ON RANK AND KERNEL OF PERFECT CODES

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

by Mercè Villanueva i Gay

Bellaterra, July 2001

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

Bellaterra, July 2001

Dr. Kevin T. Phelps
(Adviser)

Dr. Josep Rifà i Coma
(Adviser)

to my family

Abstract

In this dissertation, we will study the rank and the dimension of the kernel of binary 1-perfect codes and in general the rank of q-ary 1-perfect codes over a prime power alphabet, $\mathbb{F}_q$.

It is known the existence of binary 1-perfect codes with any possible rank and any possible size of the kernel, separately. We will consider the following problem, for what pairs of numbers (r, k) does there exist a binary 1-perfect code C of length $n = 2^m - 1$ having $r(C) = r$ and $k(C) = k$. We establish the exact upper and lower bounds on the dimension of the kernel, once the rank is fixed. In order to show that, we also establish some results on the structure of binary 1-perfect codes. We also construct binary 1-perfect codes with different dimensions of the kernel between the upper and the lower bounds for any rank, using the Doubling and Switching construction.

Finally, we establish the existence of q-ary 1-perfect codes of length $n = \dfrac{q^m - 1}{q - 1}$ with any possible rank, $\forall m \geq 4$. In order to prove that, we generalize an approach of the Switching construction to construct q-ary 1-perfect codes.

Acknowledgements

This dissertation is the final result of several years of efforts working on perfect codes, with Dr. Josep Rifà at Universitat Autònoma de Barcelona (Catalonia, Spain) and with Dr. Kevin Phelps at Auburn University (Alabama, USA). However, all this dedication would have failed without the help, advice and affection of many people. So, I would like to thank all the people that have made this dissertation possible.

I am specially grateful to my advisers Dr. Josep Rifà and Dr. Kevin Phelps for sharing with me their knowledge and experience. I thank Josep Rifà for introducing me to this subject of perfect codes and for all he has taught me. I also thank him for encouraging and supporting me in every moment. I thank Kevin Phelps for showing me his way of doing research. I have learnt a lot from him. I also thank him and his family their kindness and hospitality during my two stays in Auburn.

A special thanks to all the members of the Combinatorics and Digital Communication Group at Universitat Autònoma de Barcelona, who are not only colleagues but friends too. I thank Quim Borges, Jaume Pujol, Italo Dejter and Victor Zinov'ev for our talks about perfect codes and Cristina Fernández, Josep M. Basart and Nuria Esturau for their reviews of some parts of this dissertation.

I would also like to express my gratitude to friends, professors and graduate students in Auburn, especially to Liu Chun, Aurora Thorgerson, Dr. Lindner, Selda Kucukcifci, Sule Yazici and Anthony Hall, for their friendship and help. They made me feel very comfortable in Auburn although I was very far from my home country.

Finally, I want to thank my family, specially my mother, for their love and unconditional support, specially during difficult moments when they have been encouraging me and cheering me up. A special thanks to all my friends, I do not want to write names because I would miss some of them. Without them nothing that I have done would had been possible.

To all of you, thank you very much.

Contents

Chapter 1

Introduction

Investigating perfect codes is one of the most fascinating subjects in coding theory. Many problems regarding perfect codes are still open, for example, the main problem of the construction and enumeration of perfect codes remains unsolved. In recent years, a lot of papers have been devoted to the construction and investigation of properties of perfect codes.

Let $\mathbb{F}_q^n$ be a vector space of dimension n over a Galois Field $\mathbb{F}_q = GF(q)$. A q-ary code C of length n is *perfect* if for some integer $r \geq 0$ every $x \in \mathbb{F}_q^n$ is within distance r from exactly one codeword of C. A q-ary perfect code of length n can correct r errors, so they are also called *perfect r-error correcting codes* or *r-perfect codes*.

It is well-known that, over a prime power alphabet $\mathbb{F}_q$, the only parameter for which there exist nonequivalent perfect codes is $r = 1$. These are the q-ary 1-perfect codes. They have length $n = \dfrac{q^m - 1}{q - 1}$, q^{n-m} codewords and minimum distance 3. Linear q-ary 1-perfect codes are unique up to equivalence, they are the well-known *q-ary Hamming codes* and they exist for all $m \geq 2$. Nonlinear q-ary 1-perfect codes exist for $q = 2$, $m \geq 4$; $q \geq 3$, $m \geq 3$, and for q a prime power, $q \neq 4$ or 8, $m \geq 2$. Over other alphabets, the only known perfect codes are the trivial ones. These are the codes containing all vectors of some length and the codes consisting of only one codeword of length n. So, we will henceforth only work on 1-perfect codes over a

prime power alphabet, $\mathbb{F}_q$.

In this dissertation we will focus on two structural properties, rank and dimension of the kernel, which let us study nonlinear perfect codes. The *rank* of a code C, $r(C)$, is simply the dimension of the subspace spanned by C, $\langle C \rangle$. The *kernel* of a binary code C is defined as: $K_C = \{x \in \mathbb{F}_2^n \ : \ C = C + x\}$, in other words, it is the subset of $\mathbb{F}_2^n$ such that any vector in it leaves C invariant under translation. In general, for any q-ary code it can also be defined as the intersection of all maximal linear subcodes in that code. We will denote the dimension of the kernel of C by $k(C)$. When the code C is linear, the rank and the dimension of the kernel are the same and equal to the dimension of the code. In some sense these two parameters give information about the linearlity of a code.

The rank and the dimension of the kernel do not give a full classification of 1-perfect codes, since two nonequivalent 1-perfect codes could have the same rank and dimension of the kernel. In spite of that, they can help to a classification since if two 1-perfect codes have different rank or kernel dimension they are not equivalent. Another invariant, called *STS-Graphical invariant* for perfect codes has been studied lately, [Dej01].

Both the rank and the kernel of binary 1-perfect codes have been studied separately. Ranks of binary 1-perfect codes were investigated by Etzion and Vardy [EV94], who proved that there exist 1-perfect codes with any possible rank. Phelps and LeVan [PL95] obtained 1-perfect codes with kernels of all possible sizes. These two results are the following:

Theorem 1.1. [EV94] *For all $m \geq 4$ there exists a binary 1-perfect code, C, of length $n = 2^m - 1$ with a rank of dimension $r(C) = n - m + s$ for each $s \in \{0, 1, \ldots, m\}$.*

Theorem 1.2. [PL95] *For all $m \geq 4$ there exists a binary 1-perfect code, C, of length $n = 2^m - 1$ having a kernel of dimension j if and only if $j \in \{1, 2, \ldots, n-m-2, n-m\}$.*

The rank and kernel are known to be related, [EV98]. The first relation is established in [BGH83] and it says that for a binary 1-perfect code C, $C^{\perp} \subset K_C$ and $k(C) + r(C) \geq n + 1$.

The main question which we will address in this dissertation, about binary 1-perfect codes, is for what pairs of numbers (r, k) does there exist a binary 1-perfect code C of length n having $r(C) = r$ and $k(C) = k$. This question was posed by Etzion and Vardy in [EV98].

It is already proved by Phelps for which pairs (r, k) there exists a binary 1-perfect code C of length 15 constructed using the Doubling construction and having $r(C) = r$ and kernel dimension $k(C) = k$, [Phe00]. We will see that it does not exist any 1-perfect code, C, of length 15 with rank $r(C) \leq 14$ having a kernel of dimension different than the one of the 1-perfect codes obtained in this way. We will assure this, after showing for each rank which are the lower and the upper bounds for the dimension of the kernel. For rank $r(C) = 15$, although it is known that the admissible kernel dimensions are 1, 2, 3, 4, 5, 6 and 7, it has been only proved that there exist binary 1-perfect codes of length 15 with kernels of dimensions 1, 2, 3, 4 and 5 (see [EV98]). Summarizing, for $n = 15$, the following table shows for which pairs $(r(C), k(C))$ there exists a 1-perfect code with these parameters. The question mark sign means it is not known if there exists a 1-perfect code with that rank and dimension of the kernel.

$r(C)$	$k(C)$								
11	11								
12		9	8	7					
13			8	7	6	5	4		
14			8	7	6	5	4	3	2
15				?	?	5	4	3	2	1

In general, we will establish the exact upper and lower bounds on the kernel dimension of binary 1-perfect codes of length $n = 2^m - 1$, once the rank is fixed,

except for one case. For 1-perfect codes with maximum rank, $r(C) = n$, called full-rank 1-perfect codes, and for all $m \geq 4$, we will give an upper bound but we will not prove this upper bound is tight. Despite this, it is already known that for all $m \geq 10$ this upper bound for full-rank 1-perfect codes is tight, [EV98]. So, the only cases which remain unsolved are for $4 \leq m < 10$.

In order to construct binary 1-perfect codes of length $n = 2^m - 1$ with all the different kernel dimensions, $k(C)$, between the upper and lower bounds for any rank, $r(C)$, we will use the Doubling and Switching constructions of 1-perfect codes. We obtain a large number of cases but we do not completely settle the question, partly because we need to construct full-rank 1-perfect codes with different $k(C)$. We only know how to construct full-rank 1-perfect codes of length $n = 2^m - 1$ with the lower kernel dimension, $k(C) = 1$, for all $m \geq 4$ [PL95] and with the upper kernel dimension, for all $m \geq 10$ [EV98].

The rank and the kernel of q-ary 1-perfect codes ($q \neq 2$) have not been studied before. On the rank, we will prove the generalization of Theorem 1.1 for q-ary 1-perfect codes, when q is a prime power. In order to show this result we will also generalize the approach of the Switching construction developed in [PL95] to construct q-ary 1-perfect codes. On the kernel, we will not give any result in this dissertation.

The overview of this dissertation is the following:

Chapter 2 exposes definitions and known results we will need in chapter 3, where we can find the new results we develop in this dissertation about binary 1-perfect codes. This chapter is organized as follows: first we introduce the binary 1-perfect codes as a family of codes such that the Hamming bound holds; in section 2.2 we show some well known results about linear binary 1-perfect codes, called also binary Hamming codes; in section 2.3 we develop some known constructions of nonlinear binary 1-perfect codes; in section 2.4 we describe some properties of these codes;

finally, in section 2.5, we give the known results about two of these properties, the rank and the kernel of binary 1-perfect codes, which are the main focus of this dissertation.

Chapter 3 and 4 are the core of this work, where the new contributions regarding binary and q-ary 1-perfect codes respectively are presented.

In chapter 3, we analyze the rank and the kernel dimension for binary 1-perfect codes of length $n = 2^m - 1$. First of all, we will prove some results on the structure of 1-perfect codes. Next, we will establish the lower and upper bounds on the kernel dimension of 1-perfect codes once the rank is fixed. We will show that these bounds are tight except the upper bound of full-rank codes if $m < 10$. We will study some results that will let us to obtain 1-perfect codes with different dimensions of the kernel between the lower and upper bound, for each possible rank. Since we will not be able to construct full-rank codes we will not completely settle the question of for what pairs of numbers (r, k) does there exist a binary 1-perfect code C of length n having $r(C) = r$ and $k(C) = k$.

In chapter 4, first of all we will review definitions and known properties and constructions of q-ary perfect codes. Then, we will generalize an approach of a well-known construction of binary 1-perfect codes, the Switching construction, to obtain q-ary 1-perfect codes. Finally, using this construction, we will establish the generalization of Theorem 1.1 for q-ary 1-perfect codes, that is the existence of q-ary 1-perfect codes of length $n = \dfrac{q^m - 1}{q - 1}$ for $m \geq 4$ and rank $n - m + s$ for each $s \in \{0, 1, \ldots, m\}$.

