Intersection problem for the class of quaternary reed-muller codes

Except where reference is made to the work of others, the work described in this dissertation is my own or was done in collaboration with my advisory committee. This dissertation does not include proprietary or classified information.

Abel Ahbid Ahmed Delgado Ortiz

Certificate of Approval:

Douglas A. Leonard Professor Mathematics and Statistics	Kevin T. Phelps, Chair Professor Mathematics and Statistics
Geraldo S. De Souza Professor Mathematics and Statistics	George T. Flowers Dean Graduate School

Intersection problem for the class of quaternary reed-muller codes

Abel Ahbid Ahmed Delgado Ortiz

A Dissertation

Submitted to

the Graduate Faculty of

Auburn University

in Partial Fulfillment of the

Requirements for the

Degree of

Doctor of Philosophy

Auburn, Alabama
August 10, 2009

Intersection problem for the class of quaternary reed-muller codes

Abel Ahbid Ahmed Delgado Ortiz

_____

Signature of Author

_____

Date of Graduation

Dissertation Abstract

Intersection problem for the class of quaternary reed-muller codes

Abel Ahbid Ahmed Delgado Ortiz

Doctor of Philosophy, August 10, 2009
(M.S., University of Puerto Rico, February 16, 2003)
(B.S., Universidad Nacional San Antonio Abad, December 17, 1996)

58 Typed Pages

Directed by Kevin T. Phelps

Given two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over an alphabet F, we denote the size of their intersection by $\eta(\mathcal{C}_1, \mathcal{C}_2)$, and call this the intersection number of $\mathcal{C}_1$ and $\mathcal{C}_2$.

In general the intersection problem can be stated as follows: given a family or class of families of codes, find the spectrum of intersection numbers. The general strategy to attack this kind of problem begins by finding necessary conditions for the intersection. This leads to lower and upper bounds or a set of possible intersection numbers. Secondly, finding the sufficient conditions implies giving specific constructions of codes in such a way that the cardinality of their intersection fits those values between these bounds.

In this dissertation is presented a complete solution of the intersection problem for $\overline{\mathcal{QRM}}(r, m)$. This includes the well-known quaternary Kerdock code, the Kerdock-like code and Preparata-like code.

Style manual or journal used *Journal of Approximation Theory (together with the style known as "aums"). Bibliograpy follows van Leunen's A Handbook for Scholars.*

Computer software used *The document preparation package TEX (specifically LATEX) together with the departmental style-file* `aums.sty`.

Table of Contents

Chapter 1

Introduction

Let $\mathbb{Z}_2^n$ denote the vector space of dimension n over $\mathbb{Z}_2$. A linear subspace of dimension k will be called a *binary-$[n,k]$-linear code* over $\mathbb{Z}_2$, $[n,k]$-code for short. An element of a code C is called a *codeword*. A $k \times n$ matrix G, whose rows form a basis for an $[n,k]$-code is called a *generator matrix* of the code. An *information set* for C is any set of k linearly independent columns of G. The remaining $r = n-k$ columns are called a *redundant set* and r is the *redundancy* of C. G is called *systematic* if it has the form $[I|A]$, where I is a $k \times k$ identity matrix and A is a $k \times (n-k)$ matrix. A code C has a systematic generator matrix if and only if the first k columns of any generator matrix of C are linearly independent. In this case the information set is taken to be the set of the first k columns of the matrix.

The *inner product* of two vectors $\mathbf{x} = (x_1, \ldots, x_n)$, and $\mathbf{y} = (y_1, \ldots, y_n)$ in $\mathbb{Z}_2^n$ is

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i \pmod 2. \tag{1.1}$$

Given a $[n,k]$-code C, the *dual code* or *orthogonal code* of C is defined by

$$C^{\perp} = \{\mathbf{x} \in \mathbb{Z}_2^n \,|\, \mathbf{x} \cdot \mathbf{c} = \mathbf{0}, \forall \mathbf{c} \in C\}. \tag{1.2}$$

$C^{\perp}$ is a $[n, n-k]$-code. A code C is *self-orthogonal* provided that $C \subseteq C^{\perp}$ and *self-dual* provided that $C = C^{\perp}$.

An $(n-k) \times n$ matrix H is called a *parity-check matrix* for the $[n,k]$-code C if the columns of H form a basis for the dual code C. If $G = [I_k|A]$ is a generator matrix for the $[n,k]$-code C, then $H = [-A^T|I_{n-k}]$ is a parity-check matrix for C.

The *Hamming distance* $d(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n$ is the number of positions in which $\mathbf{x}$ and $\mathbf{y}$ differ. The minimum (*Hamming*) distance d of a code C is the smallest distance between distinct codewords. The (*Hamming*) *weight* $wt(\mathbf{x})$ of a vector $\mathbf{x} \in \mathbb{Z}_2^n$ is the number of nonzero coordinates in $\mathbf{x}$. If C is a linear code, the minimum distance d coincides with the minimum weight of the nonzero codewords of C. If the minimum weight d of an $[n, k]$-code is known, then we refer to the code as an $[n, k, d]$-code.

Let C_i be an $[n, k_i, d_i]$-code for $i \in \{1, 2\}$, both over $\mathbb{Z}_2$. The $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction produces the $[2n, k_1 + k_2, \min\{2d_1, d_2\}]$ code

$$C = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) | \mathbf{u} \in C_1, \mathbf{v} \in C_2\}. \tag{1.3}$$

If C_i has a generator matrix G_i and parity-check matrix H_i, then generator and parity-check matrices for C are

$$\begin{pmatrix} G_1 & G_2 \\ 0 & G_2 \end{pmatrix} \text{ and } \begin{pmatrix} H_1 & 0 \\ -H_2 & H_2 \end{pmatrix}. \tag{1.4}$$

Let $[n]$ be the set $\{1, 2, \ldots, n\}$. S_n denotes the symmetric group of $[n]$. Two $[n, k]$ codes C_1, C_2, are *permutation equivalent* if there exists a permutation $\pi \in S_n$ such that $C_1 = \pi(C_2)$.

Let $\mathbb{Z}_4^n$ be the set of all n-tuples over $\mathbb{Z}_4$. If $\mathcal{C}$ is an additive subgroup of $\mathbb{Z}_4^n$ then it is called a *quaternary linear* code of length n. $\mathcal{C}$ can be expressed as a direct sum of δ cyclic subgroups of order 4 of $\mathbb{Z}_4^n$ and γ cyclic subgroups of order 2 of $\mathbb{Z}_4^n$, and we say that the type of $\mathcal{C}$ is $4^\delta 2^\gamma$. Notice that $\mathcal{C}$ has 2^m elements, where $2 \cdot \delta + \gamma = m$. Alternatively, we can say that $\mathcal{C}$ is code of type (n, δ, γ) or that $\mathcal{C}$ is an (n, δ, γ)-code.

We call G a *generator matrix* of $\mathcal{C}$ if its rows generate $\mathcal{C}$.

Every quaternary linear code $\mathcal{C}$ of type $4^\delta 2^\gamma$ is permutation equivalent to a quaternary linear code with generator matrix of the form

$$\begin{pmatrix} I_\delta & A & B \\ 0 & 2I_\gamma & 2C \end{pmatrix}, \tag{1.5}$$

where I_δ and I_γ denote the identity matrices, of order δ and γ, respectively, A, C, are $\mathbb{Z}_2$-matrices, B is a $\mathbb{Z}_4$- matrix and 0 is the $\gamma \times \delta$ zero matrix.

The inner product of two vectors $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$ in $\mathbb{Z}_4^n$ is

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i \pmod 4. \tag{1.6}$$

Let $\mathcal{C}$ be a quaternary linear code of length n. Define the *dual* code of $\mathcal{C}$ as

$$\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{Z}_4^n \,|\, \mathbf{x} \cdot \mathbf{c} = \mathbf{0}, \forall \mathbf{c} \in \mathcal{C}\}. \tag{1.7}$$

Notice that $\mathcal{C}^\perp$ is a quaternary linear code. If the generator matrix of $\mathcal{C}$ is given by (1.5), then the generator matrix of $\mathcal{C}^\perp$ is given by

$$\begin{pmatrix} -B^T - C^T A^T & C^T & I_{n-\delta-\gamma} \\ 2A^T & 2I_\gamma & 0 \end{pmatrix} \tag{1.8}$$

The *Lee weights* of 0, 1, 2, 3 $\in \mathbb{Z}_4$ are 0, 1, 2, 1, respectively. For $i \in \mathbb{Z}_4$, the Lee weight of i is denoted by $w_L(i)$. The *Lee weight* $w_L(\mathbf{x})$ of $\mathbf{x} = (x_1 \ldots x_n) \in \mathbb{Z}_4^n$ is defined to be the integral sum of the Lee weights of its components,

$$w_L(\mathbf{x}) = \sum_{i=1}^{n} w_L(x_i). \tag{1.9}$$

This weight function defines a distance function $d_L(\mathbf{x}, \mathbf{y}) = w_L(\mathbf{x} - \mathbf{y})$ on $\mathbb{Z}_4^n$, which is called the *Lee distance*.

The map $\phi : \mathbb{Z}_4 \to \mathbb{Z}_4^2$, defined by $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$, and $\phi(3) = 10$, is called the *Gray map*. This map can be extended componentwise to a map, also denoted by ϕ, from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$. In general, given a quaternary linear code $\mathcal{C}$, its binary image $\phi(\mathcal{C})$ will be nonlinear. A binary code C is called $\mathbb{Z}_4$-*linear* if, after a permutation of coordinates, it is the binary image of a quaternary linear code.

An important property of the Gray map is that it is a distance preserving map from $\mathbb{Z}_4^n$ (with the Lee distance) to $\mathbb{Z}_2^{2n}$ (with the Hamming distance). Moreover if $\mathcal{C}$ i s a quaternary linear code then $\phi(\mathcal{C})$ is distance invariant.

A decomposition of a permutation $\pi \in S_n$ into nonintersecting cycles of length greater than 1, will be called *canonical*, and it is denoted as follows:

$$\pi = \prod_{j=2}^{\tau(\pi)} (\prod_{i=1}^{\tau_j} (v_{i,1}^j \cdots v_{i,j}^j)), \tag{1.10}$$

where τ_j denotes the number of j-cycles in the decomposition of π. The number of cycles will be denoted by $\tau(\pi) = \sum_{j=2}^{\ell} \tau_j$. For a cycle $\theta = (v_{p,1}^{\ell} v_{p,1}^{\ell} \ldots v_{p,\ell}^{\ell})$ of length ℓ in π, ℓ will be denoted by $\lambda(\theta)$. The sum of all lengths of the cycles in π will be denoted by $\lambda(\pi)$. $(\lambda(\pi) = \sum_{j=2}^{\tau(\pi)} j \cdot \tau_j)$.

Associated with π, there is a matrix P_π of order n, called a *permutation matrix* in which $P_\pi(i, j) = 1$, if $\pi(i) = j$ and 0 otherwise.

The *diagonal matrix* $diag(a_1, a_2, ...a_n)$ of order n is the matrix D defined by $D(i, j) := 0$ if $i \neq j$ and $D(i, i) := a_i$ where a_i are real entries.

Any matrix that can be written as the product of a permutation matrix and a diagonal matrix is called a *monomial matrix*.

Since we are interested in quaternary linear codes, we are going to use monomial matrices that have the matrix $diag(a_1, a_2, ...a_n)$ with entries a_i equal -1 or 1. Define the diagonal matrix D_i as $diag(a_1, a_2, ...a_n)$, where $a_j = -1$ if $i = j$, and $a_j = 1$, otherwise.

Associated with D_i there is a map $\rho_i : \mathbb{Z}_4^n \to \mathbb{Z}_4^n$ that multiplies the ith-coordinate of each vector of $\mathbb{Z}_4^n$ by -1. For $i = 0, \ldots, n$, ρ_i is called the *inversion of the ith-coordinate*,

where $Id = \rho_0$. In general, we will write ρ to denote an inversion of coordinates and ρ_s, when we want to emphasize the set S of coordinates. Let $\pi \in S_n$ and ρ an inversion of coordinates, the map $\rho(\pi)$ is called a *monomial map*. If P is the matrix associated to π, and D, the matrix associated to ρ, then the matrix PD is the matrix associated to the monomial map $\rho(\pi)$. Here D is the diagonal matrix that has -1 in those positions determined by ρ. From now on by monomial map or monomial matrix, we mean just what we say in this paragraph.

We say that $\mathcal{C}_1$ and $\mathcal{C}_2$ are *monomially equivalent*, provided there is a monomial map $\rho(\pi)$ such that $\rho(\pi(\mathcal{C}_1)) = \mathcal{C}_2$. Two quaternary linear codes that are equivalent are of the same type.

Given a vector $\mathbf{x} = (x_1 \dots x_n)$ and a subset $I = \{i_1, \dots, i_k\} \subset [n]$, $k < n$, the *projection* of $\mathbf{x}$ onto I is the vector $\mathbf{x}|_I = (x_{i_1}, \dots, x_{i_k})$ where $i_j < i_{j+1}$, $1 \leq j \leq k-1$. For a given permutation $\pi = \begin{pmatrix} 1\ 2 \dots n \\ i_1\, i_2 \dots i_n \end{pmatrix}$, $\mathbf{x}|_\pi = \mathbf{x}|_I$.

In chapter 2 and 3 of this dissertation we set up the reference frame for chapter 4. Specifically, chapter 2 contains the definitions and background information required to understand the main result and chapter 3 reviews the intersection problem from an historical point of view.

Chapter 4 presents the two main results: Theorem 4.7 which gives the intersection number for quaternary $t - IR$ codes and Theorem 4.9 which determines the algebraic structure of those intersections, moreover shows explicit constructions of their generator matrices. We end this chapter by applying these results to the class of quaternary Reed-Muller codes.

Chapter 5 refers to the conclusions of this dissertation, as well as open problems and future directions for research.

Chapter 2

Binary Reed-Muller codes and Quaternary Reed-Muller codes

Since the codes that are the focus of this dissertation are characterized in terms of binary Reed Muller codes, in this chapter we are going to review their principal properties. In the literature, there are several constructions of these codes, but they were first treated by D.E Muller (1954) and I.S Reed (1954). The mathematical interest of Reed-Muller codes is that they are related to affine and projective geometries.

Kumar etal. [1], presented a construction of the quaternary Kerdock code $\mathcal{K}(m)$ as well as a construction of the quaternary Preparata code $\mathcal{P}(m)$, which is the Z_4-dual of $\mathcal{K}(m)$. The Gray map image of the quaternary Kerdock code $\mathcal{K}(m)$ is a nonlinear binary code $K(m)$ that is permutation equivalent to the original definition given by Kerdock. The quaternary Preparata code is defined as $\mathcal{P}(m) = \mathcal{K}(m)^{\perp}$. The binary Gray map image of $\mathcal{P}(m)$ gives a nonlinear code, P, that has the same parameters of the original code defined by Preparata, but there is an essential difference between $\mathcal{P}(m)$ and P. The first one is contained in a nonlinear code with the same weight distribution as the extended binary Hamming code of the same length (see Theorem 9.10 of [2]). The second one, is a subcode of the extended binary Hamming code of the same length (Proposition 9.14 of [2]). It is known that there are several codes with the same parameters as the quaternary Preparata code. They are named quaternary Preparata-like codes and their $\mathbb{Z}_4$ dual are codes with the same parameters as the Kerdock codes . In [1], they also established the quaternary Reed Muller code $\mathcal{QRM}(r, m)$, as a $\mathbb{Z}_4$-version of the binary Reed Muller code, which includes quaternary Kerdock codes and Preparata codes as special cases and have the property that their images through α (mod 2) map are the binary Reed-Muller codes. Considering arbitrary Preparata-like codes it was observed in [3] that it is possible to construct a family of quaternary codes similar to

that constructed in [1], whose binary image through the $\alpha \pmod 2$ map is a Reed Muller code that contains the Kerdock-like codes and the Preparata-like codes as a special cases.

In [6], [5] a superclass that contains the $\mathcal{QRM}(r, m)$ was defined. Also various properties including the kernel and rank of the Gray map of codes in this superclass were established in [3].

2.1 Binary Reed-Muller Codes

Let $r, m \in \mathbb{Z}$ such that $0 \leq r \leq m$. Consider, the set of all binary vectors of length m ordered lexicographically. Any function $f : \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2$ is called a *Boolean* function, defined on m variables. If we evaluate f on its domain, the corresponding 2^m entries define a unique binary vector $\mathbf{f}$ of length $n = 2^m$. Conversely, given any binary vector of length n, we can associate a unique Boolean function defined on m variables whose domain is $\mathbb{Z}_2^m$. Thus, there is a bijection between Boolean functions f and the corresponding vectors $\mathbf{f}$. Since $\mathbf{f}$ has 2^m entries and each one can be 0 or 1, we have 2^{2^m} vectors and therefore the same number of Boolean functions.

