widehat{a}_j, \ldots, c_{2t} + \widehat{a}_{2t}, c_{2t}, \\ & c_t + \sum_{j=2}^{t} \widehat{a}_j, c_t + \sum_{j=3}^{t} \widehat{a}_j, \ldots, c_t + \widehat{a}_t, c_t \Bigg). \end{aligned}$$

(v) follows from Proposition 2.19. $\mathcal{QED}$

From a computational point of view, *(iv)* saves us computing time. As knowing the value of the generator a, we know the value of b and c. Therefore, by brute-force search, we only need to check different values of a.

In Subsections 3.2.1–3.2.3 we will use the permutations associated to the generators as in Proposition 3.35.

3.2.1 HFP$(t, 2, 2, 2_{\mathbf{1}})$-codes

In this subsection we assume that $C = \langle a, b, c, \mathbf{1} \mid a^t = b^2 = c^2 = \mathbf{0} \rangle$, with t even.

Proposition 3.36. *Let C be an* HFP$(t, 2, 2, 2_{\mathbf{1}})$*-code. Then t is a square number.*

Proof. We have $C \simeq C_t \times C_2^2 \times \langle \mathbf{1} \rangle = N \times \langle \mathbf{1} \rangle$, where $N = C_t \times C_2^2$. From Lemma 2.36, $|C_t \times C_2^2|$ is a square. Thus t is a square number. $\mathcal{QED}$

Proposition 3.37. *Let C be an* HFP$(t, 2, 2, 2_{\mathbf{1}})$*-code of length $4t$. If t is a power of two, then $t \in \{1, 4, 8, 16\}$.*

Proof. As $C = C_t \times C_2 \times C_2 \times \langle \mathbf{1} \rangle$, we have a Hadamard difference set in $C_t \times C_2 \times C_2$ by Proposition 2.29. From Proposition 3.36, t is also a square, so $t = 2^{2s}$ for some s. Thus, the order and the exponent of $C_{2t} \times C_2$ are 2^{2s+2} and 2^{2s}, respectively. From Proposition 2.28, it derives that $s \leq 2$. $\mathcal{QED}$

3.2.2 HFP$(t, 4_{\mathbf{1}}, 2)$-codes

In this subsection we assume that $C = \langle a, b, c \mid a^t = b^4 = c^2 = \mathbf{0}, b^2 = \mathbf{1} \rangle$, with t even.

Next lemma about Hadamard groups will be useful to build HFP$(2t, 4_{\mathbf{1}}, 2)$-codes from HFP$(2t, 4_{\mathbf{1}})$-codes.

Lemma 3.38 ([23, Corollary 2.2])**.** *Suppose that G is a Hadamard group with respect to u. If G contains an element x with $x^2 = u$ then $G \times C_2$ is Hadamard.*

Note that an HFP$(2t, 4_{\mathbf{1}})$-code has a Hadamard group structure $C_{2t} \times C_4 = \langle a, b \rangle$ respect to $\mathbf{1}$, and $b^2 = \mathbf{1}$. Then $C_{2t} \times C_4 \times C_2$ is an HFP$(2t, 4_{\mathbf{1}}, 2)$-code by Lemma 3.38. We explicit the construction in the following proposition.

Proposition 3.39. *Let $C = \langle a, b\rangle$ be an $\mathrm{HFP}(2t, 4_{\mathbf{1}})$-code of length $4t$ with rank r and dimension of the kernel k. Then there exists an $\mathrm{HFP}(2t, 4_{\mathbf{1}}, 2)$-code of length $8t$ with rank $r+1$ and dimension of the kernel $k+1$.*

Proof. Let $\hat{C}$ be the $\mathrm{HFP}(2t, 4_{\mathbf{1}}, 2)$-code generated by $\langle \hat{a}, \hat{b}, \hat{c}\rangle$, where $\hat{a} = (a, a)$. We know that $\hat{a}\hat{b} = \hat{b}\hat{a}$. Since $\hat{a} = (a, a)$, we have $\hat{b} = \pi_{\hat{a}}(\hat{b})$. Without loss of generality, $\hat{b} = (\mathbf{0}, \mathbf{1})$. Since $\pi_{\hat{b}\hat{c}} = (\pi_b, \pi_b)$ and b derives from a, then $\hat{b}\hat{c} = (b, b)$. As $\hat{c} = \hat{b} + \pi_{\hat{b}}(\hat{b}\hat{c}) + \mathbf{1}$, we have $\hat{c} = (\overline{b}, b)$. Note that $b^2 = \mathbf{1}$ so $\hat{c}$ have order 2.

Let H be the Hadamard matrix associated to the code C. It is clear that

$$\hat{H} = \begin{pmatrix} H & H \\ H & \overline{H} \end{pmatrix}$$

is the associated matrix to the code $\hat{C}$. Note that

$$H = \begin{pmatrix} a \\ a^2 \\ \vdots \\ a^{2t} \\ ab \\ a^2 b \\ \vdots \\ a^{2t} b \end{pmatrix}, \hat{H} = \begin{pmatrix} \hat{a} \\ \vdots \\ \hat{a}^{2t} \\ \hat{a}\hat{b} \\ \vdots \\ \hat{a}^{2t}\hat{b} \\ \hat{a}\hat{c} \\ \vdots \\ \hat{a}^{2t}\hat{c} \\ \hat{a}\hat{b}\hat{c} \\ \vdots \\ \hat{a}^{2t}\hat{b}\hat{c} \end{pmatrix} = \begin{pmatrix} a & a \\ \vdots & \vdots \\ a^{2t} & a^{2t} \\ a & \overline{a} \\ \vdots & \vdots \\ a^{2t} & \overline{a^{2t}} \\ ab & \overline{ab} \\ \vdots & \vdots \\ a^{2t} b & \overline{a^{2t} b} \\ ab & ab \\ \vdots & \vdots \\ a^{2t} b & a^{2t} b \end{pmatrix}.$$

As the matrix

$$\hat{H} = \begin{pmatrix} H & H \\ H & \overline{H} \end{pmatrix}$$

corresponds to Sylvester's construction, we have that the rank and the dimension of the kernel increase in one. $\mathcal{QED}$

Corollary 3.40. *There exist at least two nonequivalent $\mathrm{HFP}(16, 4_{\mathbf{1}}, 2)$-codes of length 64. The values for the rank and the dimension of the kernel are $r = 12$, $k = 3$, and $r = 14$, $k = 2$.*

Proof. From Table 3.1, there exist HFP$(16, 4_{\mathbf{1}})$-codes of length 32 with $r = 11$, $k = 2$, and $r = 13$, $k = 1$. The result follows from Proposition 3.39. $\mathcal{QED}$

Remark 3.41. *By brute force-search we cannot obtain the codes of Corollary 3.40. But we have checked with* Magma *that the construction in Proposition 3.39 works.*

The next lemma about Hadamard groups will be useful to build codes of type HFP$(2t, 4_{\mathbf{1}}, 2)$ from HFP$(2t, 2, 2_{\mathbf{1}})$-codes.

Lemma 3.42 ([23, Lemma 2.3])**.** *Suppose G and $H \times C_2$ are Hadamard with respect to involutions $u_1 \in G$ and u_2, respectively, where $C_2 = \langle u_2 \rangle$. Then $G \times H$ is Hadamard with respect u_1.*

Note that an HFP$(2t, 2, 2_{\mathbf{1}})$-code has a Hadamard group structure $C_{2t} \times C_2 \times C_2 = \langle a, b, \mathbf{1} \rangle$ respect to $\mathbf{1}$, and $C_2 = \langle \mathbf{1} \rangle$. As $G = C_4$ is an HFP-code, we have that $C_{2t} \times C_4 \times C_2$ is an HFP$(2t, 4_{\mathbf{1}}, 2)$-code by Lemma 3.42. We explicit the construction in the following proposition.

Proposition 3.43. *Let $C = \langle a, b \rangle$ be an* HFP$(2t, 2, 2_{\mathbf{1}})$*-code of length $4t$ with rank r and dimension of the kernel k. Then there exists an* HFP$(t, 4_{\mathbf{1}}, 2)$*-code of length $8t$ with rank $r + 1$ and dimension of the kernel $k + 1$.*

Proof. Let $\hat{C}$ be the HFP$(2t, 4_{\mathbf{1}}, 2)$-code generated by $\langle \hat{a}, \hat{b}, \hat{c} \rangle$, where $\hat{a} = (a, a)$. We know that $\hat{a}\hat{b} = \hat{b}\hat{a}$. Since $\hat{a} = (a, a)$, we have $\hat{b} = \pi_{\hat{a}}(\hat{b})$. Without loss of generality, $\hat{b} = (\mathbf{0}, \mathbf{1}, \mathbf{1}, \mathbf{0})$. Since $\pi_{\hat{b}\hat{c}} = (\pi_b, \pi_b)$ and b derives from a, then $\hat{b}\hat{c} = (b, b)$. As $\hat{c} = \hat{b} + \pi_{\hat{b}}(\hat{b}\hat{c}) + \mathbf{1}$, we have $\hat{c} = (\bar{\beta}, \beta, \beta, \bar{\beta})$, where $b = (\beta, \beta)$. Note that $b^2 = \mathbf{0}$ so $\hat{c}$ have order 2.

Let H be the Hadamard matrix associated to the code C. Rearranging the columns, we have that

$$\hat{H} = \begin{pmatrix} H & H \\ H & \overline{H} \end{pmatrix}$$

is the associated matrix to the code $\hat{C}$. Note that

$$H = \begin{pmatrix} a \\ a^2 \\ \vdots \\ a^{2t} \\ ab \\ a^2b \\ \vdots \\ a^{2t}b \end{pmatrix}, \hat{H} = \begin{pmatrix} \hat{a} \\ \vdots \\ \hat{a}^{2t} \\ \hat{a}\hat{b} \\ \vdots \\ \hat{a}^{2t}\hat{b} \\ \hat{a}\hat{c} \\ \vdots \\ \hat{a}^{2t}\hat{c} \\ \hat{a}\hat{b}\hat{c} \\ \vdots \\ \hat{a}^{2t}\hat{b}\hat{c} \end{pmatrix} = \begin{pmatrix} a & a \\ \vdots & \vdots \\ a^{2t} & a^{2t} \\ a & \overline{a} \\ \vdots & \vdots \\ a^{2t} & \overline{a^{2t}} \\ ab & \overline{ab} \\ \vdots & \vdots \\ a^{2t}b & \overline{a^{2t}b} \\ ab & ab \\ \vdots & \vdots \\ a^{2t}b & a^{2t}b \end{pmatrix}.$$

As the matrix

$$\hat{H} = \begin{pmatrix} H & H \\ H & \overline{H} \end{pmatrix}$$

corresponds to Sylvester's construction, we have that the rank and the dimension of the kernel increase in one. $\mathcal{QED}$

Attending to the computations with MAGMA, we present the following conjecture.

Conjecture 3.44. *There do not exist* $\mathrm{HFP}(t, 4_{\mathbf{1}}, 2)$*-codes of length* $4t$ *for* $t > 16$.

Remark 3.45. *The previous conjecture implies Conjecture 3.25, which implies that there is no circulant complex Hadamard matrix of order greater than* 16.

3.2.3 HFP$(2t_{\mathbf{1}}, 2, 2)$-codes

In this subsection we assume that $C = \langle a, b, c \mid b^2 = c^2 = \mathbf{0}, a^t = \mathbf{1} \rangle$, with t even.

Lemma 3.46. *Let* $C = \langle a, b, c \rangle$ *be an* $\mathrm{HFP}(2t_{\mathbf{1}}, 2, 2)$*-code of length* $4t = 8\tau$*. Let* h *be a divisor of* τ*. Then* $\pi_a^h(a^\tau) \neq a^\tau$.

Proof. Assume the contrary, so $\pi_a^h(a^\tau) = a^\tau$, where $\tau = hh'$. Hence, $\mathbf{1} = a^\tau + \pi_a^\tau(a^\tau) = a^\tau + (\pi_a^h)^{h'}(a^\tau) = a^\tau + a^\tau = \mathbf{0}$, which is impossible. $\mathcal{QED}$

Proposition 3.47. *Let $C = \langle a, b, c\rangle$ be a nonlinear* HFP$(2t_{\mathbf{1}}, 2, 2)$*-code of length $4t = 2^s t'$, where t' is odd. Then, for all j such that $a^j \notin \{\mathbf{0}, \mathbf{1}\}$ we have a^j, $a^j b$, $a^j c \notin \mathcal{K}(C)$.*

Proof. Suppose that $t = 2\tau$, for some τ. We begin by showing that $a^\tau \notin \mathcal{K}(C)$. Assume the contrary. From Lemma 2.8, $\pi_a \in \mathrm{Aut}(\mathcal{K}(C))$ and also, since $\mathcal{K}(C)$ is a linear space and π_a is a linear morphism, π_a is a linear isomorphism of $\mathcal{K}(C)$. We have $|\mathcal{K}(C)| = 2^k$. The amount of available values for $\pi_a(a^\tau)$ is bounded by $2^k - 2$. We know that $\pi_a^\tau(a^\tau) = a^\tau + \mathbf{1}$ and so $\pi_a^{2\tau}(a^\tau) = a^\tau$. Hence, if i is the smallest index $1 \leq i \leq 2\tau$ such that $\pi_a^i(a^\tau) = a^\tau$ then, $i \leq 2^k - 2$. Indeed, if $i > 2^k - 2$, then $\pi_a^j(a^\tau) \in \mathcal{K}(C)$ for $j \in \{1, \ldots, i\}$, which contradicts $|\mathcal{K}(C)| = 2^k$.

Now, since C is nonlinear we can apply Lemma 2.25,

$$i \leq 2^k - 2 \leq 2^{s-1} - 2. \tag{3.1}$$

Set $d = \gcd(i, \tau)$ with $d = \lambda i + \mu\tau$, for some integers λ and μ. Compute $\pi_a^d(a^\tau) = a^\tau + \delta\mathbf{1}$, where δ has the value 0 or 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 τ, which is impossible from Lemma 3.46) and therefore $2d = i$. Hence, d is a divisor of τ and $2d = i$ is not a divisor of τ. As $t = 2^{s-2}t'$ we have $d = 2^{s-2}t^*$, where $t^* \mid t'$. Finally, $i = 2d = 2^{s-1}t^* \geq 2^{s-1}$, which contradicts (3.1), so this proofs that $a^\tau \notin \mathcal{K}(C)$.

Suppose $a^j \in \mathcal{K}(C)$ for some $j \notin \{t/2, t\}$. Since the order of each element in $\mathcal{K}(C)$ is a power of two, $a^{j\nu} = a^\tau$ for some ν, and so $a^\tau \in \mathcal{K}(C)$ which is a contradiction.

Now, if $a^j b \in \mathcal{K}(C)$, then $a^{2j} \in \mathcal{K}(C)$ which contradicts *(i)* except for $2j = t$. For $j = t/2$ we can use the same arguments that in the first item when $\tau = t/2$. Analogously $a^j c \notin \mathcal{K}(C)$. $\mathcal{QED}$

Corollary 3.48. *Let $C = \langle a, b, c\rangle$ be a nonlinear* HFP$(2t_{\mathbf{1}}, 2, 2)$*-code of length $4t$. Then,*

(i) if $k = 2$, then $\mathcal{K}(C) = \langle \mathbf{1}, g\rangle$ with $g \in \{b, c, bc\}$,

(ii) if $k = 3$, then $\mathcal{K}(C) = \langle \mathbf{1}, b, c\rangle$ and $r \leq t + 2$.

Proof. It follows from Proposition 3.47. If $k = 3$, from Lemma 2.2, then $r \leq t + 2$. $\mathcal{QED}$

Let G be an HFP$(4t_{\mathbf{1}}, 2)$-code $\simeq \langle a, b \rangle$. As G is also a Hadamard group with respect to $\mathbf{1}$ and $a^{2t} = \mathbf{1}$, we have that $G \times C_2$ is a Hadamard group by Lemma 3.38. Therefore, $G \times C_2$ is an HFP$(4t_u, 2, 2)$-code. We explicit the construction in the following result.

Proposition 3.49. *Let $C = \langle a, b \rangle$ be an* HFP$(4t_{\mathbf{1}}, 2)$*-code of length $4t$ with rank r and dimension of the kernel k. Then there exists an* HFP$(4t_{\mathbf{1}}, 2, 2)$*-code of length $8t$ with rank $r + 1$ and dimension of the kernel $k + 1$.*

Proof. Applying the Sylvester construction, we obtain that $C \times C_2$ is an HFP$(4t_{\mathbf{1}}, 2, 2)$-code with rank $r + 1$ and dimension of the kernel $k + 1$, as in the proof of Proposition 3.39. $\mathcal{QED}$

3.2.4 HFP$(t, Q_{\mathbf{1}})$-codes

In this subsection we assume that $C = \langle d, a, b \mid d^t = \mathbf{1}^2 = \mathbf{0}, a^2 = b^2 = \mathbf{1}, aba = b \rangle$. These codes have been studied in Subsection 3.1.4 for t odd. We recall a method to obtain an HFP$(2t', Q_{\mathbf{1}})$-code of length $8t'$ and an HFP$(4t', Q_{\mathbf{1}})$-code of length $16t'$ from an HFP$(t', Q_{\mathbf{1}})$-code of length $4t'$, where t' is odd.