Finally, in chapter 5 we summarize the obtained results, we give the conclusions of this work and we point out possible future lines of research regarding rank and kernel of perfect codes.

Chapter 2

Definitions and previous results

In this chapter we expose definitions and known results that we will need in chapter 3, where we can find the new results we develop in this dissertation about binary 1-perfect codes. This chapter is organize as follows: first we introduce the binary 1-perfect codes as a family of codes such that the Hamming bound holds; in section 2.2 we show some well known results about linear binary 1-perfect codes, called also binary Hamming codes; in section 2.3 we develop some known constructions of nonlinear binary 1-perfect codes; in section 2.4 we describe some properties of these codes; finally, in section 2.5, we give the known results about two of these properties, the rank and the kernel of binary 1-perfect codes, which are the main focus of this dissertation.

2.1 Binary perfect codes

Let $\mathbb{F}_2^n$ be a vector space of dimension n over $GF(2)$. The *Hamming distance* between vectors $x, y \in \mathbb{F}_2^n$, denoted $d(x, y)$, is the number of coordinates in which x and y differ. The *Hamming weight* of x is given by $wt(x) = d(x, \mathbf{0})$, where $\mathbf{0}$ is the all-zero vector.

A *binary code*, C, of length n is simply a subset of $\mathbb{F}_2^n$. Without loss of generality

we shall assume, unless stated otherwise, that $\mathbf{0} \in C$ throughout this thesis. The elements of C are called *codewords*. The *minimum distance* of a code is the smallest distance between a pair of codewords. A code C is called *linear* if it is a linear space over a binary field. In other words, if x and y are codewords, then the resulting sum $x + y$ is contained in the code as well.

We say that a code is *even* if all its codewords have even weight. We shall define an *extended code* of the code C, denoted by C^*, to be the code resulting from adding an overall parity check digit to each codeword of C, thereby causing all of the codewords to have the same parity. We shall assume that the parity check digit shall cause each codeword to have even weight, so an extended code is an even code.

Two codes C_1, $C_2 \subset \mathbb{F}_2^n$ are *isomorphic* if there exists a permutation π such that $C_2 = \pi(C_1) = \{\pi(c) \ : \ c \in C_1\}$. They are *equivalent* if there exists a vector $a \in \mathbb{F}_2^n$ and a permutation π such that $C_2 = a + \pi(C_1) = \{a + \pi(c) \ : \ c \in C_1\}$. In the case where π is the identity permutation, then C_2 is said to be a *translate* or *coset* of C_1 if there exists some vector $a \in \mathbb{F}_2^n$ such that $C_1 + a = C_2$. If $C_1 = C_2$ then the mapping $c \mapsto a + \pi(c), \ \forall c \in C_1$ is said to be an automorphism of C_1. $Aut(C)$ will denote the group of all automorphisms of C.

Throughout this thesis, we shall utilize a particular family of codes, namely *binary perfect codes*. A binary code C of length n is *perfect* if for some integer $r \geq 0$ every $x \in \mathbb{F}_2^n$ is within distance r from exactly one codeword of C.

A perfect binary code attains the *sphere-packing* or *Hamming bound*, that is

$$|C| = \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r}}$$

where $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r}$ is the number of vectors of length n contain in a sphere of radius r around the codewords, [MS77]. We can also define a perfect binary code as a binary code such that the Hamming bound holds. A perfect binary code of length n can correct r errors, so they are also called *perfect r-error correcting codes* or *r-perfect codes*.

In 1973 it was proved independently by Tietäväinen [Tie73] and by Zinov'ev and Leont'ev [ZL73], that the only binary perfect codes of length n are:

- *trivial (binary) perfect codes* in cases $r = 0$ and $r = n$.
- *(binary) repetition code* in case $r = (n-1)/2$ with n odd.
- *(binary) Golay code* in case $r = 3$ with $n = 23$.
- *(binary) 1-perfect codes* in case $r = 1$ with $n = 2^m - 1$.

The binary Golay code is unique up to equivalence, [Ple68, Sno73, DG75]. The 1-perfect code with length $n = 7$ is also unique up to equivalence. Thus the only parameters for which there exists nonequivalent binary perfect codes are $r = 1$ and $n = 2^m - 1$, with $m \geq 4$, [Phe84a].

The linear 1-perfect codes are, again, unique up to equivalence, [MS77]. They are the well-known *Hamming codes*. We will explain more about these codes in the next section. Nonlinear 1-perfect codes have been constructed, for example, by Vasil'ev [Vas62], Solov'eva [Sol81], Mollard [Mol86], Phelps [Phe83, Phe84a], Bauer et al. [BGH83], Zinov'ev [Zin88], Etzion and Vardy [EV94], Phelps and LeVan [PL95] and Rifà [Rif99]. Some of these constructions are outlined in section 2.3.

The 1-perfect codes of length $n = 2^m - 1$ have dimension $k = n - m$, 2^{n-m} codewords and minimum distance 3.

A *binary 1-perfect partition* is a partition of the space $\mathbb{F}_2^n$ into $n+1$ binary 1-perfect codes $C_0, C_1, \ldots, C_n$. We can assume the zero vector is in C_0 and the vectors having a one in the i^{th} coordinate and zeros elsewhere, e_i, are in C_i, $\forall i \in \{1, \ldots, n\}$. Given a binary 1-perfect code C of length $n = 2^m - 1$ we know that there always exists $n+1$ translates of C, $C + e_0$, $C + e_1, \ldots,$ $C + e_n$, that form a binary 1-perfect partition of $\mathbb{F}_2^n$, we will call this the trivial partition. Similarly, the set $\mathbb{E}_2^{n+1}$, of all the even weight vectors in $\mathbb{F}_2^n$, can always be partitioned into even translates of an extended 1-perfect code $C^* \subset \mathbb{E}_2^{n+1}$.

Two partitions $C_0, C_1, \ldots, C_n$ and $D_0, D_1, \ldots, D_n$ are *isomorphic* if there exists a permutation π of the coordinates which maps the vectors of each class into the vectors of a class in the second partition, that is $\forall j \in \{1, \ldots, n\}$ $D_j = \{\pi(C_i)\}$ for some $i \in \{1, \ldots, n\}$. Two partitions $C_0, C_1, \ldots, C_n$ and $D_0, D_1, \ldots, D_n$ are *equivalent* if there exists a permutation π of the coordinates and a translation τ such that for all classes D_j there exists a class C_i such that $D_j = \{\pi(C_i) + \tau\}$.

2.2 Linear binary 1-perfect codes: Hamming codes

In this section we will see some known results about Hamming codes, that can be found for example in [MS77]. We will use these results in next chapters.

A *linear code* of length n is a linear space over $\mathbb{F}_2^n$. A matrix G is called a *generator matrix* of a linear code C if the rows of G form a basis for C. If C has length n and dimension k, then G is a $k \times n$ matrix.

The *dual code* of a linear code C of length n and dimension k, denoted by $C^\perp$ is the set of vectors which are orthogonal to all codewords of C, that is the set $C^\perp = \{v \in \mathbb{F}_2^n \ : \ \forall x \in C, \ v \cdot x = 0\}$. The dual code is a linear code of length n and dimension $n - k$. A matrix H is called a *parity-check matrix* of a linear code C if the rows of H form a basis for the dual code $C^\perp$. If C has length n and dimension k, then H is a $(n - k) \times n$ matrix.

A code C is *cyclic* if it is linear and if any cyclic shift of a codeword is also a codeword, that is, whenever $(c_0, c_1, \ldots, c_{n-1})$ is in C, then so is $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$. The polynomials $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$ of degree at most $n-1$ over $\mathbb{F}_2$ may be regarded as the words $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_2^n$. Thus a code C of length n can be represented as a set of polynomials over $\mathbb{F}_2$ of degree at most $n - 1$. If C is a cyclic code, there is only a monic polynomial $g(x)$ such that $C = (g(x))$, that is, $g(x)$ is a *generator polynomial* of C. If $r = deg(g(x))$, then the dimension of C is $n - r$.

A code of length $n = 2^m - 1$, $m \geq 2$, having parity-check matrix H whose columns consist of all nonzero vectors of length m is called a *Hamming code* of length $n = 2^m - 1$. This family of codes has minimum distance 3 and 2^{n-m} codewords, so attains the Hamming bound and is a family of 1-perfect codes. It is well-known that the Hamming codes are unique, up to equivalence.

If α is a primitive element of a finite field $GF(2^m)$ then $1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}$ are distinct and can be represented by distinct nonzero binary m-tuples. So a parity-check matrix of a Hamming code of length $n = 2^m - 1$ can be taken to be

$$H = (1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2})$$

where each entry is to be replaced by the corresponding column vector of length m.

The following result give us that there is a cyclic Hamming code of length $n = 2^m - 1$, for each $m \geq 2$.

Theorem 2.1. *Let α be a primitive element of $GF(2^m)$. The Hamming code given by the parity-check matrix $H = (1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2})$ is a cyclic code with generator polynomial $g(x) = m_\alpha(x)$, where $m_\alpha(x)$ is the minimal polynomial of α.*

The intersection of cyclic codes is a cyclic code. So, if we have two different cyclic Hamming codes $\mathcal{H}_1 = (m_\alpha(x))$ and $\mathcal{H}_2 = (m_\beta(x))$, where α and β are primitive elements of $GF(2^m)$, the code $\mathcal{C} = \mathcal{H}_1 \cap \mathcal{H}_2$ is a cyclic code such that $\mathcal{C} = (m_\alpha(x) \cdot m_\beta(x))$. In this case, $deg(m_\alpha(x) \cdot m_\beta(x)) = 2m$, so $dim(\mathcal{H}_1 \cap \mathcal{H}_2) = n - 2m$ and $dim(\mathcal{H}_1^\perp \cup \mathcal{H}_2^\perp) = 2m$. We will use this result in sections 2.4.3 and 3.3.

The *characteristic vector* of a subset V, where $V \subseteq \{1, 2, \ldots, n\}$, is the vector $\chi(V) = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ with $x_i = 1$ if and only if $i \in V$.

A *Steiner triple system* is an ordered pair (V, B) where V is a finite set of *points* or *symbols*, and B is a set of 3-element subsets of V called *blocks* or *triples*, such that each disordered pair of distinct elements of V is contained in exactly one triple of B. The *order* of a Steiner triple system (V, B) is the size of the set V, denoted by $|V| = n$. We will denote a Steiner triple system of order n by $STS(n)$.

The relation between STS's and Hamming codes is given by the following result:

Proposition 2.2. *If $\mathcal{H}_m$ is a Hamming code of length $n = 2^m - 1$, then the codewords of weight 3, called triples, form an $STS(n)$ if we identify the codewords with characteristic vectors of subsets of $\{1, 2, \ldots, n\}$.*

In fact, there is the same relation between STS's and 1-perfect codes (not necessarily linear) if C contains the zero vector. We will talk about this in section 2.4.1.

