Universitat Autònoma de Barcelona

Departament d Enginyeria de la Informació i de les Comunicacions

ON ADDITIVE BINARY NONLINEAR CODES AND STEGANOGRAPHY

SUBMITTED TO UNIVERSITAT AUTÒNOMA DE BARCELONA
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
Doctor of Philosophy
IN COMPUTER SCIENCE

by Lorena Ronquillo Moreno
Bellaterra, February 2012
supervised by
Dr. Josep Rifà Coma

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

Bellaterra, February 2012

Dr. Josep Rifà Coma
(Adviser)

Committee:

Dr. Marcus Greferath
Dr. Llorenç Huguet
Dr. Mercè Villanueva
Dr. Ángel del Río (substitute)
Dr. Leo Storme (substitute)

A todas aquellas personas
que iluminan nuestras vidas
con su alegría y cariño.

Abstract

A code $\mathcal{C}$ is said to be $\mathbb{Z}_2\mathbb{Z}_4$-additive if its coordinates can be partitioned into two subsets X and Y, in such a way that the punctured code of $\mathcal{C}$ obtained by removing the coordinates outside X –or, respectively, Y– is a binary linear code –respectively, a quaternary linear code–. The Gray map image of $\mathcal{C}$ is a binary and often nonlinear code called $\mathbb{Z}_2\mathbb{Z}_4$-linear code. In this dissertation, new families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are presented, with the particularity that their Gray map images are $\mathbb{Z}_2\mathbb{Z}_4$-linear codes having the same parameters and properties as the well-known family of binary linear Reed-Muller codes. Considering the class of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, which are known to be completely regular, we have used the extension, puncture, shorten and lifting constructions, and studied the uniformly packed condition and completely regularity of the obtained codes. Besides providing reliability in communication channels, coding theory has been recently applied to steganography, i.e., the science of hiding sensitive information within an innocuous-looking message –the cover object– in such a way that third parties cannot detect that information. This hiding process has been addressed in the literature either by distorting the least signi cant bit of symbols in the cover object to transmit the secret message (binary steganography), or by distorting the two least signi cant bits (± 1-steganography). With respect to ± 1-steganography, two new embedding methods based on perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are introduced, achieving a higher embedding rate for a given distortion than previous methods; while another method, based on the product of more than two perfect q-ary Hamming codes, is presented conforming to binary steganography.

Un codi $\mathcal{C}$ rep el nom de $\mathbb{Z}_2\mathbb{Z}_4$-additiu si les seves coordenades es poden dividir en dos subconjunts X i Y, de tal manera que el codi punctured de $\mathcal{C}$, obtingut en eliminar

les coordenades que no es troben a X –o, respectivament, a Y– és un codi binari lineal –respectivament, un codi quaternari lineal–. La imatge del mapa de Gray de $\mathcal{C}$ és un codi binari i, sovint, no lineal, que s anomena $\mathbb{Z}_2\mathbb{Z}_4$-lineal. Aquesta tesi presenta noves famílies de codis $\mathbb{Z}_2\mathbb{Z}_4$-additius, amb la particularitat que les seves imatges de Gray són codis $\mathbb{Z}_2\mathbb{Z}_4$-lineals que tenen els mateixos paràmetres i propietats que la coneguda família de codis de Reed-Muller binaris i lineals. També, tot considerant la classe de codis perfectes $\mathbb{Z}_2\mathbb{Z}_4$-lineals, els quals se sap que són completament regulars, es fan servir les construccions d extensió, puncture, shorten i lifting, i s estudia si els codis obtinguts són uniformement empaquetats o completament regulars. A més de proporcionar abilitat en els canals de comunicació, la teoria de codis s ha aplicat recentment a l esteganogra a, és a dir, a la ciència d ocultar informació con dencial dins d altres missatges, aparentment inofensius –l objecte recobridor–, de manera que terceres parts no puguin detectar l esmentada informació. Aquest procés s ha plantejat a la literatura modi cant el bit menys signi catiu dels símbols de l objecte recobridor per transmetre el missatge secret (esteganogra a binària), o bé modi cant els dos bits menys signi catius (± 1-esteganogra a). Respecte a la ± 1-esteganogra a, s exposen dos nous mètodes d embedding basats en codis perfectes $\mathbb{Z}_2\mathbb{Z}_4$-lineals, que assoleixen una taxa d embedding més alta que amb altres mètodes ja coneguts, per una distorsió donada; mentre que es presenta un altre mètode, basat en el producte de dos o més codis de Hamming q-aris, conforme a l esteganogra a binària.

Un código $\mathcal{C}$ recibe el nombre de $\mathbb{Z}_2\mathbb{Z}_4$-aditivo si sus coordenadas se pueden dividir en dos subconjuntos X e Y, tales que el código punctured de $\mathcal{C}$, obtenido a partir de eliminar las coordenadas que no están en X –o, respectivamente, en Y– es un código binario lineal –respectivamente, un código cuaternario lineal–. La imagen del mapa de Gray de $\mathcal{C}$ es un código $\mathbb{Z}_2\mathbb{Z}_4$-lineal, que es un código binario y, a menudo, no lineal. En esta tesis se presentan nuevas familias de códigos $\mathbb{Z}_2\mathbb{Z}_4$-aditivos, con la particularidad de que sus imágenes a través del mapa de Gray son códigos $\mathbb{Z}_2\mathbb{Z}_4$-lineales con los mismos parámetros y propiedades que la conocida familia de códigos de Reed-Muller binarios y lineales. Considerando la clase de códigos perfectos $\mathbb{Z}_2\mathbb{Z}_4$-lineales, los cuales se sabe que son completamente regulares, se han utilizado las construcciones de extensión, puncture, shorten y lifting, y estudiado si los códigos obtenidos en cada caso eran uniformemente empa-

quetados o completamente regulares. Además de proporcionar abilidad en los canales de comunicación, la teoria de códigos se ha aplicado recientemente a la esteganografía, es decir, a la ciencia de ocultar información con dencial en otros mensajes, aparentemente inofensivos –el objeto recubridor– de tal manera que dicha información no pueda ser detectada por terceros. Este proceso se ha planteado en la literatura modi cando el bit menos signi cativo de los símbolos del objeto recubridor (esteganografía binaria), o bien modi cando los dos bits menos signi cativos (± 1-esteganografía). Con respecto a la ± 1-esteganografía, se exponen dos nuevos métodos de embedding basados en códigos perfectos $\mathbb{Z}_2\mathbb{Z}_4$-lineales, que alcanzan una tasa de embedding superior a la de otros métodos anteriores, para una distorsión dada; mientras que se presenta otro método, basado en el producto de dos o más códigos de Hamming q-arios, conforme a la esteganografía binaria.

Agraïments

Darrera d aquestes pàgines s amaguen una sèrie de persones que han fet possible aquesta tesi amb el seu suport i col·laboració, ja sigui implicant-se de manera directa, tot llegint-la, donant-me la seva opinió i oferint-me els seus millors consells, com de manera indirecta, tot recolzant-me, donant-me ànims o, simplement, essent al meu costat.

Vull donar les gràcies al meu director de tesi, el Dr. Josep Rifà, pel seu temps, la seva dedicació, per compartir els seus coneixements amb mi i, sobretot, per aquest optimisme que mai ha deixat de banda i tant he agraït quan no tot funcionava com ens hauria agradat.

Gràcies també als meus companys del departament d Enginyeria de la Informació i de les Comunicacions, en especial als companys becaris, que han fet d aquesta una experiència no només acadèmica, sinó també personal. M enduc d aquesta etapa, gràcies a vosaltres, molts bons records.

Finalment, voldria agrair a la meva família el seu suport incondicional, l amor i la comprensió que he rebut i rebo sempre, i que mai he trobat a faltar quan més ho he necessitat.

A tots, moltes gràcies.

Preface

This thesis describes much of the work that I conducted while completing my PhD degree at the Universitat Autònoma de Barcelona, in the Department of Information and Communications Engineering. It is presented as a compendium of publications, thus the most important contributions of this dissertation are appended to this document in the form of publications to conferences and/or journals. Despite of being a compendium, I have attempted to make this document as complete and self-contained as possible, by including some state of the art on Coding Theory and on Steganography.

As it is already common at the Combinatorics, Coding and Security Group (CCSG) where this thesis has been developed, the name of the authors of the contributions appended to this document appear in the corresponding documents in alphabetical order.

This work was nancially supported in part by the Spanish Government under grants MTM2006-03250, MTM2009-08435, TSI2006-14005-C02-01, PCI2006-A7-0616 and also by the *Comissionat per a Universitats i Recerca del DIUE de la Generalitat de Catalunya* and the *European Social Fund* with grants FI-DGR and 2009SGR1224.

Contents

Chapter 1

Introduction

A communication system can be modelled by a scheme consisting of a message source which transmits information to a receiver through a channel. Due to physical and engineering limitations, the output of the channel may differ from the input because of noise or manufacturing defects. If no modification is made to the message being sent and it is transmitted directly over the channel, this noise may distort the message and make it unrecoverable at the other end. This is where Coding Theory, and error-correcting codes in particular, come into play, providing mechanisms to detect, and even correct, most of these modifications or errors.

There exist several mathematical models that reflect the most important characteristics of the transmission medium. The simplest and more widely used model for the channel is the additive Gaussian noise channel, illustrated in Fig. 1.1. According to this model, the message $\mathbf{x}$ generated by the source is first encoded. This process results in a *codeword* $\mathbf{c}$, which is then sent over the channel, where noise in the form of vector $\mathbf{e}$ distorts it and produces a new message $\mathbf{y}$. The received vector $\mathbf{y}$ is then decoded and, finally, an estimate $\hat{\mathbf{x}}$ of the original message is produced, where we expect $\mathbf{x} = \hat{\mathbf{x}}$.

The above problem of communication was studied by Golay, Hamming and Shannon [Sha48] in the late 1940s. From that moment on, error-correcting codes have been applied in the transmission of images of planets from deep space, in compact discs, and in any kind of electronic communication device such as mobile

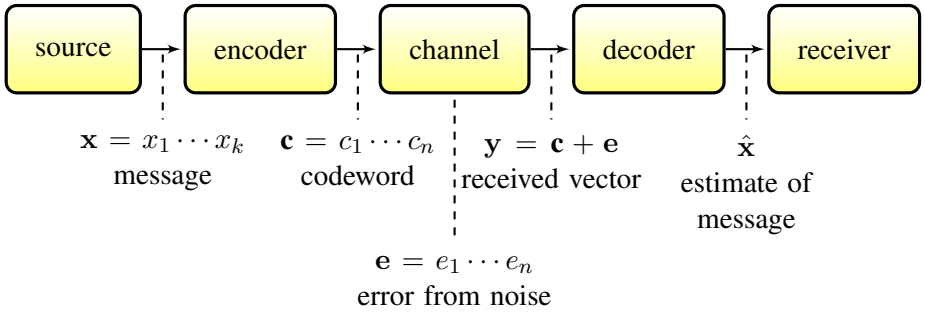

Figure 1.1: Additive Gaussian noise communication channel.

phones.

A code is a subset of words of a bigger space, whose elements are codewords. Historically, the most important codes were linear codes, that is, codes satisfying that the sum of any two codewords is also a codeword. Their importance lies on the fact that these codes have generator and parity check matrices that make them easy to be constructed, encoded and decoded. However, by no means they are the best class of codes. Indeed, there exist several binary nonlinear codes having twice as many codewords as any linear code with the same length and minimum distance. An example of this is the Nadler code [Nad62], which is a $[12, 5]$ systematic nonlinear code with covering radius $\rho = 4$ and minimum distance $d = 5$ [Lin82]. Despite of having better properties, it is not ef cient to work with this kind of codes because of being nonlinear. Fortunately, this dramatically changed after the contribution of Nechaev [Nec89] in 1989. In his work, some of these nonlinear codes were given an algebraic structure as linear codes over the ring $\mathbb{Z}_4$ of integers modulo four by means of the named *Gray map*, which made the correspondence between binary and quaternary coordinates. The term $\mathbb{Z}_4$*-linear code* was rst used to denote such a nonlinear binary code with an algebraic structure over $\mathbb{Z}_4$, whereas the codes de ned as subsets of $\mathbb{Z}_4$ were called *quaternary linear codes*. This result opened up a complete new direction in coding theory and many articles were published around this subject from that moment on.

An important contribution was the one from Hammons, Kumar, Calderbank,

Sloane and Solé [HKC$^+$94], who de ned several families of quaternary codes as well as the conditions under which some binary codes were $\mathbb{Z}_4$-linear codes.

Just as there are nonlinear binary codes which can be seen as quaternary linear codes through the inverse of the Gray map, there are also some nonlinear binary codes, known as $\mathbb{Z}_2\mathbb{Z}_4$-*linear codes*, to which an algebraic structure as subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ can be given. Codes with this structure are called $\mathbb{Z}_2\mathbb{Z}_4$-*additive codes* [BFCP$^+$10], and are binary linear codes when $\beta = 0$, and quaternary linear codes when $\alpha = 0$.

One of the simplest and most important families of linear codes are Reed-Muller codes RM. These codes are relatively easy to encode and decode using majority-logic circuits. In general, Reed-Muller codes are not $\mathbb{Z}_4$-linear codes but, throughout the years, several constructions of quaternary linear codes trying to generalize them have been presented. One of the goals of this dissertation is to construct new families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes such that their corresponding nonlinear binary images, through the Gray map, had the same parameters and fundamental properties as RM codes.

Let the sphere of radius ρ centred at the codewords of a given code be all those words in the space that are within distance ρ from the centre. These spheres are pairwise disjoint provided their radius is chosen small enough. Sometimes every word in the space will be contained in precisely one of these spheres of radius ρ. Any code for which the latter is true is said to be *perfect*. Some binary perfect codes have a $\mathbb{Z}_2\mathbb{Z}_4$-linear structure, that is, they are the binary image, through the Gray map, of some $\mathbb{Z}_2\mathbb{Z}_4$-additive code. These binary codes are referred to as *perfect* $\mathbb{Z}_2\mathbb{Z}_4$-*linear codes*.

There is a class of codes which also enjoy combinatorial, and often algebraic, symmetry akin to that observed in perfect codes, which is the class of *completely regular codes*. Indeed, perfect codes are also completely regular codes, and they have often been used to construct new families of completely regular q-ary codes [RZ06, RZ11]. Considering these previous results, we aim in this dissertation for the construction of new families of completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes from perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

This dissertation not only deals with coding theory, but also with a new application of coding theory, which has quite recently emerged: *steganography*. Along with watermarking and ngerprinting, steganography is a branch of the eld known as *data-hiding*, aimed at protecting sensitive information from third parties. Data-hiding techniques have the potential to play an important role in electronic commerce since they can be used to prevent illegal uses of digital information. In general terms, both watermarking and ngerprinting attempt to add suf cient metadata to a digital object to establish ownership, provenance, source, etc., in such a way that third parties cannot remove or replace these data. While these data can be somehow visible, as long as it is a robust mark, steganography is more concerned with hiding the very communication of the message. This is accomplished by hiding a secret message within an innocuous-looking message (the *cover object*), in such a way that just the intended sender and receiver involved in the communication process know its presence and are able to extract it. The cover object can be either an image, video, audio or text. Indeed, any electronic document with redundant or noisy data can be used as cover object, since the modi cation of this redundant data is expected to remain unnoticeable.

Given any steganographic scheme, the fewer changes it performs, the less chance that these modi cations will be detectable. However, it is also desirable to hide as much information as possible. Clearly, a trade off between both parameters must be found by the steganographer and, to this end, several metrics that evaluate steganographic schemes have been proposed in the literature. The ones we will mainly use are the *average distortion*, which measures the number of changes per symbol of the cover object, and the *embedding rate*, that indicates the amount of bits that can be hidden per symbol of the cover object.

Most steganographic problems can be posed in terms of coding theory, in particular, from the point of view of covering codes. While the most important parameter in error-correcting codes is the minimum distance d, which determines how many errors can be corrected by a given code, covering codes deal with the covering radius ρ, which is a parameter more related to the distribution of codewords in such a way that the above-mentioned spheres of radius ρ

centred at these codewords cover the whole space. Note that this description is somehow pointing to perfect codes as good candidates to construct good steganographic schemes. Binary and ternary perfect codes have been used in steganography [Cra98, Wes01, WvD05, FL07] and yielded good results with respect to the parameters of the steganographic scheme obtained. Thus another goal of this dissertation is the construction of a new steganographic scheme based on perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, as well as compare its performance against that from previous schemes.

The performance of the steganographic scheme based on perfect binary codes, known as the *matrix embedding method*, has been outperformed by a new steganographic scheme based on the product of perfect codes [RPR09]. If the previous goal of this dissertation is achieved, we expect to further improve it by designing a new steganographic scheme that uses the product of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

To sum up, the main goals of this dissertation are:

1. Constructing a new family of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes such that their image, through the Gray map, are binary codes, not necessarily linear, having the same parameters and fundamental properties as the binary linear RM codes.

2. Obtaining new completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes from previous perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

3. Designing a new steganographic scheme based on perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes that improves the performance, in terms of embedding rate and average distortion, of the existing schemes.

4. Constructing a new steganographic scheme based on the product of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes (depends on the achievement of goal 3).

This thesis is presented and organized as a compendium of publications. Because of the space constraints of most of the publications, the contributions appended to this document do not include many details nor a complete background

on the topic they deal with. It is for this reason that we found convenient to provide the appropriate background and introduce some of the main de nitions and techniques of Coding Theory and Steganography in Chapters 2 and 3, respectively. Moreover, the connection between the subject dealt in every section of these two chapters and the contributions related to it will be pointed out through the corresponding references. Chapter 4 reviews and summarizes the results of the publications making up this dissertation, shows the storyline that links them up, and discusses their relevance. Finally, Chapter 5 concludes this dissertation and proposes some future lines of research. A copy of all contributions comprising this compendium is provided at the end of this document, ordered by publication date.

Chapter 2

Coding Theory

In the current chapter we review the state of the art of some topics on combinatorial Coding Theory, and also give some basic de nitions and notation that will be helpful in the remainder of this dissertation. As well as covering classical topics such as binary codes or perfect codes, much coverage is included of recent techniques and de nitions related to the contributions appended to this document, which will assist the reader in understanding them. For an in-depth introduction to Coding Theory, the reader is referred to [Lin82, MS77, PHB98].

We start by providing a brief review on binary codes in Section 2.1, and on $\mathbb{Z}_2\mathbb{Z}_4$-additive codes in Section 2.2. Some of the most well-known constructions of new codes from old ones are studied in Section 2.3. Then, Section 2.4 is devoted to perfect codes, while Section 2.5 deals with completely regular codes. In Section 2.6 we gather some of the most remarkable results concerning the parameters and properties of binary linear Reed-Muller codes, and also about some families of quaternary Reed-Muller codes that have been proposed in several articles with the aim of generalizing them. Finally, a short review of some particular facts related to Galois elds and Galois rings is provided in Section 2.7.

2.1 Binary codes

Let $\mathbb{Z}_2^n$ denote the set of all vectors of length n over the field $\mathbb{Z}_2$ of integers modulo two. Any nonempty subset C of $\mathbb{Z}_2^n$ is a *binary code*, while a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code*. The dimension of a code is denoted by k and coincides with the dimension of the subspace C in $\mathbb{Z}_2^n$, thus the binary linear code C has $|C| = 2^k$ codewords.

The two most common ways to represent a linear code are with either a generator matrix or a parity check matrix, which are not unique matrices. A generator matrix G for a code C of length n and dimension k is any $k \times n$ matrix G for which the rows are a basis of C, i.e., $C = \{\mathbf{v}G \mid \mathbf{v} \in \mathbb{Z}_2^k\}$. Because of having this algebraic structure in the form of generator matrix or parity check matrix, linear codes have always been the most studied codes, since they are, in general, easier to describe, encode and decode than nonlinear codes. However, as briefly mentioned in Chapter 1, there are also some nonlinear codes, the named $\mathbb{Z}_4$-linear and $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, which also benefit from a certain algebraic structure, that have quite recently attracted great interest from the coding theory community. Section 2.2 studies them in more detail.

We will denote by $\mathbf{0}$ and $\mathbf{1}$ the all-zeroes and the all-ones vectors, respectively.

The number of nonzero coordinates in a vector $\mathbf{u} \in \mathbb{Z}_2^n$ is known as the *Hamming weight* $w_H(\mathbf{u})$ of $\mathbf{u}$, while the *Hamming distance* $d(\mathbf{u}, \mathbf{v})$ between two vectors $\mathbf{u}$, $\mathbf{v} \in \mathbb{Z}_2^n$ refers to the weight of their difference. One of the most important invariants of codes is the *packing radius* e, usually related to the error-correction capability of codes. The packing radius is computed by using the *minimum Hamming distance* d, which is the minimum value of $d(\mathbf{u}, \mathbf{v})$, for any $\mathbf{u}, \mathbf{v} \in C$ and $\mathbf{u} \neq \mathbf{v}$. The higher the minimum distance, the more errors the code can correct, since $e = \lfloor \frac{d-1}{2} \rfloor$. However, as we shall see, in the current dissertation we are not specially interested in the error-correcting capability of codes, but on how well they cover the space. Indeed, there are two traditional approaches in coding theory, known as *packing problem* and *covering problem*.

Given two integers n and ρ, let the *Hamming sphere* of radius ρ centred at

the codewords of a certain code of length n be all those vectors in the space that are within distance ρ from the centre. Intuitively, the packing problem consists of asking for the maximal number of non-intersecting Hamming spheres which can be placed in the n-dimensional Hamming space. Conversely, the covering problem is focused on looking for a code such that every vector in the space is contained in at least one of the spheres, i.e., the spheres cover the whole space. Such code is called a *covering code*.

Hence, it will be sometimes interesting to know how far a vector in the space can be from the closest codeword. For this purpose, and as a counterpart of the minimum distance, we can find the concept of *covering radius* ρ of a binary code C, defined as the maximum value of $d(\mathbf{v}, C) = \min_{\mathbf{x}\in C}\{d(\mathbf{v}, \mathbf{x})\}$, for any $\mathbf{v} \in \mathbb{Z}_2^n$. In terms of Hamming spheres, the covering radius ρ of a code C is the smallest integer such that the spheres with that radius centred at the codewords of C cover the whole space.

Given a binary linear code C of length n and dimension k, we can refer to the *cosets* (or *translates*) $C + \mathbf{v} = \{\mathbf{u} + \mathbf{v} \mid \mathbf{u} \in C\}$, for any $\mathbf{v} \in \mathbb{Z}_2^n$ and $\mathbf{v} \notin C$, which partition $\mathbb{Z}_2^n$ into 2^{n-k} sets of size 2^k. All vectors within the same coset $C + \mathbf{v}$ have the same syndrome, while the one (or ones) of minimum weight is called *leader of the coset*. The *weight of a coset* is the weight of the leader of that coset. Clearly, a code and its translates have the same covering radius.

For $\mathbf{u} = (u_1, \cdots, u_n)$, $\mathbf{v} = (v_1, \cdots, v_n) \in \mathbb{Z}_2^n$, the *inner product* between $\mathbf{u}$ and $\mathbf{v}$ is defined as $\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^{n} u_i v_i$. If $\langle \mathbf{u}, \mathbf{v} \rangle = 0$, then these vectors are called *orthogonal*. The *orthogonal code* of a binary code C, denoted by $C^{\perp}$, is the set of vectors which are orthogonal to all codewords of C. When C is a linear code, $C^{\perp}$ is called the *dual* of C. In this case, if C has length n and dimension k, then any generator matrix of $C^{\perp}$ has dimension $n - k$ and it is, at the same time, a parity check matrix H of C. This matrix H is useful to determine whether or not a vector $\mathbf{v} \in \mathbb{Z}_2^n$ belongs to C: it does if and only if $H\mathbf{v}^t = 0$, where t denotes transposition. The expression $H\mathbf{v}^t$ computes the named *syndrome* of $\mathbf{v} \in \mathbb{Z}_2^n$, thus we see that codewords are characterized by having syndrome 0.

Theorem 2.1.1 *[Del73b] Let C be a linear code with parity check matrix H.*

Then,

(i) The covering radius ρ of C is the weight of the coset of largest weight;

(ii) ρ is the smallest number t such that every nonzero syndrome is a combination of t or fewer columns of H, and some syndrome requires t columns.

Let A_i be the number of codewords of Hamming weight i in C. The set $\{A_0, \ldots, A_n\}$ is called the *weight distribution* of C. The *weight enumerator* of C is then de ned by the polynomial

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i,$$

which is an homogeneous polynomial of degree n in x and y.

According to the theorem below, the weight enumerator of the dual code $C^\perp$ of a binary linear code C is uniquely determined by a linear transformation of the weight enumerator of C, thus by just knowing the weight distribution of C, we can determine the weight distribution of $C^\perp$ without knowing speci cally the codewords of $C^\perp$ or anything else about its structure.

Theorem 2.1.2 *[MS77, Ch.5](MacWilliams identity) Let C be a binary linear code and $C^\perp$ its dual. Then,*

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

Two structural invariants for binary codes are the rank and the dimension of the kernel. In the case of nonlinear codes, these parameters tell us how far is the code from being linear. The *rank* of a binary code C, denoted by r_C, is the dimension of $\langle C \rangle$, which is the linear span of the codewords of C; while the *kernel* of a binary code C, denoted by $K(C)$, is the set of vectors that leave C invariant under translations, thus $K(C) = \{x \in \mathbb{Z}_2^n : C + x = C\}$. If C contains the all-zeros vector, then $K(C)$ is a binary linear subcode of C. Note that if C is a binary linear code, then the rank and the dimension of the kernel coincide with the dimension of the code C.

2.2 $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

The following definitions, related to quaternary codes, can be found in the results of Nechaev [Nec89] and of Hammons et al. [HKC+94], and they have been included here for the sake of completeness.

Let $\mathbb{Z}_4^N$ be the set of all vectors of length N over $\mathbb{Z}_4$. Any nonempty subset $\mathcal{C}$ of $\mathbb{Z}_4^N$ is called a *quaternary code*, which is said to be a *quaternary linear code* if it is a subgroup of $\mathbb{Z}_4^N$.

In contrast to binary codes, the metric used for quaternary codes is not the Hamming one, but the Lee metric. According to this metric, the elements of $\mathbb{Z}_4$ have the following Lee weights: $w_L(0) = 0$, $w_L(1) = w_L(3) = 1$ and $w_L(2) = 2$. The *Lee weight* $wt_L(\mathbf{u})$ of a vector $\mathbf{u} \in \mathbb{Z}_4^N$ is then the addition of the weights of its components, whereas the *Lee distance* $d_L(\mathbf{u}, \mathbf{v})$ between two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_4^N$ is defined as $d_L(\mathbf{u}, \mathbf{v}) = w_L(\mathbf{u} - \mathbf{v})$. The Gray map ϕ we shall see in (2.1) is an isometry between the Lee metric and the Hamming metric.

We proceed to review an important class of codes, first introduced by Borges et al. [BFCP+10], that generalizes both binary and quaternary linear codes and has been called $\mathbb{Z}_2\mathbb{Z}_4$-*additive codes*.

Let us consider the set of vectors in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, i.e., vectors with α binary coordinates and β quaternary coordinates. In general, any nonempty subgroup $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. Every $\mathbb{Z}_2\mathbb{Z}_4$-additive code corresponds to a binary code by means of the *extended Gray map*, defined as the map $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^n$, such that $\Phi(u_1, \ldots, u_\alpha | u_{\alpha+1}, \ldots, u_{\alpha+\beta}) = (u_1, \ldots, u_\alpha | \phi(u_{\alpha+1}), \ldots, \phi(u_{\alpha+\beta}))$, where $n = \alpha + 2\beta$, $(u_1, \ldots, u_\alpha, \ldots, u_{\alpha+\beta}) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, and $\phi(\cdot)$ is the usual Gray map

$$\begin{array}{rcl} \phi : \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_2^2 \\ 0 & \mapsto & 00 \\ 1 & \mapsto & 01 \\ 2 & \mapsto & 11 \\ 3 & \mapsto & 10. \end{array} \tag{2.1}$$

Clearly, $\mathbf{u} + \mathbf{v} = \Phi(\Phi^{-1}(\mathbf{u}) + \Phi^{-1}(\mathbf{v}))$, for any $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n$.

The weight of any vector in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ can be computed by adding the Hamming weight of the first α coordinates and the Lee weight of the last β coordinates. Moreover, the extended Gray map is a distance preserving mapping. Indeed, the Lee distance of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ of α binary coordinates and β quaternary coordinates coincides with the Hamming distance of the binary code $C = \Phi(\mathcal{C})$ of length $n = \alpha + 2\beta$.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is isomorphic to an abelian structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ has $|\mathcal{C}| = 2^\gamma 4^\delta$ codewords, from which $2^{\gamma+\delta}$ codewords have order two. This code $\mathcal{C}$ will from now on be referred to as a *$\mathbb{Z}_2\mathbb{Z}_4$-additive code of type* $(\alpha, \beta; \gamma, \delta)$, although in some cases we will also refer to it as a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where κ is the dimension of the binary linear code obtained by taking first the subcode of $\mathcal{C}$ containing all order-two codewords, and then deleting the β quaternary coordinates. The binary image $C = \Phi(\mathcal{C})$ will be called a *$\mathbb{Z}_2\mathbb{Z}_4$-linear code of type* $(\alpha, \beta; \gamma, \delta)$ (or type $(\alpha, \beta; \gamma, \delta; \kappa)$, if applicable). It is also worth pointing out that the binary code $C = \Phi(\mathcal{C})$ may be nonlinear. A natural question is to ask under which conditions the Gray image is linear. One criterion to determine this is given in Lemma 1.

Note that, indeed, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes can be seen as a generalization of binary and quaternary linear codes: a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with $\alpha = 0$ is a quaternary linear code, whereas a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with $\beta = 0$ is a binary linear code itself.

The *standard inner product* of $\mathbf{u} = (u_1, \ldots, u_\alpha | u_{\alpha+1}, \ldots, u_{\alpha+\beta})$ and $\mathbf{v} = (v_1, \ldots, v_\alpha | v_{\alpha+1}, \ldots, v_{\alpha+\beta})$, where $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, is defined as:

$$\langle \mathbf{u}, \mathbf{v} \rangle = 2\left(\sum_{i=1}^{\alpha} u_i v_i\right) + \sum_{j=\alpha+1}^{\alpha+\beta} u_j v_j \ \in \ \mathbb{Z}_4, \tag{2.2}$$

where computations are made considering zeroes and ones in the α binary coordinates as quaternary zeroes and ones, respectively (see [BFCP$^+$10]). Note that for the case $\alpha = 0$, the inner product is the usual one for quaternary vectors; while for $\beta = 0$, it is twice the usual one for binary vectors.

Lemma 1 *[BFCP$^+$10] Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. The $\mathbb{Z}_2\mathbb{Z}_4$-linear code*

$C = \Phi(\mathcal{C})$ is a binary linear code if and only if $2\langle \mathbf{u}, \mathbf{v}\rangle \in \mathcal{C}$, for all $\mathbf{u}, \mathbf{v} \in \mathcal{C}$.

By using the inner product (2.2), we can now de ne the $\mathbb{Z}_2\mathbb{Z}_4$-*additive dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, as the set of vectors which are orthogonal to all codewords of $\mathcal{C}$. Therefore, we have $|\mathcal{C}||\mathcal{C}^\perp| = 2^{\alpha+2\beta}$.

The binary image of $\mathcal{C}^\perp$, via the extended Gray map Φ, is a binary code $C_\perp = \Phi(\mathcal{C}^\perp)$ of length $n = \alpha + 2\beta$, which is called $\mathbb{Z}_2\mathbb{Z}_4$-*dual code* of C. When $\alpha = 0$, the code $\mathcal{C}^\perp$ is also called the *quaternary dual code* of $\mathcal{C}$, whereas $C_\perp$ is the $\mathbb{Z}_4$-*dual code* of C. Moreover, codes C and $C_\perp$ are formal duals since although they are not necessarily dual in the binary linear sense, the weight enumerator polynomial of $C_\perp$ is related to that of C by a generalization to nonlinear codes of the MacWilliams identity seen in Theorem 2.1.2.