Proposition 3.50 ([75, Prop. 145])**.** *Let C be an* HFP$(t, Q_{\mathbf{1}})$*-code of length $4t$ with t odd. Then,*

(i) There exists an HFP$(2t, Q_{\mathbf{1}})$*-code of length $8t$ with rank $4t$ and dimension of the kernel 2.*

(ii) There exists an HFP$(4t, Q_{\mathbf{1}})$*-code of length $16t$ with rank $4t + 1$ and dimension of the kernel 3.*

Remark 3.51. *A construction to obtain* HFP$(t, Q_{\mathbf{1}})$*-codes for any t remains open.*

In the following, we show that we can build an HFP$(t, Q_{\mathbf{1}})$-code from a Williamson Hadamard matrix, and vice versa. For convenience, we set the

following permutations to the generators of an HFP$(t, Q_{\mathbf{1}})$-code:

$$\begin{aligned}\pi_{\hat{d}} =&(1,2,\ldots,t)(t+1,\ldots,2t)(2t+1,\ldots,3t)(3t+1,\ldots,4t),\\ \pi_{\hat{a}} =&(1,t+1)(2,t+2)\ldots(t,2t)\\ &(2t+1,3t+1)(2t+2,3t+2)\ldots(3t,4t),\\ \pi_{\hat{b}} =&(1,2t+1)(2,2t+2)\ldots(2t,4t).\end{aligned} \tag{3.2}$$

Note that these permutations are equivalent to the permutations of Proposition 3.26. Let H be a Williamson Hadamard matrix of order $4t$ with the following block distribution,

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

where A, B, C, D are circulant matrices. Let a, b, c, d be the first rows of A, B, C, D, respectively. Let $\pi_{\hat{d}}$ be the permutation result of the product of the permutations $\pi_{d_1}\pi_{d_2}\pi_{d_3}\pi_{d_4}$, where $\pi_{d_1} = (1, 2, \ldots, t)$, $\pi_{d_2} = (t+1, \ldots, 2t)$, $\pi_{d_3} = (2t+1, \ldots, 3t)$, and $\pi_{d_4} = (3t+1, \ldots, 4t)$. We can state the matrices A, B, C, D in the following way

$$A = \begin{pmatrix} a \\ \pi_{d_1}(a) \\ \pi_{d_1}^2(a) \\ \vdots \\ \pi_{d_1}^{t-1}(a) \end{pmatrix}, B = \begin{pmatrix} b \\ \pi_{d_2}(b) \\ \pi_{d_2}^2(b) \\ \vdots \\ \pi_{d_2}^{t-1}(b) \end{pmatrix}, C = \begin{pmatrix} c \\ \pi_{d_3}(c) \\ \pi_{d_3}^2(c) \\ \vdots \\ \pi_{d_3}^{t-1}(c) \end{pmatrix}, D = \begin{pmatrix} d \\ \pi_{d_4}(d) \\ \pi_{d_4}^2(d) \\ \vdots \\ \pi_{d_4}^{t-1}(d) \end{pmatrix}.$$

Let $\hat{d}$ be the vector

$$\begin{aligned}\hat{d} &= (a + \pi_{d_1}^{t-1}(a),\, b + \pi_{d_2}^{t-1}(b),\, c + \pi_{d_3}^{t-1}(c),\, d + \pi_{d_4}^{t-1}(d))\\ &= (\hat{d}_1, \hat{d}_2, \hat{d}_3, \hat{d}_4).\end{aligned}$$

Thus, $\hat{d}$ is the generator of an HFP$(t, Q_{\mathbf{1}})$-code of length $4t$. Indeed, if we sum

$\pi_{d_1}^{t-1}(a)$ to each row of A we obtain

$$\begin{pmatrix} a+\pi_{d_1}^{t-1}(a) \\ \pi_{d_1}(a)+\pi_{d_1}^{t-1}(a) \\ \pi_{d_1}^2(a)+\pi_{d_1}^{t-1}(a) \\ \vdots \\ \pi_{d_1}^{t-1}(a)+\pi_{d_1}^{t-1}(a) \end{pmatrix} = \begin{pmatrix} \hat{d_1} \\ \hat{d_1^2} \\ \hat{d_1^3} \\ \vdots \\ \hat{d_1^t} \end{pmatrix} = \hat{D}_1.$$

Repeating the same operation to b, c, d, and from the permutations (3.2) we have that

$$\begin{pmatrix} \hat{D}_1 & \hat{D}_2 & \hat{D}_3 & \hat{D}_4 \\ \hat{A}_1+\hat{D}_2 & \hat{A}_2+\hat{D}_1 & \hat{A}_3+\hat{D}_4 & \hat{A}_4+\hat{D}_3 \\ \hat{B}_1+\hat{D}_3 & \hat{B}_2+\hat{D}_4 & \hat{B}_3+\hat{D}_1 & \hat{B}_4+\hat{D}_2 \\ \hat{(AB)}_1+\hat{D}_4 & \hat{(AB)}_2+\hat{D}_3 & \hat{(AB)}_3+\hat{D}_2 & \hat{(AB)}_4+\hat{D}_1 \end{pmatrix},$$

which is the Hadamard matrix corresponding to an HFP$(t, Q_{\mathbf{1}})$-code, where

$$\hat{A}_i = \begin{pmatrix} \hat{a}_i \\ \vdots \\ \hat{a}_i \end{pmatrix}, \hat{B}_i = \begin{pmatrix} \hat{b}_i \\ \vdots \\ \hat{b}_i \end{pmatrix}, \hat{(AB)}_i = \begin{pmatrix} \hat{(ab)}_i \\ \vdots \\ \hat{(ab)}_i \end{pmatrix}$$

with

$$\begin{aligned} \hat{a} &= (\hat{a}_1, \hat{a}_2, \hat{a}_3, \hat{a}_4), \\ \hat{b} &= (\hat{b}_1, \hat{b}_2, \hat{b}_3, \hat{b}_4), \text{ and} \\ \hat{(ab)} &= (\hat{(ab)}_1, \hat{(ab)}_2, \hat{(ab)}_3, \hat{(ab)}_4). \end{aligned}$$

3.2.5 HFP$(t, D_{\mathbf{1}})$-codes

In this subsection we assume that $C = \langle d, a, b \mid d^t = b^2 = \mathbf{1}^2 = \mathbf{0}, a^2 = \mathbf{1}, aba = b \rangle$, with t even.

Proposition 3.52. *Let C be an* HFP$(t, D_{\mathbf{1}})$*-code. Then, up to equivalence, we have*

(i) $\pi_d = (1, 5, \ldots, 4t-3)(2, 6, \ldots, 4t-2)(3, 7, \ldots, 4t-1)(4, 8, \ldots, 4t)$,

(ii) $\pi_a = (1, 2)(3, 4)\ldots(4t-1, 4t)$,

(iii) $\pi_b = (1,3)(2,4)\dots(4t-3,4t-1)(4t-2,4t)$,

(iv) $a = (A_1, A_2, \dots, A_t)$ *where* $A_i \in \{(0,1,0,1),(1,0,1,0),(0,1,1,0),(1,0,0,1)\}$,

(v) Knowing the value of a *is enough to define* b,

(vi) $\Pi = C_t \times C_2^2$.

Proof. i),ii) and *iii)* are analogous to the proof of the Proposition 3.35.

iv) Let $a = (a_1, \dots, a_{4t}) = (A_1, \dots, A_t)$ where

$$A_i = (a_{4i-3}, a_{4i-2}, a_{4i-1}, a_{4i}).$$

As $a^2 = a + \pi_a(a) = \mathbf{1}$ then

$$A_i = (a_{4i-3}, \bar{a}_{4i-3}, a_{4i-1}, \bar{a}_{4i-1}).$$

v) From $aba = b$ we have that $a + \pi_a(b) = b + \pi_b(a^{-1}) = b + \pi_b(a^3) = b + \pi_b(\bar{a})$, so $a + \pi_b(\bar{a}) = b + \pi_a(b)$. Note that $a + \pi_b(\bar{a}) = (\hat{A}_1, \dots, \hat{A}_t)$ where $\hat{A}_i = (1,1,1,1)$ or $(0,0,0,0)$.

$$\hat{A}_i = \begin{cases} (1,1,1,1) \text{ if } A_i \in \{(0,1,0,1),(1,0,1,0)\} \\ (0,0,0,0) \text{ if } A_i \in \{(0,1,1,0),(1,0,0,1)\} \end{cases}$$

Let $b = (b_1, \dots, b_{4t}) = (B_1, \dots, B_t)$ where

$$B_i = (b_{4i-3}, b_{4i-2}, b_{4i-1}, b_{4i}),$$

as $b^2 = \mathbf{0}$ then

$$B_i = (b_{4i-3}, b_{4i-2}, b_{4i-3}, b_{4i-2}).$$

Thus,

$$B_i \in \begin{matrix} \{(0,1,0,1),(1,0,1,0)\} \text{ if } A_i \in \{(0,1,0,1),(1,0,1,0)\} \\ \{(0,0,0,0),(1,1,1,1)\} \text{ if } A_i \in \{(0,1,1,0),(1,0,0,1)\} \end{matrix}$$

vi) It follows from Proposition 2.19. $\mathcal{QED}$

3.2.6 Magma computations

In Table 3.2, we show the values of the rank and the dimension of the kernel of the HFP-codes with associated group $C_t \times C_2 \times C_2$ that we have computed with Magma, fulfilling the analytic results.

t	$(t,2,2,2_{\mathbf{1}})$		$(t,4_{\mathbf{1}},2)$		$(t,Q_{\mathbf{1}})$		$(t,D_{\mathbf{1}})$		$(2t_{\mathbf{1}},2,2)$	
	r	k	r	k	r	k	r	k	r	k
1	3	3	3	3	x	x	x	x	3	3
2	✓	✓	4	4	4	4	x	x	x	x
3	✓	✓	✓	✓	11	1	✓	✓	✓	✓
4	5	5	5	5	5	5	5	5	5	5
	x	x	7	2	7	2	7	2	x	x
5	✓	✓	✓	✓	19	1	✓	✓	✓	✓
6	✓	✓	x	x	12	2	x	x	x	x
7	✓	✓	✓	✓	27	1	✓	✓	✓	✓
8	✓	✓	6	6	8	3	6	6	8	3
			7	4	9	2	7	4	x	x
			8	3	11	2	9	3	x	x
			9	2	x	x	9	2	x	x
			11	2	x	x	11	2	x	x
			12	1	x	x	12	1	x	x
9	✓	✓	✓	✓	35	1	✓	✓	✓	✓
10	✓	✓			20	2				
					20	1				
16			12	3						
16			14	2						

Table 3.2: Rank and dimension of the kernel of Hadamard full propelinear codes with associated group $C_t \times C_2 \times C_2$. Symbol x means that the non-existence was checked with Magma by exhaustive search, and symbol ✓means that the non-existence was proved analytically. When the values for the rank and the dimension of the kernel appears in a box it means that they are the only values for that box.

Making use of the shape of the generators a and b from Proposition 3.26, we can apply some restrictions on the generators of $\mathrm{HFP}(t, Q_{\mathbf{1}})$-codes. Therefore, we were be able to build codes of larger order (see Table 3.3).

t	2	3	4		5	6	7	8			9	10	
r	4	11	5	7	19	12	27	8	9	11	35	20	20
k	4	1	5	2	1	2	1	3	2	2	1	2	1
t	11	12	13	14	15	16	17	18	19	20			
r	43	13	51	22	59		67	36	75	21			
k	1	3	1	2	1		1	2	1	3			
t	21	22	23	24	25	26	27	28	29	30			
r	83		91		99	52	107	23		60			
k	1		1		1	2	1	3		2			

Table 3.3: Rank and dimension of the kernel of HFP-codes with group structure $C_t \times Q$.

Now, we present some examples of the Hadamard full propelinear codes introduced in this section.

Example 3.53. *Let a, b, and c be the following vectors of $\mathbb{F}^{32}$*

$$\begin{aligned} a = (&0,1,1,1,1,1,1,1, \quad 1,1,0,1,0,1,0,1,\\ &0,0,1,0,1,0,1,0, \quad 1,0,0,0,0,0,0,0),\\ b = (&0,1,1,0,0,1,1,0, \quad 0,1,1,0,0,1,1,0,\\ &0,1,1,0,0,1,1,0, \quad 0,1,1,0,0,1,1,0),\\ c = (&1,0,1,0,1,0,1,0, \quad 1,0,1,0,1,0,1,0,\\ &1,0,1,0,1,0,1,0, \quad 1,0,1,0,1,0,1,0), \end{aligned}$$

with associated permutations

$$\begin{aligned} \pi_a =&(1,2,3,4,5,6,7,8)(9,10,11,12,13,14,15,16)\\ &(17,18,19,20,21,22,23,24)(25,26,27,28,29,30,31,32),\\ \pi_b =&(1,17)(2,18)(3,19)(4,20)(5,21)(6,22)(7,23)(8,24)\\ &(9,25)(10,26)(11,27)(12,28)(13,29)(14,30)(15,31)(16,32),\\ \pi_c =&(1,25)(2,26)(3,27)(4,28)(5,29)(6,30)(7,31)(8,32)\\ &(9,17)(10,18)(11,19)(12,20)(13,21)(14,22)(15,23)(16,24). \end{aligned}$$

Computing the powers of a, b, c and their products, we obtain $a^8 = \mathbf{1}$, $b^2 =$

$c^2 = \mathbf{0}$, $ab = ba$, $ac = ca$, *and* $bc = cb$. *Thus, the code*

$$\begin{aligned} C = \{&a, a^2, \ldots, a^{16}, \\ &ab, a^2b, \ldots, a^{16}b, \\ &ac, a^2c, \ldots, a^{16}c, \\ &abc, a^2bc, \ldots, a^{16}bc\} \end{aligned}$$

is an $\mathrm{HFP}(16_{\mathbf{1}}, 2, 2)$*-code of length* 32*, which is an* $\mathrm{HFP}(2t_{\mathbf{1}}, 2, 2)$*-code with* $t = 8$. *Computing with* MAGMA *the rank and the dimension of the kernel of* C *we obtain* $r = 8$ *and* $k = 3$. *Moreover,* $\mathcal{K}(C) = \langle \mathbf{1}, b, c \rangle$. *The Hadamard matrix of order* 32 *associated to* C *is*

$$
\begin{pmatrix} a \\ a^2 \\ a^3 \\ a^4 \\ a^5 \\ a^6 \\ a^7 \\ a^8 \\ ab \\ a^2b \\ a^3b \\ a^4b \\ a^5b \\ a^6b \\ a^7b \\ b \\ ac \\ a^2c \\ a^3c \\ a^4c \\ a^5c \\ a^6c \\ a^7c \\ c \\ abc \\ a^2bc \\ a^3bc \\ a^4bc \\ a^5bc \\ a^6bc \\ a^7bc \\ bc \end{pmatrix} = \begin{pmatrix}
0,1,1,1,1,1,1,1,1,1,0,1,0,1,0,1,0,0,1,0,1,0,1,0,1,0,0,0,0,0,0,0 \\
1,1,0,0,0,0,0,0,0,0,1,1,1,1,1,1,0,0,1,1,1,1,1,1,1,1,0,0,0,0,0,0 \\
0,0,0,1,1,1,1,1,0,1,0,0,1,0,1,0,1,0,1,1,0,1,0,1,1,1,1,0,0,0,0,0 \\
1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0 \\
0,0,0,0,0,1,1,1,1,0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1,1,1,1,1,0,0,0 \\
1,1,1,1,1,1,0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,1,1,1,1,1,1,1,0,0 \\
0,0,0,0,0,0,0,1,0,1,0,1,0,1,0,0,1,0,1,0,1,0,1,1,1,1,1,1,1,1,1,0 \\
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 \\
0,1,0,0,1,1,0,0,1,1,1,0,0,1,1,0,0,0,0,1,1,0,0,1,1,0,1,1,0,0,1,1 \\
0,1,0,1,1,0,0,1,1,0,1,0,0,1,1,0,1,0,1,0,0,1,1,0,0,1,0,1,1,0,0,1 \\
1,1,0,1,0,0,1,1,1,0,0,0,0,1,1,0,0,1,1,1,1,1,0,0,1,0,0,1,0,1,1,0 \\
1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0 \\
0,0,1,1,0,1,0,0,1,0,0,1,1,1,1,0,0,1,1,0,0,0,0,1,1,1,0,0,1,0,1,1 \\
0,1,1,0,0,1,0,1,1,0,0,1,1,0,1,0,1,0,0,1,1,0,1,0,0,1,1,0,0,1,0,1 \\
1,1,0,0,1,1,0,1,1,0,0,1,1,0,0,0,0,1,1,0,0,1,1,1,0,0,1,1,0,0,1,0 \\
0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0 \\
0,0,1,0,1,0,1,0,1,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,1,0,1,0,1 \\
0,1,1,0,1,0,1,0,1,0,0,1,0,1,0,1,1,0,0,1,0,1,0,1,0,1,1,0,1,0,1,0 \\
0,1,0,0,1,0,1,0,0,0,0,1,1,1,1,1,1,1,0,0,0,0,0,1,0,1,1,0,1,0,1 \\
0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0 \\
0,1,0,1,0,0,1,0,1,1,1,1,1,0,0,0,0,0,0,0,0,1,1,1,1,0,1,0,1,1,0,1 \\
0,1,0,1,0,1,1,0,1,0,1,0,1,0,0,1,1,0,1,0,1,0,0,1,0,1,0,1,0,1,1,0 \\
0,1,0,1,0,1,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,1,0,1,0,1,0,1,1 \\
1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0 \\
0,0,0,1,1,0,0,1,1,0,1,1,0,0,1,1,0,1,0,0,1,1,0,0,1,1,1,0,0,1,1,0 \\
1,1,1,1,0,0,1,1,0,0,0,0,1,1,0,0,0,0,0,0,0,1,1,0,0,1,1,1,1,0,0,1,1 \\
1,0,0,0,0,1,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,0,0,1,1,1,1,0,0,1 \\
0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0 \\
0,1,1,0,0,0,0,1,1,1,0,0,1,0,1,1,0,0,1,1,0,1,0,0,1,0,0,1,1,1,1,0 \\
1,1,0,0,1,1,1,1,1,0,0,1,1,0,0,0,0,0,0,1,1,0,0,0,0,1,1,0,0,1,1,1,1 \\
1,0,0,1,1,0,0,0,1,1,0,0,1,1,0,1,0,0,1,1,0,0,1,0,0,1,1,0,0,1,1,1 \\
1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0
\end{pmatrix}.
$$

Example 3.54. *Let d, a, and b be the following vectors of $\mathbb{F}^{32}$*

$$\begin{aligned} d = (&1,1,0,0, \quad 1,1,1,1, \quad 1,1,0,0, \quad 1,1,1,1,\\ &1,1,0,0, \quad 0,0,0,0, \quad 1,1,0,0, \quad 0,0,0,0),\\ a = (&0,1,0,1, \quad 0,1,0,1, \quad 0,1,0,1, \quad 0,1,0,1,\\ &0,1,0,1, \quad 0,1,0,1, \quad 0,1,0,1, \quad 0,1,0,1),\\ b = (&1,0,1,0, \quad 1,0,1,0, \quad 0,1,0,1, \quad 0,1,0,1,\\ &1,0,1,0, \quad 1,0,1,0, \quad 0,1,0,1, \quad 0,1,0,1). \end{aligned}$$

with associated permutations

$$\begin{aligned} \pi_d =&(1,5,9,13,17,21,25,29)(2,6,10,14,18,22,26,30)\\ &(3,7,11,15,19,23,27,31)(4,8,12,16,20,24,28,32),\\ \pi_a =&(1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)\\ &(17,18)(19,20)(21,22)(23,24)(25,26)(27,28)(29,30)(31,32),\\ \pi_b =&(1,3)(2,4)(5,7)(6,8)(9,11)(10,12)(13,15)(14,16)\\ &(17,19)(18,20)(21,23)(22,24)(25,27)(26,28)(29,31)(30,32). \end{aligned}$$