Another known result about Hamming codes is the following:

Theorem 2.3. *The codewords of weight 3 in the Hamming code are a spanning set for the code.*

A finite *projective geometry* consists of a finite set Ω of *points* and a collection of subsets called *lines*, which satisfies:

1. There is a unique line (denoted by (pq)) passing through any two distinct points p and q.

2. Every line contains at least 3 points.

3. If distinct lines L, M have a common point p, and if q, r are points of L not equal to p, and s, t are points of M not equal to p, then the lines (qt) and (rs) also have a common point.

4. For any point p there are at least two lines not containing p, and for any line L there are at least two points not on L.

A projective geometry $PG(t, q)$ can be constructed taken the points of Ω as the nonzero vectors of length $t + 1$ over $GF(q)$ with the rule that $(a_0, a_1, \ldots, a_t)$ and

$(\lambda a_0, \lambda a_1, \ldots, \lambda a_t)$ are the same point, where λ is any nonzero element of $GF(q)$. These are called *homogeneous coordinates* for the points. The number of points in Ω is $\frac{q^{t+1}-1}{q-1}$. The line through two distinct points $(a_0, a_1, \ldots, a_t)$ and $(b_0, b_1, \ldots, b_t)$ consists of the points $(\lambda a_0 + \mu b_0, \ldots, \lambda a_t + \mu b_t)$, where $\lambda, \mu \in GF(q)$ are not both zero. A line contains $q+1$ points since there are q^2-1 choices for λ, μ and each point appears $q-1$ times in $(\lambda a_0 + \mu b_0, \ldots, \lambda a_t + \mu b_t)$.

The coordinates of a Hamming code of length $n = 2^m - 1$ are in one-to-one correspondence with the columns of its parity-check matrix which in turn correspond to points in the binary projective space $PG(m-1, 2)$. The Steiner triple system associated to the Hamming code is in fact lines of the projective space. So, we can refer to coordinates being *independent* if the corresponding columns (points) are independent. Equivalently, we will say that a set of r points is independent if and only if the smallest subsystem containing these points is a system of order $2^r - 1$. In particular, if a set of r points is independent, then no three points are collinear.

2.3 Constructions of binary 1-perfect codes

In this section we briefly outline some known constructions of nonlinear binary 1-perfect codes.

Many constructions of 1-perfect codes exist. In [Sol00a] we can find a short summary of constructions which we include now. In 1962, Vasil'ev [Vas62] constructed a large number of nonequivalent 1-perfect codes. In 1977, Heden [Hed77] constructed 1-perfect codes which are not equivalent to the Vasil'ev codes. The class of 1-perfect codes described by Solov'eva in [Sol81] (they are not equivalent to the Vasil'ev codes) contains the Heden codes properly. Two years later, Phelps [Phe83] independently discovered Solov'eva's construction and generalized it [Phe84a]. A generalization of Vasil'ev's construction can be found in [Mol86]. In 1970 and 1988, Zinov'ev [Zin88] gave two constructions of 1-perfect codes with the method of concatenation. In 1988

Solov'eva presented another class of 1-perfect codes [Sol88] and generalized it with Vasil'ev in [VS95]. In 1994 Vardy and Etzion described a class of 1-perfect codes of full rank [EV94]. There are also three codes of length 15 (Bauer et al. [BGH83]) and three codes of length 15 described by Heden in [Hed94]. In 1995 Phelps and LeVan [PL95] presented 1-perfect codes with all possible sizes of kernels. In 1996 Avgustinovich and Solov'eva [AS97] gave a construction of 1-perfect codes which led to a new lower bound on the number of different 1-perfect codes. In 1996 Lobstein and Zinov'ev generalized the concatenation construction of 1-perfect codes [LZ97]. In 1997 Rifà and Pujol [RP97] constructed a family of 1-perfect codes called perfect additive propelinear codes. In 1999 Borges and Rifà [BR99] give a full characterization of 1-perfect additive codes. In the same year, Rifà [Rif99] constructed 1-perfect codes from some Steiner triple systems.

2.3.1 Vasil'ev construction

Nonlinear 1-perfect codes were first constructed by Vasil'ev, [Vas62].

For $v \in \mathbb{F}_2^n$, let $p(v) = wt(v) \bmod 2$. Let C_n be a 1-perfect binary code of length $n = 2^m - 1$. Let $f : C_n \to \{0, 1\}$ be an arbitrary mapping, such that $f(\mathbf{0}) = 0$ and $f(c_1) + f(c_2) \neq f(c_1 + c_2)$ for some $c_1, c_2, c_1 + c_2 \in C_n$.

Proposition 2.4. [Vas62] *The code C_{2n+1} defined by*

$$C_{2n+1} = \{(v|v + c|p(v) + f(c)) \ : \ v \in \mathbb{F}_2^n, \ c \in C_n\}$$

where $(\cdot|\cdot)$ denotes concatenation, is perfect.

We can construct $2^{|C|-1}$ 1-perfect codes of length n from a 1-perfect code C of length $(n-1)/2$ using the above construction. This will give 2^{15} different 1-perfect codes of length 15 (containing the zero vector) but Herget [Her82] prove that there are only 19 nonequivalent codes.

The following construction, due to Mollard [Mol86], is in a sense a generalization of Proposition 2.4.

For $x = (x_{11}, x_{12}, \ldots, x_{1n_2}, x_{21}, x_{22}, \ldots, x_{n_1n_2}) \in \mathbb{F}_2^{n_1n_2}$, define the generalized parity functions $p_1(x) = (\sigma_1, \sigma_2, \ldots, \sigma_{n_1}) \in \mathbb{F}_2^{n_1}$ and $p_2(x) = (\sigma'_1, \sigma'_2, \ldots, \sigma'_{n_2}) \in \mathbb{F}_2^{n_2}$ by setting $\sigma_i = \sum_{j=1}^{n_2} x_{ij}$ and $\sigma'_j = \sum_{i=1}^{n_1} x_{ij}$. Let C_1 and C_2 be two 1-perfect codes of lengths n_1 and n_2, respectively. Let $f : C_1 \to \mathbb{F}_2^{n_2}$ be an arbitrary mapping.

Proposition 2.5. [Mol86] *The code F defined by*

$$F = \{(x|c_1 + p_1(x)|c_2 + p_2(x) + f(c_1)) \ : \ x \in \mathbb{F}_2^{n_1n_2},\ c_1 \in C_1,\ c_2 \in C_2\}$$

is a 1-perfect code of length $n = n_1n_2 + n_1 + n_2$.

Note that for $n_2 = 1$, Proposition 2.5 reduces to Vasil'ev's construction.

2.3.2 Doubling construction

The following construction of 1-perfect codes of length $2n + 1$ from 1-perfect codes of length n is due to Phelps [Phe83] and Solv'eva [Sol81], so it is also called Phelps-Solov'eva construction.

Let e_i denote the binary vector of length n having all components equal to zero, except the i^{th} component, which contains a one. Let $X \subset \mathbb{F}_2^n$ and $Y \subset \mathbb{F}_2^m$. Then, the direct sum of X and Y, denoted by $X \oplus Y \in \mathbb{F}_2^{n+m}$ is as follows:

$$X \oplus Y = \{(x, y) \ : \ x \in X,\ y \in Y\}$$

Let C_1 be a 1-perfect code of length n and C_2^* be an extended 1-perfect code of length $n + 1$.

Proposition 2.6. [Phe83, Sol81] *The code*

$$C = (C_1 \oplus C_2^*) \bigcup_{i=1}^{n} (C_1 + e_i \oplus (C_2 + e_{\pi(i)})^*)$$

where π is a permutation on the set $\{1, 2, \ldots, n\}$, is a 1-perfect code of length $2n+1$.

In section 3.4, we will establish results on the rank and the kernel of binary 1-perfect codes constructed with this construction. We will use these results to construct binary 1-perfect codes with different ranks and dimensions of the kernel, in sections 3.3, 3.5 (or see [PV01a]) and 3.7.

The next proposition is a more general variant of the above construction.

Let $C_0^*, C_1^*, \ldots, C_n^*$ and $D_0^*, D_1^*, \ldots, D_n^*$ be partitions of $\mathbb{E}_2^{n+1}$ and $\mathbb{F}_2^{n+1} \backslash \mathbb{E}_2^{n+1}$, respectively, into extended 1-perfect codes by extending with an even parity coordinate the first ones and with an odd parity coordinate the second ones. Let π be a permutation on the set $\{0, 1, \ldots, n\}$.

Proposition 2.7. [Phe83, Sol81] *The code C defined by*

$$C = \{(c|d) \ : \ c \in C_i^*, \ d \in D_{\pi(i)}^*\}$$

is an extended 1-perfect code of length $2n + 2$.

Puncturing any coordinate of C gives a 1-perfect code of length $2n + 1$.

Let R be an extended 1-perfect code of length k. For each $r \in R$, let Q_r be a minimum distance 2 code of length k over an alphabet of $n + 1$ symbols, with $|Q_r| = (n + 1)^{k-1}$.

Proposition 2.8. [Phe84a] *The code P defined by*

$$P = \{(c_1|c_2|\cdots|c_k) \ : \ c_i \in C_{j_i}^{r_i}, \ r = (r_1, r_2, \ldots, r_k) \in R, \ (j_1, j_2, \ldots, j_k) \in Q_r\}$$

is an extended 1-perfect code of length $k(n + 1)$.

Puncturing any coordinate of P gives a 1-perfect code of length $k(n + 1) - 1$.

Note that for $k = 2$, R is an extended 1-perfect code consisting of a single vector 01, and the code Q_r is in effect a permutation on the set $\{0, 1, \cdots, n\}$. Thus Proposition 2.7 is a special case of Proposition 2.8.

The following construction, due to Etzion and Vardy [EV94], is in some sense a generalization of the construction of Phelps [Phe83] and Solov'eva [Sol81].

Let V be a subset of $\mathbb{F}_2^n$. Let $\mathcal{A} = \{A_1, A_2, \ldots, A_k\}$ and $\mathcal{B} = \{B_1, B_2, \ldots, B_k\}$ be two ordered sets of subsets of V. For $v \in V$, define

$$\Lambda_A(v) = \{i \ : \ v \in A_i\} \qquad \Lambda_B(v) = \{i \ : \ v \in B_i\}$$

where $A_i \in \mathcal{A}$ and $B_i \in \mathcal{B}$. We say that $\mathcal{A}$ and $\mathcal{B}$ form a *perfect segmentation* of order k of the set V, if both $\cup_{i\in\Lambda_B(v)} A_i$ and $\cup_{i\in\Lambda_A(v)} B_i$ are 1-perfect codes of length n, for all $v \in V$.

Proposition 2.9. [EV94] *Let $\mathcal{A}$ and $\mathcal{B}$ be a perfect segmentation of $\mathbb{F}_2^n$. The code C defined by*

$$C = \{(u|v) \ : \ u \in A_i^*, \ v \in B_i\}$$

is a 1-perfect code of length $2n + 1$.

Note that any two partitions of $\mathbb{F}_2^n$ into $n + 1$ 1-perfect codes form a perfect segmentation of $\mathbb{F}_2^n$. Thus Proposition 2.7 is a special case of Proposition 2.9. In fact, $n+1$ is the minimum order of any perfect segmentation of $\mathbb{F}_2^n$. In [EV94], it is shown that perfect segmentation of higher order exist.

2.3.3 Switching construction

This construction consists on starting with a 1-perfect code C of length n and switching out one specially selected set of codewords $S \subset C$ for another set of vectors S'. The resulting code $C' = (C \backslash S) \cup S'$ would be a 1-perfect code.