Theorem 2.2.1 *[BFCP+10] Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$. The $\mathbb{Z}_2\mathbb{Z}_4$-additive dual code $\mathcal{C}^\perp$ is then of type $(\alpha, \beta; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$, where*

$$\begin{aligned}\bar{\gamma} &= \alpha + \gamma - 2\kappa,\\ \bar{\delta} &= \beta - \gamma - \delta + \kappa,\\ \bar{\kappa} &= \alpha - \kappa.\end{aligned}$$

Two $\mathbb{Z}_2\mathbb{Z}_4$-additive codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of the same length are said to be *monomially equivalent* if one can be obtained from the other by permuting the coordinates and, if necessary, changing the sign of some quaternary coordinates. If these $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, $\mathcal{C}_1$ and $\mathcal{C}_2$, differ just in one permutation of coordinates, then they are *permutation equivalent*.

Clearly, the abelian group $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is not a free module, thus a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta)$ may not have a basis. However, it turns out that every codeword can be uniquely expressible in the form

$$\sum_{i=1}^{\gamma} \lambda_i \mathbf{u}^{(i)} + \sum_{j=\gamma+1}^{\gamma+\delta} \mu_j \mathbf{v}^{(j)}, \tag{2.3}$$

where $\lambda_i \in \mathbb{Z}_2$ for $1 \leq i \leq \gamma$, $\mu_j \in \mathbb{Z}_4$ for $\gamma + 1 \leq j \leq \gamma + \delta$ and $\mathbf{u}^{(i)}$, $\mathbf{v}^{(j)}$ are vectors in $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$ of order two and order four, respectively (see [BFCP+10]).

The above γ different vectors $\mathbf{u}^{(i)}$ and δ different vectors $\mathbf{v}^{(j)}$ give us a generator matrix $\mathcal{G}$ for $\mathcal{C}$ which can be written as follows:

$$\mathcal{G} = \left(\begin{array}{c|c} B_2 & Q_2 \\ \hline B_1 & Q_1 \end{array} \right), \tag{2.4}$$

where B_2 and B_1 are binary matrices of size $(\gamma \times \alpha)$ and $(\delta \times \alpha)$, respectively; Q_2 is a $(\gamma \times \beta)$-matrix whose elements are in $\{0, 2\} \subset \mathbb{Z}_4$ and Q_1 is a quaternary $(\delta \times \beta)$-matrix with row vectors of order four. Refer to [BFCP+10] for further details.

We will focus on $\mathbb{Z}_2\mathbb{Z}_4$-additive codes with $\alpha \neq 0$ throughout the remaining sections of this dissertation. Moreover, we will talk about a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of type $(n, 0; k, 0)$ to refer to a binary linear code of length n and dimension k.

Finally, this section is concluded with a diagram (see Figure 2.1) showing the relationship between binary codes, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, $\mathbb{Z}_4$-linear codes and binary linear codes (or $\mathbb{Z}_2$-linear codes).

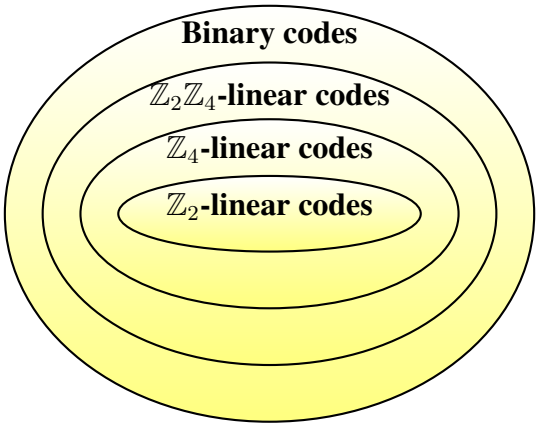

Figure 2.1: Relationship between codes.

2.3 Construction of new codes from old ones

In this section we review some of the most important ways to construct new binary codes by modifying existing ones. An extensive treatment of the following constructions can be found in [MS77, Ch.1].

We will start from a $\mathbb{Z}_2\mathbb{Z}_4$-linear code C of type $(n, 0; k, 0)$, minimum distance d, covering radius ρ, where G and H are, respectively, any of its generator and parity check matrices.

2.3.1 Puncturing codes

The binary linear code C can be *punctured* by deleting the same coordinate i in each codeword. The obtained code, denoted by $C^{(p)}$, is also linear, has length $n-1$, and its generator matrix $G^{(p)}$ can be constructed from the generator matrix G by deleting the column i and omitting any all-zeroes or duplicate rows that may occur. In general, each time a coordinate is deleted, the number of codewords remains unchanged.

Next theorem can be found in several surveys on coding theory such as [MS77], although we will consider $\mathbb{Z}_2\mathbb{Z}_4$-linear codes with $\beta = 0$ to refer to binary linear codes.

Theorem 2.3.1 *Let C be a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of type $(n, 0; k, 0)$, minimum distance d, and covering radius ρ. Let $C^{(p)}$ be the code C punctured on the i-th coordinate.*

i) When $d > 1$, code $C^{(p)}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of type $(n-1, 0; k, 0)$ and minimum distance $d' = d - 1$ if C has a minimum weight codeword with a nonzero i-th coordinate, or $d' = d$ otherwise.

ii) When $d = 1$, we have that $C^{(p)}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of type $(n-1, 0; k, 0)$ and minimum distance $d' = 1$ if C has no codeword of weight 1 whose nonzero entry is in coordinate i; otherwise, if $k > 1$, then $C^{(p)}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of type $(n-1, 0; k-1, 0)$ with minimum distance $d' \geq 1$.

iii) The covering radius of $C^{(p)}$ *is* ρ *or* $\rho - 1$.

In general, a code C can be punctured on the coordinate set T by deleting components indexed by that set from all codewords of C.

2.3.2 Extending codes

Extending a code means obtaining a longer code by adding a coordinate. The most common way to do so is by adding an overall parity check coordinate that makes all codewords to have even weight, that is, adding a 0 to those codewords of even weight, and a 1 to those of odd weight. Thus, the *extended* code $C^{(e)}$ is de ned as

$$C^{(e)} = \{(v_1, \ldots, v_{n+1}) \in \mathbb{Z}_2^{n+1} \mid (v_1, \ldots, v_n) \in C \text{ with } v_1 + \cdots + v_{n+1} = 0\}.$$

Clearly, given a binary linear code C of length n, the code $C^{(e)}$ is also linear, has length $n + 1$ and the same number of codewords as C. If ρ is the covering radius of C, then it is easy to see that the covering radius of $C^{(e)}$ is $\rho + 1$.

One can obtain the generator matrix $G^{(e)}$ of $C^{(e)}$ by adding a column to G so that the sum of coordinates of every row is 0. As for a parity check matrix $H^{(e)}$ of $G^{(e)}$, it can be obtained from H through the following construction:

$$H^{(e)} = \begin{pmatrix} 1 & \cdots & 1 \\ 0 & & \\ \vdots & \boxed{H} & \\ 0 & & \end{pmatrix}.$$

The extended code $C^{(e)}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of type $(n+1, 0; k, 0)$ and minimum distance $d' = d$ if d is even, or $d' = d + 1$ if d is odd.

Note that if we extend a code and then puncture the new coordinate, we end up obtaining the original code. However, performing the operations in the other way around yields, in general, a different code.

2.3.3 Shortening codes

Let T be any set of t coordinates, and let us consider the set of codewords in C which are 0 (sometimes we can also shorten a symbol different from 0) on the coordinates indexed by T. Clearly, this set is a subcode of C. Puncturing this subcode on the components indexed by T gives a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length $n-t$ called the *shortened code* on T, denoted by $C^{(s)}$. The procedure of shortening decreases the length as well as the number of codewords, but it does not lower the minimum distance. Moreover, note that if the deleted coordinate is not 0, this procedure can change a linear code to a nonlinear code, in general.

Again, we will consider $\mathbb{Z}_2\mathbb{Z}_4$-linear codes with $\beta = 0$ to refer to binary linear codes in next theorem.

Theorem 2.3.2 *[MS77] Let C be a $\mathbb{Z}_2\mathbb{Z}_4$-linear code of type $(n, 0; k, 0)$ and minimum distance d, and let T be a set of t coordinates. Then:*

i) $(C^{\perp})^{(s)} = (C^{(p)})^{\perp}$ *and* $(C^{\perp})^{(p)} = (C^{(s)})^{\perp}$.

ii) If $t < d$, then $C^{(p)}$ and $(C^{\perp})^{(s)}$ have dimensions k and $n-t-k$, respectively.

iii) If $t = d$ and T is the set of coordinates where a minimum weight codeword is nonzero, then $C^{(p)}$ and $(C^{\perp})^{(s)}$ have dimensions, respectively, $k-1$ and $n-d-k+1$.

2.3.4 The Plotkin construction

Two codes of the same length can be combined to construct a third one having twice their length by means of the Plotkin construction.

Let C_1 and C_2 be two $\mathbb{Z}_2\mathbb{Z}_4$-linear codes of types $(n, 0; k_1, 0)$ and $(n, 0; k_2, 0)$, and minimum distances d_1 and d_2, respectively. The *Plotkin construction* de nes a new binary linear code in terms of C_1 and C_2 as follows:

$$PC(C_1, C_2) = \{(\mathbf{u}|\mathbf{u}+\mathbf{v}) \mid \mathbf{u} \in C_1, \mathbf{v} \in C_2\},$$

where "|" denotes concatenation. This construction can also be de ned in terms of generator or parity check matrices. If G_1 and G_2 are any of the generator matrices of C_1 and C_2, respectively, and H_1 and H_2 are any of their parity check matrices, then code $PC(C_1, C_2)$ has the following generator and parity check matrices:

$$G_{PC} = \begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix} \quad H_{PC} = \begin{pmatrix} H_1 & 0 \\ H_2 & H_2 \end{pmatrix}.$$

The obtained $\mathbb{Z}_2\mathbb{Z}_4$-linear code $PC(C_1, C_2)$ is of type $(2n, 0; k_1 + k_2, 0)$ and minimum distance $d' = \min\{2d_1, d_2\}$.

As we shall see in Section 2.6, the Plotkin construction is used to obtain an interesting family of binary linear codes known as Reed-Muller codes.

2.4 Perfect codes

Let C be a binary code of length n. Code C is said to be *perfect* if for some integer t, $t \geq 0$, every $\mathbf{v} \in \mathbb{Z}_2^n$ is within distance t from exactly one codeword of C. This is equivalent to say that the covering radius ρ of C coincides with the packing radius e of C. In this case, C is said to be an e-perfect code.

An interesting fact is that no nontrivial binary perfect codes exist other than perfect single-error-correcting codes, and Golay codes [Gol49] of length $n = 23$ and packing radius $e = 3$. This was suspected for a long time and nally proved by Tietäväinen [Tie73] and Zinoviev [ZL73]. A rather complete survey article on perfect codes, which includes references to early work as well, can be found in [Lin75]. We will focus on 1-perfect codes.

Binary 1-perfect codes have length $n = 2^m - 1$, minimum distance $d = 3$ and 2^{n-m} codewords, for any integer m. When linear, they are called *Hamming codes*, and they exist for any $m \geq 2$. Hamming codes are unique up to equivalence, however, there are also many binary nonlinear 1-perfect codes for any $m \geq 4$ [Vas62].

By extending (see Section 2.3.2) a binary (either linear or nonlinear) 1-perfect code of length $2^m - 1$, we obtain an *extended* 1*-perfect code* of length 2^m and

minimum distance 4.

Given an extended Hamming code $C^{(e)}$, it is known that $(C^{(e)})^{\perp}$ is a linear Hadamard code, that is, a binary code with 2^{m+1} codewords, minimum distance 2^{m-1}, and whose codewords have Hamming weight $n/2$, except the all-ones and the all-zeroes vectors, where n is the length.

Some 1-perfect binary codes are $\mathbb{Z}_2\mathbb{Z}_4$-linear, that is, they can be seen as the Gray map image of some $\mathbb{Z}_2\mathbb{Z}_4$-additive codes; and there are also some extended 1-perfect binary codes that have a $\mathbb{Z}_4$-linear structure. The $\mathbb{Z}_2\mathbb{Z}_4$-dual code of every extended perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code is a Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear code, while the $\mathbb{Z}_4$-dual of every extended perfect $\mathbb{Z}_4$-linear code is a Hadamard $\mathbb{Z}_4$-linear code. The interested reader can find a complete classification of these codes in [BR99] and [Kro01].

Theorem 2.4.1 *[BR99] For any integer $m \geq 3$ and each $\delta \in \{0, \ldots, \lfloor \frac{m}{2} \rfloor\}$ there is a unique (up to isomorphism) perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code C of binary length $n = 2^m - 1$, such that the $\mathbb{Z}_2\mathbb{Z}_4$-dual code of C is of type $(\alpha, \beta; \gamma, \delta)$ with $\alpha \neq 0$, where $\alpha = 2^{m-\delta} - 1$, $\beta = 2^{m-1} - 2^{m-\delta-1}$, $n = \alpha + 2\beta$, and $\gamma = m - 2\delta$.*

We can call $\mathbb{Z}_2\mathbb{Z}_4$-*additive extended perfect codes* to all those $\mathbb{Z}_2\mathbb{Z}_4$-additive codes yielding, after the Gray map, a code with the same parameters as an extended perfect binary code, be it linear or not. Apart from the case when $\beta = 0$, there are clearly two different kinds of $\mathbb{Z}_2\mathbb{Z}_4$-additive extended perfect codes when $\beta \neq 0$: those with $\alpha = 0$ and those with $\alpha \neq 0$.

Theorem 2.4.2 *[Kro01] For any integer $m \geq 3$ and each $\delta \in \{1, \ldots, \lfloor \frac{m+1}{2} \rfloor\}$ there is a unique (up to isomorphism) extended perfect $\mathbb{Z}_4$-linear code C of binary length $n = 2^m$, such that the $\mathbb{Z}_4$-dual code of C is of type $(0, \beta; \gamma, \delta)$, where $\beta = 2^{m-1}$ and $\gamma = m + 1 - 2\delta$.*

The previous two theorems let us construct Table 2.1 and Table 2.2, which show, respectively, the type of all existing extended perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear and $\mathbb{Z}_4$-linear codes for small values of m, as well as the type of the corresponding dual code.

Table 2.1: Extended perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes ($\alpha \neq 0$).

m	δ	$(\alpha, \beta; \gamma, \delta)$ of the $\mathbb{Z}_2\mathbb{Z}_4$-dual code	$(\alpha, \beta; \gamma', \delta')$ of the code
2	0	$(4, 0; 3, 0)$	$(4, 0; 1, 0)$
3	0, 1	$(8, 0; 4, 0)$, $(4, 2; 2, 1)$	$(8, 0; 4, 0)$, $(4, 2; 2, 1)$
4	0, 1 2	$(16, 0; 5, 0)$, $(8, 4; 3, 1)$, $(4, 6; 1, 2)$	$(16, 0; 11, 0)$, $(8, 4; 5, 3)$, $(4, 6; 3, 4)$
5	0, 1 2	$(32, 0; 6, 0)$, $(16, 8; 4, 1)$, $(8, 12; 2, 2)$	$(32, 0; 26, 0)$, $(16, 8; 12, 7)$, $(8, 12; 6, 10)$
6	0, 1 2, 3	$(64, 0; 7, 0)$, $(32, 16; 5, 1)$, $(16, 24; 3, 2)$, $(8, 28; 1, 3)$	$(64, 0; 57, 0)$, $(32, 16; 27, 15)$, $(16, 24; 13, 22)$, $(8, 28; 7, 25)$
...	...	...	...

Table 2.2: Extended perfect $\mathbb{Z}_4$-linear codes ($\alpha = 0$).

m	δ	type $(\alpha, \beta; \gamma, \delta)$ of the $\mathbb{Z}_4$-dual code	type $(\alpha, \beta; \gamma', \delta')$ of the code
2	1	$(0, 2; 1, 1)$	$(0, 2; 1, 0)$
3	1, 2	$(0, 4; 2, 1)$, $(0, 4; 0, 2)$	$(0, 4; 2, 1)$, $(0, 4; 0, 2)$
4	1, 2	$(0, 8; 3, 1)$, $(0, 8; 1, 2)$	$(0, 8; 3, 4)$, $(0, 8; 1, 5)$
5	1, 2 3	$(0, 16; 4, 1)$, $(0, 16; 2, 2)$, $(0, 16; 0, 3)$	$(0, 16; 4, 11)$, $(0, 16; 2, 12)$, $(0, 16; 0, 13)$
6	1, 2 3	$(0, 32; 5, 1)$, $(0, 32; 3, 2)$, $(0, 32; 1, 3)$	$(0, 32; 5, 26)$, $(0, 32; 3, 27)$, $(0, 32; 1, 28)$
...	...	...	...

From Theorem 2.4.1 we have that for $m = 3$, the two existing extended perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes (see Table 2.1) are isomorphic, while for $m \geq 3$, all the codes are non-isomorphic and unique. The overall number of non-isomorphic perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes of binary length $n = 2^m$ is then $\lfloor \frac{m+2}{2} \rfloor$ for $m > 3$, and 1 for $m = 2$ and $m = 3$.

The parity check matrix $\mathcal{H}$ of any $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ having a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ binary image can be easily expressed, for any given δ, in form (2.4): the rst α columns are all possible nonzero vectors in $\mathbb{Z}_2^{\gamma+\delta}$, and the last β columns are all possible order four vectors in $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$, up to scalar multiples. It is also well known [BR99] that codewords in $\mathcal{C}^{\perp}$, thus generated by matrix $\mathcal{H}$, have Lee weight 2^{m-1}.

Example 1 *For $m = 4$, there are three different perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes C_1, C_2 and C_3, all of them of length $n = 2^4 - 1 = 15$, which correspond to the possible values of $\delta \in \{0, 1, 2\}$ (see Theorem 2.4.1). Let us consider the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, $\mathcal{C}_1 = \Phi^{-1}(C_1)$, $\mathcal{C}_2 = \Phi^{-1}(C_2)$ and $\mathcal{C}_3 = \Phi^{-1}(C_3)$.*

For $\delta = 0$, code $\mathcal{C}_1$ corresponds to the Hamming code having the following parity check matrix:

$$\mathcal{H}_1 = \left(\begin{array}{cccccccccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right),$$

and its $\mathbb{Z}_2\mathbb{Z}_4$-additive dual code $\mathcal{C}_1^{\perp}$ is of type $(15, 0; 4, 0)$; for $\delta = 1$, code $\mathcal{C}_2$ has parity check matrix $\mathcal{H}_2$ and a $\mathbb{Z}_2\mathbb{Z}_4$-additive dual code $\mathcal{C}_2^{\perp}$ of type $(7, 4; 2, 1)$; and finally, for $\delta = 2$, code $\mathcal{C}_3$ has parity check matrix $\mathcal{H}_3$, while its $\mathbb{Z}_2\mathbb{Z}_4$-additive dual code $\mathcal{C}_3^{\perp}$ is of type $(3, 6; 0, 2)$.

$$\mathcal{H}_2 = \left(\begin{array}{ccccccc|cccc} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 2 & 2 \\ \hline 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

$$\mathcal{H}_3 = \left(\begin{array}{ccc|cccccc} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 2 \\ 1 & 1 & 0 & 1 & 0 & 1 & 2 & 3 & 1 \end{array}\right)$$

We can now obtain the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-additive extended perfect codes by adding the all-zeroes column vector at the beginning of the binary part of the parity check matrix, and then adding the row vector having $\alpha + 1$ binary ones followed by β quaternary twos. Let $\mathcal{C}_1^{(e)}$, $\mathcal{C}_2^{(e)}$ and $\mathcal{C}_3^{(e)}$ be the $\mathbb{Z}_2\mathbb{Z}_4$-additive codes obtained from extending, respectively, $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_3$. Then, their respective parity check matrices are:

$$\mathcal{H}_1^{(e)} = \left(\begin{array}{cccccccccccccccc} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ \mathbf{0} & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ \mathbf{0} & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ \mathbf{0} & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right),$$

$$\mathcal{H}_2^{(e)} = \left(\begin{array}{cccccccc|cccc} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} \\ \mathbf{0} & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 2 \\ \mathbf{0} & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 2 & 2 \\ \hline \mathbf{0} & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{array}\right),$$

$$\mathcal{H}_3^{(e)} = \left(\begin{array}{cccc|cccccc} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} \\ \hline \mathbf{0} & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 2 \\ \mathbf{0} & 1 & 1 & 0 & 1 & 0 & 1 & 2 & 3 & 1 \end{array}\right),$$

and the type of $(\mathcal{C}_1^{(e)})^\perp$, $(\mathcal{C}_2^{(e)})^\perp$ *and* $(\mathcal{C}_3^{(e)})^\perp$ *are, respectively,* $(16, 0; 5, 0)$, $(8, 4; 3, 1)$ *and* $(4, 6; 1, 2)$*, as shown in Table 2.1.*

Note that, as it can be seen in Table 2.2, for $m = 4$ there are two extended perfect $\mathbb{Z}_4$-linear codes, whose dual code is of type $(0, 8; 3, 1)$ and $(0, 8; 1, 2)$, respectively. However, they do not come from extending any of the codes $\mathcal{C}_1$, $\mathcal{C}_2$ nor $\mathcal{C}_3$ just seen in Example 1. These $\mathbb{Z}_4$-linear codes are precisely the ones introduced and classi ed by Krotov [Kro01].

2.5 Completely regular codes

Let C be a binary code of length n, not necessarily linear. Recall, from Section 2.1, that the covering radius of C is de ned as

$$\rho = \max_{\mathbf{v} \in \mathbb{Z}_2^n} \{d(\mathbf{v}, C)\}.$$

The distance of any vector $\mathbf{v} \in \mathbb{Z}_2^n$ to C is

$$d(\mathbf{v}, C) = \min_{\mathbf{x} \in C} \{d(\mathbf{v}, \mathbf{x})\}.$$

Any binary code C determines a natural partition in sets $C(i)$ of the space $\mathbb{Z}_2^n$ according to the distance from C, where $C(i) = \{\mathbf{v} \in \mathbb{Z}_2^n : d(\mathbf{v}, C) = i\}$, and $1 \leq i \leq \rho$. Then $\{C(0), C(1), \ldots, C(\rho)\}$ is the *distance partition* of $\mathbb{Z}_2^n$ with respect to C.

We will say that two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n$ are *neighbours* whenever the distance from each other is one, i.e., when $d(\mathbf{u}, \mathbf{v}) = 1$.

Let us assume that C contains the all-zeroes codeword. Let $(\eta_0, \ldots, \eta_n)$ be its *distance distribution* (or inner distribution), i.e., η_i is the number of ordered pairs of codewords at a distance i apart, divided by $|C|$:

$$\eta_i = \frac{1}{|C|} \left| \{(\mathbf{u}, \mathbf{v}), \text{ such that } \mathbf{u}, \mathbf{v} \in C \text{ and } d(\mathbf{u}, \mathbf{v}) = i\} \right|.$$

Thus $\eta_0 = 1$. Note that if C is linear, the distance distribution is the weight distribution. Let $(\eta'_0, \ldots, \eta'_n)$ be the MacWilliams transform (see [MS77, Ch.5]) of $(\eta_0, \ldots, \eta_n)$. The number s of nonzero components η'_i for $1 \leq i \leq n$ is called the *external distance*.

Theorem 2.5.1 *[Del73b] Let C be a code of length n and external distance s. Then, for any vector $\mathbf{v} \in \mathbb{Z}_2^n$ there is a codeword at distance less than or equal to s from $\mathbf{v}$.*

The above theorem is then showing that the covering radius ρ of a code is at most equal to s. If C is a linear code, then s is the number of different nonzero weights of codewords in the dual code $C^\perp$.

According to [BZZ74], a binary code C of length n and covering radius ρ is said to be *uniformly packed* "in the wide sense" if there exist rational numbers $\tau_0, \ldots, \tau_\rho$ such that, for any $\mathbf{v} \in \mathbb{Z}_2^n$,

$$\sum_{i=0}^{\rho} \tau_i \zeta_i(\mathbf{v}) = 1,$$

where $\zeta_i(\mathbf{v}) = |\{\mathbf{u} \in C : d(\mathbf{u}, \mathbf{v}) = i\}|$.

Since their introduction in 1973 [Del73a], completely regular codes in the Hamming metric have been of interest to coding theorists and graph theorists alike. These highly regular substructures were de ned as a generalization of perfect and uniformly packed error-correcting codes, and included many codes

having very small minimum distance which were fundamental to the study of distance-regular graphs.

We will use here the de nition given by Neumaier [Neu92], according to which a binary code C of length n and covering radius ρ is said to be *completely regular* if, for any $i \geq 0$, every vector $\mathbf{u} \in C(i)$ has the same number a_i of neighbours in $C(i)$, the same number b_i of neighbours in $C(i+1)$, and the same number c_i of neighbours in $C(i-1)$. Note that $a_i + b_i + c_i = n$ and $c_0 = b_\rho = 0$. The ordered pair of sequences $(b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_\rho)$ is then said to be the *intersection array* of C. Figure 2.2 shows the distance partition of the space, given by a completely regular code and its translates. A detailed treatment of completely regular codes can be found in [BCN89].

The above de nition is equivalent to say that a binary code C is completely regular if for all $\mathbf{v} \in \mathbb{Z}_2^n$ such that $d(\mathbf{v}, C) = t$, the number of codewords at distance i ($0 \leq i \leq n$) from $\mathbf{v}$ depends only on t and i.

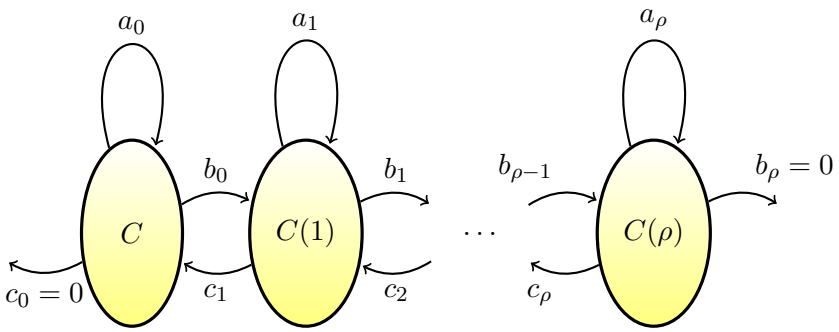

Figure 2.2: Completely regular code C.

It is well known that any completely regular linear code C implies the existence of a coset distance-regular graph.

The following proposition summarizes one of the most important results concerning the subject we are on.

Proposition 2.5.1 *Let C be a code (not necessarily linear) with packing radius $e \geq 1$, covering radius ρ and external distance s. Then:*

(i) [BZ77] *$\rho = s$ if and only if code C is uniformly packed "in the wide sense".*

(ii) [BCN89] *If C is completely regular, then it is also uniformly packed "in the wide sense".*

(iii) [Del73a] *If $2e + 1 \geq 2s - 1$, then C is completely regular.*

Throughout the years, many constructions of binary and non-binary completely regular codes have been introduced, some of them relatively recent [RZ07, BRZ08, RZ10]. Some constructions which particularly gave very good results were introduced in [RZ06, RZ11], where perfect q-ary codes are modified in several ways (namely, extended, punctured, shortened, and also lifted to the finite field over q^r, for any integer r), and proved to be completely regular codes.

The article "J. Rifà, L. Ronquillo, Construction of new completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes from old, in 7th International Workshop on Coding and Cryptography, 71–79, April 2011" in Appendix D, studies the uniformly packed condition and the completely regularity of the codes obtained from applying several constructions, namely extension, puncturing, shortening and lifting, to a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code.

2.6 Reed-Muller codes

Reed-Muller codes are one of the oldest and most interesting families of binary linear codes. They were first constructed by D.E. Muller [Mul54] and their decoding algorithm was described by I.S. Reed [Ree54]. These codes are easy to implement and decode, and their combinatorial properties are of great interest to produce new optimal codes. In this section, we will pay special attention to some of the properties of Reed-Muller codes.

Let $RM(r, m)$ be a binary linear Reed-Muller code of order r and length $n = 2^m$, for $0 \leq r \leq m$. As shown in [MS77, Ch.13], any binary linear Reed-Muller code $RM(r + 1, m + 1)$ of order $r + 1$ and length $n = 2^{m+1}$, for $m \geq 2$, can be

described in terms of two Reed-Muller codes of half its length: the code $RM(r+1,m)$ of order $r+1$, and the code $RM(r,m)$ of order r. This is achieved by using the Plotkin construction:

$$RM(r+1,m+1) = \{(\mathbf{u}|\mathbf{u}+\mathbf{v}) \mid \mathbf{u} \in RM(r+1,m), \mathbf{v} \in RM(r,m)\},$$

where $RM(0,m)$ is the repetition code $\{\mathbf{0},\mathbf{1}\}$ and $RM(m,m)$ is the entire space $\mathbb{Z}_2^{2^m}$. In terms of generator matrices, if $G(r,m)$ is a generator matrix of $RM(r,m)$, then the above statement is equivalent to say that the following is a generator matrix of $RM(r+1,m+1)$ code:

$$G(r+1,m+1) = \begin{pmatrix} G(r+1,m) & G(r+1,m) \\ 0 & G(r,m) \end{pmatrix}, \tag{2.5}$$

where $G(0,m) = (\mathbf{1})$.

We will denote the family of all Reed-Muller codes

$$\{RM(0,m), RM(1,m), \ldots, RM(m,m)\}$$

having length $n = 2^m$ by the set $\{RM(r,m)\}$. We can start from the sequence $\{RM(-1,2), RM(0,2), RM(1,2), RM(2,2)\}$ in order to construct all different families, where $RM(-1,2)$ is the code with only an all-zeroes vector, $RM(0,2)$ is the binary repetition code of length 4 with basis $\{\mathbf{1}\}$, $RM(1,2)$ is the even code of length 4, and $RM(2,2)$ is the entire space $\mathbb{Z}_2^4$. Each time we apply the Plotkin construction to a family of Reed-Muller codes $\{RM(r,m)\}$, it is necessary to add two new codes to the resulting family: codes $RM(-1,m+1) = \{\mathbf{0}\}$ and $RM(m+1,m+1) = \mathbb{Z}_2^{2^{m+1}}$.

It is easy to compute, from their de nitions, the dimension, minimum distance and duals of the binary Reed-Muller codes.

Theorem 2.6.1 *[MS77, Ch.13] The binary Reed-Muller code $RM(r,m)$ of order r and length 2^m, $0 \le r \le m$, $m \ge 1$, has the following properties:*

i) The dimension is $k = \sum_{i=0}^{r} \binom{m}{i}$.

ii) The minimum distance is $d = 2^{m-r}$.

iii) For all $r < m$*, we have* $RM(r,m) \subseteq RM(r+1,m)$*. Code* $RM(0,m)$ *is the repetition code* $\{\mathbf{0},\mathbf{1}\}$*, code* $RM(m-1,m)$ *is the even code, which consists of all even weight words of length* 2^m*, and* $RM(m,m)$ *is the full space* $\mathbb{Z}_2^{2^m}$.

iv) $RM(r,m)^{\perp} = RM(m-r-1,m)$*, for any* $0 \leq r < m$*. For instance, the code* $RM(1,m)$ *is the binary linear Hadamard code whereas the code* $RM(m-2,m)$ *is its dual, i.e., the extended binary Hamming code of length* 2^m.

2.6.1 Quaternary Reed-Muller codes

Hammons, Kumar, Calderbank, Sloane and Solé [HKC+94], conjectured in 1994 the $\mathbb{Z}_4$-linearity of binary linear Reed-Muller codes, stated in the following theorem.

Theorem 2.6.2 *The* r*th-order Reed-Muller code RM(r,m) of length* $n = 2^m$*, for* $m \geq 1$*, is* $\mathbb{Z}_4$*-linear for* $r \in \{0,1,2,m-1,m\}$ *and it is not* $\mathbb{Z}_4$*-linear for* $r \in \{3,\ldots,m-2\}$.