Computing the powers of d, a, b, and their products, we obtain $d^8 = b^2 = \mathbf{0}$, $a^2 = \mathbf{1}$, $aba = b$, $ad = da$, and $bd = db$. Thus, the code

$$\begin{aligned} C = \{&d, d^2, \ldots, d^8,\\ &da, d^2a, \ldots, d^8a,\\ &db, d^2b, \ldots, d^8b,\\ &dab, d^2ab, \ldots, d^8ab,\\ &da^2, d^2a^2, \ldots, d^8a^2,\\ &da^3, d^2a^3, \ldots, d^8a^3,\\ &da^2b, d^2a^2b, \ldots, d^8a^2b,\\ &da^3b, d^2a^3b, \ldots, d^8a^3b\} \end{aligned}$$

is an $\mathrm{HFP}(8, D_{\mathbf{1}})$*-code of length* 32*. Computing with* MAGMA*, we obtain we obtain $r = 7$ and $k = 4$. Moreover, $\mathcal{K}(C) = \langle \mathbf{1}, d^4, a, b \rangle$. The Hadamard matrix*

of order 32 *associated to* C *is*

$$\begin{pmatrix} d \\ d^2 \\ d^3 \\ d^4 \\ d^5 \\ d^6 \\ d^7 \\ d^8 \\ da \\ d^2a \\ d^3a \\ d^4a \\ d^5a \\ d^6a \\ d^7a \\ a \\ db \\ d^2b \\ d^3b \\ d^4b \\ d^5b \\ d^6b \\ d^7b \\ b \\ dab \\ d^2ab \\ d^3ab \\ d^4ab \\ d^5ab \\ d^6ab \\ d^7ab \\ ab \end{pmatrix} = \begin{pmatrix} 1,1,0,0,1,1,1,1,1,1,0,0,1,1,1,1,1,1,0,0,0,0,0,0,1,1,0,0,0,0,0,0 \\ 1,1,0,0,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,1,1,0,0,1,1,0,0,1,1,0,0 \\ 0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,1,1,1,1,0,0,1,1,0,0,0,0,1,1,0,0 \\ 0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0 \\ 1,1,0,0,1,1,1,1,0,0,1,1,0,0,0,0,1,1,0,0,0,0,0,0,0,0,1,1,1,1,1,1 \\ 0,0,1,1,0,0,1,1,0,0,1,1,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,0,0,1,1 \\ 1,1,1,1,1,1,0,0,1,1,1,1,1,1,0,0,0,0,0,0,1,1,0,0,0,0,0,0,1,1,0,0 \\ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 \\ 1,0,0,1,1,0,1,0,1,0,0,1,1,0,1,0,1,0,0,1,0,1,0,1,1,0,0,1,0,1,0,1 \\ 1,0,0,1,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,1,0,0,1,1,0,0,1,1,0,0,1 \\ 0,1,0,1,0,1,1,0,1,0,1,0,1,0,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,0,1 \\ 0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1,0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1 \\ 1,0,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,0,1,0,1,0,1,0,1,1,0,1,0,1,0 \\ 0,1,1,0,0,1,1,0,0,1,1,0,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,0,1,1,0 \\ 1,0,1,0,1,0,0,1,1,0,1,0,1,0,0,1,0,1,0,1,1,0,0,1,0,1,0,1,1,0,0,1 \\ 0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1 \\ 1,0,0,1,0,1,0,1,0,1,1,0,1,0,1,0,1,0,0,1,1,0,1,0,0,1,1,0,0,1,0,1 \\ 1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0,0,1,1,0 \\ 1,0,1,0,0,1,1,0,1,0,1,0,0,1,1,0,1,0,1,0,1,1,0,0,1,0,1,0,1,1,1,0 \\ 1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1 \\ 1,0,0,1,0,1,0,1,1,0,0,1,0,1,0,1,1,0,0,1,1,0,1,0,1,0,0,1,1,0,1,0 \\ 0,1,1,0,0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1 \\ 0,1,0,1,1,0,0,1,1,0,1,0,0,1,1,0,1,0,1,0,1,1,0,0,1,0,1,0,1,0,1,0 \\ 1,0,1,0,1,0,1,0,0,1,0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1,0,1,0,1,0,1 \\ 0,0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,1,1,0,0,0,0,1,1,0,0,1,1,1,1 \\ 0,0,1,1,1,1,1,0,0,0,0,1,1,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,1,1,0 \\ 0,0,0,0,1,1,0,0,0,0,0,0,1,1,0,0,1,1,1,1,1,1,1,0,0,1,1,1,1,1,1,0 \\ 0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1 \\ 0,0,1,1,1,1,1,1,1,0,0,1,1,1,1,1,1,0,0,1,1,0,0,0,0,0,0,1,1,0,0,0 \\ 1,1,0,0,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,0,0,1,1,1,1,0,0,0,0,1,1 \\ 1,1,1,1,0,0,1,1,0,0,0,0,1,1,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,0 \\ 0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1 \end{pmatrix}.$$

Chapter 4

Generalized Hadamard full propelinear codes

"It's not what you know, it's what you can prove."

Alonzo Harris. Training Day.

Robust or secure communications are often based on codes built from Hadamard matrices or from relative difference sets. When it is necessary to have an alphabet larger than the binary field, then generalized Hadamard matrices are used. The concept of binary Hadamard matrices was generalized by Butson [20] and Drake [33] independently. Butson Hadamard matrices have entries in the complex m^{th} roots of unity such that its rows are pairwise orthogonal under the Hermitian inner product, but they are not necessarily pairwise row and column balanced. The generalized Hadamard matrices introduced by Drake have entries in a finite group. The main characteristics that they have in common with the binary Hadamard matrices is that rows are pairwise balanced, and exhibits a kind of orthogonality over the group ring, but they are not necessarily invertible. Throughout this chapter, generalized Hadamard matrices are the matrices presented by Drake. The codes built from generalized Hadamard matrices meet the Plotkin bound, i.e., when the length and minimum distance are fixed, the generalized Hadamard codes have the maximum number of codewords.

Cocyclic generalized Hadamard matrices have been studied by Horadam [43] and Horadam and Perera [60]. However, aside from [16] not much has

been done for q-ary propelinear codes, especially for the class of full propelinear codes. To build generalized Hadamard full propelinear codes we will endow generalized Hadamard matrices with a full propelinear structure. We take the theory of cocycles as starting point.

Example 4.1 ([44, Example 9.2.1.4 and Theorem 9.48])**.** *Let G be the additive group of the finite field $\mathbb{F}_{3^a}$ and $\phi_{(a,b)}(g) = g^{(3^b+1)/2}$, $g \in G$ where $\gcd(a,b) = 1$, b is odd and $1 < b < 2a-1$. Then*

$$\partial\phi_{(a,b)}(g,h) = \phi_{(a,b)}(g+h) - \phi_{(a,b)}(g) - \phi_{(a,b)}(h)$$

is an orthogonal coboundary. Hence, $M_{\partial\phi_{(a,b)}}$ is a $\mathrm{GH}(3^a,1)$. Later in Example 4.24, we will deal with $a = 4$ and $b = 3$.

Remark 4.2. *(i) Coulter and Mathews found $\phi_{(a,b)}$ as a new class of planar power functions over $\mathbb{F}_{3^a}$ (see [24]).*

(ii) The symmetric orthogonal coboundaries $\partial\phi_{(a,b)}$ cannot be multiplicative. In particular, the resulting ternary Hadamard codes are nonlinear 3^a-ary codes (see [44, p.227]).

(iii) The orthogonal coboundaries $\partial\phi_{(a,b)}$ and $\partial\phi_{(a,2a-b)}$ determine equivalent Hadamard codes (see [46, Lemma 4.1]). Hence we may restrict to the range $3 \leq b \leq a-1$.

Remind that $\mathbb{F}_q$ denote the finite field of order $q = p^r$, where p is prime. In particular, $\mathbb{F}_q$ is an additive elementary abelian group of order q. Let H be a normalized generalized Hadamard matrix $\mathrm{GH}(q, v/q)$ over $\mathbb{F}_q$ (see definition 2.40), we denote by F_H the q-ary code consisting of the rows of H, and C_H the one defined as

$$C_H = \bigcup_{\alpha\in\mathbb{F}_q} (F_H + \alpha\mathbf{1}),$$

where $\alpha\mathbf{1}$ denotes the all-α vector. The code C_H over $\mathbb{F}_q$ is called *generalized Hadamard code* (briefly, GH-code) of length v, which has qv codewords and minimum distance $v - v/q$, i.e., C_H is a $(v, qv, v-v/q)_q$-code. Hence, generalized Hadamard codes meet the Plotkin bound [44]. Note that F_H and C_H are generally nonlinear codes over $\mathbb{F}_q$.

A binary Hadamard matrix of order $v = 4t$ corresponds to a $\mathrm{GH}(2, 2t)$, where $U = \langle -1 \rangle$. In this case two further equivalences are known.

Proposition 4.3. *When $U = \langle -1 \rangle \simeq \mathbb{Z}_2$, the equivalent statements of Theorem 2.41 are further equivalent to the following statements.*

(iv) There is a Hadamard group E_ψ [37].

(v) C_H is a Hadamard full propelinear code [67].

In this chapter, we prove the analog of Proposition 4.3 when U is the additive group of a finite field (i.e. additive elementary abelian group). As a consequence, the class of generalized Hadamard full propelinear codes is introduced. Concerning equivalence *(iv)*, let us mention that the Hadamard group E_ψ in the binary case is effectively what is referred to as the *extension group* of a cocyclic Hadamard matrix, which is also defined for generalized Hadamard matrices with entries in U. Therefore, if the existence of a generalized Hadamard full propelinear code is equivalent to the existence of an orthogonal cocycle ψ, then there is an extension group E_ψ. Finally, let us point out that it seems that a generalized Hadamard matrix over any abelian group U (should it exist) would afford the same theory, assuming similar definitions of propelinear codes over groups and so forth.

4.1 q-ary propelinear codes

Assuming the Hamming metric, any isometry of $\mathbb{F}_q^n$ is given by a coordinate permutation π and n permutations $\sigma_1, \ldots, \sigma_n$ of $\mathbb{F}_q$. We denote by $\mathrm{Aut}(\mathbb{F}_q^n)$ the group of all isometries of $\mathbb{F}_q^n$:

$$\mathrm{Aut}(\mathbb{F}_q^n) = \{(\sigma, \pi) \mid \sigma = (\sigma_1, \ldots, \sigma_n) \,\mathrm{with}\, \sigma_i \in \mathrm{Sym}\mathbb{F}_q,\ \ \pi \in \mathcal{S}_n\}$$

where $\mathrm{Sym}\mathbb{F}_q$ and $\mathcal{S}_n$ denote, respectively, the symmetric group of permutations on $\mathbb{F}_q$ and on the set $\{1, \ldots, n\}$.

For any $\sigma = (\sigma_1, \ldots, \sigma_n)$ where $\sigma_i \in \mathrm{Sym}\mathbb{F}_q$, $\pi \in \mathcal{S}_n$ and $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$, we write $\sigma(v)$ and $\pi(v)$ to denote $(\sigma_1(v_1), \ldots, \sigma_n(v_n))$ and $(v_{\pi^{-1}(1)}, \ldots, v_{\pi^{-1}(n)})$, respectively.

The action of (σ, π) is defined as

$$(\sigma, \pi)(v) = \sigma(\pi(v)) \quad \text{for any } v \in \mathbb{F}_q^n,$$

and the group operation in $\mathrm{Aut}(\mathbb{F}_q^n)$ is the composition

$$(\sigma, \pi) \circ (\sigma', \pi') = ((\sigma_1 \circ \sigma'_{\pi^{-1}(1)}, \ldots, \sigma_n \circ \sigma'_{\pi^{-1}(n)}), \pi \circ \pi')$$

for all $(\sigma, \pi), (\sigma', \pi') \in \mathrm{Aut}(\mathbb{F}_q^n)$. Here and throughout the entire chapter, we use the convention $f \circ g(v) = f(g(v))$, for $v \in \mathbb{F}_q^n$. We denote by $\mathrm{Aut}(C)$ the group of all isometries of $\mathbb{F}_q^n$ fixing the code C and we call it the *automorphism group* of the code C.

At this point, we introduce some basic background on automophism group of a matrix. Let K be a multiplicative group isomorphic to the additive elementary abelian group $\mathbb{F}_q$, and let $\phi : \mathbb{F}_q \to K$ be an isomorphism. *An automorphism of a matrix* M with entries in a group K is a pair of monomial matrices (P, Q) with non-zero entries in K such that $PMQ^* = M$, where Q^* denotes the matrix obtained from the transpose of Q by replacing each non-zero entry with its inverse in K, and matrix multiplication is carried out over the group ring $\mathbb{Z}[K]$. *The automorphism group* $\mathrm{Aut}(M)$ of M is the set of all such pairs of matrices, closed under the multiplication $(P, Q)(R, S) = (PR, QS)$. *The permutation automorphism group of* M is the subgroup $\mathrm{PAut}(M) \subset \mathrm{Aut}(M)$ comprised of all pairs of permutation matrices in $\mathrm{Aut}(M)$.

Lemma 4.4 ([27])**.** *Let M be a K-monomial matrix of order n. Then M has a unique factorization $D_M P_M$ where D_M is a diagonal matrix and P_M is a permutation matrix.*

Here we will focus on GH-codes, C_H, where H denotes a generalized Hadamard matrix of order v with entries in the additive elementary abelian group $\mathbb{F}_q$ and write $\phi(H) = [\phi(h_{ij})]_{1 \le i,j \le v}$.

In what follows, we will make explicit the correspondence between the elements of the automorphism group $\mathrm{Aut}(\phi(H))$ and certain isometries of C_H (elements of $\mathrm{Aut}(C_H)$). Let $(M, N) \in \mathrm{Aut}(\phi(H))$, $x = [[D_M]_{1,1}, \ldots, [D_M]_{v,v}]$ and X be the $v \times v$ matrix such that each column is equal to x^T. It follows that $\phi(X + H) = D_M \phi(H)$. Likewise, if Y is a $v \times v$ matrix over $\mathbb{F}_q$ such that each row is equal to $y = [[D_N]_{1,1}, \ldots, [D_N]_{v,v}]$, then $\phi(H - Y) = \phi(H) D_N^*$. So, $\phi(X +$

$P_M H P_N^T - Y) = M\phi(H)N^* = \phi(H)$. Thus $X + P_M H P_N^T - Y = H$ and $(\sigma, \pi) \in \mathrm{Aut}(C_H)$ where $\sigma_i(u) = u + [D_N]_{i,i}$ and $\pi(1, \ldots, v) = (1, \ldots, v)P_N$. We will say that (σ, π) is the isometry of C_H associated to the automorphism (M, N) of $\phi(H)$. Now, the following question arises naturally: Given an isometry (σ, π) of C_H, is it possible to define an automorphism (M, N) of $\phi(H)$ associated to (σ, π)? We will answer this question affirmatively in a particular case in the next section.

Definition 4.5 (Borges et al. [16]). *A q-ary code C of length n, $\mathbf{0} \in C$, has a propelinear structure if for any codeword $x \in C$ there exist $\pi_x \in \mathcal{S}_n$ and $\sigma_x = (\sigma_{x,1}, \ldots, \sigma_{x,n})$ with $\sigma_{x,i} \in \mathrm{Sym}\mathbb{F}_q$ satisfying:*

(i) $(\sigma_x, \pi_x)(C) = C$ *and* $(\sigma_x, \pi_x)(\mathbf{0}) = x$,

(ii) if $y \in C$ *and* $z = (\sigma_x, \pi_x)(y)$, *then* $(\sigma_z, \pi_z) = (\sigma_x, \pi_x) \circ (\sigma_y, \pi_y)$.

A q-ary code C is called *transitive* if the $\mathrm{Aut}(C)$ acts transitively on its codewords, i.e., the code satisfies the property *(i)* of the above definition.

Assuming that C has a propelinear structure then a binary operation $\star$ can be defined as

$$x \star y = (\sigma_x, \pi_x)(y) \quad \text{for any } x, y \in C.$$

Therefore, $(C, \star)$ is a group, which is not abelian in general. This group structure is compatible with the Hamming distance, that is, $d(x \star u, x \star v) = d(u, v)$ where $u, v \in \mathbb{F}_q^n$. The vector $\mathbf{0}$ is always a codeword where $\pi_{\mathbf{0}} = Id_n$ is the identity coordinate permutation and $\sigma_{\mathbf{0},i} = Id_q$ is the identity permutation on $\mathbb{F}_q$ for all $i \in \{1, \ldots, n\}$. Hence, $\mathbf{0}$ is the identity element in C and $\pi_{x^{-1}} = \pi_x^{-1}$ and $\sigma_{x^{-1},i} = \sigma_{x,\pi_x(i)}^{-1}$ for all $x \in C$ and for all $i \in \{1, \ldots, n\}$. We call $(C, \star)$ a *propelinear code*. Henceforth we use C instead of $(C, \star)$ if there is no confusion.

Clearly, the propelinear class is more general than the linear code class. Since, every linear code C has the following trivial propelinear structure:

$$\sigma_a(x) = a + x, \quad \text{and} \quad \pi_a(x) = x \quad \forall a, x \in C.$$

In Examples 4.21, 4.22, 4.23 we show linear codes which can be endowed with a nontrivial propelinear structure. In Example 4.24 we present a nonlinear propelinear code. The following result is the q-ary generalization of Proposition 2.5.