Let C and D be two (disjoint) 1-perfect codes. In general, we choose $D = C + e_i$ a translate of C. We can form a bipartite graph G with vertex set $C \cup D$ and edges $[x, y]$ for $x \in C$ and $y \in D$ where $d(x, y) < 3$.

Proposition 2.10. *If C is a 1-perfect code and $M \cup M + e_i$ is a nontrivial component in the graph G, then $C' = (C \backslash M) \cup (M + e_i)$ is also a 1-perfect code.*

Another equivalent formulation of this construction, due to Solov'eva [Sol88], is the following:

For a 1-perfect code of length n, we define the *minimum distance graph* of C as a graph $G(C) = (C, E)$ with the codewords in C as vertices and edges $[x, y] \in E$ if and only if $d(x, y) = 3$.

We define a subgraph $G_i(C) = (C, E_i)$ as the subset E_i of all the edges $[x, y]$ in $G(C)$ where codewords x and y disagree with the i^{th} coordinate. Solov'eva in [Sol88] introduced this subgraph $G_i(C)$ and established that the number of components m satisfies the following inequalities,

$$2 \leq m \leq \frac{2^{\frac{n+1}{2}}}{n+1}$$

so the subgraph G_i is not connected.

Proposition 2.11. [Sol88] *If C is a 1-perfect code and $S \subset C$ is a component of G_i, then $C' = (C \backslash S) \cup (S + e_i)$ is also a 1-perfect code.*

Another approach of the switching construction can be found in [AS97] or [Sol00b]. A *neighborhood* $K(M)$ of a set M in $\mathbb{F}_2^n$ is the union of spheres of radius 1 with centers at the vectors of M. We can also say that a set $C \subseteq F_2^n$ is a *1-perfect code* of length n if $K(C) = \mathbb{F}_2^n$ and for any $x, y \in C$ one has $K(x) \cap K(y) = \emptyset$. A set $M \subset C$ is an *i-component* of the 1-perfect code C if $K(M) = K(M + e_i)$. It is easy to see the following result:

Proposition 2.12. [AS97] *If C is a 1-perfect code and $M \subset C$ is an i-component, then $C' = (C \backslash M) \cup (M + e_i)$ is also a 1-perfect code.*

In the next chapters we will use the following approach to the switching construction due to Phelps and LeVan [PL95].

Define T_i to be the linear subcode of a Hamming code, generated by the codewords of weight 3 having a 1 in the i^{th} component. There will be a path from x to y in G_i if and only if there is a sequence of codewords of weight 3 $t_1, t_2, \ldots, t_s \in T_i$ such that $x + t_1 + t_2 + \cdots + t_s = y$ which is equivalent to saying if and only if $y \in T_i + x$. Thus $T_i + x$ is a component of G_i in the graph of the Hamming code. We can say that in the Hamming code the components in the subgraph G_i are cosets of a linear subcode.

Proposition 2.13. [PL95] *Given a Hamming code H_m of length $n = 2^m - 1$, let T_i, $x_i \in H_m$. Then,*

$$C = (H_m \backslash (T_i + x_i)) \cup (T_i + x_i + e_i)$$

is a nonlinear 1-perfect code of length n, $\forall i \in \{1, \ldots, n\}$.

This idea has been used to solve a number of important problems, [EV94, PL95, AS95, AS96]. For example, in [AS97], Avgustinovich and Solov'eva used this to obtain an important lower bound on the number of nonequivalent 1-perfect codes of a given length n. In this article, they raise the question of if all 1-perfect codes can be obtained from the Hamming code by a sequence of such switches. In [PL99], Phelps and LeVan present a 1-perfect code of length 15 and show that it can not be obtained from the Hamming code by switching. In [Sol00b] it is showed that the Vasil'ev's construction is a switching construction.

2.4 Properties of binary 1-perfect codes

In [Sol00b] we can find a short summary of properties of 1-perfect codes. In this section we will only see the ones that we will use in the next chapters. In the next section we will talk specifically about two properties that are the main focus of this dissertation: rank and kernel.

Let C be a code of length n, and let A_i be the number of codewords on distance i from a fixed codeword in C. The numbers $A_0,\ A_1, \ldots,\ A_n$ are called the *weight distribution* of C. Of course $A_0 + A_1 + \cdots + A_n = |C|$. A code is *distance invariant* if the number A_i does not depend on the choice of the codeword.

It is easy to see that the linear codes are distance invariants. However, in a nonlinear code this need not be true. For example, the nonlinear code given by the following codewords, $C = \{(0,0),\ (0,1),\ (1,1)\}$, is not distance invariant.

In 1959 Shapiro and Slotnik [SS59] proved the following results:

Proposition 2.14. *If a nonlinear code is distance invariant, and it contains the all ones vector, then for every word contained in the code, its complement is also contained in the code.*

Theorem 2.15. *The (extended) 1-perfect codes are distance invariant codes. Thus, the complement of a codeword is again a codeword.*

If the complement of a codeword is again a codeword, we will say that the code is *self-complementary*.

2.4.1 STS and 1-perfect codes

A *Steiner triple system* is an ordered pair (V, B) where V is a finite set of *points* or *symbols*, and B is a set of 3-element subsets of V called *blocks* or *triples*, such that each disordered pair of distinct elements of V is contained in exactly one triple of B. The *order* of a Steiner triple system (V, B) is the size of the set V, denoted by $|V| = n$. We will denote a Steiner triple system of order n by $STS(n)$.

The existence problem of $STS(n)$ was solved by Kirkman [Kir47], who proved the following result. We can also see its proof in many books of design theory, for example in [HP85] or [LR97].

Proposition 2.16. [Kir47] *An $STS(n)$ exists if and only if $n \equiv 1,\ 3\ (mod\ 6)$.*

Given two $STS(n)$, (V, B) and (V, B'), we will say that they are *isomorphic* if there exists a permutation π on the set V such that $B = \pi(B')$. We will denote by $(V, B) \cong (V, B')$.

For $n = 3, 7$ and 9, there only exist one $STS(n)$ up to isomorphisms. There are two $STS(13)$ up to isomorphisms. For $n = 15$, there are 80 nonisomorphic $STS(15)$, [WCC19]. In [Gib76] and [Rif99], we can see two methods of uniquely identifying the 80 nonisomorphic $STS(15)$. For $n = 31$, there are of the order of 10^{200}. The methods of uniquely identifying the nonisomorphic $STS(15)$ are not useful for $n > 15$.

We say that (V, B) is a *partial Steiner triple system* if every pair of elements of V is in at most one triple of B.

A *Steiner quadruple system* is an ordered pair (V, B) where V is a finite set of points, and B is a set of 4-element subsets of V called *quadruples*, such that each 3-element subset of V is contained in exactly one quadruple of B. We will denote a Steiner quadruple system by $SQS(n)$, where $|V| = n$.

The *characteristic vector* of a subset V, where $V \subseteq \{1, 2, \ldots, n\}$, is the vector $\chi(V) = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ with $x_i = 1$ if and only if $i \in V$.

The relation between STS and 1-perfect codes is given by the following result that we can find in [GvT75] or [Til76].

Proposition 2.17. *If C is a 1-perfect code of length n containing the zero vector, then the minimum weight codewords (of weight 3) in the code form an $STS(n)$ if we identify the codewords with characteristic vectors of subsets of $\{1, 2, \ldots, n\}$. Similarly, the words of weight 4 in C^* form a $SQS(n + 1)$.*

A *derived Steiner triple system* is a Steiner triple system which can be extended to a Steiner quadruple system. For length 15, it has already been shown [DSd85] that all 80 nonisomorphic $STS(15)$ are derived. However, the problem of whether every $STS(n)$ is derived or not is still unsolved for all admissible $n > 15$.

Any 1-perfect code C of length n can be extended to a code C^* of length $n+1$ by adding an overall parity check bit. Thus, the codewords of weight 3 in C that have become codewords of weight 4 in C^*, along with the codewords of weight 4 already contained in the code, form a $SQS(n+1)$. This show us that if we have a 1-perfect code containing a Steiner triple system, then this must necessarily be a derived Steiner triple system. We will say that a Steiner triple system is *perfect* if it is contained in a 1-perfect code of length n.

In [Phe84a], Phelps show that at least 23 of these (derived) $STS(15)$ are perfect. In [LeV95], it is shown that 8 more $STS(15)$ are perfect using switching techniques. In [Rif99], Rifà constructed 1-perfect partitions of $\mathbb{F}_2^n$ and, therefore, 1-perfect codes from some $STS(n)$ called *well-ordered*.

2.4.2 The dual code

By the *dual* or *orthogonal code* of a code C of length n, denoted by $C^\perp$, we mean the dual of the subspace spanned by C, that is the set of vectors which are orthogonal to all codewords of C

$$C^\perp = \{u \in \mathbb{F}_2^n \ : \ u \cdot v = 0, \ \forall v \in C\}$$

The dimension of $C^\perp$ is $n - r(C)$, where $r(C)$ is the dimension of the subspace spanned by C, $\langle C \rangle$. We will say that $r(C)$ is the *rank* of C and that C is a *full-rank* code if $r(C) = n$.

Proposition 2.18. [BGH83] *Let C be a 1-perfect code of length $n = 2^m - 1$. Any non-zero codeword in the dual code $C^\perp$ must have weight $(n+1)/2 = 2^{m-1}$.*

In [EV94], Etzion and Vardy give a necessary and sufficient condition for a code C of length $n = 2^m - 1$ to be perfect if there exists a vector $w \in C^\perp$ of weight $(n+1)/2 = 2^{m-1}$. Without loss of generality assume that the nonzero entries of w are in the first $(n+1)/2$ positions, and hence for each $(u|v) \in C$ such that $v \in \mathbb{F}_2^{(n-1)/2}$,

$wt(u)$ is even. Define

$$T(u) = \{v \in \mathbb{F}_2^{(n-1)/2} \ : \ (u|v) \in C\}$$

$$H(v) = \{u \in \mathbb{E}_2^{(n+1)/2} \ : \ (u|v) \in C\}$$

Proposition 2.19. [EV94] *The code C is perfect if and only if the following two conditions hold.*

1. $\forall u \in \mathbb{E}_2^{(n+1)/2}$, $T(u)$ *is a perfect code of length* $(n-1)/2$.
2. $\forall v \in \mathbb{F}_2^{(n-1)/2}$, $H(v)$ *is an extended perfect code of length* $(n+1)/2$.

Notice that if C is a 1-perfect code, by Proposition 2.18 all the nonzero vectors in $C^\perp$ have weight 2^{m-1}. Then, if $C^\perp \neq \{0\}$, that is if $r(C) < n$, we can construct 1-perfect codes $T(u)$ and extended 1-perfect codes $H(v)$. Actually, the following result is also true for such a perfect codes.

Given a code C, we can shorten a code by considering the subcode

$$C_I = \{c \in C \ : \ c_i = 0, \ \forall i \in I\}$$

The *support* of a nonzero vector $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ is the subset of indexs of its nonzero coordinates, $supp(x) = \{i \ : \ x_i \neq 0\}$.

Theorem 2.20. *Let C be a 1-perfect code. For any non-zero codeword w in the dual code of C, the shortened code $C_{supp(w)}$ is a 1-perfect code of length* $(n-1)/2$.