This theorem was proved in [HKC+94] for the particular case $r = m-2$, while the remaining values of $3 \leq r \leq m-2$ were not validated until the contributions of Hou, Lahtonen and Koponen [HLK98] in 1998.

Since then, several families of quaternary linear codes have been proposed and studied in the literature, all of them trying to generalize binary linear Reed-Muller codes. To this end, one of the first families to appear was the family of $\mathcal{QRM}(r,m)$ codes, constructed in [HKC+94] and defined as all those quaternary linear codes such that, for every value of r, $0 \leq r \leq m$, their modulo two yields a binary linear Reed-Muller code RM. In a subsequent work [BFP05], the parameters of such family of codes were studied and computed, and the family

$\mathcal{QRM}(r,m)$ itself was generalized by a class $\overline{QRM}(r,m)$ of quaternary linear codes that included them.

A quaternary generalization of the Plotkin construction was used in [Sol07] to obtain a sequence of quaternary Reed-Muller codes, known as $\mathcal{LRM}$ codes, whose corresponding images under the Gray map were binary codes with the same parameters as the binary linear Reed-Muller codes. However, $\mathcal{LRM}$ codes did not satisfy properties $iii)$ and $iv)$ of Theorem 2.6.1.

As a natural step from the previous constructions, a new family of quaternary linear codes was then presented in [PRS07, PRS09]. This new family was denoted by $\mathcal{RM}(r,m)$, and their binary image, under the Gray map, were $\mathbb{Z}_4$-linear codes having the same parameters and fundamental properties as the binary linear Reed-Muller codes. We will go now into further details concerning this family of codes.

It is known, from Theorem 2.4.2, that for any m there exist $\lfloor \frac{m+1}{2} \rfloor$ non-isomorphic extended perfect $\mathbb{Z}_4$-linear codes. It follows that, unlike the binary case RM, in which there is only one RM family for each different value of m, in the quaternary case there are $\lfloor \frac{m+1}{2} \rfloor$ different families for each m, and each one of them contains a different and non-isomorphic extended perfect $\mathbb{Z}_4$-linear code. Following the same notation as in [PRS07], every family $\{\mathcal{RM}_s(r,m)\}$ is identi ed by a subindex $s \in \{0,\ldots,\lfloor \frac{m-1}{2} \rfloor\}$.

In what follows we proceed to show the two different constructions that allow us to obtain all the $\mathcal{RM}_s$ codes. The rst construction, described in Theorem 2.6.3, is based on a quaternary generalization of the binary Plotkin construction (see Section 2.3.4); while the second one, de ned in Theorem 2.6.4, is called the *BQ-Plotkin construction*.

Let $\mathcal{RM}_s(r,m-1)$ and $\mathcal{RM}_s(r-1,m-1)$, $0 \leq s \leq \lfloor \frac{m-2}{2} \rfloor$, be any two $\mathcal{RM}$ codes of types $(0,N;\gamma^s_{r,m-1},\delta^s_{r,m-1})$ and $(0,N;\gamma^s_{r-1,m-1},\delta^s_{r-1,m-1})$; binary length $n=2^{m-1}$; number of codewords 2^{k_r} and $2^{k_{r-1}}$; minimum distances 2^{m-r-1} and 2^{m-r}, respectively, where

$$k_r = \sum_{i=0}^{r} \binom{m-1}{i},\ k_{r-1} = \sum_{i=0}^{r-1} \binom{m-1}{i}.$$

Let $\mathcal{G}_s(r,m)$ be a generator matrix of $\mathcal{RM}_s(r,m)$.

Theorem 2.6.3 *[PRS07] For any r and $m \geq 2$, $0 < r < m$, the code whose generator matrix is obtained by using the quaternary Plotkin construction*

$$\mathcal{G}_s(r,m) = \begin{pmatrix} \mathcal{G}_s(r,m-1) & \mathcal{G}_s(r,m-1) \\ 0 & \mathcal{G}_s(r-1,m-1) \end{pmatrix},$$

where $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, is an $\mathcal{RM}_s(r,m)$ code of type $(0, 2N; \gamma^s_{r,m}, \delta^s_{r,m})$, where $\gamma^s_{r,m} = \gamma^s_{r,m-1} + \gamma^s_{r-1,m-1}$ and $\delta^s_{r,m} = \delta^s_{r,m-1} + \delta^s_{r-1,m-1}$; binary length $n = 2^m$; 2^k codewords, where $k = \sum_{i=o}^{r} \binom{m}{i}$; minimum distance 2^{m-r} and, moreover, $\mathcal{RM}_s(r-1,m) \subset \mathcal{RM}_s(r,m)$.

Let $\mathcal{RM}_{s-1}(r,m-2)$, $\mathcal{RM}_{s-1}(r-1,m-2)$ and $\mathcal{RM}_{s-1}(r-2,m-2)$, $0 < s \leq \lfloor \frac{m-3}{2} \rfloor$, $m \geq 3$, be any three $\mathcal{RM}$ codes of type $(0, N; \gamma^{s-1}_{r,m-2}, \delta^{s-1}_{r,m-2})$, $(0, N; \gamma^{s-1}_{r-1,m-2}, \delta^{s-1}_{r-1,m-2})$ and $(0, N; \gamma^{s-1}_{r-2,m-2}, \delta^{s-1}_{r-2,m-2})$; of binary length $n = 2^{m-2}$; number of codewords 2^{k_r}, $2^{k_{r-1}}$, $2^{k_{r-2}}$; minimum distances 2^{m-r-2}, 2^{m-r-1} and 2^{m-r}, respectively, where

$$k_r = \sum_{i=0}^{r} \binom{m-2}{i},\ k_{r-1} = \sum_{i=0}^{r-1} \binom{m-2}{i},\ k_{r-2} = \sum_{i=0}^{r-2} \binom{m-2}{i}.$$

Let $\mathcal{G}_s(r,m)$ be a generator matrix of $\mathcal{RM}_s(r,m)$, $\mathcal{G}'_s(r,m)$ be the matrix obtained from $\mathcal{G}_s(r,m)$ after switching twos by ones in its $\gamma^s_{r,m}$ rows of order two, and $\hat{\mathcal{G}}_s(r,m)$ be the matrix obtained from $\mathcal{G}_s(r,m)$ after removing all $\gamma^s_{r,m}$ rows of order two.

Theorem 2.6.4 *[PRS07] For any r and $m \geq 3$, $0 < r < m-1$, the code $\mathcal{RM}_s(r,m)$, $s > 0$, obtained by using the BQ-Plotkin construction, has the following generator matrix $\mathcal{G}_s(r,m)$:*

$$\begin{pmatrix} \mathcal{G}_{s-1}(r,m-2) & \mathcal{G}_{s-1}(r,m-2) & \mathcal{G}_{s-1}(r,m-2) & \mathcal{G}_{s-1}(r,m-2) \\ \mathbf{0} & \mathcal{G}'_{s-1}(r-1,m-2) & 2\mathcal{G}'_{s-1}(r-1,m-2) & 3\mathcal{G}'_{s-1}(r-1,m-2) \\ \mathbf{0} & \mathbf{0} & \hat{\mathcal{G}}_{s-1}(r-1,m-2) & \hat{\mathcal{G}}_{s-1}(r-1,m-2) \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathcal{G}_{s-1}(r-2,m-2) \end{pmatrix},$$

and it is a quaternary linear code of type $(0, 4N; \gamma^s_{r,m}, \delta^s_{r,m})$*, where* $\gamma^s_{r,m} = \gamma^{s-1}_{r,m-2} + \gamma^{s-1}_{r-2,m-2}$*,* $\delta^s_{r,m} = \delta^{s-1}_{r,m-2} + \gamma^{s-1}_{r-1,m-2} + 2\delta^{s-1}_{r-1,m-2} + \delta^{s-1}_{r-2,m-2}$*; binary length* $n = 2^m$*;* 2^k *codewords, where* $k = \sum_{i=0}^{r} \binom{m}{i}$*; minimum distance* 2^{m-r} *and, moreover,* $\mathcal{RM}_s(r-1, m) \subset \mathcal{RM}_s(r, m)$*.*

The quaternary linear Reed-Muller code $\mathcal{RM}_s(-1, m)$ is de ned as the all-zeroes codeword code, the code $\mathcal{RM}_s(0, m)$ is the repetition code with only one nonzero codeword (the all-twos quaternary vector). For $r = m - 1$ and $r = m$, codes $\mathcal{RM}_s(m-1, m)$ and $\mathcal{RM}_s(m, m)$ are de ned as the even weight code and the entire space $\mathbb{Z}_4^{2^m}$, respectively. For any integer $m \geq 1$ and $0 \leq s \leq m$, code $\mathcal{RM}_s(1, m)$ is a quaternary linear Hadamard code, and code $\mathcal{RM}_s(m-2, m)$ is an extended quaternary linear 1-perfect code.

The rank of some speci c families of $\mathcal{RM}$ codes and the kernel dimension of the whole family of $\mathcal{RM}$ codes are established, respectively, in [PPV09] and [PPV11], thus generalizing some known results about the rank and kernel dimension of Hadamard $\mathbb{Z}_4$-linear and extended 1-perfect $\mathbb{Z}_4$-linear codes.

We conclude this section with a theorem that remarks that, as for the case of binary linear Reed-Muller codes, quaternary linear Reed-Muller codes $\mathcal{RM}$ also satisfy the duality relationship between the corresponding codes within the same family.

Theorem 2.6.5 *[PRS09] For any integer* $m \geq 2$*,* $N = 2^{m-1}$ *and* $s = \frac{m-1}{2}$*, let the set* $\{\mathcal{RM}_s(r, m)\}$ *be the family of* $\mathcal{RM}$ *codes obtained in Theorem 2.6.3 by using the Plotkin construction, or in Theorem 2.6.4 by using the BQ-Plotkin construction. Then, for each* $0 \leq r \leq m$*, the code* $\mathcal{RM}_s(r, m)$ *is the quaternary dual of the code* $\mathcal{RM}_s(m-r-1, m)$*.*

Refer to Appendix E for a table with the type $(\alpha, \beta; \gamma, \delta)$ of the families of quaternary linear Reed-Muller codes $\mathcal{RM}$ of smaller length.

The article "J. Pujol, J. Rifà, and L. Ronquillo, Construction of Additive Reed-Muller Codes, in Lecture Notes in Computer Science, 5527: 223–226, June 2009"

in Appendix A, introduces a generalization of the well known Plotkin construction which let us obtain new families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes such that their corresponding binary image, under the Gray map, are codes having the same length, dimension, minimum distance, inclusion and duality properties as the usual binary linear Reed-Muller codes.

2.7 Galois fields $GF(q)$ and Galois rings $GR(q^m)$

Let $GF(q)$ be a *Galois field* with $q = p^r$ elements, where p is prime. There exist essentially two ways to uniquely represent the elements of a Galois field. Given a primitive element ξ in $GF(q)$, any nonzero element $\mathbf{v} \in GF(q^r)$ can be written in the additive representation as

$$\mathbf{v} = a_0 + a_1\xi + \cdots + a_{r-1}\xi^{r-1},$$

where $a_i \in \mathbb{Z}_p$ and $0 \leq i \leq r-1$, while in the multiplicative representation, any element $\mathbf{v} \in GF(q)$ can be expressed as a power of ξ.

Let $GR(q^m)$ be a *Galois ring* of cardinality q^m, for $q = p^r$ and p prime. This Galois ring is isomorphic to the residue class ring $\mathbb{Z}_q[x]/(h(x))$, where $\mathbb{Z}_q[x]$ is the ring of polynomials over the ring $\mathbb{Z}_q$ of integers mod q, and $h(x)$ is a monic basic irreducible polynomial of degree m over $\mathbb{Z}_q[x]$, that is, it is a monic polynomial such that, if we apply the modulo p to each coefficient of $h(x)$, then the obtained polynomial in $\mathbb{Z}_p[x]$ is irreducible. Note that if $r = 1$, then $GR(q^m) = GF(q^m)$, while if $m = 1$, then $GR(q) = \mathbb{Z}_q$.

The theory of Galois rings was initiated by Krull [Kru24], and later independently rediscovered by Janusz [Jan66] and Raghavendran [Rag69]. As for Galois fields, there are also two ways to represent the elements of a Galois ring. In the additive representation, any element $\mathbf{w} \in GR(q^m)$ can be expressed as

$$\mathbf{w} = a_0 + a_1\psi + \cdots + a_{m-1}\psi^{m-1},$$

where $a_i \in \mathbb{Z}_q$, $0 \leq i \leq m-1$, and $\psi \in GR(q^m)$ is a zero of $h(x)$ and has

order $p^m - 1$; while in the multiplicative representation, also known as the *p-adic representation*, any element $\mathbf{w} \in GR(q^m)$ can be uniquely written as

$$\mathbf{w} = b_0 + b_1 p + \cdots + b_{r-1} p^{r-1},$$

where $b_j \in \{0, 1, \psi, \psi^2, \ldots, \psi^{p^m-2}\}$, $0 \leq j \leq r-1$, and $\psi \in GR(q^m)$ is again a zero of $h(x)$ of order $p^m - 1$.

Chapter 3

Steganography

The purpose of this chapter is to provide a brief introduction to the theory and design of systems to hide or embed information in signals such as images, video, audio, text and so on. This eld is known in general as *data-hiding* but we will focus our study on one of its branches: *steganography*.

As in Chapter 2, we do not attempt to cover all the research done in steganography, but to give an overview of the concepts and facts related to the contributions comprising this thesis. The interested reader is referred to [Mun11] to nd a comprehensive background on the topic and some related work.

We start, in Section 3.1, by introducing steganography and its relation to cryptography. Within the same section, we also give a formal de nition of steganographic schemes which, as we shall see, involves specifying an embedding function and a retrieval function which ful l certain properties. Section 3.2 draws the connection between steganography and coding theory, mainly by means of covering codes and the steganographic scheme known as *matrix embedding* [Cra98], whose most famous implementation is the *F5 Algorithm* [Wes01]; whereas Section 3.3 establishes some metrics such as the *average distortion* or the *embedding rate*, used by the steganographic community in order to evaluate and compare the performance of any steganographic system. This section also gives a theoretical bound every steganographer aims to approach when designing a new steganographic scheme. In Section 3.4 we describe a method based on the product of

perfect codes, which improves the matrix embedding method and was introduced in [RPR09]. Finally, Section 3.5 deals with a different kind of steganography which has been quite recently introduced in the steganography literature, and it is called ± 1-*steganography*, in comparison to *binary steganography*. Both terms are therein de ned, while subsection 3.5.1 describes the principles of a steganographic embedding scheme based on ternary codes [WvD05], which has so far represented the most common implementation of ± 1-steganography.

3.1 Introduction

The word *steganography* means "concealed writing" and it comes from the Greek words *steganos* and *graphei*, which mean "covered" and "writing", respectively.

Techniques of data protection have been of great interest for the scienti c community within the eld of information security. Among these techniques, the undeniable leading role has always belonged to cryptography. However, new interesting ideas have emerged in the last years, introducing digital steganography as an alternative, and sometimes even as a complement, of cryptography.

Steganography is a way of protecting information in which the communication itself is kept secret. Thus, unlike other kinds of data-hiding problems, in steganography problems the signal containing the embedded message is expected to look like a normal and unmodi ed signal. By contrast, the purpose of cryptography is to hide the contents of the transmitted messages, thus third parties are completely aware of the existence of these messages but are unable to read them. For this reason, cryptography and steganography are more and more used together to ensure a comprehensive protection of information.

The approach of steganography aimed at detecting the presence of hidden information in a signal is known as *steganalysis* [MK05].

The steganography problem was originally formalized by Simmons [Sim84] as the *Prisoners' Problem*: Alice and Bob are imprisoned and want to hatch an escape plan. They are allowed to communicate to each other through a warden (the *steganalyzer*), providing that he can read their messages and verify that they

are not communicating secretly. For this reason, Alice and Bob resort to steganography and hide their conspiracy messages under innocuous-looking messages (the *cover objects*) in order to avoid raising the warden s suspicion. In this problem and, in general, in data-hiding, two general directions can be distinguished, which are determined by the power of the adversary (the warden, in Prisoners Problem). One direction is aimed at avoiding the detection of the message by passive third parties. Thus, it is assumed that third parties will only read the messages but will not try to modify them. Another direction is focused on hiding the message assuming that third parties are active and, therefore, they can modify the message by introducing other fraudulent messages to deceive the parties involved in the communication. In this dissertation, third parties are assumed to be passive.

Some attempts to give a formal de nition of steganographic security can be found in [ZFK$^+$98, Sal04, KP02]. Cachin [Cac04] proposed an information-theoretic model for steganography which de ned the security of steganographic methods against passive adversaries. In this model, given a probabilistic distribution model for any possible cover object and for any possible *stego-object* (cover object containing embedded information), the adversary is expected to compute the relative entropy between both distributions and then decide from this whether or not a certain message contains embedded information. In this context, assuming that breaking a steganographic scheme means detecting the use of steganography to embed a message, a scheme is said to be *perfect* if the above-mentioned relative entropy is zero.

In order to give some de nitions we will assume, as in [WvD05], that the cover object is an image, in which message symbols from some nite eld are embedded at each pixel, and that the sender can use all pixels for embedding, i.e., the embedding is not constrained to any selection channel [FGS05]. As shown in Fig. 3.1, let us assume that a discrete source produces a sequence $\mathbf{x} = (x_1, \ldots, x_N)$, where N is the block length, $x_i \in \aleph = \{0, 1, \ldots, 2^B - 1\}$, and B is the *bit-depth* of the image, which is $B = 1$ for black and white images, $B = 8$ for gray-scale images, $B = 12$ for medical and satellite images, etc. Then, given a secret message $\mathbf{s} \in M$ and the above source $\mathbf{x}$, data embedding consists of modifying the values

of certain pixels so that the modi ed image $\mathbf{y} = (y_1, \ldots y_N)$ conveys the secret message, where $y_i \in \aleph$.

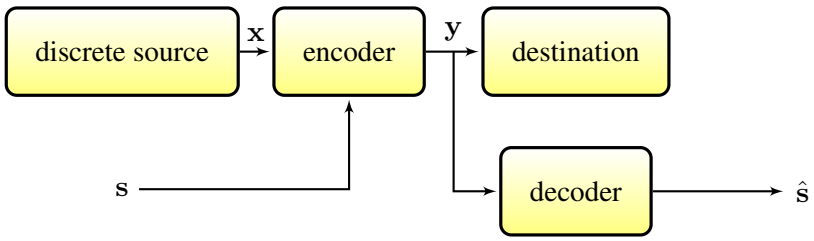

Figure 3.1: Model of an information embedding system.

The impact of embedding is captured by a distortion metric which, for $B = 1$, it is just computed as the number of coordinates in which $\mathbf{x}$ and $\mathbf{y}$ differ, thus

$$d(\mathbf{x}, \mathbf{y}) = |\{i : \ x_i \neq y_i, \text{ for } 1 \leq i \leq N\}|,$$

and sometimes it is assumed to be, as in [WvD05], of squared-error type

$$d(\mathbf{x}, \mathbf{y}) = |\mathbf{y} - \mathbf{x}|^2 = \sum_{i=1}^{N} |y_i - x_i|^2.$$

An *embedding scheme* with a distortion bound R is de ned as a pair of embedding Emb and extraction Ext functions,

$$Emb : \mathbb{F}_q^N \times M \longrightarrow \mathbb{F}_q^N \text{ and } Ext : \mathbb{F}_q^N \longrightarrow M, \tag{3.1}$$

$$d(\mathbf{x}, Emb(\mathbf{x}, \mathbf{s})) \leq R \text{ for all } \mathbf{s} \in M \text{ and all } \mathbf{x} \in \mathbb{F}_q^N, \tag{3.2}$$

such that $Ext(Emb(\mathbf{x}, \mathbf{s})) = \mathbf{s}$ for all messages $\mathbf{s} \in M$ and all $\mathbf{x} \in \mathbb{F}_q^N$.

We further assume that there is a *symbol-assignment function* $v : \aleph \to \mathbb{F}_p$, that assigns an element of a nite eld $\mathbb{F}_p$, where p is prime, to each possible pixel value of the cover object. One of the most well-known steganographic algorithms to hide information in images is the *LSB method*, which uses the following

assignment function

$$v(x_i) = x_i \ mod \ 2 \tag{3.3}$$

to embed a message in the least signi cant bit of pixel values. Note that, in a random case, half of the least signi cant bits will not need to be changed because they will already coincide with the message to be hidden. The problem of this method is that, although imperceptible by the human visual system, these modi cations produce an information loss which can be easily detected through statistical methods (see [Wes01, WP00, FGD01, FG02, Ker05a] and references therein).

3.2 Connection with coding theory

Most steganographic problems can be formulated as coding theory problems. Both elds have been usually related from the point of view of error-correcting codes, as it is the case of [ZL05], which describes the link between maximum length embeddable (MLE) codes and perfect error-correcting codes. However, Crandall [Cra98] showed in his essay posted in the steganography mailing list in 1998, that the performance of steganographic schemes can be improved by applying covering codes to the embedding process. This fact was later independently rediscovered by Galland et al. [GK03].

In particular, a linear code can be used to construct an embedding scheme, called *matrix embedding*, in which the message is communicated as a syndrome for an appropriate linear code.

Let C be a code of length N and dimension k, having parity check matrix H and covering radius ρ. Let $\mathbf{x}$ be the vector obtained after applying the symbol-assignment function to the cover object, and let $\mathbf{s} \in \mathbb{F}_q^{N-k}$ be the secret message. The embedding scheme below allows us to communicate $N-k$ symbols, applying at most ρ changes in every block of N symbols.

$$\begin{aligned} Emb(\mathbf{x}, \mathbf{s}) &= \mathbf{x} - \mathbf{e}_L = \mathbf{y}, \\ Ext(\mathbf{y}) &= H\mathbf{y}, \end{aligned}$$

where $\mathbf{e}_L$ is a leader of the class of vectors in $\mathbb{F}_q^N$ whose syndrome is $H\mathbf{x} - \mathbf{s}$.

Applying the extraction function to $\mathbf{y}$ we obtain, indeed, the hidden information $\mathbf{s}$, since $Ext(Emb(\mathbf{x}, \mathbf{s})) = H\mathbf{x} - H\mathbf{e}_L = H\mathbf{x} - H\mathbf{x} + \mathbf{s} = \mathbf{s}$. Note that the Hamming weight of $\mathbf{e}_L$ indicates how many coordinates will be changed from vector $\mathbf{x}$, thus the maximum distortion of the steganographic method is the covering radius ρ of C.

There is a steganographic method, developed in [Wes01], which is based on a speci c implementation of the matrix embedding method by means of Hamming codes. This method is known as the *F5 Algorithm*, and it allows us to embed m bits of message in $2^m - 1$ cover symbols by changing one of them at most, as shown in Example 2.

Example 2 *Let the following matrix be a parity check matrix of the Hamming code of length* $n = 2^3 - 1$*,*

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

Note that the columns are made up of all possible and different nonzero vectors of length 3*.*

By using this code, we are able to hide 3 *bits of secret message in a cover object (codeword) of length* 7 *by changing at most* 1 *bit (the covering radius of the code).*

Let $\mathbf{x} = (1001000) \in \mathbb{Z}_2^7$ *and* $\mathbf{s} = (110) \in \mathbb{Z}_2^3$ *be, respectively, the cover and the secret messages. The F5 Algorithm claims that it is possible to replace* $\mathbf{x}$ *by* $\mathbf{y} \in \mathbb{Z}_2^7$ *such that* $Ext(\mathbf{y}) = \mathbf{s}$ *by changing at most one bit of* $\mathbf{x}$*.*

We have $H\mathbf{x} = (101)$*, so* $H\mathbf{x} - \mathbf{s} = (101) - (110) = (011)$*, and then* $\mathbf{e}_L = (0010000) \in \mathbb{Z}_2^7$*. Finally,* $Emb(\mathbf{x}, \mathbf{s}) = (1001000) - (0010000) = (1011000) = \mathbf{y}$*. Therefore, in order to embed* $\mathbf{s}$ *in* $\mathbf{x}$ *the third bit of* $\mathbf{x}$ *needs to be changed from* 0 *to* 1*.*

Different authors have suggested other codes to implement the matrix embedding method, such as the binary Golay code [vDW01], binary BCH [SW06], random codes of small dimension [FS06] and Reed-Solomon codes [FG09]. Non-linear codes constructed by means of the block-wise direct sum have been proved to give better results in [BF08] than most of the linear codes that had been using until the moment. In particular, Preparata codes, which are known to be completely regular and $\mathbb{Z}_4$-linear codes, have been used to embed information.

3.3 Measures to evaluate steganographic protocols

The performance of a steganographic method can be measured in terms of some parameters. Given a steganographic method applied to a cover object of N symbols, the *average distortion* D or change rate is de ned as

$$D = \frac{R_a}{N} \text{ (changes/symbol)} , \tag{3.4}$$

where R_a is the expected number of changes over uniformly distributed messages; while the *embedding rate* E or information rate is the amount of bits, say t, that can be hidden in a cover object, and it is then computed by

$$E = \frac{t}{N} \text{ (bits/symbol)} . \tag{3.5}$$

We will refer to the tuple (D, E) as the *CI-rate* of the steganographic method, which stands for *Change* and *Information* rate [FL07].

In general, a good steganographic protocol is expected to have the highest possible embedding rate and the lowest possible average distortion. Moreover, assuming two embedding methods share the same source of cover objects, the same embedding operation, and the same embedding rate, the one introducing fewer embedding changes will be less detectable and, therefore, preferable. The relation between both parameters, embedding rate and average distortion, is also known as the *embedding efficiency*, used by some authors instead of the embedding rate, and de ned as the average number of embedded bits per one embedding change. This

concept was first introduced by Westfeld [Wes01] and has since been accepted as an important attribute of steganographic schemes.

The steganographic method based on the matrix embedding method (see Section 3.2) has an embedding rate E which coincides with the code redundancy, and an average distortion D bounded by ρ/N, where ρ is the covering radius of the code. One might conclude from this that in the class of linear codes of fixed length and dimension, the smallest average distortion, for a given embedding rate, is achieved by the code with the smallest covering radius. However, this statement has been proved to be false in [FLS07]: the smallest average distortion is attained for a code with the smallest average distance to the code, that is, the code having the lowest value of R_a, where

$$R_a = \frac{1}{q^n} \sum_{\mathbf{x} \in \mathbb{F}_q^N} d(\mathbf{x}, C).$$

Even though the average distance to code and the covering radius are two different values which are not necessarily optimized by the same code, in [FLS07, CMS11] it is also shown that, in the binary case, these two concepts asymptotically coincide with increasing length of the code and fixed embedding rate.

From the above considerations we have that when using the F5 Algorithm there are 2^{N-m} words whose distance to code is 0, and $2^N - 2^{N-m}$ words $\mathbf{x} \in \mathbb{Z}_2^N$ whose distance to code is 1, for $N = 2^m - 1$. Thus the average distance to code is $R_{aF_5} = \frac{2^N - 2^{N-m}}{2^N}$ and, therefore, the average distortion D_{F_5} and the embedding rate E_{F_5} of the F5 Algorithm are, respectively,

$$D_{F5} = \frac{1}{2^m} \text{ and } E_{F5} = \frac{m}{2^m - 1}. \tag{3.6}$$

In general, given a code, it is computationally difficult to find either its covering radius or the average distance to the code. The complexity of the former has been investigated in [CHLL97]. However, there exist some kind of codes where this computation is easier, as it is the case of completely regular codes (see Section 2.5).

A steganographic embedding scheme with block length N, embedding rate E and average distortion D is said to be *optimal* if any other embedding scheme with the same block length N has an embedding rate $E' \leq E$ or an average distortion $D' \geq D$.

Moulin and Wang claim in [MW04] that there is a theoretical bound on embedding rates for a given distortion D when the only modi cations of bits are those performed by the embedding scheme [1]. This concept is also known as *embedding capacity* $C(D)$. When the set of cover symbols is in $\mathbb{Z}_2$, that is, the symbol-assignment function (3.3) is used, and their sequence satis es the distribution of Bernoulli with probability $1/2$, the hiding capacity coincides with the entropy of the average distortion, and therefore it is given by

$$C(D) = H(D) = -D\log_2(D) - (1-D)\log_2(1-D), \tag{3.7}$$

where $0 \leq D \leq 1/2$, and $H(D)$ is the binary entropy function.

It is shown in [GK03] that matrix embedding performed with random linear codes of increasing code length can asymptotically achieve the bound (3.7), under the assumption of a xed relative message length $\frac{t}{N}$. In [FGS06], this scheme is generalized to the case when only a subset of pixels known to the sender is allowed to be modi ed (the so-called *wet paper codes*).

3.4 Product perfect codes

One of the methods of reference in steganography is the F5 Algorithm which, as shown in Section 3.2, uses binary Hamming codes of length $N = 2^m - 1$. Note that with this method we can only obtain a steganographic scheme for every integer value of m, thus not for any length N. We proceed to explain how the current scheme can be extended in order to nd a new one with an average distortion D different to the one given by a Hamming code. Let us take two Hamming codes

[1] Recall that we are considering the warden to be passive.

with average distortions $D_1 = 1/2^m$ and $D_2 = 1/2^{m+1}$, respectively, such that

$$D = \lambda D_1 + (1 - \lambda) D_2, \tag{3.8}$$

where $0 \leq \lambda \leq 1$. Then, both Hamming codes can be used, in the proportion given by λ, to hide information. The average distortion of the obtained method is the one shown in (3.8), while the embedding rate is

$$E = \lambda \frac{m}{2^m - 1} + (1 - \lambda) \frac{m + 1}{2^{m+1} - 1}.$$

Graphically, doing this is equivalent to draw a straight line from the point of CI-rate (D_1, E_1) to the point (D_2, E_2).

The F5 Algorithm has been improved by using the product of Hamming codes (hereafter denoted by PPC) [RPR09]. Given two binary linear codes, C_1 and C_2, of length n_1 and n_2, respectively, the product code $C_1 \otimes C_2$ can be de ned as the tensor product of C_1 and C_2. Therefore, it is generated by the vectors of the form

$$\mathbf{u} \otimes \mathbf{v} = (u_i v_j \mid 1 \leq i \leq n_1, 1 \leq j \leq n_2),$$

where $\mathbf{u} = (u_1, \ldots, u_{n_1}) \in C_1$ and $\mathbf{v} = (v_1, \ldots, v_{n_2}) \in C_2$. From the above de nition, it follows that $C_1 \otimes C_2$ can be seen as the set of matrices in which every row is an element in C_2 and every column is an element in C_1.

For the speci c case of two Hamming codes, C_1 and C_2, of the same length $N = 2^m - 1$, the product code $C_1 \otimes C_2$ is the code of length $n = (2^m - 1)^2$, dimension $k = (N - m)^2$ and whose codewords can be seen as matrices of size $(2^m - 1) \times (2^m - 1)$, where rows as well as columns are codewords in the binary Hamming code of length N.

The embedding method using this product code was introduced in [RPR09] and consists of taking blocks of size $(2^m - 1) \times (2^m - 1)$ in the cover object, and then apply the matrix embedding method, combining all the rows and the rst c columns, for $1 \leq c \leq 2^{m-1} - 1$. Compared to the F5 Algorithm, this steganographic scheme has a higher embedding rate for the same average distortion, thus

it has a better performance when compared to that of the F5 Algorithm.

The steganographic method based on the product of Hamming codes has an average distortion $D_{PPC} = \frac{R_{aPPC}}{(2^m-1)^2}$, where

$$R_{aPPC} = \frac{(2^m-1)^2}{2^m} + \frac{(2^m-1)(2^{m+1}+3c+1)c}{2^{m+1}2^m},$$

and an embedding rate

$$E_{PPC} = \frac{m(2^m-1)+mc}{(2^m-1)^2}.$$

The improvement introduced by the product of perfect codes with respect to the F5 Algorithm (see (3.6)) is shown in Fig. 3.2. Note that, as it can be seen in the aforementioned gure, the CI-rate (D_{PPC}, E_{PPC}) of the method based on the product of perfect codes is closer to the binary upper bound (3.7) than the CI-rate (D_{F5}, E_{F5}) of the F5 Algorithm. The reader is referred to [RPR09] for further details on the scheme using product perfect codes.

