Universitat Autònoma de Barcelona

On Z_2s-linear Hadamard codes and their classification using the rank and kernel

Carlos Vela Cabello

Universitat Autònoma de Barcelona

Departament d'Enginyeria de la Informació i de les Comunicacions

On $\mathbb{Z}_{2^s}$-linear Hadamard codes and their classification using the rank and kernel

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

by Carlos Vela Cabello
Cerdanyola del Vallès, September 2018

Advisors: Dr. Cristina Fernández Córdoba and Dr. Mercè Villanueva Gay
Professors at Universitat Autònoma de Barcelona

I certify that I have read this thesis entitled "On $\mathbb{Z}_{2^s}$-linear Hadamard codes and their classification using the rank and kernel" and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

Cerdanyola del Vallès, September 2018

Dr. Cristina Fernández Córdoba
(Advisor)

Dr. Mercè Villanueva Gay
(Advisor)

A mi familia,
que aunque estemos lejos,
siempre les noto cerca.

Abstract

The $\mathbb{Z}_{2^s}$-additive codes are subgroups of $\mathbb{Z}_{2^s}^n$, and can be seen as a generalization of linear codes over $\mathbb{Z}_2$ and $\mathbb{Z}_4$. A $\mathbb{Z}_{2^s}$-linear Hadamard code is a binary Hadamard code which is the Gray map image of a $\mathbb{Z}_{2^s}$-additive code. It is known that either the rank or the dimension of the kernel can be used to give a complete classification for the $\mathbb{Z}_4$-linear Hadamard codes.

The aim of this thesis is to classify the family of $\mathbb{Z}_{2^s}$-linear Hadamard codes obtained from the Carlet's generalized Gray map through the rank and dimension of the kernel. First, we give a recursive construction of the generator matrices of the corresponding $\mathbb{Z}_{2^s}$-additive Hadamard codes. By using this construction, we present a new proof to show that the generated codes are indeed Hadamard. The kernel of these $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t and its dimension are established for any $s > 2$, and it allows to give a partial classification of such codes. Moreover, we prove that this invariant provides a complete classification for some values of t and s. Later, the rank of these codes is computed for $s = 3$, and it is proved that this invariant, along with the dimension of the kernel, provides a complete classification for $\mathbb{Z}_8$-linear Hadamard codes, once $t \geq 3$ is fixed. In this case, the number of nonequivalent such codes is also established. Finally, we prove that some families of $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t are equivalent, once t is fixed. This allows us to improve the previous results on the partial classification of these codes. An upper and a lower bound are given for the amount of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t. Moreover, after some computations, the exact amount of nonequivalent such codes of length 2^t up to $t = 11$ is found.

Resum

Els codis $\mathbb{Z}_{2^s}$-additius són subgrups de l'anell $\mathbb{Z}_{2^s}^n$ i poden considerar-se com una generalització dels codis lineals sobre $\mathbb{Z}_2$ i $\mathbb{Z}_4$. Es diu codi Hadamard $\mathbb{Z}_{2^s}$-lineal a un codi binari Hadamard que és la imatge, via l'aplicació de Gray, d'un $\mathbb{Z}_{2^s}$-additiu. Està demostrat que per donar una classificació completa dels codis Hadamard $\mathbb{Z}_4$-lineals es pot usar el rang o la dimensió del nucli.

L'objectiu d'aquesta tesi és classificar la família dels codis Hadamard $\mathbb{Z}_{2^s}$-lineals obtinguda a través de l'aplicació de Gray generalitzada definida per Carlet, usant el rang i la dimensió del nucli. Primer, donem una construcció recursiva de les matrius generadores dels codis Hadamard $\mathbb{Z}_{2^s}$-additius corresponents. Gràcies a aquesta construcció, donem una demostració nova de que les imatges, via l'aplicació de Gray generalitzada, dels codis generats són Hadamard. Construïm el nucli dels codis Hadamard $\mathbb{Z}_{2^s}$-lineals de longitud 2^t per a $s > 2$, obtenim la seva dimensió i la usem per obtenir una classificació parcial d'aquests codis. A continuació, donem el rang d'aquests codis per a $s = 3$ i demostrem que, juntament amb la dimensió del nucli, podem obtenir una classificació completa dels codis Hadamard $\mathbb{Z}_8$-lineals, fixant $t \geq 3$. També, per a $s = 3$, establim la quantitat exacta de codis no equivalents d'aquest tipus. Finalment, provem que algunes famílies de codis Hadamard $\mathbb{Z}_{2^s}$-lineals de longitud 2^t són equivalents fixant $t \geq 3$. Això ens permet millorar els resultats anteriors relacionats amb la classificació parcial. També donem cotes superiors i inferiors per a la quantitat de codis Hadamard $\mathbb{Z}_{2^s}$-lineals no equivalents de longitud 2^t. Més encara, calculem la quantitat exacta de codis no equivalents fins a $t = 11$.

Resumen

Los códigos $\mathbb{Z}_{2^s}$-aditivos son subgrupos del anillo $\mathbb{Z}_{2^s}^n$ y pueden considerarse como una generalización de los códigos lineales sobre $\mathbb{Z}_2$ y $\mathbb{Z}_4$. Se llama código Hadamard $\mathbb{Z}_{2^s}$-lineal a un código binario Hadamard que es la imagen, vía la aplicación de Gray, de uno $\mathbb{Z}_{2^s}$-aditivo. Está demostrado que para dar una clasificación completa de los códigos Hadamard $\mathbb{Z}_4$-lineales se puede usar el rango o la dimensión del núcleo.

El objetivo de esta tesis es clasificar la familia de los códigos Hadamard $\mathbb{Z}_{2^s}$-lineales obtenida a través de la aplicación de Gray generalizada definida por Carlet, usando el rango y la dimensión del núcleo. Primero, damos una construcción recursiva de las matrices generadoras de los códigos Hadamard aditivos sobre $\mathbb{Z}_{2^s}$ correspondientes. Gracias a esta construcción, damos una demostración nueva de que las imagenes, vía la aplicación de Gray generalizada, de los códigos generados son Hadamard. Construimos el núcleo de los códigos Hadamard $\mathbb{Z}_{2^s}$-lineales de longitud 2^t para $s > 2$, obtenemos su dimensión y la usamos para obtener una clasificación parcial de estos códigos. A continuación, damos el rango de estos códigos para $s = 3$ y demostramos que, junto con la dimensión del núcleo, podemos obtener una clasificación completa de los códigos Hadamard $\mathbb{Z}_8$-lineales, fijando $t \geq 3$. También, para $s = 3$, establecemos la cantidad exacta de códigos no equivalentes de este tipo. Por último, probamos que algnas familias de códigos Hadamard $\mathbb{Z}_{2^s}$-lineales de longitud 2^t son equivalentes fijando $t \geq 3$. Esto nos permite mejorar los resultados anteriores relacionados con la clasificación parcial. También damos cotas superiores e inferiores para la cantidad de códigos Hadamard $\mathbb{Z}_{2^s}$-lineales no equivalentes de longitud 2^t. Más aún, calculamos la cantidad exacta de códigos no equivalentes hasta $t = 11$.

Acknowledgements

Me gustaría empezar agradeciendo a mis directoras, Mercè Villanueva y Cristina Fernández toda la paciencia que han tenido conmigo y el buen criterio con el que han sabido guiarme estos breves, pero muy intensos, años. Gracias por vuestro tiempo y esfuerzo.

I would like to give thanks to Alessandro Neri and Prof. Joachim Rosenthal for took care of me during my stay in Zurich. I spent a really good time there with you guys. Also, I would like to give a little wink of gratitude to Gianira, you are awesome.

En el DeiC me he sentido como en casa, y no sólo porque haya pasado tanto tiempo en el departamento como en mi morada, si no porque me acogieron como uno mas desde el principio. Una mención especial a todos mis compañeros de fatiga doctorandos, que poco a poco se van convirtiendo en doctores. De entre ellos, me gustaría agradecerle su paciencia, a mi compañero de despacho Iván Bailera, que ha sabido soportar mi verborrea, y con el que he compartido discusiones de todo tipo (unas de trabajo y otras no).

Otro lugar en el que me he sentido como en casa era en mi piso. Las vueltas del departamento no hubieran sido tan geniales si no hubiese gente tan genial esperándote para tomar una cerveza, ver una película o acabar a cientos de kilómetros. Gracias a Oscar, Shannon y Sergi por hacer que llegar a casa fuese llegar a mi hogar.

Continuar agradeciendo al "TX" y compañía todo su apoyo. Siempre habéis sabido darme vuestro ánimo y mostrarme vuestro cariño a pesar de estar repartidos por el mundo. El destino ha querido que esté escribiendo estas líneas 10 años después de empezar a conoceros, y espero que sea la

primera de muchas décadas mas con vosotros.

Me gustaría darle las gracias a PauLA por estar dispuesta a acompañarme en este viaje y por todas las cosas que me ha enseñado. Aún habiendonos separado el destino, sin tus palabras esta aventura no hubiera sido tan magnífica.

Por último, pero no por ello menos importante, agradecerle a mi familia toda la paciencia, comprensión y amor inestimables que me han ayudado en los momentos mas adversos y acompañado en los no tanto. Sois geniales.

Contents

Chapter 1

Introduction

"Education never ends, Watson. It is a series of lessons, with the greatest for the last."
–Sir Arthur Conan Doyle, The last bow

Initially, coding theory appeared as a solution to an engineering problem related with the transmission of information without errors from a source to a receiver. The medium, through which the message is sent from the source to the receiver, is called *channel*. The general scheme of a communication is the following:

Figure 1.1: Scheme of communication

In general, the channel we use for communications may produce errors in our messages. When the channel produces errors, it is called *noisy channel* and it is for those channels for which coding theory makes sense. Since we need to solve the problems derived from the use of noisy channels, we introduce error-correcting codes and a process to encode and decode in the communication scheme as it is shown in Figure 1.2.

In a noisy channel, if we want to correct the errors, the process of communication is as follows. The source generates a message m, which we need

Figure 1.2: Scheme of accurately communication incorporating error-correcting codes

to encode by using error-correcting codes that add some redundancy. Once m is encoded, we obtain a codeword c, which will be sent through the noisy channel where errors may happen. These errors change the sent codeword producing a received vector r. Now, to decode, we need to detect and correct the errors obtaining an estimation $\tilde{c}$ from r that hopefully will coincide with the original codeword c. Since there is a one-to-one correspondence between codewords and messages, we therefore obtain an estimation $\tilde{m}$ of the original message m from $\tilde{c}$.

Despite coding theory was an engineering problem, this theory has been developed by using mathematical techniques such as linear algebra, theory of groups and discrete mathematics. Thus, nowadays, coding theory has become an active part of mathematical research.

Coding theory has its origins in lately 1940's in [Sha48] and [Ham50] by Shannon and Hamming, respectively. Specifically, the theory was developed so that electronic information could be transmitted and stored without errors. In general, the information is represented as series of zeros and ones, since the electronic information is represented by using these symbols. Therefore, the binary field, $\mathbb{F}_2$, was rapidly selected as the alphabet for coding theory, and the codes over this alphabet are called binary codes.

Later, the results were generalized for fields with q elements, $\mathbb{F}_q$, and all the research related to coding theory was developed over finite fields. In the early 1970's, in [Bla72] and [Bla75], Blake initiates the incursion of rings into coding theory. However, it was with the paper [HKC$^+$94] that the study of codes over rings starts to increase. The interest in these codes is due to the discovery that certain nonlinear binary codes, which have twice as many codewords as the best known comparable linear code, were the images of linear codes over $\mathbb{Z}_4$ under a nonlinear map called Gray map. Some

of these codes, and the ones studied in later works, belong to well-known families of codes such as extended Hamming, Hadamard, QRM, ZRM and Reed-Muller codes, which have been studied and classified [Kro01, BPR03, PRV06, BFP05, BFP08, PPV11, PRS09]. The study of codes over $\mathbb{Z}_4$ quickly encouraged the study of codes over the rings $\mathbb{Z}_k$ or commutative rings of order 4, and their binary images under Gray maps [AS14, AS13, Car91, BGL05, Kro07, DF11, TV03]. Further information on codes over commutative rings can be found in [Dou17].

In this dissertation, we concentrate our efforts in the study of binary nonlinear Hadamard codes with associated structures over $\mathbb{Z}_{2^s}$. The initial point of this work was the paper [Kro01], which studies the $\mathbb{Z}_4$-linear Hadamard codes. There are many possible generalizations of $\mathbb{Z}_4$-linear Hadamard codes. One of them gives rise to the so-called $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes studied in [PRV06, KV15]. Giving one more step in this direction, in [MR15] the Hadamard $\mathbb{Z}_2\mathbb{Z}_4\mathcal{Q}_8$-codes were introduced. Finally, another possible generalization of $\mathbb{Z}_4$-linear Hadamard codes are the $\mathbb{Z}_{2^s}$-linear Hadamard codes [Car91, Kro07], which are the main studied codes in the present thesis. The overview of the dissertation is the following:

- Chapter 2 provides an introduction to coding theory so that this dissertation is as self contained as possible. Firstly, we review basic definitions and results about binary codes emphasizing the concepts related to two invariants for binary codes, the rank and dimension of the kernel. We also give definitions related to the well-known family of Hadamard codes which, in general, are nonlinear. Secondly, we give a brief survey about $\mathbb{Z}_4$-additive, $\mathbb{Z}_4$-linear and $\mathbb{Z}_4$-linear Hadamard codes. Later, we present the generalized Gray map that will be used in this dissertation. Finally, we review basic definitions and properties of $\mathbb{Z}_{2^s}$-additive and $\mathbb{Z}_{2^s}$-linear codes, which are the main topic of this thesis.

- Chapter 3 provides a recursive construction of the $\mathbb{Z}_{2^s}$-additive Hadamard codes whose images under the generalized Gray map give the $\mathbb{Z}_{2^s}$-linear Hadamard codes. By making a study of this Gray map, we provide ourselves with tools, first, to show that, in fact, the images of

the constructed codes are Hadamard codes and, secondly, to see for which types of these codes the obtained binary codes are linear.

- In Chapter 4, we generalize the computation of the kernel and its dimension for $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s > 2$ and give a partial classification of these codes by using this invariant. As in the previous chapter, the study of some properties of the generalized Gray map, allows us to provide ourselves with tools to achieve a construction of the kernel for $\mathbb{Z}_{2^s}$-linear Hadamard codes. Once we have the kernel, we also obtain its dimension and we use it to give a partial classification for these codes. Finally, we also give some bounds on the amount of nonequivalent such codes when t is fixed.

- Chapter 5 presents a full classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes for $s \in \{2, 3\}$. In this chapter, first, we provide a construction of the span of the codes with $s = 3$, since for $s = 2$ is already done. Then, we obtain the rank of the codes for $s = 3$ and a complete classification for them by using both invariants, the rank and dimension of the kernel. Finally, we give the full classification for all these codes with $s \in \{2, 3\}$ and the amount of nonequivalent codes that there exists for a given length 2^t.

- In Chapter 6, we improve the partial classification presented in Chapter 4. First, we establish some equivalent relations among the $\mathbb{Z}_{2^s}$-linear Hadamard codes with $2 \leq s \leq t + 1$. Finally, by using these relations, we also enhance the previous partial classification and refine the bounds, given in Chapter 4, on the amount of nonequivalent codes when t is fixed.

- Chapter 7 presents our conclusions and proposes future research lines on this topic.

Finally, we must mention that part of the research included in this dissertation was presented at several conferences and published in their proceedings [FVV16, FVV17, FVV18a]:

[FVV16] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "Construction and classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes," in Proc. of the *Discrete Mathematics Days, JMDA16. Electronic Notes in Discrete Mathematics*, 54, pp. 247–252 (2016).

[FVV17] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On the kernel of $\mathbb{Z}_{2^s}$-linear Hadamard codes," in Proc. of the *5th International Castle Meeting on Coding Theory and Applications, ICMCTA 2017. Lecture Notes in Computer Science*, 10495, pp. 107–117 (2017).

[FVV18a] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On the rank of $\mathbb{Z}_8$-linear Hadamard codes," in Proc. of the *2nd IMA Conference on Theoretical and Computational Discrete Mathematics. Electronic Notes in Discrete Mathematics*, to be published (2018).

The results showed in Chapter 6 have been presented in *Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT),* held in Svetlogorsk (Kaliningrad region), Russia. The given talk was entitled "On some equivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes".

Moreover, the results presented in Chapters 3 and 4 have already been published in a journal [FVV18b], whereas those of Chapter 5 have been submitted [FVV18c]:

[FVV18b] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On $\mathbb{Z}_{2^s}$-linear Hadamard codes: kernel and partial classification," to appear in *Designs, Codes and Cryptography* (2018).

[FVV18c] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On $\mathbb{Z}_8$-linear Hadamard codes: rank and classification," submitted to *IEEE Transactions on Information Theory* (2018).

This work has been partially supported by the Spanish MINECO under Grants TIN2013-40524-P, TIN2016-77918-P (AEI/FEDER, UE) and also

MTM2015-69138-REDT, and by the Catalan AGAUR under Grant 2014SGR-691.

Finally, I visited Prof. Dr. Joachim Rosenthal at the Department of Mathematics at University of Zurich, in Zurich, Switzerland, from 17 January to 19 April 2018 with the objective of getting in touch with the different research lines about codes that there are in this department. My research during this visit was focused on *networking codes*. More specifically, on *equidistant codes*, *orbit codes*, *equidistant subspace codes* and *rank metric codes*. For more information about these codes, the reader is referred to [TMB+11, GR16, Gab85, ER14, Lam13].

Chapter 2

State of art

"The mind is not a vessel to be filled, but a fire to be kindled."

–Plutarch

The aim of this chapter is to introduce previous concepts which are necessary to understand the main results of this dissertation. First, in Section 2.1, we describe the main concepts about linear and nonlinear binary codes. Secondly, in Section 2.2, we introduce two invariants for the binary codes, the rank and the dimension of the kernel. Since the Hadamard codes are the main family of codes that we study, Section 2.3 is dedicated to them. Later, in Sections 2.4 and 2.5, as a motivation for the thesis, we see the definition and some properties of the $\mathbb{Z}_4$-linear codes and $\mathbb{Z}_4$-linear Hadamard codes, since these codes have been deeply studied. As a necessary step, in Section 2.6, we study some generalizations of the Gray map and see in more detail the one we use in this dissertation to map linear codes over $\mathbb{Z}_{2^s}$ to (possibly nonlinear) binary codes. Finally, in Section 2.7, we see the definition and some basic properties of $\mathbb{Z}_{2^s}$-linear codes.

2.1 Basic concepts of binary codes

Let $\mathbb{Z}_2$ be the ring of integers modulo 2 and let $\mathbb{Z}_2^n$ denote the set of all binary vectors of length n. Any nonempty subset C of $\mathbb{Z}_2^n$ is a *binary code* of length

n, and a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code* of length n. From now on, the elements of a code will be called codewords. A binary linear code of length n can also be seen as a linear subspace of $\mathbb{Z}_2^n$. In this case, the dimension k of the code is defined as the dimension of the linear subspace over $\mathbb{Z}_2$.

The *Hamming weight* of a binary vector $\mathbf{u} \in \mathbb{Z}_2^n$, denoted by $\mathrm{wt}_H(\mathbf{u})$, is the number of nonzero coordinates of $\mathbf{u}$. The *minimum Hamming weight* of a binary code C, denoted by $\mathrm{wt}_H(C)$, is the minimum value of $\mathrm{wt}_H(\mathbf{u})$ with $\mathbf{u} \in C$ and $\mathbf{u} \neq \mathbf{0}$, where $\mathbf{0}$ is the all-zero vector. The *Hamming distance* of two binary vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n$, denoted by $d_H(\mathbf{u}, \mathbf{v})$, is the number of coordinates in which they differ. Note that $d_H(\mathbf{u}, \mathbf{v}) = \mathrm{wt}_H(\mathbf{v}-\mathbf{u})$. The *minimum Hamming distance* of a binary code C is $d(C) = \min\{d_H(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}$. It is well known that if C is a binary linear code, $d(C) = \mathrm{wt}_H(C)$. The minimum Hamming distance of a binary code will be denoted by d only if the code we are referring to is clear from the context.

The minimum Hamming distance d of a binary code C determines the number of errors that the code can correct. Let y be a received vector (as in Figure 1.2). If the amount of errors that occur in the corresponding message m is less than or equal to $\lfloor (d-1)/2 \rfloor$, then there is only one codeword $c \in C$ such that $d(c, y) \leq \lfloor (d-1)/2 \rfloor$. The parameter

$$t = \lfloor (d-1)/2 \rfloor$$

is called the *error-correcting capability* of the code, which is said to be a t-error-correcting code. Another parameter also related to the minimum distance of a binary code is the *detection capability*, that is the amount of errors that a code is able to detect, and it is given by the expression $(d-1)$.

The most common ways to describe a linear code are with either, a generator or a parity check matrix. A *generator matrix* for a linear code C of length n and dimension k is a $k \times n$ matrix G whose rows form a basis of C. In general, there are different generator matrices for a linear code. A *parity check matrix* H for a linear code C is a $(n-k) \times n$ matrix of dimension $n-k$ whose null space is the code C, i.e., $\mathbf{u}H^T = \mathbf{0}$ for all $\mathbf{u} \in C$, where H^T

denotes the transpose matrix of H. A generator matrix G and a parity check matrix H for the linear code C satisfy $GH^T = \mathbf{0}$. A generator matrix G is said to be in *standard form* if its first k columns form the identity matrix of size k, denoted by Id_k. If $G = (\mathrm{Id}_k \,|A)$ is a generator matrix for the linear code C in standard form, then

$$H = (-A^T | \,\mathrm{Id}_{n-k}) \tag{2.1}$$

is a parity check matrix for C. A parity check matrix H as in (2.1) is said to be in standard form.

The *inner product* of two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n$ is defined as

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

If $\langle \mathbf{u}, \mathbf{v} \rangle = 0$, then $\mathbf{u}$ and $\mathbf{v}$ are called *orthogonal*. Denote the set of vectors which are orthogonal to all codewords of a binary code C by $C^\perp$, that is,

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

Note that $C^\perp$ is always a linear code. When C is linear, then $C^\perp$ is called the *dual* of the code C, otherwise $C^\perp$ is called the *orthogonal code*. If G and H are a generator and a parity check matrix, respectively, for C, then H and G are a generator and a parity check matrix, respectively, for $C^\perp$.

Let $\mathcal{S}_n$ be the symmetric group of permutations on the set $\{1, \ldots, n\}$. Two binary codes, C_1 and C_2, are said to be *permutation equivalent* if there exists a permutation of coordinates $\pi \in \mathcal{S}_n$ such that $C_2 = \{\pi(\mathbf{c}) : \mathbf{c} \in C_1\}$. They are *equivalent* if there exists a vector $\mathbf{a} \in \mathbb{Z}_2^n$ and a permutation of coordinates $\pi \in \mathcal{S}_n$ such that $C_2 = \{\mathbf{a} + \pi(\mathbf{c}) : \mathbf{c} \in C_1\}$.

We take as an example, one of the very first binary codes being defined, the *Hamming code* [Ham50]. For $t \geq 2$, the $t \times (2^t - 1)$ matrix whose columns are the binary expansion of the numbers $1, 2, \ldots, 2^t - 1$ is the parity check matrix of a binary linear code of length $2^t - 1$, dimension $2^t - 1 - t$ and minimum Hamming distance 3. Any rearrangement of the columns of this

matrix gives an equivalent code, and any one of these equivalent codes will be called *binary Hamming code* of length $2^t - 1$. A *binary simplex code* of length $2^t - 1$, denoted by S_t, is the dual of a binary Hamming code of length $2^t - 1$.

Example 1. *For $t = 4$, the matrix*

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

has as columns all the $2^4 - 1 = 15$ nonzero vectors in $\mathbb{Z}_2^4$. Then, H is a parity check matrix for a binary Hamming code of length 15. The matrix H is also a generator matrix in standard form for a binary simplex code S_4.

For more information about linear and nonlinear codes, the reader is referred to [HP03, MS77] and [Zen14], respectively.

2.2 Invariants for binary codes

Two structural properties of binary codes are the rank and the dimension of the kernel. The *rank* of a binary code C is simply the dimension of the linear span, $\langle C \rangle$, of C. The *kernel* of a binary code C, denoted by $\mathrm{K}(C)$, is defined as the set of all codewords that leaves the code invariant by translation [BGH83],

$$\mathrm{K}(C) = \{\mathbf{x} \in \mathbb{Z}_2^n : \mathbf{x} + C = C\}.$$

If the all-zero vector belongs to C, then $\mathrm{K}(C)$ is a linear subcode of C. Note also that if C is linear, then $K(C) = C = \langle C \rangle$. Otherwise, if C is nonlinear, then $K(C) \subsetneq C \subsetneq \langle C \rangle$ as shown in Figure 2.1. Therefore, we can take them as a measure of the nonlinearity of the code.

We denote the rank of a binary code C as $\mathrm{rank}(C)$ and the dimension of the kernel as $\ker(C)$. These parameters can be used to distinguish between nonequivalent binary codes, since equivalent ones have the

same rank and dimension of the kernel. Note that if two codes have different rank or dimension of the kernel, then they are nonequivalent. In [BPR03, Kro01, PRV06, PPV11], the authors compute the rank and the dimension of the kernel of different families of binary codes. In these cases, these invariants are used to give a classification and determine nonequivalent codes.

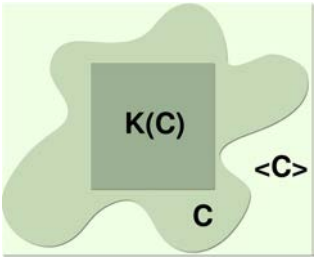


Figure 2.1: Scheme of a nonlinear code C, its kernel and its span

Example 2. *Let C be the binary code that contains the following codewords:*

$$
\begin{gathered}
(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),\\
(0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1),\\
(0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1),\\
(0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0),\\
(0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1),\\
(0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0),\\
(0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0),\\
(0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,1),\\
(0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1),\\
(0,0,1,1,0,1,0,1,1,1,0,0,1,0,1,0),\\
(0,1,0,1,0,0,1,1,1,0,1,0,1,1,0,0),\\
(0,1,1,0,0,1,1,0,1,0,0,1,1,0,0,1),\\
(0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0),\\
(0,0,1,1,1,0,1,0,1,1,0,0,0,1,0,1),\\
(0,1,0,1,1,1,0,0,1,0,1,0,0,0,1,1),\\
(0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0),
\end{gathered}
$$

and their complements. It is easy to check that the span of C is a binary linear code generated by

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

It is also possible to compute the kernel of C, which is the linear code $K(C)$ generated by

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Therefore, we have that $rank(C) = 6$ and $ker(C) = 3$, and we know that C is a binary nonlinear code.

2.3 Binary Hadamard codes

A *Hadamard matrix* H of order n is a $n \times n$ matrix of $+1's$ and $-1's$ such that $HH^T = n\,\mathrm{Id}_n$. It is well known that if a Hadamard matrix H or order n exists, then n is $1, 2$ or a multiple of 4 [MS77, Ch.2 §3] [AK92]. Two Hadamard matrices are *equivalent* if one matrix can be obtained from the other by permuting rows and (or) columns and multiplying rows and (or) columns by -1. We can change the first row and column of H into $+1's$ and we obtain an equivalent Hadamard matrix H', which is called normalized. If $+1's$ are replaced by $0's$ and $-1's$ by $1's$, H' is changed into a *binary Hadamard matrix* $c(H')$. The binary code consisting of the rows of $c(H')$ and their complements is called a *binary Hadamard code* [MS77, Ch.13 §3].

A binary Hadamard code of length n is a binary code with $2n$ codewords and minimum distance $n/2$. In a binary Hadamard code, all codewords,

except the all-one and all-zero codewords, have Hamming weight $n/2$. In general, binary Hadamard codes are nonlinear. In fact, it is well known that there is a unique binary linear Hadamard code H_t of length $n = 2^t$, for any $t \geq 2$, which is the dual of the extended Hamming code of length 2^t [MS77, Ch.2]. A generator matrix G for H_t can be constructed as follows:

$$G = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{0} & G' \end{pmatrix}, \tag{2.2}$$

where G' is a matrix having as columns the $2^t - 1$ nonzero vectors from $\mathbb{Z}_2^t$. Note that G' can be seen as a generator matrix of the binary simplex code S_t of length $2^t - 1$, as noticed in Section 2.1.

Example 3. *Let H_4 be the binary linear Hadamard code of length 16 with generator matrix*

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \tag{2.3}$$

constructed as in (2.2), where G' is the generator matrix for the binary simplex code S_4 of length 15 given in Example 1.

It is also well known that if H is a Hadamard matrix of order n, then

$$\begin{pmatrix} H & H \\ H & -H \end{pmatrix} \tag{2.4}$$

is a Hadamard matrix of order $2n$ [Syl1867]. Starting from the Hadamard matrix $\mathrm{S}_0 = (1)$ of order 1 and applying (2.4), we can recursively define matrices S_t, called *Sylvester* matrices, of order 2^t for $t \geq 1$. The binary Hadamard code corresponding to S_t is the binary linear Hadamard code and is also known as the first order Reed-Muller code of length 2^t [MS77, Ch.13 §3].

Example 4. *By starting with* $\mathrm{S}_0 = (1)$ *and applying (2.4), we obtain the following matrices:*

$$\mathrm{S}_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \mathrm{S}_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

$$\mathrm{S}_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix},$$

$$\mathrm{S}_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{pmatrix}.$$

The corresponding binary Hadamard matrix of S_4 *is*

$$c(\mathrm{S}_4) = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0\\
0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&1&0&1&1&0&1&0&0&1&0&1&1&0&1&0\\
0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0\\
0&1&1&0&1&0&0&1&0&1&1&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1\\
0&1&0&1&0&1&0&1&1&0&1&0&1&0&1&0\\
0&0&1&1&0&0&1&1&1&1&0&0&1&1&0&0\\
0&1&1&0&0&1&1&0&1&0&0&1&1&0&0&1\\
0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0\\
0&1&0&1&1&0&1&0&1&0&1&0&0&1&0&1\\
0&0&1&1&1&1&0&0&1&1&0&0&0&0&1&1\\
0&1&1&0&1&0&0&1&1&0&0&1&0&1&1&0
\end{pmatrix}.$$

Note that the binary code consisting of the rows of this last matrix $c(\mathrm{S}_4)$ *and their complements is linear. Moreover, it is permutation equivalent to the code* H_4 *given in Example 3.*

Example 5. *Let* H *be the following (normalized) Hadamard matrix*

$$\begin{pmatrix} \mathrm{S}_3 & \mathrm{S}_3 \\ \rho(\mathrm{S}_3) & -\rho(\mathrm{S}_3) \end{pmatrix},$$

where S_3 *is the matrix given in Example 4, and* $\rho = (2,3) \in S_{16}$*. The corresponding binary Hadamard code coincides with the one given in Example 2, so it is a nonlinear binary Hadamard code.*

The rank and the dimension of the kernel of binary Hadamard codes have been deeply studied in [Kro01, PRV05, PRV06, RR13, MR15, KV15, DRV15, RS17]. In some of these papers, the authors consider binary Hadamard

codes having linear structures over different rings. Also in some of them, bounds for these invariants are given. In this dissertation, we study the binary Hadamard codes which have associated a linear structure over $\mathbb{Z}_{2^s}$ with $s \geq 2$.

Thanks to the great correction capability of Hadamard codes, these have been used in real word applications. They were used in early satellite transmissions, for example, in the 70's Mariner and Voyager missions to the planets of the solar system [Hor07]. Modern CDMA cellphones use Hadamard matrices to modulate transmission on the uplink and minimise interference with other transmissions to the base station [LT94]. The Walsh-Hadamard Transform [Wal23] is in common use as a fast discrete transform for the transmission of information in image compression and image encoding [Jai89]. New applications for these codes are pattern recognition [KB73], neuroscience [Her12] and optical communication [HS79], among others. In addition, they are also used in cryptography and steganography [Hor07].

Hadamard matrices of order $n = 2^t$, $t \geq 0$, were constructed for the first time by Sylvester [Syl1867]. Later, in [Had1893], Hadamard proved that Hadamard matrices could exist for other orders. In fact, he proved that such matrices could exist only if n is 1, 2 or a multiple of 4. This observation is the basis of the Hadamard's conjecture, which states that a Hadamard matrix of order $4k$ exists for every positive integer k. Currently, the smallest order for which no Hadamard matrix is known is 668 [KT05].

In order to attack the Hadamard's conjecture, in [Ito94, Fla97, LFH00, RS14], the Hadamard matrices are related with different concepts as *cocyclic Hadamard matrices* [Fla97], *Hadamard groups* [Ito94], *different sets* [LFH00] and *Hadamard full propelinear codes* [RS14]. These concepts have been studied in the last years in, for example, [Ito96, Cat12, RS17, AAF+09].

2.4 $\mathbb{Z}_4$-linear codes

The study of codes over rings has its initial point in [Bla72] and [Bla75]. However, it became more significant with the paper [HKC+94], where the

codes were defined over the ring of integers modulo 4, $\mathbb{Z}_4$. For more information about codes over $\mathbb{Z}_4$ see [Wan97], and codes over rings in general see [Dou17].

Let $\mathbb{Z}_4^n$ be the set of all n-tuples over the ring $\mathbb{Z}_4$. Henceforth, the elements of $\mathbb{Z}_4^n$ will also be called vectors despite of the fact that $\mathbb{Z}_4^n$ is not a vector space. Any nonempty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is a *quaternary code* of length n and a subgroup of $\mathbb{Z}_4^n$ is called a *quaternary linear code* of length n.

The Lee weight of an element $i \in \mathbb{Z}_4$ is $\mathrm{wt}_L(i) = \min\{i, 4-i\}$ and the Lee weight of a vector $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{Z}_4^n$ is $\mathrm{wt}_L(\mathbf{u}) = \sum_{j=1}^{n} \mathrm{wt}_L(u_j) \in \mathbb{Z}_4$. The *minimum Lee weight* of a code, $\mathcal{C}$, over $\mathbb{Z}_4$ denoted as $\mathrm{wt}_L(\mathcal{C})$ is the minimum value of $\mathrm{wt}_L(\mathbf{u})$ with $\mathbf{u} \in \mathcal{C}$ and $\mathbf{u} \neq \mathbf{0}$. The Lee distance of two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_4^n$ is $d_L(\mathbf{u}, \mathbf{v}) = \mathrm{wt}_L(\mathbf{v} - \mathbf{u})$. The minimum Lee distance of a quaternary linear code $\mathcal{C}$ is $d_L(\mathcal{C}) = \min\{d_L(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\}$.

The usual *Gray map*, denoted by ϕ, maps $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ as follows:

$$\phi(0) = (0,0),\ \phi(1) = (0,1),\ \phi(2) = (1,1),\ \phi(3) = (1,0). \tag{2.5}$$

We can define the Gray map Φ as a coordinate-wise extension of the usual Gray map, that maps $\mathbb{Z}_4^n$ into $\mathbb{Z}_2^{2n}$, that is,

$$\Phi((y_1, \ldots, y_n)) = (\phi(y_1), \ldots, \phi(y_n)). \tag{2.6}$$

Quaternary codes can be viewed as binary codes under the Gray map Φ. The Gray map is an isometry which transforms Lee distances over $\mathbb{Z}_4^n$ into Hamming distances over $\mathbb{Z}_2^{2n}$. Therefore, the minimum Lee distance of a quaternary code $\mathcal{C}$ coincides with the minimum Hamming distance of $C = \Phi(\mathcal{C})$, that is, $d_L(\mathcal{C}) = d(\Phi(\mathcal{C}))$.

Two quaternary codes, $\mathcal{C}_1$ and $\mathcal{C}_2$, of length n are said to be *permutation equivalent* if they differ only by a permutation of coordinates, that is, if there is a permutation of coordinates $\pi \in \mathcal{S}_n$ such that $\mathcal{C}_2 = \{\pi(\mathbf{c}) : \mathbf{c} \in \mathcal{C}_1\}$.

Let $\mathcal{C}$ be a quaternary linear code of length n. The image, under the Gray map, of $\mathcal{C}$ is a binary code $C = \Phi(\mathcal{C})$ of length $2n$, which is called $\mathbb{Z}_4$-linear code. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, it is isomorphic to an abelian group

$\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ and we say that $\mathcal{C}$ (or equivalently, the corresponding $\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$) is of type $2^\gamma 4^\delta$ as a group. The code $\mathcal{C}$ of type $2^\gamma 4^\delta$ has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords, where $2^{\gamma+\delta}$ of them have order two.

A quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ can also be seen as a $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^n$. As a $\mathbb{Z}_4$-module, $\mathcal{C}$ may or may not be free. Recall that a $\mathbb{Z}_4$-module M is free if there exists a subset $E \subseteq M$ such that every element in M is uniquely expressible as a linear combination over $\mathbb{Z}_4$ of the elements in E [HP03]. Then, the quaternary linear code $\mathcal{C}$ is free if $\gamma = 0$. Although $\mathcal{C}$ is not a free module in general, there exist $\{\mathbf{u}_i\}_{i=1}^\gamma$ and $\{\mathbf{v}_j\}_{j=1}^\delta$ such that every codeword is uniquely expressible in the form

$$\sum_{i=1}^{\gamma} \lambda_i \mathbf{u}_i + \sum_{j=1}^{\delta} \mu_j \mathbf{v}_j,$$

where $\lambda_i \in \{0,1\} \subset \mathbb{Z}_2$ for all $1 \leq i \leq \gamma$, $\mu_j \in \mathbb{Z}_4$ for all $1 \leq j \leq \delta$ and $\mathbf{u}_i, \mathbf{v}_j$ are codewords of $\mathcal{C}$ of order two and four, respectively. The matrix $\mathcal{G}$ that has as rows the codewords $\{\mathbf{u}_i\}_{i=1}^\gamma$ and $\{\mathbf{v}_j\}_{j=1}^\delta$ is a generator matrix for $\mathcal{C}$. As for linear codes, there is a standard form for the generator matrix of $\mathcal{C}$. In [HKC+94], it was shown that any quaternary linear code of type $2^\gamma 4^\delta$ is permutation equivalent to a quaternary linear code $\mathcal{C}_S$ with a generator matrix of the following form

$$\mathcal{G}_S = \begin{pmatrix} 2T & 2\,\mathrm{Id}_\gamma & \mathbf{0} \\ S & R & \mathrm{Id}_\delta \end{pmatrix}, \tag{2.7}$$

where R, T are matrices over $\mathbb{Z}_4$ with entries in $\{0,1\} \subseteq \mathbb{Z}_4$ of size $\delta \times \gamma$ and $\gamma \times (\beta - \gamma - \delta)$, respectively; and S is a matrix over $\mathbb{Z}_4$ of size $\delta \times (\beta - \gamma - \delta)$.

In general, a $\mathbb{Z}_4$-linear code is not necessarily linear. The following lemmas are useful when dealing with the linearity of $\mathbb{Z}_4$-linear codes. Let $\mathbf{u} * \mathbf{v}$ denote the component-wise product of two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_4^n$.

Lemma 6 ([HKC+94, Wan97]). *For all $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_4^n$, we have*

$$\Phi(\mathbf{u} + \mathbf{v}) = \Phi(\mathbf{u}) + \Phi(\mathbf{v}) + \Phi(2\mathbf{u} * \mathbf{v}).$$

Lemma 7 ([HKC+94, Wan97]). *Let $\mathcal{C}$ be a quaternary linear code. The $\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ is a binary linear code if and only if $2\mathbf{u} * \mathbf{v} \in \mathcal{C}$ for all $\mathbf{u}, \mathbf{v} \in \mathcal{C}$.*

One can strengthen Lemma 7 via the generators of order four of the quaternary linear code. Specifically, if $\mathcal{G}$ is a generator matrix of a quaternary linear code $\mathcal{C}$ of type $2^\gamma 4^\delta$ and $\{\mathbf{u}_i\}_{i=1}^{\gamma}$ and $\{\mathbf{v}_j\}_{j=1}^{\delta}$ are the rows of order two and order four in $\mathcal{G}$, respectively, then the $\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ is a binary linear code if and only if $2\mathbf{v}_i * \mathbf{v}_j \in \mathcal{C}$, for all $1 \leq i < j \leq \delta$. It is clear that $2\mathbf{u}_i * \mathbf{v} = \mathbf{0} \in \mathcal{C}$ for all $1 \leq i \leq \gamma$ and $\mathbf{v} \in \mathcal{C}$; and $2\mathbf{v}_j * \mathbf{v}_j = 2\mathbf{v}_j \in \mathcal{C}$ for all $1 \leq j \leq \delta$.

Example 8. *Let $\mathcal{C}$ be the quaternary linear code of length 16 with generator matrix*

$$\mathcal{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \end{pmatrix}. \tag{2.8}$$

Denote the ith row of matrix (2.8) by $\mathbf{v}_i$. It is straightforward to check that

$$2\mathbf{v}_2 * \mathbf{v}_3 = (0000020200000202) \notin \mathcal{C}.$$

Thus, by Lemma 7, the $\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ is a binary nonlinear code. The quaternary linear code $\mathcal{C}$ is permutation equivalent, by using the permutation $(1, 14, 11, 8, 5, 16, 13, 10, 7, 4, 2, 15, 12, 9, 6, 3) \in \mathcal{S}_{16}$, to a quaternary linear code $\mathcal{C}_S$ with generator matrix $\mathcal{G}_S$ in standard form (2.7), where

$$\mathcal{G}_S = \begin{pmatrix} 3 & 2 & 3 & 2 & 1 & 3 & 2 & 1 & 0 & 2 & 1 & 0 & 3 & 1 & 0 & 0 \\ 2 & 3 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 0 & 0 & 1 \end{pmatrix}. \tag{2.9}$$

The code $\mathcal{C}$ is of type $2^0 4^3$, so it has $4^3 = 64$ codewords.

Example 9. *Let $\mathcal{C}$ be the quaternary linear code of length 16 with generator*

matrix

$$\mathcal{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix} = \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{u}_1 \\ \mathbf{u}_2 \end{pmatrix} \quad (2.10)$$

It is easy to see that $2\mathbf{v}_1 * \mathbf{v}_2 = 2\mathbf{v}_2 \in \mathcal{C}$*, so* $C = \Phi(\mathcal{C})$ *is a binary linear code by Lemma 7. The code* $\mathcal{C}$ *is permutation equivalent via the permutation* $(1, 15, 11, 7, 4, 2, 16, 12, 8, 5, 13, 9, 14, 10, 6, 3) \in \mathcal{S}_{16}$ *to a quaternary linear code* $\mathcal{C}_S$ *with generator matrix* $\mathcal{G}_S$ *in standard form (2.7), where*

$$\mathcal{G}_S = \begin{pmatrix} 0 & 0 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 0 & 0 \\ 3 & 2 & 0 & 3 & 2 & 0 & 3 & 2 & 1 & 0 & 3 & 2 & 1 & 1 & 1 & 0 \\ 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad (2.11)$$

The code $\mathcal{C}$ *is of type* $2^2 4^2$*, so it has* $2^2 4^2 = 64$ *codewords.*

The *inner product* of two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_4^n$ is defined as

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^{n} u_i v_i \in \mathbb{Z}_4.$$

Given a quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$, the *quaternary dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined as

$$\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{Z}_4^n : \langle \mathbf{x}, \mathbf{u} \rangle = 0, \text{ for all } \mathbf{u} \in \mathcal{C}\}.$$

The code $\mathcal{C}^\perp$ is a quaternary linear code of length n and type $2^\gamma 4^{n-\gamma-\delta}$ [HKC+94]. The weight enumerator polynomial of $\mathcal{C}^\perp$ is related to the weight enumerator polynomial of $\mathcal{C}$ by the MacWilliams identity [MS77, Ch. 5]. The corresponding binary code $\Phi(\mathcal{C}^\perp)$ is denoted by $C_\perp$ and called the $\mathbb{Z}_4$-*dual*

code of C. We have the following scheme:

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\Phi} & C \\ \downarrow{\scriptstyle \perp} & & \\ \mathcal{C}^{\perp} & \xrightarrow{\Phi} & C_{\perp} \end{array} \tag{2.12}$$

The codes C and $C_\perp$ are not necessarily linear, so they are not dual in the binary linear sense. However, the weight enumerator of $C_\perp$ is the MacWilliams transform of the weight enumerator of C and they are called *formally dual*.

Since 1994, quaternary linear codes became significant because, in some cases, after applying the Gray map, we obtain binary nonlinear codes better than any known binary linear code with the same parameters: length, number of codewords and minimum distance. This is the case, for example, of Kerdock and Preparata codes. This discovery is due to the influential paper [HKC$^+$94] where, among other things, it is shown that the Kerdock codes and some Preparata-like codes are $\mathbb{Z}_4$-linear codes and, moreover, the $\mathbb{Z}_4$-dual code of the Kerdock code is a Preparata-like code. Later, other $\mathbb{Z}_4$-linear codes with the same parameters as some well known families of binary linear codes (for example, extended Hamming, Hadamard, QRM, ZRM and Reed-Muller codes) have been studied and classified [BPR03, Kro01, PRV06, PRS09, PPV11, AA09, BV16a, BPRZ03, FPV08, Wan97].

After [HKC$^+$94], a lot of research has been done on quaternary linear codes and linear codes over more general finite rings. Nevertheless, the examples of better-than-linear codes found since then are comparatively sparse. In [KZ13], the *extended dualized Kerdock codes* $\hat{\mathcal{K}}^*_{k+1}$ ($k \geq 3$ odd), which are quaternary linear codes with high minimum Lee distance, are constructed. In [KWZ16], it is shown that the codes $\hat{\mathcal{K}}^*_4$ and $\hat{\mathcal{K}}^*_6$ satisfy that the minimum Hamming distance of their Gray map images is higher than the minimum Hamming distance of any comparable binary linear code. A table with the current better-than-linear codes can be found in [KWZ16]. For moderate lengths, in order to determine whether a nonlinear code is better-than-linear or not, the online tables [Gra09, BCFS16] containing the best known linear codes can be used. Tables with the best known $\mathbb{Z}_4$-linear codes and binary

nonlinear codes are also available at [AA09] and [LRS99], respectively.

There are many possible generalization of $\mathbb{Z}_4$-linear codes. One of them give rise to the so-called $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. A code $\mathcal{C}$ is said to be $\mathbb{Z}_2\mathbb{Z}_4$-additive if the set of coordinates can be partitioned into two subsets X and Y such that the punctured code of $\mathcal{C}$ by deleting the coordinates outside X (respectively, Y) is a binary linear code (respectively, a quaternary linear code). Their corresponding binary images, via the generalized Gray map $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \to \mathbb{Z}_2^n$, where $n = \alpha + 2\beta$, defined as

$$\Phi(\mathbf{x}, \mathbf{y}) = (\mathbf{x}, \phi(y_1), \ldots, \phi(y_\beta)), \tag{2.13}$$

for any $\mathbf{x} \in \mathbb{Z}_2^\alpha$, $\mathbf{y} \in \mathbb{Z}_4^\beta$, are called $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. The fundamental parameters as well as the standard forms for generator and parity check matrices and the duality concepts for these codes are studied in [BFP$^+$10, BFP$^+$14]. Other possible generalizations of $\mathbb{Z}_4$-linear codes are $\mathbb{Z}_{2^s}$-linear codes, which are defined as the binary image of linear codes over $\mathbb{Z}_{2^s}$ by generalized Gray maps in [Car91, Kro07, BFR01, BFR09]. Finally, it is also worth mentioning that in [AS13, AS14] $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive and $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes are introduced, generalizing naturally both $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and linear codes over $\mathbb{Z}_{2^s}$, respectively.

2.5 $\mathbb{Z}_4$-linear Hadamard codes

As we said in the previous Section 2.3, binary Hadamard codes are nonlinear, in general. In this case, it is desirable to have a subjacent algebraic structure, like a group or a ring. From the coding theory perspective, it is also desired that the algebraic structure preserves the Hamming distance. This is the case of $\mathbb{Z}_4$-linear codes. The quaternary linear codes that, under the Gray map Φ, give a binary Hadamard code are called *quaternary linear Hadamard codes*, and the corresponding $\mathbb{Z}_4$-linear codes are called $\mathbb{Z}_4$-*linear Hadamard codes*.