2.4.3 Intersections of 1-perfect codes

Given two binary codes C_1, C_2 of the same length, the *intersection number* of C_1 and C_2 is defined as $\eta(C_1, C_2) = |C_1 \cap C_2|$.

The largest possible intersection number of 1-perfect codes was determined in [EV94], where Etzion and Vardy showed that if C_1 and C_2 are two distinct 1-perfect codes of length $n = 2^m - 1$, then

$$\eta(C_1, C_2) \leq 2^{2^m - m - 1} - 2^{2^{m-1} - 1}$$

and this bound is tight, for all $m \geq 3$. There exist perfect codes C_1, C_2 of length 2^m-1 such that $\eta(C_1, C_2) = 2^{2^m-m-1}-2^{2^{m-1}-1}$. This bound was established using a switch of one i-component in Vasil'ev's construction. Moreover using multiple switchings they obtained intersection numbers of the form $k2^{2^{m-1}-1}$ for all $k = 1, 2, \ldots, 2^{2^{m-1}-m} - 1$, [EV98].

The smallest possible (nonzero) intersection number of two 1-perfect codes is 2 because since all perfect codes are self-complementary, their intersection must have even cardinality. This implies that if C_1, C_2 are 1-perfect codes and $\eta(C_1, C_2) \neq 0$, then $\eta(C_1, C_2) \geq 2$. In [EV98], Etzion and Vardy proved that, for each $m \geq 3$, there exist two 1-perfect codes C_1, C_2 of length $2^m - 1$ such that $\eta(C_1, C_2) = 2$. This lower bound was constructed exploring a switch for the concatenation construction of the Hamming code.

It follows from these results that the intersection number of any two distinct 1-perfect codes C_1, C_2 of length $n = 2^m - 1$ is in the range

$$2 \leq \eta(C_1, C_2) \leq 2^{2^m-m-1} - 2^{2^{m-1}-1}$$

and both bounds are achievable for all $m \geq 3$. In [EV98] is given many different intersection numbers but the problem of enumerating all possible intersection numbers of 1-perfect codes remains open. Even for the case of length 15, a complete enumeration does not seem to be easy.

However, in [EV98] Etzion and Vardy provide a complete solution to this problem, that is, to find all possible intersection numbers, if the perfect codes are linear codes, namely, the Hamming codes of length $n = 2^m - 1$. Now, we will explain the solution to this problem and the construction of these codes by induction. We will use it in section 3.3 to prove the main result in that section.

Let $\mathcal{H}_1$, $\mathcal{H}_2$ be two Hamming codes of length $n = 2^m - 1$. Since Hamming codes are unique, $\mathcal{H}_1$ and $\mathcal{H}_2$ are necessarily isomorphic. Since both codes are linear, their intersection number is necessarily a power of 2.

For $m = 3$ and $n = 7$, it is easy to find specific permutation such that $\eta(\mathcal{H}_1, \mathcal{H}_2) = 2, 4$ or 8. For example, let $\mathcal{H}_1$ the code defined by the parity-check matrix whose columns are ordered lexicographically, and let $\mathcal{H}_2$ be a code defined by the parity-check matrix

$$\begin{bmatrix} 0011011 \\ 0110110 \\ 1000111 \end{bmatrix} \quad or \quad \begin{bmatrix} 0011011 \\ 0110101 \\ 1000111 \end{bmatrix} \quad or \quad \begin{bmatrix} 0001111 \\ 0110011 \\ 1100101 \end{bmatrix} \tag{2.1}$$

respectively. In fact, it is showed that a similar situation occurs for all $m \geq 3$, namely, all the powers of 2 in the range $2^{n-2m}, 2^{n-2m+1}, \ldots, 2^{n-m-1}$ are attainable as intersection numbers of distinct Hamming codes of length $n = 2^m - 1$.

Let H_1, H_2 be parity-check matrices of the Hamming codes $\mathcal{H}_1$ and $\mathcal{H}_2$ of length $n = 2^m - 1$. Then $\mathcal{C} = \mathcal{H}_1 \cap \mathcal{H}_2$ is a linear code, whose parity-check matrix is given by

$$H = \left[\frac{H_1}{H_2}\right]$$

We shall henceforth write $H = H_1 \| H_2$ to denote this structure. It is obvious that $rank(H) \leq 2m$, since H_1 and H_2 each have m rows, and therefore,

$$\eta(\mathcal{H}_1, \mathcal{H}_2) = |\mathcal{C}| = 2^{n-rank(H)} \geq 2^{n-2m}$$

It is also obvious that $\eta(\mathcal{H}_1, \mathcal{H}_2) \leq 2^{n-m-1}$ if the codes $\mathcal{H}_1$ and $\mathcal{H}_2$ are distinct.

Lemma 2.21. [EV98] *For each $m \geq 3$, there exist two Hamming codes $\mathcal{H}_1$, $\mathcal{H}_2$ of length $n = 2^m - 1$ such that $\eta(\mathcal{H}_1, \mathcal{H}_2) = 2^{n-2m}$.*

We could take $\mathcal{H}_1$ and $\mathcal{H}_2$, for example, two different cyclic Hamming codes $\mathcal{H}_1 = (m_\alpha(x))$ and $\mathcal{H}_2 = (m_\beta(x))$, where α and β are primitive elements of $GF(2^m)$. See the comments after the Theorem 2.1 in section 2.2. In [EV98] these Hamming codes are constructed in a different way.

The following theorem give the solution of the intersection number for Hamming codes. We will also include the proof to give the construction of these Hamming codes.

Theorem 2.22. [EV98] *For each $m \geq 3$, there exist two Hamming codes $\mathcal{H}_1$, $\mathcal{H}_2$ of length $n = 2^m - 1$, such that*

$$\eta(\mathcal{H}_1, \mathcal{H}_2) = 2^{n-r} \quad for \quad r = m+1, m+2, \ldots, 2m$$

Proof: The proof is by induction on m. The induction basis for $m = 3$ is established in (2.1). Now assume that, for each $r = m, m+1, \ldots, 2(m-1)$, there exist parity-check matrices H_1' and H_2' of two Hamming codes of length $2^{m-1} - 1$, such that $rank(H_1' \| H_2') = r$. Take

$$H_1 = \begin{bmatrix} 0 \cdots 0 & 1 & 1 \cdots 1 \\ H_1' & 0 & H_1' \end{bmatrix} \qquad H_2 = \begin{bmatrix} 0 \cdots 0 & 1 & 1 \cdots 1 \\ H_2' & 0 & H_2' \end{bmatrix}$$

It is easy to see that H_1, H_2 are parity-check matrices of isomorphic Hamming codes of length $2^m - 1$, and that

$$rank(H_1 \| H_2) = rank(H_1' \| H_2') + 1 = r + 1$$

Thus, all ranks in the range $r + 1 = m + 1, m + 2, \ldots, 2m - 1$ are attainable. Finally, the rank of $2m$ is also attainable by Lemma 2.21, which completes the induction. ∎

2.5 Rank and kernel of binary 1-perfect codes

The nonlinear 1-perfect codes are not fully classified. Two structural properties of nonlinear codes are the *rank* and *kernel*. They have been defined in order to study these codes.

The *rank* of C, $r(C)$, is simply the dimension of the subspace spanned by C, $\langle C \rangle$. We say that C is of *full-rank* if $r(C) = n$ or equivalently if $\langle C \rangle = \mathbb{F}_2^n$

The *kernel* of C is defined as: $K_C = \{x \in \mathbb{F}_2^n \ : \ C = C + x\}$, in other words, it is the subset of $\mathbb{F}_2^n$ such that any vector in it leaves C invariant under translation. If the zero vector is in C, then the kernel of C is actually contained in C, and moreover,

the kernel is a linear subcode of C. Thus, if C is linear, then the kernel of C is itself. In general, C can be written as the union of cosets of K_C and K_C is the largest such linear code for which this is true [BGH83]. It is also easy to prove that the kernel of a code is the intersection of all maximal linear subcodes in that code. We will denote the dimension of the kernel of C by $k(C)$.

Both the rank and kernel of 1-perfect codes have been studied. In this section, we will give some known results about these two parameters. We can also find a summary in [Sol00b].

Ranks of binary 1-perfect codes were investigated by Etzion and Vardy [EV94, EV98]. In [EV94], they proved the following result:

Theorem 2.23. [EV94] *For all $m \geq 4$ there exists a binary 1-perfect code, C, of length $n = 2^m - 1$ with a rank of dimension $r(C) = n - m + s$ for each $s \in \{0, 1, \ldots, m\}$.*

In 1994, Heden [Hed94] constructed three 1-perfect codes of length 15 which had kernels of dimension 1, 2 and 3. In 1995, Phelps and LeVan [PL95] obtained 1-perfect codes with kernels of all possible sizes, by multiple special switching.

Theorem 2.24. [PL95] *For all $m \geq 4$ there exists a binary 1-perfect code, C, of length $n = 2^m - 1$ having a kernel of dimension j if and only if $j \in \{1, 2, \ldots, n - m - 2, n - m\}$.*

The rank and kernel are known to be related, [EV98]. The first relation is established in [BGH83].

Proposition 2.25. [BGH83] *For a 1-perfect code C, $C^{\perp} \subset K_C$ and*

$$k(C) + r(C) \geq n + 1$$

This follows easily from two facts: first, the complement of any codeword is always a codeword, so the all ones word is always in the kernel; second, the dual of C is always a subcode of the kernel K_C.

The question which we will address in chapter 3 is, for what pairs of numbers (r, k) does there exist a 1-perfect code C of length n having $r(C) = r$ and $k(C) = k$. This question was posed by Etzion and Vardy in [EV98].

In section 2.5.1 and 2.5.2 we describe the construction of the 1-perfect codes given by Theorem 2.23 and Theorem 2.24 respectively. In section 2.5.3 we will give some known results about full-rank 1-perfect codes and kernels, since in chapter 3 we will not be able to construct such that codes with kernels of different dimensions. In section 2.5.4 we will establish the known results for length $n = 15$.

2.5.1 Ranks of binary 1-perfect codes

In [EV94], Etzion and Vardy proved the following results about the rank of 1-perfect codes obtained from different constructions.

Let $V(n)$ be the set of all the 1-perfect codes of length n that may be obtained using the Vasil'ev construction, see Proposition 2.4.

Lemma 2.26. [EV94] *For* $C_{2n+1} \in V(2n+1)$, $rank(C_{2n+1}) = rank(C_n) + n + 1$.

Let $M(n)$ be the set of all the 1-perfect codes resulting from the construction due to Mollard and given by Proposition 2.5.

Lemma 2.27. [EV94] *For* $F \in M(n)$, $rank(F) \leq n + rank(C_1) - n_1$.

Let $P_k(k(n+1)-1)$ the set of all the 1-perfect codes obtained by puncturing the codes given by Proposition 2.8.

Lemma 2.28. [EV94] *For* $C \in P_k(k(n+1)-1)$, $rank(C) \leq k(n+1) + rank(R) - k$.

Using the construction given by Proposition 2.9, it is possible to construct 1-perfect codes of length n and any rank in the range of $n - m + 1$ to $n - 1$ in the following way, [EV94].