The article "J. Rifà, and L. Ronquillo, Product Perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear Codes in Steganography, in Proceedings of the 2010 International Symposium of Information Theory and its Applications, 696–701, 2010" in Appendix B, proposes a new steganographic scheme based on a generalization of the product of Hamming codes method just shown in the current section, by taking the product of more than two q-ary Hamming codes.

3.5 ± 1-steganography

As explained in Section 3.1, the LSB method uses the least signi cant bit of each pixel of the cover object to hide information. This kind of steganography is sometimes referred to as *binary steganography*. However, LSB ipping is a rather

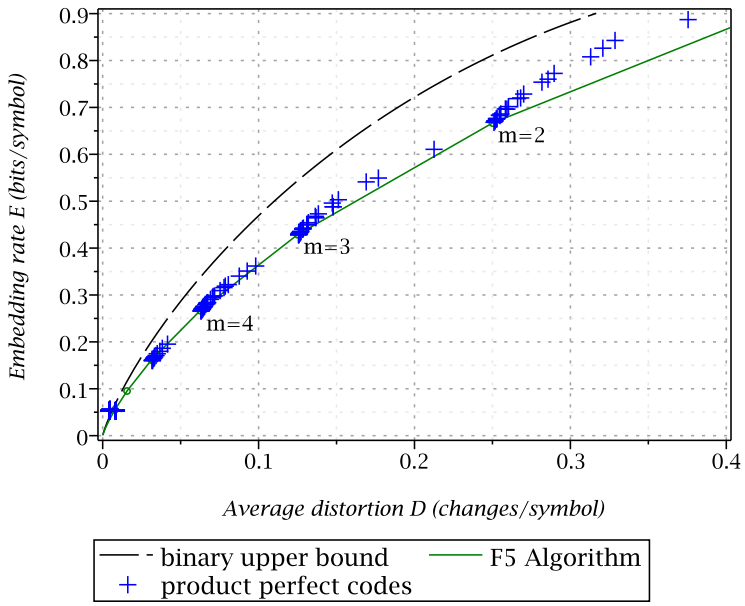

Figure 3.2: Embedding rate E of the steganographic schemes based, respectively, on the product of Hamming codes and on the F5 Algorithm, as a function of the average distortion D.

detectable operation, because during embedding, assuming that the bit-depth is $B = 8$, the grayscale value $2i$ is either left unchanged or changed to $2i + 1$, but it is never changed to $2i - 1$ for $0 \leq i \leq 127$, and all LSB detectors rely somehow on this fact.

A quite simple countermeasure is to make the embedding operation symmetrical and allow changes in both directions for all pixel values, thus any pixel x_i can be changed into $x_i + c$ for $c \in \{0, +1, -1\}$ and this means that the information is now carried by the two LSBs of every pixel. The absolute value of c is known as the *amplitude* of an embedding change.

This form of embedding is called ± 1-*steganography* [SFG05, WCT05], and sometimes it is also known as *LSB matching* [Ker05b, Ker05c]. It has traditionally led to consider the following symbol-assignment function

$$v(x_i) = x_i \; mod \; 3,$$

and thus the symbol embedded in each pixel is usually a ternary symbol.

In ± 1-steganography, the embedding rate of a given steganographic scheme is compared to the upper bound

$$C(D) = H(D) + D, \tag{3.9}$$

where $H(D)$ is the binary entropy function and $0 \leq D \leq 2/3$ is the average distortion. The aim of steganographers is, of course, designing schemes which approach this upper bound.

In [Fri06], it is established that ternary embedding is a good choice for steganography if our goal is to minimize the embedding distortion, which in turn con rms the heuristic conclusions in [FLS07] that one should not increase the amplitude of embedding changes hoping that their smaller number will lead to a less detectable scheme. Additionally, in [Fri06] it is proved that grouping pixels to form q-ary symbols does not improve the situation either.

3.5.1 Embedding based on ternary Hamming codes

Willems et al. [WvD05] proposed the use of ternary Hamming and Golay codes to improve the embedding ef ciency of ± 1-steganography. We proceed to study the performance of the steganographic scheme based on ternary Hamming codes.

Let C be a ternary Hamming code of length $N = \frac{3^m-1}{2}$. Note that this code has 3^m cosets, thus we can hide 3^m different ternary secret messages s. In order to determine the average distortion D, note that there is a probability of $\frac{1}{3^m}$ that the cover object of N ternary symbols already contains, by chance, the secret message embedded; and a probability of $\frac{3^m-1}{3^m}$ that it does not. Thus, the expected number of changes R_{aH_3} is

$$R_{aH_3} = \frac{1}{3^m} \cdot 0 + \frac{3^m - 1}{3^m} \cdot 1$$

and the average distortion is then $D_{H_3} = 2/3^m$. As for the embedding rate, it is

$$E_{H_3} = \frac{2 \log_2 3^m}{3^m - 1}.$$

The above CI-rate (D_{H_3}, E_{H_3}) is plotted in Fig. 3.3, and compared to the ternary upper bound (3.9).

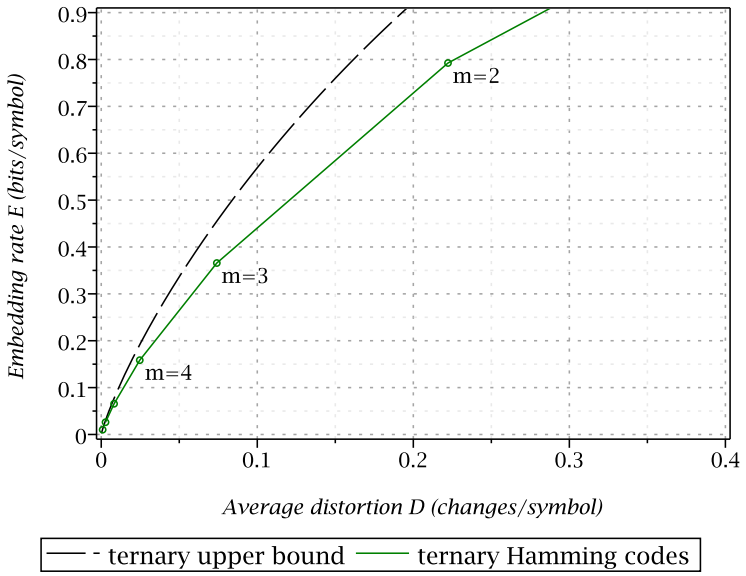

Figure 3.3: Embedding rate E_{H_3} of the steganographic scheme based on ternary Hamming codes, as a function of the average distortion D_{H_3}.

In [WvD05] the ternary Hamming and Golay codes are proved to be optimal, assuming that the distortion is of squared-error type. Independently, some other methods appeared in [ZW06] and [FL07] introducing new family of codes which included the ternary Hamming code as a subset. A method based on rainbow colouring graphs using q-ary Hamming codes, for q a prime power, which performed better than ternary Hamming codes when q was not a power of 3, was proposed by Fridrich et al. in [FL07]. However, there is a small remark, made by the authors of [WvD05] and [FL07], that it is worth to mention. If the cover object contains any pixel of the minimum or the maximum possible values, that is, either 0 or $2^B - 1$, then the embedding operations -1 and $+1$, which would lead the corresponding pixels to a value out of the range $\{0, \ldots, 2^B - 1\}$, are replaced

by the equivalent operations $+2$ and -2. The corresponding authors acknowledge that this would introduce a larger distortion, but they also argue that the effect of doing this can be neglected if the probability of nding a pixel value equal to 0 or $2^B - 1$ is not too large.

With the aim of providing a better approach to deal with these boundary grayscale values, the article "H. Rifà, J. Rifà, and L. Ronquillo, $\mathbb{Z}_2\mathbb{Z}_4$-Additive Perfect Codes in Steganography, in Advances in Mathematics of Communications, 5(3):425–433, 2011" in Appendix C, proposes a new steganographic scheme based on perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes which is optimal.

The article "J. Rifà, and L. Ronquillo, Product Perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear Codes in Steganography, in Proceedings of the 2010 International Symposium of Information Theory and its Applications, 696–701, 2010" in Appendix B, proposes an improvement of the above steganographic scheme by using the product of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, based on the ideas proposed in [RPR09].

Chapter 4

Contributions

In this chapter we present, summarize and discuss the results of the contributions making up this dissertation. Chapters 2 and 3 have already given a glimpse of the storyline that relates the articles appended to this document to each other. However, we summarize it here, with the aim of justifying the thematic unity of this compendium.

The aforesaid contributions are the publications listed below. They do not appear here in chronological order of publication, but in the order in which they were developed.

i) J. Pujol, J. Rifà, L. Ronquillo, *Construction of Additive Reed-Muller Codes*, Lecture Notes in Computer Science, vol. 5527, pp. 223–226. ISSN: 0302-9743, June 2009. (see Appendix A)

ii) H. Rifà-Pous, J. Rifà, L. Ronquillo, $\mathbb{Z}_2\mathbb{Z}_4$*-additive perfect codes in steganography*, Advances in Mathematics of Communications, vol. 5, no. 3, pp. 425-433. DOI: 10.3934/amc.2011.5.425, August 2011. (see Appendix C)

iii) J. Rifà, L. Ronquillo, *Product Perfect* $\mathbb{Z}_2\mathbb{Z}_4$*-linear codes in steganography*, in Proceedings of the 2010 International Symposium of Information Theory and its Applications. IEEE catalog number: CFP10767-USB, pp. 696-701. ISBN: 978-1-4244-6014-4, October 2010. (see Appendix B)

iv) J. Rifà, L. Ronquillo, *Construction of new completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes from old*, in 7th International Workshop on Coding and Cryptography, pp. 71-79, April 2011. (see Appendix D)

4.1 On Reed-Muller $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

As shown in Section 2.6, since the conjecture of the $\mathbb{Z}_4$-linearity of the binary linear Reed-Muller codes RM, in 1994, there have been several attempts to construct new quaternary linear codes that could generalize them. One can find in the literature the family of $\mathcal{QRM}(r,m)$ codes, $\overline{QRM}(r,m)$ codes [BFP05] and $\mathcal{LRM}$ codes [Sol07]. Nonetheless, one of the most successful attempts was the construction of the family of $\mathcal{RM}(r,m)$ codes [PRS07, PRS09], for it is the only family of quaternary linear codes whose corresponding binary images, under the Gray map, are binary codes ($\mathbb{Z}_4$-linear codes) having the same parameters and all the properties of Reed-Muller codes listed in Theorem 2.6.1.

In order to obtain $\mathcal{RM}$ codes, two constructions are used: one of them based on a quaternary generalization of the well-known binary Plotkin construction (see Section 2.3.4 for a description of the Plotkin construction and Theorem 2.6.3 for details on the quaternary generalization), and another one called *BQ-Plotkin construction* by the corresponding authors (see Theorem 2.6.4). As expected, for any integer values of m and s, the code $\mathcal{RM}_s(1,m)$ is a Hadamard $\mathbb{Z}_4$-linear code of length 2^m, while the code $\mathcal{RM}_s(m-2,m)$ is its $\mathbb{Z}_4$-dual code, i.e., an extended 1-perfect $\mathbb{Z}_4$-linear code. Table E.1 shows the type $(\alpha,\beta;\gamma,\delta)$ of $\mathcal{RM}$ codes for small values of m.

Recall, from Section 2.4, that apart from those 1-perfect binary codes which are linear (i.e., Hamming codes), and those extended 1-perfect binary codes which are $\mathbb{Z}_4$-linear – and which are included, as we have just seen, in the family of quaternary linear $\mathcal{RM}$ codes–, there exist also 1-perfect binary codes that have a $\mathbb{Z}_2\mathbb{Z}_4$-linear structure. For this reason, contribution i) was developed motivated by the search of a new family of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes that could generalize the binary linear Reed-Muller codes RM and contain the extension of the above-mentioned

1-perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. From the fruit of this search, contribution i) proposes and constructs new families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes called *Additive Reed-Muller codes*, denoted by $\mathcal{ARM}(r, m)$. These codes have the particularity that their image, under the Gray map, are binary codes ($\mathbb{Z}_2\mathbb{Z}_4$-linear codes), not necessarily linear, which have the same parameters and properties as Reed-Muller codes. The generalization is so obvious that, as a matter of fact, the rst family of $\mathcal{ARM}$ codes is exactly the family of binary linear Reed-Muller codes RM.

All members making up these new families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes can be obtained by means of two constructions: one coming from a generalization of the Plotkin construction to $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, and another one whose generator matrix slightly reminds of the matrix obtained when applying the Plotkin construction twice. The latter construction has been called *BA-Plotkin construction*.

The type of $\mathcal{ARM}$ codes for small values of m can be seen in Table E.1. Recall, from Section 2.4, that there are $\lfloor \frac{m+2}{2} \rfloor$ non-isomorphic perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes for any value of m and, therefore, there is the same number of non-isomorphic extended perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. From contribution i) we have that, for each m, there are $\lfloor \frac{m+2}{2} \rfloor$ different families of $\mathcal{ARM}$ codes of length 2^m, distinguished by a subindex s, $0 \leq s \leq \lfloor m/2 \rfloor$, and each of these families includes a different extended perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code. In particular, for any integer values of m and s, the code $\mathcal{ARM}_s(1, m)$ is a Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear code, while the code $\mathcal{ARM}_s(m-2, m)$ is its $\mathbb{Z}_2\mathbb{Z}_4$-dual code, that is, an extended 1-perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code. This fact can be seen by noting that in Table E.1, the type of the codes corresponding to columns $\mathcal{ARM}_s(1, m)$ and $\mathcal{ARM}_s(m-2, m)$, for any given m and s, is the same as that shown in Table 2.1 of Section 2.4.

The proofs of the statements in contribution i), as well as some examples, can be found in [PRR11].

4.2 On perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes and steganography

We now leave for a while the contributions devoted to coding theory, to talk in terms of steganography. The connection between steganography and coding theory has already been established in Section 3.2, and it mainly consists of using a parity check matrix of the corresponding code to embed information (the named *matrix embedding method*).

One of the contributions related to steganography is focused only on ± 1-steganography, while the other is focused on both binary and ± 1-steganography. In general terms, only the least signi cant bits of every pixel[1] are used to embed information in binary steganography; while in ± 1-steganography, the two least signi cant bits are used. In addition, ± 1-steganography is less detectable than binary steganography. See Section 3.5 for further information on these two forms of steganography.

Traditionally, ± 1-steganography has been approached by using ternary linear codes. There are two outstanding and most representative references in the literature showing this. In the rst one, Willems et al. [WvD05] propose a new steganographic scheme based on ternary Hamming and Golay codes; in the second one, Fridrich et al. [FL07] suggest a new method based on rainbow colouring graphs that uses q-ary Hamming codes, where q is a prime power, which clearly includes ternary Hamming codes when $q = 3$. In particular, the use of ternary Hamming codes has been proved to be optimal [WvD05, FL07]. However, as described in Section 3.5.1, these schemes unfortunately have the same drawback, related to the treatment of extreme grayscale values, for which they suggest a workaround that involves applying a change of magnitude greater than one to certain symbols of the cover object. To the best of our knowledge, there are no previous works in the literature that tackle this problem in a better way, and this was one of the aims of contribution ii).

Since perfect codes, in general, have shown to yield very good results in

[1] As in Chapter 3, the cover object is assumed to be an image.

steganography [Wes01, WvD05, FL07], it was natural to study and design a new method that used perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes to embed information. Recall that, as mentioned in Section 2.4, these kinds of codes include the binary Hamming codes as a subset, thus by proposing a new scheme, we would be at the same time generalizing previous steganographic methods based on the use of Hamming codes.

Given a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code C of type $(\alpha, \beta; \gamma, \delta)$, a cover object in the form of a vector $\mathbf{w} \in \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, and a secret message in the form of a vector $\mathbf{s} \in \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$, contribution ii) describes the different steps necessary to embed $\mathbf{s}$ within $\mathbf{w}$, and how to reverse the process to extract $\mathbf{s}$ at the receiver end. Since it is based on the matrix embedding method, the embedding process makes use of a parity check matrix of the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C} = \Phi^{-1}(C)$. Moreover, recall that the covering radius of C is $\rho = 1$, and it follows that it is possible to embed any message $\mathbf{s}$ in any possible cover object $\mathbf{w}$ by modifying, at most, one[2] coordinate of $\mathbf{w}$, which is good in terms of distortion (see Section 3.3 for a brief review on some of the parameters used to evaluate the performance of a steganographic scheme). What makes this new scheme suitable to address the ± 1-steganography is the fact that the two least signi cant bits of every pixel of the initial digital image are selected to end up with a set of bits that are later grouped together to form a vector $\mathbf{w}$ having α binary coordinates and β quaternary coordinates.

This new steganographic scheme has been proved to be optimal, in the sense that it achieves the smallest possible distortion at a given embedding rate for a xed block length. In addition, it performs better than the scheme based on the direct sum of ternary Hamming codes with the same average distortion.

As regards to the problem concerning the extreme grayscale values of the above-mentioned previous works, contribution ii) proposes a solution. The idea of the new approach is simple yet effective: it is based on performing two changes of magnitude one, instead of making one change of magnitude greater than one, as suggested by Willems, Fridrich et al. [WvD05, FL07], which was not compliant

[2]We will soon see that there is a special case in which we will need to modify up to two coordinates.

with ± 1-steganography. Taking into account that the distortion being computed is of squared-error type (see Section 3.1), the new approach to deal with extreme grayscale values provides a higher embedding rate for a given distortion, and it also makes the embedding less statistically detectable than those others based on ternary Hamming codes.

As for contribution iii), it consists of three main results: the introduction of a new parameter to measure the performance of any steganographic scheme, the improvement of an existing scheme addressing binary steganography, and the improvement of the steganographic scheme presented in contribution ii). The new proposed parameter measures the amount of information that can be hidden in a cover object, similar to what the embedding rate does, and it has been called *normalized embedding rate* e. This new parameter has been de ned as

$$e = \frac{H_q^{-1}(E)}{D},$$

where E and D are, respectively, the embedding rate and the average distortion, $H_q(x) = \frac{1}{\log_2(q)}(H(x) + x\log_2(q-1))$ is the q-ary entropy function on the interval $[0, (q-1)/q]$ for any integer q, $H(x)$ is the usual binary entropy function, and $H_q^{-1}(\cdot)$ is the inverse of $H_q(x)$. Thus all plots in contribution iii) depict points (D, e), instead of the usual CI-rate (D, E). As discussed in Chapter 3, the theoretical embedding upper bound any steganographic scheme is expected to reach or approach depends on whether we are dealing with binary or ± 1 steganography. The binary entropy function $H(x)$ is the upper bound on the embedding rate of binary steganography, while the ternary entropy function $H_3(x)$ is the upper bound of the ± 1-steganography. The bene ts from using the normalized embedding rate e instead of the embedding rate E, is that it eases the representation of the performance of any steganographic method, since the upper bound to which the points (D, e) are compared is always the same, no matter the type of steganography embedding.

In binary steganography, the steganographic scheme using the product of two perfect codes to embed information (see Section 3.4 for a review and [RPR09]

for further details) improves the CI-rate of the matrix embedding method. In contribution iii), we propose a new scheme that generalizes and also improves the aforementioned method, by taking the product of more than two q-ary Hamming codes, which has been called *Kronecker product technique* (KP-technique). The corresponding publication provides a description of the different steps comprising the new method, as well as a plot which compares the performance of the KP-technique, the product of two perfect codes, and of the $F5$ algorithm. This plot makes it clear that given an average distortion D, the proposed method achieves a normalized embedding rate e which is higher than that from the product of two perfect codes or the $F5$ algorithm.

The strategy of using the product of more than two perfect codes to embed information has also been applied to the steganographic scheme introduced in contribution ii), thus the product of more than two perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes has been used to obtain a new steganographic scheme within the scope of ± 1-steganography. As expected, this improvement results in a steganographic scheme which outperforms the scheme that simply uses perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

4.3 On completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

Finally, the last contribution of this compendium, contribution iv), studies a set of existing constructions from which we have proved to obtain some new completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. As discussed in Section 2.5, completely regular codes are highly regular substructures which were initially de ned as a generalization of perfect and uniformly packed error-correcting codes. In particular, completely regular codes are interesting from the point of view of steganography. Recall, from Section 3.3, that in order to compute the average distortion D of a steganographic scheme based on a certain code, it is necessary to compute the average distance to the code, and this is a computationally dif cult operation. When working with completely regular codes, however, this computation is, by de nition, easier and feasible.

There have been many constructions of completely regular codes, both binary

and non-binary. Some of them, like those proposed in [RZ06, RZ11], consist of modifying a perfect code, which is known to be completely regular, by extending, puncturing, shortening or lifting it. The three first constructions are discussed in Section 2.3, while the latter is a new one, first introduced in [RZ11], which let us obtain a new code over $GF(p^r)$ from an initial code over $GF(p)$, for any integer r and prime p.

The idea behind contribution iv) is very similar to that from the papers mentioned above. Given a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code, which is also completely regular, this code has been extended, punctured, shortened or lifted from $GF(2)$ to $GF(2^r)$, for any integer r. In turn, given an extended perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code, the lifting to $GF(4)$ has been made. Then, the corresponding paper has studied the completely regularity of the obtained codes, and also computed their intersection array, when applicable.

As a result of the above constructions, the extended, the punctured and also the shortened perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes have been proved to be completely regular under certain conditions. Moreover, it is interesting to note that, despite of having obtained new completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, these codes have the same intersection array as the corresponding linear codes. That is, the intersection arrays of the extended and of the shortened codes are the same, respectively, as those from the extended and from the shortened Hamming codes of the same length; while the intersection array of the punctured perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code coincides with the intersection array of the punctured Hamming code when the coordinate being punctured in the perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code is binary, and of the 2-punctured Hamming code when the coordinate being punctured in the perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code is quaternary. As for the perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code lifted to $GF(2^r)$, it has been proved to be completely regular only for $r = 2$, while for any other value $r > 2$ it is not uniformly packed, thus it is not completely regular either (see Proposition 2.5.1). Finally, the code in $GF(4)$ obtained by lifting an extended perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code has been proved to be uniformly packed and not completely regular.

Chapter 5

Conclusions

5.1 Summary

Since the inception of coding theory [Sha48], codes have been used in many diverse ways; in addition to providing reliability in communication channels, new uses have been constantly appearing. Among them, we can find steganography, which is a branch of digital data-hiding aimed at concealing sensitive information within another message –the cover object–, in such a way that the resulting message does not arouse third parties suspicions, and just the intended sender and receiver involved in the communication process know there is hidden information and are able to extract it.

Indeed, coding theory and steganography can be seen as two fields complementing each other. While every recently discovered code or family of codes can mean a new chance to obtain good steganographic schemes, at the same time, every step made towards the search of steganographic schemes that might approach the theoretical upper bound on the embedding rate can reveal new problems and challenges for which new codes will be necessary. It is for this reason, that every contribution presented in this compendium has somehow meant an incremental advance in either of both fields.

It is known that there are certain codes, such as perfect codes and completely regular codes, which hold some characteristics –small covering radius and the

regular distribution of the codewords in the space, respectively–, that might be interesting to be used to obtain new steganographic schemes with low average distortion and high embedding rate. In particular, all contributions of this dissertation concerning coding theory are either related to perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes or to completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, while those that concern steganography present new embedding schemes based on perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

Among the contributed results of this dissertation we have presented new infinites families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes [PRR09] which are interesting for two main reasons. First, because the image of these codes, through the Gray map, yields binary codes which sometimes are linear and sometimes are not, yet they always have the same parameters and properties as the well-known binary linear Reed-Muller codes [Mul54, Ree54]. This involves having a recursive definition through various constructions, namely Plotkin and BQ-Plotkin, and fulfilling the inclusion and the duality properties, among other properties. And second, because the previous reason means that, among other implications, these new families include the existing extended perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

In this dissertation a new parameter, besides the well-known embedding rate E and average distortion D, has been introduced. This parameter has been called normalized embedding rate, denoted by e, and let us depict the performance of any steganographic scheme in an easier way, since the theoretical upper bound to which the points (D, e) should be compared is always the straight line $e = 1$, regardless of whether the scheme is addressing binary or ± 1-steganography.

With respect to binary steganography, that is, the kind of steganography embedding in which the cover object is made up of the least significant bit of every symbol, a new steganographic scheme that outperforms the embedding scheme [RR10] based on the product of two perfect codes [RPR09] has been proposed. This new scheme is inspired in the previous scheme, so that the code used to embed information is the result of performing the Kronecker product of more than two q-ary Hamming codes.

Steganography known as ± 1-steganography [SFG05, WCT05] is a form of steganography embedding mainly used when the cover object is an image, and

pixels are distorted by one magnitude of change at most, either by adding $(+1)$ or substracting (-1) one unit –or by performing no changes at all–, thus the two least signi cant bits of every pixel are used to embed the secret message. We have designed and presented a new steganographic scheme [RPRR11] based on the matrix embedding method, that uses perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. This new method comes at a time in which most embedding methods addressing ± 1-steganography were mainly using ternary codes [WvD05, FL07]. As proved in the corresponding publication, the proposed scheme is as optimal as those schemes based on the direct sum of ternary Hamming codes and, for the same average distortion, it allows to embed a higher amount of information. Moreover, the new method is prepared to deal with extreme grayscale values, in such a way that no changes of magnitude greater than one are ever performed. Compared to previous results in the literature [WvD05, FL07], given the same embedding rate, this behaviour involves a lower distortion.

Since perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are binary codes, often nonlinear, which have an algebraic structure over $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, we can perform the Kronecker product of two or more of these $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and use the resulting code to embed information. This scheme has been introduced in the current dissertation and has been proved to signi cantly improve the previous scheme that did not perform any product, for it involves a lower distortion and allows to hide a higher amount of data.

Finally, in a contribution more devoted to coding theory, we have studied completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes [RR11]. Starting from a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code which, as any perfect code, is known to be completely regular, we have seen that the extension, the puncturing and also the shortening of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes yield new completely regular codes whose intersection array has been computed. In turn, the extension of a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code, once lifted to $GF(4)$, has been proved to be uniformly packed.

5.2 Future research

In this section, we point out some open problems that derive from this dissertation and deserve further investigation.

First of all, it would be interesting to complement the study of the families of $\mathbb{Z}_2\mathbb{Z}_4$-additive Reed-Muller codes introduced in this thesis by computing the rank and the dimension of the kernel of the obtained codes, just as it was done in [PPV09, PPV11] for the family of quaternary linear Reed-Muller codes $\mathcal{RM}(r, m)$.

Also related to these families of codes, it would be very helpful for coding theorists to develop and implement a complete MAGMA[1] package providing the tools to construct these families and work with them.

As we have seen throughout this dissertation, perfect codes yield very good results when used to embed information. Because of the regular nature of completely regular codes –recall, furthermore, that completely regular codes include perfect codes–, their use in steganography would certainly make the computation of the average distortion easier, thanks to the fact that, in these codes, it is computationally easy to obtain the number of words that are at a certain distance from others. Indeed, Bierbrauer et al. [BF08] studied the performance of some steganographic schemes based on Preparata codes, which are known to be completely regular and $\mathbb{Z}_4$-linear codes. For all the reasons above, it would be interesting to exhaustively study the completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes we have obtained in this thesis to be used in steganography.

Finally, we think further work in the direction of wet paper codes [FGS06] is needed. As very brie y mentioned in Chapter 3, wet paper codes are steganographic schemes in which not all symbols of the cover object are allowed to be modi ed during the embedding process, but a subset of them, called *dry coor-*

[1] MAGMA is a software package designed to solve computationally hard problems in algebra, number theory, geometry and combinatorics. Currently, it supports the basic facilities for linear codes over integer residue class rings and Galois rings, including additional functionality for the special case of codes over $\mathbb{Z}_4$ and also for $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. In particular, the latter package, among others, has been developed by the Combinatorics, Coding and Security Group (CCSG) (http://www.ccg.uab.cat) in which this thesis has been conducted.

dinates. This restriction has been usually modelled by performing the shorten construction of a given code. Thus, to fully grasp the possibilities of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, another line of research would be to study the use of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes in wet paper codes, as well as the bene ts of doing so.

Bibliography

[BCN89] A.E. Brouwer, A.M. Cohen, and A. Neumaier. *Distance-Regular Graphs*, volume 2. Springer-Verlag, 1989.

[BF08] J. Bierbrauer and J. Fridrich. Constructing good covering codes for applications in steganography. In Yun Shi, editor, *Transactions on Data Hiding and Multimedia Security III*, volume 4920 of *Lecture Notes in Computer Science*, pages 1–22. Springer Berlin / Heidelberg, 2008.

[BFCP+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*, 54:167–179, 2010.

[BFP05] J. Borges, C. Fernández, and K.T. Phelps. Quaternary Reed-Muller codes. *IEEE Transactions on Information Theory*, 51(7):2686–2691, July 2005.

[BR99] J. Borges and J. Rifà. A characterization of 1-perfect additive codes. *IEEE Transactions on Information Theory*, 45(5):1688–1697, July 1999.

[BRZ08] J. Borges, J. Rifà, and V.A. Zinoviev. On non-antipodal binary completely regular codes. *Discrete Mathematics*, 308(16):3508–3525, 2008.

[BZ77] L.A. Bassalygo and V.A. Zinoviev. Remark on uniformly packed codes. *Problems Information Transmission*, 13(3):22–25, 1977.

[BZZ74] L.A. Bassalygo, G.V. Zaitsev, and V.A. Zinoviev. Uniformly packed codes. *Problems Information Transmission*, 10(1):9–14, 1974.

[Cac04] C. Cachin. An information-theoretic model for steganography. *Information and Computation*, 192(1):41–56, July 2004.

[CHLL97] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein. *Covering Codes*, volume 54. North-Holland Mathematical Library, Elsevier, Amsterdam, 1997.

[CMS11] G. Cohen, C. Munuera, and P. Solé. The average radius of codes: Survey and new results. In *Proceedings of the 2011 IEEE International Symposium on Information Theory (ISIT)*, pages 1792–1795, St. Petersburg, 2011.

[Cra98] R. Crandall. Some notes on steganography. Posted on steganography mailing list http://www.dia.unisa.it/∼ads/corso-security/www/CORSO-0203/steganogra a/LINKS%20LOCALI/matrix-encoding.pdf, 1998.

[Del73a] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Research Reports Supplements*, 10, 1973.

[Del73b] P. Delsarte. Four fundamental parameters of a code and their combinatorial signi cance. *Information and Control*, 23(5):407–438, December 1973.

[FG02] J. Fridrich and M. Goljan. Practical steganalysis of digital images - state of the art. In *Proceedings on SPIE*, volume 4675, pages 1–13. Photonics West, January 2002.

[FG09] C. Fontaine and F. Galand. How Reed-Solomon codes can improve steganographic schemes. *EURASIP Journal on Information Security, special issue on secure steganography in multimedia content*, 2009, 2009.

[FGD01] J. Fridrich, M. Goljan, and R. Du. Detecting LSB steganography in color, and gray-scale images. *IEEE Multimedia (Special Issue on Security)*, 8(4):22–28, 2001.

[FGS05] J. Fridrich, M. Goljan, and D. Soukal. Steganography via codes for memory with defective cells. In *43rd Conference on Coding, Communications, and Control*, September 2005.

[FGS06] J. Fridrich, M. Goljan, and D. Soukal. Wet paper codes with improved embedding ef ciency. *IEEE Transactions on Information Forensics and Security*, 1(1):102–110, March 2006.

[FL07] J. Fridrich and P. Lisonek. Grid colorings in steganography. *IEEE Transactions on Information Theory*, 53(4):1547–1549, April 2007.