Proposition 4.6. *Let $(C, \star) \subset \mathbb{F}_q^n$ be a group. C is a propelinear code if and only if the group* $\mathrm{Aut}(C)$ *(the isometries) contains a regular subgroup acting transitively on C.*

Proof. Firstly, we assume C is propelinear. Let $\rho_x : C \to C$ given by $\rho_x(v) = x \star v$. Let x, y, z be any codewords in C, we have $\rho_x\rho_y(z) = \rho_x(y \star z) = x \star (y \star z) = (x \star y) \star z = \rho_{x\star y}(z)$. From [16, Lemma 5], we have $d(x \star y, x \star z) = d(y, z)$, and so $d(\rho_x(y), \rho_x(z)) = d(x \star y, x \star z) = d(y, z)$. Therefore, $G = \{\rho_x \mid x \in G\}$ is a subgroup of $\mathrm{Aut}(C)$, and $|G| = |C|$. Given $x, y \in C$, we take $z = y \star x^{-1}$, and so we have $\rho_z(x) = z \star x = y \star x^{-1} \star x = y$. Hence, G acts transitively on C.

Conversely, we assume $\mathrm{Aut}(C)$ contains a regular subgroup G acting transitively on C, so $|G| = |C|$. We call ρ_x the element of G such that $\rho_x(\mathbf{0}) = x$. Note that $G \to C$ given by $\rho_x \to x$ is a bijection since G is regular and acts transitively on C. For $x \in C$, we define $(\sigma_x, \pi_x)(y) = \rho_x(y)$. Note that $(\sigma_x, \pi_x) \in \mathrm{Aut}(C)$ because ρ_x is an isometry on C. We define $x \star y = (\sigma_x, \pi_x)(y) = \rho_x(y)$, where $x \in C$. Let us see that the operation $\star$ is propelinear, and so C has a propelinear structure. It is clear that $(\sigma_x, \pi_x)(C) = \rho_x(C) = C$, and $x \star \mathbf{0} = \rho_x(\mathbf{0}) = x$ for any $x \in C$. As G acts transitively on C, we have $\rho_x\rho_y = \rho_{x\star y}$ if and only if $\rho_x\rho_y(\mathbf{0}) = \rho_{x\star y}(\mathbf{0})$. Let $x, y \in C$, then $\rho_{x\star y}(\mathbf{0}) = x \star y = \rho_x(y) = \rho_x(\rho_y(\mathbf{0})) = \rho_x\rho_y(\mathbf{0})$. Thus, $(\sigma_{x\star y}, \pi_{x\star y})(z) = \rho_{x\star y}(z) = \rho_x\rho_y(z) = \rho_x((\sigma_y, \pi_y)(z)) = (\sigma_x, \pi_x) \circ (\sigma_y, \pi_y)(z)$. $\mathcal{QED}$

Let C be a binary propelinear code. From Lemma 2.8, $x \in \mathcal{K}(C)$ if and only if $\pi_x \in \mathrm{Aut}(C)$. As a code is linear if and only if its dimension is equal to the dimension of its kernel and to its rank, we have that a binary propelinear code C is linear if and only if $\pi_x \in \mathrm{Aut}(C)$ for all $x \in C$. The analog of this result about the linearity for q-ary propelinear codes remains an open problem.

Definition 4.7. *A full propelinear code is a propelinear code C such that for every $a \in C$, $\sigma_a(x) = a + x$ and π_a has no fixed coordinates when $a \neq \alpha\mathbf{1}$ for $\alpha \in \mathbb{F}_q$. Otherwise, $\pi_a = Id_n$.*

A generalized Hadamard code, which is also full propelinear, is called *generalized Hadamard full propelinear code* (briefly, GHFP-code).

Lemma 4.8. *Let C be a GHFP-code and $a, b \in C$. If $a - b = \lambda\mathbf{1}$ where $\lambda \in \mathbb{F}_q$ then $\pi_a = \pi_b$.*

Proof. We have $b \star \lambda\mathbf{1} = b + \pi_b(\lambda\mathbf{1}) = b + \lambda\mathbf{1} = a$ and $a \star \lambda\mathbf{1} = \lambda\mathbf{1} \star a$. On the other hand, $\pi_a(x) = a \star x - a = (b \star \lambda\mathbf{1}) \star x - (b + \lambda\mathbf{1}) = (b \star x) \star \lambda\mathbf{1} - (b + \lambda\mathbf{1}) = (b \star x) + \lambda\mathbf{1} - (b + \lambda\mathbf{1}) = b \star x - b = \pi_b(x)$, for all $x \in C$. $\mathcal{QED}$

Lemma 4.9. *Let C be a GHFP-code and e_i be the unitary vector with only nonzero coordinate at the i-th position. If $x, y \in C$ then $\pi_x^{-1}(e_i) = \pi_y^{-1}(e_i)$ if and only if $x = y + \lambda\mathbf{1},\ \lambda \in \mathbb{F}_q$. Furthermore, if $x, y \in F_H$ then $x = y$.*

Proof. We have $\pi_x^{-1}(e_i) = \pi_y^{-1}(e_i) \Leftrightarrow e_i = \pi_x\pi_y^{-1}(e_i) = \pi_x\pi_{y^{-1}}(e_i) = \pi_{x \star y^{-1}}(e_i)$. Since C is full propelinear then $x \star y^{-1} = \lambda\mathbf{1},\ \lambda \in \mathbb{F}_q$. $\mathcal{QED}$

Lemma 4.10. *Let C be a GHFP-code, $\Pi = \{\pi_x \mid x \in C\}$ and $C_1 = \{\lambda\mathbf{1} \mid \lambda \in \mathbb{F}_q\}$. Then $C_1 \subset \mathcal{K}(\mathcal{C})$ and Π is isomorphic to C/C_1.*

Proof. It is immediate that $C_1 = \{\lambda\mathbf{1} \mid \lambda \in \mathbb{F}_q\} \subset \mathcal{K}(\mathcal{C})$. The map $x \to \pi_x$ is a group homomorphism from C to Π. Since C is full propelinear, the kernel of this homomorphism is C_1. Hence, we conclude with the desired result. $\mathcal{QED}$

4.2 GHFP-codes and cocyclic GH matrices

From now on, H denotes a generalized Hadamard matrix of order v with entries in the additive elementary abelian group $\mathbb{F}_q$. K denotes a multiplicative group isomorphic to the additive elementary abelian group $\mathbb{F}_q$, and let $\phi : \mathbb{F}_q \to K$ be an isomorphism. Write

$$\phi(H) = [\phi(h_{ij})]_{1 \le i,j \le n}.$$

Consider the $qv \times v$ matrix $E_{\phi(H)}$ comprised of the q blocks

$$k_0\phi(H), \ldots, k_{q-1}\phi(H),$$

where $K = \{k_0 = 1, k_1, \ldots, k_{q-1}\}$. Assuming that C_H is a GHFP-code and $a, x \in C_H$, then the action of a on C_H defined by

$$\rho_a(x) = a \star x = a + \pi_a(x) \in C_H,$$

($\rho_a \in \mathrm{Aut}(C_H)$) is equivalent to the action of N^* on $E_{\phi(H)}$ by right matrix multiplication where $N^* = Q^*D^*_{-a}$, with Q being the permutation matrix according to π_a, and D_a the diagonal matrix with diagonal $\phi(a)$. Since

the action of a on C preserves C, there is a $qv \times qv$ permutation matrix P' such that $P'E_{\phi(H)}N^* = E_{\phi(H)}$. Moreover, the rows of $E_{\phi(H)}$ are the rows of $\phi(H), k_1\phi(H), \ldots, k_{q-1}\phi(H)$. Thus there is a $v \times v$ monomial matrix $M = D_kP$ with k a vector of length v over K such that $M\phi(H)N^* = \phi(H)$, where for all $1 \leq i, j \leq v$ and $0 \leq d \leq q-1$, if P' permutes row $j + dv$ to row i then

- P permutes row j to row i, and
- the i-th entry of k is k_d.

Thus (M, N) is an automorphism of $\phi(H)$. If $a = \lambda\mathbf{1}$ for some $\lambda \in \mathbb{F}_q$, then the corresponding automorphism is of the form $(\phi(-\lambda)I, \phi(-\lambda)I)$. This proves the following result where R denotes the subset of the $\mathrm{Aut}(\phi(H))$ with elements (M, N), the corresponding automorphism associated to $a \in C_H$.

Theorem 4.11. *If H is a generalized Hadamard matrix over the additive abelian group of $\mathbb{F}_q$ such that the rows of H comprise a GHFP-code C, then the group $(C, \star) \simeq R \subseteq \mathrm{Aut}(\phi(H))$. Moreover, $(kI, kI) \in R$ for all $k \in K$, and R acts transitively on rows of $\phi(H)$.*

Remark 4.12. *R acts transitively on rows of $\phi(H)$ since $\rho_a(x) = \rho_b(x)$ if and only if $a = b$ but not regularly since $|R| \neq v$.*

Now, for a generalized Hadamard matrix M with entries in K, $\mathrm{Aut}(M) \simeq \mathrm{PAut}(\mathcal{E}_M)$ where $\mathcal{E}_M = [k_ik_jM]_{0 \leq i,j \leq q-1}$ (this is a special case of [27, Theorem 9.6.14]). Where $\Theta : \mathrm{Aut}(M) \to \mathrm{PAut}(\mathcal{E}_M)$ is the isomorphism outlined in [27, pp. 110–111]), we note that the center of $\mathrm{Aut}(M)$ contains the group of pairs of diagonal matrices $Z = \{(kI, kI) \mid k \in K\}$, and thus $\Theta(Z)$ is a central subgroup of $\mathrm{PAut}(\mathcal{E}_M)$. We require that $\pi_{\lambda\mathbf{1}} = Id_n$ in order for C to be full propelinear. The transitivity requirement of the group $(C, \star)$ on C for full propelinear codes then gives the following.

Theorem 4.13. *C is a generalized Hadamard full propelinear code if and only if there is a subgroup $R \subseteq \mathrm{Aut}(\phi(H))$ with $Z \subseteq R$ such that $\mathrm{PAut}(\mathcal{E}_{\phi(H)})$ contains a regular subgroup $\Theta(R)$, with $\Theta(Z) \subseteq \Theta(R)$.*

Proof. Let $K = \{k_0 = 1, k_1, \ldots, k_{q-1}\}$ and $Z = \{z_i = (k_iI, k_iI) \mid i \in \{0, \ldots, q-1\}\}$ and let C be a generalized Hadamard full propelinear code. Theorem 4.11 gives that $(C, \star) \simeq R \subseteq \mathrm{Aut}(\phi(H))$ where $Z \subseteq R$, and R acts transitively on

the rows of $\phi(H)$. Since Z is central and acts only by multiplication on rows of $\phi(H)$, there is a right transversal S of Z in R where for any $j \in \{1, \ldots, n\}$ there is $s_j \in S$ such that $\phi(H)_j = (s_j\phi(H))_1$. Thus $\Theta(z_i s_j)$ permutes row 1 of $\mathcal{E}_{\phi(H)}$ to row $iq + j$, proving that $\Theta(R)$ is transitive on rows of $\mathcal{E}_{\phi(H)}$. By Theorem 4.11, $|R| = |(C, \star)|$ and thus $\Theta(R)$ acts regularly.

Conversely, assuming that H is generalized Hadamard over $\mathbb{F}_q$ and that there is a subgroup $R \subseteq \mathrm{Aut}(\phi(H))$ with $Z \subseteq R$ such that $\Theta(R) \subseteq \mathrm{PAut}(\mathcal{E}_{\phi(H)})$ is regular and $\Theta(Z) \subseteq \Theta(R)$. Label the rows of $\mathcal{E}_{\phi(H)}$ with the codewords of C_H in the order of the rows of E_H such that the first n entries of the row of $\mathcal{E}_{\phi(H)}$ are the entries in the codeword labelling the row. For any $x \in C_H$ there is $(M_x, N_x) \in \Theta(R)$ such that M_x sends row x to row 0. In the preimage of Θ, N_x corresponds to a monomial matrix $D_{-x}Q_x$. For each x, let π_x be coordinate the permutation according to the action of Q^* on columns of $\phi(H)$, and let $\sigma_x(a) = a + x$ for all $a \in E_H$, (i.e., π_x and σ_x are determined by the column action of N_x). It follows that if $(\pi_x, \sigma_x) \circ (\pi_y, \sigma_y) = (\pi_z, \sigma_z)$ then $N_x N_y = N_z$. It also follows that $(\sigma_x, \pi_x)(\mathbf{0}) = x$ for all x.

Then let $f : \Theta(R) \to C_H$ be the map such that $f(M_x, N_x) = x$. Clearly this map is bijective. Further, where $\lambda \in \mathbb{F}_q$, it follows that $(M_{\lambda\mathbf{1}}, N_{\lambda\mathbf{1}}) \in \Theta(Z)$, where $\pi_{\lambda\mathbf{1}} = Id_n$. Because $R \subseteq \mathrm{Aut}(\phi(H))$, it follows that $(\sigma_x, \pi_x)(C_H) = C_H$ for all x.

Now, if $N_x N_y = N_z$, then we have $z = (\sigma_z, \pi_z)(\mathbf{0}) = (\sigma_x, \pi_x)(\sigma_y, \pi_y)(\mathbf{0}) = (\sigma_x, \pi_x)(y)$ and so $z = x \star y$. Thus $f(M_x, N_x) \star f(M_y, N_y) = x \star y = z = f(M_z, N_z)$. Hence, f is a homomorphism and C_H has a propelinear structure. $\mathcal{QED}$

Let G be a group of order n and let $\psi : G \times G \to K$ be a 2-cocycle. Then let E_ψ denote the canonical central extension of K by G obtained from ψ. The following is a special case of [27, Theorem 14.6.4].

Theorem 4.14. *A generalized Hadamard matrix H over K is cocyclic with cocycle ψ if and only if there exists a centrally regular embedding of E_ψ into* $\mathrm{PAut}(\mathcal{E}_H)$.

Corollary 4.15. *The code C_H comprised of the rows of E_H is a generalized Hadamard full propelinear code if and only if the matrix H is cocyclic over some cocycle ψ, with extension group $E_\psi \simeq R \simeq (C_H, \star)$ where R is a regular subgroup of* $\mathrm{PAut}(\mathcal{E}_H)$.

Remark 4.16. *We observe that a generalized Hadamard matrix H may be cocyclic over several distinct cocycles ψ, and that the extension groups E_ψ are not necessarily isomorphic. As such, given a cocyclic generalized Hadamard matrix H, there may be several codes $(C_H, \star)$ that are equal setwise, i.e., they contain the same set of codewords, but are not isomorphic as groups.*

In what follows, we will make explicit the correspondence between the elements of E_ψ and $(C_H, \star)$.

Assuming $\psi \in Z^2(G, K)$. We recall that K denotes the multiplicative group isomorphic to the additive elementary abelian group $\mathbb{F}_q$. For a fixed order in $G = \{g_0 = 1, g_1, \ldots, g_{v-1}\}$ and in $K = \{k_0 = 1, k_1, \ldots, k_{q-1}\}$, we can define the following map:

$$\Phi \colon E_\psi \to K^v$$

given an element $(k, g) \in E_\psi$,

$$[\Phi(k, g)]_j = k_l, \quad \text{if } (k, g)^{-1} t_j \in T(\psi)\,(k_l, 1),$$

where $T(\psi) = \{(t_0 = (1, 1), t_2 = (1, g_1), \ldots, t_{v-1} = (1, g_{v-1})\}$. Obviously, $T(\psi)\,(c_i, 1) = (c_i, 1)T(\psi)$ and Φ is well-defined. After some calculations,

$$[\Phi(k, g)]_j = (k\psi(g, g^{-1}))^{-1}\,\psi(g^{-1}, g_j).$$

Hence, $\Phi(k, g)$ is equal to $(k\psi(g, g^{-1}))^{-1}$-times the row of M_ψ indexed with the element g^{-1}.

Clearly, Φ is an injective map. The inverse of Φ (over the $\operatorname{Im}\Phi$) is

$$\Phi^{-1}(\lambda\,(\psi(g, g_1), \ldots, \psi(g, g_v))) = ((\lambda\,\psi(g^{-1}, g))^{-1},\, g^{-1}),$$

where $\lambda \in K$ and $g \in G$.

Proposition 4.17. *If $\psi \in Z^2(G, K)$ is orthogonal then $C = (\Phi(E_\psi), \star)$ is a GHFP-code where $x \star y = \Phi(\Phi^{-1}(x) \cdot \Phi^{-1}(y))$ with $x, y \in \Phi(E_\psi)$.*

Proof. Firstly, we will show that $\pi_x \in \mathcal{S}_v$ where $\pi_x(y) = x \star y - x$. We know that every codeword has to be a multiple of a row of M_ψ. We take $x = \lambda\,(\psi(g, g_1), \ldots, \psi(g, g_v))$ and $y = \mu\,(\psi(h, g_1), \ldots, \psi(h, g_v))$. By a routine

computation, we get that

$$[x \star y]_j = \lambda\mu\psi(g^{-1}, g)\psi(h^{-1}, h)\left(\psi(g^{-1}, h^{-1})\psi((hg)^{-1}, hg)\right)^{-1}\psi(hg, g_j).$$

Putting together,

$$\begin{aligned}
[\pi_x(y)]_j &= [x \star y]_j - [x]_j \\
&= \mu\psi(g^{-1}, g)\psi(h^{-1}, h)\left(\psi(g^{-1}, h^{-1})\psi((hg)^{-1}, hg)\right)^{-1} \\
&\quad \psi(hg, g_j)(\psi(g, g_j))^{-1} \\
&= \mu\psi(h, gg_j).
\end{aligned}$$

In the last identity we have used these properties coming from (2.1)

- $\psi(hg, g_j)(\psi(g, g_j))^{-1} = \psi(h, gg_j)(\psi(h, g))^{-1}$.
- $\psi(h^{-1}, h)(\psi(h, g))^{-1} = \psi(h^{-1}, hg)$.
- $\psi(g^{-1}, h^{-1})\psi(g^{-1}h^{-1}, hg) = \psi(g^{-1}, g)\psi(h^{-1}, hg)$.

Hence, the map π_x is an element of $\mathcal{S}_v$. Specifically, for any y, π_x moves the l-th coordinate of y to j-th coordinate where $g_l = gg_j$. As a consequence of this fact, it is immediate that if $x = \lambda\mathbf{1}$, with $\lambda \in \mathbb{F}_q$, then $\pi_x = Id_v$ since $g = 1$ is the identity of G. Furthermore, if $g \neq 1$ (or equivalently $x \neq \lambda\mathbf{1}$), then π_x has no fixed coordinates.