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two isomorphic Hamming codes of length $n' = (n-1)/2$ and rank $n' - m'$, where $m' = m - 1$, such that $C' = \mathcal{H}_1 \cap \mathcal{H}_2$ has cardinality $2^{n'-m'-1}$. Then $\mathcal{H}_1 = C' \cup (c_1 + C')$ and $\mathcal{H}_2 = C' \cup (c_2 + C')$ for some $c_1 \in \mathcal{H}_1 \backslash C'$ and $c_2 \in \mathcal{H}_2 \backslash C'$. Let $V = \mathcal{H}_1 \cup (c_2 + \mathcal{H}_1) = \mathcal{H}_2 \cup (c_1 + \mathcal{H}_2)$. It is easy to prove that $\{A_1, A_2, A_3, A_4\}$ and $\{B_1, B_2, B_3, B_4\}$ form a perfect segmentation of V taken $A_1 = C'$, $A_2 = c_1 + C'$, $A_3 = c_2 + C'$, $A_4 = c_1 + c_2 + C'$ and $B_1 = \mathcal{H}_1$,$B_2 = \mathcal{H}_2$, $B_3 = c_1 + \mathcal{H}_2$, $B_4 = c_2 + \mathcal{H}_1$. Let $(a_0 + \mathcal{H}_1)$, $(a_1 + \mathcal{H}_1), \ldots,$ $(a_{n'} + \mathcal{H}_1)$ and $(b_0 + \mathcal{H}_1), (b_1 + \mathcal{H}_1), \ldots, (b_{n'} + \mathcal{H}_1)$ be two partitions of $\mathbb{F}_2^{n'}$ into cosets of $\mathcal{H}_1$, such that $a_0 = b_0 = \mathbf{0}$ and $a_1 = b_1 = c_2$. Define a perfect segmentation of $\mathbb{F}_2^{n'}$ by completing $\{A_1, A_2, A_3, A_4\}$ and $\{B_1, B_2, B_3, B_4\}$ with $A_{i+3} = a_i + \mathcal{H}_1$ and $B_{i+3} = b_i + \mathcal{H}_1$, for $i = 2, 3, \ldots, n'$.

The rank of a 1-perfect code constructed by applying Proposition 2.9 to this perfect segmentation, is given by

$$rank(C) = 2 \cdot rank(\mathcal{H}_1) + rank(\Gamma)$$

where $\Gamma = \{(\mathbf{0}|\mathbf{0}), (c_2|\mathbf{0}), (\mathbf{0}|c_2)\} \cup \{(a_i|b_i) \ : \ i = 2, 3, \ldots, n'\}$. Obviously, $m \leq rank(\Gamma) \leq 2(m-1)$ and the vectors $a_2, a_3, \ldots, a_{n'}$ and $b_2, b_3, \ldots, b_{n'}$ can be always chosen such as to make Γ have any rank in the above range. Since $rank(\mathcal{H}_1) = n' - m'$, the rank of C can be made to attain any value in the range of $n - m + 1$ to $n - 1$

This construction does not give full-rank 1-perfect codes. However it is shown that for $n = 15$, it gives a 1-perfect code of rank 14 which can not be constructed using neither Vasil'ev construction (Proposition 2.4) nor its generalization by Mollard (Proposition 2.5) nor any of Phelps constructions (Proposition 2.8). We can see this from Lemmas 2.26, 2.27 and 2.28.

Using switchings of i-components, Etzion and Vardy [EV94] also constructed full-rank 1-perfect codes of length n from the Hamming code for all admissible n. In fact, this construction gives 1-perfect codes of all possible ranks. To describe these codes we will give the approach developed by Phelps and LeVan in [PL95]. We will also use this technique to generalize this result for q-ary 1-perfect codes in chapter 4.

Let T_i be the linear subcode of a Hamming code, generated by the codewords of weight 3 having a 1 in the i^{th} component. The following result allow us to make different switches as the described by Proposition 2.13.

Lemma 2.29. [PL95] *Let H_m be a binary Hamming code of length $n = 2^m - 1$, $m \geq 4$, with $\{1, 2, \ldots m\}$ as a set of its independent points. Then, there exists $x_1, x_2, \ldots, x_m$ such that for $i, j \in \{1, 2, \ldots, m\}$, $T_i + x_i$ is disjoint from $T_j + x_j$ for $i \neq j$.*

The following result is not stated this way in [PL95], but it is proved.

Proposition 2.30. [PL95] *Let H_m be a binary Hamming code of length $n = 2^m - 1$, $m \geq 4$, with $\{1, 2, \ldots, m\}$ as a set of its independent points. Let*

$$C' = \left(H_m \setminus \bigcup_{i=1}^{s} (T_i + x_i)\right) \cup \bigcup_{i=1}^{s} (T_i + x_i + e_i)$$

Then, $r(C') = n - m + s$, $\forall s \in \{1, \ldots, m\}$.

So, we have the result given by Theorem 2.23.

2.5.2 Kernels of binary 1-perfect codes

In this section we will describe the results in [PL95], where Phelps and LeVan construct 1-perfect codes with kernels of all the admissible dimensions.

In order to do that, they showed the following result about the kernel of 1-perfect codes constructed using the Doubling construction given by Proposition 2.6, as long as the dimension of the kernel K_1 of C_1 is less than $(n-1)/2$. In chapter 3, Theorem 3.17, we will generalize this result for any K_1, not necessarily with dimension less than $(n-1)/2$.

Lemma 2.31. [PL95] *Let $C = (C_1 \oplus C_2^*) \cup_{i=1}^{n} (C_1 + e_i \oplus (C_2 + e_{\pi(i)})^*)$ where C_1, C_2 are 1-perfect codes of length n, then the kernel of C is $K_1 \oplus K_2^*$, where K_1, K_2^* are the kernels of C_1, C_2^* respectively, as long as the dimension of K_1 is less than $(n-1)/2$.*

As a consequence of this lemma we have that:

Corollary 2.32. [PL95] *If there exists C_1, C_2 1-perfect codes of length n with kernels K_1, K_2, respectively, where $dim(K_1) < (n-1)/2$, then there exists a 1-perfect code C of length $2n+1$ having a kernel $K = K_1 \oplus K_2^*$, where $dim(K) \in \{2, 3, \ldots, n\}$.*

They also proved the following results about the kernel of 1-perfect codes constructed with the Switching construction given by Proposition 2.13. Before this, we will write the results about the size of the intersection of the subspaces we have defined as T_i. In chapter 4 we will show these results for q-ary Hamming codes.

Let H_m be a Hamming code of length $n = 2^m - 1$. Let T_i be the linear subcode of a Hamming code, H_m, generated by the codewords of weight 3 having a 1 in the i^{th} component.

Lemma 2.33. [PL95] *The dimension of T_i is $(n-1)/2$.*

Lemma 2.34. [PL95] *For $r \geq 2$ independent points in the projective space associated with the words of weight three in the Hamming code of length $n = 2^m - 1$, the subspace $T_1 \cap T_2 \cap \cdots \cap T_r$ has dimension 2^{m-r}.*

We assume that $\{1, 2, \ldots, m\}$ are independent points. In order to make different switches, by Lemma 2.29, we can choose $x_1, x_2, \ldots, x_m$ such that $T_i + x_i$ and $T_j + x_j$ are always disjoint for all $j \neq i$ and $m \geq 4$.

Theorem 2.35. [PL95] *Let H_m be a Hamming code of length $n = 2^m - 1$, $m \geq 4$, and let*

$$C' = \Big(H_m \setminus \bigcup_{i=1}^{m} (T_i + x_i)\Big) \cup \bigcup_{i=1}^{m} (T_i + x_i + e_i)$$

Then, $K_{C'} = \bigcap_{i=1}^{m} T_i$ and $dim(K_{C'}) = 1$.

In fact, by the proof of this Theorem, we also have the following more general result.

Theorem 2.36. [PL95] *Let H_m be a Hamming code of length $n = 2^m - 1$, $m \geq 4$, and let*

$$C' = \left(H_m \setminus \bigcup_{i=1}^{s} (T_i + x_i)\right) \cup \bigcup_{i=1}^{s} (T_i + x_i + e_i)$$

Then, $K_{C'} = \bigcap_{i=1}^{s} T_i \quad \forall s \in \{1, 2, \ldots, m\}$.

Independently, Heden [Hed94] found a 1-perfect code of length 15 and kernel of dimension 1.

It is also possible to make multiple switches from the same coset at one time, taking a subspace K such that it contains T_i.

Lemma 2.37. [PL95] *Let H_m be a Hamming code, and let K be a subspace of H_m such that $T_i \subseteq K \subseteq H_m$, and $dim(K) \leq dim(H_m) - 2$. Then,*

$$C' = (H_m \setminus (K + y)) \cup (K + y + e_i)$$

is a 1-perfect code with kernel K.

Corollary 2.38. [PL95] *There exists C', a 1-perfect code of length $n = 2^m - 1$, having kernel K where the $dim(K) \in \{(n-1)/2, \ldots, n - m - 2\}$.*

Using all of these results, Phelps and LeVan proved Theorem 2.24. By Theorem 2.35, we have 1-perfect codes of length $n = 2^m - 1$, $m \geq 4$, containing a kernel of dimension one. From Corollary 2.38, we can find codes containing kernels of all dimensions from $(n-1)/2$ up through $n - m - 2$, and also $n - m$. From Corollary 2.32, we have a recursive construction of 1-perfect codes having kernels of dimension 2 up through $(n-1)/2$. It is only necessary to see this result for the case $n = 15$.

For a kernel of dimension 1 we can use the Theorem 2.35, for dimensions 7, 8, 9 and 11, Corollary 2.38. Theorem 2.36 give 1-perfect codes having kernels T_1, $T_1 \cap T_2$ and $T_1 \cap T_2 \cap T_3$ if we only make one, two or three switches respectively, so we also have codes with kernels of dimension 4 and 2. Finally, Heden [Hed94] and [BGH83]

have constructed 1-perfect codes of length 15 having kernels of dimensions 3, 5 and 6.

So, we have the result given by Theorem 2.24.

2.5.3 Full-rank codes and kernels

In order to prove that for all $n \geq 10$, there exists a full-rank tiling of $\mathbb{F}_2^n$, Etzion and Vardy [EV98] obtained certain bounds relating the dimension of the kernel of full-rank 1-perfect codes. In fact, they proved which is the largest possible dimension of the kernel of a full-rank 1-perfect code of length $n = 2^m - 1$ for all $m \geq 10$. We will also see in this section that the existence of full-rank tilings of $\mathbb{F}_2^n$ for some values of n is closely related to the existence of full-rank 1-perfect codes with kernels of high dimension.

A *tiling* of $\mathbb{F}_2^n$ is a pair (V, A) of subsets of F_2^n such that every $x \in \mathbb{F}_2^n$ has a unique representation of the form $x = v + a$, with $v \in V$ and $a \in A$. Thus (V, A) is a tiling if and only if

$$V + A = \mathbb{F}_2^n \quad \textit{and} \quad (V + V) \cap (A + A) = \{\mathbf{0}\}.$$

Without loss of generality, we can always assume that $\mathbf{0} \in V \cap A$. A tiling (V, A) of $\mathbb{F}_2^n$ is *trivial* if one of the sets V, A is $\{\mathbf{0}\}$ and the other is $\mathbb{F}_2^n$. It is of *full-rank* if $\langle V \rangle = \langle A \rangle$ or, equivalently, $rank(V) = rank(A) = n$.

First of all we show the connections between tilings and 1-perfect codes.