[FLS07] J. Fridrich, P. Lisonek, and D. Soukal. On steganographic embedding ef ciency. In *Information Hiding*, volume 4437 of *Lecture Notes on Computer Science*, pages 282–296, Berling Heidelberg, 2007. Springer-Verlag.

[Fri06] J. Fridrich. Minimizing the embedding impact in steganography. In J. Dittmann and J. Fridrich, editors, *Proceedings of the 8th Workshop on Multimedia and Security*, pages 2–10, New York, 2006. ACM.

[FS06] J. Fridrich and D. Soukal. Matrix embedding for large payloads. *IEEE Transactions on Information Forensics and Security*, 1(3):390–395, August 2006.

[GK03] F. Galand and G. Kabatiansky. Information hiding by coverings. In *Proceedings of the IEEE Information Theory Workshop*, pages 151–154, 2003.

[Gol49] M. J. E. Golay. Notes on digital coding. In *Proceedings of the IRE*, volume 37, page 657, 1949.

[HKC+94] A Hammons, 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 Transactions on Information Theory*, 40:301–319, 1994.

[HLK98] X.-D. Hou, J. T. Lahtonen, and S. Koponen. The Reed-Muller code $R(r, m)$ is not $\mathbb{Z}_4$-linear for $3 \leq r \leq m - 2$. *IEEE Transactions on Information Theory*, 44(2):798–799, 1998.

[Jan66] G. J. Janusz. Separable algebra over commutative rings. *Transactions of the American Mathematical Society*, 122(2):461–479, April 1966.

[Ker05a] A. Ker. A General Framework for Structural Analysis of LSB Replacement. In M. Barni, J. Herrera-Joancomarti, S. Katzenbeisser, and F. Perez-Gonzales, editors, *Information Hiding. 7th International Workshop*, volume 3727 of *Lectures Notes on Computer Science*, pages 296–311, Berlin Heidelberg, 2005. Springer-Verlag.

[Ker05b] A. Ker. Resampling and the detection of LSB matching in color bitmaps. In E. Delp and P.W. Wong, editors, *Proceedings of the SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VII*, volume 5681, pages 1–15, San Jose, CA, January 2005.

[Ker05c] A.D. Ker. Steganalysis of LSB matching in grayscale images. *IEEE Signal Processing Letters*, 12(6):441–444, 2005.

[KP02] S. Katzenbeisser and F.A.P. Petitcolas. De ning security in steganographic systems. In *Proceedings of the SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents IV*, volume 4675, pages 50–56, San Jose, CA, 2002.

[Kro01] D.S. Krotov. $\mathbb{Z}_4$-linear Hadamard and extended perfect codes. In *International Workshop on Coding and Cryptography*, volume 8-12, pages 329–334, Paris, France, January 2001.

[Kru24] W. Krull. Algebraische theorie der ringe. *Mathematische Annalen*, 92(3-4):183–213, 1924.

[Lin75] J. H. v. Lint. A survey of perfect codes. *Rocky Mountain Journal of Mathematics*, 5(2):199–224, 1975.

[Lin82] J. H. van Lint. *Introduction to Coding Theory*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1982.

[MK05] P. Moulin and R. Koetter. Data-hiding codes. *Proceedings of the IEEE*, 93(12):2083–2126, December 2005.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, Amsterdam, 1977.

[Mul54] D. E. Muller. Application of boolean algebra to switching circuit design and to error detection. *IEEE Transactions on Computers*, 3:6–12, 1954.

[Mun11] C. Munuera. *Algebraic Geometric modelling in Information Theory*, chapter Steganography from a coding theory point of view. Series on Coding Theory and Cryptography. World Scienti c, May 2011.

[MW04] P. Moulin and Y. Wang. New results on steganographic capacity. In *Proceedings of Conference on Information Sciences and Systems*, University of Princeton, Princeton, New Jersey, 2004. Available at: http://www.ifp.uiuc.edu/∼ywang11/paper/CISS04_204.pdf.

[Nad62] M. Nadler. A 32-point $n = 12$, $d = 5$ code. *IRE Transactions on Information Theory*, 8:58, 1962.

[Nec89] A. A. Nechaev. The Kerdock code in a cyclic form. *Diskret Math.*, 1(4):123–139, 1989. English translation in Discrete Math. Appl. 1 (1991), 365-384.

[Neu92] A. Neumaier. Completely regular codes. *Discrete Maths. 106/107*, 106-107(1):335–360, September 1992.

[PHB98] V. S. Pless, W. C. Huffman, and R. A. Brualdi. *Handbook of Coding Theory : Volume I*. North-Holland, 1998.

[PPV09] J. Pernas, J. Pujol, and M. Villanueva. Rank for some families of quaternary Reed-Muller codes. In M Bras-Amorós and T. Høholdt, editors, *Proceedings of the Applied Algebra, Algebraic Algorithms and Error-correcting codes*, volume 5527 of *Lecture Notes in Computer Science*, pages 43–52. Springer Berlin / Heidelberg, June 2009.

[PPV11] J. Pernas, J. Pujol, and M. Villanueva. Classi cation of some families of quaternary Reed–Muller codes. *IEEE Transactions on Information Theory*, 57(9):6043–6051, September 2011.

[PRR09] J. Pujol, J. Rifà, and L. Ronquillo. Construction of Additive Reed–Muller codes. In M. Bras-Amorós and T. Høholdt, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 5527 of *Lecture Notes in Computer Science*, pages 223–226. Springer Berlin / Heidelberg, 2009.

[PRR11] J. Pujol, J. Rifà, and L. Ronquillo. Construction of Additive Reed-Muller codes. http://arxiv.org/abs/0909.3185v2, 2011.

[PRS07] J. Pujol, J. Rifà, and F. I. Solov eva. Quaternary Plotkin constructions and quaternary Reed-Muller codes. In S. Boztas and H.F. Lu, editors, *Proceedings of the 17th international conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 4851 of *Lecture Notes in Computer Science*, pages 148–157. Springer-Verlag, 2007.

[PRS09] J. Pujol, J. Rifà, and F. I. Solov eva. Construction of $\mathbb{Z}_4$-linear Reed–Muller codes. *IEEE Transactions on Information Theory*, 55(1):99–104, January 2009.

[Rag69] R. Raghavendran. Finite associative rings. *Compositio Mathematica*, 21:55–58, 1969.

[Ree54] I.S. Reed. A class of multiple-error-correcting codes and the decoding scheme. *IRE Professional Group on Information Theory*, 4(4):38–49, 1954.

[RPR09] H. Rifà-Pous and J. Rifà. Product perfect codes and steganography. *Digital Signal Processing*, 19(4):764–769, July 2009.

[RPRR11] H. Rifà-Pous, J. Rifà, and L. Ronquillo. $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes in steganography. *Advances in Mathematics of Communications*, 5(3):425–433, August 2011. 10.3934/amc.2011.5.425.

[RR10] J. Rifà and L. Ronquillo. Product perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes in steganography. In *Proceedings of the 2010 International Symposium of Information Theory and its Applications*, pages 696–701, October 2010. ISBN: 978-1-4244-6014-4.

[RR11] J. Rifà and L. Ronquillo. Construction of new completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes from old. In *7th International Workshop on Coding and Cryptography*, pages 71–79, April 2011.

[RZ06] J. Rifà and V.A. Zinoviev. On completely regular codes from perfect codes. In *Proceedings of the 10th International Workshop on Algebraic and Combinatorial Coding Theory*, pages 225–229, Zvenigorod (Russia), 2006.

[RZ07] J. Rifà and V.A. Zinoviev. On new completely regular q-ary codes. *Problems of Information Transmission*, 43(2):97–112, 2007.

[RZ10] J. Rifà and V.A. Zinoviev. New completely regular q-ary codes, based on Kronecker products. *IEEE Transactions on Information Theory*, 56(1):266–272, January 2010.

[RZ11] J. Rifà and V.A. Zinoviev. On lifting perfect codes. *IEEE Transactions on Information Theory*, 57(9):5918–5925, September 2011.

[Sal04] P. Sallee. Model based steganography. In T. Kalker, I.J. Cox, and Y.M. Ro, editors, *International Workshop on Digital Watermarking*, volume 2939 of *Lecture Notes in Computer Science*, pages 154–167. Springer Berlin / Heidelberg, New York, 2004.

[SFG05] D. Soukal, J. Fridrich, and M. Goljan. Maximum likelihood estimation of secret message length embedded using $\pm$-k steganography in spatial domain. In E. Delp and P.W. Wong, editors, *Proceedings of the SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VII*, volume 5681, pages 595–606, San Jose, CA, January 2005.

[Sha48] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423, 1948.

[Sim84] G. J. Simmons. The Prisoners Problem and the subliminal channel. In D. Chaum, editor, *Advances in Cryptology: Proceedings of Crypto'83*, Lecture Notes on Computer Science, pages 51–67. Plenum Press, 1984.

[Sol07] F. I. Solov eva. On $\mathbb{Z}_4$-linear codes with the parameters of Reed–Muller codes. *Problems of Information Transmission*, 43(1):26–32, 2007.

[SW06] D. Schönfeld and A. Winkler. Embedding with syndrome coding based on BCH codes. In S. Voloshynovskiy, J. Dittmann, and J. Fridrich, editors, *Proceedings of the 8th ACM Multimedia and Security Workshop*, pages 214–223, September 2006.

[Tie73] A. Tietäväinen. On the nonexistence of perfect codes over nite elds. *SIAM Journal of Applied Mathematics*, 24(1):88–96, January 1973.

[Vas62] J. L. Vasil ev. On nongroup close-packed codes. *Problemy Kibernetiki*, 8:337–339, 1962. (in Russian).

[vDW01] M. van Dijk and F. Willems. Embedding information in grayscale images. In *Proceedings of the 22nd Symposium on Information and Communication Theory*, 147–154, May 2001.

[WCT05] P.W. Wong, H. Chen, and Z. Tang. On steganalysis of plus-minus one embedding in continuous-tone images. In E. Delp and P.W. Wong, editors, *Proceedings of the SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VII*, volume 5681, pages 643–652, San Jose, CA, January 2005.

[Wes01] A. Westfeld. High capacity despite better steganalysis (F5 - a steganographic algorithm). In I. S. Moskowitz, editor, *Information Hiding. 4th International Workshop*, volume 2137 of *Lecture Notes on Computer Science*, pages 289–302, Berlin Heidelberg, 2001. Springer-Verlag.

[WP00] A. Westfeld and A. P tzmann. Attacks on steganographic systems. In A. P tzmann, editor, *Information Hiding: 3rd International Workshop*, volume 1768 of *Lecture Notes in Computer Science*, pages 61–75. Springer Berlin / Heidelberg, 2000.

[WvD05] F.M.J. Willems and M. van Dijk. Capacity and codes for embedding information in gray-scale signals. *IEEE Transactions on Information Theory*, 51(3):1209–1214, March 2005.

[ZFK+98] J. Zöllner, H. Federrath, H. Klimant, A. P tzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf. Modeling the security of steganographic systems. In D. Aucsmith, editor, *Information Hiding.*

2nd International Workshop, volume 1525 of *Lecture Notes in Computer Science*, pages 344–354. Springer Berlin / Heidelberg, 1998.

[ZL73] V. A. Zinoviev and V. K. Leontiev. The nonexistence of perfect codes over Galois elds. *Problems Control and Information Theory*, 2:123–132, 1973. (in Russian).

[ZL05] W. Zhang and Shiqu Li. Steganographic codes - a new problem of coding theory. Available at (http://arxiv.org/abs/cs/0505072), 2005.

[ZW06] X. Zhang and S. Wang. Ef cient steganographic embedding by exploiting modi cation direction. *IEEE Communications Letters*, 10(11):781–783, 2006.

Appendices

Appendix A

Construction of Additive Reed-Muller Codes

Construction of Additive Reed-Muller Codes*

J. Pujol, J. Rifà, and L. Ronquillo

Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain.

Abstract. The well known Plotkin construction is, in the current paper, generalized and used to yield new families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, whose length, dimension as well as minimum distance are studied. These new constructions enable us to obtain families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes such that, under the Gray map, the corresponding binary codes have the same parameters and properties as the usual binary linear Reed-Muller codes. Moreover, the first family is the usual binary linear Reed-Muller family.

Key Words: $\mathbb{Z}_2\mathbb{Z}_4$-Additive codes, Plotkin construction, Reed-Muller codes, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

1 Introduction

The aim of our paper is to obtain a generalization of the Plotkin construction which gave rise to families of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes such that, after the Gray map, the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-linear codes had the same parameters and properties as the family of binary linear RM codes. Even more, we want the corresponding codes with parameters $(r, m) = (1, m)$ and $(r, m) = (m-2, m)$ to be, respectively, any one of the non-equivalent $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard and $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect codes.

2 Constructions of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

In general, any non-empty subgroup $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code*, where $\mathbb{Z}_2^\alpha$ denotes the set of all binary vectors of length α and $\mathbb{Z}_4^\beta$ is the set of all β-tuples in $\mathbb{Z}_4$.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, and let $C = \Phi(\mathcal{C})$, where $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^n$ is given by the map $\Phi(u_1, \ldots, u_\alpha | v_1, \ldots, v_\beta) = (u_1, \ldots, u_\alpha | \phi(v_1), \ldots, \phi(v_\beta))$ where $\phi(0) = (0, 0)$, $\phi(1) = (0, 1)$, $\phi(2) = (1, 1)$, and $\phi(3) = (1, 0)$ is the usual Gray map from $\mathbb{Z}_4$ onto $\mathbb{Z}_2^2$.

Since the Gray map is distance preserving, the Hamming distance of a $\mathbb{Z}_2\mathbb{Z}_4$-linear code C coincides with the Lee distance computed on the $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C} = \phi^{-1}(C)$.

* This work has been partially supported by the Spanish MICINN Grants MTM2006-03250, TSI2006-14005-C02-01, PCI2006-A7-0616 and also by the *Comissionat per a Universitats i Recerca de la Generalitat de Catalunya* under grant FI2008.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is also isomorphic to an abelian structure like $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$. Therefore, $\mathcal{C}$ has $|\mathcal{C}| = 2^{\gamma} 4^{\delta}$ codewords and, moreover, $2^{\gamma+\delta}$ of them are of order two. We call such code $\mathcal{C}$ a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code of type* $(\alpha, \beta; \gamma, \delta)$ and its binary image $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_2\mathbb{Z}_4$-*linear code of type* $(\alpha, \beta; \gamma, \delta)$.

Although $\mathcal{C}$ may not have a basis, it is important and appropriate to define a generator matrix for $\mathcal{C}$ as:

$$\mathcal{G} = \left(\begin{array}{c|c} B_2 & Q_2 \\ \hline B_4 & Q_4 \end{array} \right), \tag{1}$$

where B_2 and B_4 are binary matrices of size $\gamma \times \alpha$ and $\delta \times \alpha$, respectively; Q_2 is a $\gamma \times \beta$-quaternary matrix which contains order two row vectors; and Q_4 is a $\delta \times \beta$-quaternary matrix with order four row vectors.

2.1 Plotkin construction

In this section we show that the well known Plotkin construction can be generalized to $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

Definition 1 (Plotkin Construction) *Let $\mathcal{X}$ and $\mathcal{Y}$ be any two $\mathbb{Z}_2\mathbb{Z}_4$-additive codes of types $(\alpha, \beta; \gamma_{\mathcal{X}}, \delta_{\mathcal{X}})$, $(\alpha, \beta; \gamma_{\mathcal{Y}}, \delta_{\mathcal{Y}})$ and minimum distances $d_{\mathcal{X}}$, $d_{\mathcal{Y}}$, respectively. If $\mathcal{G}_{\mathcal{X}}$ and $\mathcal{G}_{\mathcal{Y}}$ are the generator matrices of $\mathcal{X}$ and $\mathcal{Y}$, then the matrix*

$$\mathcal{G}_P = \begin{pmatrix} \mathcal{G}_{\mathcal{X}} & \mathcal{G}_{\mathcal{X}} \\ 0 & \mathcal{G}_{\mathcal{Y}} \end{pmatrix}$$

is the generator matrix of a new $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$.

Proposition 2 *Code $\mathcal{C}$ defined above is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(2\alpha, 2\beta; \gamma, \delta)$, where $\gamma = \gamma_{\mathcal{X}} + \gamma_{\mathcal{Y}}$, $\delta = \delta_{\mathcal{X}} + \delta_{\mathcal{Y}}$, binary length $n = 2\alpha + 4\beta$, size $2^{\gamma+2\delta}$ and minimum distance $d = \min\{2d_{\mathcal{X}}, d_{\mathcal{Y}}\}$.*

2.2 BA-Plotkin construction

Applying two Plotkin constructions, one after another, but slightly changing the submatrices in the generator matrix, we obtain a new construction with interesting properties with regard to the minimum distance of the generated code. We call this new construction *BA-Plotkin construction.*

Given a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ with generator matrix $\mathcal{G}$ we denote, respectively, by $\mathcal{G}[b_2]$, $\mathcal{G}[q_2]$, $\mathcal{G}[b_4]$ and $\mathcal{G}[q_4]$ the four submatrices B_2, Q_2, B_4, Q_4 of $\mathcal{G}$ defined in (1); and by $\mathcal{G}[b]$ and $\mathcal{G}[q]$ the submatrices of $\mathcal{G}$, $\left(\begin{array}{c} B_2 \\ \hline B_4 \end{array} \right)$, $\left(\begin{array}{c|c} Q_2 \\ \hline Q_4 \end{array} \right)$, respectively.

Definition 3 (BA-Plotkin Construction) *Let $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ be any three $\mathbb{Z}_2\mathbb{Z}_4$-additive codes of types $(\alpha, \beta; \gamma_{\mathcal{X}}, \delta_{\mathcal{X}})$, $(\alpha, \beta; \gamma_{\mathcal{Y}}, \delta_{\mathcal{Y}})$, $(\alpha, \beta; \gamma_{\mathcal{Z}}, \delta_{\mathcal{Z}})$ and minimum distances $d_{\mathcal{X}}$, $d_{\mathcal{Y}}$, $d_{\mathcal{Z}}$, respectively. Let $\mathcal{G}_{\mathcal{X}}$, $\mathcal{G}_{\mathcal{Y}}$ and $\mathcal{G}_{\mathcal{Z}}$ be the generator matrices*

of the $\mathbb{Z}_2\mathbb{Z}_4$-additive codes $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, respectively. We define a new code $\mathcal{C}$ as the $\mathbb{Z}_2\mathbb{Z}_4$-additive code generated by

$$\mathcal{G}_{BA} = \left(\begin{array}{cc|cccccc} \mathcal{G}_{\mathcal{X}}[b] & \mathcal{G}_{\mathcal{X}}[b] & 2\mathcal{G}_{\mathcal{X}}[b] & \mathcal{G}_{\mathcal{X}}[q] & \mathcal{G}_{\mathcal{X}}[q] & \mathcal{G}_{\mathcal{X}}[q] & \mathcal{G}_{\mathcal{X}}[q] \\ 0 & \mathcal{G}_{\mathcal{Y}}[b_2] & \mathcal{G}_{\mathcal{Y}}[b_2] & 0 & 2\mathcal{G}'_{\mathcal{Y}}[q_2] & \mathcal{G}'_{\mathcal{Y}}[q_2] & 3\mathcal{G}'_{\mathcal{Y}}[q_2] \\ 0 & \mathcal{G}_{\mathcal{Y}}[b_4] & \mathcal{G}_{\mathcal{Y}}[b_4] & 0 & \mathcal{G}_{\mathcal{Y}}[q_4] & 2\mathcal{G}_{\mathcal{Y}}[q_4] & 3\mathcal{G}_{\mathcal{Y}}[q_4] \\ \mathcal{G}_{\mathcal{Y}}[b_4] & \mathcal{G}_{\mathcal{Y}}[b_4] & 0 & 0 & 0 & \mathcal{G}_{\mathcal{Y}}[q_4] & \mathcal{G}_{\mathcal{Y}}[q_4] \\ 0 & \mathcal{G}_{\mathcal{Z}}[b] & 0 & 0 & 0 & 0 & \mathcal{G}_{\mathcal{Z}}[q] \end{array}\right),$$

where $\mathcal{G}'_{\mathcal{Y}}[q_2]$ is the matrix obtained from $\mathcal{G}_{\mathcal{Y}}[q_2]$ after switching twos by ones in its $\gamma_{\mathcal{Y}}$ rows of order two, and considering the ones from the third column of the construction as ones in the quaternary ring $\mathbb{Z}_4$.

Proposition 4 *Code $\mathcal{C}$ defined above is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(2\alpha, \alpha + 4\beta; \gamma, \delta)$ where $\gamma = \gamma_{\mathcal{X}} + \gamma_{\mathcal{Z}}$, $\delta = \delta_{\mathcal{X}} + \gamma_{\mathcal{Y}} + 2\delta_{\mathcal{Y}} + \delta_{\mathcal{Z}}$, binary length $n = 4\alpha + 8\beta$, size $2^{\gamma+2\delta}$ and minimum distance $d = \min\{4d_{\mathcal{X}}, 2d_{\mathcal{Y}}, d_{\mathcal{Z}}\}$.*

3 Additive Reed-Muller codes

We will refer to $\mathbb{Z}_2\mathbb{Z}_4$-additive Reed-Muller codes as $\mathcal{ARM}$. Just as there is only one RM family in the binary case, in the $\mathbb{Z}_2\mathbb{Z}_4$-additive case there are $\lfloor \frac{m+2}{2} \rfloor$ families for each value of m. Each one of these families will contain any of the $\lfloor \frac{m+2}{2} \rfloor$ non-isomorphic $\mathbb{Z}_2\mathbb{Z}_4$-linear extended perfect codes which are known to exist for any m [3].
We will identify each family $\mathcal{ARM}_s(r, m)$ by a subindex $s \in \{0, \ldots, \lfloor \frac{m}{2} \rfloor\}$.

3.1 The families of $\mathcal{ARM}(r, 1)$ and $\mathcal{ARM}(r, 2)$ codes

We start by considering the case $m = 1$, that is the case of codes of binary length $n = 2^1$. The $\mathbb{Z}_2\mathbb{Z}_4$-additive Reed-Muller code $\mathcal{ARM}(0, 1)$ is the repetition code, of type $(2, 0; 1, 0)$ and which only has one nonzero codeword (the vector with only two binary coordinates of value 1). The code $\mathcal{ARM}(1, 1)$ is the whole space $\mathbb{Z}_2^2$, thus a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(2, 0; 2, 0)$. Both codes $\mathcal{ARM}(0, 1)$ and $\mathcal{ARM}(1, 1)$ are binary codes with the same parameters and properties as the corresponding binary $RM(r, 1)$ codes (see [8]). We will refer to them as $\mathcal{ARM}_0(0, 1)$ and $\mathcal{ARM}_0(1, 1)$, respectively.

The generator matrix of $\mathcal{ARM}_0(0, 1)$ is $\mathcal{G}_0(0, 1) = \begin{pmatrix} 1 & 1 \end{pmatrix}$ and the generator matrix of $\mathcal{ARM}_0(1, 1)$ is $\mathcal{G}_0(1, 1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

For $m = 2$ we have two families, $s = 0$ and $s = 1$, of additive Reed-Muller codes of binary length $n = 2^2$. The family $\mathcal{ARM}_0(r, 2)$ consists of binary codes obtained from applying the Plotkin construction defined in Proposition 2 to the family $\mathcal{ARM}_0(r, 1)$. For $s = 1$, we define $\mathcal{ARM}_1(0, 2)$, $\mathcal{ARM}_1(1, 2)$ and $\mathcal{ARM}_1(2, 2)$ as the codes with generator matrices $\mathcal{G}_1(0, 2) = \left(\begin{array}{cc|c} 1 & 1 & 2 \end{array}\right)$, $\mathcal{G}_1(1, 2) = \left(\begin{array}{cc|c} 1 & 1 & 2 \\ \hline 0 & 1 & 1 \end{array}\right)$ and $\mathcal{G}_1(2, 2) = \left(\begin{array}{cc|c} 1 & 1 & 2 \\ 0 & 1 & 0 \\ \hline 0 & 1 & 1 \end{array}\right)$, respectively.

3.2 Plotkin and BA-Plotkin constructions

Take the family $\mathcal{ARM}_s$ and let $\mathcal{ARM}_s(r, m-1)$, $\mathcal{ARM}_s(r-1, m-1)$ and $\mathcal{ARM}_s(r-2, m-1)$, $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, be three consecutive codes with parameters $(\alpha, \beta; \gamma', \delta')$, $(\alpha, \beta; \gamma'', \delta'')$ and $(\alpha, \beta; \gamma''', \delta''')$; binary length $n = 2^{m-1}$; minimum distances 2^{m-r-1}, 2^{m-r} and 2^{m-r+1}; and generator matrices $\mathcal{G}_s(r, m-1)$, $\mathcal{G}_s(r-1, m-1)$ and $\mathcal{G}_s(r-2, m-1)$, respectively. By using Proposition 2 and Proposition 4 we can prove the following results:

Theorem 5 *For any r and $m \geq 2$, $0 < r < m$, code $\mathcal{ARM}_s(r, m)$ obtained by applying the Plotkin construction from Definition 1 on codes $\mathcal{ARM}_s(r, m-1)$ and $\mathcal{ARM}_s(r-1, m-1)$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(2\alpha, 2\beta; \gamma, \delta)$, where $\gamma = \gamma' + \gamma''$ and $\delta = \delta' + \delta''$; binary length $n = 2^m$; size 2^k codewords, where $k = \sum_{i=0}^{r} \binom{m}{i}$; minimum distance 2^{m-r} and $\mathcal{ARM}_s(r-1, m) \subset \mathcal{ARM}_s(r, m)$.*

We consider $\mathcal{ARM}_s(0, m)$ to be the repetition code with only one nonzero codeword (the vector with 2α ones and 2β twos) and $\mathcal{ARM}_s(m, m)$ be the whole space $\mathbb{Z}_2^{2\alpha} \times \mathbb{Z}_4^{2\beta}$.

Theorem 6 *For any r and $m \geq 3$, $0 < r < m$, $s > 0$, use the BA-Plotkin construction from Definition 3, where generator matrices $\mathcal{G}_\mathcal{X}$, $\mathcal{G}_\mathcal{Y}$, $\mathcal{G}_\mathcal{Z}$ stand for $\mathcal{G}_s(r, m-1)$, $\mathcal{G}_s(r-1, m-1)$ and $\mathcal{G}_s(r-2, m-1)$, respectively, to obtain a new $\mathbb{Z}_2\mathbb{Z}_4$-additive $\mathcal{ARM}_{s+1}(r, m+1)$ code of type $(2\alpha, \alpha + 4\beta; \gamma, \delta)$, where $\gamma = \gamma' + \gamma'''$, $\delta = \delta' + \gamma'' + 2\delta'' + \delta'''$; binary length $n = 2^{m+1}$; 2^k codewords, where $k = \sum_{i=0}^{r} \binom{m+1}{i}$, minimum distance 2^{m-r+1} and, moreover, $\mathcal{ARM}_{s+1}(r-1, m+1) \subset \mathcal{ARM}_{s+1}(r, m+1)$.*

To be coherent with all notations, code $\mathcal{ARM}_{s+1}(-1, m+1)$ is defined as the all zero codeword code, code $\mathcal{ARM}_{s+1}(0, m+1)$ is defined as the repetition code with only one nonzero codeword (the vector with 2α ones and $\alpha + 4\beta$ twos), whereas codes $\mathcal{ARM}_{s+1}(m, m+1)$ and $\mathcal{ARM}_{s+1}(m+1, m+1)$ are defined as the even Lee weight code and the whole space $\mathbb{Z}_2^{2\alpha} \times \mathbb{Z}_4^{\alpha+4\beta}$, respectively.

Using both Theorem 5 and Theorem 6 we can now construct all $\mathcal{ARM}_s(r, m)$ codes for $m > 2$. Once applied the Gray map, all these codes give rise to binary codes with the same parameters and properties as the RM codes. Moreover, when $m = 2$ or $m = 3$, they also have the same codewords.

References

1. J. Borges, J. Rifà, A characterization of 1-perfect additive codes. *IEEE Trans. Inform. Theory*, 45(5): 1688-1697, 1999.
2. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 1977.

Appendix B

Product perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes in steganography

Product Perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes in Steganography

Josep Rifà and Lorena Ronquillo
Department of Information and Communications Engineering,
Universitat Autònoma de Barcelona,
08193-Cerdanyola del Vallès, Spain.
Email: Josep.Rifa@autonoma.edu, Lorena.Ronquillo@autonoma.edu

***Abstract*—Product perfect codes have been proven to enhance the performance of the $F5$ steganographic method, whereas perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes have been recently introduced as an efficient way to embed data, conforming to the ±1-steganography. In this paper, we present two steganographic methods. On the one hand, a generalization of product perfect codes is made. On the other hand, this generalization is applied to perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. Finally, the performance of the proposed methods is evaluated and compared with those of the aforementioned schemes.**

I. Introduction

Digital steganography is an information hiding application which consists of hiding data within seemingly innocuous host media, by distorting it in such a way that unintended recipients are not only unable to detect the presence of embedded data, but also given no reason for suspecting that anything is unusual. This is the main difference from encryption, which only prevents the adversary from decoding the message and not from suspecting that a secret message is being sent.

Many steganographic schemes have been developed and proposed. One well known scheme is *matrix encoding*, first introduced by Crandall [5] and later analyzed by Bierbrauer et al. [2], which requires the sender and the recipient to agree in advance on a parity check matrix H, and the secret message is then extracted by the recipient as the syndrome (with respect to H) of the received cover object. This method was made popular by Westfeld [10], who incorporated a specific implementation using Hamming codes. The resulting method is known as the $F5$ algorithm, and it can embed t bits of message in 2^t-1 cover symbols by changing, at most, one of them.

As Willems et al. in [11], we will also assume that a discrete source produces a sequence $\mathbf{x}=(x_1,\dots,x_N)$, where N is the block length, $x_i\in\aleph=\{0,1,\dots,2^B-1\}$, and $B\in\{8,12,16\}$ depends on the kind of source (digital image, CD audio, etc). Let $\mathbf{s}\in\{1,\dots,M\}$ be the message we want to hide into a host sequence $\mathbf{x}$, which produces a composite sequence $\mathbf{y}=f(\mathbf{x},\mathbf{s})$, for $\mathbf{y}=(y_1,\dots y_N)$ and $y_i\in\aleph$. The sequence $\mathbf{y}$ is obtained from distorting $\mathbf{x}$, and that distortion will be assumed to be of squared-error type (see [11]), that is $|\mathbf{y}-\mathbf{x}|^2=\sum_{i=1}^N|y_i-x_i|^2$. In these conditions, information can be carried by the least significant bit (LSB) or by the two least significant bits of each x_i. An appropriate solution for the first case comes from applying the $F5$ algorithm [10], which has been improved in [7] by using the Kronecker product of the corresponding generator matrices of two binary perfect codes. The latter case is known as "±1-steganography" and the magnitude of changes is limited to 1, that is, $y_i=x_i+c$, where $c\in\{0,+1,-1\}$. This case has usually involved the use of ternary codes [6], [11] until the results from [8], which introduces a method based on perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. This kind of codes are not linear but have a representation using a parity check matrix that makes them as efficient as the Hamming codes. The steganographic method therein presented not only outperforms the one obtained by direct sum of ternary Hamming codes, but it also deals better with the boundary grayscale values problem. That is, the problem we may have when the steganographic method requires adding one unit to a grayscale value which already has the maximum allowed value 2^B-1, or substracting one unit from a grayscale of value 0. Schemes from [6], [11] suggest, in these cases, performing changes of magnitude greater than one, while the magnitude of changes performed by the method in [8] is never greater than one.

The following two parameters are often used to evaluate the performance of a steganographic method over a cover message of N symbols: the *average distortion* $D=\frac{R_a}{N}$, where R_a is the expected number of changes over uniformly distributed messages; and the *embedding rate* $E=\frac{t}{N}$, which is the amount of bits that can be hidden in a cover message. Given two methods with the same embedding rate, the one with smaller average distortion is better. Following the terminology used by Fridrich et al. [6], the tuple (D,E) will be called *CI-rate*. However, when plotting the performance results of a steganographic scheme we will use what we have called the *normalized embedding rate* e, instead of the embedding rate E.