The $\mathbb{Z}_4$-linear Hadamard codes are completely classified [Kro01, PRV06]. Specifically, for any $t \geq 3$ and each $\delta \in \{1, \ldots, \lfloor \frac{t+1}{2} \rfloor\}$, there is a unique

(up to equivalence) $\mathbb{Z}_4$-linear Hadamard code of length 2^t which is the Gray map image of a quaternary linear code $\mathcal{H}^{\delta,\gamma}$ of length $\beta = 2^{t-1}$ and type $2^\gamma 4^\delta$, where $t = \gamma + 2\delta - 1$. Moreover, for a fixed t, all these codes are pairwise nonequivalent, except for $\delta = 1$ and $\delta = 2$, which are equivalent to the binary linear Hadamard code H_t of length 2^t [Kro01]. Therefore, the number of nonequivalent $\mathbb{Z}_4$-linear Hadamard codes of length 2^t is $\left\lfloor \frac{t-1}{2} \right\rfloor$ for all $t \geq 3$. Note that when $\delta \geq 3$, the corresponding $\mathbb{Z}_4$-linear Hadamard codes are nonlinear.

Let $\mathcal{H}^{\delta,\gamma}$ be the quaternary linear Hadamard code of length $\beta = 2^{t-1}$ and type $2^\gamma 4^\delta$, where $t = \gamma + 2\delta - 1$, and let $H^{\delta,\gamma} = \Phi(\mathcal{H}^{\delta,\gamma})$ be the corresponding $\mathbb{Z}_4$-linear code of length $2\beta = 2^t$. A generator matrix $\mathcal{G}_{\delta,\gamma}$ for $\mathcal{H}^{\delta,\gamma}$ can be constructed by using the following recursive constructions:

$$\mathcal{G}_{\delta,\gamma+1} = \begin{pmatrix} \mathcal{G}_{\delta,\gamma} & \mathcal{G}_{\delta,\gamma} \\ \mathbf{0} & \mathbf{2} \end{pmatrix}, \tag{2.14}$$

$$\mathcal{G}_{\delta+1,\gamma} = \begin{pmatrix} \mathcal{G}_{\delta,\gamma} & \mathcal{G}_{\delta,\gamma} & \mathcal{G}_{\delta,\gamma} & \mathcal{G}_{\delta,\gamma} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix}, \tag{2.15}$$

starting with $\mathcal{G}_{1,0} = (1)$. First, the matrix $\mathcal{G}_{\delta,0}$ is obtained from $\mathcal{G}_{1,0}$ by using recursively $\delta - 1$ times (2.15), and then $\mathcal{G}_{\delta,\gamma}$ is constructed from $\mathcal{G}_{\delta,0}$ by using γ times (2.14). Note that the rows of order four remain in the upper part of $\mathcal{G}_{\delta,\gamma}$ while those of order two stay in the lower part.

Example 10. *The code $\mathcal{C}$ introduced in Example 8 is the quaternary linear Hadamard code $\mathcal{H}^{3,0}$ of length $\beta = 16$ and type $2^0 4^3$. The $\mathbb{Z}_4$-linear Hadamard code $H^{3,0} = \Phi(\mathcal{H}^{3,0})$ is a binary Hadamard code of length 32 with 64 codewords and minimum Hamming distance 16. The code $H^{3,0}$ is the smallest $\mathbb{Z}_4$-linear Hadamard code which is nonlinear. The corresponding generator matrix $\mathcal{G}_{3,0}$ is constructed, starting with $\mathcal{G}_{1,0} = (1)$ and carrying on as follows:*

$$\mathcal{G}_{2,0} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix} \text{ and}$$

$$\mathcal{G}_{3,0} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \end{pmatrix}.$$

As another example, the code $\mathcal{C}$ introduced in Example 9 is the quaternary linear Hadamard code $\mathcal{H}^{2,2}$ of length $\beta = 16$ and type $2^2 4^2$. The $\mathbb{Z}_4$-linear Hadamard code $H^{2,2} = \Phi(\mathcal{H}^{2,2})$ is the binary linear Hadamard code of length 32 with 64 codewords and minimum Hamming distance 16. The binary linear Hadamard code of this length can also be obtained as the Gray map image of $\mathcal{H}^{1,4}$. Therefore, both codes $H^{2,2}$ and $H^{1,4}$ are equivalent to the code H_4 given in Example 3. Finally, see that there are exactly

$$\left\lfloor \frac{t-1}{2} \right\rfloor = \left\lfloor \frac{5-1}{2} \right\rfloor = 2$$

nonequivalent $\mathbb{Z}_4$-linear Hadamard codes of length $2^5 = 32$, which are either the codes $H^{3,0}$ and $H^{2,2}$, or the codes $H^{3,0}$ and $H^{1,4}$.

The $\mathbb{Z}_4$-linear Hadamard codes have been studied and classified in [Kro01, PRV06] by using the invariants presented in Section 2.2. On one hand, in [Kro01], the author gives a complete classification of these codes by using the cardinal of the kernel.

Proposition 11 ([Kro01])**.** *Let $\mathcal{H}^{\delta,\gamma}$ be a quaternary linear Hadamard code with $\delta > 2$ and $H^{\delta,\gamma} = \Phi(\mathcal{H}^{\delta,\gamma})$ the corresponding $\mathbb{Z}_4$-linear Hadamard code. Then $|K(H^{\delta,\gamma})| = 2^{\delta+\gamma+1}$ and the code $H^{\delta,\gamma}$ is nonlinear.*

On the other hand, in [PRV06], the classification is given by using the rank of the codes.

Proposition 12 ([PRV06])**.** *Let $\mathcal{H}^{\delta,\gamma}$ be a quaternary linear Hadamard code of length 2^{t-1} and type $2^\gamma 4^\delta$, where $t = 2\delta + \gamma - 1$, and let $H^{\delta,\gamma} = \Phi(\mathcal{H}^{\delta,\gamma})$ be the corresponding $\mathbb{Z}_4$-linear code of length 2^t. Then, for $\delta \in \{3, \ldots, \lfloor \frac{t+1}{2} \rfloor\}$, we have that rank$(H^{\delta,\gamma}) = t + 1 + \binom{\delta-1}{2}$.*

Hadamard matrices with different subjacent algebraic structures have been extensively studied, as well as the links with other topics in algebraic combinatorics [Hor07]. This is the case, for example, of $\mathbb{Z}_2\mathbb{Z}_4$-linear

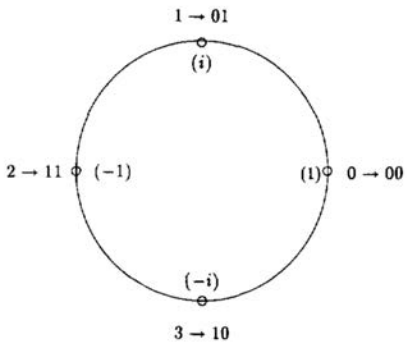
Hadamard codes and Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes. The $\mathbb{Z}_2\mathbb{Z}_4$-additive codes such that, under the generalized Gray map Φ defined in (2.13), give a binary Hadamard code are called $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard codes and the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are called $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes. These codes have been studied in [PRV06, RSV09, KV15] and represent a generalization of the $\mathbb{Z}_4$-linear Hadamard codes presented in this section. Another case are the Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes, which are binary Hadamard codes after a suitable Gray map from a subgroup of direct products of $\mathbb{Z}_2$, $\mathbb{Z}_4$, and Q_8 (where Q_8 is the quaternionic group of order eight); and have been studied in [RR13, MR15]. Finally, in a very intuitive way, the $\mathbb{Z}_{2^s}$-linear Hadamard codes are introduce in [Kro07]. They are binary Hadamard codes that are the image, under a suitable generalization of the Gray map, of codes over the ring $\mathbb{Z}_{2^s}$ for $s \geq 2$. This generalization of the Gray map is discussed in the following Section 2.6.

2.6 Generalized Gray map

In this section, we recall the definition of the Gray map and introduce different generalizations for it. One of the most useful properties of the usual Gray map is that it is an isometry which transforms Lee distances over $\mathbb{Z}_4^n$ into Hamming distances over $\mathbb{Z}_2^{2n}$.

In [HKC+94], the usual Gray map ϕ is define as follows:

> In communication systems employing quadrature phaseshift keying (QPSK), the preferred assignment of two information bits to the four possible phases is



> in which adjacent phases differ by only one binary digit. This mapping is called Gray encoding and has the advantage that, when a quaternary codeword is transmitted across an additive white Gaussian noise channel, the errors most likely to occur are those causing a single erroneously decoded information bit.
>
> (Hammons et al., 1994)

In order to generalize the results about quaternary linear codes, first, we see that there exist many generalizations of the usual Gray map ϕ that take $\mathbb{Z}_{2^s}$ into $\mathbb{Z}_2^{2^{s-1}}$ or $\mathbb{Z}_2^{2^s}$, where $\mathbb{Z}_{2^s}$ is the ring of integers modulo 2^s with $s > 1$. In [BFR01] and [BFR09], the authors define a generalization $\bar{\phi}$ that respects, as the original one, that *adjacent phases*, i.e., the images of consecutive elements in $\mathbb{Z}_{2^s}$, differ just in one bit,

$$\bar{\phi}(i) = \begin{cases} \mathbf{0}_{2^k-i}\mathbf{1}_i, & 0 \leq i \leq 2^{k-1}; \\ \mathbf{1}_{2^{k-1}} + \bar{\phi}(i - 2^{k-1}), & i > 2^{k-1}. \end{cases} \tag{2.16}$$

This generalization is also studied in [DF11].

Other two generalizations given in [Kro07] are

$$\begin{array}{rccc} \varphi: & \mathbb{Z}_{2m}^n & \to & \mathbb{Z}_2^{nm} \\ & (x_1, \ldots, x_n) & \mapsto & (\mathbf{a}_{x_1}, \ldots, \mathbf{a}_{x_n}), \end{array} \tag{2.17}$$

where $A = \{\mathbf{a}_0, \ldots, \mathbf{a}_{2m-1}\}$ is a Hadamard code of length m with $\mathbf{a}_0 = \mathbf{0}$ and $\mathbf{a}_i + \mathbf{a}_{i+m} = \mathbf{1}$, and

$$\begin{array}{rccc} \bar{\varphi}: & \mathbb{Z}_{2m}^n & \to & 2^{\mathbb{Z}_2^{nm}} \\ & (x_1, \ldots, x_n) & \mapsto & H_{x_1} \times \cdots \times H_{x_n}, \end{array} \tag{2.18}$$

where $\{H_0, \ldots, H_{2m-1}\}$ is a partition of $\mathbb{Z}_2^m$ into extended 1-perfect codes of length m.

In this section, and also in the rest of the dissertation, we focus on the Carlet's generalization given in [Car98] and also studied in [TV03]. This

generalization is the map $\phi : \mathbb{Z}_{2^s} \to \mathbb{Z}_2^{2^{s-1}}$ defined as follows:

$$\phi(u) = (u_{s-1}, \ldots, u_{s-1}) + (u_0, \ldots, u_{s-2})Y, \tag{2.19}$$

where $u \in \mathbb{Z}_{2^s}$, $[u_0, u_1, \ldots, u_{s-1}]_2$ is the binary expansion of u, that is $u = \sum_{i=0}^{s-1} 2^i u_i$ ($u_i \in \{0, 1\}$), and Y is a matrix of size $(s-1) \times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$. Note that $(u_{s-1}, \ldots, u_{s-1})$ and $(u_0, \ldots, u_{s-2})Y$ are binary vectors of length 2^{s-1}. We assume that the columns of Y are the binary expansion of the elements of $\mathbb{Z}_{2^{s-1}}$ in increasing order, since they are all the elements of $\mathbb{Z}_2^{s-1}$. The matrix Y is the parity check matrix of a binary Hamming code or the generator matrix of a simplex code after removing the all-zero column. The rows of Y are also a basis for the first order Reed-Muller code after adding the all-one row.

By definition, the Carlet's generalization holds that the Hamming weight of the image of any element $u \in \mathbb{Z}_{2^s}$ is half of the lenght, i.e., $\mathrm{wt}_H(\phi(u)) = 2^{s-2}$, except the images of 2^{s-1} and 0 that are $\mathrm{wt}_H(\phi(2^{s-1})) = 2^{s-1}$ and $\mathrm{wt}_H(\phi(0)) = 0$, respectively. This property is also held by the usual Gray map defined in [HKC+94].

The Carlet's Gray map ϕ is a particular case of the map φ presented in [Kro07], which satisfies that $\sum \lambda_i \phi(2^i) = \phi(\sum \lambda_i 2^i)$ as it was shown in [FVV18b] and will be recalled later. In fact, in [Kro07], the author mentions that the generalization given in [Car98] can be seen as a particular case of φ when A is the binary linear Hadamard code.

Example 13. *Let $s = 3$ and $\bar{\phi}$, ϕ, φ and $\bar{\varphi}$ be the generalized Gray maps defined in [BFR01, BFR09], [Car98], [Kro07] and [Kro07], respectively. Let $A = \{0000, 0101, 0011, 0110, 1111, 1010, 1100, 1001\}$, which is the only Hadamard code of length 2^2 and is linear. Let $H_0 = \{0000, 1111\}$, $H_1 = \{0011, 1100\}, \ldots$, $H_7 = \{0001, 1110\}$. Then, we have that the corresponding*

images for each generalized Gray map are

$$\begin{array}{ccccccc} \mathbb{Z}_8 & & \bar{\phi} & \phi & \varphi & \bar{\varphi} \\ 0 & \longmapsto & 0000 & 0000 & 0000 & H_0 \\ 1 & \longmapsto & 0001 & 0101 & 0101 & H_1 \\ 2 & \longmapsto & 0011 & 0011 & 0011 & H_2 \\ 3 & \longmapsto & 0111 & 0110 & 0110 & H_3 \\ 4 & \longmapsto & 1111 & 1111 & 1111 & H_4 \\ 5 & \longmapsto & 1110 & 1010 & 1010 & H_5 \\ 6 & \longmapsto & 1100 & 1100 & 1100 & H_6 \\ 7 & \longmapsto & 1000 & 1001 & 1001 & H_7. \end{array}$$

Note that the images of ϕ and φ are the same, since there is no more Hadamard codes of length 4 except the linear one.

Let $\Phi : \mathbb{Z}_{2^s}^n \to \mathbb{Z}_2^{n2^{s-1}}$ be the component-wise Gray map of ϕ defined as

$$\Phi((y_1, \ldots, y_n)) = (\phi(y_1), \ldots, \phi(y_n)),$$

where $(y_1, \ldots, y_n) \in \mathbb{Z}_{2^s}^n$. In the rest of the paper, if we need to specify that the domain is $\mathbb{Z}_{2^s}$ and $\mathbb{Z}_{2^s}^n$, then we will denote the maps by ϕ_s and Φ_s instead of ϕ and Φ, respectively. Moreover, the matrix corresponding to the definition of ϕ_s will be also denoted as Y_{s-1} since its columns are the binary expansion of the elements of $\mathbb{Z}_{2^{s-1}}$. We may consider, without loss of generality, that the elements of $\mathbb{Z}_{2^{s-1}}$ are in increasing order. Note that the matrices Y_s can be defined recursively, where $Y_1 = (0\,1)$ and

$$Y_s = \begin{pmatrix} Y_{s-1} & Y_{s-1} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}. \tag{2.20}$$

Recall that H_s is the binary linear Hadamard code corresponding to the Sylvester matrix S_s (2.4), that is, the first order Reed-Muller code of length 2^s. Note also that any element $u \in \mathbb{Z}_{2^s}$ can be written uniquely as $u = \alpha(u) + 2^{s-2}\beta(u) + 2^{s-1}\gamma(u)$, where $\alpha(u) \in \{0, \ldots, 2^{s-2} - 1\}$, $\beta(u), \gamma(u) \in \{0, 1\}$. Since the Sylvester matrix S_s is constructed recursively by using (2.4), the

Gray map ϕ for $\mathbb{Z}_{2^s}$ can also be defined recursively by using the Gray map for $\mathbb{Z}_{2^{s-1}}$ as we see through the following lemmas:

Lemma 14. *Let $u \in \mathbb{Z}_{2^s}$. Then, we have that*

$$\phi_s(u) = \Phi_{s-1}((\alpha(u) + 2^{s-2}\gamma(u), \alpha(u) + 2^{s-2}\beta(u) + 2^{s-2}\gamma(u))).$$

Proof. Let $u \in \mathbb{Z}_{2^s}$, which can be written as $u = \alpha(u) + 2^{s-2}\beta(u) + 2^{s-1}\gamma(u)$. Let $[u_0, \ldots, u_{s-2}, u_{s-1}]_2$ be the binary expansion of u. We have that $\alpha(u) = \sum_{i=0}^{s-3} 2^i u_i$, $\beta(u) = u_{s-2}$ and $\gamma(u) = u_{s-1}$, so we know that

$$\begin{aligned} & \Phi_{s-1}((\alpha(u) + 2^{s-2}\gamma(u), \alpha(u) + 2^{s-2}\beta(u) + 2^{s-2}\gamma(u))) \\ = \; & (\phi_{s-1}(\alpha(u) + 2^{s-2}\gamma(u)), \phi_{s-1}(\alpha(u) + 2^{s-2}(\beta(u) + \gamma(u))). \end{aligned} \tag{2.21}$$

Note that $[u_0, \ldots, u_{s-3}, u_{s-1}]_2$ and $[u_0, \ldots, u_{s-3}, u_{s-2} + u_{s-1}]_2$ are the binary expansion of $\alpha(u)+2^{s-2}\gamma(u)$ and $\alpha(u)+2^{s-2}(\beta(u)+\gamma(u))$, respectively. Then, we have that (2.21) is equal to

$$\begin{aligned} \big((u_{s-1}, \ldots, u_{s-1}) + (u_0, \ldots, u_{s-3})Y_{s-2}, \\ (u_{s-1}, \ldots, u_{s-1}) + (u_{s-2}, \ldots, u_{s-2}) + (u_0, \ldots, u_{s-3})Y_{s-2}\big), \end{aligned}$$

which can be written as

$$\begin{aligned} & \big(u_{s-1}, \ldots, u_{s-1}\big) + \\ & + \big[(u_0, \ldots, u_{s-3}, u_{s-2}) \begin{pmatrix} Y_{s-2} \\ \mathbf{0} \end{pmatrix}, (u_0, \ldots, u_{s-3}, u_{s-2}) \begin{pmatrix} Y_{s-2} \\ \mathbf{1} \end{pmatrix}\big]. \end{aligned} \tag{2.22}$$

Finally, we achieve that (2.22) is the same as

$$\begin{aligned} \big(u_{s-1}, \ldots, u_{s-1}\big) + (u_0, \ldots, u_{s-3}, u_{s-2}) \begin{pmatrix} Y_{s-2} & Y_{s-2} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} = \\ \big(u_{s-1}, \ldots, u_{s-1}\big) + (u_0, \ldots, u_{s-3}, u_{s-2})Y_{s-1} \end{aligned}$$

by 2.20, and it is $= \phi_s(u)$ by 2.19. $\mathcal{QED}$

Lemma 15. *Let $H_{s-2} = \{c_0, \ldots, c_{2^{s-1}-1}\}$ be the binary linear Hadamard code of length 2^{s-2} and $u \in \mathbb{Z}_{2^s}$. Then, we have that*

$$\phi_s(u) = \begin{cases} (\mathbf{c}_{\alpha(u)}, \mathbf{c}_{\alpha(u)}) & \text{if } u \in \{0, \ldots, 2^{s-2}-1\} \\ (\mathbf{c}_{\alpha(u)}, \overline{\mathbf{c}_{\alpha(u)}}) & \text{if } u \in \{2^{s-2}, \ldots, 2^{s-1}-1\} \\ (\overline{\mathbf{c}_{\alpha(u)}}, \overline{\mathbf{c}_{\alpha(u)}}) & \text{if } u \in \{2^{s-1}, \ldots, 3\cdot 2^{s-2}-1\} \\ (\overline{\mathbf{c}_{\alpha(u)}}, \mathbf{c}_{\alpha(u)}) & \text{if } u \in \{3\cdot 2^{s-2}, \ldots, 2^s-1\}, \end{cases} \tag{2.23}$$

where $\overline{\mathbf{c}}$ denote the complement of the binary vector $\mathbf{c}$.

Proof. Straightforward from the results in [Kro07]. $\mathcal{QED}$

Example 16. *The Gray map $\phi_3 : \mathbb{Z}_8 \longrightarrow \mathbb{Z}_2^4$ can be defined by using the Gray map $\phi_2 : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ in the following way:*

$$\begin{aligned} \phi_3(0) &= \Phi_2((0,0)) = (\phi_2(0), \phi_2(0)) = (0,0,0,0), \\ \phi_3(1) &= \Phi_2((1,1)) = (\phi_2(1), \phi_2(1)) = (0,1,0,1), \\ \phi_3(2) &= \Phi_2((0,2)) = (\phi_2(0), \phi_2(2)) = (0,0,1,1), \\ \phi_3(3) &= \Phi_2((1,3)) = (\phi_2(1), \phi_2(3)) = (0,1,1,0), \\ \phi_3(4) &= \Phi_2((2,2)) = (\phi_2(2), \phi_2(2)) = (1,1,1,1), \\ \phi_3(5) &= \Phi_2((3,3)) = (\phi_2(3), \phi_2(3)) = (1,0,1,0), \\ \phi_3(6) &= \Phi_2((2,0)) = (\phi_2(2), \phi_2(0)) = (1,1,0,0), \\ \phi_3(7) &= \Phi_2((3,1)) = (\phi_2(3), \phi_2(1)) = (1,0,0,1). \end{aligned}$$

Let $H_1 = \{\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, where $\mathbf{c}_i = \phi_2(i), i \in \mathbb{Z}_4$; that is, $H_1 = \{(0,0), (0,1), (1,1), (1,0)\}$. Then, $\phi_3 : \mathbb{Z}_8 \longrightarrow \mathbb{Z}_2^2$ can also be defined as follows:

$$\begin{aligned} \phi_3(0) &= (\mathbf{c}_0, \mathbf{c}_0) = (0,0,0,0) \\ \phi_3(1) &= (\mathbf{c}_1, \mathbf{c}_1) = (0,1,0,1) \\ \phi_3(2) &= (\mathbf{c}_0, \overline{\mathbf{c}_0}) = (0,0,1,1) \\ \phi_3(3) &= (\mathbf{c}_1, \overline{\mathbf{c}_1}) = (0,1,1,0) \\ \phi_3(4) &= (\overline{\mathbf{c}_0}, \overline{\mathbf{c}_0}) = (1,1,1,1) \\ \phi_3(5) &= (\overline{\mathbf{c}_1}, \overline{\mathbf{c}_1}) = (1,0,1,0) \\ \phi_3(6) &= (\overline{\mathbf{c}_0}, \mathbf{c}_0) = (1,1,0,0) \\ \phi_3(7) &= (\overline{\mathbf{c}_1}, \mathbf{c}_1) = (1,0,0,1). \end{aligned}$$

2.7 $\mathbb{Z}_{2^s}$-linear codes

In this section, we introduce the concept of $\mathbb{Z}_{2^s}$-linear codes and give a brief description of them. We generalize concepts related to $\mathbb{Z}_4$-linear codes. Let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s with $s \geq 1$. The set of n-tuples over $\mathbb{Z}_{2^s}$ is denoted by $\mathbb{Z}_{2^s}^n$. Henceforth, the elements of $\mathbb{Z}_{2^s}^n$ will also be called vectors over $\mathbb{Z}_{2^s}$ of length n. A nonempty subset, $\mathcal{C}$, of $\mathbb{Z}_{2^s}^n$ is a code over $\mathbb{Z}_{2^s}$ of length n. If $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{2^s}^n$, then it is a linear code over $\mathbb{Z}_{2^s}$ and is called a $\mathbb{Z}_{2^s}$-*additive code*. Note that, when $s = 1$, a $\mathbb{Z}_{2^s}$-additive code is a binary linear code and, when $s = 2$, it is a quaternary linear code or a linear code over $\mathbb{Z}_4$.

The Lee weight of an element $i \in \mathbb{Z}_{2^s}$ is $\mathrm{wt}_L(i) = \min\{i, 2^s - i\}$ and the Lee weight of a vector $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{Z}_{2^s}^n$ is $\mathrm{wt}_L(\mathbf{u}) = \sum_{j=1}^n \mathrm{wt}_L(u_j) \in \mathbb{Z}_{2^s}$. The *minimum Lee weight* of a code, $\mathcal{C}$, over $\mathbb{Z}_{2^s}$ denoted as $\mathrm{wt}_L(\mathcal{C})$ is the minimum value of $\mathrm{wt}_L(\mathbf{u})$ with $\mathbf{u} \in \mathcal{C}$ and $\mathbf{u} \neq \mathbf{0}$. The Lee distance of two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_{2^s}^n$ is $d_L(\mathbf{u}, \mathbf{v}) = \mathrm{wt}_L(\mathbf{v} - \mathbf{u})$. The minimum distance of a code $\mathcal{C}$, over $\mathbb{Z}_{2^s}$ is $d_L(\mathcal{C}) = \min\{d_L(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\}$.

Two $\mathbb{Z}_{2^s}$-additive codes, $\mathcal{C}_1$ and $\mathcal{C}_2$, of length n are said to be *permutation equivalent* if they differ only by a permutation of coordinates, that is, if there is a permutation of coordinates $\pi \in \mathcal{S}_n$ such that $\mathcal{C}_2 = \{\pi(\mathbf{c}) : \mathbf{c} \in \mathcal{C}_1\}$.

Let $\mathcal{C}$ be a $\mathbb{Z}_{2^s}$-additive code of length n. We say that its binary image over the generalized Gray map, that is $C = \Phi(\mathcal{C})$, is a $\mathbb{Z}_{2^s}$-linear code of length $2^{s-1}n$. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{2^s}^n$, it is isomorphic to an abelian structure $\mathbb{Z}_{2^s}^{t_1} \times \mathbb{Z}_{2^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_4^{t_{s-1}} \times \mathbb{Z}_2^{t_s}$, and we say that $\mathcal{C}$, or equivalently $C = \Phi(\mathcal{C})$, is of type $(n; t_1, \ldots, t_s)$. Note that $|\mathcal{C}| = 2^{st_1} 2^{(s-1)t_2} \cdots 2^{t_s}$.

A $\mathbb{Z}_{2^s}$-additive code $\mathcal{C}$ of type $(n; t_1, \ldots, t_s)$ can also be seen as a $\mathbb{Z}_{2^s}$-submodule of $\mathbb{Z}_{2^s}^n$. As a $\mathbb{Z}_{2^s}$-module, $\mathcal{C}$ may or may not be free. A $\mathbb{Z}_{2^s}$-module M is free if there exists a subset $E \subseteq M$ such that every element in M is uniquely expressible as a linear combination over $\mathbb{Z}_{2^s}$ of the elements in E. Then, the $\mathbb{Z}_{2^s}$-additive code $\mathcal{C}$ is free if $t_i = 0$ for all $i \in \{2, \ldots, s\}$. Although $\mathcal{C}$ is not a free module in general, every codeword is uniquely expressible in

the form

$$\sum_{j=1}^{s}\sum_{i=1}^{t_j}\lambda_i^{(j)}\mathbf{u}_i^{(j)},$$

where $\lambda_i^{(j)} \in \mathbb{Z}_{2^{s+1-j}}$ for all $1 \leq j \leq s$ and $\mathbf{u}_i^{(j)}$ are codewords of $\mathcal{C}$ of order 2^{s+1-j} for all $1 \leq j \leq s$. The matrix $\mathcal{G}$ that has as rows the codewords $\mathbf{u}_i^{(j)}$ is a generator matrix for $\mathcal{C}$. As for linear codes, there is a standard form for the generator matrix of $\mathcal{C}$. In [BDH+99], it was shown that any $\mathbb{Z}_{2^s}$-additive code of type $(n; t_1, \ldots, t_s)$ is permutation equivalent to a $\mathbb{Z}_{2^s}$-additive code $\mathcal{C}_S$ with a generator matrix of the following form:

$$\mathcal{G}_S = \begin{pmatrix} \mathrm{Id}_{t_1} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,k} \\ 0 & 2\,\mathrm{Id}_{t_2} & 2A_{1,2} & 2A_{1,3} & \cdots & \cdots & 2A_{1,k} \\ 0 & 0 & 4\,\mathrm{Id}_{t_3} & 4A_{2,3} & \cdots & \cdots & 4A_{2,k} \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 2^{s-1}\,\mathrm{Id}_{t_s} & 2^{s-1}A_{k-1,k} \end{pmatrix}, \quad (2.24)$$

where $A_{i,j}$ are matrices over $\mathbb{Z}_{2^s}$. Unlike linear codes over finite fields, linear codes over a ring do not have a basis, but there exists a generator matrix with minimum number of rows. If $\mathcal{C}$ is a $\mathbb{Z}_{2^s}$-additive code of type $(n; t_1, \ldots, t_s)$, then a generator matrix of $\mathcal{C}$ with minimum number of rows has exactly $t_1 + \cdots + t_s$ rows. Note that the matrix $\mathcal{G}$ with rows $\{u_i^{(j)}\}_{i,j}$ and the matrix $\mathcal{G}_S$ have exactly $t_1 + \cdots + t_s$ rows.

Example 17. *Let $\mathcal{C}$ be the $\mathbb{Z}_8$-additive code of length 16 with generator matrix*

$$\mathcal{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \end{pmatrix}.$$

The code $\mathcal{C}$ is permutation equivalent by subtracting the second row to the first one and via the permutation $(3, 9) \in \mathcal{S}_{16}$ to a $\mathbb{Z}_8$-additive code $\mathcal{C}_S$ with

generator matrix $\mathcal{G}_S$ in standard form (2.24), where

$$\mathcal{G}_S = \begin{pmatrix} 1 & 0 & 1 & 6 & 5 & 4 & 3 & 2 & 7 & 0 & 7 & 6 & 5 & 4 & 3 & 2 \\ 0 & 1 & 0 & 3 & 4 & 5 & 6 & 7 & 2 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \end{pmatrix}.$$

The code $\mathcal{C}$ is of type $(16; 2, 0, 1)$, so it has $8^2 2^1 = 128$ codewords.

In [Car91] the author says that the Carlet's generalized Gray map is not an isometry, i.e., there exist $u, v \in \mathbb{Z}_{2^s}$ with $s > 2$ such that $d_L(u, v) \neq d_H(\phi(u), \phi(v))$. Otherwise it is showed that it is translation-invariant distance, that means that the Hamming weigh of the difference of the Gray image of two elements is the same of the Gray image of the difference:

Proposition 18 ([Car98]). *Let u and v be two elements of $\mathbb{Z}_{2^s}$. The Hamming distance between $\phi(u)$ and $\phi(v)$ is equal to the Hamming weight of $\phi(u - v)$.*

In general, $\mathbb{Z}_{2^s}$-linear codes are not necessarily linear. For these codes, there exist results, such as Lemma 7 for the $\mathbb{Z}_4$-linear codes, which help us to deal with the problem of linearity. In [TV03] the operation "$\odot$" is introduced. Let $u, v \in \mathbb{Z}_{2^s}$ and $[u_0, u_1, \ldots, u_{s-1}]_2, [v_0, v_1, \ldots, v_{s-1}]_2$ be the binary expansions of u and v, respectively. The operation "$\odot$" on $\mathbb{Z}_{2^s}$ is defined as $u \odot v = \sum_{i=0}^{s-1} 2^i u_i v_i$. Note that the binary expansion of $u \odot v$ is $[u_0 v_0, u_1 v_1, \ldots, u_{s-1} v_{s-1}]_2$. Moreover, note that if $s = 2$, $2(u \odot v) = 2(u * v)$. We denote in the same way "$\odot$", the component-wise operation.

Proposition 19 ([TV03]). *Let $u, v \in \mathbb{Z}_{2^s}$. Then,*

$$\phi(u) + \phi(v) = \phi(u + v - 2(u \odot v)).$$

Theorem 20 ([TV03]). *Let $\mathcal{C}$ be a linear code over $\mathbb{Z}_{2^s}$. Then, for $s > 2$, the following statements are equivalent:*

(i) $\Phi(\mathcal{C})$ is linear.

(ii) $2(\mathbf{u} \odot \mathbf{v}) \in \mathcal{C}$ for all $\mathbf{u}, \mathbf{v} \in \mathcal{C}$.

Example 21. *Let $\mathcal{C}$ be the $\mathbb{Z}_8$-additive code of length* 16 *as in Example 17. Let $\mathbf{v}_i$ be the ith row of $\mathcal{G}$. In this case, we can use Theorem 20 to see that the corresponding $\mathbb{Z}_8$-linear code $C = \Phi(\mathcal{C})$ is nonlinear. We have that* $2(\mathbf{v}_1 \odot \mathbf{v}_2) = (0202020202020202)$. *It is easy to see that* $(0202020202020202) \notin \mathcal{C}$, *therefore C is nonlinear.*

Note that, these two last results are a sort of generalization of Lemmas 6 and 7, since as we said above, when $s = 2$ the operation "$\odot$" coincides with the operation "*" after multiplying by two. The result given by Lemma 7 is true just considering $\mathbf{u}, \mathbf{v} \in \mathcal{C}$ being generators of order four, as it is mentioned after this lemma. However, for $s > 2$, we cannot strengthen last theorem considering just the generators of the code.

Now, we see how to define the orthogonal code, $\mathcal{C}^\perp$, of a $\mathbb{Z}_{2^s}$-additive code $\mathcal{C}$. The images under the generalized Gray map of these codes, $\mathcal{C}$ and $\mathcal{C}^\perp$, are not always orthogonal, but we will see under which conditions these codes are formally dual, i.e., their weight enumerators hold the MacWilliams identity .

The *inner product* of two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_{2^s}^n$ is defined as

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^{n} u_i v_i \in \mathbb{Z}_{2^s}.$$

Given a $\mathbb{Z}_{2^s}$-additive code $\mathcal{C}$ of type $(n; t_1, \ldots, t_s)$, the *dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined as

$$\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{Z}_{2^s}^n : \langle \mathbf{x}, \mathbf{u} \rangle = 0, \text{ for all } \mathbf{u} \in \mathcal{C}\}.$$

The dual code $\mathcal{C}^\perp$ is also a $\mathbb{Z}_{2^s}$-additive code. Let $C_\perp = \Phi(\mathcal{C}^\perp)$. Then, we have an scheme as in (2.12).

In [Car98], the author shows that the weight enumerator of C and $C_\perp$ are not in general related by the MacWilliams identity itself, contrarily to the case of $\mathbb{Z}_4$-linear codes. This means that these codes, in general, are neither dual nor formally dual. In [Kro07], the author shows that the codes C and $\overline{C}_\perp$ are formally dual, by using two different generalized Gray maps, Φ (2.18)

and φ (2.17), and following a very similar scheme to (2.12)

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\Phi} & C \\ \downarrow{\scriptstyle \perp} & & \\ \mathcal{C}^{\perp} & \xrightarrow{\varphi} & \overline{C}_{\perp} \end{array}, \tag{2.25}$$

where $\varphi(\mathcal{C}^{\perp}) = \overline{C}_{\perp}$. Finally, in [DF11], the self dual $\mathbb{Z}_{2^s}$-linear codes are studied by using the generalized Gray map defined in (2.16). The authors determine when the Gray image of a code over $\mathbb{Z}_{2^s}$ generates a linear self-dual code and give families of codes whose image generate binary self-dual codes.

Finally, the $\mathbb{Z}_{2^s}$-additive codes that, under the Gray map, give a binary Hadamard code are called $\mathbb{Z}_{2^s}$-*additive Hadamard codes* and the corresponding $\mathbb{Z}_{2^s}$-linear codes are called $\mathbb{Z}_{2^s}$-*linear Hadamard codes*. These codes are the main object of study of this dissertation and we discuss about them all along the rest of the chapters.

Recall that in [Car98], the Gray map is defined as a map from $\mathbb{Z}_{2^s}$ onto the Reed-Muller code of order 1, $RM(1, k-1)$. The first order Reed-Muller codes $RM(1, k-1)$ are in fact binary linear Hadamard codes. They could be considered as the first $\mathbb{Z}_{2^s}$-linear Hadamard codes in history. Later, in [Kro07], the $\mathbb{Z}_{2^s}$-linear Hadamard codes were introduced for the first time for $s > 2$. In [Kro07], the author proves the existence of these codes and, furthermore, shows the nonexistence of other $\mathbb{Z}_{2^s}$-linear Hadamard codes. In this thesis, the family of $\mathbb{Z}_{2^s}$-linear Hadamard codes by using the Carlet's Gray map is constructed recursively. The kernel of these codes is studied and also the rank for $s = 3$. Our main goal is to achieve a full classification by using these invariants.

Chapter 3

Construction and linearity of $\mathbb{Z}_{2^s}$-linear Hadamard codes

"Mathematical!"

–Finn, Adventure Time

The $\mathbb{Z}_{2^s}$-linear Hadamard codes obtained from the Carlet's Gray map were introduced in [Kro07]. The aim of this chapter is to give a recursive construction of such codes and study their linearity. Specifically, in Section 3.1, we give a recursive construction of the generator matrices with minimum number of rows of these codes over $\mathbb{Z}_{2^s}$. We also show that, in fact, the Gray map image of the constructed $\mathbb{Z}_{2^s}$-additive codes are binary Hadamard codes. Finally, in Section 3.2, we establish for which types, $(n; t_1, \ldots, t_s)$, the $\mathbb{Z}_{2^s}$-linear Hadamard codes are linear or not.

3.1 Recursive construction

The description of a generator matrix having minimum number of rows for a $\mathbb{Z}_4$-additive Hadamard code, as long as recursive constructions of these matrices, are given in [Kro01]. In [Kro07], the $\mathbb{Z}_{2^s}$-additive Hadamard codes with $s > 2$ are introduced and generator matrices with minimum number of rows are given for these codes.

In this section, we present a recursive construction of these generator matrices. By using this construction, we establish that the Carlet's Gray map image of the constructed codes are binary Hadamard codes. This result, which corresponds to Theorem 32, was previously proved in [Kro07] by using a different approach.

Let $T_i = \{j \cdot 2^{i-1} : j \in \{0, 1, \ldots, 2^{s-i+1} - 1\}\}$ for all $i \in \{1, \ldots, s\}$. Note that $T_1 = \{0, \ldots, 2^s - 1\}$. Let $t_1, t_2, \ldots, t_s$ be nonnegative integers with $t_1 \geq 1$. Consider the matrix $A^{t_1,\ldots,t_s}$ whose columns are exactly all the vectors of the form $\mathbf{z}^T$, $\mathbf{z} \in \{1\} \times T_1^{t_1-1} \times T_2^{t_2} \times \cdots \times T_s^{t_s}$.

Example 22. *For $s = 3$, for example, we have the following matrices:*

$$A^{1,0,1} = \begin{pmatrix} 1\,1 \\ 0\,4 \end{pmatrix}, \quad A^{1,1,0} = \begin{pmatrix} 1\,1\,1\,1 \\ 0\,2\,4\,6 \end{pmatrix}, \quad A^{2,0,0} = \begin{pmatrix} 1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,2\,3\,4\,5\,6\,7 \end{pmatrix},$$

$$A^{1,1,1} = \begin{pmatrix} 1\,1\,1\,1 & 1\,1\,1\,1 \\ 0\,2\,4\,6 & 0\,2\,4\,6 \\ 0\,0\,0\,0 & 4\,4\,4\,4 \end{pmatrix}, \quad A^{2,0,1} = \begin{pmatrix} 1\,1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,2\,3\,4\,5\,6\,7 & 0\,1\,2\,3\,4\,5\,6\,7 \\ 0\,0\,0\,0\,0\,0\,0\,0 & 4\,4\,4\,4\,4\,4\,4\,4 \end{pmatrix},$$

$$A^{2,1,0} = \begin{pmatrix} 1\,1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,2\,3\,4\,5\,6\,7 & 0\,1\,2\,3\,4\,5\,6\,7 & 0\,1\,2\,3\,4\,5\,6\,7 & 0\,1\,2\,3\,4\,5\,6\,7 \\ 0\,0\,0\,0\,0\,0\,0\,0 & 2\,2\,2\,2\,2\,2\,2\,2 & 4\,4\,4\,4\,4\,4\,4\,4 & 6\,6\,6\,6\,6\,6\,6\,6 \end{pmatrix}.$$

Let $\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \mathbf{2^s - 1}$ be the vectors having the elements $0, 1, 2, \ldots, 2^s - 1$ from $\mathbb{Z}_{2^s}$ repeated in each coordinate, respectively. The order of a vector $\mathbf{u}$ over $\mathbb{Z}_{2^s}$, denoted by $\mathrm{ord}(\mathbf{u})$, is the smallest positive integer m such that $m\mathbf{u} = \mathbf{0}$.

Any matrix $A^{t_1,\ldots,t_s}$ can be obtained by applying the following recursive construction. We start with $A^{1,0,\ldots,0} = (1)$. Then, if we have a matrix $A = A^{t_1,\ldots,t_s}$, for any $i \in \{1, \ldots, s\}$, we may construct the matrix

$$A_i = \begin{pmatrix} A & A & \cdots & A \\ 0 \cdot \mathbf{2^{i-1}} & 1 \cdot \mathbf{2^{i-1}} & \cdots & (2^{s-i+1} - 1) \cdot \mathbf{2^{i-1}} \end{pmatrix}. \tag{3.1}$$

Finally, permuting the rows of A_i, we obtain a matrix $A^{t'_1,\ldots,t'_s}$, where $t'_j = t_j$

for $j \neq i$ and $t'_i = t_i + 1$. Note that any permutation of columns of A_i gives also a matrix $A^{t'_1,\ldots,t'_s}$.

Example 23. *From the matrix $A^{1,0,0} = (1)$, we obtain the matrix $A^{2,0,0}$; and from $A^{2,0,0}$ we can construct $A^{2,0,1}$, where $A^{2,0,0}$ and $A^{2,0,1}$ are the matrices given in Example 22. Note that we can also generate another matrix $A^{2,0,1}$ as follows: from $A^{1,0,0} = (1)$ we obtain the matrix $A^{1,0,1}$ given in Example 22, and from $A^{1,0,1}$ we can construct the matrix*

$$A_1 = \begin{pmatrix} 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,4\,0\,4\,0\,4\,0\,4\,0\,4\,0\,4\,0\,4\,0\,4 \\ 0\,0\,1\,1\,2\,2\,3\,3\,4\,4\,5\,5\,6\,6\,7\,7 \end{pmatrix}.$$

Then, after permuting the rows of A_1, we have the matrix

$$A^{2,0,1} = \begin{pmatrix} 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,1\,1\,2\,2\,3\,3\,4\,4\,5\,5\,6\,6\,7\,7 \\ 0\,4\,0\,4\,0\,4\,0\,4\,0\,4\,0\,4\,0\,4\,0\,4 \end{pmatrix},$$

which is different to the matrix $A^{2,0,1}$ of Example 22. These two matrices $A^{2,0,1}$ generate permutation equivalent codes.

Along this dissertation, we consider that the matrices $A^{t_1,t_2,\ldots,t_s}$ are constructed recursively starting from $A^{1,0,\ldots,0} = (1)$ in the following way. First, we add $t_1 - 1$ rows of order 2^s, up to obtain $A^{t_1,0,\ldots,0}$; then t_2 rows of order 2^{s-1} up to generate $A^{t_1,t_2,0,\ldots,0}$; and so on, until we add t_s rows of order 2 to achieve $A^{t_1,t_2,\ldots,t_s}$. Note that, this order in the recursive construction of the generator matrices $A^{t_1,\ldots,t_s}$ implies that the columns are also exactly all the elements of $\{1\} \times T_1^{t_1-1} \times T_2^{t_2} \times \cdots \times T_s^{t_s}$. Moreover, it determines completely the matrices $A^{t_1,\ldots,t_s}$ from the values of $t_1, \ldots, t_s$. If we change this order, we obtain the same matrix, up to a permutation of rows and columns as it is shown in Example 23.

Let $\mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{2^s}$-additive code generated by the matrix $A^{t_1,\ldots,t_s}$,

where $t_1, \ldots, t_s \geq 0$, with $t_1 \geq 1$. Let $n = 2^{t-s+1}$, where

$$t = \left(\sum_{i=1}^{s} (s-i+1) \cdot t_i \right) - 1.$$

It is easy to see that $\mathcal{H}^{t_1,\ldots,t_s}$ is of length n and has $|\mathcal{H}^{t_1,\ldots,t_s}| = 2^s n = 2^{t+1}$ codewords. Moreover, it is easy to see that $\mathrm{wt}_L(\mathcal{C}) = \mathrm{d}_L(\mathcal{C}) = n$. Note that this code is of type $(n; t_1, t_2, \ldots, t_s)$. We denote as $H^{t_1,\ldots,t_s} = \Phi(\mathcal{H}^{t_1,\ldots,t_s})$ the corresponding $\mathbb{Z}_{2^s}$-linear code.

Example 24. *The code $\mathcal{H}^{1,0,\ldots,0}$ is generated by $A^{1,0,\ldots,0} = (1)$, so $\mathcal{H}^{1,0,\ldots,0} = \mathbb{Z}_{2^s}$. This code has length $n = 1$, cardinality 2^s and minimum distance 1. Thus, $H^{1,0,\ldots,0} = \Phi(\mathcal{H}^{1,0,\ldots,0})$ has length $N = 2^{s-1}$, cardinality $2N = 2^s$ and minimum (Hamming) distance $N/2 = 2^{s-2}$, so it is a binary Hadamard code. Recall that, $H^{1,0,\ldots,0} = \Phi(\mathbb{Z}_{2^s})$ is the binary linear Hadamard code of length 2^{s-1} [Car98], or equivalently, the first order Reed-Muller code of length 2^{s-1}, denoted by $RM(1, s-1)$ [MS77, Ch.13 §3].*

In Example 24, we can see that the Gray map image of the smallest $\mathbb{Z}_{2^s}$-additive code $\mathcal{H}^{1,0,\ldots,0}$ is, in fact, a binary Hadamard code. Now, we prove that the Gray map image of any $\mathbb{Z}_{2^s}$-additive code generated by a matrix $A^{t_1,\ldots,t_s}$ is a binary Hadamard code. With this purpose, first, we recall some results and prove new ones related to the Gray map that we are considering.

The following Lemma 25 can be seen as a corollary of Proposition 19.

Lemma 25. *Let $u \in \mathbb{Z}_{2^s}$ and $0 \leq p \leq s-1$. Then,*

$$\phi(u) + \phi(2^p) = \phi(u + 2^p - 2^{p+1} u_p),$$

where $[u_0, u_1 \ldots, u_{s-1}]_2$ is the binary expansion of u.