Theorem 2.39. [CLVZ96] *Let (V, A) be a tiling of $\mathbb{F}_2^n$ and let $\nu = |V| - 1$. Further, let $H(V)$ be an $n \times \nu$ matrix having the nonzero elements of V as its columns. Define*

$$C = \{x \in \mathbb{F}_2^\nu \ : \ H(V)x^t \in A\}$$

Then, C is a 1-perfect code of length ν.

We will say that C is the 1-perfect code *associated* with the tiling (V, A). The following proposition gives that if (V, A) is a full-rank tiling, then the associated 1-perfect code C is also a full rank.

Proposition 2.40. [CLVZ96] *If C is the 1-perfect code of length ν associated with a tiling (V, A), then*

$$rank(C) = \nu - rank(V) + rank(A_{\langle V \rangle}),$$

where $A_{\langle V \rangle} = A \cap \langle V \rangle$. In particular, if $\langle V \rangle = \mathbb{F}_2^n$, then

$$rank(C) = \nu - n + rank(A)$$

Let C be the 1-perfect code associated with the tiling (V, A). Then it is easy to see that the kernel of C is $K_C = \{x \in C \ : \ H(V)x^t \in K_A\}$. Along with Proposition 2.40, this implies the following.

Proposition 2.41. [EV98] *If C is the 1-perfect code of length ν associated with a tiling (V, A), then*

$$dim(K_C) = \nu - rank(V) + dim(K_{A_{\langle V \rangle}}),$$

where $A_{\langle V \rangle} = A \cap \langle V \rangle$. In particular, if $\langle V \rangle = \mathbb{F}_2^n$, then

$$dim(K_C) = \nu - n + dim(K_A)$$

Now we will see two different constructions of tilings and how they are used to construct full-rank tilings.

Construction A Let (V, A) be a tiling of $\mathbb{F}_2^n$ and let a^* be a nonzero element of A. Consider the sets

$$V' = \{(v|0) \ : \ v \in V\} \cup \{(v|1) \ : \ v \in V\}$$

$$A' = \{(a|0) \ : \ a \in A^*\} \cup \{(a^*|1)\}$$

where $A^* = A \backslash \{a^*\}$. Then (V', A') is a tiling of $\mathbb{F}_2^{n+1}$.

Proposition 2.42. [EV98] *If (V, A) is a full-rank tiling of $\mathbb{F}_2^n$ and $rank(A^*) = n$, then the tiling (V', A') obtained by Construction A is a full-rank tiling of $\mathbb{F}_2^{n+1}$.*

Starting with a full-rank tiling (V, A) of $\mathbb{F}_2^{14}$ with $|V| = 2^{10}$ and $|A| = 2^4$ constructed in [CLVZ96], and iteratively applying Construction A, establishes the following.

Theorem 2.43. [EV98] *For all $n \geq 14$, there exists a full-rank tiling of $\mathbb{F}_2^n$.*

It was already shown in [EV94, CLVZ96] that full-rank tilings of $\mathbb{F}_2^n$ exist for all $n \geq 112$. Since full-rank tilings of $\mathbb{F}_2^n$ do not exist for $n \leq 7$, as established in [CLVZ96], these results leave only the six values $n = 8, 9, \ldots, 13$ unresolved.

Construction B Let A_0 be a subspace of $\mathbb{F}_2^n$ of dimension k. For any $V \subset \mathbb{F}_2^n$, we define V/A_0 as follows. Fix a basis $a_1, a_2, \ldots, a_k$ for A_0 and complete this to a basis $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_{n-k}$ for $\mathbb{F}_2^n$. Then each vector $v = \sum_{i=1}^{k} \alpha_i a_i + \sum_{i=1}^{n-k} \beta_i b_i$ in V is mapped onto the vector $v' = \sum_{i=1}^{n-k} \beta_i b_i$ in V/A_0. Thus V/A_0 is just the projection of V onto $\mathbb{F}_2^n/A_0$. Note that $\mathbb{F}_2^n/A_0$ may be regarded as F_2^{n-k} under an appropriate change of basis, namely, under the linear transformation that takes $b_1, b_2, \ldots, b_{n-k}$ into unit vectors. Thus we will identify $\mathbb{F}_2^n/A_0$ with $\mathbb{F}_2^{n-k}$ and think of V/A_0 as a subset of $\mathbb{F}_2^{n-k}$. Let (V, A) be a tiling of $\mathbb{F}_2^n$. Let A_0 be a k-dimensional subspace of K_A. Then, $(V/A_0, A/A_0)$ is a tiling of $\mathbb{F}_2^{n-k}$.

Proposition 2.44. [CLVZ96] *If (V, A) is a full-rank tiling of $\mathbb{F}_2^n$, then the tiling obtained by Construction B, $(V/A_0, A/A_0)$, is a full-rank tiling of $\mathbb{F}_2^{n-k}$.*

Last proposition implies the following.

Proposition 2.45. *If there exists a full-rank tiling (V, A) of $\mathbb{F}_2^n$ with $dim(K_A) = r$, then there exist full-rank tilings of $\mathbb{F}_2^{n-k}$ for all $k = 1, 2, \ldots, r$.*

Starting again with the full-rank tiling (V, A) of $\mathbb{F}_2^{14}$ with $|V| = 2^{10}$ and $|A| = 2^4$ exhibited in [CLVZ96]. Since $K_V = K_A = \{\mathbf{0}\}$, by Theorem 2.39, Proposition 2.40

and 2.41, the associated 1-perfect code C is a full-rank code of length $2^{10}-1=1023$ and $dim(K_C) = 1023 - rank(V) + dim(K_A) = 1009$. Let Λ_n denote the Hamming sphere of radius 1 in $\mathbb{F}_2^n$. Then (Λ_{1023}, C) is a full-rank tiling of $\mathbb{F}_2^{1023}$. Applying to this tiling Construction B and Proposition 2.45, we obtain full-rank tilings of $\mathbb{F}_2^n$ for all $n = 14, 15, \ldots, 1022$. So, we also have Theorem 2.43 using Construction B.

Using Construction B and starting with the full-rank tiling (Λ_{1023}, C) of $\mathbb{F}_2^{1023}$, the associated full-rank 1-perfect codes of length $n = 2^m - 1$ have kernels of dimension $\geq n-m-10$ for $m = 4, 5, \ldots, 1022$. The 1-perfect code associated with the full-rank tiling of $\mathbb{F}_2^{14}$ has kernel of dimension $n - m - 4$ for $m = 10$. The following theorem show that this is the upper bound of the dimension of the kernel for full-rank 1-perfect codes.

Theorem 2.46. [EV98] *If C is a full-rank 1-perfect code of length $n = 2^m - 1$, then*

$$dim(K_C) \leq n - m - 4$$

Furthermore, this bound is tight for $m = 10$ and $m = 11$.

More generally, Etzion and Vardy [EV98] give a complete answer to the question of which is the largest possible dimension $\alpha(m)$ of the kernel of a full-rank 1-perfect code of length $n = 2^m - 1$ for all $m \geq 10$. We also give the proof of this result because we will use the same idea to prove the upper bound on the dimension of the kernel for a 1-perfect code with any rank.

Theorem 2.47. [EV98] *Let δ be the unique integer such that $2^{\delta-1} - (\delta - 1) \leq m < 2^\delta - \delta$. Then*

$$\alpha(m) = n - m - \delta$$

for all $m \geq 10$.

Proof: We first show that $\alpha(m) \leq n - m - \delta = n - (m + \delta)$, where $n = 2^m - 1$. Assume to the contrary that there exists a full-rank perfect code C of length n such

that $dim(K_C) = n - m - \delta + 1$. Since C is the union of $|C|/|K_C|$ cosets of K_C, the total number of linearly independent vectors in C is at most

$$dim(K_C) + (\frac{|C|}{|K_C|} - 1) \geq n.$$

Substituting $dim(K_C) = n-m-\delta+1$ and $|C| = 2^{n-m}$, we obtain $m \leq 2^{\delta-1} - \delta$, which contradicts the definition of δ. By Theorem 2.46, the theorem is true for $m = 10$ and $m = 11$.

Next, we show how to construct a full-rank 1-perfect code C_{12} of length $n = 2^{12}-1$, such that $dim(K_C) = n - 17 = n - m - \delta$, for $m = 12$. Start with the full-rank tiling $(V, A) = (\Lambda_{15}, C)$ of $\mathbb{F}_2^{15}$, where C is a full-rank 1-perfect code of length 15. Then, apply Construction A to obtain a full-rank tiling (V', A') of $\mathbb{F}_2^{16}$ with $|V'| = 2^5$ and $|A'| = 2^{11}$. Now, apply Construction A again, with the roles of V' and A' interchanged. This produces a full-rank tiling (V_{12}, A_{12}) of $\mathbb{F}_2^{17}$ with $|V_{12}| = 2^{12}$ and $|A_{12}| = 2^5$. The full-rank 1-perfect code C_{12} associated with this tiling has length $n = |V_{12}| - 1 = 2^{12} - 1$ and by Proposition 2.41 and Theorem 2.46 we have $dim(K_{C_{12}}) = n - rank(V_{12}) = n - 17$.

Now, iteratively applying Construction A to (V_{12}, A_{12}), we obtain full-rank tilings (V_m, A_m) of $\mathbb{F}_2^{m+5}$ with associated full-rank 1-perfect codes of length $n = 2^m - 1$ and kernel of dimension $n - (m + 5)$. Since in all of these tilings $|A_m| = |A_{12}| = 2^5$, we can keep iterating Construction A in this way as long as $m + 5 \leq 2^5 - 1$ or, equivalently, $m < 2^5 - 5 = 27$. This proves the theorem for all $m = 12, 13, \ldots, 26$. For $m = 27, 28, \ldots, 57$, we start with the full-rank tiling (Λ_{31}, C), where C is a full-rank 1-perfect code of length 31, and proceed as before. Continuing in this manner establishes the theorem for all $m \geq 10$. ∎

Note that Theorem 2.46 is not a special case of Theorem 2.47, since it holds also for $m < 10$. For example, for $m = 4$ it follows from Theorem 2.46 that the possible dimensions of the kernel of a full-rank 1-perfect code of length 15 are $1, 2 \ldots, 7$. The problem of determining which of these kernel dimensions are attainable is closely

related to the problem of existence of full-rank tilings of $\mathbb{F}_2^n$ for $n = 8, 9, \ldots, 13$. Indeed, a full-rank 1-perfect code of length 15 and kernel of dimension k implies by Proposition 2.45 the existence of a full-rank tilings of $\mathbb{F}_2^n$ for all $n \geq 15 - k$. Furthermore, we have the following result.

Proposition 2.48. [EV98] *A full-rank 1-perfect code of length 15 with kernel of dimension 7 exists if and only if a full-rank tiling of* $\mathbb{F}_2^8$ *exists.*

It is still open if there exist a full-rank 1-perfect code of length 15 with kernel of dimension 7. However, Phelps found full-rank 1-perfect codes of length 15 with kernels of dimensions 2,3,4 and 5 (see [EV98]). This implies full-rank tilings of $\mathbb{F}_2^n$ exist for $n = 10, 11, 12$ and 13. Then, with the Proposition 2.43 we have that for all $n \geq 10$, there exists a full-rank tiling of $\mathbb{F}_2^n$, and the only values unresolved are $n = 8$ and 9.