Let $H_q(x)=\frac{1}{\log_2(q)}(H(x)+x\log_2(q-1))$ be the q-ary entropy function [1] on the interval $[0,(q-1)/q]$, where $H(x)=-x\log_2(x)-(1-x)\log_2(1-x)$ is the usual binary entropy function on the interval $[0,1/2]$. The normalized embedding rate is the ratio $e=\frac{{H_q}^{-1}(E)}{D}$, where ${H_q}^{-1}(\cdot)$ is the inverse of the q-ary entropy function $H_q(x)$. In the binary case, e will be computed by considering the binary entropy function $H_2(x)$, whereas in the ±1-steganography the

This work was partially supported by the Spanish MICINN Grants MTM2009-08435, PCI2006-A7-0616, and also by the *Comissionat per a Universitats i Recerca del DIUE de la Generalitat de Catalunya* and the *European Social Fund* with Grants 2009SGR1224 and FI-DGR.

ternary entropy function $H_3(x)$ is used. One of the purposes of steganographic methods is to approach the upper bound on the normalized embedding rate e subject to the constraint of an average distortion D. This upper bound on e for a fixed D is $e \leq 1$, and it has the advantage of being the same for any kind of steganography, either binary or ± 1-steganography.

In this paper we propose a technique based on products of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes and compare its performance with that of product binary perfect codes [7] and perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes [8].

The current paper has been organized as follows. Some basic concepts on perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, as well as the steganographic method based on these codes [8], are reviewed in Section II. Then, Section III reviews the product perfect codes method [7] and presents a generalization that enhances its performance. In Section IV, this generalization is used for perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes in ± 1-steganography. Finally, the paper is concluded in Section V.

II. Perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes and steganography

Any non-empty subgroup $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code*, where $\mathbb{Z}_2^\alpha$ denotes the set of all binary vectors of length α and $\mathbb{Z}_4^\beta$ is the set of all quaternary vectors of length β. Let ϕ be the usual *Gray map* from $\mathbb{Z}_4$ onto $\mathbb{Z}_2^2$, where $\phi(0) = (0,0)$, $\phi(1) = (0,1)$, $\phi(2) = (1,1)$, and $\phi(3) = (1,0)$; and let $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^n$ be the *extended Gray map* given by

$$\Phi(u_1, \ldots, u_\alpha | v_1, \ldots, v_\beta) = (u_1, \ldots, u_\alpha | \phi(v_1), \ldots, \phi(v_\beta)).$$

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is isomorphic to an abelian structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ has $|\mathcal{C}| = 2^\gamma 4^\delta$ codewords, where $2^{\gamma+\delta}$ of them are of order two. We call such code $\mathcal{C}$ a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code of type* $(\alpha, \beta; \gamma, \delta)$ and its binary image $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_2\mathbb{Z}_4$-*linear code of type* $(\alpha, \beta; \gamma, \delta)$. Note that the Lee distance of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ coincides with the Hamming distance of the $\mathbb{Z}_2\mathbb{Z}_4$-linear code C, and that the binary code C may not be linear.

The $\mathbb{Z}_2\mathbb{Z}_4$-*additive dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined as the set of vectors in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ that are orthogonal to every codeword in $\mathcal{C}$, being the definition of inner product in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ the following (see [3]):

$$\langle u, v \rangle = 2(\sum_{i=1}^{\alpha} u_i v_i) + \sum_{j=\alpha+1}^{\alpha+\beta} u_j v_j \in \mathbb{Z}_4, \qquad (1)$$

where $u, v \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and computations are made considering the zeros and ones in the α binary coordinates as quaternary zeros and ones, respectively.

The binary code $C_\perp = \Phi(\mathcal{C}^\perp)$, of length $n = \alpha + 2\beta$, is called the $\mathbb{Z}_2\mathbb{Z}_4$-*dual code* of C.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is said to be *perfect* if code $C = \Phi(\mathcal{C})$ is a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code, that is all vectors in $\mathbb{Z}_2^n$ are within distance one from a codeword and the distance between two codewords is, at least, 3.

It is well known [4] that for any $m \geq 2$ and each $\delta \in \{0, \ldots, \lfloor \frac{m}{2} \rfloor\}$ there exists a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code C of binary length $n = 2^m - 1$, such that its $\mathbb{Z}_2\mathbb{Z}_4$-dual code is of type $(\alpha, \beta; \gamma, \delta)$, where $\alpha = 2^{m-\delta} - 1$, $\beta = 2^{m-1} - 2^{m-\delta-1}$ and $\gamma = m - 2\delta$ (note that the binary length can be computed as $n = \alpha + 2\beta$). This allows us to write the parity check matrix $\mathcal{H}_\mathcal{C}$ of any $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect code $\mathcal{C}$ for a given value of δ. Matrix $\mathcal{H}_\mathcal{C}$ can be represented by taking as columns all possible vectors in $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$, up to sign changes. In this representation, there are α columns which correspond to the binary part of codewords in $\mathcal{C}$, and β columns of order four which correspond to the quaternary part. We agree on a representation of the α binary coordinates as coordinates in $\{0, 2\} \in \mathbb{Z}_4$. Let $\mathbf{h}_i$, for $i \in \{1, \ldots, \alpha + \beta\}$, denote the i-th column vector of $\mathcal{H}_\mathcal{C}$.

Now we proceed to review how a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ can be used in steganography. Considering its $\mathbb{Z}_2\mathbb{Z}_4$-dual code, of type $(\alpha, \beta; \gamma, \delta)$, we have a parity check matrix $\mathcal{H}_\mathcal{C}$ with γ rows of order two and δ rows of order four.

Take $N = 2^{m-1}$ and let $\mathbf{x} = (x_1, \ldots, x_N)$ be a source of grayscale symbols such that $x_i \in \aleph = \{0, 1, \ldots, 2^B - 1\}$, where, for instance, $B = 8$ for grayscale images.

We assume each grayscale symbol x_i is represented as a binary vector $(v_{(B-1)i}, \ldots, v_{1i}, v_{0i})$, obtained by first representing x_i in base 4 and then applying the Gray map ϕ to every quaternary symbol in the base 4 representation. For example, the grayscale value 239 is represented as the quaternary vector (3233), which then gives rise to the binary vector (10111010) after applying the Gray map ϕ.

The N-length packet $\mathbf{x}$ of symbols is translated into a vector $\mathbf{w}$ of α binary and β quaternary coordinates. The binary coordinates come from taking the least significant bit of the binary representation of x_1, that is v_{01}, along with the two least significant bits v_{1i}, v_{0i} of the following $(\alpha + 1)/2$ grayscale symbols x_i. The quaternary coordinates of $\mathbf{w}$ come from taking the two least significant bits of the last β symbols x_i and interpreting them as integer numbers $\phi^{-1}(v_{1i}, v_{0i})$ in $\mathbb{Z}_4$.

The obtained vector $\mathbf{w} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is then distorted according to the matrix encoding method [5], [10] in such a way that $\mathcal{H}_\mathcal{C}\mathbf{w}^T + \epsilon\mathbf{h}_i = \mathbf{s}$ holds, where $\mathbf{s} \in \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ is the secret message we want to embed in the source $\mathbf{x}$, the value of ϵ can be $\{0, 1, 3\}$, the syndrome vector of $\mathbf{w}$ is $\mathcal{H}_\mathcal{C}\mathbf{w}^T$, and $\mathbf{h}_i$ is a column vector in $\mathcal{H}_\mathcal{C}$. This method also deals with boundary grayscale values in a rather efficient way: instead of distorting a symbol x_i having a boundary value (0 or $2^B - 1$) in a way that would lead its value out of the range defined by $\aleph$, two other symbols are changed one magnitude. One of these symbols is always x_1. Since we are using a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code, with this scheme we might need to modify one coordinate or two coordinates (to deal with boundary values problems) from $\mathbf{w}$, and this distortion will involve having to add or substract one unit to/from the corresponding grayscale value. Note that the magnitude of change is never greater than 1. Thus considering the squared-error distortion, the distortion caused by this scheme is lower than that of the schemes in [6], [11]. It is easy to see that this method has

CI-rate $(D_m, E_m) = \left(\frac{2N-1+\frac{N-1}{2^{B-2}}}{2N^2}, \frac{1+\log(N)}{N}\right)$. We refer the reader to [8] for further details and examples on the steganographic scheme based on perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

III. Product of perfect codes and steganography

Let $\mathbb{F}_q$ be a finite field of q elements, where q is a prime power. Let C be a Hamming code over $\mathbb{F}_q$ of length $n = \frac{q^m-1}{q-1}$ and dimension $n-m$. Let G_C, H_C be, respectively, a generator matrix and a parity check matrix for C.

Definition 1: The Kronecker product of two matrices $A = [a_{r,t}]$ and $K = [k_{i,j}]$ over $\mathbb{F}_q$ is a new matrix $A \otimes K$ obtained by changing every element $a_{r,t}$ in A by the matrix $a_{r,t}K$.

The q-ary code $C^{\perp}_{H_C \otimes H_C}$, that is the dual of the code constructed by taking $H_C \otimes H_C$ as generator matrix, is a $[n^2, n^2 - m^2]$ code with covering radius $\rho_{C^{\perp}_{H_C \otimes H_C}} = m$ (see [9]). Codewords of $C^{\perp}_{H_C \otimes H_C}$ can be seen as $n \times n$ matrices whose rows or columns are codewords in the q-ary Hamming code C.

The q-ary code $C_{G_C \otimes G_C}$, constructed from the generator matrix $G_C \otimes G_C$ is a $[n^2, (n-m)^2]$ code with covering radius $\rho_{C_{G_C \otimes G_C}} = n + 1 + 2(n-m-1)$ [9], whose codewords can be seen as $n \times n$ matrices where both rows and columns are codewords in the q-ary Hamming code C. We will refer to code $C_{G_C \otimes G_C}$ as *product code*.

There is an efficient steganographic method [7] which uses the above defined code $C_{G_C \otimes G_C}$, for $q = 2$, to embed data. Given two binary Hamming codes of the same length $n = 2^m - 1$, their product gives a linear code of length $n = (2^m - 1)^2$, dimension $(n-m)^2$ and whose codewords can be seen as $(2^m-1) \times (2^m-1)$ matrices where every row and every column are codewords in the binary Hamming code. The embedding scheme therefore consists of first taking blocks in the cover source of size $(2^m - 1) \times (2^m - 1)$, and then applying the $F5$ algorithm to every row and to the first c columns, for $1 \leq c \leq 2^{m-1} - 1$. As proved in [7], the performance one can obtain with this method is better than the one obtained by just using the conventional $F5$ algorithm on the corresponding codes with the same average distortion. We refer to [7] for further details on this method.

Now, in this paper we will proceed with a generalization of the above procedure, by taking the product of more than two q-ary Hamming codes.

As defined at the beginning of this section, let C be a q-ary Hamming code of length $n = \frac{q^m-1}{q-1}$, dimension $n-m$, with generator matrix G_C and parity check matrix H_C. Take the code C' of all the $n \times n$ matrices such that all their rows, as well as their first column, are codewords in C. Code C' is a $[n^2, n(n-m)-m]$ code, $C_{G_C \otimes G_C} \subset C' \subset C^{\perp}_{H_C \otimes H_C}$ with covering radius $\rho_{C'} = n + 1$.

For the sake of a well understanding, the following reasoning will be limited to the binary case. However, a generalization to the q-ary case is straightforward.

Just as the method based on the product of two Hamming codes from [7], this procedure consists of a row embedding and a column embedding steps. We will take the LSB bit of every grayscale symbol in the cover source and form blocks of size $n \times n$, where $n = 2^m - 1$. Let $c_{i,j}$ be the coordinate in the i-th row and j-th column of these blocks, where $i, j \in \{1, \ldots, n\}$.

1) Rows Embedding:

   The matrix encoding standard procedure [5], [10] applied to every row lets us embed $\frac{m}{n}$ bits with an average distortion of $\frac{1}{n+1}$ coordinates, thus giving a CI-rate of $(\frac{1}{n+1}, \frac{m}{n})$.

2) Column Embedding:

   After processing all rows, we can embed $\frac{m}{n}$ additional bits with an average distortion of $\frac{1}{n+1}$ by applying the same standard procedure to the first column.
   However, note that the following situations can happen when processing this column:

   - No coordinate needs to be changed in $\frac{1}{n+1}$ cases because the first column may already have, by chance, the desired value.
   - We may need to change a coordinate $c_{i,1}$ in $\frac{n}{n+1}$ cases. In this case, the i-th row may have been already modified in the corresponding row embedding with a probability of $\frac{n}{n+1}$, while it may have not been modified with a probability of $\frac{1}{n+1}$.
     Let us consider the i-th row was modified in the j-th coordinate, $c_{i,j}$, for $j > 1$. In this case, we will also have to restore the original value of $c_{i,j}$ and distort another appropiate coordinate $c_{i,k}$, for $k \in \{2, \ldots, n\}$ and $k \neq j$, such that the distortion being introduced now by the column embedding is compensated and does not affect the embedding in the i-th row (see Lemma 2 from [7]). Note that this situation is also including the case in which the coordinate that was modified during the i-th row embedding is precisely the coordinate $c_{i,1}$ we now need to change to embed data in the column. In summary, if the i-th row was modified, no matter in which coordinate, the column embedding step will introduce one distortion besides the ones introduced by the row embedding step.

     Otherwise, if during the column embedding we need to distort a coordinate $c_{i,1}$ and the i-th row was not modified, then we will also need to distort two more coordinates within the same row, $c_{i,j}$ and $c_{i,k}$, for $j, k \in \{2, \ldots, n\}$ and $j \neq k$, to make up for this distortion. Hence, the column embedding step will be now introducing three changes.

In short, we can leave invariant the average distortion of the row embedding step, but $\frac{(n+3)/(n+1)}{n+1}$ should be added for the embedding in the first column. Note that this is only a tight upper bound on the average distortion, as we will later show.

By the method just described we can embed m bits into the first column and also in every row of the matrix; therefore, we

embed $(n+1)m$ bits in n^2 coordinates. The average distortion is upper bounded by $\frac{(n+3)/(n+1)}{n+1}$ for the coordinates in the first column and $\frac{1}{n+1}$ in each of the n rows. Summing this up, the average distortion is bounded by $\frac{n\frac{(n+3)/(n+1)}{n+1}+n^2\frac{1}{n+1}}{n^2} = \frac{1}{n+1}\left(1+\frac{(n+3)/(n+1)}{n}\right)$.

The method we propose in the present paper consists of repeating over and over the same procedure we have just described. Hence, we can generalize the computations of the average distortion and the embedding rate by using ${G_C}^l = G_C \otimes (G_C \otimes \cdots \otimes G_C)$. In each step ${G_C}^l = G_C \otimes {G_C}^{l-1}$, only the first column in the first component G_C will be used to embed information.

Let D_l be the average distortion at the l-th step. As computed before, we have $D_1 = \frac{1}{n+1}$ and $D_2 = \frac{1}{n+1}(1 + \frac{(n+3)/(n+1)}{n})$. In the general case we have:

$$D_l = \frac{1}{n+1} + \xi D_{l-1},$$

where $\xi = \frac{n+3}{n(n+1)}$.

Now, the overall average distortion can be computed as $\frac{1}{n+1}\left(1+\xi+\cdots+\xi^{l-1}\right)$, which converges asymptotically very fast to

$$\frac{1}{n+1}\left(\frac{\xi^l-1}{\xi-1}\right) \to \frac{1}{n+1}\left(\frac{1}{1-\xi}\right) = \frac{1}{n+1}\left(\frac{n(n+1)}{n^2-3}\right).$$

As for the embedding rate, it can be computed as $\frac{(1+n+n^2+\cdots+n^{l-1})m}{n^l}$, which converges to

$$\frac{(1+n+n^2+\cdots+n^{l-1})m}{n^l} = m\frac{\frac{n^l-1}{n-1}}{n^l} \to \frac{m}{n-1}.$$

Finally, we obtain the asymptotical CI-rate $\left(\frac{n}{n^2-3}, \frac{m}{n-1}\right)$.

Note that we are not able to generate an embedding scheme for any CI-rate but only for natural values of m. However, given any non-allowable parameter D for the average distortion, we can always take two codes with CI-rates (D_1, E_1) and (D_2, E_2), where $D_1 < D < D_2$, such that their direct sum gives rise to a new CI-rate (D, E), with $D = \lambda D_1 + (1-\lambda)D_2$ and $E = \lambda E_1 + (1-\lambda)E_2$.

A comparison of the normalized embedding rate $e = \frac{{H_q}^{-1}(E)}{D}$, where $q = 2$, as a function of the average distortion D for the introduced Kronecker product technique (KP-technique) and the standard matrix encoding procedures [5], [10] is shown in Fig. 1. As explained before, this plot has been made by first computing the allowable points (D, e), and then applying the direct sum between the codes corresponding to two contiguous points (D_1, e_1) and (D_2, e_2), where $D_1 < D_2$.

For the sake of simplicity, some particular cases which may produce a lower distortion have been omitted in the computation of the distortion in the above CI-rate. For this reason, the distortion D in that CI-rate is an upper bound. As an example of one of these cases, recall that the column embedding step of our procedure is introducing three distortions when we need to change the $c_{i,1}$ coordinate and the i-th row was not modified in the row embedding step. Note, however, that there is one particular case in which we may need to introduce two distortions instead of three. This happens when there exist two other coordinates in the same column, $c_{j,1}$ and $c_{k,1}$, for $j, k \in \{1, \ldots, n\}$ and $j \neq k$, whose distortion is equivalent to distort only $c_{i,1}$, and both j-th and k-th rows were modified in the row embedding step. It is easy to see that we can distort coordinates $c_{j,1}$ and $c_{k,1}$ instead of $c_{i,1}$, and perform afterwards the appropiate changes to compensate these distortions in the j-th and k-th rows, respectively. Therefore, the column embedding step will be introducing two distortions besides the ones introduced in the row embedding step, and not three, as we previously stated. However, if no two other coordinates, $c_{j,1}$ and $c_{k,1}$ can be found such that both j-th and k-th rows were modified, then the column embedding step does actually introduce three distortions. We have implemented and executed a simulation of the embedding procedure described in this section which considers, among others, this particular case. For this reason the experimental results of the Kronecker product technique ("KP-technique (simulation)" in Fig. 1) have lower average distortion than the results obtained from the above CI-rate (plotted as "KP-technique" in Fig. 1).

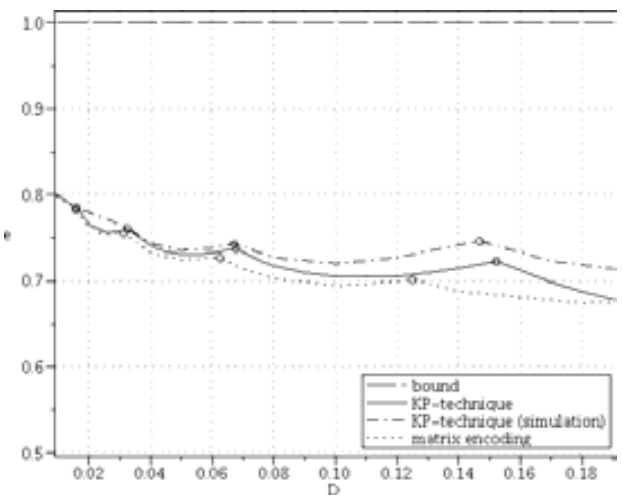

Fig. 1. Normalized embedding rate e as a function of the average distortion D of steganographic methods based on the matrix encoding procedure [5], [10], and on the Kronecker product technique, using an upper bound on the average distortion ("KP-technique") and using the experimental results ("KP-technique (simulation)").

IV. Product of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

The previous procedure deals with Hamming codes. Now, we will apply it to perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect code of type $(\alpha, \beta; \gamma, \delta)$ and binary length $n = 2^m - 1$, for $m \geq 2$, and let $\mathcal{H}_\mathcal{C}$ be its parity check matrix. Take the code $\mathcal{C}'$ whose codewords are all the $n \times N$ matrices, where $N = 2^{m-1}$, such that all rows are codewords in $\mathcal{C}$, and so is the first column after applying the inverse of the extended Gray map Φ.

Take blocks of $n \times N$ grayscale symbols in the source,

$$\begin{matrix} x_{1,1}, & \ldots, & x_{1,N} \\ \vdots & \vdots & \vdots \\ x_{n,1}, & \ldots, & x_{n,N} \end{matrix}$$

where $N = 2^{m-1}$, and translate them into n vectors of α binary and β quaternary coordinates, as reviewed in Section II and explained in depth in [8]. At the same time, the first coordinate of those n vectors is making up a binary vector of length n which can also be seen as a vector of α binary and β quaternary coordinates by means of the inverse of the extended Gray map Φ. Note that by considering the n rows and the first column, we end up having $n+1$ different vectors of binary length n.

The embedding procedure we will apply here is very similar to the KP-technique described in Section III. Once the $n+1$ vectors have been translated into $n+1$ vectors in $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, we will proceed by steps: first, we will apply the embedding scheme from [8] to every row, and then we will apply it to the first column. Each distortion in the rows will involve adding or subtracting one unit to/from a grayscale symbol, and this requires considering the possibility of having extreme grayscale values problems. Recall that, unlike vectors in rows, the vector in the first column is only made up of the least significant bit of n grayscale symbols and not of their two least significant bits. This means that any distortion over a coordinate in this vector will involve a flip in the least significant bit of a grayscale symbol $x_{i,1}$, for $i \in \{1, \ldots, n\}$, which leads us to conclude that, unlike the rows embedding step, no extreme grayscale values problem will ever crop up during the column embedding step.

Furthermore, as in the KP-technique from Section III, during the column embedding step we have to consider different situations. The embedding method may require modifying a certain coordinate in the first column, and this coordinate may correspond to a row which was (or was not) modified during the row embedding step, or to a row that contains two distorted grayscale symbols, probably to deal with an extreme grayscale value problem. In any of these cases the action to be taken may vary, but still the aim is performing the appropriate changes in the affected row so that the distortion being introduced now by the column embedding step does not affect the embedding in the row. Take any two column vectors $\mathbf{h}_j, \mathbf{h}_k$ of order four in matrix $\mathcal{H}_{\mathcal{C}}$, such that one is the complementary of the other, that is $\mathbf{h}_j = \mathbf{h}_k + \mathbf{2}$, where $\mathbf{2}$ is the all-twos vector. The changes above mentioned will consist of considering that any distortion in coordinate $x_{i,1}$, for any $i \in \{1, \ldots, n\}$, can be compensated either by doing $x_{i,j-(\alpha+1)/2} + 1$ and $x_{i,j-(\alpha+1)/2} + 1$ or by doing $x_{i,j-(\alpha+1)/2} - 1$ and $x_{i,j-(\alpha+1)/2} - 1$. Note that, whenever possible, we will avoid modifying those grayscale symbols associated with column vectors in $\mathcal{H}_{\mathcal{C}}$ that are complementary of themselves, because in these cases we would have to distort the associated symbol in two units instead of one, which would not conform to ± 1-steganography.

By means of this method we can embed m bits into the first column $x_{1,1}, \ldots, x_{n,1}$ and also in every row of the block. Since the first column is made up of n grayscale symbols and each row is made up of N symbols, we are actually embedding $(n+1)m$ bits in $nN = n(n+1)/2$ symbols. It is easy to see that an upper bound of the average distortion for the symbols in the first column is $\frac{(n+3)/(n+1)}{(n+1)}$. As for the symbols in each row, the average distortion is given by $\frac{2N-1+\frac{N-1}{2^{B-2}}}{2N^2} = \frac{2n+\frac{n-1}{2^{B-2}}}{(n+1)^2}$ (see Section II). Summing this up, an upper bound for the average distortion is

$$\frac{n\frac{(n+3)/(n+1)}{(n+1)} + \frac{n(n+1)}{2}\frac{2n+\frac{n-1}{2^{B-2}}}{(n+1)^2}}{n(n+1)/2} =$$

$$\frac{2n+\frac{n-1}{2^{B-2}}}{(n+1)^2}\left(\frac{n+3}{(n+\frac{n-1}{2^{B-1}})(n+1)}+1\right).$$

In a similar way as we did in Section III, we can repeat this method over and over and generalize the computations of the average distortion and the embedding rate by taking the code whose codewords are all the l-dimensional matrices, where $l = n \times (n \times \cdots \times n \times N)$, such that their rows and the first component of every dimension are codewords in the $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect code $\mathcal{C}$.

Let D_l be the average distortion at the l-th step. For the first steps we have $D_1 = \frac{2n+\frac{n-1}{2^{B-2}}}{(n+1)^2}$ and $D_2 = \frac{2n+\frac{n-1}{2^{B-2}}}{(n+1)^2}\left(\frac{n+3}{(n+\frac{n-1}{2^{B-1}})(n+1)}+1\right)$. In the general case we have:

$$D_l = \frac{2n+\frac{n-1}{2^{B-2}}}{(n+1)^2} + \xi D_{l-1},$$

where $\xi = \frac{n+3}{(n+\frac{n-1}{2^{B-1}})(n+1)}$.

Now, the overall average distortion can be computed as $\frac{2n+\frac{n-1}{2^{B-2}}}{(n+1)^2}\left(1+\xi+\cdots+\xi^{l-1}\right)$, which converges asymptotically very fast to

$$\frac{2n+\frac{n-1}{2^{B-2}}}{(n+1)^2}\left(\frac{1}{1-\xi}\right).$$

As for the embedding rate, it can be computed as $\frac{(1+n+n^2+\cdots+n^{l-1})m}{Nn^{l-1}}$, which converges to $\frac{mn}{N(n-1)}$.

Finally, we obtain a CI-rate of $\left(\frac{2n+\frac{n-1}{2^{B-2}}}{(n+1)^2}(\frac{1}{1-\xi}), \frac{mn}{N(n-1)}\right)$.

Fig. 2 shows a comparison of the normalized embedding rate $e = \frac{{H_q}^{-1}(E)}{D}$, for $q = 3$, as a function of the average distortion D for the steganographic method based on perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes [8], the one based on ternary Hamming codes [6], [11] and the new method based on the product of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. Recall that the distortion we have computed in the above CI-rate is an upper bound on the average distortion, meaning that lower distortion can be achieved in some particular cases, as it happened in the simulation results from Section III.

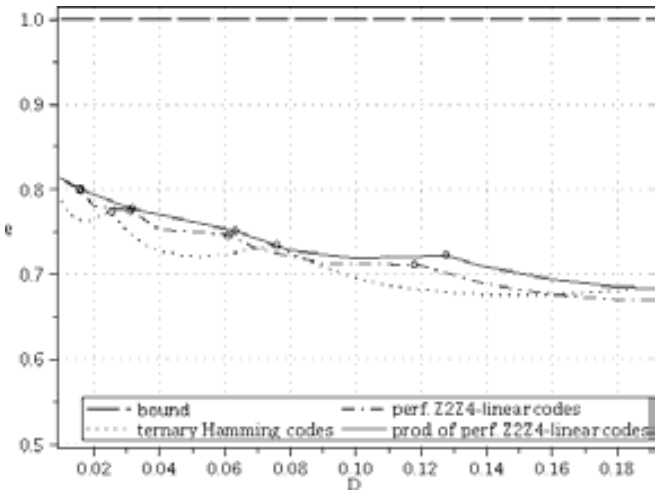

Fig. 2. Normalized embedding rate e as a function of the average distortion D, of steganographic methods based on perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes [8] ("perf. Z2Z4-linear codes"), on ternary Hamming codes [6], [11] and on the product of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes ("prod. of perf. Z2Z4-linear codes").

V. Conclusions

The use of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes in ± 1-steganography was first proposed in [8]. This method has a better performance compared to those based on the direct sum of ternary Hamming codes from [6] and [11], and also deals with boundary grayscale values more efficiently, because unlike methods in [6] and [11], no changes of magnitude greater than one are ever made.

In this paper we have presented a technique based on products of these perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. Therefore, the proposed method has all the advantages related to the performance and the processing of extreme grayscale values compared to the techniques based on the direct sum of ternary Hamming codes. Furthermore, we have shown that it performs better than the method in [8].

References

[1] J. Bierbrauer, "Crandall's problem" (Available from http://www.ws.binghamton.edu/fridrich/covcodes.pdf), 1998.

[2] J. Bierbrauer and J. Fridrich, "Constructing good covering codes for applications in steganography", in Transactions on Data Hiding and Multimedia Security III, vol. 4920 of Lecture Notes in Computer Science, pp. 1-22, Springer, Berlin, Germany, 2008.

[3] J. Borges, C. Fernández, J. Pujol, J. Rifà and M. Villanueva, "Z2Z4-linear codes: generator matrices and duality", Desings, Codes and Cryptography, vol. 54(2), pp. 167-179, January, 2010.

[4] J. Borges and J. Rifà, "A characterization of 1-perfect additive codes", IEEE Trans. Information Theory, vol. 45(5), pp. 1688-1697, 1999.

[5] R. Crandall, "Some notes on steganography", (Available from http://os.inf.tu-dresden.de/∼westfeld/crandall.pdf), 1998.

[6] J. Fridrich and P. Lisoněk, "Grid colorings in steganography", IEEE Trans. Information Theory, vol. 53(4), pp. 1547-1549, April, 2007.

[7] H. Rifà-Pous and J. Rifà, "Product perfect codes and steganography", Digital Signal Processing, vol. 19(4), pp. 764-769, July, 2009.

[8] H. Rifà-Pous, J. Rifà and L. Ronquillo, "Perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes in steganography", (Available from http://arxiv.org/abs/1002.0026v2), February, 2010.

[9] J. Rifà and V. Zinoviev, "New completely regular q-ary codes based on Kronecker products", IEEE Trans. Information Theory, vol. 56(1), pp. 266-272, January, 2010.

[10] A. Westfeld, "High capacity despite better steganalysis (F5 - A steganographic algorithm)", vol. 2137 of Lecture Notes in Computer Science, pp. 289-302, Springer-Verlag, 2001.

[11] F.M.J. Willems and M. van Dijk, "Capacity and codes for embedding information in grayscale signals", IEEE Trans. Information Theory, vol. 51(3), pp. 1209-1214, March, 2005.

Appendix C

$\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes in steganography

Advances in Mathematics of Communications
Volume 5, No. 3, 2011, 425–433
doi:10.3934/amc.2011.5.425

$\mathbb{Z}_2\mathbb{Z}_4$-ADDITIVE PERFECT CODES IN STEGANOGRAPHY

Helena Rifà-Pous
Department of Computer Science and Multimedia
Universitat Oberta de Catalunya, 08018-Barcelona, Spain

Josep Rifà and Lorena Ronquillo
Department of Information and Communications Engineering
Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain

(Communicated by Joan-Josep Climent)

Abstract. Steganography is an information hiding application which aims to hide secret data imperceptibly into a cover object. In this paper, we describe a novel coding method based on $\mathbb{Z}_2\mathbb{Z}_4$-additive codes in which data is embedded by distorting each cover symbol by one unit at most (± 1-steganography). This method is optimal and solves the problem encountered by the most efficient methods known today, concerning the treatment of boundary values. The performance of this new technique is compared with that of the mentioned methods and with the well-known rate-distortion upper bound to conclude that a higher payload can be obtained for a given distortion by using the proposed method.

1. Introduction and preliminary results

Steganography is a scientific discipline within *data hiding*, which hides information imperceptibly into innocuous media. A comprehensive overview of the core principles and the mathematical methods that can be used for data hiding can be found in [6].

An interesting steganographic method is known as *matrix encoding*, introduced by Crandall [3] and analyzed by Bierbrauer et al. [1]. Matrix encoding requires the sender and the recipient to agree in advance on a parity check matrix H, and the secret message is then extracted by the recipient as the syndrome (with respect to H) of the received cover object. This method was made popular by Westfeld [9], who incorporated a specific implementation using Hamming codes. The resulting method is known as the F5 algorithm and it can embed t bits of message in $2^t - 1$ cover symbols by changing, at most, one of them.