Proof. By Proposition 19, we have that $\phi(u) + \phi(2^p) = \phi(u + 2^p - 2(u \odot 2^p))$. The binary expansion of $u \odot 2^p$ is $[0, \ldots, 0, u_p, 0, \ldots, 0]_2$, that is also the binary expansion of $u_p 2^p$. Then, $2(u \odot 2^p) = 2^{p+1} u_p$ and the result holds. $\mathcal{QED}$

Corollary 26. *Let $u \in \mathbb{Z}_{2^s}$. Then,*

$$\phi(u) + \phi(2^{s-1}) = \phi(u + 2^{s-1}).$$

Proof. Straightforward from Lemma 25. $\mathcal{QED}$

Lemma 27. *Let $u \in \{2^{s-2}, \ldots, 2^{s-1}-1\} \cup \{3\cdot 2^{s-2}, \ldots, 2^s - 1\} \subset \mathbb{Z}_{2^s}$. Then,*

$$\phi(u) + \phi(2^{s-2}) = \phi(u + 2^{s-2} + 2^{s-1}).$$

Proof. By Proposition 19, we have that $\phi(u) + \phi(2^{s-2}) = \phi(u + 2^{s-2} - 2(u \odot 2^{s-2}))$. The binary expansion of 2^{s-2} is $[0, \ldots, 0, 1, 0]_2$ and, if $u \in \{2^{s-2}, \ldots, 2^{s-1}-1\} \cup \{3\cdot 2^{s-2}, \ldots, 2^s - 1\}$, the binary expansion of u is $[u_0, u_1, \ldots, u_{s-3}, 1, u_{s-1}]_2$. Then, $-2(u \odot 2^{s-2}) = 2^{s-1}$ and the statement follows. $\mathcal{QED}$

Corollary 28. *Let $v \in \{2^{s-2}, 3\cdot 2^{s-2}\}$ and $U = \{2^{s-2}, \ldots, 2^{s-1}-1\} \cup \{3\cdot 2^{s-2}, \ldots, 2^s - 1\} \subset \mathbb{Z}_{2^s}$. Then,*

$$\phi(u) + \phi(v) = \begin{cases} \phi(u + v + 2^{s-1}) & \text{if } u \in U \\ \phi(u + v) & \text{if } u \in \mathbb{Z}_{2^s} \setminus U. \end{cases}$$

Proof. Straightforward from Lemmas 25 and 27. $\mathcal{QED}$

Proposition 29 ([Car98])**.** *Let $u, v \in \mathbb{Z}_{2^s}$. Then,*

$$d_H(\phi(u), \phi(v)) = \mathrm{wt}_H(\phi(u - v)).$$

Lemma 30. *Let $u \in \mathbb{Z}_{2^s}$. Then,*

$$d_H(\phi(u), \phi(2^{s-1})) + d_H(\phi(u), \phi(0)) = 2^{s-1}.$$

Proof. By the properties of the distance, we have that $d_H(\phi(u), \phi(2^{s-1})) + d_H(\phi(u), \phi(0)) = \mathrm{wt}_H(\phi(2^{s-1}) - \phi(u)) + \mathrm{wt}_H(\phi(u))$. Then, since $\phi(2^{s-1}) = \mathbf{1}$, $\mathrm{wt}_H(\phi(2^{s-1}) - \phi(u)) = 2^{s-1} - \mathrm{wt}_H(\phi(u))$, and the result follows. $\mathcal{QED}$

Corollary 31. *Let $u, v \in \mathbb{Z}_{2^s}$. Then,*

$$d_H(\phi(u), \phi(v + 2^{s-1})) + d_H(\phi(u), \phi(v)) = 2^{s-1}.$$

Proof. Straightforward from Lemmas 25 and 30. $\mathcal{QED}$

The result given by Theorem 32 is already proved in [Kro07]. In that paper, it is shown that each $\mathbb{Z}_{2^s}$-linear Hadamard code is equivalent to $H^{t_1,\ldots,t_s}$ for some $t_1,\ldots,t_s \geq 0$ with $t_1 \geq 1$, considering a generalized Gray map that includes the one given by Carlet. We present a new proof of this theorem, in the case that Carlet's Gray map is considered. This new proof does not use neither the dual of the $\mathbb{Z}_{2^s}$-additive codes nor another generalization of the Gray map for these dual codes, unlike the proof given in [Kro07].

Let $\mathcal{G}$ be a generator matrix of a $\mathbb{Z}_{2^s}$-additive code $\mathcal{C}$ of length n. Then, $(\mathcal{G}\cdots\mathcal{G})$ is a generator matrix of the r-fold replication code of $\mathcal{C}$, $(\mathcal{C},\ldots,\mathcal{C}) = \{(\mathbf{c},\ldots,\mathbf{c}) : \mathbf{c}\in\mathcal{C}\}$, of length $r\cdot n$.

Theorem 32 ([Kro07])**.** *Let $t_1,\ldots,t_s$ be nonnegative integers with $t_1 \geq 1$. The $\mathbb{Z}_{2^s}$-linear code $H^{t_1,\ldots,t_s}$ of type $(n;t_1,t_2,\ldots,t_s)$ is a binary Hadamard code of length 2^t, with $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i) - 1$ and $n = 2^{t-s+1}$.*

Proof. We prove this theorem by induction on the integers t_i, $i\in\{1,\ldots,s\}$. First, by Example 24, the code $H^{1,0,\ldots,0}$ is a Hadamard code.

Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{2^s}$-additive code of length n generated by the matrix $A = A^{t_1,\ldots,t_s}$. We assume that $H = \Phi(\mathcal{H})$ is a Hadamard code of length $N = 2^{s-1}n$. Let $i\in\{1,\ldots,s\}$. Define A_i as in (3.1) and let $\mathcal{H}_i$ be the $\mathbb{Z}_{2^s}$-additive code generated by the matrix A_i. We have that $\mathcal{H}_i$ is permutation equivalent to $\mathcal{H}^{t'_1,\ldots,t'_s}$, where $t'_j = t_j$ for $j\neq i$ and $t'_i = t_i+1$. Now, we shall prove that $H_i = \Phi(\mathcal{H}_i)$ is a Hadamard code.

Note that $\mathcal{H}_i$ can be seen as the union of 2^{s-i+1} cosets of the 2^{s-i+1}-fold replication code of $\mathcal{H}$, $(\mathcal{H},\ldots,\mathcal{H})$, which are

$$(\mathcal{H},\ldots,\mathcal{H}) + r\cdot\mathbf{w}_i, \tag{3.2}$$

for $r\in\{0,\ldots 2^{s-i+1}-1\}$, where $\mathbf{w}_i = (0,\ \mathbf{2^{i-1}},\ 2\cdot\mathbf{2^{i-1}},\ \ldots,\ (2^{s-i+1}-1)\cdot\mathbf{2^{i-1}})$.

The code $\mathcal{H}$ of length n has cardinality $2^s n$. It is easy to see that $\mathcal{H}_i$ has length $n_i = 2^{s-i+1}n$ and cardinality $2^{2s-i+1}n$. Therefore, the length of $H_i = \Phi(\mathcal{H}_i)$ is $N_i = 2^{s-1}n_i$ and the cardinality $2N_i$. Now, we just have to prove that the minimum distance of H_i is $N_i/2$.

By Proposition 29, the minimum distance of H_i is equal to the minimum weight of H_i. Thus, we just have to check that the minimum weight of any coset (3.2) is $N_i/2$. When $r = 0$, we have that $\mathrm{wt}_H(\Phi((\mathbf{u},\ldots,\mathbf{u}))) = 2^{s-i+1}\mathrm{wt}_H(\Phi(\mathbf{u})) = 2^{s-i+1}N/2 = N_i/2$. Otherwise, when $r \neq 0$, we consider

$$\mathrm{wt}_H(\Phi((\mathbf{u},\ldots,\mathbf{u}) + r\cdot\mathbf{w}_i)) = d_H(\Phi((\mathbf{u},\ldots,\mathbf{u})), \Phi(r\cdot\mathbf{w}_i)). \tag{3.3}$$

Note that, by construction, the coordinates of any nonnegative multiple of $\mathbf{w}_i$ can be partitioned into two multisets V and V' such that $|V| = |V'| = 2^{s-i}$ and there is a bijection from V to V' mapping any element $\mathbf{v} \in V$ into an element $\mathbf{v}' \in V'$ such that $\mathbf{v}' - \mathbf{v} = \mathbf{2^{s-1}}$. Therefore, (3.3) can be written as

$$\sum_{\mathbf{v}\in V} d_H(\Phi(\mathbf{u}),\Phi(\mathbf{v})) + \sum_{\mathbf{v}'\in V'} d_H(\Phi(\mathbf{u}),\Phi(\mathbf{v}')) =$$

$$\sum_{\mathbf{v}\in V} d_H(\Phi(\mathbf{u}),\Phi(\mathbf{v})) + d_H(\Phi(\mathbf{u}),\Phi(\mathbf{v}+\mathbf{2^{s-1}})) =$$

$$|V|\cdot 2^{s-1}n = 2^{s-i}2^{s-1}n = N_i/2, \tag{3.4}$$

where (3.4) holds by Corollary 31. $\mathcal{QED}$

Example 33. *Let $\mathcal{H}^{2,0,0}$ be the $\mathbb{Z}_8$-additive code generated by $A^{2,0,0}$ given in Example 22. The $\mathbb{Z}_8$-linear code $H^{2,0,0} = \Phi(\mathcal{H}^{2,0,0})$ has length $N = 32$, $2N = 64$ codewords and minimum (Hamming) distance $N/2 = 16$. Therefore, it is a binary Hadamard code.*

Example 34. *Let $\mathcal{H}^{2,0,0,1}$ be the $\mathbb{Z}_{16}$-additive code generated by the matrix $A^{2,0,0,1}$, that is*

$$\begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&1&2&3&4&5&6&7&8&9&10&11&12&13&14&15&0&1&2&3&4&5&6&7&8&9&10&11&12&13&14&15\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&4&4&4&4&4&4&4&4&4&4&4&4&4&4&4
\end{pmatrix}.$$

It is easy to see that the $\mathbb{Z}_{16}$-linear code $H^{2,0,0,1} = \Phi(\mathcal{H}^{2,0,0,1})$ has length $N = 256$ and $2N = 512$ codewords. Not as easy to see but equally true is that

its minimum (Hamming) distance is $N/2 = 128$. Therefore, it is a binary Hadamard code.

3.2 Linearity

In this section, we establish for which types, $(n; t_1, \ldots, t_s)$, the $\mathbb{Z}_{2^s}$-linear Hadamard codes are binary linear codes, i.e., for which types the code is permutation equivalent to the binary linear Hadamard code, H_t, of length $n = 2^t$. In [Kro01, PRV06], the linearity of these codes for $s = 2$ is proved.

Theorem 35 ([Kro01, PRV06])**.** *Let $\mathcal{H}^{t_1,t_2}$ be the quaternary linear Hadamard code of length 2^{t-1} and type $2^{t_2}4^{t_1}$, where $t = t_2 + 2t_1 - 1$, and let $H^{t_1,t_2} = \Phi(\mathcal{H}^{t_1,t_2})$ be the corresponding $\mathbb{Z}_4$-linear code of length 2^t. Then, only for $t_1 \in \{1, 2\}$, we have that H^{t_1,t_2} is permutation equivalent to the binary linear Hadamard code H_t of length 2^t.*

Lemma 36. *Let $\lambda_i \in \mathbb{Z}_2$, $i \in \{0, \ldots, s-2\}$. Then,*

$$\sum_{i=0}^{s-2} \lambda_i \phi(2^i) = \phi(\sum_{i=0}^{s-2} \lambda_i 2^i),$$

where $2^i \in \mathbb{Z}_{2^s}$.

Proof. Let y_i be the ith row of Y, where Y is a matrix of size $(s-1) \times 2^{s-1}$ which columns are the elements of $\mathbb{Z}_2^{s-1}$. Let e_i be the vector that has 1 in the ith position and 0 otherwise. By the definition of ϕ given by (2.19), we know that $\sum_{i=0}^{s-2} \lambda_i \phi(2^i) = \sum_{i=0}^{s-2} \lambda_i e_{i+1} Y = \sum_{i=0}^{s-2} \lambda_i y_{i+1} = \boldsymbol{\lambda} Y$, where $\boldsymbol{\lambda} = (\lambda_0, \ldots, \lambda_{s-2})$. Since $[\lambda_0, \ldots, \lambda_{s-2}, 0]_2$ is the binary expansion of $\sum_{i=0}^{s-2} \lambda_i 2^i$, then we have that $\boldsymbol{\lambda} Y = \phi(\sum_{i=0}^{s-2} \lambda_i 2^i)$. $\mathcal{QED}$

Proposition 37. *The $\mathbb{Z}_{2^s}$-linear Hadamard codes $H^{1,0,\ldots,0}$ and $H^{1,0,\ldots,0,1,0}$, with $s > 2$, are linear.*

Proof. By Example 24, we know that $H^{1,0\ldots,0}$ is linear.

Now, we consider $\mathcal{H} = \mathcal{H}^{1,0,\ldots,0,1,0}$ and $H = \Phi(\mathcal{H})$. Recall that the code $\mathcal{H}$ is generated by

$$A^{1,0,\ldots,0,1,0} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2^{s-2} & 2^{s-1} & 3 \cdot 2^{s-2} \end{pmatrix}.$$

Let $\boldsymbol{\beta}_i = (2^i, 2^i, 2^i, 2^i)$ for $0 \leq i \leq s-1$, $\boldsymbol{\beta}_s = (0, 2^{s-1}, 0, 2^{s-1})$ and $\boldsymbol{\beta}_{s+1} = (0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2})$. Let C be the linear code generated by $B = \{\Phi(\boldsymbol{\beta}_i) : 0 \leq i \leq s+1\}$. Now, we prove that $C \subseteq H$. Let $\mathbf{c} = \sum_{i=0}^{s+1} \lambda_i \Phi(\boldsymbol{\beta}_i) \in C$, where $\lambda_i \in \mathbb{Z}_2$. By Corollary 26, we only have to see that

$$\mathbf{c}' = \lambda_{s+1}\Phi(\boldsymbol{\beta}_{s+1}) + \sum_{i=0}^{s-2} \lambda_i \Phi(\boldsymbol{\beta}_i) \in H.$$

On the one hand, if $\lambda_{s+1} = 0$, then we have that $\mathbf{c}' \in H$, since $\sum_{i=0}^{s-2} \lambda_i \Phi(\boldsymbol{\beta}_i) = \Phi(\sum_{i=0}^{s-2} \lambda_i \boldsymbol{\beta}_i)$ by Lemma 36. On the other hand, if $\lambda_{s+1} = 1$, then we have that $\mathbf{c}' = \Phi((0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2})) + \Phi((u, u, u, u))$, where $u = \sum_{i=0}^{s-2} \lambda_i 2^i$. Let $U = \{2^{s-2}, \ldots, 2^{s-1} - 1\} \cup \{3 \cdot 2^{s-2}, \ldots, 2^s - 1\} \subset \mathbb{Z}_{2^s}$. Then, by Corollary 28, $\mathbf{c}' = \Phi((0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2}) + (u, u, u, u) + (0, 2^{s-1}, 0, 2^{s-1}))$ if $u \in U$, and $\mathbf{c}' = \Phi((0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2}) + (u, u, u, u))$ if $u \in \mathbb{Z}_{2^s} \setminus U$. In both cases, $\mathbf{c}' \in H$.

Since $|C| = |H| = 2^{s+2}$, then $C = H$, and thus H is linear. $\mathcal{QED}$

Let $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}_{2^s}^n$ and $[u_{i,0}, u_{i,1}, \ldots, u_{i,s-1}]_2$ be the binary expansion of u_i, $i \in \{1, \ldots, n\}$. Let p be an integer such that $p \in \{0, \ldots, s-1\}$. Then, we denote by $\mathbf{u}^{(p)}$ the binary vector having in the ith coordinate the pth element of the binary expansion of u_i, that is, $\mathbf{u}^{(p)} = (u_{1,p}, \ldots, u_{n,p})$.

Lemma 38. *If* $\mathbf{v} = 2^b(0, 1, \ldots, 2^a - 1) \in \mathbb{Z}_{2^s}^n$, *with* $n = 2^a$, $a \geq 1$ *and* $a + b \leq s$, *then* $\mathrm{wt}_H(\mathbf{v}^{(p)}) = 2^{a-1}$ *for all* $p \in \{b, \ldots, a+b-1\}$.

Proof. The 2^a coordinates of $\mathbf{v}$ contain exactly the 2^a elements of $\mathbb{Z}_{2^s}$ which have a binary expansion of the form $[0, \ldots, 0, v_b, v_{b+1}, \ldots, v_{a+b-1}, 0, \ldots, 0]_2$ with $v_p \in \{0, 1\}$, for all $p \in \{b, \ldots, a+b-1\}$. Note that we have 2^a different elements of $\mathbb{Z}_{2^s}$, represented by exactly a binary coordinates. Hence, half

of the coordinates of $\mathbf{v}$ satisfy that $v_p = 1$ and the other half that $v_p = 0$. Therefore, $\mathrm{wt}_H(\mathbf{v}^{(p)}) = 2^a/2 = 2^{a-1}$ for all $p \in \{b, \ldots, a+b-1\}$. $\mathcal{QED}$

As it is shown in [Kro01], the codes H^{1,t_2} and H^{2,t_2}, $t_2 \geq 0$, are the only $\mathbb{Z}_4$-linear Hadamard codes which are linear. In [BGL05], it is proved that the codes $H^{1,0,\ldots,0,t_s}$, $t_s \geq 0$, are linear. The next result shows that, for $s > 2$ and $t_s \geq 0$, the codes $H^{1,0,\ldots,0,1,t_s}$ and $H^{1,0,\ldots,0,t_s}$ are linear, and they are the only $\mathbb{Z}_{2^s}$-linear Hadamard codes which are linear.

Theorem 39. *The codes $H^{1,0,\ldots,0,1,t_s}$ and $H^{1,0,\ldots,0,t_s}$, with $s > 2$ and $t_s \geq 0$, are the only $\mathbb{Z}_{2^s}$-linear Hadamard codes which are linear.*

Proof. First, we show that these codes are linear by induction on t_s. By Proposition 37, the codes $H^{1,0,\ldots,0}$ and $H^{1,0,\ldots,0,1,0}$ are linear. We assume that $H = \Phi(\mathcal{H})$, where $\mathcal{H} = \mathcal{H}^{1,0,\ldots,0,t_{s-1},t_s}$, $t_{s-1} \in \{0,1\}$ and $t_s \geq 0$, is linear. Now, we prove that $H_s = H^{1,0,\ldots,0,t_{s-1},t_s+1}$ is linear. Since H is a linear Hadamard code of length $2^{t_s+2t_{s-1}-1}$, it is the Reed-Muller code $RM(1, t_s + 2t_{s-1} - 1)$ [MS77, Ch.13 §3]. By the iterative construction (3.1), we have that $H_s = \{\Phi((\mathbf{h}, \mathbf{h}) + (\mathbf{0}, \mathbf{v})) : \mathbf{h} \in \mathcal{H}, \mathbf{v} \in \{\mathbf{0}, \mathbf{2^{s-1}}\}\}$. By Corollary 26, $H_s = \{(\Phi(\mathbf{h}), \Phi(\mathbf{h}) + \Phi(\mathbf{v})) : \mathbf{h} \in \mathcal{H}, \mathbf{v} \in \{\mathbf{0}, \mathbf{2^{s-1}}\}\} = \{(\mathbf{h}', \mathbf{h}' + \mathbf{v}') : \mathbf{h}' \in H, \mathbf{v}' \in \{\mathbf{0}, \mathbf{1}\}\}$, which corresponds to the Reed-Muller code $RM(1, t_s + 2t_{s-1})$. Therefore, H_s is linear.

Now, we prove the nonlinearity of $H = \Phi(\mathcal{H})$, where $\mathcal{H} = \mathcal{H}^{1,0,\ldots,0,2,0}$. Let $\mathbf{r} = (0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2})$. Recall that $\mathcal{H}$ has length 16 and is generated by

$$A^{1,0,\ldots,0,2,0} = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{r} & \mathbf{r} & \mathbf{r} & \mathbf{r} \\ \mathbf{0} & \mathbf{2^{s-2}} & \mathbf{2^{s-1}} & \mathbf{3 \cdot 2^{s-2}} \end{pmatrix}.$$

By Corollaries 26 and 28, we have $\Phi((\mathbf{r}, \mathbf{r}, \mathbf{r}, \mathbf{r})) + \Phi((\mathbf{0}, \mathbf{2^{s-2}}, \mathbf{2^{s-1}}, \mathbf{3 \cdot 2^{s-2}})) = \Phi(\mathbf{z})$, where $\mathbf{z} = (\mathbf{r}, \mathbf{r}, \mathbf{r}, \mathbf{r}) + (\mathbf{0}, \mathbf{2^{s-2}}, \mathbf{2^{s-1}}, \mathbf{3 \cdot 2^{s-2}}) + (\mathbf{0}, \mathbf{u}, \mathbf{0}, \mathbf{u})$ and $\mathbf{u} = (0, 2^{s-1}, 0, 2^{s-1})$. Since $\mathcal{H}$ is linear over $\mathbb{Z}_{2^s}$, $\mathbf{z} \in \mathcal{H}$ if and only if $(\mathbf{0}, \mathbf{u}, \mathbf{0}, \mathbf{u}) \in \mathcal{H}$. Since $\mathrm{wt}_H(\Phi((\mathbf{0}, \mathbf{u}, \mathbf{0}, \mathbf{u}))) = 4 \cdot 2^{s-1} = N/4$, where N is the length of H, $\Phi((\mathbf{0}, \mathbf{u}, \mathbf{0}, \mathbf{u})) \notin H$, so $\Phi(\mathbf{z}) \notin H$. Therefore, $H = H^{1,0,\ldots,0,2,0}$ is nonlinear.

Let $H = \Phi(\mathcal{H})$, where $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$. For any $i \in \{1,\ldots,s\}$, we define $H_i = \Phi(\mathcal{H}_i)$, where $\mathcal{H}_i = \mathcal{H}^{t'_1,\ldots,t'_s}$, $t'_i = t_i + 1$ and $t'_j = t_j$ for $j \neq i$.

Next, we consider $H = \Phi(\mathcal{H})$, where $\mathcal{H} = \mathcal{H}^{1,0,\ldots,0}$, and we prove that H_i is nonlinear for any $i \in \{1,\ldots,s-2\}$. Note that the generator matrix of $\mathcal{H}_i$ has two rows: $\mathbf{w}_1 = \mathbf{1}$ and $\mathbf{w}_2 = 2^{i-1}(0,1,\ldots,2^{s+1-i}-1)$. By Corollary 25, we know that $\Phi(\mathbf{w}_2)+\Phi(\mathbf{2^{i-1}}) = \Phi(\mathbf{w}_2+\mathbf{2^{i-1}}-2^i\mathbf{w}_2^{(i-1)})$. Therefore, we just need to show that $2^i\mathbf{w}_2^{(i-1)} \notin \mathcal{H}_i$. We have that $\mathrm{wt}_H(\mathbf{w}_2^{(i-1)}) = 2^{s-i}$ by Lemma 38. Since $2^i \notin \{0, 2^{s-1}\}$, $\mathrm{wt}_H(\phi(2^i)) = 2^{s-2}$. Then, $\mathrm{wt}_H(\Phi(2^i\mathbf{w}_2^{(i-1)})) = 2^{s-i} \cdot 2^{s-2} = 2^{2s-2-i}$. Recall that the length of H is $N = 2^t$, where $t = 2s - i$. Therefore, we have that $\mathrm{wt}_H(\Phi(2^i\mathbf{w}_2^{(i-1)})) = 2^{t-2} = N/4$, and then $\Phi(2^i\mathbf{w}_2^{(i-1)}) \notin H_i$.

Finally, in general, for $H = \Phi(\mathcal{H})$, where $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$, we prove that if H is nonlinear, then H_i is nonlinear for any $i \in \{1,\ldots,s\}$. Assume that H_i is linear. Then, by the iterative construction (3.1), for any $\mathbf{u}, \mathbf{v} \in \mathcal{H}$, we have that $(\mathbf{u},\ldots,\mathbf{u}), (\mathbf{v},\ldots,\mathbf{v}) \in \mathcal{H}_i$. Moreover, since H_i is linear, $\Phi((\mathbf{u},\ldots,\mathbf{u}))+\Phi((\mathbf{v},\ldots,\mathbf{v})) = \Phi((\mathbf{a},\ldots,\mathbf{a})+\lambda\cdot 2^{i-1}(0,1,\ldots,2^{s-i+1}-1)) \in H_i$, where $\mathbf{a} \in \mathcal{H}$ and $\lambda \in \mathbb{Z}_{2^s}$. Therefore, $\Phi(\mathbf{u}) + \Phi(\mathbf{v}) = \Phi(\mathbf{a}) \in H$, and we have that H is linear and the result follows. $\mathcal{QED}$

Table 3.1 shows the types for all $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, with $4 \leq t \leq 6$ and $2 \leq s \leq 7$. Moreover, the values for which the codes are linear are shown in bold type. The pairs (r,k), where r is the rank and k the dimension of the kernel, are also given in this table. Note that the values of the rank and dimension of the kernel are the same in these cases.

	$t=4$		$t=5$		$t=6$	
	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)
$\mathbb{Z}_4$	$(\mathbf{1},\mathbf{3})$	(5,5)	$(\mathbf{1},\mathbf{4})$	(6,6)	$(\mathbf{1},\mathbf{5})$	(7,7)
	$(\mathbf{2},\mathbf{1})$	(5,5)	$(\mathbf{2},\mathbf{2})$	(6,6)	$(\mathbf{2},\mathbf{3})$	(7,7)
			$(3,0)$	(7,4)	$(3,1)$	(8,5)
$\mathbb{Z}_8$	$(\mathbf{1},\mathbf{0},\mathbf{2})$	(5,5)	$(\mathbf{1},\mathbf{0},\mathbf{3})$	(6,6)	$(\mathbf{1},\mathbf{0},\mathbf{4})$	(7,7)
	$(\mathbf{1},\mathbf{1},\mathbf{0})$	(5,5)	$(\mathbf{1},\mathbf{1},\mathbf{1})$	(6,6)	$(\mathbf{1},\mathbf{1},\mathbf{2})$	(7,7)
			$(2,0,0)$	(8,3)	$(1,2,0)$	(8,5)
					$(2,0,1)$	(9,4)
$\mathbb{Z}_{16}$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1})$	(5,5)	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{2})$	(6,6)	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{3})$	(7,7)
			$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	(6,6)	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	(7,7)
					$(1,1,0,0)$	(9,4)
$\mathbb{Z}_{32}$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0})$	(5,5)	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$	(6,6)	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{2})$	(7,7)
					$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	(7,7)
$\mathbb{Z}_{64}$			$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0})$	(6,6)	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$	(7,7)
$\mathbb{Z}_{128}$					$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0})$	(7,7)

Table 3.1: Types for all $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t.

Chapter 4

Kernel of $\mathbb{Z}_{2^s}$-linear Hadamard codes

"Sometimes science is a lot more art, than science. A lot of people don't get that."
– Rick Sánchez, Rick and Morty

The computation of the kernel (and also of the rank) and its dimension for $\mathbb{Z}_4$-linear Hadamard codes is given in [Kro01, PRV06]. In these papers, a complete classification of these codes, up to permutation equivalence, just by using the dimension of the kernel (or the rank) is given. As a first step in the generalization of the results for $\mathbb{Z}_4$-linear Hadamard codes, in [FPV10, KV15, MR15], the dimension of the kernel for $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes and Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes is computed.

The aim of this chapter is to generalize the computation of the kernel and its dimension for $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s > 2$, in order to give a partial classification of these codes by using this invariant. In Section 4.1, we describe the kernel and compute its dimension whenever they are nonlinear. In Section 4.2, through several examples, we show that, unlike for $s = 2$, the dimension of the kernel is not enough to classify completely $\mathbb{Z}_{2^s}$-linear Hadamard codes for some values of t and s. Moreover, we give the exact amount of nonequivalent such codes up to $t = 11$ for any $s \geq 2$, by using also the rank.

4.1 Computation of the kernel

In this section, we study the kernel and its dimension of the $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s > 2$. Specifically, we give a basis of the kernel for the codes which are nonlinear, and we stablish its dimension.

Let $\mathcal{H}^{t_1,\ldots,t_s}$ be a $\mathbb{Z}_{2^s}$-additive Hadamard code and $H^{t_1,\ldots,t_s}$ its corresponding $\mathbb{Z}_{2^s}$-linear code. Let $A^{t_1,\ldots,t_s}$ be the generator matrix of $\mathcal{H}^{t_1,\ldots,t_s}$, considered along this dissertation, and let $\mathbf{w}_i$ be the ith row vector of $A^{t_1,\ldots,t_s}$. By construction, $\mathbf{w}_1 = \mathbf{1}$ and $\mathrm{ord}(\mathbf{w}_i) \leq \mathrm{ord}(\mathbf{w}_j)$ if $i > j$.

In Section 3.2, we determine which $\mathbb{Z}_{2^s}$-linear Hadamard codes $H^{t_1,\ldots,t_s}$ of length 2^t are linear. For all these cases which are linear, we have that $\ker(H^{t_1,\ldots,t_s}) = \mathrm{rank}(H^{t_1,\ldots,t_s}) = t + 1$, since $|H^{t_1,\ldots,t_s}| = 2^{t+1}$. Moreover, in this case, the set $\{\Phi(2^{p_i}\mathbf{w}_i) : 1 \leq i \leq t_1 + \cdots + t_s, 0 \leq p_i \leq \sigma_i\}$ where $\mathrm{ord}(\mathbf{w}_i) = 2^{\sigma_i}$, is a basis of $K(H^{t_1,\ldots,t_s})$ and $\langle H^{t_1,\ldots,t_s}\rangle$.

Example 40. *Considering all nonnegative integer solutions with $t_1 \geq 1$ of the equation $5 = 3t_1+2t_2+t_3-1$, we have that the $\mathbb{Z}_8$-linear Hadamard codes of length $2^t = 32$ are the following: $H^{1,0,3}$, $H^{1,1,1}$ and $H^{2,0,0}$. By Theorem 39, we have that $H^{1,0,3}$ and $H^{1,1,1}$ are linear, so $ker(H^{1,0,3}) = ker(H^{1,1,1}) = 6$. By the same theorem, we also have that $H^{2,0,0}$ is nonlinear, so $ker(H^{2,0,0}) < 6$.*

We define $\sigma \in \{1,\ldots,s\}$ as the integer such that

$$\mathrm{ord}(\mathbf{w}_2) = 2^{s+1-\sigma}. \tag{4.1}$$

Note that $\sigma = 1$ if $t_1 > 1$, and $\sigma = \min\{i : t_i > 0, i \in \{2,\ldots,s\}\}$ if $t_1 = 1$. In the case $\sigma = s$, the code is $\mathcal{H}^{1,0,\ldots,0,t_s}$, which is linear. In what follows, we will see that this parameter, σ, is a sort of measure of nonlinearity, like the rank and dimension of the kernel.

Example 41. *Considering all nonnegative integer solutions with $t_1 \geq 1$ of the equation $7 = 4t_1+3t_2+2t_3+t_4-1$, we have that the $\mathbb{Z}_{16}$-linear Hadamard codes of length $2^t = 128$ are the following: $H^{1,0,0,4}$, $H^{1,0,1,2}$, $H^{1,0,2,0}$, $H^{1,1,0,1}$ and $H^{2,0,0,0}$. The corresponding value of σ for each code is $4, 3, 3, 2$ and 1, respectively.*

Proposition 42. *Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{2^s}$-additive Hadamard code of type $(n; t_1, \ldots, t_s)$ such that $\Phi(\mathcal{H})$ is nonlinear. Let $\mathcal{H}_b$ be the subcode of $\mathcal{H}$ which contains all the codewords of order two. Let $P = \{\mathbf{2^p}\}_{p=0}^{\sigma-2}$ if $\sigma \geq 2$, and $P = \emptyset$ if $\sigma = 1$. Then,*

$$\left\langle \Phi(\mathcal{H}_b), \Phi(P), \Phi(\sum_{i=0}^{s-2} \mathbf{2^i}) \right\rangle \subseteq K(\Phi(\mathcal{H}))$$

and $ker(\Phi(\mathcal{H})) \geq \sigma + \sum_{i=1}^{s} t_i$.

Proof. Let $H = \Phi(\mathcal{H})$ and $\tau = \sum_{i=1}^{s} t_i$. Let $Q = \{(\mathrm{ord}(\mathbf{w}_q)/2)\mathbf{w}_q\}_{q=0}^{\tau}$. Since $\mathcal{H}_b$ contains all the elements of $\mathcal{H}$ of order two, we have that the set $\Phi(Q)$ is a basis for the binary linear subcode $H_b = \Phi(\mathcal{H}_b)$ of H. By Corollary 26, for all $\mathbf{b} \in \mathcal{H}_b$ and $\mathbf{u} \in \mathcal{H}$, we have that $\Phi(\mathbf{b}) + \Phi(\mathbf{u}) = \Phi(\mathbf{b} + \mathbf{u}) \in H$ and, therefore, $H_b \subseteq K(H)$.

Assume $\sigma \geq 2$. Now, we prove that $\Phi(\mathbf{2^p}) \in K(H)$ for all $p \in \{0, \ldots, \sigma - 2\}$. Equivalently, we show that $\Phi(\mathbf{2^p}) + \Phi(\mathbf{u}) \in H$ for all $\mathbf{u} \in \mathcal{H}$. If $\mathbf{u} \in \mathcal{H}$, then $\mathbf{u} = \lambda \cdot \mathbf{1} + \mathbf{u'}$, where $\lambda \in \mathbb{Z}_{2^s}$ and $\mathrm{ord}(\mathbf{u'}) \leq \mathrm{ord}(\mathbf{w}_2) = 2^{s+1-\sigma}$. Let $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}_{2^s}^n$ and $[u_{i,0}, u_{i,1}, \ldots, u_{i,s-1}]_2$ be the binary expansion of u_i, $i \in \{1, \ldots, n\}$. Let $[\lambda_0, \lambda_1, \ldots, \lambda_{s-1}]_2$ be the binary expansion of $\lambda \in \mathbb{Z}_{2^s}$. By Corollary 25, we have that $\Phi(\mathbf{2^p}) + \Phi(\mathbf{u}) = \Phi(\mathbf{2^p} + \mathbf{u} - 2^{p+1}\mathbf{u}^{(p)})$, where $\mathbf{u}^{(p)} = (u_{1,p}, \ldots, u_{n,p})$. Note that if $v \in \mathbb{Z}_{2^s}$ is of order 2^j, then its binary expansion is of the form $[0, \ldots, 0, 1, v_{s-j+1}, \ldots, v_{s-1}]_2$. Since $p \in \{0, \ldots, \sigma - 2\}$ and $\mathrm{ord}(\mathbf{u'}) \leq 2^{s+1-\sigma}$, we have that $\mathbf{u}^{(p)} = (\lambda_p, \ldots, \lambda_p)$. Therefore, $2^{p+1}\mathbf{u}^{(p)} = \lambda_p \mathbf{2^{p+1}} \in \mathcal{H}$ and $\Phi(\mathbf{2^p}) + \Phi(\mathbf{u}) = \Phi(\mathbf{2^p} + \mathbf{u} - \lambda_p \mathbf{2^{p+1}}) \in H$.

Next, we show that $\Phi(\sum_{i=0}^{s-2} \mathbf{2^i}) \in K(H)$. Let $\mathbf{u} = (u_1, \ldots, u_n) \in \mathcal{H}$ and $\mathbf{v} = (v_1, \ldots, v_n) = \sum_{i=0}^{s-2} \mathbf{2}^i$. First, we prove that $\phi(v_i) + \phi(u_i) = \phi(v_i + u_i - 2u_i)$ for all $i \in \{1, \ldots, n\}$. Note that the binary expansion of v_i and u_i are $[1, \ldots, 1, 0]_2$ and $[u_{i,0}, u_{i,1}, \ldots, u_{i,s-1}]_2$, respectively. Then, it is easy to check that $2(v_i \odot u_i) = 2u_i$. Therefore, by Proposition 19, $\phi(v_i) + \phi(u_i) = \phi(v_i + u_i - 2u_i)$. Hence, $\Phi(\mathbf{v}) + \Phi(\mathbf{u}) = \Phi(\mathbf{v} + \mathbf{u} - 2\mathbf{u}) \in H$ for all $\mathbf{u} \in \mathcal{H}$.

Finally, we have to see that the elements belonging to the set $\{\Phi(Q), \Phi(P), \Phi(\sum_{i=0}^{s-2} \mathbf{2^i})\}$ are linearly independent. By construction, the generator matrix

$A^{t_1,\ldots,t_s}$ is a block upper triangular matrix, so it is easy to see that the codewords in $\Phi(Q)$ are linearly independent of the ones in $\{\Phi(P), \Phi(\sum_{i=0}^{s-2} \mathbf{2^i})\}$. Note that $\sigma < s$ since H is nonlinear. Thus, by Lemma 36, it is easy to see that the codewords in $\{\Phi(P), \Phi(\sum_{i=0}^{s-2} \mathbf{2^i})\}$ are linearly independent. Therefore, we have that the dimension of the linear span of this set is $\sigma + \tau$, so $\ker(H) \geq \sigma + \tau$. $\mathcal{QED}$

Lemma 43. *Let $v \in \mathbb{Z}_{2^s}$ and $\lambda_i \in \mathbb{Z}_2$, $i \in \{0, \ldots, s-1\}$. Then,*

$$v \odot \sum_{i=0}^{s-1} \lambda_i 2^i = \sum_{i=0}^{s-1} v \odot \lambda_i 2^i.$$

Proof. Let $v \in \mathbb{Z}_{2^s}$ and $[v_0, v_1, \ldots, v_{s-1}]_2$ its binary expansion. By definition, we have that $v \odot \sum_{i=0}^{s-1} \lambda_i 2^i = \sum_{i=0}^{s-1} v_i \lambda_i 2^i$. Note that $v_i \lambda_i 2^i = v \odot \lambda_i 2^i$, so $v \odot \sum_{i=0}^{s-1} \lambda_i 2^i = \sum_{i=0}^{s-1} v \odot \lambda_i 2^i$. $\mathcal{QED}$

Lemma 44. *Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{2^s}$-additive Hadamard code of type $(n; t_1, \ldots, t_s)$. Let $\mathcal{N} = \{\sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{2^i} : \lambda_i \in \mathbb{Z}_2\} \setminus \{\sum_{i=\sigma-1}^{s-2} \mathbf{2^i}\}$ if $\sigma \leq s-1$. Then, $\Phi(\mathcal{N}) \cap K(\Phi(\mathcal{H})) = \{\mathbf{0}\}$.*

Proof. Let $H = \Phi(\mathcal{H})$. Let $\mathbf{u} = \sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{2^i} \in \mathcal{N}$ such that $\Phi(\mathbf{u}) \in K(H)$. We want to prove that $\mathbf{u} = \mathbf{0}$.

By construction, the second row $\mathbf{w}_2$ of $A^{t_1,\ldots,t_s}$ is a $2^{t-2s+\sigma}$-fold replication of $\mathbf{v} = 2^{\sigma-1}(0, 1, \ldots, 2^{s+1-\sigma} - 1)$, and $\mathrm{ord}(\mathbf{w}_2) = 2^{s+1-\sigma}$. By Proposition 19, we have that $\Phi(\mathbf{w}_2) + \Phi(\mathbf{u}) = \Phi(\mathbf{w}_2 + \mathbf{u} - 2(\mathbf{w}_2 \odot \mathbf{u}))$. Since $\Phi(\mathbf{u}) \in K(H)$, $2(\mathbf{w}_2 \odot \mathbf{u}) \in \mathcal{H}$. Note that, by Lemma 43, we have that $2(\mathbf{w}_2 \odot \mathbf{u}) = 2\sum_{i=\sigma-1}^{s-2} \mathbf{w}_2 \odot \lambda_i \mathbf{2^i} = 2\sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{w}_2^{(i)} 2^i \in \mathcal{H}$.

Let $\tau = \sum_{i=1}^{s} t_i$. If $\tau = 2$, then $\mathcal{H}$ has length $2^{s+1-\sigma}$ and the only rows in $A^{t_1,\ldots,t_s}$ are $\mathbf{1}$ and $\mathbf{w}_2 = \mathbf{v}$. If $\tau \geq 3$, for $i \in \{3, \ldots, \tau\}$, the ith row $\mathbf{w}_i$ of $A^{t_1,\ldots,t_s}$ contains zeros in the first $2^{s+1-\sigma}$ coordinates by construction. Since $\sigma \leq s-1$, $\tau \geq 2$, and hence any element of $\mathcal{H}$ restricted to the first $2^{s+1-\sigma}$ coordinates is of the form $\mu_1 \mathbf{1} + \mu_2 \mathbf{v}$ for some $\mu_1, \mu_2 \in \mathbb{Z}_{2^s}$. We have that $2\sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{w}_2^{(i)} 2^i$ restricted to the first $2^{s+1-\sigma}$ coordinates is $2\sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{v}^{(i)} 2^i$, so we have to find $\mu_1, \mu_2 \in \mathbb{Z}_{2^s}$ such that $2\sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{v}^{(i)} 2^i = \mu_1 \mathbf{1} + \mu_2 \mathbf{v}$.

Since the first coordinate of $\mathbf{v}$ is 0, the first coordinate of $\mathbf{v}^{(i)}$ is 0 for all i. Then, we have that $\mu_1 = 0$, so $2\sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{v}^{(i)} 2^i = \mu_2 \mathbf{v}$. Note that $\mathbf{v} = \sum_{i=0}^{s-1} \mathbf{v}^{(i)} 2^i = \sum_{i=\sigma-1}^{s-1} \mathbf{v}^{(i)} 2^i$. Therefore, $2\sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{v}^{(i)} 2^i = \mu_2 \sum_{i=\sigma-1}^{s-1} \mathbf{v}^{(i)} 2^i$. Since $\mathbf{u} \in \mathcal{N}$, there exists $j \in \{\sigma-1, \ldots, s-2\}$ such that $\lambda_j = 0$. Then, regrouping the terms, we obtain that

$$\sum_{\substack{i=\sigma-1 \\ i\neq j}}^{s-2} (\mu_2 - 2\lambda_i)\mathbf{v}^{(i)} 2^i + \mu_2 \mathbf{v}^{(j)} 2^j + \mu_2 \mathbf{v}^{(s-1)} 2^{s-1} = \mathbf{0}.$$

Note that $\{\mathbf{v}^{(i)}\}_{i=\sigma-1}^{s-1}$ is a subset of a basis of the $RM(1,t)$. Then, we have that $(\mu_2 - 2\lambda_i)2^i = 0$, for $i \in \{\sigma-1, \cdots, s-2\} \setminus \{j\}$, $\mu_2 2^j = 0$ and $\mu_2 2^{s-1} = 0$. As a result, $\mu_2 = 0$ and $\lambda_i = 0$ for all $i \in \{\sigma-1, \cdots, s-2\}$. Hence, $\mathbf{u} = \sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{2^i} = \mathbf{0}$, and the result holds. $\mathcal{QED}$

Lemma 45. *Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{2^s}$-additive Hadamard code of type $(n; t_1, \ldots, t_s)$. Let $\mathbf{w}_i$ be the ith row of $A^{t_1,\ldots,t_s}$ and $\tau = \sum_{i=1}^{s} t_i$. Let $\mathcal{M} = \{\mathbf{v} = \sum_{i=2}^{\tau-t_s} \lambda_i \mathbf{w}_i : \lambda_i \in \mathbb{Z}_{2^s}, \mathrm{ord}(\mathbf{v}) > 2\}$, $\mathcal{N} = \{\sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{2^i} : \lambda_i \in \mathbb{Z}_2\} \setminus \{\sum_{i=\sigma-1}^{s-2} \mathbf{2^i}\}$ if $\sigma \leq s-1$ and $\mathcal{M}+\mathcal{N} = \{\mathbf{v}_\mathcal{M} + \mathbf{v}_\mathcal{N} : \mathbf{v}_\mathcal{M} \in \mathcal{M} \cup \{\mathbf{0}\}, \mathbf{v}_\mathcal{N} \in \mathcal{N}\}$. Then, $\Phi(\mathcal{M}+\mathcal{N}) \cap K(\Phi(\mathcal{H})) = \{\mathbf{0}\}$.*

Proof. Let $H = \Phi(\mathcal{H})$, which has length $N = 2^t = n \cdot 2^{s-1}$. By Lemma 44, we already know that $\Phi(\mathcal{N}) \cap K(H) = \{\mathbf{0}\}$. Now, we prove that $\Phi(\mathcal{M}) \cap K(H) = \emptyset$.

Let $\mathbf{v} = \sum_{i=2}^{\tau-t_s} \lambda_i \mathbf{w}_i \in \mathcal{M}$. Since $\mathrm{ord}(\mathbf{v}) > 2$ and $\mathrm{ord}(\mathbf{w}_i) \leq 2^{s+1-\sigma}$, $\mathrm{ord}(\mathbf{v}) = 2^p$ for some $2 \leq p \leq s+1-\sigma$. By the iterative construction (3.1) of $A^{t_1,\ldots,t_s}$, we know that all the elements of $\mathbb{Z}_{2^s}$ of order equal to or less than 2^p appear as a coordinate of $\mathbf{v}$. Moreover, exactly half of the coordinates of $\mathbf{v}$ are of order 2^p. We consider two cases depending on the value of p.

First, we consider that $2 < p \leq s+1-\sigma$. We have that $\Phi(\mathbf{v}) + \Phi(\mathbf{2^{s-p}}) = \Phi(\mathbf{v} + \mathbf{2^{s-p}} - 2^{s-p+1}\mathbf{v}^{(s-p)})$ by Corollary 25. As before, it is enough to see that $2^{s-p+1}\mathbf{v}^{(s-p)} \notin \mathcal{H}$ to prove that $\Phi(\mathbf{v}) \notin K(H)$. Since half of the coordinates of $\mathbf{v}$ are of order 2^p and the other half are of order less than 2^p, we have that half of the coordinates of $2^{s-p+1}\mathbf{v}^{(s-p)}$ are equal to 2^{s-p+1} and the rest of coordinates are zero. Note that $2^{s-p+1} \notin \{0, 2^{s-1}\}$ since $p > 2$. Therefore,

since $\mathrm{wt}_H(\phi(2^{s-p+1})) = 2^{s-2}$, we have that $\mathrm{wt}_H(\Phi(2^{s-p+1}\mathbf{v}^{(s-p)})) = n/2 \cdot 2^{s-2} = 2^{t-2} = N/4$ and hence $\Phi(\mathbf{v}) \notin K(H)$.

Next, we consider that $p = 2$, that is, $\mathrm{ord}(\mathbf{v}) = 4$. Then, $\mathrm{ord}(\lambda_i \mathbf{w}_i) = 4$ or $\lambda_i = 0$ for all $i \in \{2, \ldots, \tau - t_s\}$. By Proposition 19, $\Phi(\mathbf{v}) + \Phi(2^{s-\sigma-1}\mathbf{w}_2) = \Phi(\mathbf{v} + 2^{s-\sigma-1}\mathbf{w}_2 - 2(\mathbf{v} \odot 2^{s-\sigma-1}\mathbf{w}_2))$. Again, it is enough to see that $2(\mathbf{v} \odot 2^{s-\sigma-1}\mathbf{w}_2) \notin \mathcal{H}$ to show that $\Phi(\mathbf{v}) \notin K(H)$. Note that $2^{s-\sigma-1}\mathbf{w}_2$ is a 2^{t-s-1}-fold replication of $\mathbf{b}_1 = (0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2})$. Now, we consider the coordinates divided into groups of 4 consecutive coordinates, which will be referred to as blocks. Note that every block of $\lambda_i \mathbf{w}_i$ contains the same value in its 4 coordinates, for all $i \in \{3, \ldots, \tau - t_s\}$.

If $\lambda_2 = 0$, then every block of $\mathbf{v}$ also contains the same value in its 4 coordinates. Thus, every block in $2(\mathbf{v} \odot 2^{s-\sigma-1}\mathbf{w}_2)$ is of the form $2(\mathbf{k} \odot \mathbf{b}_1)$ for some $k \in \{0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2}\}$. We have that

$$2(\mathbf{k} \odot \mathbf{b}_1) = \begin{cases} (0,0,0,0) & \text{if } k \in \{0, 2^{s-1}\} \\ (0, 2^{s-1}, 0, 2^{s-1}) & \text{if } k \in \{2^{s-2}, 3 \cdot 2^{s-2}\}. \end{cases}$$

By construction, note that $\mathbf{v}$ contains the same number of blocks $\mathbf{k}$ for each $k \in \{0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2}\}$. Then, it is easy to see that $\mathrm{wt}_H(\Phi(2(\mathbf{v} \odot 2^{s-\sigma-1}\mathbf{w}_2))) = \mathrm{wt}_H(\phi(2^{s-1})) \cdot 4 \cdot n/16 = 2^{s-1} \cdot n/4 = 2^{t-2} = N/4$, so $\Phi(\mathbf{v}) \notin K(H)$ in this case.