Secondly, we show an important property of these permutations. Concretely, given $x, y \in C$, we have that $\pi_x\pi_y = \pi_{x\star y}$. To prove it, let z be an element of C then

$$\begin{aligned}
\pi_{x\star y}(z) &= (x \star y) \star z - x \star y \\
&= x \star (y \star z) - x \star y \\
&= x + \pi_x(y \star z) - \pi_x(y) - x \\
&= \pi_x(y \star z - y) = \pi_x(\pi_y(z)).
\end{aligned}$$

$\mathcal{QED}$

Let H be a normalized generalized Hadamard matrix $\mathrm{GH}(q, v/q)$ over $\mathbb{F}_q$ and f be any row of H. D_j denotes the subset of C_H such that $x \in D_j$ if $[x]_j = 0 \in \mathbb{F}_q$. Let us observe the following facts:

(i) $D_j = \bigcup_{\alpha \in \mathbb{F}_q} \{f + (-\alpha)\mathbf{1} \mid f \in F_H \text{ and } [f]_j = \alpha\}$.

(ii) $D_1 = F_H$.

(iii) For $j > 1$, $|\{f \in F_H : [f]_j = \alpha\}| = v/q$. Since $\mathbb{F}_q$ is abelian, then H^T is a $\mathrm{GH}(q, v/q)$ (over $\mathbb{F}_q$) too [44, Lemma 4.10]. Thus, the number of entries equal to α in the j-th column of H is v/q, for all $\alpha \in \mathbb{F}_q$.

(iv) $|D_j| = v$ and $C = \bigcup_{i \geq 1} D_i$.

Proposition 4.18. *Let $(C, \star)$ be a GHFP-code of length v over $\mathbb{F}_q$ coming from H, which is a $\mathrm{GH}(q, v/q)$. Then $F_H = D_1$ is a (central) relative $(v, q, v, v/q)$-difference set in C relative to the normal subgroup $C_1 = \{\alpha\mathbf{1} \mid \alpha \in \mathbb{F}_q\} \simeq \mathbb{F}_q$.*

Proof. C_1 is a central subgroup. We have to prove:

$$|F_H \cap x \star F_H| = \begin{cases} v & x = \mathbf{0} \\ 0 & x \in C_1 \setminus \{\mathbf{0}\} \\ v/q & x \in C \setminus C_1 \end{cases}$$

- Let us observe that if $x \in C_1$ then $\pi_x = Id_v$. Now, if $f \in F_H$ then the first entry of $x \star f = x + f$ is 0 if and only if $x = \mathbf{0}$. So, we conclude with the desired result for the first and the second identities.

- Let $x \notin C_1$ and $\pi_x(1) = j$, ($j \neq 1$ since C is full propelinear). Let $\alpha_0 \in \mathbb{F}_q$ be such that $[x + \alpha_0\mathbf{1}]_j = 0$. Since $(x + \alpha_0\mathbf{1}) \star f \in D_j$ for all $f \in F_H$ and $|y \star F_H| = v$ for all $y \in C_H$, then $(x + \alpha_0\mathbf{1}) \star F_H = D_j$. As a consequence,

  $$x \star F_H = D_j - \alpha_0\mathbf{1}.$$

  Therefore, $|F_H \cap x \star F_H|$ = number of entries equal to $-\alpha_0$ in the j-th column of H what it is equal to v/q. This concludes the proof.

$\mathcal{QED}$

Corollary 4.19. *Let $(C, \star)$ be a GHFP-code of length v over $\mathbb{F}_q$ coming from H a $\mathrm{GH}(q, v/q)$. Let $G = C/C_1$ and $\sigma(f \star C_1) = f$ for $f \in F_H$. The map $\psi_{F_H} \colon G \times G \to K$ defined by*

$$\psi_{F_H}(g, h) = k, \quad \text{if } \sigma(g) \star \sigma(h) \in k\mathbf{1} \star F_H$$

is an orthogonal cocycle, i.e., $M_{\psi_{F_H}}$ is a $\mathrm{GH}(w, v/w)$*. Furthermore,* $(C, \star) \simeq E_{\psi_{F_H}}$ *where* $F_H^\star = \{(1, g) \mid g \in G\}$ *is the isomorphic image of* F_H*.*

Proof. It is a consequence of [60, Theorem 3.1] and Proposition 4.18. $\mathcal{QED}$

4.3 Examples

In this section, we provide some examples of generalized Hadamard full propelinear codes coming from cocyclic generalized Hadamard matrices. The last one (Example 4.24) has a special interest since it is a family of nonlinear GHFP-codes. We will study their rank and the dimension of their kernel. Dougherty, Rifà, and Villanueva [32] initiated the study of the rank and dimension of the kernel of codes coming from generalized Hadamard matrices. We begin with a definition of an infinite family of cocyclic generalized Hadamard matrices.

Definition 4.20 ([27, Section 9.2])**.** *Let $q = p^m$ be a prime power and denote the k-dimensional vector space over $\mathbb{F}_q$ by V. Then*

$$D_{(p,m,k)} = [xy^\top]_{x,y \in V}$$

is a $\mathrm{GH}(q, q^{k-1})$*. These are known as the generalized Sylvester matrices.*

It is well known that the generalized Sylvester matrices are cocyclic, see [44, p. 122] for example. Egan and Flannery [34] analyzed the generalized Sylvester matrices in terms of their cocyclic development. The analysis shows that these matrices have several non-isomorphic indexing and extension groups, and the number of non-isomorphic indexing and extension groups grows with k and m. They are closely related to the regular subgroups of the affine general linear group $\mathrm{AGL}_{k+1}(V)$. Therefore the matrix $H = D_{(p,m,k)}$ of order q^k is cocyclic with multiple cocycles ψ and has multiple non-isomorphic extension groups E_ψ of order q^{k+1}. As such, for each ψ the associated codes $(C, \star)$ each have the same set of codewords (the rows of E_H), but are non-isomorphic as groups. Some of the examples below are members of the generalized Sylvester matrices.

Example 4.21. *If* $G = U = \langle a, b \mid a^2 = b^2 = (ab)^2 = 1\rangle \simeq \mathbb{Z}_2^2$ *(the additive group of* $\mathbb{F}_4$ *but with multiplicative notation) with indexing* $\{1, a, b, ab\}$*, then the* G*-cocyclic matrix with coefficients in* U

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & a & ab & b \\ 1 & ab & b & a \\ 1 & b & a & ab \end{pmatrix}$$

is a generalized Hadamard matrix, $\mathrm{GH}(4, 1)$*, with entries in* $\mathbb{F}_4$*. Now, set* $C_i = \{f_i + \alpha\mathbf{1} \mid \alpha \in G\}$*, where* f_i *denotes the vector corresponding to the* i*-th row of* H *and* $\mathbf{1}$ *denotes the all-one vector. (We will follow this notation in the sequel examples). For instance,*

$$C_1 = \{(1, 1, 1, 1), (a, a, a, a), (b, b, b, b), (ab, ab, ab, ab)\}.$$

The generalized Hadamard code over U

$$C = C_1 \cup C_2 \cup C_3 \cup C_4$$

can be endowed with a full propelinear structure with the associated group Π *comprised of the following permutations*

$$\pi_x = \begin{cases} Id & x \in C_1 \\ (1,2)(3,4) & x \in C_2 \\ (1,3)(2,4) & x \in C_3 \\ (1,4)(2,3) & x \in C_4 \end{cases}$$

That is, $x \star y = x + \pi_x(y)$ *where* $(C, \star) \simeq \mathbb{Z}_4^2$ *and* $\Pi \simeq \mathbb{Z}_2^2$*. The rank and the dimension of the kernel of this code are 2.*

Example 4.22. *If* $G = \mathbb{Z}_3^2$ *with indexing* $\{(0,0),(0,1),(0,2),(1,0),\ (1,1),\ (1,2),(2,0),(2,1),\ (2,2)\}$*, then the* G*-cocyclic matrix over* $\mathbb{Z}_3$

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \end{pmatrix}$$

is a generalized Hadamard matrix (of Sylvester type), $\mathrm{GH}(3,3)$*, with entries in* $\mathbb{F}_3$*. The generalized Hadamard code over* G

$$C = C_1 \cup C_2 \cup \ldots \cup C_9$$

can be endowed with a full propelinear structure with the associated group Π *comprised of the following permutations*

$$\pi_x = \begin{cases} Id & x \in C_1 \\ (1,2,3)(4,5,6)(7,8,9) & x \in C_2 \\ (1,3,2)(4,6,5)(7,9,8) & x \in C_3 \\ (1,4,7)(2,5,8)(3,6,9) & x \in C_4 \\ (1,5,9)(2,6,7)(3,4,8) & x \in C_5 \\ (1,6,8)(2,4,9)(3,5,7) & x \in C_6 \\ (1,7,4)(2,8,5)(3,9,6) & x \in C_7 \\ (1,8,6)(2,9,4)(3,7,5) & x \in C_8 \\ (1,9,5)(2,7,6)(3,8,4) & x \in C_9 \end{cases}$$

We have $C \simeq \mathbb{Z}_3^3$ *and* $\Pi \simeq \mathbb{Z}_3^2$*. The rank and the dimension of the kernel of this code are 3.*

Example 4.23. *Let $G = U = \mathbb{Z}_2^3$ be with indexing $\{0, 1, x, x^2, x^3, x^4, x^5, x^6\}$ where*

$+$	*0*	*1*	x	x^2	x^3	x^4	x^5	x^6
0	*0*	*1*	x	x^2	x^3	x^4	x^5	x^6
1		*0*	x^3	x^6	x	x^5	x^4	x^2
x			*0*	x^4	1	x^2	x^6	x^5
x^2				*0*	x^5	x	x^3	1
x^3					*0*	x^6	x^2	x^4
x^4						*0*	1	x^3
x^5							0	x
x^5								0

then the G-cocyclic matrix over U

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \\ 0 & x & x^2 & x^3 & x^4 & x^5 & x^6 & 1 \\ 0 & x^2 & x^3 & x^4 & x^5 & x^6 & 1 & x \\ 0 & x^3 & x^4 & x^5 & x^6 & 1 & x & x^2 \\ 0 & x^4 & x^5 & x^6 & 1 & x & x^2 & x^3 \\ 0 & x^5 & x^6 & 1 & x & x^2 & x^3 & x^4 \\ 0 & x^6 & 1 & x & x^2 & x^3 & x^4 & x^5 \end{pmatrix}$$

is a generalized Hadamard matrix, $\mathrm{GH}(8, 1)$*, with entries in $\mathbb{F}_8$. The generalized Hadamard code over G*

$$C = C_1 \cup C_2 \cup \ldots \cup C_8$$

can be endowed with a full propelinear structure with the associated group Π

comprised of the following permutations

$$\pi_x = \begin{cases} Id & x \in C_1 \\ (1,2)(3,5)(4,8)(6,7) & x \in C_2 \\ (1,3)(2,5)(4,6)(7,8) & x \in C_3 \\ (1,4)(2,8)(3,6)(5,7) & x \in C_4 \\ (1,5)(2,3)(4,7)(6,8) & x \in C_5 \\ (1,6)(2,7)(3,4)(5,8) & x \in C_6 \\ (1,7)(2,6)(3,8)(4,5) & x \in C_7 \\ (1,8)(2,4)(3,7)(5,6) & x \in C_8 \end{cases}$$

We have $(C, \star) \simeq \mathbb{Z}_4^3$ *and* $\Pi \simeq \mathbb{Z}_2^3$. *The rank and the dimension of the kernel of this code are 2.*

Example 4.24. *Let* $G = U = \mathbb{Z}_3^4$ *be with indexing* $\{0000, 0001, 0002, 0010, \ldots, 2222\}$, *the irreducible polynomial which defines multiplication in the field is* $2 + x + x^4$ *and let* $\phi_{(4,3)}$ *as in Example 4.1. Then the* G*-cocyclic matrix over* U

$$[H]_{g,h} = \partial\phi_{(4,3)}(g,h)$$

is a generalized Hadamard matrix, $\mathrm{GH}(81,1)$, *with entries in* $\mathbb{F}_{81}$.

$$C = C_1 \cup C_2 \cup \ldots \cup C_{81}$$

can be endowed with a full propelinear structure. The associated group Π *and the matrix* $[H]_{g,h}$ *can be downloaded from ddd.uab.cat/record/204295 [7].*

We have that $(C, \star) \simeq \mathbb{Z}_3^8$ *and* $\Pi \simeq \mathbb{Z}_3^4$. *The rank of this code is* 11 *and the dimension of its kernel is* 1. *Thus,* C *is nonlinear as we knew.*

In Table 4.1, we consider the codes associated to $\partial\phi_{(a,b)}$ of Example 4.1. Let us recall that $\phi_{(a,b)}(g) = g^{(3^b+1)/2}$, with $g \in \mathbb{F}_{3^a}$. Moreover, if $(a,b) = 1$, b odd and $3 \leq b \leq a-1$ then $\partial\phi_{(a,b)}$ are orthogonal cocycles and the associated GHFP-codes $C_{a,b}$ are not linear but are they nonequivalent? that is, fixed a and assuming that b_1 and b_2 with $b_1 \neq b_2$ are admissible values, are C_{a,b_1} and C_{a,b_2} nonequivalent? If the conjecture below were true, we would have an affirmative answer. For instance, for $a = 7$ we have two (cocyclic) $\mathrm{GH}(3^7, 1)$ matrices (one for $b = 3$ and another for $b = 5$) where their codes ($C_{7,3}$ and

$C_{7,5}$) are nonequivalent since they have different rank. Consequently, the GH matrices are nonequivalent as well.

$b\backslash a$	4	5	6	7	8	9	10
3	(11,1)	(11,1)		(11,1)	(11,1)		(11,1)
5			(47,1)	(47,1)	(47,1)	(47,1)	
7					(191,1)	(191,1)	(191,1)
9							(767,1)

Table 4.1: The pairs (r, k) of the entries of this table denote the rank and the dimension of the kernel of the GHFP-codes $C_{a,b}$ associated to $\partial\phi_{(a,b)}$ of Example 4.1.

Let us notice that in Table 4.1, we have computed the rank and dimension of the kernel for all admissible value of b for each a in the range $3 \leq b \leq a-1$ and $4 \leq a \leq 10$. All these computations have been carried out with MAGMA [18]. We prove in Corollary 4.30 that always $k = 1$ and for the rank we conjecture that r depends only on b by $r(b) = 3 \cdot 2^{b-1} - 1$ with b odd.

4.4 Kronecker sum construction

In this section we extend the classical construction of Hadamard codes, based on Kronecker products, to the case of GHFP-codes. As application, we construct an infinite family of nonlinear GHFP-codes for each $\mathrm{GH}(3^a, 1)$ matrix as in Example 4.1. Some properties of their rank and the dimension of their kernel are studied and they have been used to prove their nonlinearity.

The *Kronecker sum construction* [73] is a standard method to construct GH matrices from other GH matrices. That is, if $H = (h_{i,j})$ is any $\mathrm{GH}(w, v/w)$ matrix over U and $B_1,\ B_2, \ldots,\ B_v$ are any $\mathrm{GH}(w, v'/w)$ matrices over U then the matrix

$$H \oplus [B_1, B_2, \ldots, B_v] = \begin{pmatrix} h_{11} + B_1 & \ldots & h_{1v} + B_1 \\ \vdots & \ddots & \vdots \\ h_{v1} + B_v & \ldots & h_{vv} + B_v \end{pmatrix}$$

is a $\mathrm{GH}(w, vv'/w)$ matrix. If $B_1 = B_2 = \ldots = B_v = B$, then we denote $H \oplus [B_1, B_2, \ldots, B_v]$ by $H \oplus B$.

If $\psi \in Z^2(G,U)$ and $\psi' \in Z^2(G',U)$, then their *tensor product* is $\psi \otimes \psi' \in Z^2(G \times G', U)$, where

$$(\psi \otimes \psi')((g,g'),(h,h')) = \psi(g,h)\psi(g',h'),$$

and $M_{\psi\otimes\psi'} = M_\psi \oplus M_{\psi'}$.

Let S_q be the normalized $\mathrm{GH}(q,1)$ matrix given by the multiplicative table of $\mathbb{F}_q$. We can recursively define S^t as a $\mathrm{GH}(q,q^{t-1})$ matrix, constructed as $S^t = S_q \oplus S^{t-1}$ for $t > 1$, (this is an alternative definition for the generalized Sylvester Hadamard matrices). It is well-known that S_q is cocyclic (see [44, p. 122]) and $\mathrm{rank}(C_{S_q}) = \ker(C_{S_q}) = 2$.

Lemma 4.25 ([32, Lemma 3])**.** *Let H_1 and H_2 be two* GH *matrices over $\mathbb{F}_q$ and $H = H_1 \oplus H_2$. Then $\mathrm{rank}(C_H) = \mathrm{rank}(C_{H_1}) + \mathrm{rank}(C_{H_2}) - 1$ and $\ker(C_H) = \ker(C_{H_1}) + \ker(C_{H_2}) - 1$.*

Immediate consequences of the previous result are that

$$\mathrm{rank}(C_{S^l}) = \ker(C_{S^l}) = l + 1.$$

On the other hand, if H_1 is linear and H_2 is not (or vice versa) then $H = H_1 \oplus H_2$ is not linear.