There are several parameters which are used to evaluate the performance of a steganographic method over a cover message of N symbols: the *average distortion* $D = \frac{R_a}{N}$, where R_a is the expected number of changes over uniformly distributed messages; the *embedding rate* $E = \frac{t}{N}$, which is the amount of bits that can be hidden in a cover message; and some authors use instead the *embedding efficiency*, which is the average number of embedded bits per change. In our case we will use

2000 *Mathematics Subject Classification:* Primary: 68P30; Secondary: 94A60, 94B60.
Key words and phrases: Steganography, $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes.
This work was partially supported by the Spanish Grants E-AEGIS, CONSOLIDER CSD2007-00004 ARES, MTM2009-08435, PCI2006-A7-0616 and also by the *Comissionat per a Universitats i Recerca del DIUE de la Generalitat de Catalunya* with Grant 2009SGR1224 and FI-DGR.

the average distortion and the embedding rate. Given two methods with the same embedding rate, the one with smaller average distortion will be said to perform better than the other. A scheme with block length N, embedding rate E, and average distortion D is called *optimal*, if all other schemes with the same block length N have embedding rate $E' \leq E$ or average distortion $D' \geq D$. Following the terminology used by Fridrich et al. [4], the tuple (D, E) will be called *CI-rate*.

As Willems et al. in [10], we will also assume that a discrete source produces a sequence $\mathbf{x} = (x_1, \quad , x_N)$, where N is the block length, $x_i \quad = \ 0, 1, \quad , 2^B -$ 1 , and $B \quad 8, 12, 16$ depends on the kind of source. The secret message $\mathbf{s}$ $1, \quad , M$ produces a composite sequence $\mathbf{y} = f(\mathbf{x}, \mathbf{s})$, where $\mathbf{y} = (y_1, \quad y_N)$ and each $y_i \quad$, by distorting $\mathbf{x}$. This distortion will be assumed to be of squared-error type (see [10]). In these conditions, we may deal with binary steganography , in which information is carried by the least significant bit (LSB) of each x_i and the appropriate solution comes from using binary Hamming codes [9], later improved using product Hamming codes [7]; or we may deal with ± 1-steganography , where $y_i = x_i + c$ for $c \quad 0, +1, -1$ and the information is carried by the two LSBs of x_i. Let the absolute value of c be the *amplitude* of an embedding change.

There are some steganographic techniques [8] in which messages carrying hidden information are statistically indistinguishable from those not carrying hidden data. However, in general, the embedding becomes statistically detectable rather quickly with the increasing amplitude of embedding changes, and our interest goes to avoid changes of amplitude greater than one. With this assumption, the embedding rate of our ± 1-steganographic scheme will be compared with the upper bound $H(D) + D$ [10], where $H(D)$ is the binary entropy function $H(D) = -D \log_2(D) - (1 - D) \log_2(1 - D)$ and $0 \leq D \leq 2/3$ is the average distortion. One of the purposes of steganographers is designing schemes in order to approach this upper bound.

In most papers, ± 1-steganography has been treated using ternary codes. Willems et al. [10] proposed a scheme based on ternary Hamming and Golay codes, which were proved to be optimal except for a remark which exposed a problem related to boundary values. Fridrich et al. [4] proposed a method based on rainbow colouring graphs using q-ary Hamming codes, where q is a prime power. This method performed better than the scheme from [10] when q is not a power of 3. However, the authors of both methods suggest making a change of magnitude greater than one in order to avoid having to apply the change $x_i - 1$ and $x_i + 1$ to a host sequence of value $x_i = 0$ and $x_i = 2^B - 1$, respectively. Note that this would introduce larger distortion and therefore make the embedding more detectable. The treatment of boundary grayscale values in steganography is important and, as far as we know, not many papers have paid attention to this issue.

In this paper we also consider ± 1-steganography. Our new method is based on $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes which, although they are not linear, they have a representation using a parity check matrix that makes them as computationally efficient as the Hamming codes. As we will later show, this new method is optimal and performs better than the method obtained by direct sum of ternary Hamming codes from [10] and the method based on rainbow colouring of graphs using q-Hamming codes [4] for the specific case $q = 3$. Furthermore, the proposed method also deals better with boundary grayscale values, because the magnitude of embedding changes is under no circumstances greater than one.

To make this paper self-contained, we review in Section 2 a few elementary concepts on $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes, relevant for our study. The new steganograph-

ic method based on these codes is described in Section 3, whereas an improvement to better deal with the extreme grayscale values problem is given in Section 4. The paper is concluded in Section 5.

2. $\mathbb{Z}_2\mathbb{Z}_4$-ADDITIVE PERFECT CODES

Any non-empty subgroup $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code*, where $\mathbb{Z}_2^\alpha$ denotes the set of all binary vectors of length α and $\mathbb{Z}_4^\beta$ is the set of all quaternary vectors of length β. Let $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \quad \mathbb{Z}_2^n$, where $n = \alpha + 2\beta$, be the *extended Gray map* given by applying the usual *Gray map* $\phi(0) = (0,0)$, $\phi(1) = (0,1)$, $\phi(2) = (1,1)$, and $\phi(3) = (1,0)$ to the quaternary coordinates.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is isomorphic to an abelian structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ has $|\mathcal{C}| = 2^\gamma 4^\delta$ codewords, where $2^{\gamma+\delta}$ of them are of order two. We call such code $\mathcal{C}$ a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code of type* $(\alpha, \beta; \gamma, \delta)$ and its binary image C is a $\mathbb{Z}_2\mathbb{Z}_4$-*linear code of type* $(\alpha, \beta; \gamma, \delta)$ which may not be linear. Note that the Lee distance of $\mathcal{C}$ coincides with the Hamming distance of $C = \Phi(\mathcal{C})$.

The $\mathbb{Z}_2\mathbb{Z}_4$-*additive dual code* of $\mathcal{C}$, denoted by $\mathcal{C}$, is defined as the set of vectors in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ that are orthogonal to every codeword in $\mathcal{C}$, where the inner product in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is defined by:

$$u, v \quad = 2\left(\sum_{i=1}^{\alpha} u_i v_i\right) + \sum_{j=\alpha+1}^{\alpha+\beta} u_j v_j \quad \mathbb{Z}_4, \tag{1}$$

where $u, v \quad \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and computations are made considering the zeros and ones in the α binary coordinates as quaternary zeros and ones, respectively.

The binary code $C \quad = \Phi(\mathcal{C} \quad)$, of length $n = \alpha + 2\beta$, is called the $\mathbb{Z}_2\mathbb{Z}_4$-*dual code* of C.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is said to be *perfect* if code $C = \Phi(\mathcal{C})$ is a perfect binary code, that is a binary code of minimum distance 3, where all vectors in $\mathbb{Z}_2^n$ are within distance one from a unique codeword.

It is well known [2] that for any $m \geq 2$ and each $\delta \quad 0, \quad , \frac{m}{2} \quad$ there exists a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code C of binary length $n = 2^m - 1$, such that its $\mathbb{Z}_2\mathbb{Z}_4$-dual code is of type $(\alpha, \beta; \gamma, \delta)$, where $\alpha = 2^{m-\delta} - 1$, $\beta = 2^{m-1} - 2^{m-\delta-1}$ and $\gamma = m - 2\delta$ (note that the binary length can be computed as $n = \alpha + 2\beta$). This allows us to write the parity check matrix H of any $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect code for a given value of δ. Matrix H can be represented by taking as columns all possible vectors in $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$, up to sign changes. In this representation, there are α columns which correspond to the binary part of vectors in $\mathcal{C}$, and β columns of order four which correspond to the quaternary part. We agree on a representation of the α binary coordinates as coordinates in $0, 2 \quad \mathbb{Z}_4$. Note that the binary Hamming code is a particular case of perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, specifically, when $\beta = 0$.

3. STEGANOGRAPHY BASED ON $\mathbb{Z}_2\mathbb{Z}_4$-ADDITIVE PERFECT CODES

Let us take a $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect code and consider its additive dual, which is of type $(\alpha, \beta; \gamma, \delta)$. As stated in the previous section, this gives us a parity check matrix H which has γ rows of order two and δ rows of order four.

For instance, for $m = 4$ and according to [2], there are three different $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes of binary length $n = 2^4 - 1 = 15$ which correspond to the possible values of $\delta \quad 0, \quad , \frac{m}{2} \quad = \quad 0, 1, 2$. For $\delta = 0$, the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect code is the usual binary Hamming code, while for $\delta = 2$ the

$\mathbb{Z}_2\mathbb{Z}_4$-additive perfect code has parameters $\alpha = 3$, $\beta = 6$, $\gamma = 0$, $\delta = 2$ and the following parity check matrix:

$$H = \left(\begin{array}{ccc|cccccc} 2 & 0 & 2 & 0 & 1 & 1 & 1 & 1 & 2 \\ 2 & 2 & 0 & 1 & 0 & 1 & 2 & 3 & 1 \end{array} \right) \tag{2}$$

Let $\mathbf{h}_i$, for $i \quad 1, \quad , \alpha+\beta$, denote the i-th column vector of H. Note that the all twos vector $\mathbf{2}$ is always one of the columns in H and, for the sake of simplicity, it will be written as column $\mathbf{h}_1$. We group the remaining first α columns in H in such a way that, for any $2 \leq i \leq (\alpha+1)/2$, vector $\mathbf{h}_{2i}$ is paired up with its complementary vector $\bar{\mathbf{h}}_{2i} = \mathbf{h}_{2i+1}$, where $\bar{\mathbf{h}}_{2i} = \mathbf{h}_{2i} + \mathbf{2}$.

To use these $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes in steganography take $N = 2^{m-1} = \frac{\alpha+1}{2} + \beta$ and let $\mathbf{x} = (x_1, \quad , x_N)$ be an N-length source of grayscale symbols such that $x_i \quad = \quad 0, 1, \quad , 2^B - 1$, where, for instance, $B = 8$ for grayscale images. We assume each grayscale symbol x_i is represented as a binary vector $(v_{(B-1)i}, \quad , v_{1i}, v_{0i})$, obtained by first representing x_i in base 4 and then applying the Gray map ϕ to every quaternary symbol in that representation. For example, value 239 is represented as the quaternary vector (3233), which then gives rise to the binary vector (10111010) after applying ϕ. We will use the two least significant bits (LSBs), v_{1i}, v_{0i}, of every grayscale symbol x_i in the source, for $i > 1$, as well as the least significant bit v_{01} of symbol x_1 to embed the secret message.

Each grayscale symbol x_i will be associated with one or more columns $\mathbf{h}_i$ in H:

1. Symbol x_1 is associated with $\mathbf{h}_1$ by taking its least significant bit, v_{01}.
2. Symbol x_i, for $2 \leq i \leq (\alpha+1)/2$, is associated with $\mathbf{h}_i$ and $\bar{\mathbf{h}}_i$, by taking, respectively, the two least significant bits, v_{1i}, v_{0i}, of x_i.
3. Symbol x_j, for $\alpha < j \leq N$, is associated with $\mathbf{h}_{j+(\alpha-1)\ 2}$ by taking its two least significant bits v_{1j}, v_{0j} and interpreting them as $\phi^{-1}(v_{1j}, v_{0j})$ in $\mathbb{Z}_4$.

In this way, the N-length packet $\mathbf{x}$ of symbols is translated into a vector $\mathbf{w}$ $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. The embedding process we propose is based on the matrix encoding method. The secret message can be any vector $\mathbf{s} \quad \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Vector $\epsilon \cdot \mathbf{h}_i$ indicates the changes needed to embed $\mathbf{s}$ within $\mathbf{x}$; that is $H\mathbf{w}^T + \epsilon \cdot \mathbf{h}_i = \mathbf{s}$, where ϵ is an integer whose value will be described bellow, $H\mathbf{w}^T$ is the syndrome vector of $\mathbf{w}$ and $\mathbf{h}_i$ is a column vector in H. We may have the following situations, depending on which column $\mathbf{h}_i$ needs to be modified:

1. If $\mathbf{h}_i = \mathbf{h}_1$, then the embedder has to change the least significant bit of x_1 by adding or subtracting one unit to/from x_1, depending on which operation will flip its least significant bit, v_{01}.
2. If $\mathbf{h}_i$ is among the first α column vectors in H and $2 \leq i \leq \alpha$, then ϵ can only be $\epsilon = 1$. In this case, since $\mathbf{h}_i$ was paired up with its complementary column vector $\bar{\mathbf{h}}_i$, then this situation is equivalent to make $(v_{1i}, 1 + v_{0i})$ or $(1 + v_{1i}, v_{0i})$, where v_{1i} and v_{0i} are the least significant bits of the symbol x_i which had been associated with those two column vectors. Hence, after the inverse of Gray map, by changing one or another we are actually adding or subtracting one unit to/from x_i. Note that a problem may crop up at this point if we need to add 1 to a symbol x_i of value $2^B - 1$ or subtract 1 from a symbol of value 0.
3. If $\mathbf{h}_i$ is one of the last β columns in H, then this situation corresponds to add $\epsilon \quad 0, 1, 2, 3$. Note that because we are using a $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect code, ϵ will never be 2. Hence, the embedder should add $(\epsilon = 1)$ or subtract $(\epsilon = 3)$

one unit to/from symbol $x_{i-(\alpha-1)\ 2}$. Once again, a problem may arise with boundary values.

Example 1. Let $\mathbf{x} = (239, 251, 90, 224, 226, 187, 229, 180)$ be an N-length source of grayscale symbols, where $x_i \quad 0, \quad , 255$ and $N = 8$, and let H be the matrix in (2). The source $\mathbf{x}$ is then translated into the vector $\mathbf{w} = (010|202310)$ in the way specified above. Let $\mathbf{s} = (02)^T$ be the vector representing the secret message we want to embed in $\mathbf{x}$. We then compute $H\mathbf{w}^T = (23)^T$ and see, by the matrix encoding method, that $\epsilon = 3$ and $\mathbf{h}_i = \mathbf{h}_9$. According to the described method, we should subtract 1 from x_8. In this way, x_8 becomes 179, and then $\mathbf{w}' = (010|202313)$, which has the expected syndrome $(02)^T$.

The problematic cases related to boundary values are also present in methods from [4] and [10], but their authors assume that the probability of gray value saturation is not too large. We argue that, though rare, this gray saturation can still occur. However, in order to compare our proposal with these others we will not consider these problems either until next section. Therefore, we proceed to compute the values of the average distortion D and the embedding rate E.

Our method is able to hide any secret vector $\mathbf{s} \quad \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ into the given N symbols. Hence, the embedding rate is $(\gamma + 2\delta)$ bits per N symbols, $E = \dfrac{\gamma + 2\delta}{N} = \dfrac{m}{2^{m-1}}$.

Concerning the average distortion D, we are using a perfect code of binary length $2^m - 1$, which corresponds to $N = 2^{m-1}$ grayscale symbols. There are $N - 1$ symbols x_i, for $2 \le i \le N$, with a probability $2/2^m$ of being subjected to a change; a symbol x_1 with a probability $1/2^m$ of being the one changed; and, finally, there is a probability of $1/2^m$ that neither of the symbols will need to be changed to embed the secret message $\mathbf{s}$. Hence, $D = \dfrac{2N-1}{N2^m} = \dfrac{2^m - 1}{2^{2m-1}}$.

The described method has a CI-rate $(D_m, E_m) = \left(\dfrac{2N-1}{2N^2}, \dfrac{1+\log(N)}{N}\right)$, where $N = 2^{m-1}$ and m is any integer $m \ge 2$.

It is shown in [10] that the linear ternary perfect codes (Hamming or Golay) are optimal in the sense that they achieve the smallest possible distortion at a given embedding rate for a fixed block length. This property is not exclusive of these codes and we will prove, in the next proposition, that the method we have described using $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes also satisfies it.

Proposition 1. *The proposed embedding method based on $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes is optimal.*

Proof. Consider a code with length $N = \frac{\alpha+1}{2} + \beta$. Suppose that the source produces a sequence $\mathbf{x}$ and assume that we have a steganographic scheme with embedding rate $E_m = \frac{1+\log(N)}{N} = \frac{\log(2N)}{N}$. Hence, there are $2N$ composite sequences $\mathbf{y}$, each one of them representing a different message. There is only one sequence $\mathbf{x}$ which does not need to be distorted, that is $\mathbf{y} = \mathbf{x}$. The smallest possible nonzero distortion is $1/N$ and it is achieved by 2β sequences $\mathbf{y}$ which differ from $\mathbf{x}$ in exactly one of the β quaternary coordinates, after multiplying by 1 or 3, that is $|\mathbf{y} - \mathbf{x}| = 1$ or $|\mathbf{y} - 3\mathbf{x}| = 1$, and the same distortion is also achieved by a sequence $\mathbf{y}$ which differs from $\mathbf{x}$ in exactly one of the α binary coordinates (i.e. they differ in a bit). So there are $\alpha + 2\beta = 2N - 1$ composite sequences $\mathbf{y}$ achieving the smallest possible nonzero distortion $1/N$, and this gives us the smallest possible maximum average

distortion $D = \dfrac{(2N-1)(1/N)}{2N} = \dfrac{2N-1}{2N^2}$, which coincides with the distortion in our method. □

Note that we are only able to generate an embedding scheme for natural values of $m \geq 2$. However, we can use the direct sum of codes [5] to obtain codes whose CI-rates are convex combinations of CI-rates of boths codes. Thus given any non-allowable parameter D for the average distortion, we can take two codes with CI-rates (D_1, E_1) and (D_2, E_2), respectively, where $D_1 < D < D_2$, and their direct sum generates a code with a new CI-rate (D, E), with $D = \lambda D_1 + (1-\lambda)D_2$ and $E = \lambda E_1 + (1-\lambda)E_2$. From a graphic point of view, this is equivalent to draw a line between two contiguous points (D_1, E_1) and (D_2, E_2), as it is shown in Figure 1.

Proposition 2. *For $m \geq 4$, the CI-rate given by the method based on $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes improves the CI-rate obtained by direct sum of ternary Hamming codes with the same average distortion.*

Proof. Optimal embedding (of course, in the allowable values of D) can be obtained by using ternary codes, as it is shown in [10]. The CI-rate of these codes is $(D_\mu, E_\mu) = \left(\dfrac{2}{3^\mu}, \dfrac{2\mu\log(3)}{3^\mu - 1}\right)$ for any integer μ. Our method, based on $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes, has CI-rate $(D_m, E_m) = \left(\dfrac{2N-1}{2N^2}, \dfrac{1+\log(N)}{N}\right)$, for $N = 2^{m-1}$ and any integer $m \geq 2$.

Take, for any $m \geq 2$, two contiguous values for μ such that $D_{\mu+1} < D_m < D_\mu$ and write $D_m = \lambda D_{\mu+1} + (1-\lambda)D_\mu$, where $0 \leq \lambda \leq 1$.

We want to prove that, for $m \geq 4$, we have $E_m \geq \lambda E_{\mu+1} + (1-\lambda)E_\mu$, which is straightforward. However, since it is neither short nor contributes to the well understanding of the method, we do not include all computations here. □

4. Solving the extreme grayscale values problem

In Section 3 we described a problem which may arise when, according to our method, the embedder is required to add one unit to a source symbol x_i containing the maximum allowed value $(2^B - 1)$, or to subtract one unit from a symbol x_i containing the minimum allowed value, 0. To face this problem, we will use the complementary column vector $\bar{\mathbf{h}}_i$ of columns $\mathbf{h}_i$ in matrix H, where $\bar{\mathbf{h}}_i = 3\mathbf{h}_i + \mathbf{2}$ and $\mathbf{h}_i$ is among the last β columns in H. Note that $\mathbf{h}_i$ and $\bar{\mathbf{h}}_i$ can coincide.

The first α column vectors in H will be paired up as before, and the association between each x_i and each column vector $\mathbf{h}_i$ in H will be also the same as in Section 3. However, given an N-length source of grayscale symbols $\mathbf{x} = (x_1, \quad, x_N)$, a secret message $\mathbf{s} \quad \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ and the vector $\epsilon \cdot \mathbf{h}_i$, such that $H\mathbf{w}^T + \epsilon \cdot \mathbf{h}_i = \mathbf{s}$, indicating the changes needed to embed $\mathbf{s}$ within $\mathbf{x}$, we can now make some variations on the kinds of changes to be done for the specific problematic cases:

- If $\mathbf{h}_i$ is among the first α columns in H, for $2 \leq i \leq \alpha$, and the embedder is required to add 1 to a symbol $x_i = 2^B - 1$, then the embedder should instead subtract 1 from x_i as well as perform the appropriate operation $(+1$ or $-1)$ over x_1 to have v_{01} flipped. Likewise, if the embedder is required to subtract 1 from a symbol $x_i = 0$, then (s)he should instead add 1 to x_i and also change x_1 to flip v_{01}.

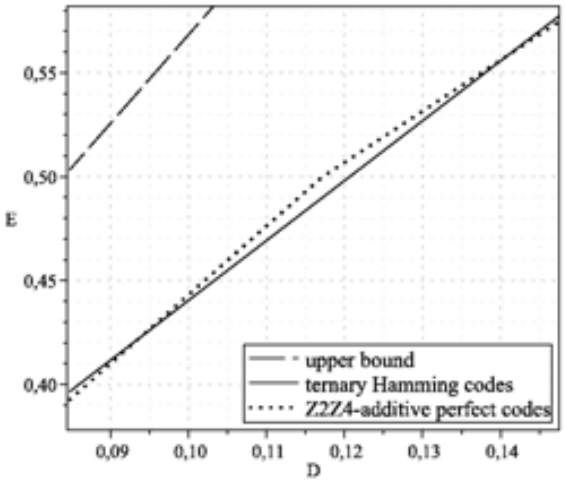

FIGURE 1. CI-rate (D, E), for $B = 8$, of steganographic methods based on ternary Hamming codes and on $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes, compared with the upper bound $H(D) + D$, where E is the embedding rate, D is the average distortion and $H(D)$ is the binary entropy function.

- If $\mathbf{h}_i$ is one of the last β columns in H, and the embedder has to add 1 to a symbol $x_i = 2^B - 1$, (s)he should instead subtract 1 from the grayscale symbol associated to $\bar{\mathbf{h}}_i$ and also change x_1 to flip v_{01}. If the method requires subtracting 1 from $x_i = 0$, then we should instead add 1 to the symbol associated to $\bar{\mathbf{h}}_i$ and, again, change x_1 to flip v_{01}.

Example 2. Let $\mathbf{s}$ and $\mathbf{x}$ be as in Example 1, except for the value of x_8 which is now $x_8 = 0$. The packet $\mathbf{x}$ is translated into vector $\mathbf{w} = (010|202310)$. However, now we are not able to make $x_8 - 1$. Instead of this, we will add one unit to x_3, which is the symbol associated with $\bar{\mathbf{h}}_9 = \mathbf{h}_4$, and subtract one unit from x_1 so as to have its LSB flipped. Therefore, we obtain $\mathbf{x}' = (238, 251, 91, 224, 226, 187, 229, 0)$ and then $\mathbf{w}' = (110|302310)$

The method above described has the same embedding rate $E = \dfrac{m}{2^{m-1}}$ as the one from Section 3 but a slightly worse average distortion. We will take into account the squared-error distortion defined in [10] for our reasoning.

As before, among the total number of grayscale symbols $N = 2^{m-1}$, there are $N - 1$ symbols x_i, for $2 \leq i \leq N$, with a probability $2/2^m$ of being changed; a symbol x_1 with a probability $1/2^m$ of being the one changed; and, finally, there is a probability of $1/2^m$ that neither of the symbols will need to be changed.

As one may have noted in this scheme, performing a certain change to a symbol x_i, associated with a column $\mathbf{h}_i$ in H, has the same effect as performing the opposite change to the grayscale symbol associated with $\bar{\mathbf{h}}_i$ and also changing the least significant bit v_{01} of x_1. This means that with probability $\frac{2^B-2}{2^B}$ we will change a symbol x_i, for $2 \leq i \leq N$, a magnitude of 1; and with probability $\frac{2}{2^B}$ we will change two other symbols also a magnitude of 1. Therefore,

$R_a = (N-1)\frac{2}{2^m}\left(\frac{2^B-2}{2^B}+2\frac{2}{2^B}\right)+\frac{1}{2^m}$ and the average distortion is thus $D = \frac{2N-1+\frac{N-1}{2^{B-2}}}{N2^m}$. Hence, the described method has CI-rate:

$$(D_m, E_m) = \left(\frac{2N-1+\frac{N-1}{2^{B-2}}}{2N^2}, \frac{1+\log(N)}{N}\right)$$

With the aim of providing a possible solution to the boundary grayscale values problem, the authors of [10] and [4] suggested to perform a change of magnitude greater than 1. However, the effects of doing this were out of the scope of ± 1-steganography.

5. Conclusions

We have presented a new method for ± 1-steganography, based on $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes. These codes correspond, through the Gray map, to binary perfect codes, which can be nonlinear but they still have a parity check matrix representation which makes them computationally efficient to work with.

As shown in sections 3 and 4, this new scheme is optimal and performs better than the one obtained by simple direct sum of ternary Hamming codes from [10] and the one based on rainbow colouring of graphs using q-ary Hamming codes [4], for $q = 3$.

If we consider the special cases in which the technique might require to subtract one unit from a grayscale symbol containing the minimum allowed value, or to add one unit to a symbol containing the maximum allowed value, our method performs even better than those aforementioned schemes. This is so because unlike them, our method never applies any change of magnitude greater than 1, but two changes of magnitude 1 instead. This is better in terms of distortion and therefore makes the embedding less statistically detectable.

As for further research, since the approach based on product Hamming codes in [7] improved the performance of basic LSB steganography and the basic $F5$ algorithm, we would also expect a considerable improvement of the CI-rate by using product $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes or subspaces of product $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes in ± 1-steganography.

Acknowledgments

The authors wish to thank the anonymous referees for useful and valuable comments which have improved some proofs in this paper.

References

[1] J. Bierbrauer and J. Fridrich, *Constructing good covering codes for applications in steganography*, in "Trans. on Data Hiding and Multimedia Security III," (2008), 1–22.

[2] J. Borges and J. Rifà, *A characterization of 1-perfect additive codes*, IEEE Trans. Inform. Theory, **45** (1999), 1688–1697.

[3] R. Crandall, *Some notes on steganography*, available from http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0203/steganografia/LINKS%20LOCALI/matrix-encoding.pdf, 1998.

[4] J. Fridrich and P. Lisoněk, *Grid colorings in steganography*, IEEE Trans. Inform. Theory, **53** (2007), 1547–1549.

[5] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland Publishing Company, 1977.

[6] P. Moulin and R. Koetter, *Data-hiding codes*, Proc. IEEE, **93** (2005), 2083–2126.
[7] H. Rifà-Pous and J. Rifà, *Product perfect codes and steganography*, Digit. Signal Process., **19** (2009), 764–769.
[8] B. Ryabko and D. Ryabko, *Asymptotically optimal perfect steganographic systems*, Probl. Inform. Transm., **45** (2009), 184–190.
[9] A. Westfeld, *High capacity despite better steganalysis (F5 - A steganographic algorithm)*, Lecture Notes in Comput. Sci., **2137** (2001), 289–302.
[10] F. M. J. Willems and M. van Dijk, *Capacity and codes for embedding information in grayscale signals*, IEEE Trans. Inform. Theory, **51** (2005), 1209–1214.

Received May 2010; revised March 2011.

E-mail address: hrifa@uoc.edu
E-mail address: Josep.Rifa@autonoma.edu
E-mail address: Lorena.Ronquillo@autonoma.edu

Appendix D

Construction of new completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes from old

Construction of New Completely Regular $\mathbb{Z}_2\mathbb{Z}_4$-linear Codes from Old *

Josep Rifà and Lorena Ronquillo

Department of Information and Communications Engineering,
Universitat Autònoma de Barcelona,
08193-Cerdanyola del Vallès, Spain.
Josep.Rifa,Lorena.Ronquillo @autonoma.edu

Abstract. A code $\mathcal{C}$ is said to be $\mathbb{Z}_2\mathbb{Z}_4$-additive if its coordinates can be partitioned into two subsets X and Y, in such a way that the punctured code of $\mathcal{C}$ obtained by removing the coordinates outside X (or, respectively, Y) is a binary linear code (respectively, a quaternary linear code). The binary image of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, through the Gray map, is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code, which is not always linear. Given a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code, which is known to be completely regular, some constructions yielding new $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are computed, and the completely regularity of the obtained codes is studied.

Keywords: additive codes, completely regular codes, perfect binary codes, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

1 Introduction

Let $\mathbb{Z}_2^\alpha$ and $\mathbb{Z}_4^\beta$ denote the set of all binary vectors of length α and the set of all quaternary vectors of length β, respectively. Let $GF(q)$ be a Galois field with q elements, q being a power of some prime number, and let $GR(q^m)$ be a Galois ring with cardinality q^m, which comes from an extension of the ring $\mathbb{Z}_q$. The classical Hamming weight $wt(\mathbf{v})$ of a vector $\mathbf{v} \in GF(q)^n$ is the number of coordinates which are different from zero, and the Hamming distance $d(\mathbf{u}, \mathbf{v})$ between two vectors $\mathbf{u}, \mathbf{v} \in GF(q)^n$ denotes the weight of their difference.

Any non-empty subgroup $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code*. Let $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ be the usual *Gray map*, that is, $\phi(0) = (0,0)$, $\phi(1) = (0,1)$, $\phi(2) = (1,1)$, and $\phi(3) = (1,0)$; and let $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^n$, where $n = \alpha + 2\beta$, be the *extended Gray map* (Id, ϕ) given by

$$\Phi(u_1, \ldots, u_\alpha | v_1, \ldots, v_\beta) = (u_1, \ldots, u_\alpha | \phi(v_1), \ldots, \phi(v_\beta)).$$

It is worth noting that the extended Gray map is an isometry which transforms Lee distances defined in a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ onto Hamming distances defined in the binary code $C = \Phi(\mathcal{C})$, where the length of C is $n = \alpha + 2\beta$.

* This work was partially supported by the Spanish MICINN Grants MTM2009-08435, PCI2006-A7-0616, and also by the *CUR del DIUE de la Generalitat de Catalunya* and the *European Social Fund* with Grants 2009SGR1224 and FI-DGR.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is isomorphic to an abelian structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Thus $\mathcal{C}$ has $|\mathcal{C}| = 2^\gamma 4^\delta$ codewords, where $2^{\gamma+\delta}$ of them are of order two. We call such code $\mathcal{C}$ a $\mathbb{Z}_2\mathbb{Z}_4$-*additive code of type* $(\alpha, \beta; \gamma, \delta)$, and its binary image $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_2\mathbb{Z}_4$-*linear code of type* $(\alpha, \beta; \gamma, \delta)$, which may not be linear.

Given a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$, its dual is also a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, denoted by $\mathcal{C}^\perp$, and defined as the set of vectors in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ which are orthogonal to every codeword in $\mathcal{C}$. We use the following definition (see [3]) of inner product in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$:

$$\langle \mathbf{u}, \mathbf{v} \rangle = 2\left(\sum_{i=1}^{\alpha} u_i v_i\right) + \sum_{j=\alpha+1}^{\alpha+\beta} u_j v_j \in \mathbb{Z}_4, \tag{1}$$

where $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and computations are made considering zeros and ones in the α binary coordinates as quaternary zeros and ones, respectively.

After the Gray map over $\mathcal{C}^\perp$, the binary code $C_\perp = \Phi(\mathcal{C}^\perp)$, of length $n = \alpha + 2\beta$, is called the $\mathbb{Z}_2\mathbb{Z}_4$-*dual code* of C.

Two $\mathbb{Z}_2\mathbb{Z}_4$-additive codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of the same length are *monomially equivalent* if one can be obtained from the other by permuting the coordinates and, if necessary, changing the sign of certain quaternary coordinates.