Otherwise, if $\lambda_2 \neq 0$, then every block of $\mathbf{v}$ is of the form $\mathbf{b}_i + \mathbf{k}$, for some $i \in \{1, 2\}$ and $k \in \{0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2}\}$, where $\mathbf{b}_1 = (0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2})$ and $\mathbf{b}_2 = (0, 3 \cdot 2^{s-2}, 2^{s-1}, 2^{s-2})$. Then, we have that

$$2((\mathbf{b}_i + \mathbf{k}) \odot \mathbf{b}_1) = \begin{cases} (0,0,0,0) & \text{if } k \in \{2^{s-2}, 3 \cdot 2^{s-2}\} \\ (0, 2^{s-1}, 0, 2^{s-1}) & \text{if } k \in \{0, 2^{s-1}\}, \end{cases}$$

for $i \in \{1, 2\}$. Again, by construction, $\mathbf{v}$ contains the same number of blocks $\mathbf{b}_i + \mathbf{k}$ for each $k \in \{0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2}\}$. Therefore, as before, $\mathrm{wt}_H(\Phi(2(\mathbf{v} \odot 2^{s-\sigma-1}\mathbf{w}_2))) = N/4$, and $\Phi(\mathbf{v}) \notin K(H)$. We have just shown that $\Phi(\mathcal{M}) \cap K(H) = \emptyset$.

Now, we prove that $\Phi(\mathcal{M} + \mathcal{N}) \cap K(H) = \{\mathbf{0}\}$. Let $\mathbf{v} = \mathbf{v}_\mathcal{M} + \mathbf{v}_\mathcal{N} \in \mathcal{M} + \mathcal{N} \backslash \{\mathbf{0}\}$, where $\mathbf{v}_\mathcal{M} \in \mathcal{M}$ and $\mathbf{v}_\mathcal{N} \in \mathcal{N}$. We just proved that $\Phi(\mathbf{v}) \notin$

$K(H)$ if $\mathbf{v}_{\mathcal{M}} = \mathbf{0}$ or $\mathbf{v}_{\mathcal{N}} = \mathbf{0}$. Therefore, we can assume that $\mathbf{v}_{\mathcal{M}} \neq \mathbf{0}$ and $\mathbf{v}_{\mathcal{N}} \neq \mathbf{0}$.

We know that $\mathbf{v}_{\mathcal{N}} = (v, \ldots, v)$. Let $[v_0, v_1, \ldots, v_{s-1}]_2$ be the binary expansion of v. Let $v_{\mathcal{N}_1}$ and $v_{\mathcal{N}_2}$ be the elements of $\mathbb{Z}_{2^s}$ having binary expansion $[0, \ldots, 0, v_{s-p}, \ldots, v_{s-1}]_2$ and $[v_0, \ldots, v_{s-p-1}, 0, \ldots, 0]_2$, respectively. Then, $\mathbf{v}_{\mathcal{N}} = \mathbf{v}_{\mathcal{N}_1} + \mathbf{v}_{\mathcal{N}_2}$, where $\mathbf{v}_{\mathcal{N}_i} = (v_{\mathcal{N}_i}, \ldots, v_{\mathcal{N}_i})$ for $i \in \{1, 2\}$. Since $\mathrm{ord}(\mathbf{v}_{\mathcal{M}}) = 2^p$ with $2 \leq p \leq s + 1 - \sigma$, the binary expansion of each one of its coordinates is of the form $[0, \ldots, 0, (v_{\mathcal{M}})_{s-p}, \ldots, (v_{\mathcal{M}})_{s-1}]_2$. Note that we also have that $\mathrm{ord}(\mathbf{v}_{\mathcal{N}_1}) \leq \mathrm{ord}(\mathbf{v}_{\mathcal{M}})$ by construction.

On the one hand, we consider $2 < p \leq s + 1 - \sigma$. It is easy to see that $2(\mathbf{v}_{\mathcal{N}_2} \odot \mathbf{2^{s-p}}) = \mathbf{0}$. Therefore, $\mathrm{wt}_H(\Phi(2(\mathbf{v} \odot \mathbf{2^{s-p}}))) = \mathrm{wt}_H(\Phi(2((\mathbf{v}_{\mathcal{M}} + \mathbf{v}_{\mathcal{N}_1}) \odot \mathbf{2^{s-p}})))$. Since $\mathrm{ord}(\mathbf{v}_{\mathcal{N}_1}) \leq \mathrm{ord}(\mathbf{v}_{\mathcal{M}})$, it is easy to see that there exists a permutation of coordinates π such that $\pi(\mathbf{v}_{\mathcal{M}} + \mathbf{v}_{\mathcal{N}_1}) = \mathbf{v}_{\mathcal{M}}$. Thus, $\mathrm{wt}_H(\Phi(2((\mathbf{v}_{\mathcal{M}} + \mathbf{v}_{\mathcal{N}_1}) \odot \mathbf{2^{s-p}}))) = \mathrm{wt}_H(\Phi(2(\mathbf{v}_{\mathcal{M}} \odot \mathbf{2^{s-p}})))$ and the result holds by using the same arguments as above.

On the other hand, we consider that $p = 2$. Note that $\mathrm{ord}(\mathbf{v}_{\mathcal{M}}) = 4$, and then $\mathrm{ord}(\mathbf{v}_{\mathcal{N}_1}) = 4$. It is easy to see that $2(\mathbf{v}_{\mathcal{N}_2} \odot 2^{s-\sigma-1}\mathbf{w}_2) = \mathbf{0}$, hence we have that $\mathrm{wt}_H(\Phi(2(\mathbf{v} \odot 2^{s-\sigma-1}\mathbf{w_2}))) = \mathrm{wt}_H(\Phi(2((\mathbf{v}_{\mathcal{M}} + \mathbf{v}_{\mathcal{N}_1}) \odot 2^{s-\sigma-1}\mathbf{w_2})))$. Recall that $2^{s-\sigma-1}\mathbf{w}_2$ is the 2^{t-s-1}-fold replication of $\mathbf{b}_1$. Taking into account that $\mathbf{v}_{\mathcal{M}} = \sum_{i=2}^{\tau-t_s} \lambda_i \mathbf{w}_i$, note that the blocks of $\mathbf{v}_{\mathcal{M}} + \mathbf{v}_{\mathcal{N}_1}$ are of the form $\mathbf{k}$ for some $k \in \{0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2}\}$ if $\lambda_2 = 0$; or $\mathbf{b}_i + \mathbf{k}$ for some $k \in \{0, 2^{s-2}, 2^{s-1}, 3 \cdot 2^{s-2}\}$ and $i \in \{1, 2\}$ if $\lambda_2 \neq 0$. Therefore, the proof is analogous to the above one to show that $\Phi(\mathbf{v}) \notin K(H)$ with $\mathbf{v} \in \mathcal{M}$. Then, the result holds. $\mathcal{QED}$

Theorem 46. *Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{2^s}$-additive Hadamard code of type $(n; t_1, \ldots, t_s)$ such that $\Phi(\mathcal{H})$ is nonlinear. Let $\mathcal{H}_b$ be the subcode of $\mathcal{H}$ which contains all the codewords of order two. Let $P = \{\mathbf{2^p}\}_{p=0}^{\sigma-2}$ if $\sigma \geq 2$, and $P = \emptyset$ if $\sigma = 1$. Then,*

$$\left\langle \Phi(\mathcal{H}_b), \Phi(P), \Phi(\sum_{i=0}^{s-2} \mathbf{2^i}) \right\rangle = K(\Phi(\mathcal{H}))$$

and $ker(\Phi(\mathcal{H})) = \sigma + \sum_{i=1}^{s} t_i$.

Proof. The result follows by Proposition 42, Lemma 44 and Lemma 45. $\mathcal{QED}$

Corollary 47. *Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{2^s}$-additive Hadamard code of type $(n; t_1, \ldots, t_s)$ such that $\Phi(\mathcal{H})$ is nonlinear. Let $\mathbf{w}_i$ be the ith row of $A^{t_1,\ldots,t_s}$ and $\tau = \sum_{i=1}^{s} t_i$. Let $Q = \{(\mathrm{ord}(\mathbf{w}_q)/2)\mathbf{w}_q\}_{q=0}^{\tau}$ and $P = \{\mathbf{2^p}\}_{p=0}^{\sigma-2}$ if $\sigma \geq 2$, and $P = \emptyset$ if $\sigma = 1$. Then, $\{\Phi(Q), \Phi(P), \Phi(\sum_{i=0}^{s-2} \mathbf{2^i})\}$ is a basis of $K(\Phi(\mathcal{H}))$.*

Proof. Straightforward from Proposition 42 and Theorem 46. $\mathcal{QED}$

Example 48. *Let $H^{2,0,0}$ be the $\mathbb{Z}_8$-linear Hadamard code considered in Example 33. By Theorem 46, we have that $ker(H^{2,0,0}) = 3$. Moreover, we can construct $K(H^{2,0,0})$ from a basis, by Corollary 47. First, we have that $Q = \{\mathbf{4}, (0,4,0,4,0,4,0,4)\}$. Since $\sigma = 1$, in this case, we have that $P = \emptyset$. Thus,*

$$K(H^{2,0,0}) = \langle \Phi(\mathbf{4}), \Phi((0,4,0,4,0,4,0,4)), \Phi(\mathbf{3}) \rangle.$$

4.2 Partial classification of $\mathbb{Z}_{2^s}$-linear Hadamard codes

The classification of the $\mathbb{Z}_4$-linear Hadamard codes of length 2^t, for any $t \geq 3$, using the rank or the dimension of the kernel is shown in [Kro01, PRV06]. In this section, we show that the dimension of the kernel can not be used to establish a complete classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, in general, for any $t \geq 3$ and $s > 2$. However, we see that this invariant allows us to show some partial results on the classification of these codes, through some examples and give bounds in the amount of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes with the same length 2^t.

First of all, recall that, for any $t \geq 3$, only the $\mathbb{Z}_4$-linear Hadamard codes H^{1,t_2} and H^{2,t_2} of length 2^t are linear [Kro01], so these are equivalent to the Reed-Muller code $RM(1,t)$. By Theorem 39, for any $t \geq 3$ and $s > 2$, there are also at most two $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, $H^{1,0,\ldots,0,1,t_s}$ and $H^{1,0,\ldots,0,t_s}$, that are linear. Moreover, the following result implies that we can focus on $t \geq 5$ and $2 \leq s \leq t-2$ to try to classify the nonlinear ones.

Theorem 49. *Let $\mathcal{A}_{t,s}$ be the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t. Then,*

$$\mathcal{A}_{t,s} = \begin{cases} 0 & \text{if } t \geq 3 \text{ and } s \geq t+2 \\ 1 & \text{if } t \geq 3 \text{ and } s \in \{t-1, t, t+1\} \\ 1 & \text{if } t = 4 \text{ and } s = 2, \end{cases}$$

and the $\mathbb{Z}_{2^s}$-linear Hadamard code is linear when $\mathcal{A}_{t,s} = 1$. Moreover, if $t \geq 5$ and $2 \leq s \leq t-2$, then $\mathcal{A}_{t,s} \geq 2$, and there is one code which is linear and at least one code which is nonlinear.

Proof. First, if $t \geq 3$ and $s \geq t+2$, then the equation

$$t = \Big(\sum_{i=1}^{s} (s-i+1) \cdot t_i \Big) - 1, \tag{4.2}$$

with $t_1 \geq 1$, does not have any nonnegative integer solution, so $\mathcal{A}_{t,s} = 0$. If $t \geq 3$ and $s = t+1$, then (4.2) has only one solution $(t_1, \ldots, t_s) = (1, 0, \ldots, 0)$. If $t \geq 3$ and $s = t$, (4.2) has only the solution $(1, 0, \ldots, 0, 1)$. If $t \geq 4$ and $s = t-1$, (4.2) has exactly two solutions $(1, 0, \ldots, 0, 2)$ and (1,0,...,0,1,0). By Theorem 39, for all the above solutions, we obtain a linear code $H^{t_1,\ldots,t_s}$. Note that, when $t = 3$ and $s = 2$, the solutions are $(1, 2)$ and $(2, 0)$; and when $t = 4$ and $s = 2$, they are $(1, 3)$ and $(2, 1)$, which also give linear codes H^{t_1,t_2}, by Theorem 35.

Finally, if $t \geq 5$ and $2 \leq s \leq t-2$, (4.2) always has the solutions $(1, 0, \ldots, 0, t-s+1)$ and $(1, 0, \ldots, 0, 1, t-s-1)$, which give a linear code. However, for these cases, there is at least another solution. On one hand, if $s = 2$, $\mathcal{A}_{t,s} = \lfloor (t-1)/2 \rfloor \geq 2$ since $t \geq 5$ [Kro01]. On the other hand, if $s = 3$, $(2, 0, \cdots, 0, t-2s+1)$ is a solution since $t \geq 2s-1$ when $t \geq 5$; and if $s \geq 4$, $(1, 0, \cdots, 0, 1, 0, t-s-2)$ is a solution. Therefore, for all the cases, $\mathcal{A}_{t,s} \geq 2$ by Theorem 39. $\mathcal{QED}$

The following example shows that the dimension of the kernel can not be used, in general, to classify completely all nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, once $t \geq 5$ and $2 < s \leq t-2$ are fixed.

Example 50. *The $\mathbb{Z}_8$-linear Hadamard codes of length $2^t = 256$ ($t = 8$) are the following: $H^{1,0,6}, H^{1,1,4}, H^{1,2,2}, H^{1,3,0}, H^{2,0,3}$, $H^{2,1,1}$ and $H^{3,0,0}$. The first two are equivalent as they are linear by Theorem 39. The remaining ones have kernels of dimension $7, 6, 6, 5$ and 4, respectively, by Theorem 46. Therefore, by using this invariant, we can say that all of them are nonequivalent, with the exception of $H^{1,3,0}$ and $H^{2,0,3}$ which have the same dimension of the kernel. For these two codes, by using the computer algebra system Magma [BCFS16], we have computed that rank$(H^{1,3,0}) = 12$ and rank$(H^{2,0,3}) = 11$, so they are also nonequivalent. Actually, all these nonlinear codes have ranks $10, 12, 11, 13$ and 17, respectively, so we can use the rank instead of the dimension of the kernel to classify completely the $\mathbb{Z}_8$-linear Hadamard codes of length 256.*

As shown in the next example, for some values of $t \geq 5$ and $2 < s \leq t-2$, it is indeed possible to establish a complete classification by using just the dimension of the kernel, like it happens for any $t \geq 5$ and $s = 2$ [Kro01].

Example 51. *By Theorem 46, it is possible to check that for any $5 \leq t \leq 7$ and $2 \leq s \leq t-2$, all nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t have a different dimension of the kernel, so this invariant allows us to classify them. For $t = 8$, $t = 9$, $t = 10$ and $t = 11$, it also works, except when $s \in \{3\}$, $s \in \{3, 4\}$, $s \in \{3, 4, 5\}$ and $s \in \{3, 4, 5, 6\}$, respectively. For these given values of t and s, we can just obtain a partial classification by using the kernel.*

By using Magma [BCFS16], we have also computed the rank of the nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, for any $5 \leq t \leq 11$ and $2 \leq s \leq t-2$. Tables 4.1, 4.4 and 4.5 show the values of $(t_1, \ldots, t_s)$ and the pair (r, k), where r is the rank and k the dimension of the kernel, for all nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, for $5 \leq t \leq 11$. Note that the results given in Examples 50 and 51 can also be checked by looking at these tables. These tables also show that all nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t have different values of the rank, once $5 \leq t \leq 11$ and $2 \leq s \leq t-2$ are fixed. Therefore, for these cases, as in Example 50,

	$t=5$		$t=6$		$t=7$		$t=8$	
	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)
$\mathbb{Z}_4$	$(3,0)$	(7,4)	$(3,1)$	(8,5)	$(3,2)$ $(4,0)$	(9,6) (11,5)	$(3,3)$ $(4,1)$	(10,7) (12,6)
$\mathbb{Z}_8$	$(2,0,0)$	(8,3)	$(1,2,0)$ $(2,0,1)$	(8,5) (9,4)	$(1,2,1)$ $(2,0,2)$ $(2,1,0)$	(9,6) (10,5) (12,4)	$(1,2,2)$ $(1,3,0)$ $(2,0,3)$ $(2,1,1)$ $(3,0,0)$	(10,7) (12,6) (11,6) (13,5) (17,4)
$\mathbb{Z}_{16}$			$(1,1,0,0)$	(9,4)	$(1,0,2,0)$ $(1,1,0,1)$ $(2,0,0,0)$	(9,6) (10,5) (14,3)	$(1,0,2,1)$ $(1,1,0,2)$ $(1,1,1,0)$ $(2,0,0,1)$	(10,7) (11,6) (13,5) (15,4)
$\mathbb{Z}_{32}$					$(1,0,1,0,0)$	(10,5)	$(1,0,0,2,0)$ $(1,0,1,0,1)$ $(1,1,0,0,0)$	(10,7) (11,6) (15,4)
$\mathbb{Z}_{64}$							$(1,0,0,1,0,0)$	(11,6)

Table 4.1: Rank and kernel for all nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t.

we have that the codes are pairwise nonequivalent, so we have a complete classification by using the rank and we can establish the following result.

Let $X_{t,s}$ be the number of nonnegative integer solutions of the equation $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i) - 1$ with $t_1 \geq 1$, that is,

$$X_{t,s} = |\{(t_1,\ldots,t_s) \in \mathbb{N}^s : t = \left(\sum_{i=1}^{s}(s-i+1)\cdot t_i\right) - 1,\ t_1 \geq 1\}|. \quad (4.3)$$

Theorem 52. *Let $\mathcal{A}_{t,s}$ be the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t. Then, for any $t \geq 3$ and $2 \leq s \leq t-1$,*

$$\mathcal{A}_{t,s} \leq X_{t,s} - 1.$$

Moreover, for any $3 \leq t \leq 11$ and $2 \leq s \leq t-1$, this bound is tight.

Proof. Straightforward from Theorem 39, the proof of Theorem 49, and Tables 4.1, 4.4 and 4.5. $\mathcal{QED}$

By Theorems 49 and 52 (or Tables 4.1, 4.4 and 4.5), we can obtain exactly the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, for

some values of t and s. Table 4.2 shows these numbers, for $3 \leq t \leq 11$ and $2 \leq s \leq 9$. The cases where the dimension of the kernel is not enough to classify these codes are shown in bold type. However, in all these cases, the rank can be used to obtain the classification.

t	3	4	5	6	7	8	9	10	11
$\mathbb{Z}_4$	1	1	2	2	3	3	4	4	5
$\mathbb{Z}_8$	1	1	2	3	4	**6**	**7**	**9**	**11**
$\mathbb{Z}_{16}$	1	1	1	2	4	5	**8**	**10**	**14**
$\mathbb{Z}_{32}$	0	1	1	1	2	4	6	**9**	**12**
$\mathbb{Z}_{64}$	0	0	1	1	1	2	4	6	**10**
$\mathbb{Z}_{128}$	0	0	0	1	1	1	2	4	6
$\mathbb{Z}_{256}$	0	0	0	0	1	1	1	2	4
$\mathbb{Z}_{512}$	0	0	0	0	0	1	1	1	2

Table 4.2: Number $\mathcal{A}_{t,s}$ of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t.

The values of $\mathcal{A}_{t,2}$ given in Table 4.2 where already proved in [Kro01]. Specifically, in that paper, it is shown that there are $\lfloor \frac{t-1}{2} \rfloor$ nonequivalent $\mathbb{Z}_4$-linear Hadamard codes of length 2^t for all $t \geq 3$. Next, we focus on establishing some relationships between the already known $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s = 2$ and the ones with $s > 2$, once only the length 2^t is fixed. First, Example 53 shows that there are $\mathbb{Z}_{2^s}$-linear Hadamard codes, with $s > 2$, which are not equivalent to any $\mathbb{Z}_4$-linear Hadamard code. Then, Example 54 also shows that there are $\mathbb{Z}_4$-linear Hadamard codes which are not equivalent to any $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s > 2$.

Example 53. *Let $H^{2,0,0}$ be the $\mathbb{Z}_8$-linear Hadamard code of length 32 considered in Examples 33 and 48. Recall that $ker(H^{2,0,0}) = 3$ by Theorem 46, and hence $H^{2,0,0}$ is nonlinear. It is known that there are three $\mathbb{Z}_4$-linear Hadamard codes of length 32, $H^{1,4}$, $H^{2,2}$ and $H^{3,0}$. The first two are linear, and the last one has $ker(H^{3,0}) = 4$ by Theorem 46 or [Kro01]. Hence, there is no $\mathbb{Z}_4$-linear Hadamard code equivalent to the $\mathbb{Z}_8$-linear Hadamard code $H^{2,0,0}$.*

Example 54. *By Table 4.1, for $t = 5$, there are only two nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes, $H^{3,0}$ and $H^{2,0,0}$. In Example 53, we have seen that*

they are not equivalent, since they have different dimension of the kernel. Other examples like this one can be found when t is odd. For example, by Tables 4.1, 4.4 and 4.5, for $t = 7$, $t = 9$ and $t = 11$, there are $\mathbb{Z}_4$-linear Hadamard codes, $H^{4,0}$, $H^{5,0}$ and $H^{6,0}$, respectively, which are not equivalent to any $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s > 2$ of the same length, by using both invariants, the rank and the dimension of the kernel.

The classification of $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes of length 2^t with $\alpha \neq 0$ is given in [PRV06], where it is shown that there are $\lfloor \frac{t}{2} \rfloor$ nonequivalent of such codes, for all $t \geq 3$; and either the rank or the dimension of the kernel can be used to classify them, like for $\mathbb{Z}_4$-linear Hadamard codes. Recall that there are $\lfloor \frac{t-1}{2} \rfloor$ nonequivalent $\mathbb{Z}_4$-linear Hadamard codes of length 2^t for all $t \geq 3$ [Kro01]. However, in [KV15], it is shown that each $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code with $\alpha = 0$, that is, each $\mathbb{Z}_4$-linear Hadamard code, is equivalent to a $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code with $\alpha \neq 0$, so there are only $\lfloor \frac{t}{2} \rfloor$ nonequivalent $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes of length 2^t.

The following example shows that there are $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes (with $\alpha \neq 0$) which are not equivalent to any $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s \geq 2$.

Example 55. *For $t = 4$, there is a $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code (with $\alpha \neq 0$) which is not equivalent to any $\mathbb{Z}_4$-linear Hadamard code [KV15]. This code has parameters $(r, k) = (6, 3)$ [PRV06], so it is not equivalent to any $\mathbb{Z}_{2^s}$-linear Hadamard code with $s \geq 2$, since all of them are linear by Theorem 49. Other examples like this one can be found when t is even. For example, for $t = 6$, $t = 8$ and $t = 10$, there is also a $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code (with $\alpha \neq 0$) which is not equivalent to any $\mathbb{Z}_4$-linear Hadamard code [KV15]. They have parameters $(10, 4)$, $(15, 5)$ and $(21, 6)$ [PRV06], respectively, so again they are not equivalent to any $\mathbb{Z}_{2^s}$-linear Hadamard code with $s \geq 2$ of length 2^6, 2^8 and 2^{10}, respectively, by Tables 4.1, 4.4 and 4.5.*

Finally, we focus on establishing how many nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t there are, once only the length 2^t is fixed for some values of t. First, we give some lower and upper bounds. From Tables 4.1,

4.4 and 4.5, we can determine a lower bound (K) taking into account just the dimension of the kernel. This lower bound can be improved (RK) if we consider both invariants, the rank and the dimension of the kernel. Note that there are codes having the same dimension of the kernel with different ranks (for $t = 7, 8, 9, 10, 11$), and codes having the same rank with different dimensions of the kernel (for $t = 9, 10, 11$). These results are summarized in Table 4.3, where we give these bounds for all $3 \leq t \leq 11$.

t	3	4	5	6	7	8	9	10	11
lower bound K	1	1	3	3	5	5	7	7	9
lower bound RK	1	1	3	3	6	7	11	13	20
upper bound	1	1	3	5	10	16	26	38	57

Table 4.3: Bounds for the number $\mathcal{A}_t$ of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t.

An upper bound can be given easily by considering all nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, once t and s are fixed, as it is shown in the next theorem. These values for all $3 \leq t \leq 11$ are also shown in Table 4.3.

Theorem 56. *Let $\mathcal{A}_{t,s}$ be the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t. Let $\mathcal{A}_t$ be the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, for any $s \geq 2$. Then,*

$$\mathcal{A}_t \leq \sum_{s=2}^{t-2} (X_{t,s} - 2) + 1 \tag{4.4}$$

and

$$\mathcal{A}_t \leq \sum_{s=2}^{t-2} (\mathcal{A}_{t,s} - 1) + 1. \tag{4.5}$$

Theorem 57. *There are exactly $1, 1, 3, 3$ and 6 nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t for t equal to $3, 4, 5, 6$ and 7, respectively.*

Proof. For t equal to $3, 4$ and 5, the result is true, since the lower and upper bounds given in Table 4.3 coincides. By using Magma [BCFS16], it is possible to check that, for $t = 6$, both $\mathbb{Z}_{2^s}$-linear Hadamard codes having the same

parameters $(r, k) = (8, 5)$ are equivalent; and the ones having $(r, k) = (9, 4)$ are also equivalent. Therefore, in this case, the upper bound goes from 5 to 3, and then coincides with the lower bound given in Table 4.3. Similarly, or $t = 7$, it is also possible to check that the codes having the same parameters (r, k) are all equivalent, so the upper bound became equal to the lower bound 6, and the result also holds. $\mathcal{QED}$

	$t=9$		$t=10$		$t=11$	
	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)
$\mathbb{Z}_4$	$(3,4)$	(11,8)	$(3,5)$	(12,9)	$(3,6)$	(13,10)
	$(4,2)$	(13,7)	$(4,3)$	(14,8)	$(4,4)$	(15,9)
	$(5,0)$	(16,6)	$(5,1)$	(17,7)	$(5,2)$	(18,8)
					$(6,0)$	(22,7)
$\mathbb{Z}_8$	$(1,2,3)$	(11,8)	$(1,2,4)$	(12,9)	$(1,2,5)$	(13,10)
	$(1,3,1)$	(13,7)	$(1,3,2)$	(14,8)	$(1,3,3)$	(15,9)
	$(2,0,4)$	(12,7)	$(1,4,0)$	(17,7)	$(1,4,1)$	(18,8)
	$(2,1,2)$	(14,6)	$(2,0,5)$	(13,8)	$(2,0,6)$	(14,9)
	$(2,2,0)$	(17,5)	$(2,1,3)$	(15,7)	$(2,1,4)$	(16,8)
	$(3,0,1)$	(18,5)	$(2,2,1)$	(18,6)	$(2,2,2)$	(19,7)
			$(3,0,2)$	(19,6)	$(2,3,0)$	(23,6)
			$(3,1,0)$	(24,5)	$(3,0,3)$	(20,7)
					$(3,1,1)$	(25,6)
					$(4,0,0)$	(32,5)
$\mathbb{Z}_{16}$	$(1,0,2,2)$	(11,8)	$(1,0,2,3)$	(12,9)	$(1,0,2,4)$	(13,10)
	$(1,0,3,0)$	(13,7)	$(1,0,3,1)$	(14,8)	$(1,0,3,2)$	(15,9)
	$(1,2,0,0)$	(18,5)	$(1,1,0,4)$	(13,8)	$(1,0,4,0)$	(18,8)
	$(1,1,0,3)$	(12,7)	$(1,1,1,2)$	(15,7)	$(1,1,0,5)$	(14,9)
	$(1,1,1,1)$	(14,6)	$(1,1,2,0)$	(18,6)	$(1,1,1,3)$	(16,8)
	$(2,0,0,2)$	(16,5)	$(1,2,0,1)$	(19,6)	$(1,1,2,1)$	(19,7)
	$(2,0,1,0)$	(20,4)	$(2,0,0,3)$	(17,6)	$(1,2,0,2)$	(20,7)
			$(2,0,1,1)$	(21,5)	$(1,2,1,0)$	(25,6)
			$(2,1,0,0)$	(28,4)	$(2,0,0,4)$	(18,7)
					$(2,0,1,2)$	(22,6)
					$(2,0,2,0)$	(27,5)
					$(2,1,0,1)$	(29,5)
					$(3,0,0,0)$	(44,4)

Table 4.4: Rank and dimension of the kernel for all nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t.

	$t=9$		$t=10$		$t=11$	
	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)
$\mathbb{Z}_{32}$	$(1,0,0,2,1)$	(11,8)	$(1,0,0,2,2)$	(12,9)	$(1,0,0,2,3)$	(13,10)
	$(1,0,1,0,2)$	(12,7)	$(1,0,0,3,0)$	(14,8)	$(1,0,0,3,1)$	(15,9)
	$(1,0,1,1,0)$	(14,6)	$(1,0,1,0,3)$	(13,8)	$(1,0,1,0,4)$	(14,9)
	$(1,1,0,0,1)$	(16,5)	$(1,0,1,1,1)$	(15,7)	$(1,0,1,1,2)$	(16,8)
	$(2,0,0,0,0)$	(26,3)	$(1,0,2,0,0)$	(19,6)	$(1,0,1,2,0)$	(19,7)
			$(1,1,0,0,2)$	(17,6)	$(1,0,2,0,1)$	(20,7)
			$(1,1,0,1,0)$	(21,5)	$(1,1,0,0,3)$	(18,7)
			$(2,0,0,0,1)$	(27,4)	$(1,1,0,1,1)$	(22,6)
					$(1,1,1,0,0)$	(29,5)
					$(2,0,0,0,2)$	(28,5)
					$(2,0,0,1,0)$	(36,4)
$\mathbb{Z}_{64}$	$(1,0,0,0,2,0)$	(11,8)	$(1,0,0,0,2,1)$	(12,9)	$(1,0,0,0,2,2)$	(13,10)
	$(1,0,0,1,0,1)$	(12,7)	$(1,0,0,1,0,2)$	(13,8)	$(1,0,0,0,3,0)$	(15,9)
	$(1,0,1,0,0,0)$	(16,5)	$(1,0,0,1,1,0)$	(15,7)	$(1,0,0,1,0,3)$	(14,9)
			$(1,0,1,0,0,1)$	(17,6)	$(1,0,0,1,1,1)$	(16,8)
			$(1,1,0,0,0,0)$	(27,4)	$(1,0,0,2,0,0)$	(20,7)
					$(1,0,1,0,0,2)$	(18,7)
					$(1,0,1,0,1,0)$	(22,6)
					$(1,1,0,0,0,1)$	(28,5)
					$(2,0,0,0,0,0)$	(48,3)
$\mathbb{Z}_{128}$	$(1,0,0,0,1,0,0)$	(12,7)	$(1,0,0,0,0,2,0)$	(12,9)	$(1,0,0,0,0,2,1)$	(13,10)
			$(1,0,0,0,1,0,1)$	(13,8)	$(1,0,0,0,1,0,2)$	(14,9)
			$(1,0,0,1,0,0,0)$	(17,6)	$(1,0,0,0,1,1,0)$	(16,8)
					$(1,0,0,1,0,0,1)$	(18,7)
					$(1,0,1,0,0,0,0)$	(28,5)
$\mathbb{Z}_{256}$			$(1,0,0,0,0,1,0,0)$	(13,8)	$(1,0,0,0,0,0,2,0)$	(13,10)
					$(1,0,0,0,0,1,0,1)$	(14,9)
					$(1,0,0,0,1,0,0,0)$	(18,7)
$\mathbb{Z}_{512}$					$(1,0,0,0,0,0,1,0,0)$	(14,9)

Table 4.5: Rank and dimension of the kernel for all nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t.

Chapter 5

Rank of $\mathbb{Z}_8$-linear Hadamard codes

"All that is gold does not glitter, not all those who wander are lost."
– J. R. R. Tolkien, The Lord of the Rings, The Fellowship of the Ring

The classification of the $\mathbb{Z}_4$-linear Hadamard codes by using the rank and the dimension of the kernel is given in [Kro01, PRV06]. In fact, it is shown that it is possible to classify these codes just by using one of these invariants. In the previous chapter, in order to classify the $\mathbb{Z}_{2^s}$-linear Hadamard codes, we compute the kernel and its dimension for these codes and show that it is not enough to obtain a complete classification by using only this invariant. The aim of this chapter is to classify the $\mathbb{Z}_{2^s}$-linear Hadamard codes for $s \in \{2, 3\}$. First, in Section 5.1, we compute the rank of the $\mathbb{Z}_8$-linear Hadamard codes by giving a basis that generates their span when the codes are nonlinear. Later, in Section 5.2, we show through an example that the rank by itself is not enough to classify these codes. Nevertheless, we give a complete classification of the codes by using both invariants, the rank and the dimension of the kernel. Finally, in Section 5.3, we find equivalences among the $\mathbb{Z}_4$-linear and $\mathbb{Z}_8$-linear Hadamard codes and achieve the goal of this chapter.

5.1 Computation of the rank

The rank of a $\mathbb{Z}_4$-linear Hadamard code of type $(2^{t-1}; t_1, t_2)$, where $t+1 = 2t_1+t_2$, is $2t_1+t_2+\binom{t_1-1}{2}$ if $t_1 > 2$, and $2t_1+t_2$ if $t_1 = 1$ or 2 by Proposition 12. In this section, we establish the rank of the $\mathbb{Z}_8$-linear Hadamard codes of type $(2^{t-2}; t_1, t_2, t_3)$, where $t+1 = 3t_1+2t_2+t_3$, in terms of the parameters t_1, t_2 and t_3 by finding a set of linear independent vectors that generate the span of these codes.

All results that we show on the Carlet's generalized Gray map are only proved for $s = 3$, that is, for $\mathbb{Z}_8$-linear Hadamard codes. In this case, the generalized Gray map $\phi : \mathbb{Z}_8 \to \mathbb{Z}_2^4$ is defined as follows:

$$\begin{array}{ll} \phi(0) = (0,0,0,0) & \phi(4) = (1,1,1,1) \\ \phi(1) = (0,1,0,1) & \phi(5) = (1,0,1,0) \\ \phi(2) = (0,0,1,1) & \phi(6) = (1,1,0,0) \\ \phi(3) = (0,1,1,0) & \phi(7) = (1,0,0,1). \end{array}$$

The construction of the generator matrices of the $\mathbb{Z}_{2^s}$-additive Hadamard codes, given in Chapter 3, allows us to present the following remark in order to make easier the comprehension of the proofs of the succeeding sections:

Remark 58. *Let $\mathcal{H}^{t_1,0,\ldots,0}$ be a $\mathbb{Z}_{2^s}$-additive Hadamard code of type $(n; t_1, 0, \ldots, 0)$. Let $\mathbf{w}_i$ be the ith row of $A^{t_1,0,\ldots,0}$ with $1 \le i \le t_1$. Let*

$$W = \begin{pmatrix} \mathbf{w}_{i_1} \\ \vdots \\ \mathbf{w}_{i_q} \end{pmatrix},$$

where $2 \le i_1 < \cdots < i_q \le t_1$. By construction, we have that each one of the 2^{sq} elements of $\mathbb{Z}_{2^s}^q$ appears $\frac{2^{s(t_1-1)}}{2^{sq}} = 2^{s(t_1-q-1)}$ times as a column of W. Therefore, there exists a permutation of coordinates $\rho \in \mathcal{S}_n$ such that

$$\rho(W) = \begin{pmatrix} \mathbf{w}_2 \\ \vdots \\ \mathbf{w}_{q+1} \end{pmatrix}.$$

Note also that $\mathbf{w}_i$ *is the* $2^{s(t_1-q-1)}$*-fold replication of* $\mathbf{w}_i^{q+1}$ *for all* $2 \leq i \leq q+1$.

Example 59. *Let* $\mathcal{H}^{4,0}$ *be the* $\mathbb{Z}_4$*-linear Hadamard code of type* $(64; 4, 0)$ *generated by* $A^{4,0}$*. Let*

$$W = \begin{pmatrix} \mathbf{w}_2 \\ \mathbf{w}_4 \end{pmatrix} = \begin{pmatrix} \mathbf{u\,u\,u\,u} & \mathbf{u\,u\,u\,u} & \mathbf{u\,u\,u\,u} & \mathbf{u\,u\,u\,u} \\ \mathbf{0\,0\,0\,0} & \mathbf{1\,1\,1\,1} & \mathbf{2\,2\,2\,2} & \mathbf{3\,3\,3\,3} \end{pmatrix},$$

where $\mathbf{u} = 0123$*. Then, applying the permutation* $\rho = (5, 17)(6, 18)(7, 19)(8, 20)(9, 33)(10, 34)(11, 35)(12, 36)(13, 49)(14, 50)(15, 51)(16, 52)(25, 37)(26, 38)(27, 39)(28, 40)(29, 53)(30, 54)(31, 55)(32, 56)(45, 57)(46, 58)(47, 59)(48, 60) \in \mathcal{S}_{64}$*, we have that*

$$\rho(W) = \begin{pmatrix} \mathbf{w}_2 \\ \mathbf{w}_3 \end{pmatrix} = \begin{pmatrix} \mathbf{u\,u\,u\,u} & \mathbf{u\,u\,u\,u} & \mathbf{u\,u\,u\,u} & \mathbf{u\,u\,u\,u} \\ \mathbf{0\,1\,2\,3} & \mathbf{0\,1\,2\,3} & \mathbf{0\,1\,2\,3} & \mathbf{0\,1\,2\,3} \end{pmatrix}.$$

Proposition 60. *Let* $t_1, t_2, \ldots, t_s$ *be nonnegative integers with* $t_1 \geq 1$*. Then,* $rank(\Phi(\mathcal{H}^{t_1,\ldots,t_s})) = t_s + rank(\Phi(\mathcal{H}^{t_1,\ldots,t_{s-1},0}))$.

Proof. We prove this result by induction on the integer $t_s \geq 0$. First, for $t_s = 0$, the result holds trivially.

Let $\mathcal{H}' = \mathcal{H}^{t_1,\ldots,t_s}$ and $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_{s-1},t_s-1}$. Let $t_s \geq 1$ and suppose that the result is true for $t_s - 1$. By the recursive construction (3.1), $\mathcal{H}'$ can be seen as the union of two cosets, that is, $\mathcal{H}' = C_0 \cup C_1$, where $C_0 = (\mathcal{H}, \mathcal{H})$ and $C_1 = (\mathcal{H}, \mathcal{H}) + (\mathbf{0}, \mathbf{2^{s-1}})$. By Corollary 26, we have that $\Phi((\mathcal{H}, \mathcal{H}) + (\mathbf{0}, \mathbf{2^{s-1}})) = \Phi((\mathcal{H}, \mathcal{H})) + \Phi((\mathbf{0}, \mathbf{2^{s-1}}))$, so $\mathrm{rank}(\Phi(\mathcal{H}')) = 1 + \mathrm{rank}(\Phi(\mathcal{H}))$. By the induction hypothesis, $\mathrm{rank}(\Phi(\mathcal{H}')) = 1 + t_s - 1 + \mathrm{rank}(\Phi(\mathcal{H}^{t_1,\ldots,t_{s-1},0})) = t_s + \mathrm{rank}(\Phi(\mathcal{H}^{t_1,\ldots,t_{s-1},0}))$. $\mathcal{QED}$

Lemma 61. *Let* $w, v \in \mathbb{Z}_{2^s}$ *such that* $\mathrm{ord}(v) = 2^i$ *with* $i < s$*. Then,* $2^{i-1}((w+v) \odot 2^{s-i}) = 2^{i-1}(w \odot 2^{s-i}) + 2^{i-1}(v \odot 2^{s-i})$.

Proof. The binary expansion of v and $w + v$ are $[0, \ldots, 0, 1, v_{s-i+1}, \ldots, v_{s-1}]_2$ and $[w_0, \ldots, w_{s-i} + 1, (w + v)_{s-i+1}, \ldots, (w + v)_{s-1}]_2$, respectively. Then, we have that the binary expansion of $w \odot 2^{s-i}, v \odot 2^{s-i}$ and $(w + v) \odot 2^{s-i}$ are $[0, \ldots, w_{s-i}, 0, \ldots, 0]_2$, $[0, \ldots, 0, 1, 0, \ldots, 0]_2$ and $[0, \ldots, 0, w_{s-i} + 1, 0, \ldots, 0]_2$,

respectively. Note that, multiplying by 2^{i-1}, the binary expansions are $[0,\ldots,0,w_{s-i}]_2$, $[0,\ldots,0,1]_2$ and $[0,\ldots,0,w_{s-i}+1]_2$, respectively. Therefore, $2^{i-1}(w \odot 2^{s-i}) + 2^{i-1}(v \odot 2^{s-i}) = 2^{i-1}((w+v) \odot 2^{s-i})$. $\mathcal{QED}$

In order to simplify the notation in the following results, we define $\mu(\mathbf{w}) = -2(\mathbf{w} \odot \mathbf{2})$ for any $\mathbf{w} \in \mathbb{Z}_8^n$. Note that $\mathrm{ord}(\mu(\mathbf{w})) = 2$ if $\mathbf{w} \neq \mathbf{0}$.

Lemma 62. *Let $\mathbf{w}, \mathbf{v} \in \mathbb{Z}_8^n$ such that $\mathrm{ord}(\mathbf{v}) < 8$. Then, $\mu(\mathbf{w}+\mathbf{v}) = \mu(\mathbf{w}) + \mu(\mathbf{v})$.*

Proof. We may assume that $\mathbf{v} \neq \mathbf{0}$. If $\mathrm{ord}(\mathbf{v}) = 4$, then $2((\mathbf{w}+\mathbf{v}) \odot 2) = 2(\mathbf{w} \odot 2) + 2(\mathbf{v} \odot 2)$ by Lemma 61, so the result follows. Finally, if $\mathrm{ord}(\mathbf{v}) = 2$, then the result also holds since $\mathbf{v} \odot 2 = \mathbf{0}$ and $(\mathbf{w}+\mathbf{v}) \odot 2 = \mathbf{w} \odot 2$. $\mathcal{QED}$

Lemma 63. *Let $\mathcal{H}^{t_1,0,0}$ be a $\mathbb{Z}_8$-additive Hadamard code of type $(n; t_1, 0, 0)$. Let $\mathbf{w}_i$ be the ith row of $A^{t_1,0,0}$ with $1 \leq i \leq t_1$. Then,*

$$\mu(\mathbf{w}_i + \mathbf{w}_j + \mathbf{w}_k) = \mu(\mathbf{w}_i + \mathbf{w}_j) + \mu(\mathbf{w}_i + \mathbf{w}_k) + \mu(\mathbf{w}_j + \mathbf{w}_k) + \mu(\mathbf{w}_i) + \mu(\mathbf{w}_j) + \mu(\mathbf{w}_k) \quad (5.1)$$

for all $1 \leq i < j < k \leq t_1$. Furthermore, for all $2 \leq i < j \leq t_1$ and $k \in \mathbb{Z}_8$,

$$\mu(\mathbf{k} + \mathbf{w}_i + \mathbf{w}_j) = \mu(\mathbf{k} + \mathbf{w}_i) + \mu(\mathbf{k} + \mathbf{w}_j) + \mu(\mathbf{w}_i + \mathbf{w}_j) + \mu(\mathbf{k}) + \mu(\mathbf{w}_i) + \mu(\mathbf{w}_j).$$

Proof. First, consider the $\mathbb{Z}_8$-additive Hadamard code $\mathcal{H}^{4,0,0}$. In this case, it is easy to check that $\mu(\mathbf{w}_i^4 + \mathbf{w}_j^4 + \mathbf{w}_k^4) = \mu(\mathbf{w}_i^4 + \mathbf{w}_j^4) + \mu(\mathbf{w}_i^4 + \mathbf{w}_k^4) + \mu(\mathbf{w}_j^4 + \mathbf{w}_k^4) + \mu(\mathbf{w}_i^4) + \mu(\mathbf{w}_j^4) + \mu(\mathbf{w}_k^4)$ for all $1 \leq i < j < k \leq 4$. Then, the result follows by Remark 58 and the fact that $\mathbf{w}_1, \ldots, \mathbf{w}_4 \in \mathcal{H}^{t_1,0,0}$ are an 8^{t_1-4}-fold replication of $\mathbf{w}_1^4, \ldots, \mathbf{w}_4^4 \in \mathcal{H}^{4,0,0}$, respectively. By using the same argument, the second equation also holds. $\mathcal{QED}$

Let $\pi_8 \in \mathcal{S}_n$ be the following permutation of coordinates:

$$\pi_8 = \prod_{i=0}^{8^{t_1-2}-1} (8i+1, 8i+2, 8i+3, 8i+4, 8i+5, 8i+6, 8i+7, 8i+8), \quad (5.2)$$

where $n = 2^{3t_1-s}$. Let π_8^k be the composition of π_8, k times, i.e., $\pi_8^k = \pi_8 \circ \overset{(k)}{\cdots} \circ \pi_8$. Note that $\pi_8^k(\mathbf{w}_2) = \mathbf{w}_2 + \mathbf{k}$ and $\pi_8^k(\mathbf{w}_i) = \mathbf{w}_i$ for all $i \in \{3, \ldots, q\}$. Moreover, note that

$$\pi_8^k \circ \mu = \mu \circ \pi_8^k. \tag{5.3}$$

Example 64. *Let $\mathcal{H}^{2,0,0}$ be the $\mathbb{Z}_8$-linear Hadamard code of type $(8; 2, 0, 0)$ generated by $A^{2,0,0}$. Let $\mathbf{w}_2 = (0\,1\,2\,3\,4\,5\,6\,7)$ be the second row of $A^{2,0,0}$. Then, we have that $\mathbf{w}_2 + \mathbf{1} = (0\,1\,2\,3\,4\,5\,6\,7) + (1\,1\,1\,1\,1\,1\,1\,1) = (1\,2\,3\,4\,5\,6\,7\,0) = \pi_8(\mathbf{w}_2)$. By induction, we also have that $\pi_8^k(\mathbf{w}_2) = \pi_8^{k-1}(\mathbf{w}_2+\mathbf{1}) = \pi_8^{k-1}(\mathbf{w}_2)+ \mathbf{1} = \mathbf{w}_2 + \mathbf{k} - \mathbf{1} + \mathbf{1} = \mathbf{w}_2 + \mathbf{k}$ for any $k \in \mathbb{Z}_8$.*

Lemma 65. *Let $\mathcal{H}^{t_1,0,0}$ be a $\mathbb{Z}_8$-additive Hadamard code of type $(n; t_1, 0, 0)$. Let $\mathbf{w}_i$ be the ith row of $A^{t_1,0,0}$ with $1 \le i \le t_1$. Let $E \subseteq \{1, \ldots, t_1\}$. Then,*

$$\mu(\sum_{i\in E} \mathbf{w}_i) = \sum_{\substack{i,j\in E \\ i<j}} \mu(\mathbf{w}_i + \mathbf{w}_j) + (|E| \bmod 2) \sum_{i\in E} \mu(\mathbf{w}_i).$$

Proof. Assume $E \subseteq \{2, \ldots, t_1\}$, and let $q = |E|$. By Remark 58, without loss of generality, we can assume that $E = \{2, \ldots, q+1\}$. Now, we prove this lemma by induction on the integer $q \ge 1$.