For example, the binary vector $\mathbf{f} = 11010010$ of length 8, corresponds to the Boolean function on three variables f, defined by its truth table:

x_1	x_2	x_3	f
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

For $1 \leq j \leq m$, denote by x_j the Boolean function defined by the correspondence rule $f(x_1, \ldots, x_m) = x_j$. The corresponding vector $\mathbf{x}_j$ of length 2^m has a 1 in the coordinate i if and only if 2^{m-j} occurs in the binary expansion of $i-1$.

For example, let $m = 3$, $j = 2$. 2^{3-2} occurs in the binary expansion of 2,3,6,7, therefore, $\mathbf{x}_2$ has 1 in the coordinates 3,4,7,8, thus $\mathbf{x}_2 = (0,0,1,1,0,0,1,1)$.

Also, the constant Boolean functions, denoted by 0 and 1 are associated with the all zeros vector $\mathbf{0}$ and the all ones vector $\mathbf{1}$. Given two Boolean functions f and g, the sum $f+g$, and the product fg correspond to the logical operators $\wedge$ and $\vee$. The function $\overline{f} = 1 - f$, correspond to the operator NOT.

The set $\mathcal{B}$ of all Boolean functions defined on m-variables, which is equal to the set of all binary functions defined on $\mathbb{Z}_2$, is a linear space over $\mathbb{Z}_2$. Thus, $\mathcal{B}$ with the standard addition and scalar multiplication of functions, is a linear space over $\mathbb{Z}_2$. Moreover, due to the standard product of functions, $\mathcal{B}$ is a commutative linear algebra. Notice, that we have the following relations:

$$x_i \cdot x_i = x_i, \text{ and } x_i \cdot x_j = x_j \cdot x_i \ . \tag{2.1}$$

We relate the Boolean functions to their corresponding binary vectors by defining the componentwise product of the vectors $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$ over $\mathbb{Z}_2$ as

$$\mathbf{ab} = (a_1 b_1, \ldots, a_n b_n) \tag{2.2}$$

Thus, binary vectors related to (2.1) are given by

$$\mathbf{x}_i \mathbf{x}_i = \mathbf{x}_i, \text{ and } \mathbf{x}_i \mathbf{x}_j = \mathbf{x}_j \mathbf{x}_i \ . \tag{2.3}$$

Using, the product and the functions x_j, we get $2^m - 1$ terms with different forms

$$x_{i_1} \cdots x_{i_k}, \text{ with } k \leq m \quad \text{and} \quad i_1 < i_2 < \cdots < i_k \tag{2.4}$$

The linear combination of the function 1 with the terms in (2.4) are linearly independent [7] and therefore the corresponding binary vectors

$$\mathbf{1}, \mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_m, \mathbf{x}_1\mathbf{x}_2, \mathbf{x}_1\mathbf{x}_3, \ldots, \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3 \cdots \mathbf{x}_m, \tag{2.5}$$

are also linearly independent and generate $\mathbb{Z}_2^n$. The next table is an example of the 16 Boolean functions that generate the space of all the Boolean functions from $\mathbb{Z}_2^4$ to $\mathbb{Z}_2$, and the corresponding binary vectors of length 16 that generate $\mathbb{Z}_2^{16}$.

Boolean function	*Vector*																
1	$\mathbf{1} =$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	$\mathbf{0} =$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x_1	$\mathbf{x}_1 =$	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
x_2	$\mathbf{x}_2 =$	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_3	$\mathbf{x}_3 =$	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_4	$\mathbf{x}_4 =$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_1x_2	$\mathbf{x}_1\mathbf{x}_2 =$	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1
x_1x_3	$\mathbf{x}_1\mathbf{x}_3 =$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
x_1x_4	$\mathbf{x}_1\mathbf{x}_4 =$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
x_2x_3	$\mathbf{x}_2\mathbf{x}_3 =$	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1
x_2x_4	$\mathbf{x}_2\mathbf{x}_4 =$	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0
$x_1x_2x_3$	$\mathbf{x}_1\mathbf{x}_2\mathbf{x}_3 =$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
$x_1x_2x_4$	$\mathbf{x}_1\mathbf{x}_2\mathbf{x}_4 =$	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
$x_1x_3x_4$	$\mathbf{x}_1\mathbf{x}_3\mathbf{x}_4 =$	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
$x_2x_3x_4$	$\mathbf{x}_1\mathbf{x}_2\mathbf{x}_4 =$	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
$x_1x_2x_3x_4$	$\mathbf{x}_1\mathbf{x}_2\mathbf{x}_3\mathbf{x}_4 =$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Let $0 \leq r \leq m$. The *rth order Reed-Muller* code $R(r,m)$ of length $n = 2^m$ is the set of codewords generated by the matrix G(r,m):

$$G(r,m) = \begin{pmatrix} G_0 \\ G_1 \\ G_2 \\ \vdots \\ G_r \end{pmatrix}.$$

where G_0 is the 1×2^m matrix equals to the all-one vector of length 2^n, G_1 is the $\binom{m}{1} \times 2^m$ matrix whose rows are the binary vectors $\mathbf{x}_1, \ldots, \mathbf{x}_n$ given in (2.4), and for $1 < r \leq m$, G_r, is the $\binom{m}{r} \times 2^m$ matrix whose rows are the binary vectors obtained by the componentwise multiplication of a choice of r rows of G_1.

There are two trivial codes: $R(0,m)$, called the *repetition* code with generator matrix $G(0,m)$ and $R(m,m)$ which is the all space $\mathbb{Z}_2^n$. As an example of a nontrivial code, we have the second order Reed-Muller code of length 16, $RM(2,4)$, given by the following generator matrix :

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

Alternatively, these codes can be constructed using the $(u|u+v)$ construction(1.3)

Theorem 2.1. *Let r, m be integers such that $0 \leq r \leq m$. The rth order Reed-Muller code $RM(r, m)$ is constructed in the following way:*

1. *The 0th order Reed-Muller code $RM(0, m)$ is the repetition code $\{\mathbf{0}, \mathbf{1}\}$, and the mth-order Reed-Muller code $RM(m, m)$ is $\mathbb{Z}_2^{2^m}$*

2. *$RM(r, m) = \{(\mathbf{u}, \mathbf{u} + \mathbf{v}) | \mathbf{u} \in RM(r, m-1), \mathbf{v} \in RM(r-1, m-1)\}$, $0 < r < m$*

For $0 < r < m$, let $G(r, m)$ be a generator matrix of the Reed-Muller code, then according to (1.4)

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

For $r = 0$, $G(r, m) = (\mathbf{1})$ and for $r = m$,

$$G(m,m) = \begin{pmatrix} G(m-1,m) \\ \mathbf{e}_i \end{pmatrix}.$$

where $\mathbf{e}_i = (0, .., 1, .., n)$. The number 1 appears at the *ith*-position.

The following theorem shows the principal properties of Reed-Muller codes.

Theorem 2.2. *Let r, m be integers such that $0 \leq r \leq m$. Then the following hold:*

1. *$R(i, m) \subseteq R(j, m)$, if $0 \leq i \leq j \leq m$.*

2. *The dimension of $R(r, m)$ equals $k = 1 + \binom{m}{1} + \binom{m}{2} + ... + \binom{m}{r}$.*

3. *The minimum weight of $R(r, m)$ equals 2^{m-r}.*

4. *$R(m, m)^{\perp} = \{\mathbf{0}\}$ and if $0 \leq r < m$, then $R(r, m)^{\perp} = RM(m - r - 1, m)$.*

2.2 The Quaternary Reed-Muller Codes

The purpose of this section is to introduce $\mathcal{QRM}(r, m)$ codes, which were defined in [1] to be quaternary Reed-Muller codes of length 2^{2^m}. In order to proceed, some terminology and notation is needed. We follow closely the book *Quaternary codes* (see [2])

In chapter 1 we saw that the Gray map relates codes of length n over $\mathbb{Z}_4$ with binary codes of length $2n$. But also, we can relate codes of length n over $\mathbb{Z}_4$ with binary codes of the same length. A natural way is to extend componentwise the additive group homomorphism $\alpha : \mathbb{Z}_4 \to \mathbb{Z}_2$, defined by $\alpha(0) = \alpha(2) = 0$, $\alpha(1) = \alpha(3) = 1$ to a map $\alpha : \mathbb{Z}_4^n \to \mathbb{Z}_2^n$. Thus, if $\mathbf{x} = (x_1, \ldots, x_n)$, then $\alpha(\mathbf{x}) = (\alpha(x_1), \ldots, \alpha(x_n))$.

Let $\mathbb{Z}_4[X]$ be the polynomial ring with coefficients in $\mathbb{Z}_4$. The map α can be naturally extended to a map from $\mathbb{Z}_4[X]$ to $\mathbb{Z}_2[X]$ as follows

$\mathbb{Z}_4[X] \to \mathbb{Z}_2[X]$

$a_0 + a_1X + \cdots + a_nX^n \to \alpha(a_0) + \alpha(a_1)X + \cdots + \alpha(a_n)X^n$

Let $h(X)$ be a monic polynomial of degree $m \geq 1$ in $\mathbb{Z}_4[X]$. If $\alpha(h(X))$ is irreducible over $\mathbb{Z}_2$, then $h(X)$ is called a *basic irreducible polynomial* of degree m in $\mathbb{Z}_4[X]$. If $h(X)$ is primitive of degree m over $\mathbb{Z}_2$ then $h(X)$ is called a *basic primitive polynomial* of degree m in $\mathbb{Z}_4[X]$.

Let $2 \leq m \in \mathbb{Z}$ and $n = 2^m - 1$. Let ζ be a root of a basic primitive polynomial $h(x)$ of degree m dividing $X^n - 1$. Since ζ is a basic primitive root of unity, $\zeta, \zeta^2, ..., \zeta^n = 1$, are n distinct root of $h(x)$. Consider the $(m+1) \times 2^m$ matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & . & . & . & 1 \\ 0 & 1 & \zeta & \zeta^2 & . & . & . & \zeta^{n-1} \end{pmatrix}, \tag{2.6}$$

whose rows are are numbered by $0, 1, ..., m$ and columns by $\infty, 0, 1..., n-1$, where ζ^j should be replaced by ${}^t(b_{1j}, ..., b_{mj})$ if $\zeta^j = b_{1j} + \cdots + b_{mj}\zeta^{m-1}$ $(j = \infty, 0, 1 \ldots, n-1)$ and we agree that $\zeta^\infty = 0$. Denote the *ith* row of the matrix by u_i, then the *quaternary rth order Reed-Muller code* $\mathcal{QRM}(r, m)$ of length 2^m is the code generated by the 2^m tuples of the form

$$u_{i_1}u_{i_2}, \ldots, u_{i_s},\ 1 \leq i_1 < i_2, \ldots, < i_s \leq m,\ 0 \leq s \leq r, \text{where } u_{i_1}u_{i_2}, \ldots, u_{i_s} = 1^{2^m} \tag{2.7}$$

when s=0.

It can be proved that these vectors, form a basis over the free $\mathbb{Z}_4$ module $\mathbb{Z}_4^{2^m}$. Basic properties of $\mathcal{QRM}(r,m)$ codes are enlisted in the following Theorem

Theorem 2.3. [1]*Let r, m integers such that $0 \leq r \leq m$. Let $\mathcal{QRM}(r,m)$ be a quaternary Reed-Muller code of length 2^m*

1. *$\mathcal{QRM}(r,m)$ is of type 4^k where $k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$.*
2. *$\mathcal{QRM}(r,m) \subset \mathcal{QRM}(r+1,m)$, $\forall r < m$.*
3. *$\alpha(\mathcal{QRM}(r,m)) = RM(r,m)$.*

When $r = 1$, $\mathcal{QRM}(1,m)$, is known as the *quaternary linear Kerdock* code and will be denoted by $\mathcal{K}(m)$. If $m \geq 2$ and $0 \leq r \leq m-1$, then $\mathcal{QRM}(r,m)^\perp = \mathcal{QRM}(m-r-1,m)$. Another well-known code is obtained when $r = m-2$, named the *quaternary linear Preparata* code, denoted by $\mathcal{P}(m)$. The quaternary Kerdock code and the quaternary Preparata code were first defined in [1].

Since $\mathcal{QRM}(m-2,m) = \mathcal{QRM}(1,m)^\perp = \mathcal{K}(m)^\perp = \mathcal{P}(m)$, the quaternary Preparata codes are duals of Kerdock codes and therefore, $\mathcal{P}(m)$ is of type 4^{k_1}, where, $k_1 = 2^m - k$, with $k = k = 1 + \binom{m}{1}$.

The Gray map image of $\mathcal{QRM}(r,m)$ is a $\mathbb{Z}_4$-linear code which is denoted by $QRM(r,m)$. Notice that this code is a nonlinear binary code.

We illustrate the previous discussion with an example. Let $h(x) = x^4+3x^3+2x^2+1$ be a basic irreducible polynomial over $\mathbb{Z}_4$. Let ζ be a root of $h(x)$ in the Galois ring $GR(4^4)$. Then, $\zeta = (0,1,0,0)$, $\zeta^2 = (0,0,1,0)$, $\zeta^3 = (0,0,0,1)$, and ζ^j for $j \geq 4$ is getting using $\zeta^4 = \zeta^3 + 2\zeta^2 + 3$. Using (3.2.1) we get the generator matrix of $\mathcal{K}(4)$:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 3 & 3 & 1 & 3 & 2 & 1 & 0 & 3 & 1 & 2 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 3 & 3 & 1 & 3 & 2 & 1 & 0 & 3 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 & 2 & 2 & 1 & 1 & 1 & 1 & 2 & 3 & 2 & 3 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 3 & 1 & 2 & 3 & 0 & 1 & 3 & 2 & 0 & 3 \end{pmatrix} = \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix}.$$

The quaternary Preparata code, $\mathcal{P}(4) = \mathcal{QRM}(2,4)$, is generated by

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 3 & 3 & 1 & 3 & 2 & 1 & 0 & 3 & 1 & 2 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 3 & 3 & 1 & 3 & 2 & 1 & 0 & 3 & 1 & 2 \\
0 & 1 & 0 & 1 & 0 & 2 & 2 & 1 & 1 & 1 & 1 & 2 & 3 & 2 & 3 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 3 & 1 & 2 & 3 & 0 & 1 & 3 & 2 & 0 & 3 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 3 & 3 & 2 & 2 & 0 & 0 & 3 & 2 & 0 \\
0 & 1 & 0 & 0 & 0 & 2 & 2 & 1 & 3 & 2 & 1 & 0 & 1 & 2 & 2 & 0 \\
0 & 1 & 0 & 0 & 0 & 3 & 1 & 1 & 2 & 2 & 0 & 0 & 1 & 2 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 2 & 3 & 1 & 3 & 2 & 2 & 0 & 2 & 3 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 3 & 2 & 1 & 0 & 1 & 0 & 2 & 0 & 2 \\
0 & 1 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 3 & 0 & 2 & 1 & 0 & 0 & 3
\end{pmatrix}
=
\begin{pmatrix}
u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_i u_2 \\ u_1 u_3 \\ u_1 u_4 \\ u_2 u_3 \\ u_2 u_4 \\ u_3 u_4
\end{pmatrix}.$$

2.3 The Class of Quaternary Reed-Muller Codes

The class $\overline{\mathcal{QRM}}(r,m)$ of quaternary Reed-Muller codes is a generalization of $\mathcal{QRM}$ codes. We describe briefly those aspects that are relevant to the purpose of this dissertation. The material used in this section can be found in the paper [6] and chapter six of [5].

Definition 2.3.1. *Let $r, m \in \mathbb{Z}$ and $0 \leq r \leq m$. $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$ if and only if :*

1. *The quaternary length of the code $\mathcal{C}$ is 2^m.*
2. *$\mathcal{C}$ is of type 4^k, where $k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$*
3. *$\alpha(\mathcal{C}) = RM(r,m)$.*

The related binary class is defined as $\overline{QRM}(r,m) = \{C | \, C = \phi(\mathcal{C}) \in QRM(r,m)\}$

By Theorem 2.3 $\mathcal{QRM}(r,m)$ codes satisfies definition 2.3.1 above. Thus, $\mathcal{QRM}(r,m) \in \overline{\mathcal{QRM}}(r,m)$. In order to give another example, let χ be the map from $\mathbb{Z}_2$ to $\mathbb{Z}_4$, which is the usual inclusion from the additive structure in Z_2 to Z_4 : $\chi(0) = 0$, $\chi(1) = 2$. This map can be extended to the map $(\chi, Id) : \mathbb{Z}_2^n \mapsto \mathbb{Z}_4^n$, which will also be denoted by χ,

(see [8]). That way, using this inclusion map, the binary vectors defined in (1.4) can be considered as a quaternary vectors. This is the case in the next example, which is denoted by $\mathcal{SRM}(r,m)$ and defined as the quaternary code which is generated by the generators of the binary Reed-Muller code $RM(r,m)$[6].