Lemma 4.26 ([32, Corollary 28])**.** *Let H be a $\mathrm{GH}(q,q^{h-1})$ matrix over $\mathbb{F}_q$, with $q > 3$ and $h \geq 1$, or $q = 3$ and $h \geq 2$. Then $\mathrm{rank}(C_H) \in \{h+1, \ldots, \lfloor q^h/2 \rfloor\}$.*

Lemma 4.27 ([32, Proposition 9])**.** *Let H be a $\mathrm{GH}(q,\lambda)$ over $\mathbb{F}_q$, where $q = p^e$ and p prime. Let $v = q\lambda = p^t s$ such that $\gcd(p,s) = 1$. Then $1 \leq \ker(C_H) \leq \ker_p(C_H) \leq 1 + t/e$.*

Lemma 4.28. *Let C be a generalized full propelinear code. Then $\mathcal{K}(C)$ is a subgroup of C.*

Proof. As $\mathbf{0} \in C$, we have that $\mathcal{K}(C)$ is linear. Let x, y be in $\mathcal{K}(C)$, so $\alpha x + C = C$ and $\alpha y + C = C$ for all $\alpha \in \mathbb{F}_q$. Therefore, $\alpha(x \star y) + C = \alpha(x + \pi_x(y)) + x \star C = \alpha x + \alpha\pi_x(y) + x + \pi_x(C) = \alpha x + x + \pi_x(\alpha y + C) = \alpha x + x + \pi_x(C) = \alpha x + x \star C = \alpha x + C = C$, and so $x \star y \in \mathcal{K}(C)$. Thus, the operation $\star$ is closed on $\mathcal{K}(C)$. Since $\mathcal{K}(C)$ is finite and $\mathbf{0} \in C$, we have that $\mathcal{K}(C)$ is a subgroup. $\mathcal{QED}$

Proposition 4.29. *Let H be a* $\mathrm{GH}(3^a, 1)$ *over $\mathbb{F}_{3^a}$ where C_H is a GHFP-code. Then* $\ker(C_H) \in \{1, 2\}$. *If* $\ker(C_H) = 2$, *then C_H is linear. Furthermore, if $a > 1$, then* $\mathrm{rank}(C_H) \geq 2$.

Proof. From Lemma 4.27, we have that $\ker(C_H) \in \{1, 2\}$. We suppose that $\mathcal{K}(C_H) = \langle \mathbf{1}, x \rangle$, for some $x \in C_H$ with $x \neq \alpha\mathbf{1}$ for any $\alpha \in \mathbb{F}_{3^a}$. Since the kernel is a linear subspace of C_H, $\mathcal{K}(C_H) = \{\alpha\mathbf{1} + \beta x \mid \alpha, \beta \in \mathbb{F}_{3^a}\}$. Thus, $|\mathcal{K}(C_H)| = 3^{2a} = |C_H|$. Hence $C_H = \mathcal{K}(C_H)$ and so C_H is linear. From Lemma 4.26, $\mathrm{rank}(C_H) \geq 2$ if $a > 1$. $\mathcal{QED}$

Corollary 4.30. *Let $H = M_{\partial\phi_{(a,b)}}$ be as in Example 4.1. Then the dimension of the kernel of C_H is* 1.

Proof. C_H is a nonlinear GHFP-code by Remark 4.2. $\mathcal{QED}$

Corollary 4.31. *If $q = 3^a$ with $a > 1$, H a* GH *matrix over $\mathbb{F}_q$ where C_H is a nonlinear GHFP-code and $H' = S_q \oplus H$. Then* $\mathrm{rank}(C_{H'}) = \mathrm{rank}(C_H) + 1 > \ker(C_{H'}) = 2$.

Proposition 4.32 ([44, Theorem 6.9])**.** *Let $\psi_i \in Z^2(G_i, U)$, $1 \leq i \leq n$ and $\psi = \psi_1 \otimes \cdots \otimes \psi_n \in Z^2(G_1 \times \cdots \times G_n, U)$. Then ψ is orthogonal if and only if ψ_i is orthogonal, $1 \leq i \leq n$.*

Remark 4.33. *As a consequence of Proposition 4.32, the Sylvester generalized Hadamard matrix S^l is cocyclic.*

Proposition 4.34. *Let B_1 be a* $\mathrm{GH}(w, v/w)$ *matrix over U and B_2 be a* $\mathrm{GH}(w, v'/w)$ *matrix over U. If C_{B_1} and C_{B_2} are GHFP-codes, then C_H is a GHFP-code too where $H = B_1 \oplus B_2$. Moreover,*

$$\pi_{a\oplus b}(x \oplus y) = \pi_a(x) \oplus \pi_b(y),$$
$$(a \oplus b) \star (x \oplus y) = (a \star x) \oplus (b \star y).$$

where $a = (a_1, a_2, \ldots, a_v)$, $b = (b_1, b_2, \ldots, b_{v'})$ and $a \oplus b = (a_1 + b_1, \ldots, a_1 + b_{v'}, a_2 + b_1, \ldots, a_2 + b_{v'}, \ldots, a_v + b_1, \ldots, a_v + b_{v'})$ are rows in B_1, B_2 and H, respectively; $x \in C_{B_1}$ and $y \in C_{B_2}$.

Proof. By Corollary 4.19, we have that $B_i = M_{\psi_i}$ for $\psi_i \in Z^2(G_i, U)$ for a specific ordering of the elements of G_i (for the rest of this proof, we are

assuming fixed this ordering in G_i) with $i = 1, 2$. Now, using Proposition 4.32, we have $H = M_{\psi_1} \oplus M_{\psi_2} = M_{\psi_1 \otimes \psi_2}$ for $\psi_1 \otimes \psi_2 \in Z^2(G_1 \otimes G_2, U)$ which is orthogonal, i.e., H is a cocyclic $\mathrm{GH}(w, vv'/w)$. Therefore, C_H is a GHFP-code by Proposition 4.17.

Now, assume that a (resp. b) corresponds with a row of B_1 (resp. B_2) indexed with the element $g \in G_1$ (resp. $h \in G_2$). By the proof of Proposition 4.17, we have $\pi_a(l) = i \Leftrightarrow g_l = gg_i$ and $\pi_b(m) = j \Leftrightarrow h_m = hh_j$, where $g_j \in G_1$ and $h_j \in G_2$. For the same reason, $\pi_{a \oplus b}((l-1)v + m) = (i-1)v + j \Leftrightarrow (g_l, h_m) = (g, h)(g_i, h_j)$. Therefore, $\pi_{a \oplus b}(x \oplus y) = \pi_a(x) \oplus \pi_b(y)$. Finally, as a direct consequence, we conclude with the desired result $(a \oplus b) \star (x \oplus y) = (a \star x) \oplus (b \star y)$. $\mathcal{QED}$

Corollary 4.35. *Let $\partial\phi_{(a,b)}$ be as in Example 4.1. Then C_H are nonlinear GHFP-codes where $H = S^l \oplus M_{\partial\phi_{(a,b)}}$ are $\mathrm{GH}(3^a, 3^{al})$ matrices with $S = S_{3^a}$, for all $l \geq 1$. Moreover,* $\ker(H) = l + 1 < \mathrm{rank}(H)$.

Chapter 5

Quasi-Hadamard full propelinear codes

"Ignoranti, quem portum petat, nullus suus ventus est."

Lucius Annaeus Seneca.

In 2018, Armario and Flannery [9] started the study of the existence, classification and combinatorics of quasi-orthogonal cocycles. For instance, equivalences with relative quasi-difference sets, quasi-Hadamard groups, and certain partially balanced incomplete block designs, afforded by the analogy with orthogonal cocycles, have been found. Keeping with the analogy, in this chapter we give a characterization of quasi-orthogonal cocyles in terms of propelinear codes. Furthermore, some structural properties of these codes are studied.

5.1 Quasi orthogonal cocycles

The Hadamard (maximal) determinant problem asks for the largest $n \times n$ determinant with entries ± 1. This is an old question which remains unanswered in general. Throughout this chapter, for convenience, when we say determinant of a matrix we mean the absolute value of the determinant. Let M be a $(-1, 1)$-matrix of order n. We call M a *D-optimal design* if the determinant of M is the maximum determinant among all $(-1, 1)$-matrices of order n, (i.e., $\det(M)$ is a solution of the Hadamard determinant problem). Hadamard showed in [40] that $n^{n/2}$ was an upper bound for the determinant of an

$n \times n$ D-optimal design. This bound can be attained only if $n = 1, 2$ or n is a multiple of 4. Recall that a matrix that attains it is called a Hadamard matrix, and it is an outstanding conjecture that one exists for any multiple of 4. Hadamard's inequality can be improved if we restrict to matrices whose orders are not divisible by 4. Indeed, if $n \equiv 2 \mod 4$ and $n \neq 2$, Ehlich [35] and independently Wojtas [79] proved that

$$\det(M) \leq (2n-2)(n-2)^{\frac{1}{2}n-1}, \tag{5.1}$$

and, moreover, there exists a $(-1,1)$-matrix achieving equality in (5.1) if and only if there exists a $(-1,1)$-matrix B of order n such that

$$BB^\top = B^\top B = \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}, \tag{5.2}$$

where $L = (n-2)I+2J$. The symbols I and J will (respectively) always denote the identity matrix and the all-ones matrix; the order of each matrix will be clear from the context in which it is used. A $(-1,1)$-matrix of order n is called an *EW matrix* if it satisfies (5.2) (or more generally, when its determinant reaches the bound in (5.1)). Clearly Hadamard matrices and EW matrices are D-optimal designs. Note that it is known that EW matrices exist only if $2(n-1)$ is the sum of two squares, a condition which is believed to be sufficient (order 198 is the lowest for which the question has not been settled yet, [31]). The interested reader is addressed to [53] for further information on what is known about maximal determinants.

Example 5.1. *The following matrix is a EW matrix of order* 10.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \end{pmatrix}. \tag{5.3}$$

In the early 1990s, de Launey and Horadam discovered *cocyclic development of pairwise combinatorial designs.* This discovery opened up a new area in design theory, that emphasizes algebraic methods drawn mainly from group theory and cohomology. Cocyclic construction has been successfully used for Hadamard matrices [44] and, more recently, for EW matrices [2, 3]. In this context, the notions of orthogonal (resp. quasi-orthogonal) cocycles associated to cocyclic Hadamard (resp. EW) matrices arose naturally.

Let G and U be finite groups, with U abelian. Let $\psi \in Z^2(G,U)$ and assume that ψ is normalized, i.e., $\psi(1,1) = 1$. Our principal focus in this chapter is the case $U = \langle -1 \rangle \simeq \mathbb{Z}_2$. Recall that ψ is orthogonal if M_ψ is a Hadamard matrix, i.e., $M_\psi M_\psi^\top = M_\psi^\top M_\psi = nI_n$, where $n = |G|$. For $n \equiv 2 \mod 4$ we say that ψ is *quasi-orthogonal* if M_ψ satisfies

$$\mathrm{abs}(M_\psi M_\psi^\top) = \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix} \tag{5.4}$$

up to row permutation, where $\mathrm{abs}(M)$ denotes the matrix $(|m_{ij}|)$ for $M = (m_{ij})$. By (5.2) it follows that any cocyclic EW matrix is quasi-orthogonal, but the reciprocal does not hold (i.e., not every quasi-orthogonal cocyclic matrix is an EW matrix). Moreover, [9, Remark 6] claims that if ψ is quasi-orthogonal then $M_\psi M_\psi^\top = M_\psi^\top M_\psi$.

When $|G| = 4t+2$ and $\psi \in Z^2(G, \langle -1 \rangle)$ is a coboundary then the identity (5.4) never holds [9, Prop 2.5.]. We say that ψ *is a quasi-orthogonal coboundary*

if M_ψ satisfies

$$\mathrm{abs}(M_\psi M_\psi^\top) = L. \tag{5.5}$$

up to row permutation. As far as we are aware, quasi-orthogonal coboundaries are only known over abelian groups and the dihedral group of six elements. In this case, $M_\psi M_\psi^\top = M_\psi^\top M_\psi$.

5.2 QHFP-codes

In this section we introduce the notion of quasi-Hadamard full propelinear codes and their equivalence with quasi-Hadamard groups is studied.

Definition 5.2. *A quasi-Hadamard matrix of order $4t+2$ is a normalized square matrix M of order $4t+2$ with entries from the set $\{-1,1\}$, with the property such that*

$$\mathrm{abs}(MM^\top) = \mathrm{abs}(M^\top M) = \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix} \tag{5.6}$$

up to row and column permutation, where $L = 4tI + 2J$.

Clearly, EW matrices are quasi-Hadamard matrices but not every quasi-Hadamard matrix is a D-optimal design. In Definition 5.2, M is said to be an *extremal* quasi-Hadamard matrix when $\mathrm{abs}(MM^\top) = \mathrm{abs}(M^\top M) = L$, where $L = 4tI + 2J$.

The matrix obtained from a quasi-Hadamard matrix, by replacing all 1's by 0's and all -1's by 1s, is called *binary quasi-Hadamard matrix*. The binary code consisting of the rows of a binary quasi-Hadamard matrix and their complements is called a *quasi-Hadamard* code, which is of length $4t+2$ and with $8t+4$ codewords. Since M is normalized, $\mathbf{0}$ and $\mathbf{1}$ are always codewords.

Proposition 5.3. *The minimum distance of a quasi-Hadamard code C of length $4t+2$ is $2t$.*

Proof. By (5.4), the inner product $x \cdot y$ is 0 or ± 2, where x, y are different rows of M (a binary quasi-Hadamard matrix associated to C). If $x \cdot y = 0$ then $d(x,y) = 2t+1$, if $x \cdot y = 2$ then $d(x,y) = 2t$, and if $x \cdot y = -2$ then $d(x,y) = 2t+2$. As $d(x,y) = 4t+2-d(x,y+u)$, then $d(x,y) \in \{2t, 2t+1, 2t+2, 4t+2\}$ for any $x, y \in C$ with $x \neq y$. $\mathcal{QED}$

The set of distances in a quasi-Hadamard code of length $4t+2$ is the same as in a Hadamard code of length $4t+4$ after puncturing two coordinates. The number of codewords in the above codes is $8t+4$ and $8t+8$, respectively. Hence, from an error-correction point of view it is slightly better the 2-punctured Hadamard code. However, quasi-Hadamard codes can be seen as a good alternative to 2-punctured Hadamard codes in that cases when we do not know about the existence of a Hadamard code of length $4t+4$.

From a Hadamard code we can always obtain a quasi-Hadamard code by puncturing twice. Let say M is a normalized Hadamard matrix of length n and fix any two different columns (also different from the first one). It is well known the design structure of M and so, in this case, the projection of the row vectors of M over these two fixed coordinates gives exactly $n/4$ times each one of the vectors $(1,1),(-1,-1),(-1,1),(1,-1)$. Puncturing these fixed two columns and removing any pair of rows such that its projection over the two punctured coordinates give two orthogonal vectors, we obtain a quasi-Hadamard matrix. However, the reciprocal is not true. It is easy to see that the quasi-Hadamard matrix in eq. (5.3) could not be extended to a Hadamard matrix. Indeed, adding two columns to that matrix the two coordinates added to the second row should be $(1,1)$ to have this row orthogonal to the first one; also the two coordinates added to the third row should be $(1,1)$ to have this row orthogonal to the first one; but now the new second and third rows are not orthogonal.

An interesting bound which Hadamard codes fit is the so called Grey-Rankin bound, applicable only to self-complementary codes to check its optimality. The quasi-Hadamard codes do not attain this bound. For a (n,M,d)-code the bound states that

$$M \leq \frac{8d(n-d)}{n-(n-2d)^2}$$

and in the case of the quasi-Hadamard code, we have a $(4t+2, 8t+4, 2t)$-code which is almost optimal taking into account the Grey-Rankin bound as it is easy to see. The left part of the inequality is $M = 8t+4$ and the right part is $8t+4+(8+\frac{12}{2t-1})$.

A quasi-Hadamard code, which is also full propelinear, is called *quasi-Hadamard full propelinear code* (briefly, QHFP-code). Now we present the analogous of Lemma 2.2 which is proven for Hadamard codes in [67, Lemma

6]. We note that the same proof is valid for quasi-Hadamard codes.

Lemma 5.4. *Let C be a quasi-Hadamard code of length $4t+2$. The rank r of C fulfils*

$$r \leq \frac{8t+4}{2^k} + k - 1,$$

where k is the dimension of the kernel.

Henceforth, we will assume that E is a finite (multiplicatively written) group of order $2n$ with identity e and normalized transversal T for a central subgroup $\langle u \rangle \simeq \mathbb{Z}_2$. We recall that this implies in particular that:

- T and uT are disjoints and $T \cup uT = E$.
- aT and $\{b, bu\}$ intersect exactly in one element, for any $a, b \in E$.

Now, we state a technical result that we will need later.

Lemma 5.5. *Let $a, b \in E$ and $A = [T \setminus (a(T \cup bT) \cap T)] \cup [a(T \cap bT) \cap T]$. Then,*

(i) $x \in T \cap bT \Rightarrow$ *either* $ax \in A$ *or* $axu \in A$.

(ii) $x \in A \Rightarrow$ *either* $a^{-1}x \in T \cap bT$ *or* $a^{-1}xu \in T \cap bT$.

As a consequence, we have $|T \cap bT| = |A|$.

Proof.

(i) $x \in T \cap bT \Rightarrow ax \in a(T \cap bT)$. Now, we have to possibilities:

- If $ax \in T$, then $ax \in a(T \cap bT) \cap T$. Thus, $ax \in A$.
- If $ax \notin T$, then $axu \in T$. Taking into account that $ax \in aT \wedge ax \in abT$ and T is a transversal (the second property above), we have $axu \notin aT \cup abT$. Thus, $axu \in T \setminus (a(T \cup bT) \cap T)$. Hence, $axu \in A$.

(ii) Follows by a similar argument.

$\mathcal{QED}$

For a fixed order in $T = \{t_1 = e, t_2, \ldots, t_n\}$ and given an element $a \in E$, we can define a n-vector $v_a \in \mathbb{F}^n$ in the following manner:

$$[v_a]_k = \begin{cases} 0 & a^{-1}t_k \in T, \\ 1 & \text{otherwise} \end{cases}$$

where $[v_a]_k$ denotes the k-th coordinate of v_a and

$$C_E = \{v_a \in \mathbb{F}^n \mid a \in E\}.$$

Let us point out that v_e is the all-zeros vector and v_u is the all-ones vector.

The next result follows immediately.