For $q = 1$ the result holds. Assume $q \ge 2$ and suppose that it is true for $q-1$. Consider $\sum_{i=2}^{q+1} \mathbf{w}_i = \sum_{i=2}^{q} \mathbf{w}_i + \mathbf{w}_{q+1}$. Let $\mathbf{y} = \sum_{i=2}^{q} \mathbf{w}_i^q$. We have that $\sum_{i=2}^{q} \mathbf{w}_i = (\mathbf{y}, \ldots, \mathbf{y})$ is the 8^{t_1-q}-fold replication of $\mathbf{y}$. Then, $\sum_{i=2}^{q+1} \mathbf{w}_i$ is the 8^{t_1-q-1}-fold replication of $(\mathbf{y}+\mathbf{0}, \mathbf{y}+\mathbf{1}, \ldots, \mathbf{y}+\mathbf{7})$. The result holds if

$$\mu(\sum_{i=2}^{q} \mathbf{w}_i + \mathbf{w}_{q+1}) = \sum_{2\le i<j\le q+1} \mu(\mathbf{w}_i + \mathbf{w}_j) + (q \bmod 2) \sum_{i=2}^{q+1} \mu(\mathbf{w}_i). \tag{5.4}$$

That is, for all $k \in \{0, \ldots, 7\}$, we have to prove that

$$\begin{aligned}\mu(\mathbf{y} + \mathbf{k}) = \mu(\sum_{i=2}^{q} \mathbf{w}_i^q + \mathbf{k}) = \sum_{2\le i<j\le q} \mu(\mathbf{w}_i^q + \mathbf{w}_j^q) + \\ + \sum_{i=2}^{q} \mu(\mathbf{w}_i^q + \mathbf{k}) + (q \bmod 2)(\mu(\mathbf{k}) + \sum_{i=2}^{q} \mu(\mathbf{w}_i^q)).\end{aligned} \tag{5.5}$$

Note that, by the induction hypothesis, the statement holds for $\sum_{i=2}^{q} \mathbf{w}_i = (\mathbf{y}, \ldots, \mathbf{y})$ and hence,

$$\mu(\mathbf{y}) = \sum_{2 \le i < j \le q} \mu(\mathbf{w}_i^q + \mathbf{w}_j^q) + ((q-1) \bmod 2) \sum_{i=2}^{q} \mu(\mathbf{w}_i^q). \tag{5.6}$$

Let $\pi_8 \in \mathcal{S}_n$ be the permutation of coordinates defined in (5.2). We have that $\mu(\mathbf{y}+\mathbf{k}) = \mu(\pi_8^k(\mathbf{y})) = \pi_8^k(\mu(\mathbf{y}))$ by the properties of π_8^k and (5.3). By applying (5.6), $\mu(\mathbf{y}+\mathbf{k}) = \sum_{2 \le i < j \le q} \pi_8^k(\mu(\mathbf{w}_i^q + \mathbf{w}_j^q)) + ((q-1) \bmod 2) \sum_{i=2}^{q} \pi_8^k(\mu(\mathbf{w}_i^q))$. By using the properties of π_8^k, we have that

$$\begin{aligned}\mu(\mathbf{y}+\mathbf{k}) = &\sum_{3 \le i < j \le q} \mu(\mathbf{w}_i^q + \mathbf{w}_j^q) + \\ &+ \sum_{i=3}^{q} \mu(\mathbf{w}_i^q + \mathbf{w}_2^q + \mathbf{k}) + ((q-1) \bmod 2)(\sum_{i=3}^{q} \mu(\mathbf{w}_i^q) + \mu(\mathbf{w}_2^q + \mathbf{k})).\end{aligned}$$

By Lemma 63, we have that $\mu(\mathbf{w}_i^q + \mathbf{w}_2^q + \mathbf{k}) = \mu(\mathbf{w}_2^q + \mathbf{k}) + \mu(\mathbf{w}_i^q + \mathbf{k}) + \mu(\mathbf{w}_2^q + \mathbf{w}_i^q) + \mu(\mathbf{w}_2^q) + \mu(\mathbf{w}_i^q) + \mu(\mathbf{k})$. Therefore, $\mu(\mathbf{y}+\mathbf{k}) = \sum_{2 \le i < j \le q} \mu(\mathbf{w}_i^q + \mathbf{w}_j^q) + \sum_{i=2}^{q} \mu(\mathbf{w}_i^q + \mathbf{k}) + (q \bmod 2)(\mu(\mathbf{k}) + \sum_{i=2}^{q} \mu(\mathbf{w}_i^q))$ and (5.5) holds.

Now, assume $1 \in E$, and let $q = |E|$. By Remark 58, without loss of generality, we can assume that $E = \{1, \ldots, q\}$. In this case, when $q = 1$ the result holds trivially since $\mu(\mathbf{w}_1) = \mathbf{0}$. Assume $q \ge 2$ and suppose that it is true for $q-1$. Consider $\sum_{i=2}^{q} \mathbf{w}_i = \sum_{i=2}^{q-1} \mathbf{w}_i + \mathbf{w}_q$. Let $\mathbf{y} = \sum_{i=2}^{q-1} \mathbf{w}_i^{q-1}$. We have that $\sum_{i=2}^{q-1} \mathbf{w}_i = (\mathbf{y}, \ldots, \mathbf{y})$ is the 8^{t_1-q+1}-fold replication of $\mathbf{y}$. Then, $\sum_{i=2}^{q} \mathbf{w}_i$ is the 8^{t_1-q}-fold replication of $(\mathbf{y}+\mathbf{0}, \mathbf{y}+\mathbf{1}, \ldots, \mathbf{y}+\mathbf{7})$. Therefore, $\mathbf{w}_1 + \sum_{i=2}^{q} \mathbf{w}_i$ is the 8^{t_1-q}-fold replication of $(\mathbf{y}+\mathbf{1}, \mathbf{y}+\mathbf{2}, \ldots, \mathbf{y}+\mathbf{7}, \mathbf{y}+\mathbf{0})$. Again, the result holds since (5.4) holds, that is, for all $k \in \{0, \ldots, 7\}$, we have that (5.5) holds. $\mathcal{QED}$

Corollary 66. *Let $\mathcal{H}^{t_1,t_2,t_3}$ be a $\mathbb{Z}_8$-additive Hadamard code of type $(n; t_1, t_2, t_3)$. Let $\mathbf{w}_i$ be the ith row of A^{t_1,t_2,t_3}, $1 \le i \le t_1$. Let $E \subseteq \{1, \ldots, t_1\}$. Then,*

$$\mu(\sum_{i \in E} \mathbf{w}_i) = \sum_{\substack{i,j \in E \\ i<j}} \mu(\mathbf{w}_i + \mathbf{w}_j) + (|E| \bmod 2) \sum_{i \in E} \mu(\mathbf{w}_i).$$

Proof. Note that $\mathcal{H}^{t_1,t_2,t_3}$ contains the $2^{2t_2+t_3}$-fold replication code of $\mathcal{H}^{t_1,0,0}$. Therefore, the result follows from Lemma 65. $\mathcal{QED}$

Proposition 67. *Let t_1 and t_2 be nonnegative integers with $t_1 \geq 1$. Then, $rank(\Phi(\mathcal{H}^{t_1,t_2+1,0})) = rank(\Phi(\mathcal{H}^{t_1,t_2,0})) + 2t_1 + t_2 + \binom{t_1-1}{2}$.*

Proof. By (3.1), the generator matrix of $\mathcal{H}' = \mathcal{H}^{t_1,t_2+1,0}$ is

$$A^{t_1,t_2+1,0} = \begin{pmatrix} A & A & A & A \\ \mathbf{0} & \mathbf{2} & \mathbf{4} & \mathbf{6} \end{pmatrix},$$

where $A = A^{t_1,t_2,0}$ is the generator matrix of $\mathcal{H} = \mathcal{H}^{t_1,t_2,0}$. Let $r = \mathrm{rank}(\Phi(\mathcal{H}))$. Note that $\mathcal{H}'$ can be seen as the union of four cosets of the 4-fold replication code of $\mathcal{H}$, $(\mathcal{H}, \mathcal{H}, \mathcal{H}, \mathcal{H})$, which are

$$\begin{array}{lllll} C_0: & (\mathcal{H},\, \mathcal{H},\, \mathcal{H},\, \mathcal{H}) & & \\ C_1: & (\mathcal{H},\, \mathcal{H},\, \mathcal{H},\, \mathcal{H}) & + & (\mathbf{0},\, \mathbf{2},\, \mathbf{4},\, \mathbf{6}) \\ C_2: & (\mathcal{H},\, \mathcal{H},\, \mathcal{H},\, \mathcal{H}) & + & (\mathbf{0},\, \mathbf{4},\, \mathbf{0},\, \mathbf{4}) \\ C_3: & (\mathcal{H},\, \mathcal{H},\, \mathcal{H},\, \mathcal{H}) & + & (\mathbf{0},\, \mathbf{6},\, \mathbf{4},\, \mathbf{2}). \end{array}$$

We have that $\mathrm{rank}(\Phi(C_0)) = \mathrm{rank}(\Phi(\mathcal{H})) = r$. Let $\{\Phi(\mathbf{g}_1), \ldots, \Phi(\mathbf{g}_r)\}$ be a basis of $\langle H \rangle$. Then, a basis of $\langle \Phi(C_0) \rangle$ is $\{\Phi(\mathbf{g}'_1), \ldots, \Phi(\mathbf{g}'_r)\}$, where $\mathbf{g}'_i = (\mathbf{g}_i, \mathbf{g}_i, \mathbf{g}_i, \mathbf{g}_i)$ for all $i \in \{1, \ldots, r\}$. By Corollary 26, we have that $\langle \Phi(C_0 \cup C_2) \rangle = \langle \Phi(\mathbf{g}'_1), \ldots, \Phi(\mathbf{g}'_r), \Phi((\mathbf{0}, \mathbf{4}, \mathbf{0}, \mathbf{4})) \rangle$. Note that, if $\mathbf{u}' \in C_3$, then $\mathbf{u}' = (\mathbf{u}, \mathbf{u}+\mathbf{6}, \mathbf{u}+\mathbf{4}, \mathbf{u}+\mathbf{2}) = (\mathbf{u}, \mathbf{u}+\mathbf{2}, \mathbf{u}+\mathbf{4}, \mathbf{u}+\mathbf{6}) + (\mathbf{0}, \mathbf{4}, \mathbf{0}, \mathbf{4})$ with $\mathbf{u} \in \mathcal{H}$. Thus, it is easy to see that $\langle \Phi(\mathcal{H}') \rangle = \langle \Phi(C_0 \cup C_1 \cup C_2 \cup C_3) \rangle = \langle \Phi(C_0 \cup C_1 \cup C_2) \rangle$, again by Corollary 26.

Let $\mathbf{u}' = (\mathbf{u}, \mathbf{u}, \mathbf{u}, \mathbf{u}) \in C_0$, $u \in \mathcal{H}$, and $\mathbf{v}' = (\mathbf{0}, \mathbf{2}, \mathbf{4}, \mathbf{6})$. By Proposition 19, we know that $\Phi(\mathbf{u}') + \Phi(\mathbf{v}') = \Phi(\mathbf{u}' + \mathbf{v}' - 2(\mathbf{u}' \odot \mathbf{v}'))$. Since $-2(\mathbf{u}' \odot \mathbf{v}')$ is a vector of order 2, we have that $\Phi(\mathbf{u}' + \mathbf{v}') = \Phi(\mathbf{u}') + \Phi(\mathbf{v}') + \Phi(-2(\mathbf{u}' \odot \mathbf{v}'))$ by Corollary 26. Let $M' = \{-2(\mathbf{u}' \odot \mathbf{v}') : \mathbf{u}' \in C_0\} = \{(\mathbf{0}, \mu(\mathbf{u}), \mathbf{0}, \mu(\mathbf{u})) : \mathbf{u} \in \mathcal{H}\}$. Then, $\langle \Phi(\mathcal{H}') \rangle = \langle \Phi(\mathbf{g}'_1), \ldots, \Phi(\mathbf{g}'_r), \Phi((\mathbf{0}, \mathbf{4}, \mathbf{0}, \mathbf{4})), \Phi(\mathbf{v}'), \Phi(M') \rangle$. Note that, if $\mathbf{u} = \mathbf{2} \in \mathcal{H}$, then $\mathbf{u}' = \mathbf{2} \in C_0$ and $-2(\mathbf{u}' \odot \mathbf{v}') = (\mathbf{0}, \mathbf{4}, \mathbf{0}, \mathbf{4}) \in M'$. Thus, $\langle \Phi(\mathcal{H}') \rangle = \langle \Phi(\mathbf{g}'_1), \ldots, \Phi(\mathbf{g}'_r), \Phi(\mathbf{v}'), \Phi(M') \rangle$. It is easy to see that

$\Phi(\mathbf{v}')$ and the elements of $\{\Phi(\mathbf{g}'_1), \ldots, \Phi(\mathbf{g}'_r)\}$ and $\Phi(M')$ are linearly independent, because of the form of every $\mathbf{g}'_i$, $i \in \{1, \ldots, r\}$, and the elements of M'. Therefore, $\operatorname{rank}(\Phi(\mathcal{H}')) = r + 1 + \dim(\langle \Phi(M') \rangle)$. Since $M' = \{(\mathbf{0}, \mu(\mathbf{u}), \mathbf{0}, \mu(\mathbf{u})) : \mathbf{u} \in \mathcal{H}\}$, $\dim(\langle \Phi(M') \rangle) = \dim(\langle \Phi(M) \rangle)$, where $M = \{\mu(\mathbf{u}) : \mathbf{u} \in \mathcal{H}\}$.

Let $\mathbf{w}_i$ be the ith row of $A^{t_1,t_2,0}$, $i \in \{1, \ldots, t_1\}$, and $\mathbf{v}_j$ the (t_1+j)th row, $j \in \{1, \ldots, t_2\}$. Note that $\operatorname{ord}(\mathbf{w}_i) = 8$ and $\operatorname{ord}(\mathbf{v}_j) = 4$ for all $i \in \{1, \ldots, t_1\}$ and $j \in \{1, \ldots, t_2\}$. Then, $\mathcal{B}_2 = \{\mathbf{w}_1, \ldots, \mathbf{w}_{t_1}, \mathbf{v}_1, \ldots, \mathbf{v}_{t_2}, 2\mathbf{w}_1, \ldots, 2\mathbf{w}_{t_1}, 2\mathbf{v}_1, \ldots, 2\mathbf{v}_{t_2}, 4\mathbf{w}_1, \ldots, 4\mathbf{w}_{t_1}\}$ is a 2-base of $\mathcal{H}$. Let $\mathbf{u} \in \mathcal{H}$. We know that $\mathbf{u} = \sum_{i=1}^{3t_1+2t_2} \lambda_i \mathbf{b}_i$, where $\mathbf{b}_i \in \mathcal{B}_2$ is the ith element of $\mathcal{B}_2$ and $\lambda_i \in \{0, 1\}$. By Lemma 62 and the fact that $\mu(2\mathbf{v}_j) = \mu(4\mathbf{w}_i) = \mathbf{0}$ for all $i \in \{1, \ldots, t_1\}$ and $j \in \{1, \ldots, t_2\}$, we have that $\mu(\mathbf{u}) = \mu(\sum_{i=1}^{t_1} \lambda_i \mathbf{b}_i) + \sum_{i=t_1+1}^{2t_1+t_2} \mu(\lambda_i \mathbf{b}_i)$. Let $E = \{1 \leq i \leq t_1 : \lambda_i \neq 0\}$. Since $\mathbf{b}_i = \mathbf{w}_i$ for all $i \in \{1, \ldots, t_1\}$, by Corollary 66,

$$\mu(\sum_{i=1}^{t_1} \lambda_i \mathbf{b}_i) = \sum_{\substack{i,j \in E \\ i<j}} \mu(\mathbf{w}_i + \mathbf{w}_j) + (|E| \bmod 2) \sum_{i \in E} \mu(\mathbf{w}_i).$$

Moreover, since $\mathbf{w}_1 = \mathbf{1}$, we have that $\mu(\mathbf{w}_1) = \mathbf{0}$ and it is easy to check that $\mu(\mathbf{w}_1 + \mathbf{w}_i) = \mu(\mathbf{w}_i) + \mu(2\mathbf{w}_i) = \mu(\mathbf{b}_i) + \mu(\mathbf{b}_{t_1+t_2+i})$ for all $i \in \{2, \ldots, t_1\}$. Therefore,

$$\mu(\mathbf{u}) = \sum_{\substack{i,j \in E \setminus \{1\} \\ i<j}} \mu(\mathbf{b}_i + \mathbf{b}_j) + \sum_{i=2}^{2t_1+t_2} \mu(\lambda'_i \mathbf{b}_i)$$

for some $\lambda'_i \in \{0, 1\}$. Let $M_1 = \{\mu(\mathbf{b}_i + \mathbf{b}_j) : 2 \leq i < j \leq t_1\}$ and $M_2 = \{\mu(\mathbf{b}_i) : 2 \leq i \leq 2t_1 + t_2\}$. Recall that $\operatorname{ord}(\mu(\mathbf{w})) = 2$ for all $\mathbf{w} \neq \mathbf{0}$. Then, by Corollary 26, $\dim(\langle \Phi(M) \rangle) = \dim(\langle \Phi(M_1), \Phi(M_2) \rangle)$. Since the elements in $\Phi(M_1) \cup \Phi(M_2)$ are linearly independent, we have that $\operatorname{rank}(\Phi(\mathcal{H}')) = r + 1 + 2t_1 + t_2 - 1 + \binom{t_1-1}{2} = r + 2t_1 + t_2 + \binom{t_1-1}{2}$. $\mathcal{QED}$

Lemma 68. *Let q be a positive integer and $[q_0, q_1, q_2, \ldots]_2$ its binary expansion. Then, $\binom{q-1}{3} + q_0\binom{q-1}{2} + (q_0 + q_1)(q-1) + q_0(q_0 + q_1) \equiv 1 \bmod 2$.*

Proof. If $q \equiv 0 \bmod 4$, then $q_0 = q_1 = 0$ and $\binom{q-1}{3} \equiv 1 \bmod 2$ since $(q-2)/2$, $q-1$ and $q-3$ are odd numbers. Similarly, if $q \equiv 1 \bmod 4$, then $q_0 = 1$, $q_1 = 0$

and $\binom{q-1}{3}+\binom{q-1}{2}+(q-1)+1 \equiv 0+0+0+1 \equiv 1 \bmod 2$. If $q \equiv 2 \bmod 4$, then $q_0 = 0$, $q_1 = 1$ and $\binom{q-1}{3}+(q-1) \equiv 0+1 \equiv 1 \bmod 2$. Finally, if $q \equiv 3 \bmod 4$, then $q_1 = 1$, $q_1 = 1$ and $\binom{q-1}{3}+\binom{q-1}{2} \equiv 0+1 \equiv 1 \bmod 2$. $\mathcal{QED}$

Lemma 69. *Let q be a positive integer and $[q_0, q_1, q_2, \ldots]_2$ its binary expansion. Then,*

(i) $q-4 \equiv q_0 \bmod 2$,

(ii) $\binom{q-4}{2} \equiv q_1 \bmod 2$,

(iii) $\binom{q-3}{2} \equiv q_0+q_1 \bmod 2$,

(iv) $\binom{q-2}{3} \equiv q_0(q_0+q_1) \bmod 2$.

Proof. These congruences can be proved easily considering the different values of q modulo 4, as in the proof of Lemma 68. $\mathcal{QED}$

Lemma 70. *Let $\mathcal{H}^{t_1,0,0}$ be a $\mathbb{Z}_8$-additive Hadamard code of type $(n; t_1, 0, 0)$. Let $E \subseteq \{1, \ldots, t_1\}$, $q = |E|$ and $[q_0, q_1, q_2, \ldots]_2$ the binary expansion of q. Let $\mathbf{w}_i$ be the ith row of $A^{t_1,0,0}$, $i \in E$. Then,*

$$\Phi(\sum_{i\in E}\mathbf{w}_i) = \sum_{\substack{i,j,k,p\in E\\ i<j<k<p}}\Phi(\mathbf{w}_i+\mathbf{w}_j+\mathbf{w}_k+\mathbf{w}_p) + q_0(\sum_{\substack{i,j,k\in E\\ i<j<k}}\Phi(\mathbf{w}_i+\mathbf{w}_j+\mathbf{w}_k)) + \\ + (q_0+q_1)(\sum_{\substack{i,j\in E\\ i<j}}\Phi(\mathbf{w}_i+\mathbf{w}_j)) + q_0(q_0+q_1)(\sum_{i\in E}\Phi(\mathbf{w}_i)).$$

Proof. First, assume $E \subseteq \{2, \ldots, t_1\}$, and let $q = |E|$. By Remark 58, without loss of generality, we can assume that $E = \{2, \ldots, q+1\}$. Now, we prove this lemma by induction on the integer $q \geq 1$.

For $q \leq 5$, it is easy to check that the result holds. Note that, for $q = 5$, it is enough to check the result for $\mathbf{w}_2^6, \ldots, \mathbf{w}_6^6$. Assume $q \geq 6$ and suppose that the statement is true for $|E| = q-1$. Consider $\sum_{i=2}^{q+1}\mathbf{w}_i = \sum_{i=2}^{q}\mathbf{w}_i + \mathbf{w}_{q+1}$. Let $\mathbf{y} = \sum_{i=2}^{q}\mathbf{w}_i^q$. We have that $\sum_{i=2}^{q}\mathbf{w}_i = (\mathbf{y}, \ldots, \mathbf{y})$ is the 8^{t_1-q-2}-fold replication of $\mathbf{y}$. Then, $\sum_{i=2}^{q+1}\mathbf{w}_i$ is the 8^{t_1-q-1}-fold replication

of $(\mathbf{y}+\mathbf{0}, \mathbf{y}+\mathbf{1}, \ldots, \mathbf{y}+\mathbf{7})$. The result holds if

$$\begin{aligned}\Phi(\sum_{i=2}^{q}\mathbf{w}_i^q+\mathbf{k}) = &\sum_{2\le i<j<k<p\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{w}_k^q+\mathbf{w}_p^q)+\\ &\sum_{2\le i<j<k\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{w}_k^q+\mathbf{k})+\\ q_0\big(&\sum_{2\le i<j<k\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{w}_k^q)+\sum_{2\le i<j\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{k})\big)+\\ (q_0+q_1)\big(&\sum_{2\le i<j\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q)+\sum_{i=2}^{q}\Phi(\mathbf{w}_i^q+\mathbf{k})\big)+\\ &q_0(q_0+q_1)\big(\sum_{i=2}^{q}\Phi(\mathbf{w}_i^q)+\Phi(\mathbf{k})\big)\end{aligned}\quad(5.7)$$

for all $k\in\{0,\ldots,7\}$.

Let $\pi_8\in\mathcal{S}_n$ be the permutation of coordinates defined in (5.2). Let $\tilde{\pi}_8^k\in\mathcal{S}_{4n}$ be a permutation such that $\Phi\circ\pi_8^k=\tilde{\pi}_8^k\circ\Phi$. We have that $\Phi(\sum_{i=2}^{q}\mathbf{w}_i^q+\mathbf{k})=\Phi(\pi_8^k(\sum_{i=2}^{q}\mathbf{w}_i^q))=\tilde{\pi}_8^k(\Phi(\sum_{i=2}^{q}\mathbf{w}_i^q))$ by the properties of π_8^k. By induction, taking into account that $(q-1)_0\equiv q_0+1 \bmod 2$ and $(q-1)_1\equiv q_0+q_1+1 \bmod 2$, and using again the properties of π_8^k and the fact that $\Phi\circ\pi_8^k=\tilde{\pi}_8^k\circ\Phi$, we have that

$$\begin{aligned}\Phi(\sum_{i=2}^{q}\mathbf{w}_i+\mathbf{k}) = &\sum_{3\le i<j<r<p\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{w}_r^q+\mathbf{w}_p^q)+\\ &\sum_{3\le i<j<r\le q}\Phi(\mathbf{w}_2^q+\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{w}_r^q+\mathbf{k})+(q_0+1)\sum_{3\le i<j<r\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{w}_r^q)+\\ &(q_0+1)\sum_{3\le i<j\le q}\Phi(\mathbf{w}_2^q+\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{k})+q_1\sum_{3\le i<j\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q)+\\ &q_1\sum_{i=3}^{q}\Phi(\mathbf{w}_2^q+\mathbf{w}_i^q+\mathbf{k})+q_1(q_0+1)\sum_{i=3}^{q}\Phi(\mathbf{w}_i^q)+q_1(q_0+1)\Phi(\mathbf{w}_2+\mathbf{k}).\end{aligned}\quad(5.8)$$

By applying again the induction hypothesis to $\Phi(\mathbf{w}_2^q+\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{w}_r^q+\mathbf{k})$, and noting that for any $\mathbf{z}\in\mathbb{Z}_8^n$ we have $\sum_{3\le i<j<r\le q}\sum_{x,y\in\{i,j,r\},\ x<y}\Phi(\mathbf{z}+\mathbf{w}_x^q+\mathbf{w}_y^q)=(q-4)\sum_{3\le i<j\le q}\Phi(\mathbf{z}+\mathbf{w}_i^q+\mathbf{w}_j^q)$ and $\sum_{3\le i<j<r\le q}\sum_{x\in\{i,j,r\}}\Phi(\mathbf{z}+\mathbf{w}_x^q)=$

$\binom{q-3}{2}\sum_{i=3}^{q}\Phi(\mathbf{z}+\mathbf{w}_i^q)$, we obtain that

$$\sum_{3\le i<j<r\le q}\Phi(\mathbf{w}_2^q+\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{w}_r^q+\mathbf{k}) = \sum_{3\le i<j<r\le q}\Phi(\mathbf{w}_2^q+\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{w}_r^q)+$$
$$(q-4)\sum_{3\le i<j\le q}\Phi(\mathbf{w}_2^q+\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{k})+\sum_{3\le i<j<r\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{w}_r^q+\mathbf{k})+$$
$$\sum_{3\le i<j<r\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{w}_r^q)+(q-4)\sum_{3\le i<j\le q}\Phi(\mathbf{w}_2^q+\mathbf{w}_i^q+\mathbf{w}_j^q)+$$
$$\binom{q-3}{2}\sum_{i=3}^{q}\Phi(\mathbf{w}_2^q+\mathbf{w}_i^q+\mathbf{k})+(q-4)\sum_{3\le i<j\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q+\mathbf{k})+$$
$$(q-4)\sum_{3\le i<j\le q}\Phi(\mathbf{w}_i^q+\mathbf{w}_j^q)+\binom{q-3}{2}\sum_{i=3}^{q}\Phi(\mathbf{w}_2^q+\mathbf{w}_i^q)+\binom{q-3}{2}\sum_{i=3}^{q}\Phi(\mathbf{w}_i^q+\mathbf{k})+$$
$$\binom{q-2}{3}\Phi(\mathbf{w}_2+\mathbf{k})+\binom{q-3}{2}\sum_{i=3}^{q}\Phi(\mathbf{w}_i^q)+\binom{q-2}{3}\Phi(\mathbf{w}_2)+\binom{q-2}{3}\Phi(\mathbf{k}). \tag{5.9}$$

By replacing (5.9) into expression (5.8), and using items (i), (iii) and (iv) of Lemma 69, we have that (5.7) holds.

Finally, consider $1\in E$. By Remark 58, we can assume that $E=\{1,\dots,q\}$. Then, $\Phi(\sum_{i\in E}\mathbf{w}_i)=\Phi(\sum_{i=2}^{q}\mathbf{w}_i+\mathbf{1})$, and we can apply the same arguments as above. $\mathcal{QED}$

The previous lemma also works when repeated elements appear in the sum, as shown in the next result.

Lemma 71. *Let $\mathcal{H}^{t_1,0,0}$ be a $\mathbb{Z}_8$-additive Hadamard code of type $(n;t_1,0,0)$. Let $q\in\mathbb{Z}$ and $[q_0,q_1,q_2,\dots]_2$ its binary expansion. Let $\mathbf{w}_i$ be the ith row of $A^{t_1,0,0}$. Then,*

$$\Phi(\sum_{i=1}^{q}\mathbf{s}_i)=\sum_{1\le i<j<k<p\le q}\Phi(\mathbf{s}_i+\mathbf{s}_j+\mathbf{s}_k+\mathbf{s}_p)+q_0(\sum_{1\le i<j<k\le q}\Phi(\mathbf{s}_i+\mathbf{s}_j+\mathbf{s}_k))+$$
$$+(q_0+q_1)(\sum_{1\le i<j\le q}\Phi(\mathbf{s}_i+\mathbf{s}_j))+q_0(q_0+q_1)(\sum_{i=1}^{q}\Phi(\mathbf{s}_i)),$$

where $\mathbf{s}_i \in \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_{t_1}\}$ *for all* $i \in \{1, 2, \ldots, q\}$.

Proof. We prove this lemma by induction on the integer $q \geq 1$. It is easy to check by computer that for $q \leq 5$ the result holds. Assume $q \geq 6$ and suppose that the statement is true for all positive integers until $q-1$.

Let r_i be the multiplicity of $\mathbf{w}_i$, $i \in \{1, \ldots, t_1\}$, that is, the number of elements $\mathbf{w}_i$ that appear in the multiset $S = \{\mathbf{s}_1, \ldots, \mathbf{s}_q\}$. If there is an element $\mathbf{w}_i$ with multiplicity $r_i \geq 4$, then we may consider that $\mathbf{s}_q = \mathbf{s}_{q-1} = \mathbf{s}_{q-2} = \mathbf{s}_{q-3} = \mathbf{w}_i$. Note that the right-hand side of the equation of the statement can be easily rewritten by replacing q by $q-4$ and adding $\Phi(4\mathbf{w}_j)$. Moreover, by Corollary 26, the left-hand side of the equation is $\Phi(\sum_{i=1}^{q-4} \mathbf{s}_i) + \Phi(4\mathbf{w}_j)$. Therefore, we may assume that $r_i \leq 3$ for all $i \in \{1, \ldots, t_1\}$.

Let W be the set containing the elements of S without repetition. On the one hand, if $\mathbf{w}_1 \notin S$, taking into account the multiplicity of each element in W and Remark 58, we may assume that $W = \{\mathbf{w}_2, \ldots, \mathbf{w}_d\}$, where $r_2 \leq \cdots \leq r_d$ and $\mathbf{s}_1 = \cdots = \mathbf{s}_{r_2} = \mathbf{w}_2, \ldots, \mathbf{s}_{q-r_d+1} = \cdots = \mathbf{s}_q = \mathbf{w}_d$. On the other hand, if $\mathbf{w}_1 \in S$, we assume that $q > r_1 + r_2$. Otherwise, if $q = r_1 + r_2$, since $q \geq 6$ and $r_1, r_2 \leq 3$, then we have to show that the statement is true for $\Phi(\mathbf{w}_2+\mathbf{w}_2+\mathbf{w}_2+\mathbf{w}_1+\mathbf{w}_1+\mathbf{w}_1)$, which can be checked easily. Since $q > r_1+r_2$, we can order all elements $\mathbf{s}_1, \ldots, \mathbf{s}_q$ as above, placing the r_1 vectors $\mathbf{w}_1$ just before the r_d vectors $\mathbf{w}_d$.

Consider $\sum_{i=1}^{q} \mathbf{s}_i = \sum_{i=1}^{q-(r_1+r_d)} \mathbf{s}_i + \sum_{i=1}^{r_1} \mathbf{w}_1 + \sum_{i=1}^{r_d} \mathbf{w}_d$. Let $\mathbf{y} = \sum_{i=1}^{q-(r_1+r_d)} \mathbf{s}_i^{d-1}$. We have that $\sum_{i=1}^{q-(r_1+r_d)} \mathbf{s}_i = (\mathbf{y}, \ldots, \mathbf{y})$ is a fold replication of $\mathbf{y}$. Then, $\sum_{i=1}^{q} \mathbf{s}_i$ is a fold replication of

$$(\mathbf{y} + r_1\mathbf{w}_1^{d-1} + \mathbf{0}, \mathbf{y} + r_1\mathbf{w}_1^{d-1} + \mathbf{1} + \overset{(r_d)}{\cdots} + \mathbf{1}, \ldots, \mathbf{y} + r_1\mathbf{w}_1^{d-1} + \mathbf{7} + \overset{(r_d)}{\cdots} + \mathbf{7}) =$$

$$(\mathbf{y} + r_1\mathbf{1}, \mathbf{y} + (r_1 + r_d)\mathbf{1}, \ldots, \mathbf{y} + (r_1 + 7r_d)\mathbf{1}).$$

The result holds if the statement is true for $\Phi(\sum_{i=1}^{q-(r_1+r_d)} \mathbf{s}_i^{d-1} + (r_1 + k \cdot r_d)\mathbf{1})$ for all $k \in \{0, \ldots, 7\}$. Moreover, as before, we may assume that $r_1 + k \cdot r_d < 4$, so we have to check that the statement is true for $\Phi(\sum_{i=1}^{q-(r_1+r_d)} \mathbf{s}_i^{d-1} + \bar{r}\mathbf{w}_1^{d-1})$, where $\bar{r} = (r_1 + k \cdot r_d) \bmod 4$, or equivalently for $\Phi(\sum_{i=1}^{q-(r_1+r_d)+\bar{r}} \mathbf{s}_i^{d-1})$, where

$\mathbf{s}_i = \mathbf{w}_1$ for all $i \in \{q-(r_1+r_d)+1, \ldots, q-(r_1+r_d)+\bar{r}\}$ if $\bar{r} \geq 1$.

If $r_1 + r_d - \bar{r} > 0$, we can apply the induction hypothesis to obtain the result. Otherwise, let $\pi_8 = \prod_{i=0}^{8^{t_1-2}-1}(8i+1, 8i+2, 8i+3, 8i+4, 8i+5, 8i+6, 8i+7, 8i+8) \in \mathcal{S}_n$ be a permutation of coordinates. Note that $\pi_8(\mathbf{w}_2) = \mathbf{w}_2 + \mathbf{1}$ and $\pi_8(\mathbf{w}_j) = \mathbf{w}_j$ for all $j \in \{3, \ldots, d\}$. Let $\tilde{\pi}_8 \in \mathcal{S}_{4n}$ be a permutation such that $\Phi \circ \pi_8 = \tilde{\pi}_8 \circ \Phi$. Therefore, we have that $\Phi(\sum_{i=1}^{r_2} \mathbf{w}_2^{d-1} + \sum_{i=r_2+1}^{q-(r_1+r_d)} \mathbf{s}_i^{d-1} + (\bar{r}-r_2)\mathbf{1} + r_2\mathbf{1}) = \Phi(\pi_8(\sum_{i=1}^{r_2} \mathbf{w}_2^{d-1} + \sum_{i=r_2+1}^{q-(r_1+r_d)} \mathbf{s}_i^{d-1} + (\bar{r}-r_2)\mathbf{1})) = \tilde{\pi}_8(\Phi(\sum_{i=1}^{r_2} \mathbf{w}_2^{d-1} + \sum_{i=r_2+1}^{q-(r_1+r_d)} \mathbf{s}_i^{d-1} + (\bar{r}-r_2)\mathbf{1}))$. Note that $\bar{r} \geq r_1 + r_d \geq r_d \geq r_2$. Then, considering $\mathbf{s}_i^{d-1} = \mathbf{w}_1$ for all $i \in \{q-(r_1+r_d)+1, \ldots, q-(r_1+r_d)+(\bar{r}-r_2)\}$ if $\bar{r} - r_2 \geq 1$, it is enough to show the statement for $\tilde{\pi}_8(\Phi(\sum_{i=1}^{r_2} \mathbf{w}_2^{d-1} + \sum_{i=r_2+1}^{q-(r_1+r_d-\bar{r}+r_2)} \mathbf{s}_i^{d-1})) = \tilde{\pi}_8(\Phi(\sum_{i=1}^{q-r^*} \mathbf{s}_i^{d-1}))$, where $r^* = r_1 + r_2 + r_d - \bar{r}$.

Now, in order to be able to apply the hypothesis induction to $\Phi(\sum_{i=1}^{q-r^*} \mathbf{s}_i^{d-1})$, we have to verify that $r^* > 0$. First, note that if $r_i \in \{0,1\}$ for all $i \in \{1, \ldots, t_1\}$, then the statement is true by Lemma 70. Therefore, we can assume that for some $i \in \{1, \ldots, t_1\}$, $r_i \geq 2$, so at least one of r_1 or r_d must be greater than 1. We also have that $r_2, r_d \in \{1,2,3\}$ and $r_1 \in \{0,1,2,3\}$. On the one hand, if $r_1 = 0$, we have that $r_d \in \{2,3\}$. Then, if $\bar{r} < 3$, clearly $r^* > 0$; and if $\bar{r} = 3$, $k \cdot r_d = 3 \bmod 4$ which implies that $r_d = 3$ and $r^* > 0$. On the other hand, if $r_1 > 0$, $r_d \in \{1,2,3\}$ and $r_1 + r_2 + r_d > 3$ which also gives that $r^* > 0$.

With the aim of verifying the statement, we consider $\tilde{\pi}_8(\Phi(\sum_{i=1}^{q-r^*} \mathbf{s}_i^{d-1}))$ under different cases depending on the value of $r_2 \in \{1,2,3\}$. First, consider that $r_2 = 1$, i.e., $\mathbf{s}_1 = \mathbf{w}_2$ and $\mathbf{s}_i \neq \mathbf{w}_2$ for all $i \in \{2, 3, \ldots, q\}$. Then, by using the same arguments as in the proof of Lemma 70, we have that the result holds. Next, consider that $r_2 = 2$. By induction hypothesis, taking into account that $(q-2)_0 \equiv q_0 \bmod 2$ and $(q-2)_1 \equiv q_1 + 1 \bmod 2$, and using

again the properties of π_8 and the fact that $\Phi \circ \pi_8 = \tilde{\pi}_8 \circ \Phi$, we have that

$$\Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \sum_{i=3}^{q-2} \mathbf{s}_i^q + \mathbf{1} + \mathbf{1}) = \sum_{3\le i<j<k<p\le q-2} \Phi(\mathbf{s}_i^d + \mathbf{s}_j^d + \mathbf{s}_k^d + \mathbf{s}_p^d) + \sum_{3\le i<j\le q-2} \Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \mathbf{s}_i^d + \mathbf{s}_j^d + \mathbf{1} + \mathbf{1}) + q_0\Big[\sum_{3\le i<j<k\le q-2} \Phi(\mathbf{s}_i^d + \mathbf{s}_j^d + \mathbf{s}_k^d) + \sum_{3\le i\le q-2} \Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \mathbf{s}_i^d + \mathbf{1} + \mathbf{1})\Big] + (q_0+q_1+1)\Big[\sum_{3\le i<j\le q-2} \Phi(\mathbf{s}_i^d + \mathbf{s}_j^d) + \Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \mathbf{1} + \mathbf{1})\Big] + q_0(q_0+q_1+1)\sum_{3\le i\le q-2} \Phi(\mathbf{s}_i^d). \quad (5.10)$$

By applying again the induction hypothesis to the terms of (5.10) having more than four addends, that is, $\Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \mathbf{s}_i^d + \mathbf{1} + \mathbf{1})$ and $\Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \mathbf{s}_i^d + \mathbf{s}_j^d + \mathbf{1} + \mathbf{1})$, we obtain that

$$\sum_{3\le i\le q-2} \Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \mathbf{s}_i^d + \mathbf{1} + \mathbf{1}) = \sum_{3\le i\le q-2} \Phi(\mathbf{s}_i^d) + \sum_{3\le i\le q-2} \Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \mathbf{s}_i^d) + \sum_{3\le i\le q-2} \Phi(\mathbf{s}_i^d + \mathbf{1} + \mathbf{1}) + (q-4)\Big[\Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \mathbf{1} + \mathbf{1}) + \Phi(\mathbf{w}_2^d + \mathbf{w}_2^d) + \Phi(\mathbf{1} + \mathbf{1})\Big] \quad (5.11)$$

and

$$\sum_{3\le i<j\le q-2} \Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \mathbf{s}_i^d + \mathbf{s}_j^d + \mathbf{1} + \mathbf{1}) = \sum_{3\le i<j\le q-2} \Phi(\mathbf{s}_i^d + \mathbf{s}_j^d) + \sum_{3\le i<j\le q-2} \Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \mathbf{s}_i^d + \mathbf{s}_j^d) + \sum_{3\le i<j\le q-2} \Phi(\mathbf{s}_i^d + \mathbf{s}_j^d + \mathbf{1} + \mathbf{1}) + \binom{q-4}{2}\Big[\Phi(\mathbf{w}_2^d + \mathbf{w}_2^d + \mathbf{1} + \mathbf{1}) + \Phi(\mathbf{w}_2^d + \mathbf{w}_2^d) + \Phi(\mathbf{1} + \mathbf{1})\Big]. \quad (5.12)$$

By replacing (5.11) and (5.12) into expression (5.10), and using items (i) and

(ii) of Lemma 69, we have that (5.10) is equal to

$$\sum_{3\le i<j<k<p\le q-2}\Phi(\mathbf{s}_i^d+\mathbf{s}_j^d+\mathbf{s}_k^d+\mathbf{s}_p^d)+\sum_{3\le i<j\le q-2}\Phi(\mathbf{w}_2^d+\mathbf{w}_2^d+\mathbf{s}_i^d+\mathbf{s}_j^d)+$$
$$\sum_{3\le i<j\le q-2}\Phi(\mathbf{s}_i^d+\mathbf{s}_j^d+\mathbf{1}+\mathbf{1})+\Phi(\mathbf{w}_2^d+\mathbf{w}_2^d+\mathbf{1}+\mathbf{1})+$$
$$q_0\Big[\sum_{3\le i<j\le q-2}\Phi(\mathbf{s}_i^d+\mathbf{s}_j^d)\sum_{3\le i\le q-2}\Phi(\mathbf{w}_2^d+\mathbf{w}_2^d+\mathbf{s}_i^d)\sum_{3\le i\le q-2}\Phi(\mathbf{s}_i^d+\mathbf{1}+\mathbf{1})\Big]+$$
$$(q_0+q_1)\Big[\sum_{3\le i<j\le q-2}\Phi(\mathbf{s}_i^d+\mathbf{s}_j^d)+\Phi(\mathbf{w}_2^d+\mathbf{w}_2^d)+\Phi(\mathbf{1}+\mathbf{1})\Big]+$$
$$q_0(q_0+q_1)\sum_{3\le i\le q-2}\Phi(\mathbf{s}_i^d).$$

Note that all the terms that are missing in order to obtain the result appear repeated in pairs, so they sum zero. Finally, the case with $r_2=3$ can also be proved by using similar arguments. Therefore, the result holds. $\mathcal{QED}$

Lemma 72. *Let $\mathcal{H}^{t_1,0,0}$ be a $\mathbb{Z}_8$-additive Hadamard code of type $(n;t_1,0,0)$. Let $\mathbf{w}_i$ be the ith row of $A^{t_1,0,0}$, $1\le i\le t_1$. Then, given $i,j,k\in\{1,\dots,t_1\}$,*

$$\Phi(2\mathbf{w}_i+\mathbf{w}_j+\mathbf{w}_k)+\Phi(\mathbf{w}_i+2\mathbf{w}_j+\mathbf{w}_k)=$$
$$\Phi(\mathbf{w}_i)+\Phi(\mathbf{w}_j)+\Phi(2\mathbf{w}_i)+\Phi(2\mathbf{w}_j)+\Phi(\mathbf{w}_i+\mathbf{w}_k)+\Phi(\mathbf{w}_j+\mathbf{w}_k)+$$
$$+\Phi(2\mathbf{w}_i+\mathbf{w}_k)+\Phi(2\mathbf{w}_j+\mathbf{w}_k)+\Phi(2\mathbf{w}_j+\mathbf{w}_i)+\Phi(2\mathbf{w}_i+\mathbf{w}_j). \quad (5.13)$$

Proof. Suppose that $2\le i<j<k$. By Remark 58, it is enough to see that (5.13) holds for $\mathbf{w}_2,\mathbf{w}_3,\mathbf{w}_4$. In fact, it is enough to show that it is true for $\mathbf{w}_2^3,\mathbf{w}_3^3,\mathbf{k}$ for all $k\in\{0,1,\dots,7\}$. Let A be the right-hand side of (5.13).

On the one hand, if $\mathbf{w}_k=\mathbf{k}$, we need to show that

$$\Phi(2\mathbf{w}_2^3+\mathbf{w}_3^3+\mathbf{k})+\Phi(\mathbf{w}_2^3+2\mathbf{w}_3^3+\mathbf{k})=$$
$$\Phi(\mathbf{w}_2^3)+\Phi(\mathbf{w}_3^3)+\Phi(2\mathbf{w}_2^3)+\Phi(2\mathbf{w}_3^3)+\Phi(\mathbf{w}_2^3+\mathbf{k})+\Phi(\mathbf{w}_3^3+\mathbf{k})+$$
$$+\Phi(2\mathbf{w}_2^3+\mathbf{k})+\Phi(2\mathbf{w}_3^3+\mathbf{k})+\Phi(2\mathbf{w}_3^3+\mathbf{w}_2^3)+\Phi(2\mathbf{w}_2^3+\mathbf{w}_3^3) \quad (5.14)$$

for all $k\in\{0,1,\dots,7\}$. Let A_1 be the right-hand side of (5.14). First,

for $k = 0$, it is easy to see that (5.14) holds. Note that, by Proposition 19, $\Phi(2\mathbf{w}_i + \mathbf{1}) = \Phi(2\mathbf{w}_i) + \Phi(\mathbf{1})$ for all $1 \leq i \leq t_1$. Then, for $k = 1$, $A_1 = \Phi(\mathbf{w}_2^3) + \Phi(\mathbf{w}_3^3) + \Phi(\mathbf{w}_2^3 + \mathbf{1}) + \Phi(\mathbf{w}_3^3 + \mathbf{1}) + \Phi(2\mathbf{w}_3^3 + \mathbf{w}_2^3) + \Phi(2\mathbf{w}_2^3 + \mathbf{w}_3^3)$. By the same proposition, we also have that $\Phi(\mathbf{w}_i) + \Phi(\mathbf{w}_i + 2\mathbf{w}_j) = \Phi(2\mathbf{w}_j) + \Phi(-2(\mathbf{w}_i \odot 2\mathbf{w}_j))$ for all $i, j \in \{2, 3\}$. Thus,

$$A_1 = \Phi(2\mathbf{w}_2^3) + \Phi(2\mathbf{w}_3^3) + \Phi(\mathbf{w}_2^3 + \mathbf{1}) + \Phi(\mathbf{w}_3^3 + \mathbf{1}) + \\ + \Phi(-2(2\mathbf{w}_3^3 \odot \mathbf{w}_2^3)) + \Phi(-2(2\mathbf{w}_2^3 \odot \mathbf{w}_3^3)).$$

Again, by Proposition 19, $\Phi(2\mathbf{w}_i) + \Phi(\mathbf{w}_j + \mathbf{1}) = \Phi(2\mathbf{w}_i + \mathbf{w}_j + \mathbf{1}) + \Phi(-2(2\mathbf{w}_i \odot (\mathbf{w}_j + \mathbf{1})))$ for all $i, j \in \{2, 3\}$, so

$$A_1 = \Phi(2\mathbf{w}_2^3 + \mathbf{w}_3^3 + \mathbf{1}) + \Phi(\mathbf{w}_2^3 + 2\mathbf{w}_3^3 + \mathbf{1}) + \Phi(-2(2\mathbf{w}_3^3 \odot \mathbf{w}_2^3)) + \Phi(-2(2\mathbf{w}_2^3 \odot \mathbf{w}_3^3)) + \\ + \Phi(-2(2\mathbf{w}_3^3 \odot (\mathbf{w}_2^3 + \mathbf{1}))) + \Phi(-2(2\mathbf{w}_2^3 \odot (\mathbf{w}_3^3 + \mathbf{1}))).$$

Let $\mathbf{x} = (0, 0, 4, 4, 0, 0, 4, 4)$, $\mathbf{y} = (0, 4, 4, 0, 0, 4, 4, 0)$, and $\mathbf{z} = (0, 4, 0, 4, 0, 4, 0, 4)$. It is easy to check that

$$\begin{aligned} -2(2\mathbf{w}_3^3 \odot \mathbf{w}_2^3) &= (\mathbf{0}, \mathbf{x}, \mathbf{0}, \mathbf{x}, \mathbf{0}, \mathbf{x}, \mathbf{0}, \mathbf{x}) \\ -2(2\mathbf{w}_3^3 \odot (\mathbf{w}_2^3 + \mathbf{1})) &= (\mathbf{0}, \mathbf{y}, \mathbf{0}, \mathbf{y}, \mathbf{0}, \mathbf{y}, \mathbf{0}, \mathbf{y}) \\ -2(2\mathbf{w}_2^3 \odot \mathbf{w}_3^3) &= (\mathbf{0}, \mathbf{0}, \mathbf{z}, \mathbf{z}, \mathbf{0}, \mathbf{0}, \mathbf{z}, \mathbf{z}) \\ -2(2\mathbf{w}_2^3 \odot (\mathbf{w}_3^3 + \mathbf{1})) &= (\mathbf{0}, \mathbf{z}, \mathbf{z}, \mathbf{0}, \mathbf{0}, \mathbf{z}, \mathbf{z}, \mathbf{0}). \end{aligned} \tag{5.15}$$

The sum of the four vectors in (5.15) is zero, since $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$, so $A_1 = \Phi(2\mathbf{w}_2^3 + \mathbf{w}_3^3 + \mathbf{1}) + \Phi(\mathbf{w}_2^3 + 2\mathbf{w}_3^3 + \mathbf{1})$ and (5.14) holds. For $k = 2$, it is easy to see that the result holds by Lemma 71. For $k = 3$, it follows also from Lemma 71, the previous result for $k = 1$, and the fact that $\Phi(2\mathbf{w}_i + \mathbf{1}) = \Phi(2\mathbf{w}_i) + \Phi(\mathbf{1})$ for all $1 \leq i \leq t_1$. Finally, for the rest of the cases, if $\mathbf{w}_k = \mathbf{k} + \mathbf{4}$, $k \in \{0, 1, 2, 3\}$, then $\Phi(2\mathbf{w}_2 + \mathbf{w}_3 + \mathbf{k} + \mathbf{4}) + \Phi(\mathbf{w}_2 + 2\mathbf{w}_3 + \mathbf{k} + \mathbf{4}) = \Phi(2\mathbf{w}_2 + \mathbf{w}_3 + \mathbf{k}) + \Phi(\mathbf{w}_2 + 2\mathbf{w}_3 + \mathbf{k})$ and the result holds since $\mathbf{w}_k$ appears 4 times in A.