The $(\mathbf{u}|\mathbf{u}+\mathbf{v})$-construction defined in (1.3) allows one to construct other codes in $\overline{\mathcal{QRM}}(r,m)$ apart from $\mathcal{QRM}(r,m)$ and $\mathcal{SRM}(r,m)$.

Theorem 2.4. *Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$ and $\mathcal{D} \in \overline{\mathcal{QRM}}(r,m)$. Then, the code $\mathcal{C}^*$ defined as $\{(\mathbf{u},\mathbf{u}+\mathbf{v})|\mathbf{u}\in\mathcal{C},\mathbf{v}\in\mathcal{D}$ belongs to the class $\overline{\mathcal{QRM}}(r+1,m+1)$.*

Theorem 2.5. *Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$, with $1 \leq r \leq m$ then*

$$\mathcal{C}^{\perp} \in \overline{\mathcal{QRM}}(m-r-1,m)$$

It is useful to characterize codes in the $\overline{\mathcal{QRM}}(r,m)$ class in terms of generator matrices. If G is a quaternary matrix with row vectors $\mathbf{x}_1,\mathbf{x}_2\ldots,\mathbf{x}_k$, then $\alpha(G)$ is defined as

$$\begin{pmatrix} \alpha(\mathbf{x}_1) \\ \alpha(\mathbf{x}_2) \\ \vdots \\ \alpha(\mathbf{x}_k) \end{pmatrix}.$$

Lemma 2.3.1. [5] *Let $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$ and let G be its generator matrix. Then $\alpha(\mathcal{C})$ is a generator matrix of $RM(r,m)$.*

Theorem 2.6. [5] *Let $\mathcal{C}$ be a quaternary code of length 2^m. $\mathcal{C}$ belongs to the class $\overline{\mathcal{QRM}}(r,m)$ if and only if there exist a binary $(\sum_{i=0}^{r}\binom{m}{i})\times 2^m$ matrix N, such that the generator matrix of $\mathcal{C}$ is $G(r,m)+2N$, where $G(r,m)$ is the generator matrix of $RM(r,m)$ defined in Theorem 2.1 above.*

Corollary 2.3.1. *If $\mathcal{C} \in \overline{\mathcal{QRM}}$, then $(\mathcal{C}/2RM(r,m),+) \approx (RM,+)$.*

Any quaternary code with the same parameters as the quaternary Preparata code is named *Preparata-like* and its $\mathbb{Z}_4$-dual is called *Kerdock-like*. The following theorem shows that these codes are members of $\mathcal{QRM}(r, m)$.

Theorem 2.7. *Let $P(2m)$ be a $\mathbb{Z}_4$-linear Preparata-like code, and $K(2m)$ a $\mathbb{Z}_4$-linear Kerdock-like code of length $n + 1 = 2^{2m}$. $P(2m) \in \overline{\mathcal{QRM}}$ and $K(2m) \in \overline{\mathcal{QRM}}$.*

Chapter 3

Intersection

3.1 Introduction

In this chapter we consider the intersection problem for coding theory first introduced by Etzion and Vardy [13] in the setting of binary perfect codes. Since then, this problem has been considered for other families of codes such as Hadamard codes and q-ary cyclic codes whose alphabets are finite fields [14], [10], [11] or for families of codes whose alphabet is the ring of integer modulo 4 [15], [23].

Given two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over an alphabet F, we denote the size of their intersection by $\eta(\mathcal{C}_1, \mathcal{C}_2)$, and call this the intersection number of $\mathcal{C}_1$ and $\mathcal{C}_2$.

In general the intersection problem can be stated as follows: given a family or class of families of codes, find the spectrum of intersection numbers.

The general strategy to attack this kind of problem begins by finding necessary conditions for the intersection. This leads to lower and upper bounds or a set of possible intersection numbers. Secondly, finding the sufficient conditions implies giving specific constructions of codes in such a way that the cardinality of their intersection fits those values between these bounds. In this chapter, the alphabet F is the finite field $GF(q)$ of q elements.

3.2 Intersection problem for q-ary linear codes

Let C_1 be an $[n, k_1]$-code. Since it is a linear subspace of F^n, it is the kernel of some linear transformation. Let H_1 be the parity-check-matrix of order $(n - k_1) \times n$. Similarly, let C_2 be an $[n, k_2]$-code, with parity-check-matrix H_2 of order $(n - k_2) \times n$. The intersection $C = C_1 \cap C_2$ is also linear, therefore, there is a matrix $H = \begin{pmatrix} H_1 \\ H_2 \end{pmatrix}$ such

that $C_1 \cap C_2 = \{x \in F_q^n | Hx^T = \mathbf{0}\}$. Notice that, $rank(H) \leq 2n - (k_1 + k_2)$. Now, since $n = dim(C) + rank(H)$, $(k_1+k_2)-n \leq dim(C)$ and the intersection $C_1 \cap C_2 = q^{dim(C_1 \cap C_2)} \geq q^{(k_1+k_2)-n}$. Thus the intersection problem can be stated as follows: Determine the values v between $\max\{0, (k_1 + k_2) - n\}$ and $\min\{k_1, k_2\}$, such that q^v are intersection numbers of C_1 and C_2.

A particular case of this problem arises when $\mathcal{C}_2 = \pi(\mathcal{C}_1)$, where $\pi \in S_n$. In this case their dimensions are the same, $k_1 = k_2 = k$. Therefore both are of the same size and we look at the values v between $2k - n$ and k.

The intersection problem for this particular case (when the codes are permutation equivalent) was solved by Bar-Yahalom and Etzion [10] for q-ary cyclic codes. The approach they used was based on a partition of the columns of the generator matrix of the code into two sets $I(C)$ and $R(C)$, called the information set and the redundant set, respectively. $R(C)$ consists of $(n - k)$ columns, among which at most t are linearly independent. A code whose generator matrix presents a partition in which t gets its maximum value is called a t-redundancy or t-IR, and an independent redundancy or (IR) if $t = r$. Now if C is an $[n, k]$ t-IR code for which $t \leq k$, then the set of t linearly independent columns in $R(C)$ can be extended by $k - t$ columns from $I(C)$ to obtain a set of k linearly independent columns. This set of k linearly independent columns is called a *free set*.

The following theorems give an enumeration method for the intersection of linear codes with the partition of the generated matrix, explained above.

Theorem 3.1. [10] *If C is an $[n, k]$ t-IR code, then for each ρ, $0 \leq \rho \leq t - 1$, there exists a permutation π_ρ, for which $|\mathcal{C} \cap \pi_\rho(\mathcal{C})| = q^{k-\rho}$.*

Theorem 3.2. [10] *Let C be an $[n, k]$ code over F. If $\mathbf{1} \in C$ then $\eta(C, \pi(C)) \geq 2$.*

Theorem 3.3. [10] *Let C be an $[n, k]$ code over F. There exists $\pi \in S_n$, such that $\eta(C, \pi(C)) = q^{k_1}$ if and only if there exists $\pi_1 \in S_n$, such that $\eta(C^\perp, \pi_1(C^\perp)) = q^{n-2k+k_1}$.*

Theorem 3.4. [10] *Let C be an (n,k) code over F, $k \geq n-k$. If all the codewords have generalized parity 0, (that is, if the sum of the entries of the codeword is 0) then q^{2k-n} is not an intersection number of C.*

Example 3.2.1. *Let's see this enumeration method for the case of the binary Reed-Muller $RM(r,m)$ code. For $0 \leq r < m$, let $k = \sum_{i=0}^{m} \binom{m}{i}$ be dimension of this code. Denote by $r^* = n-k$ the redundancy number associated to the generator matrix of $RM(r,m)$ which has k linearly independent rows and then k linearly independent columns. Here we have two cases. The first one corresponds to $r \leq \lceil (m+1)/2 \rceil$ and then $k \leq r^*$. Since k of the other $n-k$ columns are linearly independent, then we have a partition where t gets its maximum value with $t = k$. The second case corresponds to $r > \lceil (m+1)/2 \rceil$, we have that $k > n-k$. So the maximum partition is obtained with $t = r^*$.*

If $RM(r,m)$ is an k-IR code, by Theorem 3.1, for each ρ, in $0 \leq \rho \leq k-1$, $2^{k-\rho}$ is an intersection number and since $\mathbf{1} \in RM(r,m)$ by Theorem 3.2, 1 is not an intersection number ($\rho = k$). But if $RM(r,m)$ is an $(n-k)$-IR code, for each ρ in $0 \leq \rho \leq n-k-1$, $2^{k-\rho}$ is an intersection number, and since the codewords of any binary Reed-Muller code are of even weight, the generalized parity is 0 and, by Theorem 3.4, 2^{2k-n} is not an intersection number, ($\rho = n-k$). The permutation that we choose for each ρ, can be the cycle $(1,..,\rho+1)$of length $\rho+1$.

Table 3.1 shows the variation of the interval for ρ and Table 3.2, is an example that shows the cycles that act over $RM(1,5)$ in order to get its corresponding isomorphic codes and then the cardinalities of their intersections.

One interesting family of q-ary linear codes are the so called q-ary Hamming codes. Given a finite field F, the q-ary Hamming code $\mathcal{H}_{q,r}$ of length $n = (q^r-1)/(q-1)$, where $r \geq 2$, is defined by the parity-check matrix whose columns are the points (in some order) of the projective geometry $PG(q-1,r)$. (A projective geometry $PG(q-1,r)$ is the set whose elements are the 1-dimensional subspaces of F^r). Define a q-ary Hamming code by a parity-check matrix constructed in the following way: From each element in $PG(q-1,r)$, choose the representatives whose leading nonzero entry is 1. There are 2^r-1 points in which

$R(r,m)$	k	$n-k$	t	$0 \leq \rho \leq t-1$
$0,5$	1	31	1	a
$1,5$	6	26	6	$0 \leq \rho \leq 5$
$2,5$	16	16	16	$0 \leq \rho \leq 15$
$3,5$	26	6	6	$0 \leq \rho \leq 5$
$4,5$	31	1	1	a
$5,5$	32	0	0	a

Table 3.1: $RM(r,5)$

$(1,..\rho+1)$	(1)	$(1,2)$	$(1,2,3)$	$(1,2,3,4)$	$(1,2,3,4,5)$	$(1,2,3,4,5,6)$
$2^{6-\rho}$	64	32	16	8	4	2

Table 3.2: $|RM(1,5) \cap \rho(RM(1,5))|$

all its components are 0 and 1. They are the numbers $1, 2, 3, \ldots, 2^r - 1$ written in binary, then, place these columns in increasing order from 1 to $2^r - 1$. The rest of the columns can be placed in any order.

The intersection problem for binary Hamming codes was solved in [22] and for q-ary Hamming codes, in [11].

Theorem 3.5. [11] *For each $m \geq 3$, there exist two linear q-ary Hamming codes $\mathcal{H}_1$, $\mathcal{H}_2$ of length $N = \frac{q^m-1}{q-1}$, such that $\eta(\mathcal{H}_1, \mathcal{H}_2) = q^{N-l}$, for $l = m+1, m+2, \ldots, 2m$.*

3.3 Intersection problem for perfect codes

Let $\mathbf{x} \in F$, the *sphere* of radius r centered at $\mathbf{x}$ is defined by $S_r(\mathbf{x}) = \{\mathbf{y} \in F^n \mid d(\mathbf{x}, \mathbf{y}) \leq r\}$. Given a set $S \in F^n$, the *hull* of S, denoted by $K(S)$, is defined by $\bigcup_{\mathbf{x} \in S} S_r(\mathbf{x})$. If in addition the spheres are disjoint, we say that S *perfectly covers* $K(S)$ or that S is an r-*error-correcting* code. Given a set S which is an r-*error correcting* code, we say that it is an r-*perfect code* provided $K(S) = F$. In [7] it is shown that the only parameters for nontrivial perfect codes are the two Golay codes and the q-ary 1-perfect codes where q is a prime or prime power. So, from now on, q-ary 1-perfect codes will be refereed as q-ary perfect codes.

Let C be a Hamming code of length n and $\mathbf{x} \in F^n$, then the coset $C + \mathbf{x}$ is a perfect code, but not linear. In 1962, [18] Vasil'ev constructed nonlinear binary perfect codes that are not cosets of Hamming codes.

For $\mathbf{x} \in F_2^n$, let $p(\mathbf{x}) = wt(\mathbf{x}) \pmod 2$. Let C_n be a perfect binary code of length $n = 2^m - 1$. Let $f : C_n \to \{0, 1\}$ be an arbitrary mapping.

Theorem 3.6. [18] *The code* $C_{(2n+1,f)} = \{(\mathbf{x}|\mathbf{x}+\mathbf{c}|p(\mathbf{v})+f(\mathbf{c}) : \mathbf{x} \in F_2^n, \mathbf{c} \in C_n\}$ *is perfect. If* $f \equiv 0$, *then* $C_{(2n+1,f)}$ *is the Hamming code, but if* $f(\mathbf{0}) = 0$ *and* $f(\mathbf{c}_1)+f(\mathbf{c}_2) \neq f(\mathbf{c}_1+\mathbf{c}_2)$ *for some* $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_1 + \mathbf{c}_2$, *then* $C_{(2n+1,f)}$ *is not linear.*

As in the case of cosets of Hamming codes, any binary perfect code C of length n generates a partition of F_2^n into translates $C_i = C + \mathbf{x}_i$, where $\mathbf{x}_i$ is a vector of weight 1, and $|C| = |C_i|$ for all $i = 1, 2, \ldots, n$. This partition is known as the trivial partition. There are non-trivial partitions into perfect codes of F_2^n, see for example ([19], [21]).

The following construction of perfect codes of length $2n+1$ from perfect codes of length n is due to Phelps [19] and Solov'eva [20]. Etzion and Vardy [22] refer to their finding as construction A and describes it in the next theorem.

Theorem 3.7. CONSTRUCTION A *Let* E_2^n *denote the set of all the even-weight vectors in* F_2^n. *Let* $C_0, C_1 \ldots, C_n$ *and* C_0^*, $C_1^* \ldots, C_n^*$ *be partitions of* F_2^n *and* E_2^{n+1}, *into a perfect code and its translates, respectively, into an extended perfect code and its translates. Let* π *be a permutation on the set* $\{0, 1, \ldots, n\}$. *Then the code*

$C_A = \{(\mathbf{x}|\mathbf{y}) : \mathbf{x} \in C_i, \mathbf{y} \in C^*_{\pi(i)}$, *for some* $i = 0, \ldots, n\}$, *where* $(\cdot|\cdot)$, *denotes concatenation, is a perfect code of length* $2^{m+1} - 1$.

Let us discuss the intersection problem for two binary perfect codes C_1 and C_2 of the same length $n = 2^m - 1$. If $\mathbf{c} \in C_1 \cap C_2$, then its complement is also in the intersection. Thus the intersection must have even cardinality, and $\eta(C_1, C_2) \geq 2$. Etzion and Vardy [13], determined an upper bound for that intersection, which is $\eta(C_1, C_2) \leq 2^{n-m} - 2^v$, where $v = (n-1)/2$. Moreover, they constructed two perfect codes C_1 and C_2 whose intersection number shows that this upper bound is attainable for all n. The idea of the construction of

these codes is as follows. Let $\mathcal{H}_n$ a Hamming code of length $n = 2v + 1 = 2^m - 1$. Assume that the columns of its generator matrix, $H, -h_1, h_2, \ldots, h_n$, are arranged such that for some fixed column vector $z = h_n$, $h_1 + h_{i+v} = z$ for all $i = 1, 2 \ldots, v$. The code C_1 is the coset of $\mathcal{H}_n$ such that the syndrome $s(\mathbf{c}) = H\mathbf{c}^t$ is z for all $\mathbf{c} \in C_1$. Next, they obtained C_2 by modifying C_1 in the following way $C_2 = (C_1 \setminus \mathcal{B}) \cup \mathcal{A}$, where $\mathcal{A} = \{\mathbf{x}|\mathbf{x}|p(\mathbf{x}) : \mathbf{x} \in F_2^{\mathbf{v}}\}$ and $\mathcal{B} = \mathcal{A} + \mathbf{e}_{2v+1}$. Notice, that according Theorem $\mathcal{A}$ is a Hamming code of length n given by Vasil'ev construction. Now, $\eta(C_1, C_2) = 2^{n-m} - 2^v$.

In [22], Etzion and Vardy, using a combination of construction A and the construction of Vasil'ev, obtained two perfect codes with intersection number equal 2. Thus the spectrum of intersection numbers, for any two binary perfect codes of the same length, is given by the following interval

$$0 \leq \eta(C_1, C_2) \leq 2^{n-m} - 2^v \tag{3.1}$$

The following two theorems give intersection numbers in the interval (3.1), but the results do not cover the entire possible spectrum.