Lemma 5.6. *Let $b \in E$, the set of positions where the vector v_b has a 0 entry is given by $T \cap bT$ (i.e., $t_k \in T \cap bT \Leftrightarrow [v_b]_k = 0$).*

In the sequel, our main goal will be to endow C_E with a propelinear structure using the transversal T, the central subgroup $\langle u \rangle$ and the law group of E. The first step consists of finding a suitable permutation $\pi_{v_a} \in \mathcal{S}_n$ associated to an element $a \in E$. For any $b \in E$ define $\pi_{v_a}(v_b) = v_a + v_{ab}$ where $+$ is the componentwise addition in $\mathbb{F}^n$. At this moment, it is not obvious that $\pi_{v_a}(v_b)$ has the same weight as v_b and even if it did, this might not define a unique permutation. Before trying to clarify this point, we will point out that if $\pi_{v_a} \in \mathcal{S}_n$ for any $a \in E$ then $(C_E, \star)$ with $v_a \star v_b = v_a + \pi_{v_a}(v_b)$ is isomorphic to E as a group since $v_a \star v_b = v_{ab}$ by the definition of π_{v_a}. Furthermore,

Lemma 5.7. *Let $a, b \in E$ then $\pi_{v_a}\pi_{v_b} = \pi_{v_a \star v_b}$.*

Proof. For any $c \in E$, we have

$$\begin{aligned} \pi_{v_a \star v_b}(v_c) = &\ \pi_{v_{ab}}(v_c) = v_{ab} + v_{(ab)c} = v_a + \pi_{v_a}(v_b) + v_{a(bc)} \\ = &\ v_a + \pi_{v_a}(v_b) + v_a + \pi_{v_a}(v_{bc}) = \pi_{v_a}(v_b + v_{bc}) = \pi_{v_a}\pi_{v_b}(c) \end{aligned}$$

$\mathcal{QED}$

By abuse of notation, from now on we will use the same symbol a to denote v_a. Similarly, for the underlying set of the group E and C_E. The meaning of a (resp. E) will be clear from the context in which it is used.

In the sequel, for any $a, b \in E$ some properties of the map $\pi_a(b)$ (defined above) are studied.

Lemma 5.8. *Let a, b and A as in Lemma 5.5. Then,*

$$[\pi_a(b)]_k = \begin{cases} 1 & t_k \notin A, \\ 0 & t_k \in A. \end{cases}$$

Proof. To check the value of the k-th coordinate of $\pi_a(b)$, we have to compute $[a]_k + [ab]_k \mod 2$. Therefore, $[\pi_a(b)]_k = 0$ if and only if $[a]_k = [ab]_k$. Now, applying the definition of $[a]_k$ and Lemma 5.5, we conclude with the desired result. $\mathcal{QED}$

Taking into account $|A| = |T \cap bT|$ and Lemmas 5.6 and 5.8, it is proved that $\pi_a(b)$ has the same weight as b. Moreover, the following result guarantees the π_a is a permutation depending only on a.

Proposition 5.9. *The map π_a is an element of $\mathcal{S}_n$. Specifically, for any b, π_a moves the k-th coordinate of b to the h-th coordinate where*

$$t_h = \begin{cases} at_k & at_k \in T, \\ at_k u & otherwise. \end{cases}$$

Proof. We have that $[\pi_a(b)]_h = [a]_h + [ab]_h \mod 2$. It is straightforward to check that $[\pi_a(b)]_h = [b]_k$. $\mathcal{QED}$

Remark 5.10. *Let us observe that $at_k = t_h$ if $a = e$ and $at_k u = t_h$ if $a = u$. Hence, the permutation π_a does not fix any coordinate for all $a \in E \setminus \{e, u\}$ and $\pi_e = \pi_u = Id$.*

We can always assume without loss of generality that the elements of T are ordered in such a way so, $\pi_{t_k}(e_k) = e_1$ where e_k is the unitary vector with only one nonzero coordinate at the position k-th. A justification of the fact that $\pi_a(e_k) \neq \pi_b(e_k)$ for all $a, b \in T$ with $a \neq b$ is given in the proof of Theorem 5.16.

It is known in [67] that if E is a Hadamard group then the permutations of Proposition 5.9 yields a full propelinear structure on the Hadamard code C_E. From now on, we will deal with the case E being a quasi-Hadamard group and we will obtain the analog result.

Definition 5.11 (Armario and Flannery [9]). *Let E be a group of order $8t+4 \geq 12$ with central subgroup $Z = \langle u \rangle \simeq \mathbb{Z}_2$. We say that E is a quasi-Hadamard group if there exists a transversal T for Z in E of size $4t+2$ containing a subset $S \subset T \setminus Z$ of size $2t+1$ such that*

$$|T \cap xT| = \begin{cases} 2t+1 & x \in S, \\ 2t \text{ or } 2t+2 & x \in T \setminus (S \cup Z). \end{cases} \tag{5.7}$$

The transversal T is called a quasi-Hadamard subset of E. It may be assumed that $e \in T$.

Remark 5.12. *In [9, Thm 3.2], Armario and Flannery showed that quasi-orthogonal cocycle and quasi-Hadamard group are essentially the same concept.*

Let Q_{8t+4} denote the dicyclic group with presentation

$$\langle a, b \mid a^{2t+1} = b^2,\ b^4 = e,\ b^{-1}ab = a^{-1} \rangle.$$

This family provides good candidates for quasi-Hadamard groups. For instance, $T = \{e, a, a^2, b, ab, a^2b\}$ is a quasi-Hadamard subset of Q_{12}. Furthermore, in [9] it has been conjectured that Q_{8t+4} is always a quasi-Hadamard group. It can be seen as the analog of Ito's conjecture for Hadamard groups (Conjecture 2.35).

We say that a quasi-Hadamard group E is *extremal* when in Definition 5.11 the subset S is the empty set, i.e, $S = \emptyset$. Quasi-orthogonal coboundary and extremal quasi-Hadamard group are also essentially the same concept.

The following example will be useful in the proof of Proposition 5.14.

Example 5.13 ([52, Chapter 2]). *Suppose that E is a finite group with normalized transversal T for a central subgroup $U = \langle -1 \rangle \simeq \mathbb{Z}_2$, i.e., $|xT \cap yU| = 1$ for any $x, y \in E$. Put $G = E/\langle -1 \rangle$ and $\sigma(t\langle -1 \rangle) = t$ for $t \in T$. The map $\psi_T : G \times G \to \langle -1 \rangle$ defined by*

$$\psi_T(g,h) = \sigma(g)\sigma(h)\sigma(gh)^{-1} = \begin{cases} 1 & \sigma(g)\sigma(h) \in T, \\ -1 & \text{otherwise} \end{cases}$$

is a cocycle.

Proposition 5.14. *Let E be a quasi-Hadamard group and $T = \{t_1 = e, t_2, \ldots, t_n\}$ be a quasi-Hadamard subset of E. Then E is a quasi-Hadamard code with*

$$[H(T)]_{i,j} = \begin{cases} 0 & t_i^{-1}t_j \in T, \\ 1 & \textit{otherwise} \end{cases}$$

as a binary quasi-Hadamard matrix (up to normalization).

Proof. Let us point out that the codewords of E are the rows of the following $(0,1)$-matrices $H(T)$ and $\overline{H(T)}$ where $H(T) + \overline{H(T)} = J$.

Let $\psi_T \in Z^2(E/\langle u\rangle, \langle -1\rangle)$ be as in Example 5.13. By [9, Thm 3.2],

$$[M_{\psi_T}]_{i,j} = \begin{cases} 1 & t_i t_j \in T, \\ -1 & \text{otherwise} \end{cases}$$

is a quasi-orthogonal cocyclic matrix. Hence, the matrices M_{ψ_T} and $M_{\psi_T}^\top$ satisfies (5.4).

Now, let us observe that the binary version of M_{ψ_T} is equivalent to $H(T)$. Normalizing (i.e., taking the complement of the rows starting by 1 in $H(T)$) we get the binary version of M_{ψ_T} up to rows permutation, due to the fact that if $a \in E$ then $a \in T$ or $au \in T$ and v_a is the complement of v_{au}. Therefore, E is a quasi-Hadamard code with $H(T)$ as a binary quasi-Hadamard matrix up to normalization. $\mathcal{QED}$

Now, we can define a propelinear structure on E by $a \star b = a + \pi_a(b) = ab$. Finally, as an immediate consequence of the previous results above we have the following theorem.

Theorem 5.15. *Let E be a quasi-Hadamard group and $T = \{t_1 = e, t_2, \ldots, t_n\}$ be a quasi-Hadamard subset of E. Then $(E, \star)$ is a quasi-Hadamard full propelinear code.*

Proof. From Proposition 5.14, we have that E is a quasi-Hadamard code. Now, let's see that E has a propelinear structure. For each $x \in E$, we define $\pi_x(y) = x + xy$ for any $y \in E$. From Proposition 5.9, $\pi_x \in \mathcal{S}_n$ for every $x \in E$. For any $x, y \in E$, $x + \pi_x(y) = x + x + xy = xy \in E$, and by Lemma 5.7 $\pi_x\pi_y = \pi_{xy} = \pi_{x+\pi_x(y)}$. Thus $(C, \star)$ is a propelinear code, which is full by Remark 5.10. $\mathcal{QED}$

In the next result, we will show that the converse statement holds. An analogous version for Hadamard full propelinear codes appears in [66].

Theorem 5.16. *Let E be a quasi-Hadamard full propelinear code of length $4t+2$. Then E is a quasi-Hadamard group of order $8t+4$.*

Proof. Define T_1 to be the subset of E consisting of codewords with first coordinate equal to zero. Let u denotes the codeword $\mathbf{1}$. It is easy to check that

- $T_1 \cap uT_1 = \emptyset$ and $T_1 \cup uT_1 = E$.
- aT_1 and $\{b, bu\}$ intersect exactly in one element, for any $a, b \in E$.
- $\langle u \rangle \simeq \mathbb{Z}_2$ is a central subgroup of E.

We associate to each codeword in $x \in T_1$, the integer k_x such that $\pi_x^{-1}(e_1) = e_{k_x}$. Let us point out that if $x, y \in T_1$ and $x \neq y$ then $k_x \neq k_y$. Indeed, if $k_x = k_y$ then $e_1 = \pi_x \pi_y^{-1}(e_1) = \pi_x \pi_{y^{-1}}(e_1) = \pi_{xy^{-1}}(e_1)$. Now, taking into account that E is full then $xy^{-1} = e$ or $xy^{-1} = u$. Hence, $x = y$ or $\{x, y\}$ is not a subset of T_1. As a consequence, k_x ranges over all the integers between 1 and $4t+2$ when x moves in T_1.

Let H be the binary quasi-Hadamard matrix associate to E where the k_x-th row of H corresponds with the codeword x. It is straightforward to check that

$$[H]_{k_x,k_y} = 0 \quad \text{if and only if} \quad y \star x \in T_1.$$

As a consequence,

$$\begin{aligned} |T_1 \cap T_1\, x| &= \text{number of zeros of the } k_x\text{-th row of } H. \\ |T_1 \cap x\, T_1| &= \text{number of zeros of the } k_x\text{-th colum of } H. \end{aligned}$$

Let S be the set of columns of H where their number of zeros is equal to $2t+1$.

Since the $(-1, 1)$ version of H satisfies (5.4), then

- $|T_1 \cap x\, T_1| = \begin{cases} 2t+1 & x \in S, \\ 2t \text{ or } 2t+2 & x \in T \setminus (S \cup \langle u \rangle). \end{cases}$
- $|S| = 2t+1$.

Obviously, $S = \emptyset$ when H is extremal. $\mathcal{QED}$

Finally, we have studied the allowable values for the rank and for the dimension of the kernel of these codes.

Proposition 5.17. *Let E be a quasi-Hadamard full propelinear code of length $4t+2$. Then*

(i) $\dim(\mathcal{K}(E)) = k \leq 2$.

(ii) If $k = 1$, then $\mathcal{K}(E) = \langle \mathbf{1} \rangle$, and $r \leq 4t+2$.

(iii) If $k = 2$, then $\mathcal{K}(E) = \langle \mathbf{1}, s \rangle$, with $\mathrm{wt}(s) = 2t+1$, $s^2 \in \langle \mathbf{1} \rangle$, and $r \leq 2t+2$.

Proof. It is trivial that $\mathbf{1} \in K(E)$. Let $s \neq \mathbf{1}$ be a codeword in $\mathcal{K}(E)$, then $s + x \in E$ for any $x \in E$. Suppose $\mathrm{wt}(s) \in \{2t, 2t+2\}$, then for each $x \in E$ with $\mathrm{wt}(x) = 2t+1$, we have $\mathrm{wt}(s+x) = 2t+1$.

Note that we have an odd amount of rows of H (the quasi-Hadamard matrix associated to E) with weight equal to $2t+1$ because the $(-1, 1)$ version of H satisfies (5.6). Thus, there are $4t+2$ codewords with weight equal to $2t+1$. As $\mathbf{1} \in \mathcal{K}(E)$, we need to distribute the codewords with weight equal to $2t+1$ in sets of four elements, $\{x, x+s, x+\mathbf{1}, x+s+\mathbf{1}\}$, then there is a contradiction. Thus $\mathrm{wt}(s) = 2t+1$ for each codeword in $\mathcal{K}(E) \setminus \langle \mathbf{1} \rangle$.

Let s_1, s_2 be two different codewords in $\mathcal{K}(E)$ and $s_1 \neq s_2 + \mathbf{1}$. Since $\mathcal{K}(E)$ is a linear subspace, $s_1 + s_2 \in \mathcal{K}(E)$, but $\mathrm{wt}(s_1 + s_2)$ is $2t$ or $2t+2$. Then $\mathcal{K}(E)$ is at most $\langle \mathbf{1}, s \rangle$ where s is a codeword with $\mathrm{wt}(s) = 2t+1$. Also $s^2 = s + \pi_s(s) \in \mathcal{K}(E)$, but the unique possibility is that s^2 is $\mathbf{1}$ or $\mathbf{0}$.

The bounds for the rank are immediately from Lemma 5.4. $\mathcal{QED}$

5.3 Examples

In this section, we provide some examples of quasi-Hadamard full propelinear codes coming from quasi-Hadamard groups.

Example 5.18. *Let* $Q_{12} = \langle a, b \mid a^3 = b^2, b^4 = e, b^3ab = a^5 \rangle$ *be a dicyclic group of order 12. We have that* $Q_{12} = \{e, a, a^2, a^3, a^4, a^5, b, ab,\ a^2b, a^3b, a^4b, a^5b\}$. *Let* $T = \{e, a, a^2, b, ab, a^2b\}$ *be a transversal,* $Z = \langle a^3 \rangle$, *where* $a^3 = b^2$ *is an involution, and* $S = \{b, ab, a^2b\}$. *Therefore, the quasi-Hadamard matrix associated to* T *is*

$$H(T) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Thus, the generators of the QHFP-code are

$$a = (1, 0, 0, 1, 0, 0)\,,$$
$$b = (1, 0, 0, 0, 1, 1)\,,$$

and the permutations are

$$\pi_a = (1, 2, 3)(4, 5, 6),$$
$$\pi_b = (1, 4)(2, 6)(3, 5).$$

Note that $a^3 = b^2 = \mathbf{1}$. *With these values, the relation* $b^3ab = a^5$ *is fulfilled. The rank of this code is* 4 *and the dimension of its kernel is* 2, $\mathcal{K}(Q_{12}) = \langle \mathbf{1}, a^2b \rangle$.

Example 5.19. *Let* $E = \{a, b \mid a^6 = b^2 = e, ab = ba\} \simeq \mathbb{Z}_6 \times \mathbb{Z}_2$. *Let* $T = \{e, a, a^2, b, a^4b, a^5b\}$ *be a transversal,* $Z = \langle a^3 \rangle$ *where* a^3 *is an involution, and* $S = \emptyset$. *Therefore, the quasi-Hadamard matrix associated to* T *is*

$$H(T) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Thus, the generators of the QHFP-code are

$$a = (1, 0, 0, 0, 1, 0)\,,$$
$$b = (0, 1, 1, 0, 1, 1)\,,$$

and the permutations are

$$\pi_a = (1, 2, 3)(4, 5, 6),$$
$$\pi_b = (1, 4)(2, 5)(3, 6).$$

Note that $a^3 = \mathbf{1}$. *The rank of this code is* 5 *and the dimension of its kernel is* 1, $\mathcal{K}(E) = \langle u \rangle$.

Example 5.20. *Let* $E = \{a \mid a^{12} = e\} \simeq \mathbb{Z}_{12}$. *Let* $T = \{e, a, a^2, a^9, a^{10}, a^5\}$ *be a transversal,* $Z = \langle a^6 \rangle$ *where* a^6 *is an involution and* $S = \{a, a^9, a^5\}$. *Therefore, the quasi-Hadamard matrix associated to* T *is*

$$H(T) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Thus, the generator of the QHFP-code is

$$a = (1, 0, 0, 1, 0, 1)\,,$$

and the permutation is

$$\pi_a = (1, 2, 3, 4, 5, 6).$$

Note that $a^6 = \mathbf{1}$. *The rank of this code is* 6 *and the dimension of its kernel is* 1, $\mathcal{K}(E) = \langle \mathbf{1} \rangle$.

Remark 5.21. *We note that the values of the rank and the dimension of the kernel obtained in the above examples tell us that the codes are nonlinear. In the case of Hadamard full propelinear codes with length* 4 *and* 8 *do not appear nonlinear codes. When the length is* 4 *the HFP-codes have rank and dimension of the kernel equal to* 3, *and in the case of length* 8 *the rank and the dimension of the kernel are* 4.

Chapter 6

Conclusions

"I didn't say it would be easy, Neo. I just said it would be the truth."

Morpheus. The Matrix.

The core objective of this thesis has been to deepen into the study of error-correcting codes endowed with a propelinear structure. Along this dissertation we have endowed with a full propelinear structure several codes such as binary Hadamard codes, generalized Hadamard codes, and quasi-Hadamard codes. This structure bring us a way to generate codes from a few codewords, even if the code is nonlinear. The study of codes with an algebraic structure is a fruitful path to generate infinite families of codes. In general, all codes introduced in this thesis are nonlinear. Therefore, we have analyzed the allowable values of the rank and dimension of the kernel. In some cases, we have obtained bounds for these values, but in others we have determined the precise values. Moreover, we have generalized to finite fields the full propelinear structure introduced by Rifà and Suárez in [66] for binary Hadamard codes.

6.1 Summary of results

"Discutiremos el concepto con el fin de discutirlo."

Pazos. Airbag.

In Table 6.1 we summarize the results of Chapter 3. The table shows the allowable values of the rank and the dimension of the kernel for nonlinear

Hadamard full propelinear codes of length $4t$ with $\Pi = C_{2t} \times C_2$ or $\Pi = C_t \times C_2 \times C_2$. When the parameter t is odd, then there only exist codes with a group structure isomorphic to $C_t \times Q$. This group is not abelian, but this property seems that is not the key of the existence in the odd case. Indeed, the HFP$(t, D_{\mathbf{1}})$-codes are also nonabelian, but they only exist when t is even.