On the other hand, if $\mathbf{w}_i = \mathbf{k}$ (or $\mathbf{w}_j = \mathbf{k}$), we need to show that

$$\begin{aligned}\Phi(2\mathbf{k} + \mathbf{w}_2^3 + \mathbf{w}_3^3) + \Phi(\mathbf{k} + 2\mathbf{w}_2^3 + \mathbf{w}_3^3) = \\ \Phi(\mathbf{k}) + \Phi(\mathbf{w}_2^3) + \Phi(2\mathbf{k}) + \Phi(2\mathbf{w}_2^3) + \Phi(\mathbf{k} + \mathbf{w}_3^3) + \Phi(\mathbf{w}_2^3 + \mathbf{w}_3^3) + \\ + \Phi(2\mathbf{k} + \mathbf{w}_3^3) + \Phi(2\mathbf{w}_2^3 + \mathbf{w}_3^3) + \Phi(2\mathbf{w}_2^3 + \mathbf{k}) + \Phi(2\mathbf{k} + \mathbf{w}_2^3) \quad (5.16)\end{aligned}$$

for all $k \in \{0, 1, \ldots, 7\}$. Let A_2 be the right-hand side of (5.16). First, for $k = 0$, it is easy to see that (5.16) holds. For $k = 1$, by applying Proposition 19 to $\Phi(\mathbf{w}_2^3 + \mathbf{w}_3^3) + \Phi(\mathbf{2})$ and $\Phi(\mathbf{w}_3^3 + \mathbf{1}) + \Phi(2\mathbf{w}_2^3)$, we have that

$$\begin{aligned}A_2 = \Phi(\mathbf{2} + \mathbf{w}_2^3 + \mathbf{w}_3^3) + \Phi(\mathbf{1} + 2\mathbf{w}_2^3 + \mathbf{w}_3^3) \\ + \Phi(-2((\mathbf{w}_2^3 + \mathbf{w}_3^3) \odot \mathbf{2})) + \Phi(-2((\mathbf{w}_3^3 + \mathbf{1}) \odot 2\mathbf{w}_2^3)) + \Phi(\mathbf{1}) + \Phi(\mathbf{w}_2^3) \\ + \Phi(\mathbf{2} + \mathbf{w}_3^3) + \Phi(2\mathbf{w}_2^3 + \mathbf{w}_3^3) + \Phi(2\mathbf{w}_2^3 + \mathbf{1}) + \Phi(\mathbf{2} + \mathbf{w}_2^3).\end{aligned}$$

Again, applying Proposition 19 to the terms $\Phi(\mathbf{2}+\mathbf{w}_3^3)$, $\Phi(2\mathbf{w}_2^3+\mathbf{w}_3^3)$, $\Phi(2\mathbf{w}_2^3+\mathbf{1})$ and $\Phi(\mathbf{2} + \mathbf{w}_2^3)$ of A_2, we obtain that

$$\begin{aligned}A_2 = \Phi(\mathbf{2} + \mathbf{w}_2^3 + \mathbf{w}_3^3) + \Phi(\mathbf{1} + 2\mathbf{w}_2^3 + \mathbf{w}_3^3) \\ + \Phi(-2((\mathbf{w}_2^3 + \mathbf{w}_3^3) \odot \mathbf{2})) + \Phi(-2((\mathbf{w}_3^3 + \mathbf{1}) \odot 2\mathbf{w}_2^3)) \\ + \Phi(-2(\mathbf{2} \odot \mathbf{w}_3^3)) + \Phi(-2(2\mathbf{w}_2^3 \odot \mathbf{w}_3^3)) + \Phi(-2(\mathbf{2} \odot \mathbf{w}_2^3)).\end{aligned}$$

It is easy to check that

$$\begin{aligned}\Phi(-2((\mathbf{w}_2^3 + \mathbf{w}_3^3) \odot \mathbf{2})) &= (\mathbf{x}, \mathbf{y}, \mathbf{x}+\mathbf{4}, \mathbf{y}+\mathbf{4}, \mathbf{x}, \mathbf{y}, \mathbf{x}+\mathbf{4}, \mathbf{y}+\mathbf{4}) \\ \Phi(-2((\mathbf{w}_3^3 + \mathbf{1}) \odot 2\mathbf{w}_2^3)) &= (\mathbf{0}, \mathbf{z}, \mathbf{z}, \mathbf{0}, \mathbf{0}, \mathbf{z}, \mathbf{z}, \mathbf{0}) \\ \Phi(-2(2\mathbf{w}_2^3 \odot \mathbf{w}_3^3)) &= (\mathbf{0}, \mathbf{0}, \mathbf{z}, \mathbf{z}, \mathbf{0}, \mathbf{0}, \mathbf{z}, \mathbf{z}) \\ \Phi(-2(\mathbf{2} \odot \mathbf{w}_3^3)) &= (\mathbf{0}, \mathbf{0}, \mathbf{4}, \mathbf{4}, \mathbf{0}, \mathbf{0}, \mathbf{4}, \mathbf{4}) \\ \Phi(-2(\mathbf{2} \odot \mathbf{w}_2^3)) &= (\mathbf{x}, \mathbf{x}, \mathbf{x}, \mathbf{x}, \mathbf{x}, \mathbf{x}, \mathbf{x}, \mathbf{x}).\end{aligned} \quad (5.17)$$

The sum of the five vectors in (5.17) is zero, since $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$, so $A_2 = \Phi(\mathbf{2} + \mathbf{w}_2^3 + \mathbf{w}_3^3) + \Phi(\mathbf{1} + 2\mathbf{w}_2^3 + \mathbf{w}_3^3)$ and (5.16) holds. For $k \in \{2, 3\}$, it is easy to see that the result holds by Lemma 71. Finally, if $\mathbf{w}_i = \mathbf{k} + \mathbf{4}$,

$k \in \{0,1,2,3\}$, then $\Phi(2\mathbf{k}+\mathbf{8}+\mathbf{w}_2+\mathbf{w}_3)+\Phi(\mathbf{k}+\mathbf{4}+2\mathbf{w}_2+\mathbf{w}_3) = \Phi(\mathbf{4}) + \Phi(2\mathbf{k}+\mathbf{w}_2+\mathbf{w}_3)+\Phi(\mathbf{k}+2\mathbf{w}_2+\mathbf{w}_3)$ and the result follows since $\mathbf{w}_i$ appears 3 times in A.

Now, suppose that some of the elements i,j,k are equal. If $i=j=k$ or $i=j$, then (5.13) holds trivially. If $i=k$ (or $j=k$), then it is enough to show that

$$\Phi(3\mathbf{k}+\mathbf{w}_2^2)+\Phi(2\mathbf{k}+2\mathbf{w}_2^2) = \\ \Phi(\mathbf{k})+\Phi(\mathbf{w}_2^2)+\Phi(2\mathbf{w}_2^2)+\Phi(3\mathbf{k})+\Phi(\mathbf{k}+\mathbf{w}_2^2)+\Phi(2\mathbf{k}+\mathbf{w}_2^2) \quad (5.18)$$

for all $k \in \{0,1,\ldots,7\}$. Let A_3 be the right-hand side of (5.18). First, for $k=0$, it is easy to see that (5.18) holds. For $k=1$, note that, by Proposition 19, $\Phi(\mathbf{2}) = \Phi(\mathbf{3})+\Phi(\mathbf{1})$ and $\Phi(\mathbf{w}_2)+\Phi(\mathbf{2})+\Phi(\mathbf{w}_2+\mathbf{2}) = \Phi(-2(\mathbf{w}_2 \odot \mathbf{2}))$. Therefore,

$$A_3 = \Phi(2\mathbf{w}_2^2)+\Phi(\mathbf{w}_2^2+\mathbf{1})+\Phi(-2(\mathbf{w}_2^2 \odot \mathbf{2})) \\ = \Phi(2\mathbf{w}_2^2)+\Phi(\mathbf{2})+\Phi(\mathbf{w}_2^2+\mathbf{1})+\Phi(\mathbf{2})+\Phi(-2(\mathbf{w}_2^2 \odot \mathbf{2})).$$

Again, by Proposition 19, we have that

$$A_3 = \Phi(2\mathbf{w}_2^2+\mathbf{2})+\Phi(\mathbf{w}_2^2+\mathbf{3})+\Phi(-2(\mathbf{w}_2^2 \odot \mathbf{2}))+ \\ +\Phi(-2(2\mathbf{w}_2^2 \odot \mathbf{2}))+\Phi(-2((\mathbf{w}_2^2+\mathbf{1}) \odot \mathbf{2})).$$

It is easy to check that the sum of the three last terms is $\mathbf{x}+\mathbf{z}+\mathbf{y}=\mathbf{0}$. In a similar way, it holds for $k=3$. The rest of the cases, $k \in \{2,4,5,6,7\}$, can also be checked easily, so (5.18) holds.

Now, we consider that, at least one of i,j,k is equal to 1. If $i=j=k=1$, or $i=j=1$, then the result is trivial. If $i=k=1$ (or $j=k=1$), the result is equivalent to prove (5.18) with $\mathbf{k}=\mathbf{1}$. Finally, if $k=1$, it is equivalent to (5.14) with $\mathbf{k}=\mathbf{1}$, and if $i=1$ (or $j=1$), it is equivalent to (5.16) with $\mathbf{k}=\mathbf{1}$. Therefore, the result holds. $\mathcal{QED}$

Lemma 73. *Let $\mathcal{H}^{t_1,0,0}$ be a $\mathbb{Z}_8$-additive Hadamard code of type $(n;t_1,0,0)$.*

Let $\mathbf{w}_i$ *be the ith row of* $A^{t_1,0,0}$, $1 \leq i \leq t_1$. *Then, given* $i, j, k \in \{1, \ldots, t_1\}$,

$$\begin{aligned}\Phi(\mathbf{w}_i + \mathbf{w}_j + \mathbf{1}) = \Phi(2\mathbf{w}_i) + \Phi(2\mathbf{w}_j) + \Phi(\mathbf{1}) + \Phi(\mathbf{w}_i + \mathbf{1}) + \\ + \Phi(\mathbf{w}_j + \mathbf{1}) + \Phi(\mathbf{w}_i + \mathbf{w}_j) + \Phi(2\mathbf{w}_i + \mathbf{w}_j) + \Phi(\mathbf{w}_i + 2\mathbf{w}_j),\end{aligned}$$

$$\begin{aligned}\Phi(\mathbf{w}_i + \mathbf{w}_j + \mathbf{w}_k + \mathbf{1}) = \Phi(\mathbf{w}_i + \mathbf{1}) + \Phi(\mathbf{w}_i + \mathbf{w}_j) + \Phi(\mathbf{w}_i + 2\mathbf{w}_j) + \\ + \Phi(2\mathbf{w}_i + \mathbf{w}_j) + \Phi(\mathbf{w}_j + \mathbf{1}) + \Phi(\mathbf{w}_k) + \Phi(2\mathbf{w}_k) + \Phi(\mathbf{w}_k + \mathbf{1}) + \\ + \Phi(2\mathbf{w}_i + \mathbf{w}_k) + \Phi(2\mathbf{w}_j + \mathbf{w}_k) + \Phi(\mathbf{w}_i + \mathbf{w}_j + 2\mathbf{w}_k) + \Phi(\mathbf{w}_i + \mathbf{w}_j + \mathbf{w}_k).\end{aligned}$$

Proof. First, if $2 \leq i < j < k$, by Remark 58, the above equations can be showed to be true by checking that they hold for $\mathbf{w}_2^3, \mathbf{w}_3^3, \mathbf{k}$ for all $k \in \{0, 1, \ldots, 7\}$. It is also easy to see that they hold if some of the elements i, j, k are equal, or at least one of them is equal to 1. $\mathcal{QED}$

Lemma 74. *Let* $\mathcal{H}^{t_1,t_2,t_3}$ *be a* $\mathbb{Z}_8$*-additive Hadamard code of type* $(n; t_1, t_2, t_3)$. *Let* $\mathbf{w}$ *be a row of* $A^{t_1,0,0}$. *Then,*

$$\Phi(3\mathbf{w}) = \Phi(\mathbf{3}) + \Phi(\mathbf{w}) + \Phi(\mathbf{w} + \mathbf{1}) + \Phi(\mathbf{w} + \mathbf{2}).$$

Proof. Let $A = \Phi(\mathbf{3}) + \Phi(\mathbf{w}) + \Phi(\mathbf{w} + \mathbf{1}) + \Phi(\mathbf{w} + \mathbf{2})$. By Proposition 19, we have that $\Phi(\mathbf{w} + \mathbf{1}) + \Phi(\mathbf{w} + \mathbf{2}) = \Phi(2\mathbf{w} + \mathbf{3} - 2((\mathbf{w} + \mathbf{1}) \odot (\mathbf{w} + \mathbf{2})))$. It easy to check that $\mathrm{ord}(-2((\mathbf{w} + \mathbf{1}) \odot (\mathbf{w} + \mathbf{2}))) = 2$, so $A = \Phi(\mathbf{3}) + \Phi(\mathbf{w}) + \Phi(2\mathbf{w} + \mathbf{3}) + \Phi(-2((\mathbf{w} + \mathbf{1}) \odot (\mathbf{w} + \mathbf{2})))$. Now, by applying Lemma 71 to the term $\Phi(2\mathbf{w} + \mathbf{3})$ and using that $\Phi(\mathbf{1}) + \Phi(\mathbf{2}) = \Phi(\mathbf{3})$, we obtain that $A = \Phi(\mathbf{3}) + \Phi(\mathbf{w}) + \Phi(-2((\mathbf{w} + \mathbf{1}) \odot (\mathbf{w} + \mathbf{2}))) + \Phi(2\mathbf{w} + \mathbf{2}) + \Phi(2\mathbf{w} + \mathbf{1}) + \Phi(2\mathbf{w})$. By Proposition 19, we have that $\Phi(2\mathbf{w}) + \Phi(\mathbf{w}) = \Phi(3\mathbf{w}) + \Phi(-2(\mathbf{w} \odot 2\mathbf{w}))$, thus

$$\begin{aligned}A = \Phi(\mathbf{3}) + \Phi(3\mathbf{w}) + \Phi(2\mathbf{w} + \mathbf{2}) + \Phi(2\mathbf{w} + \mathbf{1}) + \\ + \Phi(-2(\mathbf{w} \odot 2\mathbf{w})) + \Phi(-2((\mathbf{w} + \mathbf{1}) \odot (\mathbf{w} + \mathbf{2}))).\end{aligned}$$

It easy to check that $\Phi(-2(\mathbf{w} \odot 2\mathbf{w})) + \Phi(-2((\mathbf{w} + \mathbf{1}) \odot (\mathbf{w} + \mathbf{2}))) = \Phi(4\mathbf{w})$. Finally, since $\Phi(-2((2\mathbf{w} + \mathbf{1}) \odot (2\mathbf{w} + \mathbf{2}))) = \mathbf{0}$, we have that $\Phi(2\mathbf{w} + \mathbf{2}) +$

$\Phi(2\mathbf{w}+\mathbf{1}) = \Phi(4\mathbf{w}+\mathbf{3}) = \Phi(4\mathbf{w}) + \Phi(\mathbf{3})$. Therefore, $A = \Phi(3\mathbf{w})$ and the result holds. $\mathcal{QED}$

Proposition 75. *Let t_1 be a positive integer. Then, rank*$(\Phi(\mathcal{H}^{t_1+1,0,0})) =$ *rank*$(\Phi(\mathcal{H}^{t_1,0,0})) + 4t_1 + 2\binom{t_1-1}{2} + 1 + \binom{t_1-1}{3}$.

Proof. By (3.1), the generator matrix of $\mathcal{H}' = \mathcal{H}^{t_1+1,0,0}$ is

$$A^{t_1+1,0,0} = \begin{pmatrix} A & A & A & A & A & A & A & A \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{7} \end{pmatrix},$$

where $A = A^{t_1,0,0}$ is the generator matrix of $\mathcal{H} = \mathcal{H}^{t_1,0,0}$. Note that $\mathcal{H}'$ can be seen as the union of eight cosets of the 8-fold replication code of $\mathcal{H}$, $(\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H})$, which are

$$\begin{array}{lllll}
C_0: & (\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H}) & & \\
C_1: & (\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H}) & + & (\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4},\mathbf{5},\mathbf{6},\mathbf{7}) \\
C_2: & (\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H}) & + & (\mathbf{0},\mathbf{2},\mathbf{4},\mathbf{6},\mathbf{0},\mathbf{2},\mathbf{4},\mathbf{6}) \\
C_3: & (\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H}) & + & (\mathbf{0},\mathbf{3},\mathbf{6},\mathbf{1},\mathbf{4},\mathbf{7},\mathbf{2},\mathbf{5}) \\
C_4: & (\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H}) & + & (\mathbf{0},\mathbf{4},\mathbf{0},\mathbf{4},\mathbf{0},\mathbf{4},\mathbf{0},\mathbf{4}) \\
C_5: & (\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H}) & + & (\mathbf{0},\mathbf{5},\mathbf{2},\mathbf{7},\mathbf{4},\mathbf{1},\mathbf{6},\mathbf{3}) \\
C_6: & (\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H}) & + & (\mathbf{0},\mathbf{6},\mathbf{4},\mathbf{2},\mathbf{0},\mathbf{6},\mathbf{4},\mathbf{2}) \\
C_7: & (\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H},\mathcal{H}) & + & (\mathbf{0},\mathbf{7},\mathbf{6},\mathbf{5},\mathbf{4},\mathbf{3},\mathbf{2},\mathbf{1}).
\end{array}$$

Note that $\mathrm{rank}(\Phi(C_0)) = \mathrm{rank}(\Phi(\mathcal{H})) = r$. Let $\{\Phi(\mathbf{g}_1),\ldots,\Phi(\mathbf{g}_r)\}$ be a basis of $\langle H\rangle$. Then, a basis of $\langle\Phi(C_0)\rangle$ is $\{\Phi(\mathbf{g}'_1),\ldots,\Phi(\mathbf{g}'_r)\}$, where $\mathbf{g}'_i = (\mathbf{g}_i,\mathbf{g}_i,\mathbf{g}_i,\mathbf{g}_i,\mathbf{g}_i,\mathbf{g}_i,\mathbf{g}_i,\mathbf{g}_i)$ for all $i\in\{1,\ldots,r\}$. Let $\mathbf{w}' = (\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4},\mathbf{5},\mathbf{6},\mathbf{7})$. By the proof of Proposition 67, we have that $\langle\Phi(C_0\cup C_2\cup C_4\cup C_6)\rangle = \langle\Phi(C_0\cup C_2\cup C_4)\rangle = \langle\Phi(\mathbf{g}'_1),\ldots,\Phi(\mathbf{g}'_r),\Phi(2\mathbf{w}'),\Phi(M')\rangle$, where M' is defined as in the mentioned proof using $2\mathbf{w}' = (\mathbf{0},\mathbf{2},\mathbf{4},\mathbf{6},\mathbf{0},\mathbf{2},\mathbf{4},\mathbf{6})$ instead of $\mathbf{v}' = (\mathbf{0},\mathbf{2},\mathbf{4},\mathbf{6})$.

Note that, if $\mathbf{u}'\in C_5$, then $\mathbf{u}' = (\mathbf{u},\mathbf{u}{+}\mathbf{5},\mathbf{u}{+}\mathbf{2},\mathbf{u}{+}\mathbf{7},\mathbf{u}{+}\mathbf{4},\mathbf{u}{+}\mathbf{1},\mathbf{u}{+}\mathbf{6},\mathbf{u}{+}\mathbf{3}) = (\mathbf{u},\mathbf{u},\mathbf{u},\mathbf{u},\mathbf{u},\mathbf{u},\mathbf{u},\mathbf{u}) + \mathbf{w}' + (\mathbf{0},\mathbf{4},\mathbf{0},\mathbf{4},\mathbf{0},\mathbf{4},\mathbf{0},\mathbf{4})$ with $\mathbf{u}\in\mathcal{H}$. Similarly, if $\mathbf{u}'\in C_7$, then $\mathbf{u}' = (\mathbf{u},\mathbf{u}+\mathbf{7},\mathbf{u}+\mathbf{6},\mathbf{u}+\mathbf{5},\mathbf{u}+\mathbf{4},\mathbf{u}+\mathbf{3},\mathbf{u}+\mathbf{2},\mathbf{u}+\mathbf{1}) = (\mathbf{u},\mathbf{u},\mathbf{u},\mathbf{u},\mathbf{u},\mathbf{u},\mathbf{u},\mathbf{u}) + 3\mathbf{w}' + (\mathbf{0},\mathbf{4},\mathbf{0},\mathbf{4},\mathbf{0},\mathbf{4},\mathbf{0},\mathbf{4})$ with $\mathbf{u}\in\mathcal{H}$. Thus, it is easy

to see that $\langle\Phi(C_0\cup C_1\cup C_2\cup C_3\cup C_4\cup C_5\cup C_7)\rangle = \langle\Phi(C_0\cup C_1\cup C_2\cup C_3\cup C_4)\rangle$, by Corollary 26. Now, we will find a base for $\langle\Phi(C_0\cup C_1\cup C_2\cup C_4)\rangle$ by extending the given base for $\langle\Phi(C_0 \cup C_2 \cup C_4)\rangle$. After that, we will see that $\langle\Phi(C_3)\rangle$ is linearly dependent of $\langle\Phi(C_0 \cup C_1 \cup C_2 \cup C_4)\rangle$.

Let $\mathcal{B}_2 = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_{t_1}, 2\mathbf{w}_1, \ldots, 2\mathbf{w}_{t_1}, 4\mathbf{w}_1, \ldots, 4\mathbf{w}_{t_1}\}$ be a 2-base of $\mathcal{H}$ and recall that $\mathrm{ord}(\mathbf{w}_i) = 8$ for all $i \in \{1, \ldots, t_1\}$. Let $\mathbf{u} \in \mathcal{H}$. We know that $\mathbf{u} = \sum_{i=1}^{3t_1} \lambda_i \mathbf{b}_i$, where $\mathbf{b}_i \in \mathcal{B}_2$ is the ith element of $\mathcal{B}_2$ and $\lambda_i \in \{0, 1\}$. Let $E = \{1 \leq i \leq 3t_1 : \lambda_i \neq 0\}$, $E_1 = \{1 \leq i \leq t_1 : i \in E\} \cup \{1 \leq i \leq t_1 : t_1 + i \in E\} \cup \{1 \leq i \leq t_1 : t_1 + i \in E\}$ as a multiset, and $E_4 = \{1 \leq i \leq t_1 : 2t_1 + i \in E\}$. Let $\mathbf{u}' = (\mathbf{u}, \mathbf{u}, \mathbf{u}, \mathbf{u}, \mathbf{u}, \mathbf{u}, \mathbf{u}, \mathbf{u})$ and $\mathbf{w}'_i = (\mathbf{w}_i, \mathbf{w}_i, \mathbf{w}_i, \mathbf{w}_i, \mathbf{w}_i, \mathbf{w}_i, \mathbf{w}_i, \mathbf{w}_i)$ for all $i \in \{1, \ldots, t_1\}$. Let $\mathbf{s}_i$ be the ith element of the ordered multiset $\{\mathbf{w}'_i : i \in E_1\}$. Now, we consider the element $\mathbf{u}'+\mathbf{w}' \in C_1$. By Corollary 26, $\Phi(\mathbf{u}'+\mathbf{w}') = \Phi(\sum_{i\in E_1} \mathbf{w}'_i+\mathbf{w}')+\sum_{i\in E_4} \Phi(4\mathbf{w}'_i)$.

Therefore, by Lemma 71, we have that $\Phi(\mathbf{u}' + \mathbf{w}') =$

$$
\begin{aligned}
= \;& \textstyle\sum_{i\in E_4} \Phi(4\mathbf{w}'_i) \\
& + \textstyle\sum_{i<j<k<p<q} \Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{s}_k + \mathbf{s}_p) + \sum_{i<j<k<q} \Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{s}_k + \mathbf{w}') \\
& + q_0\big(\textstyle\sum_{i<j<k<q} \Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{s}_k) + \sum_{i<j<q} \Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{w}')\big) \\
& + (q_0 + q_1)\big(\textstyle\sum_{i<j<q} \Phi(\mathbf{s}_i + \mathbf{s}_j) + \sum_{i<q} \Phi(\mathbf{s}_i + \mathbf{w}')\big) \\
& + q_0(q_0 + q_1)\big(\textstyle\sum_{i<q} \Phi(\mathbf{s}_i) + \Phi(\mathbf{w}')\big),
\end{aligned}
$$

where $q = |E_1| + 1$ and $[q_0, q_1, \ldots]_2$ is the binary expansion of q. We know that $\sum_{i\in E_4} \Phi(4\mathbf{w}'_i)$, $\Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{s}_k + \mathbf{s}_p)$, $\Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{s}_k)$, $\Phi(\mathbf{s}_i + \mathbf{s}_j)$, and $\Phi(\mathbf{s}_i)$ belong to $\langle\Phi(C_0)\rangle$.

We will see that $\Phi(\mathbf{u}'+\mathbf{w}')-\sum_{i\in E_4} \Phi(4\mathbf{w}'_i) \in \langle\Phi(C_0\cup C_2)\cup L_1\cup L_2\cup L_3\cup \{\Phi(\mathbf{w}')\}\rangle$, where $L_1 = \{\Phi(\mathbf{w}'_i+\mathbf{w}') : 1 \leq i \leq t_1\}\cup\{\Phi(2\mathbf{w}'_i+\mathbf{w}') : 1 \leq i \leq t_1\}$, $L_2 = \{\Phi(\mathbf{w}'_i + \mathbf{w}'_j + \mathbf{w}') : 2 \leq i < j \leq t_1\}$, and $L_3 = \{\Phi(\mathbf{w}'_i + \mathbf{w}'_j + \mathbf{w}'_k + \mathbf{w}') : 2 \leq i < j < k \leq t_1\}$. First, it is clear that $\Phi(\mathbf{s}_i + \mathbf{w}') \in L_1$. Now, we consider the terms of the form $A = \Phi(\mathbf{s}_i+\mathbf{s}_j+\mathbf{w}')$. If $A = \Phi(2\mathbf{w}'_i+\mathbf{w}')$, then $A \in L_1$; if $A = \Phi(\mathbf{1} + \mathbf{w}'_i + \mathbf{w}')$ with $2 \leq i \leq t_1$, then $A \in \langle\Phi(C_0 \cup C_2) \cup L_1\rangle$ by Lemma 73; and if $A = \Phi(\mathbf{w}'_i + \mathbf{w}'_j + \mathbf{w}')$ with $2 \leq i < j \leq t_1$, then $A \in L_2$. Next, we consider the terms of the form $B = \Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{s}_k + \mathbf{w}')$. If $B = \Phi(2\mathbf{w}'_i + \mathbf{w}' + \mathbf{w}'_k)$, then $B \in \langle\Phi(C_0 \cup C_2) \cup L_1 \cup \{\Phi(\mathbf{w}')\}\rangle$ by using

Lemma 72 and taking $\Phi(\mathbf{w}'_i + 2\mathbf{w}' + \mathbf{w}'_k) \in \Phi(C_2)$ as the other addend in the left-hand side of the equation of the lemma. If $B = \Phi(\mathbf{1} + \mathbf{w}'_i + \mathbf{w}'_j + \mathbf{w}')$ with $2 \leq i < j \leq t_1$, then $B \in \langle \Phi(C_0 \cup C_2) \cup L_1 \cup L_2 \cup \{\Phi(\mathbf{w}')\}\rangle$ by Lemma 73. Finally, if $B = \Phi(\mathbf{w}'_i + \mathbf{w}'_j + \mathbf{w}'_k + \mathbf{w}')$ with $2 \leq i < j < k \leq t_1$, then $B \in L_3$.

The elements of L_1, L_2 and L_3 are linearly independent from each other. Therefore, the elements of $L_1 \cup L_2 \cup L_3 \cup \{\Phi(\mathbf{w}')\}$ are linearly independent and $\mathrm{rank}(\langle L_1 \cup L_2 \cup L_3 \cup \{\Phi(\mathbf{w})\}\rangle) = 2t_1 + \binom{t_1-1}{2} + \binom{t_1-1}{3} + 1$. It is also easy to see that they are linearly independent from the elements in $\langle \Phi(C_0 \cup C_2 \cup C_4)\rangle$, so $rank(\langle \Phi(C_0 \cup C_1 \cup C_2 \cup C_4)\rangle) = r + 4t_1 + 2\binom{t_1-1}{2} + 1 + \binom{t_1-1}{3}$ by Proposition 67.

Finally, we will show that $\langle \Phi(C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4)\rangle = \langle \Phi(C_0 \cup C_1 \cup C_2 \cup C_4)\rangle$. We consider the element $\mathbf{u}' + 3\mathbf{w}' \in C_3$. By Corollary 26, $\Phi(\mathbf{u}' + 3\mathbf{w}') = \Phi(\sum_{i \in E_1} \mathbf{w}'_i + 3\mathbf{w}') + \sum_{i \in E_4} \Phi(4\mathbf{w}'_i)$. Therefore, by Lemma 71, we have that $\Phi(\mathbf{u}' + 3\mathbf{w}') =$

$$
\begin{aligned}
= \; & \textstyle\sum_{i \in E_4} \Phi(4\mathbf{w}'_i) \\
& + \textstyle\sum_{i<j<k<p \leq q-3} \Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{s}_k + \mathbf{s}_p) + \sum_{i<j<k \leq q-3} \Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{s}_k + \mathbf{w}') \\
& + \textstyle\sum_{i<j \leq q-3} \Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{w}' + \mathbf{w}') + \sum_{i \leq q-3} \Phi(\mathbf{s}_i + \mathbf{w}' + \mathbf{w}' + \mathbf{w}') \\
& + q_0\big(\textstyle\sum_{i<j<k \leq q-3} \Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{s}_k) + \sum_{i<j \leq q-3} \Phi(\mathbf{s}_i + \mathbf{s}_j + \mathbf{w}') \\
& + \textstyle\sum_{i \leq q-3} \Phi(\mathbf{s}_i + \mathbf{w}' + \mathbf{w}') + \Phi(\mathbf{w}' + \mathbf{w}' + \mathbf{w}')\big) \\
& + (q_0 + q_1)\big(\textstyle\sum_{i<j \leq q-3} \Phi(\mathbf{s}_i + \mathbf{s}_j) \; + \sum_{i \leq q-3} \Phi(\mathbf{s}_i + \mathbf{w}') + \Phi(\mathbf{w}' + \mathbf{w}')\big) \\
& + q_0(q_0 + q_1)\big(\textstyle\sum_{i \leq q-3} \Phi(\mathbf{s}_i) + \Phi(\mathbf{w}')\big),
\end{aligned}
$$

where $q = |E_1| + 3$. All the addends belong to $\langle \Phi(C_0 \cup C_1 \cup C_2 \cup C_4)\rangle$, except the ones of the form $\Phi(\mathbf{w}' + \mathbf{w}' + \mathbf{w}')$ and $\Phi(\mathbf{s}_i + \mathbf{w}' + \mathbf{w}' + \mathbf{w}')$. First, we have that $\Phi(3\mathbf{w}') \in \langle \Phi(C_0 \cup C_1 \cup C_2 \cup C_4)\rangle$ by Lemma 74. Finally, by using Lemma 72 with $\Phi(\mathbf{s}_i + 2\mathbf{w}' + \mathbf{w}')$ and $\Phi(2\mathbf{s}_i + \mathbf{w}' + \mathbf{w}') \in \Phi(C_2)$, we have that $\Phi(\mathbf{s}_i + \mathbf{w}' + \mathbf{w}' + \mathbf{w}') \in \langle \Phi(C_0 \cup C_1 \cup C_2 \cup C_4)\rangle$. Therefore, the result holds. $\mathcal{QED}$

Lemma 76. *Let $t, k \in \mathbb{N}$. Then,*

$$\sum_{i=1}^{t} \binom{i}{k} = \frac{(t+1-k)\binom{t+1}{k} + (k-1)\binom{1}{k}}{k+1}.$$

Proof. Straightforward by induction on the integer t. $\mathcal{QED}$

Corollary 77. *Let t_1 be a positive integer. Then,*

$$rank(\Phi(\mathcal{H}^{t_1,0,0})) = \frac{t_1^4}{24} - \frac{t_1^3}{12} + \frac{35t_1^2}{24} + \frac{7t_1}{12} + 1.$$

Proof. We know that $\text{rank}(\Phi(\mathcal{H}^{1,0,0})) = 3$. By applying Proposition 75 recursively, we have that

$$rank(\Phi(\mathcal{H}^{t_1,0,0})) = 3 + 4\sum_{i=1}^{t_1-1} i + 2\sum_{i=1}^{t_1-2}\binom{i}{2} + (t_1 - 1) + \sum_{i=1}^{t_1-2}\binom{i}{3}.$$

Finally, by Lemma 76, it is easy to see that the result holds. $\mathcal{QED}$

Corollary 78. *Let t_1 and t_2 be nonnegative integers with $t_1 \geq 1$. Then,*

$$rank(\Phi(\mathcal{H}^{t_1,t_2,0})) = rank(\Phi(\mathcal{H}^{t_1,0,0})) + \frac{t_2}{2}(t_1^2 + t_1 + t_2 + 1).$$

Proof. By applying Proposition 67 recursively, it is easy to see that

$$\text{rank}(\Phi(\mathcal{H}^{t_1,t_2,0})) = \text{rank}(\Phi(\mathcal{H}^{t_1,0,0})) + t_2\left(2t_1 + \binom{t_1-1}{2} + \frac{t_2-1}{2}\right).$$

Since $t_2(2t_1 + \binom{t_1-1}{2} + \frac{t_2-1}{2}) = \frac{t_2}{2}(t_1^2 + t_1 + t_2 + 1)$, the result follows. $\mathcal{QED}$

Theorem 79. *Let $\mathcal{H} = \mathcal{H}^{t_1,t_2,t_3}$ be a $\mathbb{Z}_8$-additive Hadamard code. Then,*

$$rank(\Phi(\mathcal{H})) = \frac{t_1^4}{24} - \frac{t_1^3}{12} + \frac{35t_1^2}{24} + \frac{7t_1}{12} + \frac{t_2}{2}(t_1^2 + t_1 + t_2 + 1) + t_3 + 1.$$

Proof. Straightforward from Proposition 60 and Corollaries 77 and 78. $\mathcal{QED}$

5.2 Classification of $\mathbb{Z}_8$-linear Hadamard codes

The classification of the $\mathbb{Z}_4$-linear Hadamard codes of length 2^t, for any $t \geq 3$, can be established by using either the rank or the dimension of the kernel [Kro01, PRV06]. In Chapter 4 it is shown that, in general, for $s > 2$, the

dimension of the kernel is not enough to establish a complete classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, for any $t \geq 3$. In this section, we show that for $s = 3$, a complete classification can be given by using both invariants: the dimension of the kernel and the rank, computed in Chapter 4 and the previous section, respectively.

First, recall that the dimension of the kernel for $\mathbb{Z}_8$-linear Hadamard codes is given by the following proposition that is, Theorem 46 for $s = 3$:

Proposition 80. *Let $\mathcal{H} = \mathcal{H}^{t_1,t_2,t_3}$ be a $\mathbb{Z}_8$-additive Hadamard code. If $\Phi(\mathcal{H})$ is nonlinear, then $\ker(\Phi(\mathcal{H})) = t_1 + t_2 + t_3 + \sigma_{t_1}$, where $\sigma_{t_1} = 1$ if $t_1 \geq 2$ and $\sigma_{t_1} = 2$ if $t_1 = 1$.*

In Chapter 4, it is also shown that, in order to obtain a complete classification of nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, it is enough to focus on $t \geq 5$, since all $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t are linear for $t < 5$. It is also mentioned in Chapter 4 that, at least for any $3 \leq t \leq 11$, these codes can be fully classified by using only the values of the rank. This pointed out that, maybe, it was possible to obtain a complete classification for any $t \geq 5$ by using just this invariant. However, the following example shows that both invariants, the rank and the dimension of the kernel, are necessary in some cases.

Example 81. *Consider the $\mathbb{Z}_8$-linear Hadamard codes of length $2^{17} = 131072$, ($t = 17$), $H^{2,6,0}$ and $H^{4,1,4}$. By Theorem 79, we have that rank$(H^{2,6,0}) =$ rank$(H^{4,1,4}) = 47$. However, since ker$(H^{2,6,0}) = 9$ and ker$(H^{4,1,4}) = 10$ by Proposition 80, they are not equivalent even though they have the same rank. The rest of 23 nonlinear such codes of length 2^{17} have a different rank, so we have that there are exactly 26 nonequivalent $\mathbb{Z}_8$-linear Hadamard codes of length 2^{17}.*

Although we cannot completely classify the $\mathbb{Z}_8$-linear Hadamard codes by using only the rank, the following result shows that if two such nonlinear codes have the same dimension of the kernel, then their values of the rank are different.

Theorem 82. *Let $5 \leq t \in \mathbb{Z}$. Then, for every pair, H^{t_1,t_2,t_3} and $H^{t'_1,t'_2,t'_3}$, of nonlinear $\mathbb{Z}_8$-linear Hadamard codes of length 2^t with $(n; t_1, t_2, t_3) \neq (n; t'_1, t'_2, t'_3)$ and $ker(H^{t_1,t_2,t_3}) = ker(H^{t'_1,t'_2,t'_3})$, we have that $rank(H^{t_1,t_2,t_3}) \neq rank(H^{t'_1,t'_2,t'_3})$.*

Proof. Let $k = \ker(H^{t_1,t_2,t_3}) = \ker(H^{t'_1,t'_2,t'_3})$. By Proposition 80, we have that $k = t_1 + t_2 + t_3 + \sigma_{t_1}$. Moreover,

$$\left.\begin{array}{rcl} t_1 + t_2 + t_3 + \sigma_{t_1} & = & k \\ 3t_1 + 2t_2 + t_3 & = & t + 1 \end{array}\right\} \Longleftrightarrow \left\{\begin{array}{rcl} t_2 & = & \sigma_{t_1} - k + t + 1 - 2t_1 \\ t_3 & = & t_1 + 2k - 2\sigma_{t_1} - t - 1. \end{array}\right. \tag{5.19}$$

By replacing the formulas in (5.19) into the expression of the rank, given by Theorem 79, we have that

$$\begin{aligned} \operatorname{rank}(H^{t_1,t_2,t_3}) = {} & \frac{t_1^4}{24} - \frac{t_1^3}{12} + \frac{35t_1^2}{24} + \frac{7t_1}{12} + \\ & + \frac{1}{2}(\sigma_{t_1} - k + t + 1 - 2t_1)(t_1^2 + t_1 + \sigma_{t_1} - k + t + 1 - 2t_1 + 1) + \\ & + t_1 + 2k - 2\sigma_{t_1} - t - 1 + 1. \end{aligned}$$

Since the above expression does not depend on t_2 and t_3, we will write $\operatorname{rank}(t_1, t, k)$ instead of $\operatorname{rank}(H^{t_1,t_2,t_3})$. Moreover, we have that this expression is equal to

$$\begin{aligned} \operatorname{rank}(t_1, t, k) = {} & \frac{t_1^4}{24} - \frac{13}{12}t_1^3 + (\frac{71}{24} + \frac{1}{2}(t - k + \sigma_{t_1}))t_1^2 - \\ & - (\frac{11}{12} + \frac{3}{2}(t - k + \sigma_{t_1}))t_1 + \frac{1}{2}((t - k + \sigma_{t_1})^2 + t + k - \sigma_{t_1} + 2). \end{aligned}$$

Now, we suppose that $\operatorname{rank}(H^{t_1,t_2,t_3}) = \operatorname{rank}(H^{t'_1,t'_2,t'_3})$ for $(n; t_1, t_2, t_3) \neq (n; t'_1, t'_2, t'_3)$ or, equivalently, $\operatorname{rank}(t_1, t, k) = \operatorname{rank}(t'_1, t, k)$ for $t_1 \neq t'_1$. Without loss of generality, we can assume that $t'_1 < t_1$. Note that if $t'_1 = t_1$, then $t_2 = t'_2$ and $t_3 = t'_3$, so both codes are equal.

First, we consider that $2 \leq t'_1 < t_1$. In this case, we have to see that $\operatorname{rank}(t_1, t, k) - \operatorname{rank}(t'_1, t, k) \neq 0$. Since $t_1, t'_1 \geq 2$, $\sigma_{t_1} = \sigma_{t'_1} = 1$ and we have

that

$$\begin{aligned}\operatorname{rank}(t_1,t,k)-\operatorname{rank}(t_1',t,k)=&\\ \frac{t_1^4}{24}-\frac{13}{12}t_1^3+(\frac{71}{24}+\frac{1}{2}(t-k+1))t_1^2-(\frac{11}{12}+\frac{3}{2}(t-k+1))t_1+&\\ -\frac{t_1'^4}{24}+\frac{13}{12}t_1'^3-(\frac{71}{24}+\frac{1}{2}(t-k+1))t_1'^2+(\frac{11}{12}+\frac{3}{2}(t-k+1))t_1'.&\end{aligned}$$

By using the identity $x^2-y^2=(x+y)(x-y)$, we have that

$$\begin{aligned}&\operatorname{rank}(t_1,t,k)-\operatorname{rank}(t_1',t,k)=\\ &\frac{1}{24}\big[(t_1+t_1')(t_1^2+t_1'^2)-26(t_1^2+t_1t_1'+t_1'^2)+(t_1+t_1')(83+12(t-k))-58-36(t-k)\big]=\\ &\qquad\frac{1}{24}\big[(t_1+t_1')(t_1^2+t_1'^2+83)-26(t_1^2+t_1t_1'+t_1'^2)-58\\ &\qquad\qquad+12(t-k)(t_1+t_1'-3)\big],\quad(5.20)\end{aligned}$$

which can be written as $\operatorname{rank}(t_1,t,k)-\operatorname{rank}(t_1',t,k)=f(t_1,t_1')+(t-k)g(t_1,t_1')$, where $f(t_1,t_1')=1/24\big[(t_1+t_1')(t_1^2+t_1'^2+83)-26(t_1^2+t_1t_1'+t_1'^2)-58\big]$ and $g(t_1,t_1')=1/2(t_1+t_1'-3)$. Note that $(t-k)g(t_1,t_1')\geq 0$ for all integer pairs $(t_1,t_1')\in D$, where $D=\{(t_1,t_1'):2\leq t_1'<t_1\}$. It is easy to see that $f(t_1,t_1')>0$ for all $t_1'\geq 26$, since we can rewrite this expression in the following form:

$$t_1^2(t_1+t_1')+t_1'^2(t_1+t_1')+83(t_1+t_1')>26t_1^2+26t_1'(t_1+t_1')-58,\quad(5.21)$$

and we can observe that $t_1^2(t_1+t_1')>26t_1^2$, $t_1'^2(t_1+t_1')\geq 26t_1'(t_1+t_1')$ and $83(t_1+t_1')>-58$. Similarly, $f(t_1,t_1')>0$ for all $t_1\geq 26$, considering the left-hand side of (5.21) as $26t_1(t_1+t_1')+26t_1'^2-58$. Therefore, if there exists a pair of integers (t_1,t_1') such that $\operatorname{rank}(t_1,t,k)-\operatorname{rank}(t_1',t,k)=0$, this pair has to be in $R=\{(t_1,t_1'):2\leq t_1'<t_1,t_1'<26,t_1<26\}\subset D$. There are $1+2+\cdots+23=276$ pairs $(t_1,t_1')\in R$, and it can be checked that any of them is a solution of the equation.

Finally, we consider that $1=t_1'<t_1$. In this case, we have to prove that $\operatorname{rank}(t_1,t,k)-\operatorname{rank}(t_1',t,k)\neq 0$. Then, since $t_1\geq 2$ and $t_1'=1$, $\sigma_{t_1}=1$,

$\sigma_{t_1'} = 2$, and we obtain that

$$\begin{aligned}\operatorname{rank}(t_1,t,k) - \operatorname{rank}(1,t,k) = \\ \frac{t_1^4}{24} - \frac{13}{12}t_1^3 + (\frac{71}{24} + \frac{1}{2}(t-k+1))t_1^2 - (\frac{11}{12} + \frac{3}{2}(t-k+1))t_1 + \\ + \frac{1}{2}((t-k+1)^2 + t + k + 1) - \\ -\frac{1}{24} + \frac{13}{12} - \frac{71}{24} - \frac{1}{2}(t-k+2) + \frac{11}{12} + \frac{3}{2}(t-k+2) - \frac{1}{2}((t-k+2)^2 + t + k).\end{aligned}$$

By simplifying, we have that

$$\operatorname{rank}(t_1,t,k) - \operatorname{rank}(1,t,k) = \frac{1}{24}\left[t_1^4 - 26t_1^3 + 83t_1^2 - 58t_1 + 12(t-k)(t_1^2 - 3t_1)\right].$$

Let $f(t_1,t,k) = \operatorname{rank}(t_1,t,k) - \operatorname{rank}(1,t,k)$. We know that $t - k = 2t_1 + t_2 - 2 \geq 2t_1 - 2$. Since $12(t-k)(t_1^2 - 3t_1) \geq 0$ for $t_1 \geq 3$, we have that $f(t_1,t,k) \geq g(t_1) = \frac{1}{24}[t_1^4 - 26t_1^3 + 83t_1^2 - 58t_1 + 12(2t_1 - 2)(t_1^2 - 3t_1)] = \frac{1}{24}[t_1(t_1^3 - 2t_1^2 - 13t_1 + 14)]$. By computing the zeros of the polynomial $g(t_1)$ and analyzing its behavior, we have that $f(t_1,t,k) \geq g(t_1) > 0$ for $t_1 \geq 5$. Therefore, we just need to compute $f(t_1,t,k)$ when $t_1 \in \{2,3,4\}$. For these cases, we have that

$$\begin{aligned} f(2,t,k) &= 1 - (t-k) &&= 0 \;\Leftrightarrow\; t - k = 1 \\ f(3,t,k) &= -2 \\ f(4,t,k) &= 2(t-k) - 13 &&= 0 \;\Leftrightarrow\; t - k = 13/2. \end{aligned}$$

Note that if $t_1 = 2$, then $t - k = t_2 + 2 \geq 2$, so $t - k \neq 1$. Therefore, for $t_1 \in \{2,3,4\}$, $f(t_1,t,k) \neq 0$ and the result holds. $\mathcal{QED}$

Recall that it is already known that there are $\lfloor \frac{t-1}{2} \rfloor$ nonequivalent $\mathbb{Z}_4$-linear Hadamard codes of length 2^t, $t \geq 3$ [Kro01]. Now, we establish how many nonequivalent $\mathbb{Z}_8$-linear Hadamard codes of length 2^t there are, once the length 2^t if fixed, for $t \geq 5$. In Chapter 4, some upper and lower bounds are given for certain values of t. By Theorems 79 and 82, we know that if H^{t_1,t_2,t_3} and $H^{t_1',t_2',t_3'}$ are nonlinear $\mathbb{Z}_8$-linear Hadamard codes of the same

length with $(t_1, t_2, t_3) \neq (t_1', t_2', t_3')$, then their corresponding pairs, (r, k), where r is the rank and k is the dimension of the kernel, are different. Then, we have the following result:

Theorem 83. *Let $\mathcal{A}_{t,3}$ be the number of nonequivalent $\mathbb{Z}_8$-linear Hadamard codes of length 2^t. Then, for any $t \geq 5$,*

$$\mathcal{A}_{t,3} = \left\lfloor \frac{t+1}{3} \right\rfloor + \sum_{i=1}^{\lfloor (t+1)/3 \rfloor} \left\lfloor \frac{t+1-3i}{2} \right\rfloor - 1.$$

Proof. An upper bound is given, by Theorem 52, for the amount of different nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes for any $t \geq 3$ and $2 \leq s \leq t-1$. In particular, when $s = 3$, we have the following bound:

$$\mathcal{A}_{t,3} \leq |\{(t_1, t_2, t_3) \in \mathbb{N}^3 : t = 3t_1 + 2t_2 + t_3 - 1,\ t_1 \geq 1\}| - 1. \tag{5.22}$$

By Theorems 79 and 82, we know that this bound is tight. Therefore, we just have to see that

$$|\{(t_1, t_2, t_3) \in \mathbb{N}^3 : t = 3t_1+2t_2+t_3-1,\ t_1 \geq 1\}| = \left\lfloor \frac{t+1}{3} \right\rfloor + \sum_{i=1}^{\lfloor (t+1)/3 \rfloor} \left\lfloor \frac{t+1-3i}{2} \right\rfloor.$$

This means that we need to compute the amount of different solutions, (t_1, t_2, t_3), of the equation $t = 3t_1 + 2t_2 + t_3 - 1$ with $t_1 \geq 1$.