Theorem 3.8. [9] *For any two integers k_1 and k_2 satisfying $1 \leq k_i \leq 2^{(n+1)/2 - log(n+1)}$, $i = 1, 2$, there exist perfect codes C_1 and C_2 both of length $n = 2^m - 1$, $m \geq 4$, with intersection number $\eta(C_1, C_2) = 2k_1k_2$.*

Theorem 3.9. [9] *For any even integer q in the interval $0 \leq q \leq 2^{(n+1)/2 - log(n+1)}$, there are two perfect codes C_1 and C_2 both of length $n = 2^m - 1$, $m \geq 4$, such that $\eta(C_1, C_2) = q$.*

3.4 Intersection problem for Hadamard Codes

A *Hadamard matrix* H of order n is an $n \times n$ matrix of $+1$'s and -1's such that $HH^{\perp} = nI$, where I is the $n \times n$ identity matrix. It is known that if a Hadamard matrix of order n exist, then n is 1,2, or a multiple of 4 [7]. Two Hadamard matrices are *equivalent* if one can be obtained from the other by permuting rows and/or columns and multiplying rows

and columns by -1. The equivalent *normalized* matrix H' is gotten from H by multiplying each row and column by ± 1, to make the entries of the first row and column all $+1$. The binary matrix $c(H')$ is obtained from H' by replacing each entry equal to 1 with 0 and each entry equal to -1 with 1. We can consider the rows of this matrix as binary vectors of length n. The binary $(n, 2n, n/2)$-code consisting of the rows of $c(H')$ and their complements is called a (binary) *Hadamard* code.

In order to get new Hadamard matrices it is useful to introduce the *Kronecker product*: If A is a matrix of order $m \times n$ and B is a matrix of order $r \times s$, then $A \otimes B$ denotes the $nr \times ms$ matrix

$$\begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & an2B & \dots & a_{nm}B \end{pmatrix}.$$

If H_1 and H_2 are Hadamard matrices of orders n_1, n_2 respectively, it easy to check that $H_1 \otimes H_2$ is a Hadamard matrix. In particular taking the Hadamard matrix $S = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and starting from a Hadamard Matrix $S_0 = (1)$, we obtain by successive Kronecker products $S_t = S_{t-1} \otimes S$, a Hadamard matrix of order 2^t for any $t \geq 0$. S_t is called a *Sylvester type* Hadamard matrix. It is known that the binary code obtained from S_t is the dual of the extended Hamming code.

The next four matrices are examples of Hadamard matrices of order 1, 2, 4 and 8, respectively. Each one of the matrices with order 1, 2 and 4 leads to an unique binary Hadamard code. The matrix of order 8 leads to an unique Hadamard code up to equivalence.

$$[1], \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}.$$

The spectrum for the intersection numbers is with respect to the length of a Hadamard code. Due to the fact that a Hadamard code contains each codeword and its complement, the numbers in the spectrum are even. Thus, for length 8, the only Hadamard code is the linear code and the intersection problem is settled for this length. The intersection numbers are $I(8) = \{0, 2, 4, 8, 16\}$. Nonlinear binary Hadamard codes appears beginning at length $n \geq 16$.

Using Hadamard codes from matrices constructed by the product $S \bigotimes [B'_1, B'_2] = \begin{pmatrix} B'_1 & B'_1 \\ B'_2 & -B'_2 \end{pmatrix}$ or its transpose, the next theorem settled the problem for the length 2^t

Theorem 3.10. [14] *For all $t \geq 3$ there exist Hadamard codes of length 2^t with intersection number i if and only if $i \in I(2^t) = \{0, 2, 4, \ldots, 2^{t+1} - 12, 2^{t+1} - 8, 2^{t+1}\}$.*

the next theorem gives a partial answer to the general case, that is, when a Hadamard matrix of lenth $4s$, where s is an odd number, exists.

Theorem 3.11. [9] *For all $t \geq 4$, if there exists a Hadamard matrix of order $4s$, there exists Hadamard codes of length $2^{t+2}s$ with intersection number $2i$ for all $2i \in \{0, 2, 4, \ldots, 2^{t+3}s - 12, 2^{t+3}s - 8, 2^{t+3}\} = I(2^{t+2}s)$.*

3.5 Intersection problem for Quaternary linear codes

The intersection problem for quaternary linear codes has been solved for quaternary extended linear perfect codes [15] and for quaternary linear Hadamard codes [23].

The characterization of the extended 1-perfect $\mathbb{Z}_4$-linear codes, up to equivalence, is given in [16], so we know that for each length, $n = 2^t$, there are exactly $\lfloor t+1/2 \rfloor$ nonequivalent extended 1-perfect $\mathbb{Z}_4$ linear codes. Each one of these codes can be given by a parity-check matrix consisting of all column vectors of the form $\overline{\mathbb{Z}}_2^{\gamma} \times \{1 \in \mathbb{Z}_4\} \times \mathbb{Z}_4^{\delta-1}$, where $t+1 = \gamma + 2\delta$ and $\overline{\mathbb{Z}}_2$ means $\{0,2\} \subset \mathbb{Z}_4$. This parity-check matrix can be seen as the generator matrix for the corresponding $\mathbb{Z}_4$-linear Hadamard code

Theorem 3.12. [16, 17] *For each $\delta \in \{1, \ldots, \lfloor (t+1)/2 \rfloor\}$ there exists a unique (up to isomorphism) extended perfect $\mathbb{Z}_4$-linear code C' of binary length $n+1 = 2^t \geq 16$, such that the $\mathbb{Z}_4$-dual code of C' is of type $(0, \beta; \gamma, \delta)$, where $\beta = 2^{t-1}$ and $\gamma = t+1-2\delta$.*

In view of this Theorem, we can create the following table:

t	δ	$(\alpha, \beta; \gamma, \delta)$
2	1	$(0,2;1,1)$
3	1,2	$(0,4;2,1)$, $(0,4;0,2)$
4	1,2	$(0,8;3,1)$, $(0,8;1,2)$
5	1,2,3	$(0,16;4,1)$, $(0,16;2,2)$, $(0,16;0,3)$
6	1,2,3	$(0,32;5,1)$, $(0,32;3,2)$, $(0,32;1,3)$
$\vdots$	$\vdots$	$\vdots$

Example 3.5.1. *In the case of length $n+1 = 32$, there are three non-isomorphic extended perfect $\mathbb{Z}_4$-linear codes, since we have three possible parameters: $\delta = 1$, $\delta = 2$ and $\delta = 3$. The following matrix is the parity-check matrix of the code $\mathcal{C}' = \Phi^{-1}(C')$ for $\delta = 2$ (also notice that $\beta = 16$ and $\gamma = 2$):*

$$\left(\begin{array}{cccccccccccccccc} 0&0&0&0&0&0&0&0&2&2&2&2&2&2&2&2 \\ 0&0&0&0&2&2&2&2&0&0&0&0&2&2&2&2 \\ \hline 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3 \end{array}\right).$$

Theorem 3.13. *For any $t \geq 3$ and any quaternary linear perfect codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of length $\beta = 2^{t-1}$, not necessary such that their quaternary dual codes contain the all-ones vector, it is true that*

$$2^{2\beta-2t-1} \leq \eta(\mathcal{C}_1, \mathcal{C}_2) \leq 2^{2\beta-t-1}.$$

Moreover, there exist such codes for any possible intersection number between these bounds.

Theorem 3.14. *For any $t \geq 3$ and any two quaternary linear Hadamard codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of length $\beta = 2^{t-1}$, it is true that $2 \leq \eta(\mathcal{C}_1, \mathcal{C}_2) \leq 2^{t+1}$.*

Theorem 3.15. *For any $t \geq 3$ there are two quaternary linear Hadamard codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of length $\beta = 2^{t-1}$, such that $\eta(\mathcal{C}_1, \mathcal{C}_2) = 2^l$, where l is any value from 1 to $t + 1$.*

The quaternary linear codes have been generalized to the $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. The intersection problem for these kind of codes is given in [15] and [23].

Chapter 4

Intersection Problem for The Class of Quaternary Reed-Muller Codes

This chapter presents results that lead to the solution of the intersection problem for $\overline{\mathcal{QRM}}(r,m)$. Remember that this class contains the most important families of quaternary codes such as the quaternary Kerdock-like codes as well the Preparata- like codes. As a consequence, the solution of the intersection problem for binary codes in $\overline{QRM}(r,m)$ is obtained. This class contains the original Kerdock code which is a nonlinear binary code, but it is the Gray map image of a quaternary linear code (a Kerdock-like code).

Our results generalize those given in [10]. This allows to us to attack the intersection problem with the same approach used in [10]. As mentioned in Chapter 3, that approach was based on a partition of the columns of the generator matrix of a $[n,k]$-code over a finite field, into two sets, one of them is a set of k linearly independent columns and the other is a set of $n-k$ columns from which t columns are linearly independent. This partition is given in such a way that t gets its maximum value. In this case, the code is called a t-independence redundance (t-IR) code, and independent redundancy (IR) code if $t=r$.

Remember, α is the $\pmod 2$ map. Now, we introduce another map, $\beta:\{0,2\}\to\mathbb{Z}_2$, which is defined by $\beta(0)=0$, and $\beta(2)=1$. β is an isomorphism of groups and the extension $\beta:\{0,2\}^n\to\mathbb{Z}_2^n$ is also an isomorphism of groups.

Theorem 4.1. [1] *Let $\mathcal{C}$ be a quaternary linear code of type $4^\delta 2^\gamma$ and length n, with generator matrix G given by (1.5). Then, the binary residue code, $\alpha(\mathcal{C})=\{\alpha(\mathbf{c})|\mathbf{c}\in\mathcal{C}\}$ is a binary linear $[n,\delta]$-code with generator matrix*

$$\begin{pmatrix} I_\delta & A & \alpha(B) \end{pmatrix},$$

and the Torsion code, $Tor(\mathcal{C})=\{\beta(\mathbf{c})|\mathbf{c}\in\mathcal{C},\alpha(\mathbf{c})=0\}$ is a binary linear $[n,\delta+\gamma]$-code with generator matrix

$$\begin{pmatrix} I_\delta & A & \alpha(B) \\ 0 & I_\gamma & C \end{pmatrix}.$$

Any quaternary linear code is equivalent to a code whose generator matrix is of form (1.5), with the additional condition that a partition of the columns into two sets, leads to the corresponding generator matrix of the binary residue code and presents a partition of its columns as specified in [10].

Let $\mathcal{C}$ be a quaternary linear code of type $4^\delta 2^\gamma$ and length n, with generator matrix G given by (1.5). Let $\alpha(\mathcal{C}) = C$, and denote by $I(\mathcal{C})$ the set of columns of G whose positions correspond to the columns of $\alpha(G)$ which are in $I(C)$. Similarly, denote by $R(\mathcal{C})$, the set of columns of G, whose positions correspond to the columns of $\alpha(G)$ which are in $R(C)$. We say that $\mathcal{C}$ is called a t-redundancy t-IR code, or redundancy (IR) code, respectively, if C is. In the same way, a set of columns of G is a *free set* if this set leads to a free set in the columns of $\alpha(G)$.

Theorem 4.2. [10] *If C is an $[n, k]$-code and T is a set of linearly independent columns in its generator matrix, $|T| = t$, then in C each t-tuple appears in the columns of T exactly in $|C|/2^t$ codewords.*

Theorem 4.2 is defined for linear codes over finite fields. The next theorem shows a similar result for codes defined over the ring $\mathbb{Z}_4$, which is not a field. This result allows us to adopt the approach from [10].

Theorem 4.3. *Let $\mathcal{C}$ be a quaternary linear code of type $4^\delta 2^\gamma$. Let G be a generator matrix of $\mathcal{C}$ and denote by $\alpha(G)$ the generator matrix of $\alpha(\mathcal{C})$. If T is a set of t linearly independent columns of $\alpha(G)$, then each t-tuple in the corresponding columns of G appears exactly in $\frac{|\mathcal{C}|}{4^t}$ codewords of $\mathcal{C}$*

Proof. Let $\mathcal{C}$ be a quaternary linear code of type $4^\delta 2^\gamma$. By Theorem 4.1 $\alpha(\mathcal{C})$ is a binary-$[n, \delta]$-code with generator matrix $\alpha(G)$, where G is of the form given by (1.5). In addition, since $\alpha : \mathcal{C} \to \alpha(\mathcal{C})$ is a surjective homomorphism, then $\frac{\mathcal{C}}{Ker(\alpha)} \approx \alpha(\mathcal{C})$. Notice that

$2\mathcal{C} \subseteq Ker(\alpha) \subset \mathcal{C}$ and $2\mathcal{C}$ is of type $4^0 2^\delta$ and $Ker(\alpha)$ of type $4^0 2^{\gamma+\delta}$. Moreover, given a codeword $\mathbf{c} \in \mathcal{C}$, then $2\mathcal{C} + \mathbf{c} \subseteq Ker(\alpha) + \mathbf{c}$, each class $Ker(\alpha) + \mathbf{c}$ can be divided by 2^γ classes of $\frac{\mathcal{C}}{2\mathcal{C}}$ each having the same cardinality.

Let $J = \{i_1, i_2, \ldots, i_t\} \subset [n]$ be a set of indices that label a set of t linearly independent columns of $\alpha(G)$. Let $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ be a codeword in $\mathcal{C}$, and $\mathbf{c}|_J = (c_{i_1}, c_{i_2}, \ldots, c_{i_t})$ be the projection of the codeword $\mathbf{c}$ on the set J. Since $\alpha(\mathbf{c}) = \bar{\mathbf{c}} = (\bar{c_1}, \bar{c_2}, \ldots, \bar{c_n}) \in \alpha(\mathcal{C})$, $\alpha(\mathbf{c})$ is associated to a unique class $Ker(\alpha) + \mathbf{c}$. By Theorem 4.2 $(\bar{c_{i_1}}, \bar{c_{i_2}}, \ldots, \bar{c_{i_t}})$ appears in exactly $\frac{2^\delta}{2^t}$ codewords of $\alpha(\mathcal{C})$. Denote these codewords by $\mathbf{d}_i$ where $i = 1, \ldots, \frac{2^\delta}{2^t}$, and they are such that their projection to J is $\mathbf{d}_i|_J = (\bar{c_{i_1}}, \bar{c_{i_2}}, \ldots, \bar{c_{i_t}})$. For some i, $d_i = \alpha(\mathbf{c})$.

Now, notice that $(i_1, \ldots, i_t)$ label t linearly independent columns of the generator matrix of $Tor(\mathcal{C})$. So if $\mathbf{h} \in Tor(\mathcal{C})$, then by Theorem 4.2 $\mathbf{h}|_J = (h_{i_1}, h_{i_2}, \ldots, h_{i_t})$ will appear in $\frac{2^{\delta+\gamma}}{2^t}$ codewords of $Tor(\mathcal{C})$. Since $Tor(\mathcal{C}) = Ker(\alpha)$ and β is an isomorphism, the t-tuple $(2h_{i_1}, 2h_{i_2}, \ldots, 2h_{i_t})$ will appear in $\frac{2^{\delta+\gamma}}{2^t}$ codewords of $Ker(\alpha)$. But $Ker(\alpha)$ is the union of 2^γ classes of $\frac{\mathcal{C}}{2\mathcal{C}}$ that means, given any of such classes it contains $\frac{2^\delta}{2^t}$ codewords whose projection is the t-tuple $(2h_{i_1}, 2h_{i_2}, \ldots, 2h_{i_t})$. In particular this is true for the vector all zeros, $\mathbf{0} = (0, \ldots, 0)$, since $\mathbf{0} \in 2\mathcal{C} \subseteq Ker(\alpha)$. That way, $Ker(\alpha) + \mathbf{c}$ will have 2^γ classes each one having $\frac{2^\delta}{2^t}$ codewords with the same vector projection $\mathbf{c}|_J$. Now repeat the same argument for the remaining $\frac{2^\delta}{2^t} - 1$ d_i codeword of $\mathcal{C}$. They give the same number of codewords with projection $\mathbf{c}|_J$ that was obtained by d_i. That way, the total number is $\frac{2^\delta}{2^t} 2^\gamma \frac{2^\delta}{2^t}$ and this proves the theorem.

□

Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_4^n$ and $J = \{i_1, \ldots, i_j\} \subset [n]$. Let π be a permutation defined on J and ρ_s be an inversion of coordinates with associated subset $S \subseteq J$, and $\rho_s\pi$ a monomial map. Define the function $\varphi_{\rho_s\pi} : \mathbb{Z}_4^n \to \mathbb{Z}_4^n$ as $\varphi_{\rho_s\pi}(\mathbf{h}) = \mathbf{h} - \rho_s(\pi(\mathbf{h}))$. Notice that φ is an homomorphism of groups. When $\mathcal{C} \subseteq \mathbb{Z}_4^n$ is a quaternary linear code, $\varphi_{\rho\pi}$ will be helpful in determining those codewords that are in the intersection of $\mathcal{C}$ and $\rho_s(\pi(\mathcal{C}))$. So, in the following definition we give a special name to the set $\varphi_{\rho_s\pi}(\mathbb{Z}_4^n)$, which reflects this fact.