HFP$(\cdot,\cdot,\cdot)$	t	r	k
$(4t_{\mathbf{1}}, 2)$	even	$\leq 2t$	1
$(2t, 2, 2_{\mathbf{1}})$	even square	$\leq 2t$	$1, 2, 3$
$(2t, 4_{\mathbf{1}})$	even	$\leq 2t$	$1, 2, 3$
$(t, 2, 2, 2_{\mathbf{1}})$	even square	$\leq 2t$	$1, 2, 3$
$(t, 4_{\mathbf{1}}, 2)$	even	$\leq 2t$	$1, 2, 3, 4$
$(2t_{\mathbf{1}}, 2, 2)$	even	$\leq 2t$	$1, 2, 3$
$(t, Q_{\mathbf{1}})$	odd	$4t - 1$	1
	even	$\leq 2t$	$1, 2, 3$
$(t, D_{\mathbf{1}})$	even	$\leq 2t$	$1, 2, 3, 4$

Table 6.1: Allowable values of the rank r, and dimension of the kernel k for nonlinear HFP$(\cdot,\cdot,\cdot)$-codes of length $4t$.

Attending to the results obtained in Chapter 3, we propose the following conjecture.

Conjecture 6.1. *Let C be a Hadamard full propelinear code of length $4t$ with generators g_i and associated permutations π_{g_i} which are products of j_i-cycles, with $i \in \{1, \ldots, n\}$ and $j_i \in \{2, \ldots, 2t\}$. Let j_k be the maximum of $\{j_1, \ldots, j_n\}$. The dimension of the kernel of C is bounded by*

$$k \leq 2 + \log_2(4t/j_k).$$

Note that the codes studied in Section 3.1 have $2t$-cycles, so $k \leq 3$, and the codes presented in Section 3.2 have t-cycles, so $k \leq 4$.

In Chapter 4 we have studied codes based on cocyclic generalized Hadamard matrices. In Proposition 4.6, we have characterized the propelinear structure of a q-ary code C depending on the existence of a regular subgroup in $\mathrm{Aut}(C)$ acting transitively on C. This result extends the one for binary codes (see Proposition 2.5). In Definition 4.7 we have introduced the full propelinear structure for q-ary codes, and subsequently the generalized Hadamard full propelinear codes. In Section 4.2, we have proved several results to establish

the connection between generalized Hadamard full propelinear codes and the cocyclic generalized Hadamard matrices. Furthermore, Proposition 4.18 gives the equivalence between GHFP-codes and central relative difference sets. In Proposition 4.34, we have showed a construction of GHFP-codes from two GHP-codes, giving explicitly the structure. Making use of this construction, in Corollary 4.35 we have provided an example of an infinite family of nonlinear GHFP-codes.

In Chapter 5 we have introduced quasi-Hadamard full propelinear codes. In Theorems 5.15 and 5.16, we have proved the equivalence between quasi-Hadamard groups and QHFP-codes. In Remark 5.21 we have noted that there exist nonlinear full propelinear codes based on quasi-Hadamard matrices for lower length than based on Hadamard matrices. In Proposition 5.17, we have established that the dimension of the kernel of any nonlinear QHFP-code is lower than or equal to 2.

6.2 Future work

"But once we pass that windmill, it's the future or bust."

Doc. Back to the future. Part III.

To conclude, we propose several research problems that have arisen as a consequence of the work carried out in this thesis.

In Remark 2.18 we say that a linear code could have a full propelinear structure, but there is not clear when a linear code have it. There would be interesting to study invariants of linear codes to determine when they have a full propelinear structure.

Research problem 1. Characterize when a linear code has a full propelinear structure.

We also could try to solve this in general.

Research problem 2. Characterize when a code has a full propelinear structure.

There could be useful to benefit from the structure of the permutations associated to the generators of an HFP-code in order to establish a bound for the dimension of the kernel, as Conjecture 6.1 proposes.

Research problem 3. Solve the Conjecture 6.1.

To build a family of nonequivalent nonlinear generalized Hadamard full propelinear codes, we could prove the following conjecture about the value of the rank of codes associated to the cocycles of Example 4.1. Note that the conjecture is based in the results obtained in Table 4.1.

Research problem 4. Let $C_{a,b}$ be the GHFP-codes associated to $\phi_{(a,b)}(g) = g^{(3^b+1)/2}$, with $g \in \mathbb{F}_{3^a}$. Moreover, if $(a,b) = 1$, b odd and $3 \leq b \leq a-1$ then $\partial\phi_{(a,b)}$ are orthogonal cocycles and the associated GHFP-codes $C_{a,b}$ are not linear. Then r depends only on b by $r(b) = 3 \cdot 2^{b-1} - 1$ with b odd.

Since we have defined GHFP-codes over finite fields, the next natural step is to extend the concept to rings.

Research problem 5. Define Hadamard full propelinear codes over rings.

Recall that quasi-Hadamard codes can be seen as a good alternative to 2-punctured Hadamard codes in that cases when we do not know about the existence of a Hadamard code of length $4t$.

Research problem 6. Build quasi-Hadamard matrices of order $4t-2$ for t such that there is not known Hadamard matrices of order $4t$. Build QHFP-codes of length $4t-2$ for t such that there is not known cocyclic Hadamard matrices of order $4t$.

The propelinear structure gives place to the propelinear operation $x \star y = x + \pi_x(y)$. Thus, $(C, \star)$ is a group. We could generalized the propelinear structure in different ways. For instance, we could set an operation $\hat{\star}$ given by $x \,\hat{\star}\, y = \pi_\alpha(x) + \pi_x(y)$. Note that if $\pi_\alpha = Id$, then the operation $\hat{\star}$ is the propelinear operation $\star$.

Research problem 7. Generalize the propelinear structure over a code C in order to obtain different algebraic structures $(C, \hat{\star})$.

In some cases we have detected that the generators of some HFP-codes have autocorrelation properties (Golay pairs, negaperiodic Golay pairs, periodic autocorrelation sequences).

Research problem 8. Study the relation between the structure of the generators of the HFP-codes and different types of autocorrelation sequences.

As a final comment, there is a proverb that says "rectify is of wise people." The Cambridge Dictionary defines rectify as "to correct something or make something right". Therefore, error-correction codes make humans, in part, wiser.

"Condenado a estar toda la vida preparando alguna despedida."

Robe. Extremoduro.

Bibliography

[1] Ahlswede R., Cai N., Li S.R., Yeung R.W.: Network information flow. IEEE Trans. Inf. Theory **46**(4), 1204–1216 (2000).

[2] Álvarez V., Armario J.A., Frau M.D., Gudiel F.: The maximal determinant of cocyclic $(-1, 1)$-matrices over D_{2t}. Linear Algebra Appl. **436**, 858–873 (2012).

[3] Álvarez V., Armario J.A., Frau M.D., Gudiel F.: Determinants of $(-1, 1)$-matrices of the skew-symmetric type: a cocyclic approach. Open Math. **13**, 16–25 (2015).

[4] Álvarez V., Gudiel F., Güemes M.B.: On $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices. J. Combin. Designs **23**(8), 352–368 (2015).

[5] Arasu K.T., de Launey W., Ma S.L.: On Circulant Complex Hadamard Matrices. Des. Codes Cryptogr. **25**(2), 123–142 (2002).

[6] Armario J.A., Bailera I., Borges J., Rifà, J.: Quasi-Hadamard Full Propelinear Codes. Math. Comput. Sci. **12**(4), 419–428 (2018).

[7] Armario J.A., Bailera I., Egan R.: Example 5. Generalized Hadamard full propelinear codes. Universitat Autònoma de Barcelona, 2019. https://ddd.uab.cat/record/204295.

[8] Armario J.A., Bailera I., Egan R.: Generalized Hadamard full propelinear codes. arXiv:1906.06220 [math.CO].

[9] Armario J.A., Flannery D.L.: On quasi-orthogonal cocycles. J. Combin. Designs **26**(8), 401–411 (2018).

[10] Assmus E.F., Key J.D.: Designs and Their Codes. Cambridge University Press, Great Britain (1992).

[11] 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).

[12] Bailera I., Borges J., Rifà J.: On Hadamard full propelinear codes with associated group $C_{2t} \times C_2$. To appear in Adv. Math. Commun.

[13] Baliga A., Horadam K.J.: Cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$. Australas. J. Combin. **11**, 123–134 (1995).

[14] Barrera Acevedo S., Dietrich H.; Perfect sequences over the quaternions and $(4n, 2, 4n, 2n)$-relative difference sets in $C_n \times Q_8$. Cryptogr. Commun. **10**(2), 357–368 (2018).

[15] Borges J., Mogilnykh I.Y., Rifà J., Solov'eva F.I.: Structural properties of binary propelinear codes. Adv. Math. Commun. **6**(3), 329–346 (2012).

[16] Borges J., Mogilnykh I.Y., Rifà J. Solov'eva F.: On the number of nonequivalent propelinear extended perfect codes. Electronic J. Combinatorics **20**(2), 1–14 (2013).

[17] Bose R.C.: An affine analogue of Singer's theorem. J. Indian Math. Soc. **6**, 1–15 (1942).

[18] Bosma W., Cannon J.J., Fieker C., Steel A.: Handbook of Magma functions, Edition 2.22 (2016).

[19] Bruck R.H.: Difference sets in a finite group. Trans. Amer. Math. Soc. **78**, 464–481 (1955).

[20] Butson A.T.: Generalized Hadamard Matrices. Proceedings of the American Mathematical Society **13**(6), 894–898 (1962).

[21] Butson A.T.: Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences. Canad. J. Math. **15**, 42–48 (1963).

[22] Carlet C.: $\mathbb{Z}_{2^k}$-linear codes. IEEE Trans. Inf. Theory **44**, 1543–1547 (1998).

[23] Cho J.R., Ito N., Kim P.S., Sim H.S.: Hadamard 2-groups with arbitrarily large derived length. Australas. J Combin. **16**, 83–86 (1997).

[24] Coulter R., Matthews R.: Planar functions and planes of Lenz-Barlotti class II. Des. Codes Cryptogr. **10**(2), 167–184 (1997).

[25] Crnković D., Egan R., Švob A.: Orbit matrices of Hadamard matrices and related codes. Discrete Math. **341**, 1199–1209 (2018).

[26] Davis J.A.: Construction of relative difference sets in p-groups. Discrete Math. **103**(1), 7–15 (1992).

[27] de Launey W., Flannery D.L.: Algebraic design theory. Mathematical Surveys and Monographs, vol. 175. American Mathematical Society, Providence, RI (2011).

[28] de Launey W., Flannery D.L., Horadam K.J.: Cocyclic Hadamard matrices and difference sets. Discrete Appl. Math. **102**(1-2), 47–61 (2000).

[29] de Launey W., Horadam K.J.: A weak difference set construction for higher dimensional designs. Des. Codes Cryptogr. **3**, 75–87 (1993).

[30] Dillon J.F.: Some REALLY beautiful Hadamard matrices, Cryptogr. Commun. **2**(2), 271–292 (2010).

[31] Đoković D.Ž., Kotsireas I.S.: D-Optimal Matrices of Orders 118, 138, 150, 154 and 174. Colbourn C. (eds) Algebraic Design Theory and Hadamard Matrices. Springer Proceedings in Mathematics & Statistics **133**. Springer, Cham (2015).

[32] Dougherty S.T., Rifà J., Villanueva M.: Ranks and kernels of codes from generalized Hadamard matrices. IEEE trans. Inf. Theory **62**(2), 687–694 (2016).

[33] Drake D.A.: Partial λ-Geometries and Generalized Hadamard Matrices Over Groups. Canad. J. Math. **31**(3), 617–627 (1979).

[34] Egan R., Flannery D.L.: Automorphisms of generalized Sylvester Hadamard matrices. Discrete Math. **340**(3), 516–523 (2017).

[35] Ehlich H.: Determinanten Abschätzungen für binäre Matrizen. Math. Z. **83**, 123–132 (1964).

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

[37] Flannery D.L.: Cocyclic Hadamard matrices and Hadamard groups are equivalent. J. Algebra **192**(2), 749–779 (1997).

[38] Goethals J.M., Seidel J.J.: Orthogonal Matrices with Zero Diagonal. Can. J. Math. **19**, 1001–1010 (1967).

[39] Goethals J.M., Seidel J.J.: A skew Hadamard matrix of order 36. J. Austral. Math. Soc. **11**(3), 343–344 (1970).

[40] Hadamard J.: Résolution d'une question relative aux déterminants. Bull. Sci. Math. Sér. 2 **17**, 240–246 (1893).

[41] Hall M.: Cyclic projective planes. Duke Math. J. **14**, 1079–1090 (1947).

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

[43] Horadam K.J.: An introduction to cocyclic generalised Hadamard matrices. Discrete Appl. Math. **102**(1-2), 115–131 (2000).

[44] Horadam K.J.: Hadamard Matrices and Their Applications. Princeton University Press, Princeton, NJ (2007).

[45] Horadam K.J., de Launey W.: Generation of Cocyclic Hadamard Matrices. In: Bosma W., van der Poorten A. (eds) Computational Algebra and Number Theory. Mathematics and Its Applications **325**. Springer, Dordrecht (1995).

[46] Horadam K.J., Udaya P.: A new class of ternary cocyclic Hadamard codes. Applic. Algebra En. Commun. Comp. **14**(1), 65–73 (2003).

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

[48] Ito N.: On Hadamard groups II. J. Algebra **169**(3), 936–942 (1994).

[49] Ito N.: On Hadamard groups III. Kyushu J. Math. **51**(2), 369–379 (1997).

[50] Jedwab J., Davis J.A.: A survey of Hadamard difference sets. Hewlett Packard Technical Reports, HPL-94-14. HP Laboratories, Bristol (1994).

[51] Jungnickel D.: On automorphism groups of divisible designs. Canad. J. Math. **34**, 257–297 (1982).

[52] Karpilovsky G.: Projective representations of finite groups. Marcel Dekker, New York (1985).

[53] Kharaghani H., Orrick. W.: D-optimal matrices. The CRC Handbook of Combinatorial Designs, C. J. Colbourn and J. Dinitz (Editors), 296–298. CRC press, Boca Raton (2006).

[54] Koetter R., Kschischang F.R.: Coding for Errors and Erasures in Random Network Coding. IEEE Trans. Inf. Theory **54**(8), 3579–3591 (2008).

[55] Kraemer R.G.: Proof of a conjecture on Hadamard 2-groups. J. Combin. Theory Ser. A **63**, 1–10 (1993).

[56] Li S.R., Yeung R.W., Cai N.: Linear network coding. IEEE Trans. Inf. Theory **49**(2), 371–381 (2003).

[57] Nechaev A.: Kerdock code in a cyclic form. Dis. Math. and Applic. **1**(4), 365–384 (1991).

[58] Ó Catháin P., Röder M.: The cocyclic Hadamard matrices of order less than 40. Des. Codes Cryptogr. **58**(1), 73–88 (2011).

[59] Paley R.E.A.C.: On orthogonal matrices. J. Math. Phys. **12**, 311–320 (1933).

[60] Perera A.A.I., Horadam K.J.: Cocyclic generalized Hadamard matrices and central relative difference sets. Des. Codes Cryptogr. **15**(2), 187–200 (1998).

[61] Phelps K.T., Rifà J.: On binary 1-perfect additive codes: some structural properties. IEEE Trans. Inf. Theory **48**(9), 2587–2592 (2002).

[62] Phelps K.T., Rifà J., Villanueva M.: Hadamard codes of length $2^t s$ (s odd). Rank and kernel. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes LNCS 3857 (ed. H. F. Lu), 328-337. Springer, Berlin (2006).

[63] Rifà J.: Circulant Hadamard matrices as HFP-codes of type $C_{4n} \times C_2$, preprint, ifundefinedhref `arxiv:1711.09373v1` `arXiv:1711.09373v1`.

[64] Rifà J., Basart J.M., Huguet L.: On completely regular propelinear codes. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. LNCS 357, 341–355. Springer, Berlin (1989).

[65] Rifà J., Pujol J.: Translation-invariant propelinear codes. IEEE Trans. Inf. Theory **43**(2), 590–598 (1997).

[66] Rifà J., Suárez E.: About a class of Hadamard propelinear codes. Electron. Notes Discret. Math. **46**, 289-296 (2014).

[67] Rifà J., Suárez E.: Hadamard full propelinear codes of type Q; rank and kernel. Des. Codes Cryptogr. **86**(9), 1905–1921 (2018).

[68] Ryser H.J.: Combinatorial Mathematics. The Carus Mathematical Monographs, Mathematical Association of America, New York (1963).

[69] Schmidt B.: Cyclotomic integers and finite geometries. J. Amer. Math. Soc. **12**, 929–952 (1999).

[70] Schmidt B.: Williamson matrices and a conjecture of Ito's. Des. Codes Cryptogr. **17**(1-3), 61–68 (1999).

[71] Schmidt B.: Towards Ryser's conjecture. Proceedings of the Third European Congress of Mathematics (eds C. Casacubertaet al.), Progress in Mathematics 201, 533–541. Birkhuser, Boston (2001).

[72] Shannon C.: A mathematical theory of communication. Bell Systems Techn. J. **27**, 379–423, 623–656 (1948).

[73] Shrikhande S.S.: Generalized Hadamard matrices and orthogonal arrays of strength two. Can. J. Math. **16**, 736–740 (1964).

[74] Singer J.: A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc. **43**, 377–385 (1938).

[75] Suárez E.: Hadamard full propelinear codes of type Q; Rank and Kernel. PhD diss., Universitat Autònoma de Barcelona (2018).

[76] Sylvester J.J.: LX. Thoughts on inverse 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. Philosophical Magazine Series 4 **34**(232), 461–475 (1867).

[77] Turyn R.J.: Character sums and difference sets. Pacific J. Math. **15**(1), 319–346 (1965).

[78] Williamson J.: Hadamard's determinant theorem and the sum of four squares. Duke Math. J. **11**(1), 65–81 (1944).

[79] Wojtas W.: On Hadamard's inequality for the determinants of order non-divisible by 4. Colloq. Math. **12**(1), 73–83 (1964).

Ivan Bailera
Cerdanyola del Vallès, July 2020