It is easy to see that $1 \leq t_1 \leq \left\lfloor \frac{t+1}{3} \right\rfloor$. Once the value of t_1 is fixed, we can see that t_2 is bounded by $0 \leq t_2 \leq \left\lfloor \frac{t+1-3t_1}{2} \right\rfloor$. Note that, once t_1 and t_2 are fixed, there is a unique value for t_3. Then, the amount of different solutions of $t = 3t_1 + 2t_2 + t_3 - 1$ with $t_1 \geq 1$, or equivalently $|\{(t_1, t_2, t_3) \in \mathbb{N}^3 : t = 3t_1 + 2t_2 + t_3 - 1,\ t_1 \geq 1\}|$, is

$$\sum_{i=1}^{\lfloor (t+1)/3 \rfloor} \left(\left\lfloor \frac{t+1-3i}{2} \right\rfloor + 1 \right) = \left\lfloor \frac{t+1}{3} \right\rfloor + \sum_{i=1}^{\lfloor (t+1)/3 \rfloor} \left\lfloor \frac{t+1-3i}{2} \right\rfloor,$$

so the result holds. $\mathcal{QED}$

5.3 Equivalences among $\mathbb{Z}_4$-linear and $\mathbb{Z}_8$-linear Hadamard codes

Next, we show that there are $\mathbb{Z}_8$-linear Hadamard codes which are equivalent to a $\mathbb{Z}_4$-linear Hadamard code. Actually, we will see that these codes coincide with the ones that have the same invariants, rank and dimension of the kernel. Table 5.1 shows the type, rank, and dimension of the kernel for all $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, with $s \in \{2,3\}$ and $6 \leq t \leq 9$, where the types of the ones having the same invariants are unified.

From now on, in order to avoid any confusion, let $\Phi_4 : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ and $\Phi_8 : \mathbb{Z}_8^n \to \mathbb{Z}_2^{4n}$ be the Gray maps over $\mathbb{Z}_4$ and $\mathbb{Z}_8$, respectively. Let $\gamma = (2,3) \in \mathcal{S}_4$. Then, for $n = 1$ we have that

$$\begin{array}{rcll}
\Phi_8((0)) & = & (0,0,0,0) & = \quad \gamma((0,0,0,0)) = \gamma(\Phi_4((0,0))) \\
\Phi_8((1)) & = & (0,1,0,1) & = \quad \gamma((0,0,1,1)) = \gamma(\Phi_4((0,2))) \\
\Phi_8((2)) & = & (0,0,1,1) & = \quad \gamma((0,1,0,1)) = \gamma(\Phi_4((1,1))) \\
\Phi_8((3)) & = & (0,1,1,0) & = \quad \gamma((0,1,1,0)) = \gamma(\Phi_4((1,3))) \\
\Phi_8((4)) & = & (1,1,1,1) & = \quad \gamma((1,1,1,1)) = \gamma(\Phi_4((2,2))) \\
\Phi_8((5)) & = & (1,0,1,0) & = \quad \gamma((1,1,0,0)) = \gamma(\Phi_4((2,0))) \\
\Phi_8((6)) & = & (1,1,0,0) & = \quad \gamma((1,0,1,0)) = \gamma(\Phi_4((3,3))) \\
\Phi_8((7)) & = & (1,0,0,1) & = \quad \gamma((1,0,0,1)) = \gamma(\Phi_4((3,1))).
\end{array} \tag{5.23}$$

We can define the function $\tau : \mathbb{Z}_8 \to \mathbb{Z}_4^2$ given by

$$\tau(u) = \Phi_4^{-1}(\gamma^{-1}(\Phi_8(u))), \tag{5.24}$$

for $u \in \mathbb{Z}_8$. Note that, for $u \in \{0,1,2,3\}$, we have that $\tau(2u) = (u,u)$ and $\tau(4u) = 2(u,u)$. Moreover, we have the following result:

Lemma 84. *Let $u_i \in \{0,2,4,6\}$ for $i \in \{2,\ldots,n\}$ and $u_1 \in \mathbb{Z}_8$. Then,*

$$\tau(\sum_{i=1}^{n} u_i) = \sum_{i=1}^{n} \tau(u_i). \tag{5.25}$$

Proof. Let $u_i = 2v_i$, $v_i \in \{0,1,2,3\}$ for $i \in \{2,\ldots,n\}$ and $v_1 = \lambda + 2v_1$

for $\lambda \in \{0,1\}$, $v_1 \in \{0,1,2,3\}$. By (5.23) it is easy to see that $\tau(\lambda + 2v_1) = \tau(\lambda) + \tau(2v_1)$. Then, $\sum_{i=1}^{n} \tau(u_i) = \tau(\lambda) + \sum_{i=1}^{n} \tau(2v_i) = \lambda(0,2) + \sum_{i=1}^{n}(v_i, v_i) = \lambda(0,2) + (\sum_{i=1}^{n} v_i, \sum_{i=1}^{n} v_i) = \tau(\lambda) + \tau(2\sum_{i=1}^{n} v_i) = \tau(\lambda + 2\sum_{i=1}^{n} v_i) = \tau(\sum_{i=1}^{n} u_i)$.

$\mathcal{QED}$

Corollary 85. *Let $u_i \in \{0,2,4,6\}$ for $i \in \{2,\ldots,n\}$ and $u_1 \in \mathbb{Z}_8$. Then,*

$$\Phi_8(\sum_{i=1}^{n} u_i) = \gamma(\Phi_4(\sum_{i=1}^{n} \tau(u_i))). \tag{5.26}$$

Proof. Straightforward from Lemma 84. $\mathcal{QED}$

Note that Corollary 85 also works for codewords such that $\mathrm{ord}(\mathbf{u}_1) \leq 8$ and $\mathrm{ord}(\mathbf{u}_i) \leq 4$ for $i \in \{2,\ldots,n\}$.

	$t=7$		$t=8$		$t=9$	
	type	(r,k)	type	(r,k)	type	(r,k)
$\mathbb{Z}_4$	$(1,6)$	(8,8)	$(1,7)$	(9,9)	$(1,8)$	(10,10)
	$(2,4)$	(8,8)	$(2,5)$	(9,9)	$(2,6)$	(10,10)
	$(4,0)$	(11,5)			$(5,0)$	(16,6)
$\mathbb{Z}_4$	$(3,2)$	(9,6)	$(3,3)$	(10,7)	$(3,4)$	(11,8)
	$(1,2,1)$		$(1,2,2)$		$(1,2,3)$	
$\mathbb{Z}_8$			$(4,1)$	(12,6)	$(4,2)$	(13,7)
			$(1,3,0)$		$(1,3,1)$	
$\mathbb{Z}_8$	$(1,0,5)$	(8,8)	$(1,0,6)$	(9,9)	$(1,0,7)$	(10,10)
	$(1,1,3)$	(8,8)	$(1,1,4)$	(9,9)	$(1,1,5)$	(10,10)
	$(2,0,2)$	(10,5)	$(2,0,3)$	(11,6)	$(2,0,4)$	(12,7)
	$(2,1,0)$	(12,4)	$(2,1,1)$	(13,5)	$(2,1,2)$	(14,6)
			$(3,0,0)$	(17,4)	$(2,2,0)$	(17,5)
					$(3,0,1)$	(18,5)

Table 5.1: Type, rank and kernel of all $\mathbb{Z}_4$-linear and $\mathbb{Z}_8$-linear Hadamard codes of length 2^t.

Now, we component-wise extend τ in (5.24) to $\tau : \mathbb{Z}_8^n \to \mathbb{Z}_4^{2n}$ and define

$\tilde{\tau} = \rho^{-1} \circ \tau$, where $\rho \in \mathcal{S}_{2n}$ is defined as

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & n & n+1 & \dots & n+i & \dots & 2n \\ 1 & 3 & \dots & 2i-1 & \dots & 2n-1 & 2 & \dots & 2i & \dots & 2n \end{pmatrix}. \quad (5.27)$$

If $\mathbf{u} = (u_1, u_2, \dots, u_n) \in \mathbb{Z}_8^n$ and $\tau(u_i) = (u_i^1, u_i^2)$ for all $i \in \{1, \dots, n\}$, then $\tau(\mathbf{u}) = (u_1^1, u_1^2, u_2^1, u_2^2, \dots, u_n^1, u_n^2)$ and $\tilde{\tau}(\mathbf{u}) = (u_1^1, \dots, u_n^1, u_1^2, \dots, u_n^2)$.

Let $\bar{\mathbf{w}}_i$ and $\mathbf{w}_i$ be the ith row of A^{t_1,t_2} and $A^{t_1,t_2,0}$, respectively, $1 \le i \le t_1$; and $\bar{\mathbf{v}}_j$ and $\mathbf{v}_j$ be the (t_1+j)th row of A^{t_1,t_2} and $A^{t_1,t_2,0}$, respectively, $1 \le j \le t_2$. Note that $\bar{\mathbf{w}}_1 = \mathbf{1}$ and $\mathbf{w}_1 = \mathbf{1}$ by construction and, for $1 \le i \le t_1$, $1 \le j \le t_2$, we have that $\mathbf{w}_i$ is a codeword of order 8, $\bar{\mathbf{w}}_i$ and $\mathbf{v}_j$ are codewords of order 4, and $\bar{\mathbf{v}}_j$ is a codeword of order 2.

Lemma 86. *Let $\mathbf{w}_1$, $\mathbf{v}_1, \dots, \mathbf{v}_{t_1-1}$ be the rows of $A^{1,t_1-1,0}$ and $\bar{\mathbf{w}}_1, \dots, \bar{\mathbf{w}}_{t_1}, \bar{\mathbf{v}}_1$ the rows of $A^{t_1,1}$. Then,*

(i) $\tilde{\tau}(\mathbf{w}_1) = \bar{\mathbf{v}}_1$, $\tilde{\tau}(2\mathbf{w}_1) = \bar{\mathbf{w}}_1$, $\tilde{\tau}(4\mathbf{w}_1) = 2\bar{\mathbf{w}}_1$,

(ii) $\tilde{\tau}(\mathbf{v}_i) = \bar{\mathbf{w}}_{i+1}$ and $\tilde{\tau}(2\mathbf{v}_i) = 2\bar{\mathbf{w}}_{i+1}$, $1 \le i \le t_1 - 1$.

Proof. First, we have that $\tilde{\tau}(\mathbf{w}_1) = \tilde{\tau}(\mathbf{1}) = (\mathbf{0}, \mathbf{2}) = \bar{\mathbf{v}}_1$, $\tilde{\tau}(2\mathbf{w}_1) = \tilde{\tau}(\mathbf{2}) = (\mathbf{1}, \mathbf{1}) = \bar{\mathbf{w}}_1$ and $\tilde{\tau}(4\mathbf{w}_1) = \tilde{\tau}(\mathbf{4}) = (\mathbf{2}, \mathbf{2}) = 2\bar{\mathbf{w}}_1$.

Note that if $\mathbf{u} = (u_1, \dots, u_n) \in \mathbb{Z}_8^n$, with $u_i \in \{0, 1, 2, 3\}$ for all $i \in \{1, \dots, n\}$, then $\tilde{\tau}(2\mathbf{u}) = (\mathbf{u}, \mathbf{u})$ and $\tilde{\tau}(4\mathbf{u}) = 2(\mathbf{u}, \mathbf{u})$. Let $\mathbf{v}_i^*$ be the vector whose coordinates are in $\{0, 1, 2, 3\}$ and $2\mathbf{v}_i^* = \mathbf{v}_i$, for all $i \in \{1, \dots, t_1 - 1\}$. Note that $\bar{\mathbf{w}}_{i+1} = (\mathbf{v}_i^*, \mathbf{v}_i^*)$ by construction. Therefore, $\tilde{\tau}(\mathbf{v}_i) = \tilde{\tau}(2\mathbf{v}_i^*) = (\mathbf{v}_i^*, \mathbf{v}_i^*) = \bar{\mathbf{w}}_{i+1}$ and $\tilde{\tau}(2\mathbf{v}_i) = \tilde{\tau}(4\mathbf{v}_i^*) = 2(\mathbf{v}_i^*, \mathbf{v}_i^*) = 2\bar{\mathbf{w}}_{i+1}$. $\mathcal{QED}$

Proposition 87. *Let $t_1 \in \mathbb{Z}$, with $t_1 \ge 1$. Then, the Hadamard codes $H^{t_1,1}$ and $H^{1,t_1-1,0}$ are permutation equivalent.*

Proof. Let $\mathcal{H}^{t_1,1}$ be the $\mathbb{Z}_4$-additive code such that $H^{t_1,1} = \Phi_4(\mathcal{H}^{t_1,1})$ and $\mathcal{H}^{1,t_1-1,0}$ be the $\mathbb{Z}_8$-additive code such that $H^{1,t_1-1,0} = \Phi_8(\mathcal{H}^{1,t_1-1,0})$. Since $H^{t_1,1}$ and $H^{1,t_1-1,0}$ have both length 2^t, where $t = 2t_1$, the length of $\mathcal{H}^{t_1,1}$ and $\mathcal{H}^{1,t_1-1,0}$ are 2^{t-1} and 2^{t-2}, respectively.

Let $\mathbf{w}_1$, $\mathbf{v}_1, \dots, \mathbf{v}_{t_1-1}$ be the rows of $A^{1,t_1-1,0}$ and $\bar{\mathbf{w}}_1, \dots, \bar{\mathbf{w}}_{t_1}, \bar{\mathbf{v}}_1$ the rows of $A^{t_1,1}$. If we consider $\mathcal{B}_8 = \{\mathbf{b}_1^8, \dots, \mathbf{b}_{2t_1+1}^8\} = \{\mathbf{w}_1, 2\mathbf{w}_1, 4\mathbf{w}_1, \mathbf{v}_1, \dots, \mathbf{v}_{t_1-1},$

$2\mathbf{v}_1, \ldots, 2\mathbf{v}_{t_1-1}\}$ the 2-base of $\mathcal{H}^{1,t_1-1,0}$ and $\mathcal{B}_4 = \{\mathbf{b}_1^4, \ldots, \mathbf{b}_{2t_1+1}^4\} = \{\bar{\mathbf{v}}_1, \bar{\mathbf{w}}_1, 2\bar{\mathbf{w}}_1, \bar{\mathbf{w}}_2, \ldots, \bar{\mathbf{w}}_{t_1}, 2\bar{\mathbf{w}}_2, \ldots, 2\bar{\mathbf{w}}_{t_1}\}$ the 2-base of $\mathcal{H}^{t_1,1}$, then we have that $\tilde{\tau}(\mathbf{b}_i^8) = \mathbf{b}_i^4$ for $1 \leq i \leq 2t_1 + 1$ by Lemma 86.

Let $\tilde{\rho} \in \mathcal{S}_{2^t}$ be a permutation such that $\Phi_4 \circ \rho = \tilde{\rho} \circ \Phi_4$, where ρ is defined as in (6.1). Let $\gamma = \Pi_{i=0}^{2^{t-2}-1}(4i+2\,, 4i+3) \in \mathcal{S}_{2^t}$, i.e., the permutation that permute the two coordinates in the middle of each block of four coordinates. Then, by (5.24), $\Phi_8(\mathbf{b}_i^8) = \gamma(\Phi_4(\tau(\mathbf{b}_i^8))) = \gamma(\Phi_4(\rho(\tilde{\tau}(\mathbf{b}_i^8)))) = \gamma(\tilde{\rho}(\Phi_4(\mathbf{b}_i^4))) = (\gamma \circ \tilde{\rho})(\Phi_4(\mathbf{b}_i^4))$.

Now, let $\mathbf{w} = \sum_{i=1}^{2t_1+1} \lambda_i \mathbf{b}_i^8$ be a codeword of $\mathcal{H}^{1,t_1-1,0}$, where $\lambda_i \in \{0,1\}$. Then, by Corollary 85, we have that

$$\Phi_8(\mathbf{w}) = \Phi_8(\sum_{i=1}^{2t_1+1} \lambda_i \mathbf{b}_i^8) = (\gamma \circ \tilde{\rho})(\Phi_4(\sum_{i=1}^{2t_1+1} \lambda_i \mathbf{b}_i^4))).$$

Since $\sum_{i=1}^{2t_1+1} \lambda_i \mathbf{b}_i^4 \in \mathcal{H}^{t_1,1}$, we have that the result holds. $\mathcal{QED}$

Example 88. *Let $\mathcal{H}^{1,1,0}$ be the $\mathbb{Z}_8$-additive Hadamard code, which is generated by*

$$A^{1,1,0} = \begin{pmatrix} 1111 \\ 0246 \end{pmatrix},$$

and $\mathcal{H}^{2,1}$ be the $\mathbb{Z}_4$-additive Hadamard code, which is generated by

$$A^{2,1} = \begin{pmatrix} 1111 & 1111 \\ 0123 & 0123 \\ 0000 & 2222 \end{pmatrix}.$$

Let $\mathbf{w}_1, \mathbf{v}_1$ be the rows of $A^{1,1,0}$ and $\bar{\mathbf{w}}_1, \bar{\mathbf{w}}_2, \bar{\mathbf{v}}_1$ be the rows of $A^{2,1}$. The set $\mathcal{B}_8 = \{\mathbf{b}_1^8, \ldots, \mathbf{b}_5^8\} = \{\mathbf{w}_1, 2\mathbf{w}_1, 4\mathbf{w}_1, \mathbf{v}_1, 2\mathbf{v}_1\}$ is a 2-base of $\mathcal{H}^{1,1,0}$ and $\mathcal{B}_4 = \{\mathbf{b}_1^4, \ldots, \mathbf{b}_5^4\} = \{\bar{\mathbf{v}}_1, \bar{\mathbf{w}}_1, 2\bar{\mathbf{w}}_1, \bar{\mathbf{w}}_2, 2\bar{\mathbf{w}}_2\}$ a 2-base of $\mathcal{H}^{2,1}$. Let $\gamma = (2,3)(6,7)(10,11)(14,15) \in \mathcal{S}_{16}$. Let

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 5 & 7 & 2 & 4 & 6 & 8 \end{pmatrix} \in \mathcal{S}_8,$$

so $\rho((u_1^1, \ldots, u_4^1, u_1^2, \ldots, u_4^2)) = (u_1^1, u_1^2, u_2^1, u_2^2, \ldots, u_4^1, u_4^2)$, and $\tilde{\rho} \in \mathcal{S}_{16}$ such

that $\Phi_4 \circ \rho = \tilde{\rho} \circ \Phi_4$. *We have that* $\Phi_8(\sum_{i=1}^{5} \lambda_i \mathbf{b}_i^8) = \gamma \circ \tilde{\rho} \circ \Phi_4(\sum_{i=1}^{5} \lambda_i \mathbf{b}_i^4) = \gamma \circ \Phi_4(\rho(\sum_{i=1}^{5} \lambda_i \mathbf{b}_i^4))$, $\lambda_i \in \{0,1\}$. *Actually, for the elements of the 2-base, we have that*

$$\begin{gathered}
\Phi_8(\mathbf{w}_1) = \Phi_8(1111) = \gamma(\Phi_4(\rho(\bar{\mathbf{v}}_1))) = \gamma(\Phi_4(02020202)) \\
\Phi_8(2\mathbf{w}_1) = \Phi_8(2222) = \gamma(\Phi_4(\rho(\bar{\mathbf{w}}_1))) = \gamma(\Phi_4(11111111)) \\
\Phi_8(4\mathbf{w}_1) = \Phi_8(4444) = \gamma(\Phi_4(\rho(2\bar{\mathbf{w}}_1))) = \gamma(\Phi_4(22222222)) \\
\Phi_8(\mathbf{v}_1) = \Phi_8(0246) = \gamma(\Phi_4(\rho(\bar{\mathbf{w}}_2))) = \gamma(\Phi_4(00112233)) \\
\Phi_8(2\mathbf{v}_1) = \Phi_8(0404) = \gamma(\Phi_4(\rho(2\bar{\mathbf{w}}_2))) = \gamma(\Phi_4(00220022)).
\end{gathered}$$

Therefore, the codes $H^{2,1} = \Phi_4(\mathcal{H}^{2,1})$ *and* $H^{1,1,0} = \Phi_8(\mathcal{H}^{1,1,0})$ *of length* 16 *are permutation equivalent.*

Example 89. *Let* $\mathcal{H}^{1,2,0}$ *be the* $\mathbb{Z}_8$*-additive Hadamard code, which is generated by*

$$A^{1,2,0} = \begin{pmatrix} 1111 & 1111 & 1111 & 1111 \\ 0246 & 0246 & 0246 & 0246 \\ 0000 & 2222 & 4444 & 6666 \end{pmatrix},$$

and $\mathcal{H}^{3,1}$ *be the* $\mathbb{Z}_4$*-additive Hadamard code, which is generated by*

$$A^{3,1} = \begin{pmatrix} 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \\ 0123 & 0123 & 0123 & 0123 & 0123 & 0123 & 0123 & 0123 \\ 0000 & 1111 & 2222 & 3333 & 0000 & 1111 & 2222 & 3333 \\ 0000 & 0000 & 0000 & 0000 & 2222 & 2222 & 2222 & 2222 \end{pmatrix}.$$

Let $\mathbf{w}_1, \mathbf{v}_1, \mathbf{v}_2$ *be the rows of* $A^{1,2,0}$ *and* $\bar{\mathbf{w}}_1, \bar{\mathbf{w}}_2, \bar{\mathbf{w}}_3, \bar{\mathbf{v}}_1$ *be the rows of* $A^{3,1}$. *The set* $\mathcal{B}_8 = \{\mathbf{b}_1^8, \ldots, \mathbf{b}_7^8\} = \{\mathbf{w}_1, 2\mathbf{w}_1, 4\mathbf{w}_1, \mathbf{v}_1, \mathbf{v}_2, 2\mathbf{v}_1, 2\mathbf{v}_2\}$ *is a 2-base of* $\mathcal{H}^{1,2,0}$ *and* $\mathcal{B}_4 = \{\mathbf{b}_1^4, \ldots, \mathbf{b}_7^4\} = \{\bar{\mathbf{v}}_1, \bar{\mathbf{w}}_1, 2\bar{\mathbf{w}}_1, \bar{\mathbf{w}}_2, \bar{\mathbf{w}}_3, 2\bar{\mathbf{w}}_2, 2\bar{\mathbf{w}}_3\}$ *a 2-base of* $\mathcal{H}^{3,1}$. *Let* $\gamma = (2,3)(6,7)(10,11)(14,15)(18,19)(22,23)(26,27)(30,31)(34,35)(38,39)(42,43)\ (46,47)(50,51)(54,55)(58,59)(62,63) \in \mathcal{S}_{2^6}$. *Let*

$$\rho = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & 16 & 17 & \ldots & 16+i & \ldots & 32 \\ 1 & 3 & \ldots & 2i-1 & \ldots & 31 & 2 & \ldots & 2i & \ldots & 32 \end{pmatrix} \in \mathcal{S}_{32},$$

so $\rho((u_1^1, \ldots, u_{16}^1, u_1^2, \ldots, u_{16}^2)) = (u_1^1, u_1^2, u_2^1, u_2^2, \ldots, u_{16}^1, u_{16}^2)$, *and* $\tilde{\rho} \in \mathcal{S}_{64}$

such that $\Phi_4 \circ \rho = \tilde{\rho} \circ \Phi_4$. *We have that* $\Phi_8(\sum_{i=1}^{7} \lambda_i \mathbf{b}_i^8) = \gamma \circ \tilde{\rho} \circ \Phi_4(\sum_{i=1}^{7} \lambda_i \mathbf{b}_i^4) = \gamma \circ \Phi_4(\rho(\sum_{i=1}^{7} \lambda_i \mathbf{b}_i^4))$, $\lambda_i \in \{0,1\}$. *Actually, for the elements of the 2-base, we have that*

$$\begin{aligned}
\Phi_8(\mathbf{w}_1) &= \Phi_8(1111111111111111) = \gamma(\Phi_4(\rho(\bar{\mathbf{v}}_1))) \\
&= \gamma(\Phi_4(02020202020202020202020202020202)) \\
\Phi_8(2\mathbf{w}_1) &= \Phi_8(2222222222222222) = \gamma(\Phi_4(\rho(\bar{\mathbf{w}}_1))) \\
&= \gamma(\Phi_4(11111111111111111111111111111111)) \\
\Phi_8(4\mathbf{w}_1) &= \Phi_8(4444444444444444) = \gamma(\Phi_4(\rho(2\bar{\mathbf{w}}_1))) \\
&= \gamma(\Phi_4(22222222222222222222222222222222)) \\
\Phi_8(\mathbf{v}_1) &= \Phi_8(0246024602460246) = \gamma(\Phi_4(\rho(\bar{\mathbf{w}}_2))) \\
&= \gamma(\Phi_4(00112233001122330011223300112233)) \\
\Phi_8(\mathbf{v}_2) &= \Phi_8(0000222244446666) = \gamma(\Phi_4(\rho(\bar{\mathbf{w}}_3))) \\
&= \gamma(\Phi_4(00000000111111112222222233333333)) \\
\Phi_8(2\mathbf{v}_1) &= \Phi_8(0404040404040404) = \gamma(\Phi_4(\rho(2\bar{\mathbf{w}}_2))) \\
&= \gamma(\Phi_4(00220022002200220022002200220022)) \\
\Phi_8(2\mathbf{v}_2) &= \Phi_8(0000444400004444) = \gamma(\Phi_4(\rho(2\bar{\mathbf{w}}_3))) \\
&= \gamma(\Phi_4(00000000222222220000000022222222)).
\end{aligned}$$

Therefore, the codes $H^{3,1} = \Phi_4(\mathcal{H}^{3,1})$ *and* $H^{1,2,0} = \Phi_8(\mathcal{H}^{1,2,0})$ *of length* 2^6 *are permutation equivalent.*

Theorem 90. *Let* $t_1, t_2 \in \mathbb{Z}$, *with* $t_1 \geq 1$ *and* $t_2 \geq 1$. *Then, the Hadamard codes* H^{t_1,t_2} *and* H^{1,t_1-1,t_2-1} *are permutation equivalent.*

Proof. We proof this theorem by induction on the integer t_2. Note that, by Proposition 87, the statement holds for $t_2 = 1$. Now, we suppose that it is true for t_2. Let $\rho \in \mathcal{S}_{2^t}$ be the permutation such that $H^{1,t_1-1,t_2-1} = \rho(H^{t_1,t_2})$ and we define $\rho' = (\rho, \rho) \in \mathcal{S}_{2^{t+1}}$.

By construction, we have that $\mathcal{H}^{1,t_1-1,t_2} = C_0 \cup C_0 + (\mathbf{0}, \mathbf{4})$ and $\mathcal{H}^{t_1,t_2+1} = C_0' \cup C_0' + (\mathbf{0}, \mathbf{2})$, where $C_0 = (\mathcal{H}^{1,t_1-1,t_2-1}, \mathcal{H}^{1,t_1-1,t_2-1})$ and $C_0' = (\mathcal{H}^{t_1,t_2}, \mathcal{H}^{t_1,t_2})$. Then, $\Phi_8(\mathcal{H}^{1,t_1-1,t_2}) = \Phi_8(C_0 \cup C_0 + (\mathbf{0}, \mathbf{4})) = \Phi_8(C_0) \cup \Phi_8(C_0 + (\mathbf{0}, \mathbf{4}))$.

On one hand, by the induction hypothesis, $\Phi_8(C_0) = \Phi_8((\mathcal{H}^{1,t_1-1,t_2-1}, \mathcal{H}^{1,t_1-1,t_2-1})) = (H^{1,t_1-1,t_2-1}, H^{1,t_1-1,t_2-1}) = \rho'((H^{t_1,t_2}, H^{t_1,t_2})) = \rho'(\Phi_4(($

$\mathcal{H}^{t_1,t_2}, \mathcal{H}^{t_1,t_2}))) = \rho'(\Phi_4(C_0'))$. On the other hand, by Corollary 26 and taking into account that $\Phi_8((\mathbf{0},\mathbf{4})) = \Phi_4((\mathbf{0},\mathbf{2})) = \rho'(\Phi_4(\mathbf{0},\mathbf{2}))$, we also have that $\Phi_8(C_0 + (\mathbf{0},\mathbf{4})) = \Phi_8(C_0) + \Phi_8((\mathbf{0},\mathbf{4})) = \rho'(\Phi_4(C_0')) + \rho'(\Phi_4((\mathbf{0},\mathbf{2}))) = \rho'(\Phi_4(C_0') + \Phi_4((\mathbf{0},\mathbf{2}))) = \rho'(\Phi_4(C_0' + (\mathbf{0},\mathbf{2})))$.

Therefore, $H^{1,t_1-1,t_2} = \Phi_8(\mathcal{H}^{1,t_1-1,t_2}) = \rho'(\Phi_4(C_0')) \cup \rho'(\Phi_4(C_0' + (\mathbf{0},\mathbf{2}))) = \rho'(\Phi_4(C_0' \cup C_0' + (\mathbf{0},\mathbf{2})) = \rho'(H^{t_1,t_2+1})$ and the result holds. $\mathcal{QED}$

Now, we know that there are nonlinear Hadamard codes which are both, $\mathbb{Z}_4$-linear and $\mathbb{Z}_8$-linear. From the above results, we can finally give the classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes for $s \in \{2,3\}$.

Proposition 91. *Every $\mathbb{Z}_4$-linear Hadamard code of length 2^t is equivalent to a $\mathbb{Z}_8$-linear Hadamard code, except the $\mathbb{Z}_4$-linear Hadamard code $H^{(t+1)/2,0}$ with $t \geq 5$ odd. Therefore, the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $s \in \{2,3\}$ coincides with $\mathcal{A}_{t,3}$ if t is even or $t \leq 3$, and with $\mathcal{A}_{t,3} + 1$ if t is odd and $t \geq 5$.*

Proof. First of all, we know that for $t \leq 4$, all $\mathbb{Z}_{2^s}$-linear Hadamard codes are linear, so they are permutation equivalent to the binary linear Hadamard code of length 2^t. Recall that, for $s = 2$, we have that $t = 2t_1 + t_2 - 1$. Then, if t is even, all the solutions for $t = 2t_1 + t_2 - 1$ satisfy that $t_2 \geq 1$. Then, by using Theorem 90, we have that every $\mathbb{Z}_4$-linear Hadamard code H^{t_1,t_2} of length 2^t is permutation equivalent to the $\mathbb{Z}_8$-linear Hadamard code H^{1,t_1-1,t_2-1}.

If t is odd, then there exists one solution for $t = 2t_1 + t_2 - 1$ with $t_2 = 0$, that is, when $t_1 = (t+1)/2$. For the rest of solutions with $t_2 \geq 1$, again by using Theorem 90, we know that each $\mathbb{Z}_4$-linear Hadamard code is permutation equivalent to a $\mathbb{Z}_8$-linear Hadamard code. Finally, we have to see that the code $H^{(t+1)/2,0}$ is not permutation equivalent to a $\mathbb{Z}_8$-linear Hadamard code.

Suppose that there exists a $\mathbb{Z}_8$-linear Hadamard code H^{t_1,t_2,t_3} that is permutation equivalent to $H^{(t+1)/2,0}$. We know that both codes should have the same length and dimension of the kernel. Recall that $\ker(H^{(t+1)/2,0}) = (t+1)/2 + 1$ since $t \geq 5$ [Kro01]. We also have that $\ker(H^{t_1,t_2,t_3}) = t_1 + t_2 +$

$t_3 + \sigma_{t_1}$, where $\sigma_{t_1} = 1$ if $t_1 \geq 2$ and $\sigma_{t_1} = 2$ if $t_1 = 1$ by Proposition 80. On the one hand, if $t_1 = 1$, then $\sigma_{t_1} = 2$ and from the equations $t+1 = 3+2t_2+t_3$ and $(t+1)/2 + 1 = 1 + t_2 + t_3 + 2$ we obtain that $t_3 = -1$. On the other hand, if $t_1 \geq 2$, then $\sigma_{t_1} = 1$ and we have the following equations

$$\left.\begin{array}{rcl} t+1 & = & 3t_1 + 2t_2 + t_3 \\ \dfrac{t+1}{2} + 1 & = & t_1 + t_2 + t_3 + 1 \end{array}\right\} \Rightarrow \left\{\begin{array}{rcl} t_3 & = & t_1 \\ t_2 & = & \dfrac{t+1-4t_1}{2} \end{array}\right. .$$

These two codes should also have the same rank, so $\mathrm{rank}(H^{t_1,(t+1-4t_1)/2,t_1}) = \mathrm{rank}(H^{(t+1)/2,0})$. By Proposition 12, we have that if $t_1 \geq 1$ and $t_2 \geq 0$, then

$$\mathrm{rank}(\Phi(\mathcal{H}^{t_1,t_2})) = 2t_1 + t_2 + \binom{t_1 - 1}{2}.$$

Moreover, by Theorem 79 and after simplifying, we obtain that

$$t_1^3 - 26t_1^2 + (6t + 65)t_1 - 18t - 4 = 0. \tag{5.28}$$

Note that the right-hand side of equation (5.28) is strictly positive for $t_1 \geq 26$, since we can rewrite it as $t_1^3 + (6t + 65)t_1 > 26t_1^2 + 18t + 4$. For $t_1 \in \{3, 6, 8, 9, 10, 12, \ldots, 25\}$, equation (5.28) has no any integer solution for t. For $t_1 = 1$, it has solution $t = 3$, but recall that $t \geq 4$. For $t_1 = 4$, it has solution $t = 16$, but in this case $t_2 = 1/2 \notin \mathbb{Z}$. Finally, for $t_1 \in \{2, 5, 7, 11\}$, it has solutions $t = 5, 17, 20, 23$, respectively, but in all these cases, $t_2 < 0$. Therefore, the result holds. $\mathcal{QED}$

We have shown that the classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes for $s \in \{2, 3\}$ is complete. Specifically, there exists only one binary nonlinear Hadamard code of length 2^t that is $\mathbb{Z}_4$-linear, but not $\mathbb{Z}_8$-linear, when t odd. When t is even, all the $\mathbb{Z}_4$-linear Hadamard codes of length 2^t are also $\mathbb{Z}_8$-linear. This means that to generate all the $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s \in \{2, 3\}$ of a certain length, it is enough to generate all the $\mathbb{Z}_8$-linear Hadamard codes and, if t is odd, add the code $H^{(t+1)/2,0}$.

Chapter 6

Equivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes

"Logic merely sanctions the conquests of the intuition."

–Jacques Hadamard

In Chapter 4, the dimension of the kernel for $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s > 2$ is established, and it is proved that this invariant only provides a complete classification for some values of t and s. The rank is computed in Chapter 5 only for $s = 3$, and it is proved that in this case the rank together with the dimension of the kernel provides a full classification for any $t \geq 3$. Furthermore, it is shown that it gives a full classification for $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s \in \{2, 3\}$. Along this thesis, we have observed that there are many nonlinear such codes having the same rank and dimension of the kernel for different values of s, once the length 2^t is fixed (see Tables 4.4, 4.5 and 5.1, and Examples 50 and 81). In Chapter 6, we show that these codes, the ones having the same rank and dimension of the kernel, are in fact equivalent, which allows us to obtain a more accurate classification than the one given in Chapter 4. More specifically, in Section 6.1, we show that there exist families of equivalent codes with different values of s, once t is fixed. Finally, in Section 6.2, we improve the partial classification given in Chapter 4 by refining the upper bound on the number of nonequivalent such

codes of length 2^t, denoted by $\mathcal{A}_t$; and we show that this bound is tight for $3 \leq t \leq 11$.

6.1 Equivalences among $\mathbb{Z}_{2^s}$-linear Hadamard codes

In this section, we give some properties of the generalized Gray map Φ and some equivalence relations among the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, once t is fixed.

Recall that, to specify that the domain is $\mathbb{Z}_{2^s}$ and $\mathbb{Z}_{2^s}^n$, we will denote the Gray maps by ϕ_s and Φ_s instead of ϕ and Φ, respectively. Let $\gamma_s \in \mathcal{S}_{2^{s-1}}$ be the permutation defined as

$$\begin{pmatrix} 1 & 2 & \dots & 2^{s-2} & 2^{s-2}+1 & 2^{s-2}+2 & \dots & 2^{s-1} \\ 1 & 3 & \dots & 2^{s-1}-1 & 2 & 4 & \dots & 2^{s-1} \end{pmatrix}.$$

For example, we have that $\gamma_3 = (2,3) \in \mathcal{S}_4$ and $\gamma_4 = (2,3,5)(4,7,6) \in \mathcal{S}_8$. Then, we can define the generalization of function τ given in (5.24), $\tau_s : \mathbb{Z}_{2^s} \to \mathbb{Z}_{2^{s-1}}^2$, as

$$\tau_s(u) = \Phi_{s-1}^{-1}(\gamma_s^{-1}(\phi_s(u))), \tag{6.1}$$

for $u \in \mathbb{Z}_{2^s}$.

Example 92. *For $s = 3$, the relations that define the map τ_3 are shown in*

(5.23). For $s = 4$, we have that

$$\begin{aligned}
\phi_4(0) &= (0,0,0,0,0,0,0,0) = \gamma_4((0,0,0,0,0,0,0,0)) = \gamma_4(\Phi_3((0,0)))\\
\phi_4(1) &= (0,1,0,1,0,1,0,1) = \gamma_4((0,0,0,0,1,1,1,1)) = \gamma_4(\Phi_3((0,4)))\\
\phi_4(2) &= (0,0,1,1,0,0,1,1) = \gamma_4((0,1,0,1,0,1,0,1)) = \gamma_4(\Phi_3((1,1)))\\
\phi_4(3) &= (0,1,1,0,0,1,1,0) = \gamma_4((0,1,0,1,1,0,1,0)) = \gamma_4(\Phi_3((1,5)))\\
\phi_4(4) &= (0,0,0,0,1,1,1,1) = \gamma_4((0,0,1,1,0,0,1,1)) = \gamma_4(\Phi_3((2,2)))\\
\phi_4(5) &= (0,1,0,1,1,0,1,0) = \gamma_4((0,0,1,1,1,1,0,0)) = \gamma_4(\Phi_3((2,6)))\\
\phi_4(6) &= (0,0,1,1,1,1,0,0) = \gamma_4((0,1,1,0,0,1,1,0)) = \gamma_4(\Phi_3((3,3)))\\
\phi_4(7) &= (0,1,1,0,1,0,0,1) = \gamma_4((0,1,1,0,1,0,0,1)) = \gamma_4(\Phi_3((3,7)))\\
\phi_4(8) &= (1,1,1,1,1,1,1,1) = \gamma_4((1,1,1,1,1,1,1,1)) = \gamma_4(\Phi_3((4,4)))\\
\phi_4(9) &= (1,0,1,0,1,0,1,0) = \gamma_4((1,1,1,1,0,0,0,0)) = \gamma_4(\Phi_3((4,0)))\\
\phi_4(10) &= (1,1,0,0,1,1,0,0) = \gamma_4((1,0,1,0,1,0,1,0)) = \gamma_4(\Phi_3((5,5)))\\
\phi_4(11) &= (1,0,0,1,1,0,0,1) = \gamma_4((1,0,1,0,0,1,0,1)) = \gamma_4(\Phi_3((5,1)))\\
\phi_4(12) &= (1,1,1,1,0,0,0,0) = \gamma_4((1,1,0,0,1,1,0,0)) = \gamma_4(\Phi_3((6,6)))\\
\\
\phi_4(13) &= (1,0,1,0,0,1,0,1) = \gamma_4((1,1,0,0,0,0,1,1)) = \gamma_4(\Phi_3((6,2)))\\
\phi_4(14) &= (1,1,0,0,0,0,1,1) = \gamma_4((1,0,0,1,1,0,0,1)) = \gamma_4(\Phi_3((7,7)))\\
\phi_4(15) &= (1,0,0,1,0,1,1,0) = \gamma_4((1,0,0,1,0,1,1,0)) = \gamma_4(\Phi_3((7,3))).
\end{aligned}$$

These equalities define the map $\tau_4 : \mathbb{Z}_{16} \to \mathbb{Z}_8^2$ as $\tau_4(0) = (0,0)$, $\tau_4(1) = (0,4)$, $\tau_4(2) = (1,1)$, $\tau_4(3) = (1,5)$, $\tau_4(4) = (2,2)$, $\tau_4(5) = (2,6)$, $\tau_4(6) = (3,3)$, $\tau_4(7) = (3,7)$, $\tau_4(8) = (4,4)$, $\tau_4(9) = (4,0)$, $\tau_4(10) = (5,5)$, $\tau_4(11) = (5,1)$, $\tau_4(12) = (6,6)$, $\tau_4(13) = (6,2)$, $\tau_4(14) = (7,7)$ and $\tau_4(15) = (7,3)$.

Lemma 93. *Let $s \geq 2$. Then,*

(i) $\tau_s(1) = (0, 2^{s-2})$,

(ii) $\tau_s(2^i u) = 2^{i-1}(u,u)$ *for all* $i \in \{1, \ldots, s-1\}$ *and* $u \in \{0, 1, \ldots, 2^{s-1}-1\}$.

Proof. First, $\tau_s(1) = \Phi_{s-1}^{-1}(\gamma_s^{-1}(\phi_s(1))) = \Phi_{s-1}^{-1}(\gamma_s^{-1}((0,1,0,1,\ldots,0,1))) = \Phi_{s-1}^{-1}((\mathbf{0},\mathbf{1})) = (0, 2^{s-2})$, and (i) holds.

In order to prove (ii), let $u \in \mathbb{Z}_{2^s}$ and $[u_0, \ldots, u_{s-1}]_2$ be its binary expansion. The binary expansion of $2^i u$ is $[0, \ldots, 0, u_0, \ldots, u_{s-i-1}]_2$ and we have

that $\phi_s(2^i u) = (u_{s-i-1}, \ldots, u_{s-i-1}) + (0, \ldots, 0, u_0, \ldots, u_{s-i-2})Y_{s-1}$. It is easy to see by (2.20) that

$$\gamma_s^{-1}(Y_{s-1}) = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ Y_{s-2} & Y_{s-2} \end{pmatrix}. \tag{6.2}$$

Then, we have that

$$\begin{aligned}
&\gamma_s^{-1}(\phi_s(2^i u)) = \\
&= (u_{s-i-1}, \overset{(2^{s-1})}{\ldots}, u_{s-i-1}) + (0, \overset{(i)}{\ldots}, 0, u_0, \ldots, u_{s-i-2}) \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ Y_{s-2} & Y_{s-2} \end{pmatrix} = \\
&= (u_{s-i-1}, \overset{(2^{s-1})}{\ldots}, u_{s-i-1}) + (0, \overset{(i-1)}{\ldots}, 0, u_0, \ldots, u_{s-i-2}) \begin{pmatrix} Y_{s-2} & Y_{s-2} \end{pmatrix} = \\
&= (\phi_{s-1}(2^{i-1}u), \phi_{s-1}(2^{i-1}u)) = \Phi_{s-1}(2^{i-1}(u,u)).
\end{aligned}$$

Therefore, $\tau_s(2^i u) = \Phi_{s-1}^{-1}(\gamma_s^{-1}(\phi_s(2^i u))) = 2^{i-1}(u,u)$, and (ii) holds. $\mathcal{QED}$

Proposition 94. *Let $s \geq 2$ and $\lambda_i \in \{0,1\} \subset \mathbb{Z}_{2^s}$, $i \in \{0, \ldots, s-1\}$. Then,*

$$\phi_s(\sum_{i=0}^{s-1} \lambda_i 2^i) = \gamma_s(\Phi_{s-1}(\sum_{i=0}^{s-1} \tau_s(\lambda_i 2^i))). \tag{6.3}$$

Proof. By Lemma 93, we know that for all $i \in \{1, \ldots, s-1\}$, $\tau_s(2^i) = (2^{i-1}, 2^{i-1})$ and $\tau_s(1) = (0, 2^{s-2})$. Then, by Lemma 36, we have that

$$\gamma_s(\Phi_{s-1}(\sum_{i=0}^{s-1} \tau_s(\lambda_i 2^i))) = \gamma_s(\sum_{i=0}^{s-1} \Phi_{s-1}(\tau_s(\lambda_i 2^i))).$$

Moreover, since γ_s commute with the summation, and applying the definition (6.1) of τ_s, we obtain that

$$\gamma_s(\Phi_{s-1}(\sum_{i=0}^{s-1} \tau_s(\lambda_i 2^i))) = \sum_{i=0}^{s-1} \gamma_s(\Phi_{s-1}(\tau_s(\lambda_i 2^i))) = \sum_{i=0}^{s-1} \phi_s(\lambda_i 2^i),$$

which is equal to $\phi_s(\sum_{i=0}^{s-1} \lambda_i 2^i)$, by Lemma 36. $\mathcal{QED}$

Now, we extend the permutation $\gamma_s \in \mathcal{S}_{2^{s-1}}$ to a permutation $\gamma_s \in$

$\mathcal{S}_{2^{s-1}n}$ such that restricted to each set of 2^{s-1} coordinates $\{2^{s-1}i+1, 2^{s-1}i+2, \cdots, 2^{s-1}(i+1)\}$, $i \in \{0,\ldots,n-1\}$, acts as $\gamma_s \in \mathcal{S}_{2^{s-1}}$. Then, we component-wise extend function τ_s defined in (6.1) to $\tau_s : \mathbb{Z}_{2^s}^n \to \mathbb{Z}_{2^{s-1}}^{2n}$ and define $\tilde{\tau}_s = \rho^{-1} \circ \tau_s$, where $\rho \in \mathcal{S}_{2n}$ is defined as

$$\begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n & n+1 & \ldots & n+i & \ldots & 2n \\ 1 & 3 & \ldots & 2i-1 & \ldots & 2n-1 & 2 & \ldots & 2i & \ldots & 2n \end{pmatrix}.$$

If $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{Z}_{2^s}^n$ and $\tau_s(u_i) = (u_i^1, u_i^2)$ for all $i \in \{1,\ldots,n\}$, then $\tau_s(\mathbf{u}) = (u_1^1, u_1^2, u_2^1, u_2^2, \ldots, u_n^1, u_n^2)$ and $\tilde{\tau}_s(\mathbf{u}) = (u_1^1, \ldots, u_n^1, u_1^2, \ldots, u_n^2)$. Note also that

$$\Phi_s(\mathbf{u}) = \gamma_s(\Phi_{s-1}(\rho(\tilde{\tau}_s(\mathbf{u}))))$$

for all $\mathbf{u} \in \mathbb{Z}_{2^s}^n$, since $\tilde{\tau}_s(\mathbf{u}) = \rho^{-1}(\tau_s(\mathbf{u})) = \rho^{-1}(\Phi_{s-1}^{-1}(\gamma_s^{-1}(\Phi_s(\mathbf{u}))))$.