Definition 4.0.1. *Let $\rho_s\pi$ be a monomial map. The index of $\rho_s\pi$ is the set $X_{\rho_s\pi} = \{\mathbf{x} \in \mathbb{Z}_4^n : \exists \mathbf{h} \in \mathbb{Z}_4^n : \varphi_{\rho_s\pi}(h) = \mathbf{x}\}$. If $\mathbf{x} \in X_{\rho\pi}$, then $\mathbf{x}$ is called the* index *of $\mathbf{h}$, with respect $\rho\pi$, and we will write $\mathbf{x} = \mathbf{h}_{\rho\pi}$, and we say that $\mathbf{h}$ is attached to the index $\mathbf{x}$.*

Remark 4.0.1. *Let $\mathbf{h} = (h_1, h_2, ..., h_n) \in \mathbb{Z}_4^n$. Let's examine the index of $\mathbf{h}$ projected on the coordinates determinated by a cycle θ of the permutation π, and the inversion of coordinates ρ. Without loss of generality, we can assume that $\theta = (1, 2 \ldots, \ell)$.*

The projection of $\mathbf{h}$ to the coordinates labeled by θ is given by $\mathbf{h}|_\theta = (h_1, \ldots, h_\ell)$, and $\rho(\mathbf{h}|_\theta) = (\pm h_1, \ldots, \pm h_\ell)$, where we choose $(-)$ if ρ multiplies the corresponding coordinate by -1. In other words, by doing a selection of signs in the components of $\mathbf{h}|_\theta$, we are determining implicitly the set S associated to ρ_s. Thus, we have $\theta(\rho(\mathbf{h}|_\theta)) = (\pm h_2, \ldots, \pm h_\ell, \pm h_1)$ and $x|_\theta = \mathbf{h}|_\theta - \theta(\rho(\mathbf{h}|_\theta)) = (x_1, \ldots, x_\ell)$ where:

$$\begin{aligned} x_2 &= h_1 \pm h_2 \\ x_3 &= h_2 \pm h_3 \\ \vdots &= \vdots \quad \vdots \quad \vdots \\ x_\ell &= h_{\ell-1} \pm h_\ell \\ x_1 &= h_\ell \pm h_1. \end{aligned} \tag{4.1}$$

Theorem 4.4. *Let $\rho_s\pi$ a monomial map as in the remark, then $\mathbf{x} \in X_{\rho_s\pi}$ if and only if*

1. *For every cycle $(1, \ldots, \ell)$ in π, the vector $\mathbf{x}|_\theta = (x_1, \ldots, x_\ell)$, satisfies $\sum_{i=1}^{\ell} x_i = 0 \pmod 2$*

2. *For every $s \in [n]$ which is not a label of a coordinate of $\mathbf{x}|_\theta$, $\mathbf{x}_s = 0$.*

Proof. 1. If $\mathbf{x} \in X_{\pi\rho}$, then there exists $\mathbf{h} \in \mathbb{Z}_4^n$ such that $\mathbf{h} - \pi\rho(\mathbf{h}) = \mathbf{x}$. Let $\theta = (v_{p,1}^\ell, v_{p,2}^\ell \ldots v_{p,\ell}^\ell)$ be a cycle of π. Then, all possible cases for ρ with respect to $\mathbf{h}|_\theta = (h_1, h_2, ..., h_j, ..., h_\ell)$, are given, by (4.1) and the projection $\mathbf{x}|_\theta$ satisfies the following

relation

$$\sum_{i=1}^{\ell} x_i = \sum_{i=1}^{\ell-1}(h_i \pm h_{i+1}) + h_\ell \pm h_1 = \sum_{i=1}^{\ell} h_i \pm \sum_{i=1}^{\ell} h_i = 0 \pmod 2$$

2. This follows directly by definition 4.0.1.

Conversely, assume that there exist a vector $\mathbf{x} \in \mathbb{Z}_4^n$ that satisfies 1) and 2). We are going to show that there is a vector $\mathbf{h} \in \mathbb{Z}_4^n$ such that $\mathbf{x} = \mathbf{h}_{\rho(\pi)}$. Following [10], the values of h_s for s satisfying condition 2) may be chosen arbitrarily. For a cycle $\theta = (1, 2, \ldots, \ell)$, in π, select an arbitrary value for h_1. Notice that if ρ multiply by -1 the first coordinate, then we had chosen $-h_1$. As we did before, we are going to use the notation $\pm h_1$ to express this fact. Now, proceed by the formula

$$\forall j,\ \ 2 \leq j \leq \ell, \quad \pm h_j = \pm h_{j-1} - x_j.$$

Since, $\sum_{i=1}^{\ell} x_i = 0 \pmod 2$, it follows that $\pm h_1 = \pm h_\ell - x_\ell$.

From these formulae we have that for all i, $1 \leq i \leq n$, $x_i = h_i - h_{\rho\pi(i)}$, or by definition of index set, $\mathbf{x} = \mathbf{h}_{\rho\pi(i)}$.

□

Lemma 4.0.1. *1. Let $\mathbf{h} \in \mathbb{Z}_4^n$. If ρ is an inversion of an odd number of coordinates in a cycle θ of π, then the initial choice of h_1 in $\mathbf{h}|\theta$ is restricted to two elements in the set $\{0, 1, 2, 3\}$.*

2. If ρ is an inversion of an even number of coordinates in a cycle θ of π, then initial choice of h_1 in $\mathbf{h}|\theta$ can be made in four ways from the set $\{0, 1, 2, 3\}$.

Proof. Let $\mathbf{h} = (h_1, h_2, \ldots, h_n)$ be a word in $\mathbb{Z}_4^n$, $\pi \in S_n$ and $\theta = (1, \ldots, \ell)$, a cycle of length ℓ in the decomposition of π, and take a subset $S = \{i_1, \ldots, i_k\}$ of $[\ell]$ where $k \leq \ell$. Consider $\mathbf{x}|_\theta = \mathbf{h}|_\theta - \rho(\theta(\mathbf{h}|_\theta))$, where $\rho = \rho_s$. By Theorem 4.4, $\sum_{i=1}^{\ell} x_i = 0 \pmod 2$. Assume that $\mathbf{x} = \mathbf{h}_{\rho(\theta)} = \mathbf{0}$, then $\sum_{i=1}^{\ell} x_i = 0 \pmod 4$. From the system (4.1), we get:

$\sum_{i=1}^{\ell} x_i = \sum_{i\in[\ell]\setminus S} x_i + \sum_{i\in S} x_i = 2h_{i_1} + \cdots + 2h_{i_k} = \pm 2h_1 + \cdots \pm 2h_1 = 0$. Now it is easy to see that if k is odd, $h_1 \in \{0, 2\}$ and if k is even, $h_1 \in \{0, 1, 2, 3\}$. Moreover, if k is odd and $h_1 = 0$ then, $\mathbf{h}|_\theta = (\underbrace{0, \ldots, 0}_{\ell\, times})$, but if $h_1 = 2$, then $\mathbf{h}|_\theta = (\underbrace{2, \ldots, 2}_{\ell\, times})$. If k is even and either $h_1 = 0$ or 2, $\mathbf{h}|_\theta$ is exactly as in the previous case. Now if $h_1 = 1$, then $\mathbf{h}|_\theta = (\underbrace{1, 3, \ldots, 3, 1}_{\ell\, times})$ but if $h_1 = 3$, then $\mathbf{h}|_\theta = (\underbrace{3, 1, \ldots, 1, 3}_{\ell\, times})$

Since $\varphi_{\rho_s\theta}$ is a surjective homomorphism from $\mathbb{Z}_4^n$ to $\varphi_{\rho_s\theta}(\mathbb{Z}_4^n)$, it is true that $\frac{\mathbb{Z}_4^n}{Ker(\varphi_{\rho_s\theta})} \approx \varphi_{\rho_s\theta}(\mathbb{Z}_4^n)$. Thus, to each index we can associate a unique equivalence class in $\frac{\mathbb{Z}_4^n}{Ker(\varphi_{\rho_s\theta})}$. Notice that $Ker(\varphi_{\rho_s\theta})$ is the set of vectors attached to the index zero. Now, assume that $\mathbf{x} = \mathbf{h}_{\rho\theta} \neq \mathbf{0}$, then its associated class is $Ker(\varphi_{\rho_s\theta}) + \mathbf{h}$. For all $\mathbf{u} \in Ker(\varphi_{\rho_s\theta}) + \mathbf{h}$, consider the following two cases, if ρ_s inverts an odd number of coordinates, then $\mathbf{u}|_\theta = (h_1, h_2, \ldots, h_\ell)$ or $\mathbf{u}|_\theta = (h_1 + 2, h_2 + 2, \ldots, h_\ell + 2)$. For the set of vectors attached to the index $\mathbf{x} = \mathbf{h}_{\rho(\theta)}$, the initial choice of h_1 can be done only in two ways. Now, assume that ρ_s performs an even number of coordinates. In this case, if $h_1 = 0$ or $h_1 = 2$, $\mathbf{u}|_\theta$ is like the previous case. If $h_1 = 1$, then $\mathbf{u}|_\theta = (h_1 + 1, h_2 + 3, \ldots, h_{\ell-1} + 1, h_\ell + 3)$, but if $h_1 = 3$ then $\mathbf{u}|_\theta = (h_1 + 3, h_2 + 1, \ldots, h_{\ell-1} + 3, h_\ell + 1)$. Thus, in this case, also we can choose h_1 in four ways.

□

Lemma 4.0.2. *If $\mathcal{C}$ is quaternary linear code of type $4^\delta 2^\gamma$, and $\rho\pi$ is a monomial map, then $\rho(\pi(\mathbf{h})) \in \mathcal{C} \cap \rho(\pi(\mathcal{C}))$ if and only if $\mathbf{h}_{\rho\pi} \in \mathcal{C}$.*

Proof. $\mathbf{h} - \rho(\pi(\mathbf{h})) \in \mathcal{C}$ if and only if $\rho(\pi(\mathbf{h})) \in \mathcal{C}$ if and only if $\rho(\pi(\mathbf{h})) \in \mathcal{C} \cap \rho(\pi(\mathcal{C}))$ □

Lemma 4.0.3. *Let $\mathcal{C}$ be a quaternary linear code of type $4^\delta 2^\gamma$, and $\mathcal{D}$ be an equivalent code to $\mathcal{C}$. If $\rho\pi$ is a monomial map, then $\eta(\mathcal{C}, \rho(\pi(\mathcal{C}))) = \eta(\mathcal{D}, \rho(\pi(\mathcal{D})))$ and both intersections are of the same type.*

Proof. Since $\mathcal{C}$ and $\mathcal{D}$ are equivalent, they are isomorphic as abelian groups. Then, they are of the same type. Since, $\mathcal{C} \cap \rho(\pi(\mathcal{C}))$ and $\mathcal{D} \cap \rho(\pi(\mathcal{D}))$ are subgroups of $\mathcal{C}$, and $\mathcal{D}$,

respectively, the image of restriction of the isomorphism to $\mathcal{C} \cap \rho(\pi(\mathcal{C}))$ is $\mathcal{D} \cap \rho(\pi(\mathcal{D}))$. Thus, the conclusion of the lemma follows. □

Lemma 4.0.4. *Let $\mathcal{C}$ be a quaternary linear code of type $4^\delta 2^\gamma$,*

1. *Let $\rho\pi$ be a monomial map, $\delta > 0$, $\mathbf{1} \in \mathcal{C}$, then $\eta(\mathcal{C}, \rho(\pi(\mathcal{C}))) \geq 2$*
2. *Let π be a permutation, $\delta = 0$, $\gamma > 0$, $\mathbf{2} \in \mathcal{C}$, $\eta(\mathcal{C}, \rho(\pi(\mathcal{C}))) \geq 2$.*

Proof. 1. If $\mathbf{1} \in \mathcal{C}$, then $\mathbf{1} \in \pi(\mathcal{C})$ and the intersection has at least 4 elements. Now, $\rho(\pi(\mathcal{C}))$ leave invariant codewords of order 2. So the intersection at least is 2.

2. If $\mathbf{2} \in \mathcal{C}$, then $\mathbf{2} \in \pi(\mathcal{C})$ and the intersection has at least 2 elements.

□

Theorem 4.5. *Let $\mathcal{C}$ a quaternary linear code of type $4^\delta 2^\gamma$. Assume that $\mathcal{C} = \mathcal{C}_1 \bigoplus \mathcal{C}_2$, where $\mathcal{C}_1$ is of type $4^\delta 2^0$, $\mathcal{C}_2$ is of type $4^0 2^\gamma$ and $\bigoplus$ represents the direct sum. Assume that $\mathcal{C} \cap \rho(\pi(\mathcal{C}))$ is of type $4^{\delta_1} 2^{\gamma_1}$, where $1 \leq \delta_1 < \delta$, $1 \leq \gamma_1 < \gamma$, and $\rho\pi$ is a monomial map. Then, $\mathcal{C}_1 \cap \rho(\pi(\mathcal{C}_1))$ is of type $4^{\delta_1} 2^0$, $\mathcal{C}_2 \cap \rho(\pi(\mathcal{C}_2))$ is of type $4^0 2^{\gamma_1}$ and $\mathcal{C} \cap \rho(\pi(\mathcal{C})) = \mathcal{C}_1 \cap \rho(\pi(\mathcal{C}_1)) \bigoplus \mathcal{C}_2 \cap \rho(\pi(\mathcal{C}_2))$.*

For a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_4^n$, the *generalized parity* of x, $gp(\mathbf{x})$, is defined as $gp(\mathbf{x}) = \sum_{i=1}^n x_i \pmod 2$. Let $\mathcal{C}$ be a a quaternary linear code of type $4^\delta 2^\gamma$. Let G be a generator matrix given by 1.5. Let π a permutation of columns of a free set of G, and let S be a set of labels of columns of a free set of G, then, $\rho(\pi)$ is called a *free monomial map.*

Theorem 4.6. *Let $\mathcal{C}$ be a t-IR quaternary linear code of type $4^\delta 2^\gamma$.*

1. *Let π be a free permutation with respect to $\mathcal{C}$. Then, every word is attached to one index only, and every index $\mathbf{x} \in \mathcal{C} \cap X_\pi$ has exactly $2^\gamma 4^{\delta - \lambda(\pi) + \tau(\pi)}$ codewords attached to it and $\eta(\mathcal{C}, \pi(\mathcal{C})) = |\mathcal{C} \cap X_\pi| 2^\gamma 4^{\delta - \lambda(\pi) + \tau(\pi)}$.*
2. *Let $\rho\pi$ a free monomial map with respect to $\mathcal{C}$. Then, every word is attached to one index only, and each index in $\mathcal{C} \cap X_{\rho\pi}$ has exactly $2^{\tau(\pi)^o} \cdot 4^{\tau(\pi)^e} \cdot 4^{\delta - \lambda(\pi)}$ codewords attached to it and $\eta(\mathcal{C}, \rho(\pi(\mathcal{C}))) = |\mathcal{C} \cap X_{\pi\rho}| 2^{\tau(\pi)^o} \cdot 4^{\tau(\pi)^e} \cdot 4^{\delta - \lambda(\pi)}$*

Proof. 1. Let $\mathbf{x} \in X_\pi \cap \mathcal{C}$. Then there exists $\mathbf{h} \in \mathcal{C}$ such that $\mathbf{h} - \pi(\mathbf{h}) = \mathbf{x}$. Let θ be a cyclic in π. For any choice of h_1, the vector projection $\mathbf{h}|_\theta$ is uniquely determined. Since $h_1 \in \{0, 1, 2, 3\}$, we have four different $\mathbf{h}|_\theta$ vectors. Since θ was taken arbitrarily in π, it follows that the number of different vectors $\mathbf{h}|_\pi$ each one of length $\lambda(\theta)$ is $4^{\tau(\pi)}$, By Theorem 4.3, there are $\frac{2^\gamma 4^\delta}{4^{\lambda(\pi)}}$ codeword in $\mathcal{C}$, for each $\mathbf{h}|\pi$. So there are attached to $\mathbf{x}$, $4^{\tau(\pi)} \cdot \frac{2^\gamma 4^\delta}{4^{\lambda(\pi)}} = 4^{\delta+\tau(\pi)-\lambda(\pi)}$ codewords. Since any index in X_π has exactly the same number of attached codewords, it follows that $\eta(\mathcal{C}, \pi(\mathcal{C})) = |\mathcal{C} \cap X_\pi| 2^\gamma 4^{\delta-\lambda(\pi)+\tau(\pi)}$.