Although a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ of type $(\alpha, \beta; \gamma', \delta')$ may not have a basis, every codeword is uniquely expressible in the form

$$\sum_{i=1}^{\gamma'} \lambda_i \mathbf{u}^{(i)} + \sum_{j=\gamma'+1}^{\gamma'+\delta'} \mu_j \mathbf{v}^{(j)}, \tag{2}$$

where $\lambda_i \in \mathbb{Z}_2$ for $1 \le i \le \gamma'$, $\mu_j \in \mathbb{Z}_4$ for $\gamma' + 1 \le j \le \gamma' + \delta'$ and $\mathbf{u}^{(i)}$, $\mathbf{v}^{(j)}$ are vectors in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ of order two and order four, respectively (see [3]).

Vectors $\mathbf{u}^{(i)}$, $\mathbf{v}^{(j)}$ give us a generator matrix $\mathcal{G}$ which can be written as follows:

$$\mathcal{G} = \left(\begin{array}{c|c} B_2 & Q_2 \\ \hline B_1 & Q_1 \end{array}\right), \tag{3}$$

where B_2 and B_1 are binary matrices of size $(\gamma' \times \alpha)$ and $(\delta' \times \alpha)$, respectively; Q_2 is a $(\gamma' \times \beta)$-matrix whose elements are in $\{0, 2\} \subset \mathbb{Z}_4$ and Q_1 is a quaternary $(\delta' \times \beta)$-matrix with row vectors of order four. Refer to [3] for further details.

Depending on the computations we are doing it might be convenient to take a different representation for the above matrix.

Let $\mathcal{D}$ be a matrix written as follows:

$$\mathcal{D} = \left(\begin{array}{c|c} B_2' & Q_2' \\ \hline B_1' & Q_1' \end{array}\right), \tag{4}$$

where B_2' and B_1' are binary matrices of size $(\psi \times \alpha)$ and $(\theta \times \alpha)$, respectively, in which binary zeros and ones have been represented as quaternary zeros and twos; Q_2' is a $(\psi \times \beta)$-matrix whose elements are in $\{0, 2\} \subset \mathbb{Z}_4$ and Q_1' is a quaternary $(\theta \times \beta)$-matrix with row vectors of order four. We will refer to this

matrix as a *matrix of type* $(\alpha, \beta; \psi, \theta)$. Note that matrix in (4) represents a group homomorphism

$$\mathcal{D} : \mathbb{Z}_2^{\psi} \times \mathbb{Z}_4^{\theta} \longrightarrow \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta},$$

where for any $\mathbf{v} = (\lambda_1, \ldots, \lambda_\psi, \mu_{\psi+1}, \ldots, \mu_{\psi+\theta}) \in \mathbb{Z}_2^{\psi} \times \mathbb{Z}_4^{\theta}$, vector $\mathcal{D}(\mathbf{v})$ is computed as in (2). From a matrix point of view, this can be done by computing $\mathbf{v}\mathcal{D}$, which yields a vector in $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$ whose binary zeros and ones are represented, respectively, by quaternary zeros and twos.

Given a code $\mathcal{C}^{\perp}$ of type $(\alpha, \beta; \gamma, \delta)$, corresponding to the $\mathbb{Z}_2\mathbb{Z}_4$-additive dual code of $\mathcal{C}$, its generator matrix $\mathcal{H}$ is a parity check matrix of $\mathcal{C}$. Thus all codewords in $\mathcal{C}$ are orthogonal to every row vector in $\mathcal{H}$ through the inner product in (1). As for the usual case of codes over a finite field, given a vector $\mathbf{v} \in \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, we can refer to the syndrome $S_{\mathbf{v}}$ as the vector in $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$ obtained by computing $\mathbf{v}\mathcal{H}^T$, where $\mathcal{H}^T$ is the matrix obtained by writing the rows in $\mathcal{H}$ as column vectors, and it is written as in (4).

Let C be a binary code. The distance of any vector $\mathbf{v} \in \mathbb{Z}_2^n$ to C is $d(\mathbf{v}, C) = \min_{\mathbf{x} \in C}\{d(\mathbf{v}, \mathbf{x})\}$, and the covering radius of C is $\rho = \max_{\mathbf{v} \in \mathbb{Z}_2^n}\{d(\mathbf{v}, C)\}$. Let us also define $C(i) = \{\mathbf{v} \in \mathbb{Z}_2^n : d(\mathbf{v}, C) = i\}$, $i = \{1, \ldots, \rho\}$.

We say that two vectors $\mathbf{u}$ and $\mathbf{v}$ are *neighbours* if $d(\mathbf{u}, \mathbf{v}) = 1$. In this paper, the definition of completely regularity given in [9] will be used.

Definition 1. *A code C with covering radius ρ is completely regular, if for all $l \geq 0$ every vector $x \in C(l)$ has the same number a_l of neighbours in $C(l)$, the same number b_l of neighbours in $C(l+1)$, and the same number c_l of neighbours in $C(l-1)$. Moreover, note that $a_l + b_l + c_l = n$ and $c_0 = b_\rho = 0$. The intersection array of C is then $(b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_\rho)$.*

It is well known that any linear completely regular code C implies the existence of a coset distance-regular graph. Binary images of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are nonlinear binary codes, but we can also construct the quotient graph which is distance-regular when the initial $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are completely regular.

Given a code C, its *external distance* is the number of nonzero terms in the MacWilliams transform. From any $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ we can construct the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-additive dual code $\mathcal{C}^{\perp}$ and, in this case, their respective weight enumerator polynomials are related by the MacWilliams identity [7]. Thus in the specific cases of $\mathbb{Z}_4$ or $\mathbb{Z}_2\mathbb{Z}_4$ additivity, we can also refer to [10] and, hence the external distance of $C = \Phi(\mathcal{C})$ coincides with the number of nonzero weights occurring in the distance distribution of $C_{\perp} = \Phi(\mathcal{C}^{\perp})$.

Throughout this paper we will use the concept of *uniformly packed code* (usually called "in the wide sense") defined in [1].

Definition 2 ([1]). *Let C be a binary code of length n and covering radius ρ. We say that C is uniformly packed "in the wide sense" if there exist rational numbers $\tau_0, \ldots, \tau_\rho$ such that, for any $\mathbf{v} \in \mathbb{Z}_2^n$,*

$$\sum_{k=0}^{\rho} \tau_k A_k(\mathbf{v}) = 1,$$

where $A_k(\mathbf{v})$ is the number of codewords in C at distance k from $\mathbf{v}$.

In the following Proposition we summarize a few well known results.

Proposition 1. *Let C be a code (not necessarily linear) with error correcting capability $e \geq 1$, covering radius ρ and external distance s. Then:*

(i) **[8]** *$\rho \leq s$.*
(ii) **[2]** *$\rho = s$ if and only if code C is uniformly packed (in the wide sense).*
(iii) **[6]** *If C is completely regular, then it is uniformly packed (in the wide sense).*
(iv) **[7, 10]** *If C is a $\mathbb{Z}_2\mathbb{Z}_4$-linear code, then the external distance s of C coincides with the number of nonzero weights occurring in the $\mathbb{Z}_2\mathbb{Z}_4$-dual code of C.*
(v) **[7]** *If $2e + 1 \geq 2s - 1$, then C is a completely regular code.*

A perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ of length $n = 2^m - 1$ is a binary perfect code, that is, a binary code of minimum distance 3, where all vectors in $\mathbb{Z}_2^n$ are within distance one from a unique codeword.

It is well known [5] that for any $m \geq 2$ and each $\delta \in \{0, \ldots, \lfloor \frac{m}{2} \rfloor\}$ there exists a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code C of binary length $n = 2^m - 1$, such that its $\mathbb{Z}_2\mathbb{Z}_4$-dual code is of type $(\alpha, \beta; \gamma, \delta)$, where $\alpha = 2^{m-\delta} - 1$, $\beta = 2^{m-1} - 2^{m-\delta-1}$ and $m = \gamma + 2\delta$ (recall that the binary length can be computed as $n = \alpha + 2\beta$). This allows us to write, for a given value of δ, the parity check matrix $\mathcal{H}$ of any $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ corresponding to a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$. This parity check matrix can be expressed in form (3) where the first α columns are all possible nonzero vectors in $\mathbb{Z}_2^{\gamma+\delta}$, and the last β columns are all possible order four vectors in $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$, up to scalar multiples, where binary zeros and ones are respectively represented as quaternary zeros and twos (see [4]).

In this paper we construct some completely regular codes by modifying, in various ways, a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code C. In Section 2 we extend, puncture and also shorten code C, while in Section 3 we describe a new method to obtain nonlinear completely regular codes in $GF(4)$ by lifting perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes defined over $GF(2)$. The same approach is also taken in Section 4 to obtain uniformly packed codes in $GF(4)$ by lifting extended perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes over $GF(2)$.

2 Extending, puncturing and shortening perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, with parity check matrix $\mathcal{H}$, such that its binary image $C = \Phi(\mathcal{C})$ is a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length $n = 2^m - 1$, for $m \geq 3$, and its $\mathbb{Z}_2\mathbb{Z}_4$-additive dual code $\mathcal{C}^{\perp}$ is of type $(\alpha, \beta; \gamma, \delta)$.

Let $\hat{\mathcal{C}}$ be the extended code of $\mathcal{C}$, that is, the $\mathbb{Z}_2\mathbb{Z}_4$-additive code whose parity check matrix $\hat{\mathcal{H}}$ is obtained from $\mathcal{H}$ by first adding a zero column at the beginning of the binary part, and then adding the all-twos row vector, where the twos in the first $\alpha+1$ coordinates are representing binary ones. The binary code $\hat{C} = \Phi(\hat{\mathcal{C}})$ has length $n = 2^m$ and every codeword has even weight.

Let $\dot{\mathcal{C}}$ be the punctured code of $\mathcal{C}$, that is, the $\mathbb{Z}_2\mathbb{Z}_4$-additive code obtained by removing the i-th column of the generator matrix of $\mathcal{C}$ or, equivalently, obtained by deleting the i-th coordinate from each codeword in $\mathcal{C}$. Each time a coordinate is deleted in $\mathcal{C}$, the length of the corresponding binary code $\dot{C} = \Phi(\dot{\mathcal{C}})$ drops by 1 when $1 \leq i \leq \alpha$, or by 2 when $\alpha+1 \leq i \leq \alpha+\beta$.

Let $\mathcal{C}^*$ be the shortened code of $\mathcal{C}$, that is, the $\mathbb{Z}_2\mathbb{Z}_4$-additive code obtained by taking all codewords in $\mathcal{C}$ having a zero as their i-th component, where $1 \leq i \leq \alpha+\beta$, and subsequently delete the i-th component from these codewords. The procedure of shortening a code obviously decreases its length, thus the binary code $C^* = \Phi(\mathcal{C}^*)$ is of length $n = 2^m - 2$ if $1 \leq i \leq \alpha$, and of length $n = 2^m - 3$ if $\alpha+1 \leq i \leq \alpha+\beta$.

The following propositions can be proved.

Proposition 2. *External distance.*

(i) *Code $\hat{C}$ has external distance $s = 2$.*
(ii) *Code $\dot{C}$ has external distance $s = 1$.*
(iii) *Code C^* has external distance $s = 2$ when the i-th shortened coordinate is $1 \leq i \leq \alpha$, and $s = 3$ when the i-th shortened coordinate is $\alpha+1 \leq i \leq \alpha+\beta$.*

Proposition 3. *Covering radius.*

(i) *The covering radius of $\hat{C}$ is $\rho = 2$.*
(ii) *The covering radius of $\dot{C}$ is $\rho = 1$.*
(iii) *The covering radius of C^* is $\rho = 2$.*

Using properties (**ii**) and (**v**) from Proposition 1, the following proposition is straightforward.

Proposition 4. *Uniformly packed codes.*

(i) *Code $\hat{C}$ is uniformly packed.*
(ii) *Code $\dot{C}$ is uniformly packed.*
(iii) *Code C^* is uniformly packed only when the i-th shortened coordinate is $1 \leq i \leq \alpha$.*

Finally, we can state the following proposition which is given without proof.

Proposition 5. *Completely regular codes.*

(i) *Code $\hat{C}$ is a completely regular code with intersection array $(2^m, 2^m-1; 1, 2^m)$.*

(ii) *Code $\dot{C}$ is a completely regular code with intersection array $(2^m - 2; 2)$ when the i-th punctured coordinate is $1 \leq i \leq \alpha$, and with intersection array $(2^m - 4; 4)$ when $\alpha + 1 \leq i \leq \alpha + \beta$.*

(iii) *Code C^* is completely regular with intersection array $(2^m - 2, 1; 1, 2^m - 2)$, when the i-th shortened coordinate is $1 \leq i \leq \alpha$.*

Remark 1. Notice that in those cases where the extended (shortened) codes are completely regular codes, the intersection array coincides, respectively, with that of the extended (shortened) Hamming binary code of the same length. As for the punctured code, its intersection array coincides with that of the punctured Hamming binary code of the same length when we are puncturing a coordinate within the first α binary coordinates, while it coincides with the intersection array of the 2-punctured Hamming binary code when we are puncturing a quaternary coordinate. In other words, we have constructed new completely regular codes, but with the same intersection array as the corresponding linear codes.

3 Lifting perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

Lifting of binary perfect linear codes was previously studied in [12]. In this article we now introduce and study lifted perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes.

As in Section 2, let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, with parity check matrix $\mathcal{H}$, such that its binary image $C = \Phi(\mathcal{C})$ is a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length $n = 2^m - 1$, for $m \geq 3$, and its $\mathbb{Z}_2\mathbb{Z}_4$-additive dual code $\mathcal{C}^\perp$ is of type $(\alpha, \beta; \gamma, \delta)$. We define the code C_r over an extension $GF(2^r)$ of the binary finite field as

$$C_r = C + \xi C + \xi^2 C + \ldots + \xi^{r-1} C,$$

where $\xi^i C$ denotes the result of multiplying every codeword in C by ξ^i, and ξ is a primitive element in $GF(2^r)$. Let $\mathcal{C}_r = \Phi^{-1}(C_r)$ be the corresponding code in $GF(2^r)^\alpha \times GR(4^r)^\beta$. Code $\mathcal{C}_r$ has $\mathcal{H}_r$ as parity check matrix, where $\mathcal{H}_r$ can be seen as an $\alpha \times \beta \times r$ matrix in which each submatrix (h_{ijk}) for a fixed $k \in \{1, \ldots, r\}$ coincides with the parity check matrix $\mathcal{H}$ of $\mathcal{C}$. We will say that code C_r is obtained by lifting the perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code C. Note that code C_r may not be linear over $GF(2^r)$.

Any vector $\mathbf{v} \in \mathcal{C}_r$ can be seen as a matrix of size $r \times (\alpha + \beta)$ by representing every coordinate in $GF(2^r)$ from the first α coordinates and every coordinate in $GR(4^r)$ from the last β coordinates, as a column vector in $GF(2)^r$ and in $GR(4)^r$, respectively. This matrix therefore contains r row vectors in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. Moreover, we will represent the binary zeros and ones in the first α coordinates of every such rows as quaternary zeros and twos, respectively. Let this matrix representation of $\mathbf{v}$ be denoted by $[\mathbf{v}]$.

Proposition 6. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code having a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code binary image $C = \Phi(\mathcal{C})$ of length $n = 2^m - 1$, for $m \geq 3$; let $\mathcal{C}_r$ be the code defined over $GF(2^r)^\alpha \times GR(4^r)^\beta$, obtained by lifting $\mathcal{C}$, and let C_r be the corresponding binary image of $\mathcal{C}_r$. For $r = 2$, the covering radius ρ of C_r is 2.*

Proof. Let $\mathbf{v}$ be any vector in $GF(4)^\alpha \times GR(16)^\beta$ and not in $\mathcal{C}_2$, and let $S_\mathbf{v} = \mathbf{v}\mathcal{H}^T \in GF(4)^\gamma \times GR(16)^\delta$ be its syndrome. We can then write $\mathbf{v} = \mathbf{w} + \mathbf{e}$, where $\mathbf{w} \in \mathcal{C}_2$ and $\mathbf{e}$ is a vector in $GF(4)^\alpha \times GR(16)^\beta$ of minimum weight such that its syndrome is $S_\mathbf{e} = S_\mathbf{v}$. Therefore, the distance from $\mathbf{v}$ to $\mathcal{C}_2$ is the weight of vector $\mathbf{e}$, that is $d(\mathbf{v}, \mathcal{C}_2) = wt(\mathbf{e})$.

Let us represent vector $\mathbf{e}$ as a matrix $[\mathbf{e}]$ of two row vectors in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. Since the covering radius of any perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code is 1, we have that the Lee weight of every row in $[\mathbf{e}]$ is at most 1. Therefore, we know that $wt(\mathbf{e}) \leq 2$, thus $d(\mathbf{v}, \mathcal{C}_2) \leq 2$ and the covering radius of C_2 is $\rho \leq 2$.

However, since C_2 is not a perfect code, we know that ρ cannot be 1. Hence the covering radius ρ of C_2 is 2.

Lemma 1. *Let $\mathbf{v}$ be a vector in $GF(4)^\alpha \times GR(16)^\beta$, and let $(x, y)^T$ be a column vector in the matrix representation $[\mathbf{v}]$ of $\mathbf{v}$, where $x, y \in \mathbb{Z}_4$. Then,*

$$wt_L(\mathbf{v}) = \sum_{i=1}^{\alpha+\beta} wt_L(([\mathbf{v}]_{1,i}, [\mathbf{v}]_{2,i})^T),$$

where $wt_L((x, y)^T) = \max\{wt_L(x), wt_L(y), wt_L(x - y)\}$.

Recall, when computing the Lee weight defined in Lemma 1, that the first α column vectors in $[\mathbf{v}]$ contain quaternary zeros and twos which are representing binary zeros and ones, respectively. The lemma above let us go further on the Lee weights of codewords in the dual code of $\mathcal{C}_2$.

Proposition 7. *The nonzero Lee weights of the codewords in $\mathcal{C}_2^\perp$ are 2^{m-1} and $2^{m-1} + 2^{m-2}$, where $m = \gamma + 2\delta$.*

From the above proposition it is clear that the external distance of C_2 is $s = 2$, which leads us to the following proposition.

Proposition 8. *Code C_2 is uniformly packed.*

We include a technical lemma, which will help us later in Theorem 1.

Lemma 2. *Let $\mathcal{C}_2$ be the code defined over $GF(4)^\alpha \times GR(16)^\beta$, and let C_2 be the corresponding binary image which we know has covering radius 2. Let μ_i be the number of cosets in $C_2(i)$, for $0 \leq i \leq \rho$. Then,*

$$\mu_1 = 3n;\ \mu_2 = n(n-1), \text{ where } n = \alpha + 2\beta\ .$$

Now, we can prove the main theorem.

Theorem 1. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, with parity check matrix $\mathcal{H}$, such that its binary image $C = \Phi(\mathcal{C})$ is a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length $n = 2^m - 1$, for $m \geq 3$, and its $\mathbb{Z}_2\mathbb{Z}_4$-additive dual code $\mathcal{C}^\perp$ is of type $(\alpha, \beta; \gamma, \delta)$. Let $\mathcal{C}_2$ be the code defined over $GF(4)^\alpha \times GR(16)^\beta$, obtained by lifting $\mathcal{C}$, and let C_2 be the corresponding binary image of $\mathcal{C}_2$. Code C_2 is a completely regular code with intersection array $(3n, 2(n-1); 1, 6)$.*

Proof. Code C_2 is a projective code, hence $e \geq 1$. From Proposition 6 and Proposition 8 it is easy to see that code C_2 satisfies item (**v**) in Proposition 1 and so, code C_2 is completely regular.

For the computation of the intersection array $(b_0, b_1; c_1, c_2)$, as we know the code is completely regular, we easily have that $c_1 = 1$ and $c_2 = 6$; $|C_2|b_0 = |C_2(1)|c_1$ and $|C_2(1)|b_1 = |C_2(2)|c_2$. From Lemma 2 we know that $|C_2(1)| = 3n|C_2|$ and $|C_2(2)| = n(n-1)|C_2|$. In summary, we have $b_0 = 3n$; $c_1 = 1$; $c_2 = 6$; $b_1 = 6\frac{|C_2(2)|}{|C_2(1)|} = 6\frac{n(n-1)}{3n} = 2(n-1)$.

In general, the lifted code C_r, when $r > 2$, is neither completely regular, nor uniformly packed. We can take a specific example for the case $r = 3$ and show that the corresponding code C_3 has $\rho \neq s$. The same happens, in general, for $r \geq 3$.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code whose $\mathbb{Z}_2\mathbb{Z}_4$-additive dual code is of type $(3, 6; 0, 2)$, and having the following parity check matrix:

$$\mathcal{H} = \left(\begin{array}{c|c} 2\,0\,2 & 0\,1\,1\,1\,1\,2 \\ 2\,2\,0 & 1\,0\,1\,2\,3\,1 \end{array}\right). \tag{5}$$

Code $\mathcal{C}$ corresponds to a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C = \Phi(\mathcal{C})$ of length $n = 15$. Let $\mathcal{C}_r$ be the code defined over $GF(2^r)^3 \times GR(4^r)^6$, obtained by lifting $\mathcal{C}$, for $r = 3$, and let C_3 be its binary image.

Let $\mathbf{v}$ be any vector in $GF(8)^3 \times GR(64)^6$, and not in $\mathcal{C}_3$. As in the proof of Proposition 6, we have $d(\mathbf{v}, \mathcal{C}_3) = wt_L(\mathbf{e})$, where $\mathbf{v} = \mathbf{w} + \mathbf{e}$, $\mathbf{w} \in \mathcal{C}_3$, and $\mathbf{e}$ is a vector in $GF(8)^3 \times GR(64)^6$ of minimum weight in the coset of $\mathbf{v}$.

Since the covering radius of any perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code is 1, it follows that the Lee weight of every row in the matrix representation $[\mathbf{e}]$ of vector $\mathbf{e}$ is at most 1. Therefore, the covering radius of C_3 is $\rho \leq 3$.

We proceed to compute the external distance of $\mathcal{C}_3$. Let $\mathbf{w}$ be a codeword in $\mathcal{C}_3^{\perp}$, and let $[\mathbf{w}]$ be its matrix representation.

Let $w_1 = (220|123011)$, $w_2 = (202|011112)$, $w_3 = w_1 + w_2 = (022|130123)$ and $w_4 = 3(w_1 + w_2) = (022|310321)$ be four vectors generated by matrix in (5). Note that the Lee weight of $\mathbf{w}$ is 13 when $[\mathbf{w}]$ has vectors w_1, w_2 and w_3 as rows; it is 15 when $[\mathbf{w}]$ has vectors w_1, w_2 and w_4; it is 8 when $[\mathbf{w}]$ has vector w_1 and two zero rows and, finally, it is 12 when $[\mathbf{w}]$ has vector w_1, w_2 and one zero row. Thus the external distance s of C_3 is $s \geq 4$ and, therefore, C_3 is not a uniformly packed code.

Remark 2. As already mentioned at the beginning of this article, the quotient graph corresponding to the binary image of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code is distance-regular when that $\mathbb{Z}_2\mathbb{Z}_4$-linear code is completely regular.

From the completely regular codes C_2 described in this paper, we obtain distance-regular graphs with classical parameters. The bilinear forms graphs [6, Sec. 9.5] have the same parameters and they were not described, until recently in [12], as coset graphs of completely regular linear codes. The interesting point here is that Theorem 1 is giving now the same description but using nonlinear codes.

4 Lifting extended perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code having a perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear code binary image $C = \Phi(\mathcal{C})$ of length $n = 2^m - 1$, for $m \geq 3$, and let $\hat{\mathcal{C}}$ be the extended code of $\mathcal{C}$, studied in Section 2. Let $\hat{\mathcal{C}}_r$, for $r = 2$, be the code defined over $GF(4)^{\alpha+1} \times GR(16)^{\beta}$ obtained by lifting code $\hat{\mathcal{C}}$. Code $\hat{\mathcal{C}}_2$ has $\hat{\mathcal{H}}_2$ as parity check matrix, where $\hat{\mathcal{H}}_2$ is an $(\alpha+1) \times \beta \times 2$ matrix in which each submatrix (h_{ijk}) for a fixed $k \in \{1, 2\}$ coincides with the parity check matrix of $\hat{\mathcal{C}}$, that is $\hat{\mathcal{H}}$. Let $\hat{C}_2$ be the corresponding binary image of $\hat{\mathcal{C}}_2$.

The following proposition can be proved.

Proposition 9. *Code $\hat{C}_2$ has covering radius $\rho = 3$ and it is uniformly packed, but not completely regular.*

References

1. L.A. Bassalygo, G.V. Zaitsev and V.A. Zinoviev: Uniformly packed codes. Problems Information Transmission, vol. 10(1), (1974) 9–14.
2. L.A. Bassalygo and V.A Zinoviev: Remark on uniformly packed codes. Problems Information Transmission, vol. 13(3), (1977) 22–25.
3. J. Borges, C. Fernández, J. Pujol, J. Rifà and M. Villanueva: Z2Z4-linear codes: generator matrices and duality. Designs, Codes and Cryptography, vol. 54(2), (2010) 167–179.
4. J. Borges, K. T. Phelps and J. Rifà: The rank and kernel of extended 1-perfect Z4-linear codes and additive non-Z4-linear codes. IEEE Trans. Information Theory, vol. 49(8), (2003) 2028–2034.
5. J. Borges and J. Rifà: A characterization of 1-perfect additive codes. IEEE Trans. Information Theory, vol. 45(5), (1999) 1688–1697.
6. A.E. Brouwer, A.M. Cohen and A. Neumaier: Distance-Regular Graphs. Springer-Verlag, vol. 24(2), (1989).
7. P. Delsarte: An algebraic approach to the association schemes of coding theory. Philips Research Reports Supplements, vol. 10, (1973).
8. P. Delsarte: Four Fundamental Parameters of a Code and Their Combinatorial Significance. Information and Control, vol. 23(5), (1973) 407–438.
9. A. Neumaier: Completely regular codes. Discr. Math. 106/107, (1992) 335–360.
10. J. Rifà and J. Pujol: Translation Invariant Propelinear Codes. IEEE Trans. Information Theory, vol. 43(2), (1997) 590–598.
11. J. Rifà, J. Solov'eva and M. Villanueva: On the intersection of Z2Z4-additive Hadamard codes. IEEE Trans. Information Theory, vol. 55(4), (2009) 1766–1774.
12. J. Rifà and V.A. Zinoviev: On lifting perfect codes. To appear in IEEE Trans. Information Theory. Now, available from http://arxiv.org/abs/1002.0295, (2010).

Appendix E

$\mathbb{Z}_2\mathbb{Z}_4$-additive and quaternary linear Reed-Muller codes

Table E.1: $\mathbb{Z}_2\mathbb{Z}_4$-additive Reed-Muller codes $\mathcal{ARM}_s(r,m)$ and quaternary linear Reed-Muller codes $\mathcal{RM}_s(r,m)$.

		s \ r	0	1	2	3	4	5	6
$m=1$	$\mathbb{Z}_2\mathbb{Z}_4$	0	$(2,0;1,0)$	$(2,0;2,0)$					
	$\mathbb{Z}_4$	0	$(0,1;1,0)$	$(0,1;0,1)$					
$m=2$	$\mathbb{Z}_2\mathbb{Z}_4$	0	$(4,0;1,0)$	$(4,0;3,0)$	$(4,0;4,0)$				
		1	$(2,1;1,0)$	$(2,1;1,1)$	$(2,1;2,1)$				
	$\mathbb{Z}_4$	0	$(0,2;1,0)$	$(0,2;1,1)$	$(0,2;0,2)$				
$m=3$	$\mathbb{Z}_2\mathbb{Z}_4$	0	$(8,0;1,0)$	$(8,0;4,0)$	$(8,0;7,0)$	$(8,0;8,0)$			
		1	$(4,2;1,0)$	$(4,2;2,1)$	$(4,2;3,2)$	$(4,2;4,2)$			
	$\mathbb{Z}_4$	0	$(0,4;1,0)$	$(0,4;2,1)$	$(0,4;1,3)$	$(0,4;0,4)$			
		1	$(0,4;1,0)$	$(0,4;0,2)$	$(0,4;1,3)$	$(0,4;0,4)$			
$m=4$	$\mathbb{Z}_2\mathbb{Z}_4$	0	$(16,0;1,0)$	$(16,0;5,0)$	$(16,0;11,0)$	$(16,0;15,0)$	$(16,0;16,0)$		
		1	$(8,4;1,0)$	$(8,4;3,1)$	$(8,4;5,3)$	$(8,4;7,4)$	$(8,4;8,4)$		
		2	$(4,6;1,0)$	$(4,6;1,2)$	$(4,6;3,4)$	$(4,6;3,6)$	$(4,6;4,6)$		
	$\mathbb{Z}_4$	0	$(0,8;1,0)$	$(0,8;3,1)$	$(0,8;3,4)$	$(0,8;1,7)$	$(0,8;0,8)$		
		1	$(0,8;1,0)$	$(0,8;1,2)$	$(0,8;1,5)$	$(0,8;1,7)$	$(0,8;0,8)$		
$m=5$	$\mathbb{Z}_2\mathbb{Z}_4$	0	$(32,0;1,0)$	$(32,0;6,0)$	$(32,0;16,0)$	$(32,0;26,0)$	$(32,0;31,0)$	$(32,0;32,0)$	
		1	$(16,8;1,0)$	$(16,8;4,1)$	$(16,8;8,4)$	$(16,8;12,7)$	$(16,8;15,8)$	$(16,8;16,8)$	
		2	$(8,12;1,0)$	$(8,12;2,2)$	$(8,12;4,6)$	$(8,12;6,10)$	$(8,12;7,12)$	$(8,12;8,12)$	
	$\mathbb{Z}_4$	0	$(0,16;1,0)$	$(0,16;4,1)$	$(0,16;6,5)$	$(0,16;4,11)$	$(0,16;1,15)$	$(0,16;0,16)$	
		1	$(0,16;1,0)$	$(0,16;2,2)$	$(0,16;2,7)$	$(0,16;2,12)$	$(0,16;1,15)$	$(0,16;0,16)$	
		2	$(0,16;1,0)$	$(0,16;0,3)$	$(0,16;2,7)$	$(0,16;0,13)$	$(0,16;1,15)$	$(0,16;0,16)$	
$m=6$	$\mathbb{Z}_2\mathbb{Z}_4$	0	$(64,0;1,0)$	$(64,0;7,0)$	$(64,0;22,0)$	$(64,0;42,0)$	$(64,0;57,0)$	$(64,0;63,0)$	$(64,0;64,0)$
		1	$(32,16;1,0)$	$(32,16;5,1)$	$(32,16;12,5)$	$(32,16;20,11)$	$(32,16;27,15)$	$(32,16;31,16)$	$(32,16;32,16)$
		2	$(16,24;1,0)$	$(16,24;3,2)$	$(16,24;6,8)$	$(16,24;10,16)$	$(16,24;13,22)$	$(16,24;15,24)$	$(16,24;16,24)$
		3	$(8,28;1,0)$	$(8,28;1,3)$	$(8,28;4,9)$	$(8,28;4,19)$	$(8,28;7,25)$	$(8,28;7,28)$	$(8,28;8,28)$
	$\mathbb{Z}_4$	0	$(0,32;1,0)$	$(0,32;5,1)$	$(0,32;10,6)$	$(0,32;10,16)$	$(0,32;5,26)$	$(0,32;1,31)$	$(0,32;0,32)$
		1	$(0,32;1,0)$	$(0,32;3,2)$	$(0,32;4,9)$	$(0,32;4,19)$	$(0,32;3,27)$	$(0,32;1,31)$	$(0,32;0,32)$
		2	$(0,32;1,0)$	$(0,32;1,3)$	$(0,32;2,10)$	$(0,32;2,20)$	$(0,32;1,28)$	$(0,32;1,31)$	$(0,32;0,32)$
...	...	...	...	...	...	...	...	...	...

Lorena Ronquillo Moreno
Bellaterra, February 2012