Let $\mathbf{w}_i^{(s)}$ be the ith row of $A^{t_1,\ldots,t_s}$, $1 \le i \le t_1 + \cdots + t_s$. By construction, $\mathbf{w}_1^{(s)} = \mathbf{1}$ and $\mathrm{ord}(\mathbf{w}_i^{(s)}) \le \mathrm{ord}(\mathbf{w}_j^{(s)})$ if $i > j$. Let σ_i be the integer such that $\mathrm{ord}(\mathbf{w}_i^{(s)}) = 2^{\sigma_i}$. Then, $\mathcal{B}^{t_1,\ldots,t_s} = \{2^{p_i}\mathbf{w}_i^{(s)} : 1 \le i \le t_1 + \cdots + t_s,\ 0 \le p_i \le \sigma_i - 1\}$ is a 2-base of $\mathcal{H}^{t_1,\ldots,t_s}$.

Example 95. *Let $\mathcal{H}^{2,1}$ and $\mathcal{H}^{1,1,0}$ be the $\mathbb{Z}_4$-additive and $\mathbb{Z}_8$-additive Hadamard codes, which are generated by*

$$A^{2,1} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \end{pmatrix}, \quad \textit{and} \quad A^{1,1,0} = \begin{pmatrix} 1\,1\,1\,1 \\ 0\,2\,4\,6 \end{pmatrix},$$

respectively. The corresponding 2-bases are $\mathcal{B}^{2,1} = \{(1,1,1,1,1,1,1,1), (2,2,2,2,2,2,2,2), (0,1,2,3,0,1,2,3), (0,2,0,2,0,2,0,2), (0,0,0,0,0,2,2,2,2)\}$, and $\mathcal{B}^{1,1,0} = \{(1,1,1,1), (2,2,2,2), (4,4,4,4), (0,2,4,6), (0,4,0,4)\}$.

Proposition 96. *Let $t_s \ge 1$, and $\mathcal{H}^{t_1,\ldots,t_s}$ and $\mathcal{H}^{1,t_1-1,t_2,\ldots,t_{s-1},t_s-1}$ be the $\mathbb{Z}_{2^s}$-additive and $\mathbb{Z}_{2^{s+1}}$-additive Hadamard codes with generator matrices $A^{t_1,\ldots,t_s}$ and $A^{1,t_1-1,t_2,\ldots,t_{s-1},t_s-1}$, respectively. Let $\mathbf{w}_i^{(s)}$ and $\mathbf{w}_i^{(s+1)}$ be the ith row of $A^{t_1,\ldots,t_s}$ and $A^{1,t_1-1,t_2,\ldots,t_{s-1},t_s-1}$, respectively. Then, we have that*

(i) $\tilde{\tau}_{s+1}(2^{p_i}\mathbf{w}_i^{(s+1)}) = 2^{p_i}\mathbf{w}_i^{(s)}$, for all $i \in \{2,\ldots,t_1+\cdots+t_s-1\}$ and $p_i \in \{0,\ldots,\sigma_i-1\}$, where σ_i is the integer such that $\mathrm{ord}(\mathbf{w}_i^{(s)}) = 2^{\sigma_i}$;

(ii) $\tilde{\tau}_{s+1}(2^{j+1}\mathbf{w}_1^{(s+1)}) = 2^j\mathbf{w}_1^{(s)}$, *for all* $j \in \{0,\ldots,s-1\}$;

(iii) $\tilde{\tau}_{s+1}(\mathbf{w}_1^{(s+1)}) = \mathbf{w}_{t_s}^{(s)}$.

Proof. Consider $A^{t_1,\ldots,t_s}$ with $t_s \geq 1$, and $\mathbf{w}_i^{(s)}$ its ith row for $i \in \{1,\ldots,t_1+\cdots+t_s\}$. Then, the matrix over $\mathbb{Z}_{2^{s+1}}$

$$\begin{pmatrix} \mathbf{w}_1^{(s)} \\ 2\mathbf{w}_2^{(s)} \\ \vdots \\ 2\mathbf{w}_{t_1+\cdots+t_s}^{(s)} \end{pmatrix}$$

is, by definition, $A^{1,t_1-1,t_2,\ldots,t_{s-1},t_s}$. Moreover, by construction we have that

$$A^{1,t_1-1,t_2,\ldots,t_{s-1},t_s} = \begin{pmatrix} A^{1,t_1-1,t_2,\ldots,t_{s-1},t_s-1} & A^{1,t_1-1,t_2,\ldots,t_{s-1},t_s-1} \\ \mathbf{0} & \mathbf{2^s} \end{pmatrix}.$$

Therefore, if $\mathbf{w}_i^{(s+1)}$ is the ith row of $A^{1,t_1-1,t_2,\ldots,t_{s-1},t_s-1}$ for $i \in \{2,\ldots,t_1+t_2+\cdots+t_s-1\}$, we have that $(\mathbf{w}_i^{(s+1)},\mathbf{w}_i^{(s+1)}) = 2\mathbf{w}_i^{(s)}$ and $\mathrm{ord}(\mathbf{w}_i^{(s)}) = \mathrm{ord}(\mathbf{w}_i^{(s+1)}) = \sigma_i$. Let $\mathbf{v}_i^{(s+1)}$ be the vector over $\mathbb{Z}_{2^{s+1}}$ such that $\mathbf{w}_i^{(s+1)} = 2\mathbf{v}_i^{(s+1)}$ and $\mathbf{w}_i^{(s)} = (\mathbf{v}_i^{(s+1)},\mathbf{v}_i^{(s+1)})$. Let $(\mathbf{v}_i^{(s+1)})_j$ be the jth coordinate of $\mathbf{v}_i^{(s+1)}$. By the definition of $\tilde{\tau}_{s+1}$ and Lemma 93, for $p_i \in \{0,\ldots,\sigma_i-1\}$, we have that

$$\begin{aligned}\tilde{\tau}_{s+1}(2^{p_i}\mathbf{w}_i^{(s+1)}) &= \rho^{-1}(\tau_{s+1}(2^{p_i}\mathbf{w}_i^{(s+1)})) = \rho^{-1}(\tau_{s+1}(2^{p_i+1}\mathbf{v}_i^{(s+1)})) = \\ &= \rho^{-1}(2^{p_i}((\mathbf{v}_i^{(s+1)})_1,(\mathbf{v}_i^{(s+1)})_1,\ldots,(\mathbf{v}_i^{(s+1)})_n,(\mathbf{v}_i^{(s+1)})_n)) = \\ &= 2^{p_i}(\mathbf{v}_i^{(s+1)},\mathbf{v}_i^{(s+1)}) = 2^{p_i}\mathbf{w}_i^{(s)},\end{aligned}$$

and (i) holds.

Since $\mathbf{w}_1^{(s)} = (\mathbf{w}_1^{(s+1)},\mathbf{w}_1^{(s+1)}) = \mathbf{1}$ and $\mathbf{w}_{t_s}^{(s)} = (\mathbf{0},\mathbf{2^{s-1}})$, then the equalities in items (ii) and (iii) hold, by the definition of $\tilde{\tau}_{s+1}$ and Lemma 93. $\mathcal{QED}$

Note that, from the previous proposition, we have that $\tilde{\tau}_s$ is a bijection between the 2-bases, $\mathcal{B}^{t_1,\ldots,t_s}$ and $\mathcal{B}^{1,t_1-1,\ldots,t_{s-1},t_s-1}$.

Example 97. *Let $\mathcal{H}^{1,1,0}$ and $\mathcal{H}^{2,1}$ be the same codes considered in Example 95. The length of $\mathcal{H}^{1,1,0}$ is $n = 4$. Then, the extension of $\gamma_3 = (2,3) \in \mathcal{S}_4$ is $\gamma_3 = (2,3)(6,7)(10,11)(14,15) \in \mathcal{S}_{16}$, and*

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 5 & 7 & 2 & 4 & 6 & 8 \end{pmatrix} \in \mathcal{S}_8. \tag{6.4}$$

In this case, we have that

$$\begin{aligned}
&\Phi_3((1,1,1,1)) = \gamma_3(\Phi_2(0,2,0,2,0,2,0,2)) = \gamma_3(\Phi_2(\rho(0,0,0,0,2,2,2,2))) \\
&\Phi_3((2,2,2,2)) = \gamma_3(\Phi_2(1,1,1,1,1,1,1,1)) = \gamma_3(\Phi_2(\rho(1,1,1,1,1,1,1,1))) \\
&\Phi_3((4,4,4,4)) = \gamma_3(\Phi_2(2,2,2,2,2,2,2,2)) = \gamma_3(\Phi_2(\rho(2,2,2,2,2,2,2,2))) \\
&\Phi_3((0,2,4,6)) = \gamma_3(\Phi_2(0,0,1,1,2,2,3,3)) = \gamma_3(\Phi_2(\rho(0,1,2,3,0,1,2,3))) \\
&\Phi_3((0,4,0,4)) = \gamma_3(\Phi_2(0,0,2,2,0,0,2,2)) = \gamma_3(\Phi_2(\rho(0,2,0,2,0,2,0,2))).
\end{aligned}$$

Since $\Phi_3(\mathbf{u}) = \gamma_3(\Phi_2(\rho(\tilde{\tau}_3(\mathbf{u}))))$ for all $\mathbf{u} \in \mathbb{Z}_8^4$, the map $\tilde{\tau}_3$ sends the elements of the 2-base $\mathcal{B}^{1,1,0}$ into the elements of the 2-base $\mathcal{B}^{2,1}$. That is, as it is shown in Proposition 96,

$$\begin{aligned}
\tilde{\tau}_3(\mathbf{w}_1^{(3)}) &= \Phi_3((1,1,1,1)) = (0,0,0,0,2,2,2,2) = \mathbf{w}_3^{(2)} \\
\tilde{\tau}_3(2\mathbf{w}_1^{(3)}) &= \Phi_3((2,2,2,2)) = (1,1,1,1,1,1,1,1) = \mathbf{w}_1^{(2)} \\
\tilde{\tau}_3(4\mathbf{w}_1^{(3)}) &= \Phi_3((4,4,4,4)) = (2,2,2,2,2,2,2,2) = 2\mathbf{w}_1^{(2)} \\
\tilde{\tau}_3(\mathbf{w}_2^{(3)}) &= \Phi_3((0,2,4,6)) = (0,1,2,3,0,1,2,3) = \mathbf{w}_2^{(2)} \\
\tilde{\tau}_3(2\mathbf{w}_2^{(3)}) &= \Phi_3((0,4,0,4)) = (0,2,0,2,0,2,0,2) = 2\mathbf{w}_2^{(2)},
\end{aligned} \tag{6.5}$$

so $\tilde{\tau}_3$ is a bijection between both 2-bases. By Proposition 94, it is easy to check that the corresponding binary codes of length 16, $H^{2,1} = \Phi_2(\mathcal{H}^{2,1})$ and $H^{1,1,0} = \Phi_3(\mathcal{H}^{1,1,0})$, are, in fact, equivalent.

The following theorem determines which $\mathbb{Z}_{2^{s'}}$-linear Hadamard codes are equivalent to a given $\mathbb{Z}_{2^s}$-linear Hadamard code $H^{t_1,\ldots,t_s}$. We denote by $\mathbf{0}^j$ the all-zero vector of length j. Let σ be the integer such that $\mathrm{ord}(\mathbf{w}_2^{(s)}) = 2^{s+1-\sigma}$, so $\sigma = s + 1 - \sigma_2$.

Theorem 98. *Let $H^{t_1,\ldots,t_s}$ be a $\mathbb{Z}_{2^s}$-linear Hadamard code.*

(i) If $\sigma = 1$ and $t_s \geq 1$, then $H^{t_1,\ldots,t_s}$ is equivalent to the $\mathbb{Z}_{2^{s+\ell}}$-linear Hadamard code $H^{1,\mathbf{0}^{\ell-1},t_1-1,t_2,\ldots,t_{s-1},t_s-\ell}$, for $\ell \in \{1,\ldots,t_s\}$.

(ii) If $\sigma > 1$, then $(t_1,\ldots,t_s) = (1,\mathbf{0}^{\sigma-2},t_\sigma,\ldots,t_s)$ and $H^{t_1,\ldots,t_s}$ is equivalent to the $\mathbb{Z}_{2^{s+\ell}}$-linear Hadamard code $H^{1,\mathbf{0}^{\sigma-2+\ell},t_\sigma,\ldots,t_s-\ell}$, for $\ell \in \{2-\sigma,\ldots,t_s\}$, and to the $\mathbb{Z}_{2^{s-\sigma+1}}$-linear Hadamard code $H^{t_\sigma+1,t_{\sigma+1},\ldots,t_{s-1},t_s+\sigma-1}$.

Proof. Straightforward from Propositions 94 and 96. $\mathcal{QED}$

Corollary 99. *Let $H^{t_1,\ldots,t_s}$ be a $\mathbb{Z}_{2^s}$-linear Hadamard code. Then, there exists a $\mathbb{Z}_{2^{s+\ell}}$-linear Hadamard code equivalent to $H^{t_1,\ldots,t_s}$, for all $\ell \in \{1-\sigma,\ldots,t_s\}$.*

Example 100. *The $\mathbb{Z}_{2^3}$-linear Hadamard code $H^{2,1,3}$, with $\sigma = 1$ and $t_3 = 3 \geq 1$, is equivalent to the following $\mathbb{Z}_{2^{s'}}$-linear Hadamard codes: $H^{1,1,1,2}$, $H^{1,0,1,1,1}$ and $H^{1,0,0,1,1,0}$, with $s' = 4, 5$ and 6, respectively. An example with $\sigma > 1$ is the $\mathbb{Z}_{2^5}$-linear Hadamard code $H^{1,0,0,2,2}$, with $\sigma = 4$. In this case, the code is equivalent to $H^{3,5}$, $H^{1,2,4}$, $H^{1,0,2,3}$, $H^{1,0,0,2,2}$, $H^{1,0,0,0,2,1}$ and $H^{1,0,0,0,0,2,0}$, with $s' = 2, 3, 4, 5, 6$ and 7, respectively.*

If $H^{t_1,\ldots,t_s}$ is a $\mathbb{Z}_{2^s}$-linear Hadamard code with $\sigma = 1$ and $t_s = 0$, then Theorem 98 cannot be applied. In this case, we conjecture that $H^{t_1,\ldots,t_s}$ is not equivalent to any other code $H^{t'_1,\ldots,t'_{s'}}$, for $s' \neq s$. From Tables 4.1, 4.4 and 4.5, we can see that this conjecture is satisfied for $t \leq 11$. The values of $(t_1,\ldots,t_s)$ for which the codes $H^{t_1,\ldots,t_s}$ are not equivalent to any other such code can be found in Table 6.1 for $t \leq 11$.

Example 101. *There is no other $\mathbb{Z}_{2^s}$-linear Hadamard code $H^{t_1,\ldots,t_s}$ of length 2^7 equivalent to $H^{2,1,0}$.*

In Tables 4.1, 4.4 and 4.5, for $t \leq 11$ and $s \in \{2,\ldots,t+1\}$, we show all possible values $(t_1,\ldots,t_s)$ for which there exists a $\mathbb{Z}_{2^s}$-linear Hadamard code $H^{t_1,\ldots,t_s}$ of length 2^t. For each one of them, the values (r,k), where r is the rank and k is the dimension of the kernel, are also shown. These two invariants have been computed by using the computer algebra system Magma [BCFS16, PV17]. Note that if two codes have different values (r,k), then they are not equivalent. Now, by Theorem 98, we have that the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $t \leq 11$ having the same values (r,k) are equivalent.

$t = 5$	(3,0), (2,0,0)
$t = 7$	(4,0), (2,1,0), (2,0,0,0)
$t = 8$	(3,0,0)
$t = 9$	(5,0), (2,2,0), (2,0,1,0), (2,0,0,0,0)
$t = 10$	(3,1,0), (2,1,0,0)
$t = 11$	(6,0), (2,3,0), (4,0,0), (2,0,2,0), (3,0,0,0), (2,0,0,1,0), (2,0,0,0,0,0)

Table 6.1: Type of all $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $\sigma = 1$ and $t_s = 0$.

Example 102. *From Table 4.1, we can see that there are four $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^8 having rank equal to 10 and dimension of the kernel equal to 7: the $\mathbb{Z}_4$-linear Hadamard code $H^{3,3}$, the $\mathbb{Z}_8$-linear Hadamard code $H^{1,2,2}$, the $\mathbb{Z}_{16}$-linear Hadamard code $H^{1,0,2,1}$, and the $\mathbb{Z}_{32}$-linear Hadamard code $H^{1,0,0,2,0}$. By Theorem 98, all these codes are equivalent.*

6.2 Improvement of the partial classification

In this section, we improve some partial results, given in Section 4.2, on the classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, once t is fixed.

Given $t \geq 3$ and $2 \leq s \leq t+1$, recall that we define $\mathcal{A}_{t,s}$ as the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t. Given $t \geq 3$, $\mathcal{A}_t$ denote the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with any $s \geq 2$. In Section 4.2, Theorems 52 and 56 give upper bounds for $\mathcal{A}_{t,s}$ and $\mathcal{A}_t$, respectively.

In Table 6.2, for $t \in \{3, \ldots, 11\}$, the lower bound given by the number of different dimensions of the kernel and the upper bound given by (4.4) in Theorem 56 are shown.

Corollary 103. *Let $H^{t_1,\ldots,t_s}$ be a $\mathbb{Z}_{2^s}$-linear Hadamard code. Then, $H^{t_1,\ldots,t_s}$ is equivalent to exactly one $\mathbb{Z}_{2^{s'}}$-linear Hadamard code $H^{t'_1,\ldots,t'_{s'}}$ with $t'_1 > 1$.*

Proof. If $t_1 > 1$, then $s' = s$ and $t'_i = t_i$ for all $i \in \{1, \ldots, s\}$. Otherwise, if $t_1 = 1$, the result holds by (ii) of Theorem 98. $\mathcal{QED}$

By Corollary 99, we have that any $\mathbb{Z}_{2^s}$-linear Hadamard code $H^{t_1,\ldots,t_s}$ is

t	3	4	5	6	7	8	9	10	11
lower bound	1	1	3	3	5	5	7	7	9
upper bound (6.6)	1	1	3	3	6	7	11	13	20
upper bound (6.7)	1	1	3	4	9	12	22	28	47
upper bound (4.4)	1	1	3	5	10	16	26	38	57
upper bound (4.5)	1	1	3	5	10	16	26	38	57

Table 6.2: Bounds for the number $\mathcal{A}_t$ of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $t \in \{3, \ldots, 11\}$.

equivalent to $\sigma + t_s$ $\mathbb{Z}_{2^{s'}}$-linear Hadamard codes (including $H^{t_1,\ldots,t_s}$). Moreover, Corollary 103 tells us that, always, exactly one of these $\sigma+t_s$ equivalent codes has $t_1 > 1$.

Example 104. *For $t = 7$, by Theorem 98, we can see that the codes $H^{3,2}$, $H^{1,2,1}$, $H^{1,0,2,0}$ are equivalent and only one of them, $H^{3,2}$, has $t_1 > 1$ as it is shown in Corollary 103. Similarly, the codes $H^{2,0,2}$, $H^{1,1,0,1}$ and $H^{1,0,1,0,0}$ are also equivalent and one of them, $H^{2,0,2}$, satisfies that $t_1 > 1$.*

Corollary 105. *Let H be a nonlinear $\mathbb{Z}_{2^s}$-linear Hadamard code of length 2^t. If $s \in \{\lfloor (t+1)/2 \rfloor + 1, \ldots, t+1\}$, then there exists an equivalent $\mathbb{Z}_{2^{s'}}$-linear Hadamard code of length 2^t with $s' \in \{2, \ldots, \lfloor (t+1)/2 \rfloor\}$.*

Proof. Let $H^{t_1,\ldots,t_s}$ be a $\mathbb{Z}_{2^s}$-linear Hadamard code with $s \in \{\lfloor (t+1)/2 \rfloor + 1, \ldots, t+1\}$. Since $\sum_{i=1}^{s}(s+1-i)t_i = t+1$, then $t_1 = 1$ and we have that $\sigma > 1$. Therefore, by the (ii) in Theorem 98, $H^{t_1,\ldots,t_s}$ is permutation equivalent to the $\mathbb{Z}_{2^{s-\sigma+1}}$-linear Hadamard code $H = H^{t_\sigma+1, t_{\sigma+1}, \ldots, t_{s-1}, t_s+\sigma-1}$.

Now, we just need to see that $s-\sigma+1 < \lfloor (t+1)/2 \rfloor$. Since the length of H is 2^t, we have that $t+1 = (s-\sigma+1)(t_\sigma+1) + \sum_{i=2}^{s-\sigma+1}(s-\sigma+2-i)t_{\sigma-1+i} + \sigma - 1$. Therefore, $(s-\sigma+1)(t_\sigma+1) \leq t+1$ and $s-\sigma+1 \leq (t+1)/(t_\sigma+1)$. By the definition of t_σ, we know that $t_\sigma \geq 1$, so $s-\sigma+1 \leq \lfloor (t+1)/2 \rfloor$. $\mathcal{QED}$

From the previous two corollaries, note that we can focus on the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with $s \in \{2, \ldots, \lfloor (t+1)/2 \rfloor\}$ in order to classify all such codes for a given $t \geq 3$. Let $\tilde{X}_{t,s} = |\{(t_1, \ldots, t_s) \in \mathbb{N}^s : t+1 = \sum_{i=1}^{s}(s-i+1)t_i,\ t_1 \geq 2\}|$ for $s \in \{3, \ldots, \lfloor (t+1)/2 \rfloor\}$ and

$\tilde{X}_{t,2} = |\{(t_1, t_2) \in \mathbb{N}^2 : t + 1 = 2t_1 + t_2,\ t_1 \geq 3\}|$. Note that we define $\tilde{X}_{t,2}$ with $t_1 \geq 3$ because, if $t_1 = 2$, the code is linear [Kro01].

Theorem 106. *For $t \geq 3$,*

$$\mathcal{A}_t \leq 1 + \sum_{s=2}^{\lfloor \frac{t+1}{2} \rfloor} \tilde{X}_{t,s} \tag{6.6}$$

and

$$\mathcal{A}_t \leq 1 + \sum_{s=2}^{\lfloor \frac{t+1}{2} \rfloor} (\mathcal{A}_{t,s} - 1). \tag{6.7}$$

Moreover, for $3 \leq t \leq 11$, first bound is tight.

Proof. Straightforward from Theorem 98. $\mathcal{QED}$

This last result improves the partial classification given in Section 4.2, since it gives a better bounds for $\mathcal{A}_t$. It is easy to see that (6.6) is a better upper bound than (4.4) since $\tilde{X}_{t,s} \leq X_{t,s}$, for all t and $s \in \{2, \ldots, t-2\}$, and also the amount of addends is lower. It is also trivial to see that (6.7) is a better bound than (4.5) since the amount of addends is lower.

Chapter 7

Conclusions

"Even the very wise cannot see all ends."
–J. R. R. Tolkien, Gandalf, The Lord of the Rings, The Fellowship of the Ring

7.1 Summary

In [HKC+94], a linear structure over $\mathbb{Z}_4$ is provided for some families of non-linear binary codes such that Kerdock, Preparata, Goethal and related codes. Later, in [Kro01, PRV06], also the well-known family of binary Hadamard codes having a linear structure over $\mathbb{Z}_4$ are studied and classified. The main goal of this dissertation is to generalize this research line. We consider a family of the binary Hadamard codes having linear structures over $\mathbb{Z}_{2^s}$ constructed in [Kro07] and study their classification by using two invariants, the rank and dimension of the kernel.

In Chapters 1 and 2, we contextualize the research presented in this dissertation. We also give basic concepts and previous known results on binary codes, binary Hadamard codes, rank and kernel of binary codes, $\mathbb{Z}_{2^s}$-linear codes, and generalized Gray maps.

Later, in Chapter 3, we give a recursive construction of the generator matrices with minimum number of rows of the $\mathbb{Z}_{2^s}$-additive Hadamard codes. We also show that the Gray map images of the constructed codes, called

$\mathbb{Z}_{2^s}$-linear Hadamard codes, are, in fact, binary Hadamard codes. We also determine for which types the $\mathbb{Z}_{2^s}$-linear Hadamard codes are linear.

In Chapter 4, the kernel of $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t has been studied for $s > 2$. We compute the kernel of these codes and its dimension in order to classify them. In general, we have seen that we cannot completely classify these codes by using only the dimension of the kernel, once t and s are fixed. Nevertheless, we have determined for wich values of $t \leq 11$ and any s, we can use this invariant to distinguish between nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t. Computationally, for these values of t and s, we have also shown that the rank is enough to classify them. Finally, we have established some bounds for the exact number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, when both t and s are fixed, and also when just t is fixed; denoted by $\mathcal{A}_{t,s}$ and $\mathcal{A}_t$, respectively. Again, computationally, we have provided their exact values for $t \leq 11$.

In Chapter 5, we focus on $s = 3$. We study the rank of the $\mathbb{Z}_8$-linear Hadamard codes of length 2^t, giving an explicit construction of the linear independent vectors that generate the span. We observe that the rank, by itself, is not enough to obtain a complete classification. The first value of t for which the rank does not classify is $t = 17$. However, we prove that the full classification is possible by using both of the invariants, the rank and dimension of the kernel. We also provide the amount of nonequivalent $\mathbb{Z}_8$-linear Hadamard codes of length 2^t for a given t. Finally, we show that all the generated $\mathbb{Z}_4$-linear Hadamard codes are permutation equivalent to a $\mathbb{Z}_8$-linear Hadamard code except the codes of type $(n; t_1, 0)$ with $t_1 \geq 3$.

The results presented in Chapter 6 allow us to improve the partial classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, given in Chapter 4 and obtained by using the rank and dimension of the kernel, once t is fixed. Specifically, we establish that there are some families of such codes which are equivalent. This result permit us to give a new upper bound on the number of nonequivalent such codes, once t is fixed. Moreover, we have that this upper bound coincides with the lower bound and is tight for any $3 \leq t \leq 11$.

7.2 Future research

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

- The $\mathbb{Z}_4$-linear Hadamard codes can be classified by using just the dimension of the kernel [Kro01]. Establish for which values of t and s, the dimension of the kernel is enough to classify the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t. From the results up to $t = 11$, given in Chapter 4, we conjecture that only for any $t \geq 8$ and $s \in \{2, t-4, t-3, t-2\}$ the dimension of the kernel can be used to classify all $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t once we fix s and t.

- For $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, with $t \leq 11$, we have seen that the dimension of the kernel belongs to $\{3, ..., t-1, t+1\}$ if t is odd, and it belongs to $\{4, \ldots, t-1, t+1\}$ if t is even. Establish whether this fact is also true for any fixed t. Moreover, prove that there exists a $\mathbb{Z}_{2^s}$-linear Hadamard code having any possible dimension of the kernel.

- In Chapter 5, a basis of the span and its dimension, the rank, for the $\mathbb{Z}_8$-linear Hadamard codes, in terms of the type of the code, are computed. This result for $\mathbb{Z}_4$-linear Hadamard codes is given in [PRV06]. Generalize these results for the $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s \geq 4$.

- In case that an explicit formula for the rank of the $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s \geq 4$ is not found, compute the values for such codes when $t \geq 12$ and $s \geq 4$. Up to $t = 11$, these values have been found by using Magma [BCFS16] and our own developed functions. When $t \geq 12$, it takes too long, so it is necessary to use another approach to speed up the computations.

- The $\mathbb{Z}_4$-linear Hadamard codes can be classified by using just the rank [PRV06]. From the formula that gives the rank of the $\mathbb{Z}_8$-linear Hadamard codes, given in Chapter 5, we have that this invariant allows us to classify these codes for any $t \leq 16$; and it is not possible for

$t = 17$. Determine for which values of $t \geq 18$, the rank is enough to classify them. In general, determine for which values of t and $s \geq 3$, the rank classifies all $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t once we fix s and t.

- There are values of t and s for which neither the dimension of the kernel nor the rank, independently, can be used to classify $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t; for example, for $t = 17$ and $s = 3$. However, in Chapter 5, we have shown that for any t and $s = 3$, the classification is possible by using both invariants. Prove that it is also possible for any t and $s \geq 4$ or find counterexamples in this direction.

- Recall that $\mathcal{A}_{t,s}$ is the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t. An explicit expression for $s = 2$ is given in [Kro01]. In Chapter 4, an upper bound for $\mathcal{A}_{t,s}$ is established. Moreover, computationally, the exact values for any $t \leq 11$ and $s \geq 3$, which coincide with the upper bound, have been found. Determine an explicit expression for $\mathcal{A}_{t,s}$ for any t and $s \geq 3$.

- Recall that $\mathcal{A}_t$ is the number of nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t with any $s \geq 2$. When only t is fixed, we have seen that it is necessary to take into account the rank and dimension of the kernel to distinguish between nonequivalent $\mathbb{Z}_{2^s}$-linear Hadamard codes of the same length. A lower bound for $\mathcal{A}_t$ considering these two invariants can be defined. Computationally, the exact values for any $t \leq 11$, which coincide with this lower bound, have been determined in Chapter 6. An upper bound is also given from the number of different nonlinear such codes. Improve these bounds or determine an explicit expression for $\mathcal{A}_t$ for any t.

- In Chapter 5, we have shown that $\mathbb{Z}_4$-linear Hadamard codes of length 2^t, $t \geq 5$, and type $(n; t_1, t_2) = (2^{t-1}; (t+1)/2, 0)$ are not equivalent to any $\mathbb{Z}_8$-linear Hadamard code. Note that in this case t is odd and $t_1 > 1$. Later, in Chapter 6, we have seen that $\mathbb{Z}_{2^s}$-linear Hadamard codes of type $(n; t_1, \cdots, t_s)$ with $t_1 > 1$ and $t_s = 0$ are not equivalent

to any other $\mathbb{Z}_{2^{s'}}$-linear Hadamard code with $s \neq s'$ for $t \leq 11$. Find for which types $(n; t_1, \ldots, t_s)$ the code is not equivalent to any other $\mathbb{Z}_{2^{s'}}$-linear Hadamard code of the same length.

- Establish whether all $\mathbb{Z}_{2^s}$-linear Hadamard codes of the same length, having the same rank and dimension of the kernel, are equivalent. This is equivalent to prove whether it is enough to use both invariants to classify all $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, once t is fixed. In this dissertation, we have seen that this fact is true for t up to $t = 11$.

- Show all equivalence relations among the $\mathbb{Z}_{2^s}$-linear Hadamard codes considered in this dissertation, that is, the ones obtained from the Carlet's Gray map. This map is a particular case of the Krotov's generalization of the Gray map [Kro07]. Consider other families of $\mathbb{Z}_{2^s}$-linear Hadamard codes obtained from a Krotov's Gray map, and establish whether there exist nonequivalent nonlinear Hadamard codes in the new families. Compare the new families with the one studied in this dissertation to determine whether there are other $\mathbb{Z}_{2^s}$-linear Hadamard codes that are not equivalent to those obtained as images of the Carlet's Gray map.

- The classification of all $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes of length 2^t with $\alpha \neq 0$ is given in [PRV06]. In [KV15], it is shown that each $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code with $\alpha \neq 0$ is equivalent to a $\mathbb{Z}_4$-linear Hadamard code, except the one of type $2^1 4^\delta$ as a group when $t = 2\delta$ is even. In Chapter 4, through an example, we have seen that these $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes for $t \in \{4, 6, 8, 10\}$ are not equivalent to any $\mathbb{Z}_{2^s}$-linear Hadamard code with $s \geq 3$. Prove whether this is also true for any $t \geq 12$ even.

- In [BBFV15], a permutation decoding algorithm is described for $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, and in particular for $\mathbb{Z}_4$-linear ones. In [BV15, BV16a], PD-sets with minimum number of elements were given, to perform a partial permutation decoding for some families of $\mathbb{Z}_4$-linear codes, including $\mathbb{Z}_4$-linear Hadamard codes. Generalize these results describing

a permutation decoding algorithm for $\mathbb{Z}_{2^s}$-linear codes and finding PD-sets for the ones that are Hadamard. In a more general approach, find other efficient decoding algorithms for $\mathbb{Z}_{2^s}$-linear codes in general, and for $\mathbb{Z}_{2^s}$-linear Hadamard codes in particular.

- All computational results given in this dissertation have been done using the computer algebra system Magma [BCFS16]. We have also used some functions from the packages [PPV12, PV17], which are for linear codes over $\mathbb{Z}_4$ and for nonlinear codes over finite fields, respectively. New functions to deal with $\mathbb{Z}_{2^s}$-additive codes and their corresponding Gray map images, based on these packages, have been implemented. Complete these functions in order to develop a new Magma package for these codes.

- In [SWK18], the results given in [Kro07] are generalized. Specifically, the authors show that, considering two different generalized Gray maps ϕ and φ, if C is a $\mathbb{Z}_p\mathbb{Z}_{p^s}$-additive code and $C^\perp$ its dual, the weight enumerators of $\phi(C)$ and $\varphi(C^\perp)$ are formally dual. Moreover, they prove the existence of 1-perfect codes over mixed alphabets of the form $\mathbb{Z}_p\mathbb{Z}_{p^2}\cdots\mathbb{Z}_{p^s}$. Classify, and obtain similar results to the ones given in this dissertation, for the dual of these 1-perfect codes codes over the mixed alphabets, which represent generalized Hadamard codes over $\mathbb{Z}_p$.

Bibliography

[AAF+09] V. Álvarez , J. A. Armario, M. D. Frau, and P. Real "The homological reduction method for computing cocyclic Hadamard matrices," *Journal of Symbolic Computation*, vol. 44, pp. 558–570, 2009.

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

[AA09] N. Aydin and T. Asamov, "A database of $\mathbb{Z}_4$ codes," *Journal of Combinatorics, Information and System Sciences*, vol. 34, nos. 1–4, pp. 1–12, 2009. `http://Z4Codes.info/`.

[AS13] I. Aydogdu and I. Siap, "The structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes: bounds on the minimum distance," *Appl. Math. Inf. Sci.*, vol. 7, no. 6, pp. 2271–2278, 2013.

[AS14] I. Aydogdu and I. Siap, "On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes," *Linear and Multilinear Algebra*, vol. 63, pp. 2089–2102, 2014.

[BDH+99] E. Bannai, S. T. Dougherty, M. Harada, and M. Oura, "Type II codes, even unimodular lattices, and invariant rings," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1194–1205, 1999.

[BV15] R. D. Barrolleta and M. Villanueva, "PD-sets for (nonlinear) Hadamard $\mathbb{Z}_4$-linear codes," in Proc. of the *21st Conference on Aplications of Computer Algebra (ACA 2015)*, Kalamata, Greece, pp. 135–139, 20–23 July 2015.

[BV16a] R. D. Barrolleta and M. Villanueva, "Partial permutation decoding for binary linear and $\mathbb{Z}_4$-linear Hadamard codes," *Designs, Codes and Cryptography*, vol. 86, no. 3, pp. 569-586, 2017.

[BV16c] R. D. Barrolleta and M. Villanueva, "Partial permutation decoding for several families of $\mathbb{Z}_4$-linear codes,' to appear in *IEEE Trans. Inf. Theory*, 2018. DOI:10.1109/tit.2018.2840226

[BGH83] H. Bauer, B. Ganter, and F. Hergert, "Algebraic techniques for nonlinear codes," *Combinatorica*, vol. 3, no. 1, pp. 21–33, 1983.

[BBFV15] J. J. Bernal, J. Borges, C. Fernández-Córdoba, and M. Villanueva, "Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes," *Designs, Codes and Cryptography*, vol. 76, no. 2, pp. 269–277, 2015.

[BGL05] M. C. Bhandari, M. K. Gupta, and A. K. Lal, "On linear codes over $\mathbb{Z}_{2^s}$," *Designs, Codes and Cryptography*, vol. 36, no. 3, pp. 227–244, 2005.

[Bla72] I. F. Blake, "Codes over certain rings," *Information and Control,* vol. 20, pp. 396–404, 1972.

[Bla75] I. F. Blake, "Codes over integer residue rings," *Information and Control,* vol. 29, no. 4, pp. 295–300, 1975.

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

[BFP+14] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, "Survey on $\mathbb{Z}_2\mathbb{Z}_4$-additive codes," in Proc. of the *Contact Forum Galois Geometries and Applications*. Royal Flemish Academy of Belgium for Science and the Arts (October 5, 2012), pp. 19–67, 2014.

[BFP05] J. Borges, C. Fernández-Córdoba, and K. T. Phelps, "Quaternary Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2686–2691, 2005.

[BFP08] J. Borges, C. Fernández-Córdoba, and K. T. Phelps, "ZRM codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 380–386, 2008.

[BFR01] J. Borges, C. Fernández and J. Rifà, *Every $\mathbb{Z}_{2k}$-code is a binary propelinear code*, in "COMB'01. Electronic Notes in Discrete Mathematics," **10** (2001), Elsevier Science.

[BFR09] J. Borges, C. Fernández and J. Rifà, *Propelinear structure of $\mathbb{Z}_{2k}$-linear codes*, arXiv:0907.5287, 2009

[BPR03] J. Borges, K. T. Phelps, and J. Rifà, "The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear and additive non-$\mathbb{Z}_4$-linear codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 8, pp. 2028–2034, 2003.

[BPRZ03] J. Borges, K. T. Phelps, J. Rifà, and V. Zinoviev, "On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2834–2843, 2003.

[BCFS16] W. Bosma, J. J. Cannon, C. Fieker, and A. Steel (eds.), *Handbook of Magma functions*, Edition 2.22 (2016) 5669 pages. `http://magma.maths.usyd.edu.au/magma/`.

[Car91] C. Carlet, "The automorphism group of Kerdock codes," *Journal of Information and Optimization Sciences*, vol. 12, pp. 378–400, 1991.

[Car98] C. Carlet, "$\mathbb{Z}_{2^k}$-linear codes," *IEEE Trans. Inf. Theory*, vol. 44, pp. 1543–1547, 1998.

[Cat12] P. Ó Catháin, "Different sets and doubly transitive actions on Hadamard matrices," *Journal of Combinatorial Theory*, vol. 119, no. 6, pp. 1235–1249, 2012.

[Dou17] S. T. Dougherty, *Algebraic Coding Theory Over Finite Commutative Rings*, Springer, 2017.

[DF11] S. T. Dougherty and C. Fernández-Córdoba, "Codes over $\mathbb{Z}_{2^k}$, Gray map and self-dual codes," *Adv. in Math. of Commun.*, vol. 5, no. 4, pp. 571–588, 2011.

[DRV15] S. T. Dougherty, J. Rifà, and M. Villanueva, "Ranks and kernels of codes from generalized Hadamard matrices," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 687–694, 2016.

[ER14] T. Etzion and N. Raviv, "Equidistant codes in the Grassmannian," *Discrete Applied Mathematics*, vol. 186, pp. 87–97, 2015.

[FPV08] C. Fernández-Córdoba, J. Pujol, and M. Villanueva, "On rank and kernel of $\mathbb{Z}_4$-linear codes," *Lecture Notes in Computer Science*, vol. 5228, pp. 46–55, 2008.

[FPV10] C. Fernández-Córdoba, J. Pujol, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel," *Designs, Codes and Cryptography*, vol. 56, no. 1, pp. 43–59, 2010.

[FVV16] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "Construction and classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes," *Electronic Notes in Discrete Mathematics*, vol. 54, pp. 247–252, 2016.

[FVV17] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On the kernel of $\mathbb{Z}_{2^s}$-linear Hadamard codes," in Proc. of the *5th International Castle Meeting on Coding Theory and Applications, ICMCTA 2017. Lecture Notes in Computer Science*, vol. 10495, pp. 107–117, 2017.

[FVV18a] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On the rank of $\mathbb{Z}_8$-linear Hadamard codes," in Proc. of the *2nd IMA Conference on Theoretical and Computational Discrete Mathematics.* To apperar in *Electronic Notes in Discrete Mathematics*, 2018.

[FVV18b] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On $\mathbb{Z}_{2^s}$-linear Hadamard codes: kernel and partial classification," to appear in *Designs, Codes and Cryptography*, 2018. DOI :10.1007/s10623-018-0546-6.

[FVV18c] C. Fernández-Córdoba, C. Vela, and M. Villanueva, "On $\mathbb{Z}_8$-linear Hadamard codes: rank and classification," *Submitted to IEEE Trans. Inf. Theory*, 2018.

[Fla97] D. L. Flannery, "Cocyclic Hadamard matrices and Hadamard groups are equivalent," *Journal of Algebra*, vol. 192, pp. 47–61, 1997.

[Gab85] E. Gabidulin, "Theory of codes with maximal rank distance (translation)," *Problems of Information Transmission,* vol. 21, pp. 1–12, 1985.

[GR16] E. G. Gorla and A. Ravagnani, "Equidistant subspace codes," *Linear Algebra and its Applications,* vol. 490, pp. 48–65, 2016.

[Gra09] M. Grassl, "Code tables: bounds on the parameters of various types of codes," online available at `http://www.codetables.de`. Accessed on 2016-09-18.

[Had1893] J. Hadamard, "Resolution d'une question relative aux determinants," *Bull. des Sciences Mathematiques,* vol. 17, pp. 240–246, 1893.

[Ham50] R. W. Hamming, "Error detecting and error correcting codes," *Bell Syst. Tech. J.*, vol. 29, pp. 147–160, 1950.

[HKC+94] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, 1994.

[HS79] M. Harwit and N. J. A. Sloane, *Hadamard Transform Optics*, Elsevier, Academic Press, Sydney, 1979.

[Her12] A. Herbert, "A neural architecture based on Hadamard designs," *The Open Neuroscience Journal*, vol. 6, pp. 1–9, 2012.

[Hor07] K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, U.S.A., 2007.

[Huf98] W. C. Huffman, *Codes and Groups,* Handbook of Coding Theory, (V. S. Pless and W. C. Huffman, eds.), Elsevier, 1998.

[HP03] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[Ito94] N. Ito, "On Hadamard groups II," *Journal of Algebra*, vol. 169, pp. 936–942, 1994.

[Ito96] N. Ito, "Remarks on Hadamard groups," *Kyushu J. Math.*, vol. 50, pp. 1–9, 1996.

[Jai89] A. A. Jain, *Fundamentals of Digital Image Processing*, Prentice-Hall, Englewood Cliffs, 1989.

[KT05] H. Kharaghani and B. Tayfeh-Rezaie, "A Hadamard matrix of order 428," *Journal of Combinatorial Designs*, vol. 13, no. 6, pp. 435–440, 2005.

[KWZ16] M. Kiermaier, A. Wassermann, and J. Zwanzger, "New upper bounds on binary linear codes and a $\mathbb{Z}_4$-code with a better-than-linear Gray image," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 6768–6771, 2016.

[KZ13] M. Kiermaier and J. Zwanzger, "New ring-linear codes from dualization in projective Hjelmslev geometries," *Designs, Codes and Cryptography*, vol. 66, nos. 1–3, pp. 39–55, 2013.

[KB73] B. R. Kowalski and C. F. Bender "The Hadamard transform and spectral analysis by pattern recognition," *Anal. Chem.*, vol. 45, no. 13, pp. 2234–2239, 1973.

[Kro01] D. S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes," *Electronic Notes in Discrete Mathematics*, vol. 6, pp. 107–112, 2001.

[Kro07] D. S. Krotov, "On $\mathbb{Z}_{2^k}$-dual binary codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 4, pp. 1532–1537, 2007.

[KV15] D. S. Krotov and M. Villanueva, "Classification of the $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes and their automorphism groups," *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 887–894, 2015.

[LT94] A. W. Lam and S. Tantaratana, *Theory and Applications of Spread Spectrum Systems*, IEEE/EAB Self-Study Course, IEEE Inc., Piscataway, 1994.

[Lam13] L. Lambert, *Random Network Coding and Designs over* $\mathbb{F}_q$, Master dissertation, Ghent University, 2013. `http://www.network-coding.eu/pubs/Thesis-Lien.pdf`.

[LFH00] W. De Launey, D. L. Flannery, and K. J. Horadam "Cocyclic Hadamard matrices and different sets," *Discrete Applied Mathematics*, vol. 120, pp. 47–61, 2000.

[LRS99] S. Litsyn, R. M. Rains, and N. J. A. Sloane, "Table of nonlinear binary codes," online available at `http://www.eng.tau.ac.il/ litsyn/tableand/`. Accessed on 2016-09-18.

[MS77] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, U.S.A., 1977.

[MR15] P. Montolio and J. Rifà, "Construction of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes for each allowable value of the rank and dimension of the kernel," *IEEE Trans. Inf. Theory*, vol. 61, no. 4, pp. 1948–1958, 2015.

[PPV11] J. Pernas, J. Pujol, and M. Villanueva, "Classification of some families of quaternary Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 6043–6051, 2011.

[PPV12] J. Pernas, J. Pujol, and M. Villanueva, "Codes over $\mathbb{Z}_4$. A MAGMA package," version 2.1, Universitat Autònoma de Barcelona, 2017. `http://ccsg/uab.cat`.

[PRV05] K. T. Phelps, J. Rifà, and M. Villanueva, "Rank and kernel of binary Hadamard codes," *IEEE Trans. Inf. Theory*, vol. 51, pp. 3931–3937, 2005.

[PRV06] K. T. Phelps, J. Rifà, and M. Villanueva, "On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: rank and kernel," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 316–319, 2006.

[PRS09] J. Pujol, J. Rifà, and F. I. Solov'eva, "Construction of $\mathbb{Z}_4$-linear Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 99–104, 2009.

[PV17] J. Pujol and M. Villanueva, "Q-ary codes. A MAGMA package," version 1.0, Universitat Autònoma de Barcelona, 2017. `http://ccsg/uab.cat`.

[RSV09] J. Rifà, F. I. Solov'eva, and M. Villanueva, "On the intersection of $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1766–1774, 2009.

[RS14] J. Rifà and E. Suarez, "About a class of Hadamard propelinear codes," *Electronic Notes in Discrete Mathematics*, vol. 46, pp. 289–296, 2014.

[RS17] J. Rifà and E. Suarez, "Hadamard full propelinear codes of type Q; rank and kernel," *Designs, Codes and Cryptography*, vol. 86, pp. 1905–1921, 2018.

[RR13] A. del Rio and J. Rifà, "Families of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 5140–5151, 2013.

[Sha48] C. E. Shannon, "A mathematical theory of communications," *Bell System Technical Journal*, vol. 27, pp. 379–423 and 623–656, 1948.

[SWK18] M. Shi, R. Wu, and D. S. Krotov, "On $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive codes and their duality," *arXiv:1809.00008 [cs.IT]*, 2018.

[Syl1867] J. J. Sylvester, "Thoughts on inverse orthogonal matrices, simultaneous sign successions and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tile work and the theory of numbers," *Phil. Mag.*, vol. 34, pp. 461–475, 1867.

[TV03] H. Tapia-Recillas and G. Vega, "On $\mathbb{Z}_{2^k}$-linear and quaternary codes," *SIAM J. Discrete Math.*, vol. 17, no. 1, pp. 103–113, 2003.

[TMB+11] A. L. Trautmann, F. Manganiello, and J. Rosenthal, "Orbit codes - a new concept in the area of network coding," in Proc. of the *2010 IEEE Information Theory Workshop (ITW 2010),* Dublin, Ireland, pp. 1-4, 2010.

[Wal23] J. L. Walsh, "A closed set of normal orthogonal functions," *American Journal of Mathematics*, vol. 55, pp. 5-24, 1923.

[Wan97] Z.-X. Wan, *Quaternary Codes*, World Scientific, Singapore, 1997.

[Zen14] F. Zeng, *Nonlinear Codes: Representation, Constructions, Minimum Distance Computation and Decoding*, PhD Thesis, Universitat Autònoma de Barcelona, 2014.

Carlos Vela Cabello
Cerdanyola del Vallès, September 2018