2. Let θ be a cycle of length ℓ in the decomposition of the free permutation π. Consider the vector $\mathbf{h}$ and its projection $\mathbf{h}|_\theta$. Let ρ be a map which produce an inversion on an odd number of coordinates of $\mathbf{h}|_\theta$. Assume that $\mathbf{h}$ is attached to the index $\mathbf{0}$. By lemma 4.0.1, for each initial choice of h_1, $\mathbf{h}|_\theta$ is uniquely determined, but we have only two choices possible: 0 and 2. Thus there exist only two different vectors $\mathbf{h}|_\theta$. Let $\tau(\pi)^o$ be the number of cycles which corresponding projections present an odd number of coordinates with inversions. So, we have $2^{\tau(\pi)^o}$ distinct projections of $\mathbf{h}$ on those cycles. Moreover, if π had cycles with an even number of inversions (including cycles without inversions), by lemma 4.0.1 we will have $4^{\tau(\pi)^e}$ different projections of $\mathbf{h}$ on those cycles, where $\tau(\pi)^e$ denotes the number of cycles of π in which is realized an even number of inversions. In this way we have $2^{\tau(\pi)^o} 4^{\tau(\pi)^e}$ different codewords each one with $\lambda(\pi)$ coordinates. Since π is a free permutation, it follows that for each $\mathbf{h}|\pi$, there are $\frac{2^\gamma 4^\delta}{4^{\lambda(\pi)}}$ codewords. Thus, the index $\mathbf{0}$ has $2^{\tau(\pi)^o} 4^{\tau(\pi)^e} \cdot 4^{\delta-\lambda(\pi)}$codewords attached to it. Since any index in $X_{\rho\pi}$ has exactly the same number of attached words, it follows that $\eta(\mathcal{C}, \rho(\pi(\mathcal{C}))) = |\mathcal{C} \cap X_{\pi\rho}| 2^{\tau(\pi)^o} \cdot 4^{\tau(\pi)^e} \cdot 2^\gamma \cdot 4^{\delta-\lambda(\pi)}$.

□

Theorem 4.7. *Let $\mathcal{C}$ be a quaternary linear t-IR code of type $4^\delta 2^0$. There exists a subset $A \subset \{0, 1, 2, \ldots, t-1\} \times \{0, 1, 2, \ldots, t\}$ such that for all $(\ell, j) \in A$ there is a permutation π*

and a set S_j associated to a monomial map ρ_{s_j} such that

$$\eta(\mathcal{C}, \rho_{s_j}(\pi(\mathcal{C}))) = \begin{cases} 4^{\delta-\ell}, & \text{if } 1 \leq \ell \leq t-1,\ j = 0; \\ 2^1 4^{\delta-\ell-1}, & \text{if } 1 \leq \ell \leq t-1,\ j = 1; \\ 2^{j-\ell-1} 4^{\delta-(j-1)}, & \text{if } \ell \text{ is odd, } \ell+1 < j \leq t; \\ 2^{j-\ell} 4^{\delta-j}, & \text{if } \ell \text{ is even, } \ell+1 < j \leq t; \\ 2^j 4^{\delta-j}, & \text{if } \ell = 0,\ j \in \{0, 1, ..., t\}. \end{cases}$$

Proof. Let $\mathcal{C}$ be a quaternary linear t-IR code of length n, and type $4^\delta 2^0$. Let G be a generator matrix with the columns of $R(\mathcal{C})$ placed first, followed by the δ columns of the information set $I(\mathcal{C})$. Let $1 < \ell \leq t-1$. In order to define the permutation π and the set S associated to ρ_s, we distinguish two cases **a)** $0 \leq j \leq \ell+1$ and **b)** $\ell+1 < j \leq t-1$. Let's us discuss each case separately.

a) $0 \leq j \leq \ell+1$. Define $\pi = (1, 2 \ldots, \ell+1)$ a permutation consisting of one cycle, and for $j = 0$, define $S_0 = \{0\}$, and $\rho_{s_o} = Id$. So $\tau(\pi) = 1$, $\lambda(\pi) = \ell+1$ and by Theorem 4.6, $\eta(\mathcal{C}, \pi(\mathcal{C})) = 4^{\delta-\ell}$.

For $j = 1$, define $S_1 = \{1\}$, then $\tau(\pi)^o = 1$, $\tau(\pi)^e = 0$, $\lambda(\pi) = \ell+1$. Thus, $\eta(\mathcal{C}, \rho_{s_1}(\pi(\mathcal{C}))) = 2^1 4^{\delta-\ell-1}$. Notice that the first new intersection number appears at $j = 1$. For $j > 1$, the intersection numbers are alternating between $2^1 4^{\delta-\ell-1}$ and $4^{\delta-\ell}$.

b) $\ell+1 < j \leq t$. If ℓ is odd, new intersection numbers appears when $j \geq \ell+3$, so we require $\ell+3 \leq n-\delta$. Consider the permutation $\pi_j = (1, 2, \ldots, \ell+1)(\ell+2)\Pi_{s=\ell+3}^{j}(s)$, where $S_j = \{1, \ldots, j\}$ is the set associated to the monomial map ρ_{s_j}. Thus, $\tau(\pi_j)^o = j-\ell-1$, $\tau(\pi_j)^e = 1$, $\lambda(\pi_j) = j$. Thus, $\eta(\mathcal{C}, \rho_{s_j}(\pi(\mathcal{C}))) = |\mathcal{C} \cap X_{\rho_s \pi_j}| 2^{j-1} 4^{\delta-j-1}$.

If ℓ is even, the new intersection numbers appears when $j \leq \ell+2$, so we require $\ell+2 < n-\delta$. Consider the permutation $\pi_j = (1, 2, \ldots, \ell+1)\Pi_{s=\ell+2}^{j}(s)$, where $S_j = \{1, \ldots, j\}$ is the set associated to the monomial map ρ_{s_j}. Thus, $\tau(\pi_j)^o = j-\ell-1+1 = j-\ell$, $\tau(\pi_j)^e = 0$, $\lambda(\pi_j) = j$. Thus, $\eta(\mathcal{C}, \rho_{s_j}(\pi(\mathcal{C}))) = |\mathcal{C} \cap X_{\rho_s \pi_j}| 4^{\delta-j} 2^{j-\ell}$.

Now, considering each element in the set $S_j = \{1, \ldots, j\}$, $1 \leq j \leq t-1$, as a permutation consisting of a cycle of length 1, one can write $\pi = (1) \ldots, (j)$. Thus, there are, j

cycles of length 1. This implies $\tau(\pi)^o = j$, $\tau(\pi)^e = 0$, $\lambda(\pi) = j$. Thus, by Theorem 4.6 $\eta(\mathcal{C}, \rho_{s_j}(\pi(\mathcal{C}))) = |\mathcal{C} \cap X_{\rho_{s_j}\pi}|2^j 4^{\delta-j}$.

Now we are going to prove that for each one of these cases, $\mathcal{C} \cap X_{\rho\pi} = \{\mathbf{0}\}$. That is, the vector of all zeros is the unique codeword that is also an index. Let $\mathbf{c} \in \mathcal{C} \cap X_{\rho\pi}$ which in terms of its components can be written as $\mathbf{c} = (b_1, \ldots, b_{n-\delta-1}, a_1, \ldots, a_\delta)$, where b_i denotes the parity-check symbols or the labels of the columns of R(C), and a_i are the information symbols or the labels of the columns of I(C). Also, $a_i = b_{n-\delta+1}$, $i \in \{1, \ldots, \delta\}$. By definition of the index set, $a_1 = \ldots = a_\delta = 0$. Since $b_i = \sum_{j=1}^{\delta} c_{ij}a_j$, $a_j \in \mathbb{Z}_4$, it follows that $b_i = 0$, for all $i \in \{1, \ldots, n-\delta\}$. Thus $\mathbf{c} = \mathbf{0}$. □

Example 4.0.2. *Let $\mathcal{C}$ a quaternary linear code of type $4^6 2^0$ whose generator matrix is given by*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 3 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 3 & 0 & 3 & 3 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 3 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 3 & 3 & 1 & 1 & 2 & 0 \end{pmatrix}$$

Since the dimension of $\alpha(G)$ $\delta = 6$, $I(\mathcal{C})$ is the set of columns 1,2,3,4,5,6. $R(\mathcal{C})$ is the set of columns 7,8,9,10,11,12. Notice that in this set, all the columns are linearly independent. Thus $t = \delta = 6$. Now A is subset of $\{0, 1, \ldots, 5\} \times \{0, 1, \ldots, 6\}$. In order to get the monomial maps, we proceed as in the theorem, placing the columns of $R(\mathcal{C})$ first, and second the columns of $I(\mathcal{C})$.

a *$1 \leq \ell \leq 5$, $0 \leq j \leq \ell + 1$. If $j = 0$, we have the following table:*

(ℓ, j)	$(1, \ldots, \ell+1)$	S_j	$4^{6-\ell}$
$(1,0)$	$(1,2)$	$\{0\}$	4^5
$(2,0)$	$(1,2,3)$	$\{0\}$	4^4
$(3,0)$	$(1,2,3,4)$	$\{0,\}$	4^3
$(4,0)$	$(1,2,3,4,5)$	$\{0\}$	4^2
$(5,0)$	$(1,2,3,4,5,6)$	$\{0\}$	4^1

If $j = 1$, we have the following table

(ℓ, j)	$(1, \ldots, \ell+1)$	S_1	$2^1 4^{6-\ell-1}$
$(1,1)$	$(1,2)$	$\{1\}$	$2^1 4^4$
$(2,1)$	$(1,2,3)$	$\{1\}$	$2^1 4^3$
$(3,1)$	$(1,2,3,4)$	$\{1\}$	$2^1 4^2$
$(4,1)$	$(1,2,3,4,5)$	$\{1\}$	24^1
$(5,1)$	$(1,2,3,4,5,6)$	$\{1\}$	$2^1 4^0$

b *$1 \leq \ell \leq 5$, ℓ odd, $\ell + 1 \leq j \leq 6$. New intersection numbers appears when $j \geq \ell + 3$. Also, we require that $\ell+3 \leq 6$. Thus $\ell \in \{1, 3\}$. This implies that if $\ell = 1$, then $j \in \{4, 5, 6\}$, but if $\ell = 3$, then $j \in \{6\}$,*

(ℓ, j)	$\pi_j = (1, 2, \ldots, \ell+1)(\ell+2)\Pi_{s=\ell+3}^{j}(s)$	S_j	$2^{j-\ell-1}4^{6-(j-1)}$
$(1,4)$	$\pi_4 = (1,2)(3)(4)$	$\{1,2,3,4\}$	$2^2 4^3$
$(1,5)$	$\pi_5 = (1,2)(3)(4)(5)$	$\{1,2,3,4,5\}$	$2^3 4^2$
$(1,6)$	$\pi_6 = (1,2)(3)(4)(5)(6)$	$\{1,2,3,4,5,6\}$	$2^4 4^1$

(ℓ, j)	$(1, \ldots, \ell+1)$	S_6	$2^{j-\ell-1)}4^{6-(\ell-1)}$
$(3,6)$	$(1,2,3,4)(5)(6)$	$\{1,2,3,4,5,6\}$	$2^2 4^1$

If ℓ is even, $\ell + 1 \leq j \leq 6$. New intersection numbers appears when $j \geq \ell + 2$. Also, we require that $\ell + 2 \leq 6$. Thus $\ell \in \{2, 4\}$. This implies that if $\ell = 2$, then $j \in \{4, 5, 6\}$, but if $\ell = 4$, then $j \in \{6\}$,

(ℓ, j)	$\pi_j = (1, 2 \ldots, \ell+1)\Pi_{s=\ell+2}^{j}(s)$	S_j	$2^{j-\ell}4^{6-(\delta-j)}$
$(1,4)$	$\pi_4 = (1,2)(3)(4)$	$\{1,2,3,4\}$	$2^2 4^2$
$(1,5)$	$\pi_5 = (1,2)(3)(4)(5)$	$\{1,2,3,4,5\}$	$2^3 4^1$
$(1,6)$	$\pi_6 = (1,2)(3)(4)(5)(6)$	$\{1,2,3,4,5,6\}$	$2^4 4^0$

(ℓ, j)	$(1, \ldots, \ell+1)$	S_6	$2^{j-\ell)}4^{6-(\delta-j)}$
$(3,6)$	$(1,2,3,4)(5)(6)$	$\{1,2,3,4,5,6\}$	$2^2 4^0$

*(**c**)* $\ell = 0$ *and* $j \in \{0, 1, \ldots, t\}$

(ℓ, j)	$(1, \ldots, \ell+1)$	S_j	$2^j 4^{\delta-j}$
$(0,0)$	(1)	$\{0\}$	$4^6 2^0$
$(0,1)$	(1)	$\{0,1\}$	$4^5 2^1$
$(0,2)$	(1)	$\{0,1,2\}$	$4^4 2^2$
$(0,3)$	(1)	$\{0,1,2,3\}$	$4^3 2^3$
$(0,4)$	(1)	$\{0,1,2,3,4\}$	$4^2 2^4$
$(0,5)$	(1)	$\{0,1,2,3,4,5\}$	$4^1 2^5$
$(0,6)$	(1)	$\{0,1,2,3,4,5,6\}$	$4^0 2^6$

Theorem 4.8. *Let $\mathcal{C}$ be a t-IR quaternary linear code of type $4^\delta 2^\gamma$. Then, $2^{t-\ell}4^{\delta-t}$, where ℓ is odd and $1 \leq \ell < t-1$,is an intersection number.*

Proof. By the previous Theorem, it is easy to see that for ℓ odd, $2^{t-\ell}4^{\delta-t}$ is a number which does not come by the conclusion of the theorem. Let $(1, 2, \ldots, \ell+1)$ be cycle of length $\ell+1$. Let $S = \{2, \ldots, t\}$ and consider ρ_s. That is, this is an inversion of all coordinates determined by the cycle, except the first one plus the inversion of the following $t-(\ell+1)$ coordinates. Since the cycle has now an odd number of inversions, it follows that $\tau(\pi)^o = 1 + t - \ell - 1 = t - \ell$, $\tau(\pi)^e = 0$, $\gamma(\pi) = t$. Since all these coordinates, correspond to columns of a free set, it follows that the number of codewords attached to any index is $2^{t-\ell}4^{\delta-t}$= and $\eta(\mathcal{C}, \rho(\pi(\mathcal{C})) = |\mathcal{C} \cap X_{\rho_s\pi}|2^{t-\ell}4^{\delta-t}$. Since coordinates from $t+1$ to n belong to columns of $I(\mathcal{C})$ and are zeros from any vector in $X_{\rho_s\pi}$, it follows that the unique codeword in this set is the codeword all zeros. Now the conclusion follows. □

Example 4.0.3. *We continue with the code given in the previous example. That code satisfies the hypothesis of the theorem.* $\ell \in \{1,3\}$, $t = 6 = \delta$. *So,* $4^0 2^5$ *and* $4^0 2^3$ *are new intersection numbers. The permutation for the first number is* $\pi = (1,2)(3)(4)(5)$ *and* $S = S_6 \setminus \{1\}$ *is the set of* ρ_s. *For the second number,* $\pi = (1,2,3)(4)(5)(6)$ *and the set* S *is like the first intersection number.*

Theorem 4.9. *Let* $\mathcal{C}$ *be t-IR quaternary linear code of type* 4^δ. *The expression of the intersection numbers computed in theorem 4.7, gives also the type, of the intersection.*

Proof. **Case 1**: $\eta(\mathcal{C}, \rho_{s_j}(\pi(\mathcal{C}))) = 4^{\delta-\ell}$, if, $1 \leq \ell \leq t-1$, $j = 0$.

CLAIM. The quaternary linear code $\mathcal{C} \cap \rho_s(\pi(\mathcal{C}))$ constructed in the proof of Theorem 4.7 can be expressed as a direct sum of $\delta - \ell$ cyclic subgroups of order 4.

In this case $S_0 = \{0\}$ and $\rho_0 = Id$, this means that there is no inversion of coordinates of the code $\mathcal{C}$. Thus, the permutation is the cycle $\theta = (1, \ldots, \ell+1)$, and we are going to write θ instead of $\rho_s\theta$. We prove the claim by showing that does not exist in the intersection a codeword of order 2 which is not the sum of one codeword in the intersection of order 4 with itself. By Theorem 4.7 we know that $\mathcal{C} \cap X_\theta = \{\ \mathbf{0}\}$. Thus the index zero has attached $4^{\delta-\ell}$ codewords. By lemma 4.4 these are all the codewords in the intersection. In other words, $\mathbf{h} \in \mathcal{C} \cap \theta(\mathcal{C})$ if and only if $\mathbf{h}_\theta = \mathbf{0}$. The projection $\mathbf{h}|_\theta$ satisfies the system (4.1) and by lemma 4.0.1 for each choice of h_1 we have 4 possibilities, 0, 1, 2 and 3. Thus, if $\mathbf{h} \in \mathcal{C} \cap \theta(\mathcal{C})$, either $\mathbf{h}|_\theta = (\underbrace{0, \ldots, 0}_{\ell+1})$ or $\mathbf{h}|_\theta = (\underbrace{1, \ldots, 1}_{\ell+1})$ or $\mathbf{h}|_\theta = (\underbrace{2, \ldots, 2}_{\ell+1})$ or $\mathbf{h}|_\theta = (\underbrace{3, \ldots, 3}_{\ell+1})$. In this way, $\mathcal{C} \cap \theta(\mathcal{C})$ can be expressed as the union of four disjoint sets (another way to see that the four sets above are disjoint consists of noticing that the relation defined in the intersection, $h_1 \sim h_2$ if and only if $h_{1|_\theta} = h_{2|_\theta}$ is the equivalence). Denote these sets by $[(\underbrace{0, \ldots, 0}_{\ell+1})]$, $[(\underbrace{1, \ldots, 1}_{\ell+1})]$, $[(\underbrace{2, \ldots, 2}_{\ell+1})]$ and $[(\underbrace{3, \ldots, 3}_{\ell+1})]$. It is clear that these sets are defined by $[(\underbrace{a, \ldots, a}_{\ell+1})] = \{h \in \mathcal{C} \cap \theta(\mathcal{C}) : \mathbf{h}|_\theta = (\underbrace{a, \ldots, a}_{\ell+1})\}$. Observe that $[(\underbrace{0, \ldots, 0}_{\ell+1})]$ is a subgroup of $\mathcal{C} \cap \theta(\mathcal{C})$ and the other are its cosets. Since the intersection is a finite group, each coset has the same cardinality. Notice, that the cosets that contain a codeword of

order two are $[(\underbrace{2,\ldots,2}_{\ell+1})]$ and $[(\underbrace{0,\ldots,0}_{\ell+1})]$ whereas the cosets that contain only codewords of order four are $[(\underbrace{1,\ldots,1}_{\ell+1})]$ and $[(\underbrace{3,\ldots,3}_{\ell+1})]$. Moreover, using the fact that $\mathcal{C} \cap \theta(\mathcal{C})$ is an additive group $\{\mathbf{h}+\mathbf{h} : \mathbf{h} \in [(\underbrace{1,\ldots,1}_{\ell+1})]\} = \{\mathbf{h}+\mathbf{h} : \mathbf{h} \in [(\underbrace{3,\ldots,3}_{\ell+1})]\} = [(\underbrace{2,\ldots,2}_{\ell+1})]$, $\{\mathbf{h}_1+\mathbf{h}_2 : \mathbf{h}_1 \in [(\underbrace{1,\ldots,1}_{\ell+1})], \mathbf{h}_2 \in [(\underbrace{3,\ldots,3}_{\ell+1})]\} = [(\underbrace{0,\ldots,0}_{\ell+1})]$.

That means, that any element of order two, is obtained by adding a codeword of order four by itself or is obtained by adding to different codeword the order 4 in the intersection. Thus, the type of the intersection is $4^{\delta-\ell}$.

Now, let us consider is the generator matrix of this intersection. Take $\mathbf{h} \in [(\underbrace{1,\ldots,1}_{\ell+1})]$. Then $\mathbf{2h} \in [(\underbrace{2,\ldots,2}_{\ell+1})]$ and $\mathbf{3h} \in [(\underbrace{3,\ldots,3}_{\ell+1})]$. Thus, the intersection can be obtained as a direct sum of the subgroup generated by $\mathbf{h}$ and the coset $[(\underbrace{0,\ldots,0}_{\ell+1})]$. Since the the type of the intersection is $4^{\delta-\ell}$, the type of $[(\underbrace{0,\ldots,0}_{\ell+1})]$ should be $4^{\delta-\ell-1}$, otherwise we will have a contradiction with the Fundamental Theorem of Abelian groups. Now, choose $\delta-\ell-1$ codewords of $[(\underbrace{0,\ldots,0}_{\ell+1})]$ of the form $c_{\ell+1+i} = (\underbrace{0,\ldots,0}_{\ell+1}\ \underbrace{0,\ldots,1,0\ldots,0}_{t-\ell+1}, c_{t+1}\ldots,c_n)$, where $1 \leq i \leq \delta-\ell-1$, and $\ell+1+i$ indicates the position in which is placed the number 1. Now the generator matrix is obtained in the following way, place the codeword $\mathbf{h}$, as the first row of the matrix and then, place the $\delta-\ell-1$ codewords $c_{\ell+i}$ as the last rows of the matrix.

Case 2: $\eta(\mathcal{C}, \rho_{s_j}(\theta(\mathcal{C}))) = 2^1 4^{\delta-\ell-1}$ if $1 \leq \ell \leq t-1$, $j=1$.

CLAIM: The quaternary linear code $\mathcal{C} \cap \rho_{s_1}\theta(\mathcal{C})$, constructed in the proof of Theorem 4.7 can be expressed as a direct sum of $\delta-\ell-1$ cyclic subgroups of order 4 and 1 cyclic subgroup of order 2.

If in the generator matrix constructed in case 1, we multiply by -1, the first coordinate of each row, we see that ρ_1, change the first coordinate of the codeword $\mathbf{h}$, which is in the first row. The last $\delta-\ell-1$ rows are invariant since their first coordinate is 0. $<\mathbf{h}>$ is a cyclic subgroup of order 4 generated by $\mathbf{h}$, and $<\rho_1(\mathbf{h})>$ is a cyclic subgroup of order 4 generated by $\rho_1(\mathbf{h})$, and $<\mathbf{h}> \cap <\rho_1(\mathbf{h})> = \{\mathbf{0}, 2\mathbf{h}\}$. This means that in the cyclic

subgroup generated by $\mathbf{h}$, the codewords of order two are invariant. Thus, the generator matrix for $\mathcal{C} \cap \rho_{s_1}\theta(\mathcal{C})$ is obtained by the generator matrix of $\mathcal{C} \cap \theta(\mathcal{C})$ by multiplying the first row by 2.

Case 3: $\eta(\mathcal{C}, \rho_{s_j}(\theta(\mathcal{C}))) = 2^{j-\ell}4^{\delta-j}$ if ℓ is even $\ell+1 \leq j \leq t$, $j = 1$.

CLAIM: The quaternary linear code $\mathcal{C} \cap \rho_{s_j}(\pi_j(\mathcal{C}))$, constructed in the proof of Theorem 4.7 can be expressed as a direct sum of $\delta - j$ cyclic subgroups of order 4 and $j - \ell$ cyclic subgroups of order 2.

For $S_{\ell+1}$, with ℓ even, $\mathcal{C} \cap \rho_{s_{\ell+1}}(\theta(\mathcal{C}))$ is of type $2^1 4^{\delta-\ell-1}$ and the generator matrix has in the first row $2\mathbf{h}$, where $\mathbf{h} \in [(\underbrace{1, \ldots, 1}_{\ell+1})]$, and the last $\delta - \ell - 1$ are occupied for codewords in $[(\underbrace{0, \ldots, 0}_{\ell+1})]$ Now, consider $S_{\ell+2}$ and the permutation $\pi_{\ell+2} = (1, 2 \ldots, \ell+1)(\ell+2)$. Notice that in the generator matrix of $\mathcal{C} \cap \rho_{s_{\ell+1}}(\theta(\mathcal{C}))$, the second row is given by $\mathbf{c}_{\ell+2} = (\underbrace{0, \ldots, 0}_{\ell+1}\ \underbrace{1, \ldots, 0, 0 \ldots, 0}_{t-\ell+1}, c_{t+1} \ldots, c_n)$, but the other rows have 0 in that component, as a result, the new generator matrix is obtained by only multiplying by 2, the codeword $c_{\ell+2}$. Assume $j = \ell + 1 + i$ and consider the permutation $\pi_{\ell+1+i} = (1, 2 \ldots, \ell+1)\Pi_{s=\ell+2}^{\ell+1+i}(s)$. The generator matrix of $\mathcal{C} \cap \rho_{s_{\ell+i-1}}(\pi_{\ell+i-1}(\mathcal{C}))$ has the first row is occupied by $2h$, the next $\ell + i - 1$ rows by $2\mathbf{c}_{\ell+i-1}$ and the last $\delta - (\ell + i)$ by codewords of order four that belong to $[(\underbrace{0, \ldots, 0}_{\ell+1})]$. In this matrix, the row $c_{\ell+i} = \mathbf{c}_{\ell+2} = (\underbrace{0, \ldots, 0}_{\ell+i}\ \underbrace{1, \ldots, 0, 0 \ldots, 0}_{t-\ell+1}, c_{t+1} \ldots, c_n)$ is the unique codeword that has 1 in the coordinate $\ell + i$. So, after the application of the monomial map, the new generator matrix is obtained by multiplying this codeword by 2. Thus, we have $i + 1$ codewords of order two and $\delta - (\ell + i + 1)$ codewords of order four. Since $j = \ell + 1 + i$, then $j - \ell = 1 + i$ and the conclusion of the claim follows.

Case 4: $\eta(\mathcal{C}, \rho_{s_j}(\pi(\mathcal{C}))) = 2^{j-\ell-1}4^{\delta-(j-1)}$, if ℓ is odd, $\ell + 1 < j \leq t - 1$

CLAIM: The quaternary linear code $\mathcal{C} \cap \rho_{s_j}(\theta(\mathcal{C}))$, constructed in the proof of Theorem 4.7 can be expressed as a direct sum of $\delta - (j-1)$ cyclic subgroups of order 4 and $j - \ell - 1$ cyclic subgroups of order 2.

We omit the proof of this case since is similar to the previous case.

Case 5: $\eta(\mathcal{C}, \rho_{s_j}(\theta(\mathcal{C}))) = 2^j 4^{\delta-j}$ if $\ell = 0$, $j \in \{0, 1, ..., t\}$.

CLAIM: The quaternary linear code $\mathcal{C} \cap \rho_{s_j}(\theta(\mathcal{C}))$, constructed in the proof of Theorem 4.7 can be expressed as a direct sum of $\delta - j$ cyclic subgroups of order 4 and j cyclic subgroups of order 2.

In this case $S_j = \{1, \ldots, t\}$ and since $\ell = 0$ there is no permutation, so we just write $\rho_{s_j}(\mathcal{C})$ instead of a $\rho_{s_j}(\theta(\mathcal{C}))$. Put the generator matrix of $\mathcal{C}$ in the form $G = (I_\delta | A)$. Denote by G' the generator matrix of $\rho_{s_j}(\mathcal{C})$. G' differs from$G$, in the j first rows, and coincide in the last $\delta - j$ rows. Since each row of G is a codeword of order 4, these $\delta - j$ rows of G' are of order 4. Notice that, for $1 \leq i \leq j$, ρ_{s_j}, multiplies by -1, the i-th coordinate of the *i-th* row of G. Seeing the code as a finite direct sum of cyclic subgroups, the rows of G are the generators of cyclic groups of order 4 in that direct sum ρ_{s_j}, changes the *j-th* coordinate in each of the 4 codewords that correspond to the cyclic subgroup generated by the j-th row. But in this subgroup we know that only two codewords in the j-th coordinate, have 0 or 2, which mean these codewords remains after the inversion of that coordinate. As a result we have that $\mathcal{C} \cap \rho_{s_j}(\theta(\mathcal{C}))$ is expressed as a direct sum of $4^{\delta - j}$ subgroups of order 4 and 2^j subgroups of order 2.

□

Theorem 4.10. *[15] Let $\mathcal{C}_1$, $\mathcal{C}_2$, be two quaternary linear codes. Then,*

$$\langle \mathcal{C}_1^\perp, \mathcal{C}_2^\perp \rangle \quad = \quad (\mathcal{C}_1 \cap \mathcal{C}_2)^\perp \tag{4.2}$$

Theorem 4.10 allows one to see the parity-check matrix of the intersection of two quaternary linear codes $\mathcal{C}_1$, $\mathcal{C}_2$, similar to the case of linear codes defined over finite fields. That is, if H_1 and H_2 are the respective parity-check matrices, then,

$$H = \begin{pmatrix} H_1 \\ H_2 \end{pmatrix}. \tag{4.3}$$

is the parity matrix of the intersection.

Suppose that the type of $\mathcal{C}_1 \cap \mathcal{C}_2$ is $4^\delta 2^\gamma$, by Theorem 4.10 and 1.8, H will have $n - k_1$ rows that δ rows that are vectors of order 4 plus γ rows that are vectors of order 2, where k_1 is the number of rows in the generator matrix of $\mathcal{C}_1 \cap \mathcal{C}_2$.

Theorem 4.11. *Let $\mathcal{C}$ be a quaternary linear code of type $4^\delta 2^0$ then k_1 is the Pseudodimension of $\mathcal{C} \cap \rho_s(\pi(\mathcal{C}))$, if and only if $n - 2\delta + k_1$ is the Pseudodimension of $\mathcal{C}^\perp \cap \rho_s(\pi(\mathcal{C}^\perp))$*

Proof. Let G be a generator matrix of $\mathcal{C}$, given by (1.5). Let H and $\rho_s(\pi(H))$ be parity-check matrices of both, $\mathcal{C}$ and $\rho_s\pi(\mathcal{C})$. Let $H_1 = (H \parallel \rho_s(\pi(H)))$, the parity-check matrix of $\mathcal{C} \cap \rho_s(\pi(\mathcal{C}))$. The Pseudo-dimension of this matrix is $n - k_1$ then $n - k_1 = k_2 + 2(n - \delta - k_2)$ and hence $k_2 = n - 2\delta + k_1$. Similarly, if $k_2 = n - 2\delta + k_1$ is the Pseudodimension of $\mathcal{C}^\perp \cap \rho_s(\pi(\mathcal{C}^\perp))$, then $n - 2(n - k) + k_2 = k_1$.

□

Corollary 4.0.1. *Let $\mathcal{C}$ be a quaternary linear t-IR code of type $4^\delta 2^0$, $\delta \geq n - \delta$, $gp(x) = 0$, for all $\mathbf{x} \in \mathcal{C}$, then $2\delta - n$ is not pseudo-dimension of the intersection.*

Proof. By contradiction, suppose that the pseudo-dimension of the intersection is $2\delta - n$, then by Theorem 4.11 the only possible intersection of $\mathcal{C}^\perp$ with any of its equivalent codes is 1. Since the vector $\mathit{1} \in \mathcal{C}^\perp$, Theorem 4.0.4 say that the intersection should be at least 2. □

Theorem 4.12. *Let C be an (n, k) t-IR code and G its generator matrix, where $I(C) = \{n - k + 1, n - k + 2, \ldots, n\}$, columns $1, 2, \ldots, t, n - k + 1$ are linearly independent, the first row of G doesn't have generalized parity 0, and the last $k - 1$ entries in this row are zeroes. Then there exists a permutation π such that $\eta(C, \pi(C)) = 2^{k-t}$.*

Due to the fact that $\beta : \{0, 2\}^n \to \mathbb{Z}_2^n$ is an isomorphism, any quaternary linear code of type 2^γ can be identified as an binary code of dimension γ. Thus, the theorem 4.12 above, can be applied if we want to compute intersection numbers of codes of that type.

When the quaternary code is of type 4^δ, a slightly modification of the statement in Theorem 4.12 gives the following result

Theorem 4.13. *Let $\mathcal{C}$ be an (n, δ) t-IR code and G its generator matrix, where $I(\mathcal{C}) = \{n-\delta+1, n-\delta+2, \ldots, n\}$, columns in $\alpha(G)$ $1, 2, \ldots, t, n-\delta+1$ are linearly independent, the first row of G doesn't have generalized parity 0 or 2 and the last $\delta - 1$ entries in this row are zeroes. Then there exists a permutation π such that $\eta(\mathcal{C}, \pi(\mathcal{C})) = 4^{\delta-t}$.*

4.1 Application to $\overline{\mathcal{QRM}}(r, m)$

In this section we are going to apply the results of the previous section to the class $\overline{\mathcal{QRM}}(r, m)$. First of all, we need to establish the possible spectrum of the intersection of two codes in this class.

Let $r \geq 1$, Let $\mathcal{C}_1 \in \overline{\mathcal{QRM}}(r, m)$ of type $(0, \delta_1, n)$, then $\mathcal{C}_2 = \rho(\pi(\mathcal{C}_1)) \in \overline{\mathcal{QRM}}(r, m)$ and has the same type same type $(0, \delta_1, n)$ then by proposition 3.6.2 $\langle \mathcal{C}_1, \mathcal{C}_2 \rangle$ is a quaternary linear code of type code of type (γ, δ, n) where

$$\delta \quad \in \quad \{\delta_1, ..., min(2\delta_1, n)\} \tag{4.4}$$

and

$$max(\delta, \delta_1) \quad \leq \quad \delta + \gamma \leq min(2\delta_1, n) \tag{4.5}$$

By 3.6.1

$$\eta(\mathcal{C}_1, \mathcal{C}_2) \quad = \quad |\mathcal{C}_1 \cap \mathcal{C}_2| = \frac{4^{2\cdot\delta_1}}{|\langle \mathcal{C}_1, \mathcal{C}_2 \rangle|} \tag{4.6}$$

If we choose $2\delta_1 < n$, in (4.0.1) then $\delta \in \{\delta_1, ..., 2\delta_1\}$, and $\delta_1 \leq \delta + \gamma \leq 2\delta_1$ If we select $\gamma = 0$ and $\delta = 2\delta_1$, we obtain the maximum lower bound $\eta(\mathcal{C}_1, \mathcal{C}_2) \geq 1$.

If $2\delta_1 > n$, then $\delta \in \{\delta_1, ..., n\}$, and $\delta_1 \leq \delta + \gamma \leq n$. Again, if we select $\gamma = 0$ and $\delta = n$,we obtain the maximum lower bound for this intersection, $\eta(\mathcal{C}_1, \mathcal{C}_2) \geq 4^{2\cdot\delta_1 - n}$. Thus, we have the following proposition.

Theorem 4.14. *Let* $r \geq 1$,$\mathcal{C}_1$, $\mathcal{C}_2 \in \overline{\mathcal{QRM}}(r,m)$ *both of type* $(0, \delta_1, n = 2^m)$, *Then If* $2\delta_1 < n$

$$1 \leq \eta(\mathcal{C}_1, \mathcal{C}_2) \leq 4^{\delta_1}$$

If, $2\delta_1 > n$

$$4^{2\cdot\delta_1 - n} \leq \eta(\mathcal{C}_1, \mathcal{C}_2) \leq 4^{\delta_1}.$$

Now, we need to see that given a code $\mathcal{C} \in \overline{\mathcal{QRM}}(r,m)$, it is an t-(IR) code. By Theorem 2.6, we know that the generator matrix of $\mathcal{C}$ can be written as $G = G(r,m) + 2N$, where $G(r,m)$ is the generator matrix of the Reed-Muller code with parameters $[n, \delta]$, which we know, (see example 3.2.1) is a t-(IR) code and therefore $\mathcal{C}$. As in the binary case, when $r \leq \lceil (m+1)/2 \rceil$,we have that $\delta \leq r^*$, where $r^* = n - \delta$ and $t = \delta$. According to 4.7, there exists a subset $A \subset \{0, 1, 2, \ldots, \delta - 1\} \times \{0, 1, 2, \ldots, \delta\}$ such that for all $(\ell, j) \in A$, there is a permutation π_ℓ and a set S_j associated to the map such that $\eta(\mathcal{C}, \rho_{s_j}(\pi(\mathcal{C})))$ satisfies the values given by Theorem 4.7. By construction we know that A can be expressed as follows: $A = \bigsqcup_{i=1}^{5} A_i$, where, $A_1 = \{(\ell, 0), 1 \leq \ell \leq \delta - 1\}$, $A_2 = \{(\ell, 1), 1 \leq \ell \leq \delta - 1\}$,
$A_3 = \{(\ell, j), \ell \text{ is odd}, 1 \leq \ell \leq \delta - 1, \ell + 1 < j \leq \delta - 1\}$,
$A_4 = \{(\ell, j), \ell \text{ is even}, 1 \leq \ell \leq \delta - 1, \ell + 1 < j \leq \delta - 1\}$, $A_5 = \{(0, j), 0 \leq j \leq \delta\}$.

The minimum intersection number obtained by Theorem 4.7 is 2 and is given by the ordered pair $(\delta - 1, 1)$ which belong to the subset A_2. Since 1 is a lower bound of the possible spectrum for these codes we still need to see if it is an intersection number. Notice that $\mathbf{1} \in \mathcal{C}$, then by Theorem 4.0.4, 1 is not an intersection number.

Similarly, if $r \geq \lceil (m+1)/2 \rceil$,we have that $\delta \geq r^*$, where $r^* = n - \delta$ and $t = n - \delta$. A is a subset of $\{0, 1, 2, \ldots, n - \delta - 1\} \times \{0, 1, 2, \ldots, n - \delta\}$. As in the previous case, this set is the union of the following five sets:
$A_1 = \{(\ell, 0), 1 \leq \ell \leq \delta - 1\}$, $A_2 = \{(\ell, 1), 1 \leq \ell \leq n - \delta - 1\}$,
$A_3 = \{(\ell, j), \ell \text{ is odd}, 1 \leq \ell \leq n - \delta - 1, \ell + 1 < j \leq n - \delta - 1\}$,
$A_4 = \{(\ell, j), \ell \text{ is even}, 1 \leq \ell \leq n - \delta - 1, \ell + 1 < j \leq \delta - 1\}$, $A_5 = \{(0, j), 0 \leq j \leq n - \delta\}$.

Again, the minimum intersection number obtained by Theorem 4.7, is $4^{\delta-1}2^1$. We still need to see if $4^{2\delta-n}$ is and intersection number. Since for all $\mathbf{x} \in \mathcal{C}$, $gp(\mathbf{x}) = \mathbf{0}$ by corollary 4.0.1 $4^{2\delta-n}$ is not an intersection number.

Considering both cases, we can say that the minimum intersection number for the class of quaternary Reed-Muller codes is given by $\max\{4^{2\delta-n}, 2\}$.

Additional intersection number are obtained by Theorem 4.8 in the following way. For $t = \delta$, consider ℓ odd in the interval $1 \leq \ell < \delta - 1$, with $S = \{2, \ldots, \delta\}$, and for $t = n - \delta$, consider ℓ odd $1 \leq \ell < n - \delta - 1$, with $S = \{2, \ldots, n - \delta\}$.

Now, we discuss particular cases. If $\mathcal{C} = \mathcal{QRM}(1, m)$, then it is a quaternary Kerdock code. Since $n - \delta \leq \delta$, the minimum intersection is 2. If $\mathcal{C} = \mathcal{QRM}(m-2, m)$ then, it is the quaternary linear Preparata code, then $n - \delta \geq \delta$, and the minimum intersection number is $4^{\delta-1}2^1$ if $n - \delta > \delta$.

Chapter 5

Concluding Remarks

In this dissertation we solved the intersection problem for the class of quaternary Reed-Muller codes, that is, we have found all the intersection numbers by considering intersections of monomial equivalent codes. In addition, we determined the abelian structure of that intersections and their respective generator matrices. The class of quaternary Red-Muller codes contains two important families, the Kerdock-like codes, and Preparata-like codes. Note that since nonlinear binary Kerdock-like codes and Preparata-like codes are $\mathbb{Z}_4$-linear codes, the spectrum for these codes are also determined. It should be noted that trying to solve the intersection problem for these codes in the realm of $\mathbb{Z}_2$ would be much more laborious. For example, solving the intersection problem for the quaternary Kerdock code $\mathcal{K}$ is less involved than solving it for nonlinear binary Kerdock-codes.

One problem that is remaining is the intersection problem for binary non-linear codes that have the same parameters as Kerdock-like codes, and Preparta-like codes, but are not $\mathbb{Z}_4$-linear codes, that is, they are not binary Gray map images of quaternary linear codes. So, the intersection problem for these codes can not be solved by using the linear structure provided by $\mathbb{Z}_4$.

We have developed enough theory that allows to us to solve the intersection problem for other families of codes apart of those already examined, that is, Goethals codes, Delsarte-Goethals codes, ZRM codes and quaternary cyclic codes. Let's see briefly, how we can apply the results of chapter 4 to quaternary cyclic codes of length n.

According to their types, quaternary cyclic codes can be classified into three classes of types $2^0 4^\delta$, $2^\gamma 4^\delta$ and $2^\gamma 4^0$. If the cyclic code is of type $2^0 4^\delta$, its residue binary cyclic code is an $[n, \delta]$-code. The first δ columns of its generator matrix are linearly independent and the last δ columns are also linearly independent. So, this binary cyclic code is a t-IR code

for $t = min\{\delta, r\}$. Thus the quaternary cyclic code is also a t-IR code for $t = min\{\delta, r\}$. So all the values specified by Theorem 4.7 are intersection numbers.

Cyclic codes of type $2^\gamma 4^0$ behave as a binary cyclic codes. That way, they are t-IR codes for $t = min\{\gamma, n-\gamma\}$. Also the concepts of monomial equivalence and permutation equivalence, coincide. By Theorem 4.7 for each ℓ, $0 \leq \ell \leq t-1$, there is a permutation π_ℓ, for which $\eta(\mathcal{C}, \pi(\mathcal{C})) = 2^{\gamma-\ell}$. Notice that in this case, $max\{1, n-2(n-\gamma)+1\} \leq t \leq n-\gamma$.

The case of cyclic codes of type $2^\gamma 4^\delta$ is treated using Theorem 4.5. That is, this case is the union of the two previous cases.

In the first case, it remains to discuss whether $max\{1, 2^0 4^{n-2(n-\delta)}\}$ is also an intersection number and, in the second case, whether $max\{1, 2^{n-2(n-\gamma)} 4^0\}$ is also an intersection number. This question can be solved by considering whether the vector $\mathbf{1}$ is a codeword or not, for codes of type $2^\gamma 4^\delta$ with $\delta > 0$; and whether the vector $\mathbf{2}$ is a codeword or not, for codes of type $2^\gamma 4^\delta$ with $\delta = 0$ and $\gamma > 0$. As matter of example, we consider only the case when $\mathbf{1}$ is in the code, (respectively when $\mathbf{2}$ is in the code).

Denote the code by $\mathcal{C}$ and by g its generator polynomial. $\mathbf{1} \in \mathcal{C}$ implies that $\alpha(\mathbf{1}) \in \alpha(\mathcal{C})$. Thus, $\alpha(g)(\mathbf{1}) = 1$, where $\alpha(g)$ is the polynomial generator of $\alpha(\mathcal{C})$. Therefore, either $g(\mathbf{1}) = 1$ or $g(\mathbf{1}) = 3$, which mean that the first row of the generator matrix of $\mathcal{C}$ of the generator matrix doesn't have generalized parity 0 or 2. If the code is of type $4^\delta 2^0$, then for $\delta > n-\delta$, $(t = n-\delta)$ the conditions of theorem 4.13 are satisfies and therefore $4^{\delta-t} = 4^{n-2(n-\delta)}$ is an intersection number; for $\delta \leq n-\delta$, $(t = \delta)$ we have $1 = max\{1, 4^{n-2(n-\delta)}\}$ and by Lemma 4.0.4, one is not an intersection number. If $\mathbf{2}$ is in the code which is of type $4^0 2^\gamma$, then for $\gamma > n-\gamma$ $(t = n-\gamma)$ the conditions of theorem 4.12 are satisfies and therefore $2^{\gamma-t} = 2^{n-2(n-\gamma)}$ is an intersection number; for $\gamma \leq n-\gamma$, we have $1 = max\{1, 2^{n-2(n-\gamma)}\}$ and by Lemma 4.0.4 one is not an intersection number. Using Theorem 4.5, the general case, can be obtained by combining the two previous cases.

The intersection problem for perfect codes is still unsolved. In the binary case, part of the spectrum is known. It is interesting to note that in each admissible length, this spectrum does not have holes in the interval $[0, a(n)]$, where $0 \leq a(n) \leq 2^{n-m} - 2^v$. Considering that

those intersections numbers were found using essentially the construction of Vasil'ev, we can consider the possibility that each integer even number z, such that $0 \leq z \leq 2^{n-m} - 2^v$ is actually an intersection number by trying to construct pairs of perfect binary codes, using for example, Phelps construction, or Phelps-Soloveva's construction among others or combining them in a more or less ingenious way.

Recently, Östergärd, and Pottonin,[24] obtained a complete classification of all non inequivalent perfect binary codes of length 15. By computer search this number is 5983. Thus, for the case of length 15, we will know the spectrum of the intersection by computer search. If the spectrum covers all the interval specified above, then one can try to prove this result for all admissible length. On the contrary, if the spectrum has holes then probably this is true for all admissible lengths.

The intersection problem for q-ary perfect codes is considered in [12]. It is interesting to notice that there are some differences with respect to the binary perfect codes. In the binary case, the minimum intersection number is 2, instead [12] provides one example of two ternary perfect codes with intersection number equal to 1, which in turn implies that the intersection number for q-ary perfect codes, where $q > 2$, is not necessarily even. Also, [12] gives the spectrum of intersection numbers of non-linear perfect codes by the switchings of simple components.

Essentially we can classify the known constructions under two groups, those based on the approach of switching constructions and those base on the approach of concatenation constructions. It would be interesting determine the spectrum of intersection numbers of intersection of non-linear q-ary perfect codes using this last approach.

The intersection problem can be seen from another point of view; for example, in the case of perfect codes, the kernel is their biggest linear sub-code. An obvious question is how is the spectrum of the intersection of two kernels of the same dimension. It is known that there are many constructions of perfect codes and we can find two perfect codes having kernels with the same dimension but coming from different constructions. It would be interesting to compare the intersections of kernels of perfect codes obtained by the same

construction with the intersection of those coming from different constructions. The same question can be formulated for the rank of a perfect code, which is its smallest linear superspace.

Bibliography

[1] A. Jamos, P.V. Kumar, A.R. Calderbank, N.J.A Sloane, and P. Sole, "The $\mathbb{Z}_4$ Linearity of kerdock, preparata, Goethals, and related codes", *IEEE Trans. Inform. Theory*, vol. 40, pp. 301-319, 1994.

[2] Z.-X.Wan, "Quaternary Codes", World Scientific, Singapore, 1997,

[3] J.Borges-K.T. Phelps,J. Rifá, "Kerdok-Like, and preparata-like", *IEEE Trans. Inform. Theory*, vol. 49, pp. 2834-2843, 2003.

[4] J. Borges and J. Rifà, "A characterization of 1-additive perfect codes", *IEEE Trans. Inform. Theory*, vol. 45, no. 5, pp. 1688–1697, 1999.

[5] C. Fernandez, "On Reed-Muller and related quaternary codes",Universitat Autnoma de Barcelona Universitat Autnoma de Barcelona, Barcelona, ISBN:84-689-7933-3, October, 2005.

[6] Borges, C. Fernandez, and K.T Phelps, "Quaternary Reed-Muller Codes", *IEEE Trans. Inform. Theory*, vol. 51, no. 5, pp. 2686–2691, 2005.

[7] F. I. MacWilliams and N. J. Sloane, *The theory of Error-Correcting codes*, North-Holland, New York, 1977.

[8] J. Borges, C. Fernández, J. Pujol, J. Rifà and M. Villanueva, "add-linear codes: generator matrices and duality", submitted to *Designs, Codes and Cryptography*, arXiv:0710.1149, 2008.

[9] S. V. Avgustinovich, O. Heden, F. I. Solov'eva, "On intersection problem for perfect binary codes", *Designs. Codes and Cryptography.*, vol. 39, pp. 317–322, 2006.

[10] E. Bar-Yahalom, T. Etzion, "Intersection of isomorphic linear codes", *Journal of Comb. Theory*, Series A 80, pp. 247-256, 1997.

[11] F. I. Solov'eva and A. V. Los', "On intersections of q-ary perfect codes", *Proc. Tenth Int. Workshop "Algebraic and Combinatorial Coding Theory"*. Zvenigorod, Russia. September, pp. 244-247, 2006.

[12] F. I. Solov'eva and A. V. Los', "Intersections of q-ary perfect codes", *Siberian Math. Journal*, vol. 49, no. 2, pp. 464-474, 2008.

[13] T. Etzion, and A. Vardy, "On Perfect Binary Codes: Constructions, Properties, and Enumeration", *IEEE Trans. Inform. Theory*, vol. 40, no. 3, pp.754-763, 1994

[14] K. T. Phelps and M. Villanueva, "Intersection of Hadamard codes", *IEEE Trans. Inform. Theory*, vol. 53, no. 5, pp. 1924–1928, 2007.

[15] J. Rifà, F. I. Solov'eva and M. Villanueva, "On the intersection of add-additive perfect codes", *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 1346–1356, 2008.

[16] D. S. Krotov, "$\mathbb{Z}_4$-linear perfect codes", Discrete Analysis and Operation Research, Novosibirsk, Institute of Math. SB RAS, vol. 7, N. 4, pp. 78–90, 2000 (in Russian). (translation available at http://arxiv.org//abs/0710.0198).

[17] D. S. Krotov, D. S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes", *Proc. of the International Workshop on Coding and Cryptography*, Paris (France), Jan. 8-12, pp. 329–334, 2001.

[18] J. L.Vasilev, On nongroup close-packed codes, *Probl. Kibernet*, vol. 8, pp. 375378. 1962.

[19] K.T. Phelps, A combinatorial construction of perfect Codes, *SIAM J. Alg. Meth. Inform*, vol. 4, pp. 398-403. 1983.

[20] F.I. Solove'va, On binary nongroup codes, *Methodi Diskr. Analiza*, vol. 37, pp. 65-76. 1981.

[21] J. Rifá, Well-Ordered steiner triple system and 1-perfect partitions of the N-cube, *SIAM J. Discrete Math*, vol. 12, pp. 35-47. 1999.

[22] T. Etzion, and A. Vardy, On Perfect Codes and tilings: Problems and solutions,*SIAM J. Discrete Math*, vol. 11, pp. 205-223. 1998.

[23] J. Rifà, F. I. Solov'eva and M. Villanueva, "On the intersection of $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard codes", *IEEE Trans. Inform. Theory*, vol. 55, no. 4, pp. 1766–1774, 2009.

[24] Patrick R.J Ostergad, and Olli Pottonin, The Perfect Binary One-Error-Correcting Codes of Length 15: Part I-Classification, *arXiv:0806.2513v2*,22 jun 2009.