2.5.4 Rank and kernel for n = 15

In this section, we will show for which pairs (r, k) there exists a 1-perfect code of length 15 constructed using the Doubling construction and having rank $r(C) = r$ and dimension of the kernel $k(C) = k$. Using the Doubling construction described by Proposition 2.7 we can get extended 1-perfect codes of length $2n + 2$ from two given extended 1-perfect partitions of $\mathbb{E}_2^{n+1}$. Puncturing these codes we obtain 1-perfect codes of length $2n + 1$.

In order to enumerate all nonequivalent extended 1-perfect codes of length 16 that can be constructed by the Doubling construction, Phelps [Phe00] found all nonequivalent 1-perfect partitions of $\mathbb{F}_2^7$ into 1-perfect codes of length 7 in the following way.

There are 30 different, but isomorphic, Hamming codes of length 7 corresponding to the 30 different Steiner triple system of order 7. Each linear code has 8 cosets. Any 1-perfect partition will either have at least 2 cosets of these linear codes or will have at most one coset of any linear code. In the first case, we can choose one linear code

and its coset and enumerate all solutions. In this way, Phelps found 192 different partitions but only 10 nonequivalent partitions. In the second case he found only one nonequivalent solution. So, there are 11 nonequivalent 1-perfect partitions of $\mathbb{F}_2^7$, [Phe00]. Of these 11 partitions, six had previously been also found by Phelps [Phe83].

Doubling construction uses extended 1-perfect partitions. As with 1-perfect codes and extended 1-perfect codes, if two partitions are equivalent then the corresponding extended partitions will also be equivalent; however, the converse is false. Puncturing extended partitions in different coordinates can result nonequivalent partitions. In fact, although there are 11 nonequivalent 1-perfect partitions of $\mathbb{F}_2^7$, there are only 10 nonequivalent extended 1-perfect partitions of length 8.

For each pair of extended 1-perfect partitions of length 8 it was constructed different nonequivalent 1-perfect codes of length 15. Finally, computing the rank and the kernel of these 1-perfect codes, Phelps [Phe00] obtain the following table which shows the number of nonequivalent codes by rank and kernel.

$r(C)/\ k(C)$	11	9	8	7	6	5	4	3	2	1
11	1									
12		2	2	3						
13			7	11	38	34	20			
14			1	4	48	210	374	172	36	
15										

In chapter 3, we will see that it does not exist any 1-perfect code, C, of length 15 with rank $r(C) \leq 14$ having a kernel of dimension different than the one of the 1-perfect codes obtained in this way. In that chapter, we will assure this after showing for each rank which are the lower and the upper bounds for the dimension of the kernel.

For rank $r(C) = 15$, although it is known by Theorem 2.46 and 2.35 that the admissible dimensions of the kernel are 1, 2, 3, 4, 5, 6 and 7, it has been only proved that there exist full-rank binary 1-perfect codes of length 15 with kernels of dimensions

1, 2, 3, 4 and 5 (see [PL95] and [EV98]). We also constructed these codes ourselves independently.

Summarizing, for $n = 15$, the following table shows for which pairs $(r(C), k(C))$ there exists a 1-perfect code with these parameters. The question mark sign means it is not known if there exists a 1-perfect code with that rank and dimension of the kernel.

$r(C)$	$k(C)$									
11	11									
12		9	8	7						
13			8	7	6	5	4			
14			8	7	6	5	4	3	2	
15				?	?	5	4	3	2	1

Chapter 3

Rank and Kernel of binary 1-perfect codes

In this chapter, we analyze the rank and the dimension of the kernel for binary 1-perfect codes of length $n = 2^m - 1$. First of all, we will prove some results on the structure of 1-perfect codes. Next, we will establish the lower and upper bounds on the dimension of the kernel of 1-perfect codes once the rank is fixed. We will show these bounds are tight except for one case. For 1-perfect codes with maximum rank $r(C) = n$, called full-rank 1-perfect codes, we do not prove the upper bound is tight, $\forall m \geq 4$. Despite this, it is already known this upper bound for full-rank 1-perfect codes is tight, $\forall m \geq 10$, by Etzion and Vardy [EV98]. So, the only cases that will remain unsolved will be whether there exist full-rank 1-perfect codes with that upper bound for $4 \leq m < 10$. These results given in this chapter are new and they will be also shown in [PV01a].

We will also see that using the Doubling construction and some new results, we can construct binary 1-perfect codes C of length $n = 2^m - 1$ with any rank $r(C) < n$ and different dimensions of the kernel, $k(C)$, between the upper and lower bounds. We will obtain a large number of cases but we will not completely settle the question, partly because we need to construct full-rank 1-perfect codes with different $k(C)$.

We only know how to construct full-rank 1-perfect codes of length $n = 2^m - 1$ with the lower dimension of the kernel, $k(C) = 1$, $\forall m \geq 4$ [PL95] and with the upper dimension of the kernel, $\forall m \geq 10$ [EV98].

3.1 Properties on the structure of 1-perfect codes

As we can see by Proposition 2.17, the codewords of weight 3 in a 1-perfect code of length n form a $STS(n)$, (V, B), if we identify the set of codewords of weight 3 with the set of triples B, and V is the set of coordinates. In this way, we can say that the linear code of a Steiner triple system (V, B) is just the span of B. It is well-known that the dual code of the $STS(n)$ is an equidistant code with all nonzero codewords having weight $(n+1)/2$, [DHV78] (see also [Her85, EV94]). In fact, much more has been established about the structure of the $STS(n)$ and that of its dual code (see [DHV78, Tei80, Her85, Bon84]).

For any binary code C of length n and minimum distance 3, then we can define a *neighborhood triple system*, $NTS(x)$, for each codeword $x \in C$

$$NTS(x) = \{x + y \ : \ y \in C, \ d(x, y) = 3\}$$

It is easy to see that if the code C has minimum distance 3 then the $NTS(x)$ is a partial triple system for each $x \in C$. It is well known that if C is a 1-perfect code of length n then the neighborhood triple systems are in fact $STS(n)$. Moreover, this property characterizes 1-perfect codes.

Theorem 3.1. *A code C of length n and minimum distance 3 is a 1-perfect code if and only if every neighborhood triple system is a Steiner triple system.*

Proof: Let C be a code of length n and minimum distance 3 where every neighborhood triple system is a Steiner triple system. C is 1-perfect if every word is either a code word or distance one from a unique codeword. Let $y \in F^n$, $y \notin C$. Let $x \in C$ be the closest codeword to y. Assume $d(x, y) \geq 2$ and that these words disagree at least

in coordinates i, j. Because the $NTS(x)$ is an $STS(n)$, there exits $x' \in NTS(x)$ such that x' disagrees with x in exactly 3 coordinates i, j, k (i.e. the support of $x + x'$). But then x' agrees with y in coordinates i, j and could disagree with y in coordinate k. Hence x' is closer to y than x, contradicting the choice of x. Thus we conclude that $d(x, y) = 1$ and C is perfect. ∎

Clearly, any word in the dual of a 1-perfect code C must be in the dual of every neighborhood triple system $NTS(x)$, $x \in C$. This conversely implies that each $NTS(x)$ must have a common structure induced by $C^{\perp}$. First, we review the structure of a Steiner triple system induced by its dual code when $n = 2^m - 1$. Define a sub-$STS(q)$ of a Steiner triple system, (V, B), as a pair (S_q, B_q), where $S_q \subset V$, $B_q \subset B$ where B_q restricted to the subset of coordinates S_q is a $STS(q)$.

Lemma 3.2. [DHV78, Tei80] *Given a Steiner triple system, B, of order $n = 2^m - 1$, and its dual code $B^{\perp}$, then for every subspace D of dimension $m - s$ in $B^{\perp}$ there is a corresponding sub-$STS(n_s)$ in B, $n_s = 2^s - 1$, on the set of coordinates*

$$S_D = \{i \ : \ c_i = 0 \ \forall (c_1, c_2, \ldots, c_n) \in D\}$$

Note, that for $s = 0, 1$ we have the trivial triple systems on 0 and 1 points respectively with no triples and for $s = m$ we get the entire $STS(n_m)$ which is not a proper subsystem.

We also have:

Lemma 3.3. [DHV78, Tei80] *The dual of a 1-perfect code C of length $n_m = 2^m - 1$ is a subcode of the dual of a Hamming code of length n_m.*

We need to introduce some notation in order to discuss the subcodes of a 1-perfect code C. Given a subset of coordinates $S \subset V = \{1, 2, \ldots, n_m\}$, and a codeword $y \in C$ define

$$C_S(y) = \{x_S \ : \ x \in C, \ x_i = y_i \ \forall i \notin S\}$$

where x_S is the restriction of the codeword x to the subset of coordinates S.

Theorem 3.4. *Given a 1-perfect code C of length $n_m = 2^m - 1$ and its dual code $C^\perp$, then for every subspace $D \subseteq C^\perp$ of dimension $m - s$, $s > 0$, and for every $y \in C$, the subcode $C_{S_D}(y)$ is a 1-perfect code of length $n_s = 2^s - 1$ where S_D is as above, the set of coordinates which are zero in every codeword of D. Moreover, when $s > 1$, the characteristic vector $\chi(S_D)$ is in the kernel of C.*

Proof: Given the subspace $D \subseteq C^\perp$ of dimension $m - s$, then $|S_D| = n_s = 2^s - 1$. For any $y \in C$, consider the subcode $C_{S_D}(y)$ and any codeword $x' \in C_{S_D}(y)$. Since for every $x \in C$, the $NTS(x)$ has a $sub - STS(n_s)$ on the set S_D, then the $NTS(x')$ is an $STS(n_s)$ where x' is the restriction of x to S_D. By Theorem 3.1, this means that $C_{S_D}(y)$ is a 1-perfect code.

We know that the all–ones vector (of length n_s) is in the kernel of every 1-perfect code $C_{S_D}(y)$ when $s > 1$. But, this implies that $\chi(S_D)$, the codeword that has a 1 in the coordinates S_D (and zero elsewhere), is in the kernel of C. ∎

Corollary 3.5. *If C is a 1-perfect code and $C^\perp$ is the dual of C, then $C^\perp \subset C$.*

3.2 Lower bounds

The lower bound on the dimension of the kernel of a 1-perfect code in terms of the rank of the code is given by the following result, which comes from Theorem 3.4.

Theorem 3.6. *Let C be a 1-perfect code of length $n_m = 2^m - 1$, rank $r(C) = n - m + s$ and a kernel of dimension $k(C)$, then*

$$\begin{aligned} k(C) &\geq 2^{m-s} \quad if\ s > 1 \\ k(C) &\geq 2^{m-1} - 1 \quad if\ s = 1 \end{aligned}$$

Proof: Let C be a 1-perfect code of length n_m having rank $r(C) = n - m + s$, $s \geq 1$. Then $C^\perp$ has dimension $m - s$ and has $2^{m-s} - 1$ subspaces of dimension $m - s - 1$. Let S be the set of coordinates corresponding to the subspace $C^\perp$ and let S_j, $j = 1, 2, \ldots, 2^{m-s} - 1$ correspond to the subspaces of dimension $m - s - 1$. By

the definition of the subsets S and S_j, $S \subset S_j$. Moreover, the $2^{m-s}-1$ codewords $\chi(S_j)$ are independent and in the kernel for $s \geq 1$. If $s > 1$ then the codeword $\chi(S)$ is in the kernel and is also independent giving $2^{m-s}-1+1$ independent words in the kernel of C. ∎

The bound established in Theorem 3.6 is the exact lower bound. The following result is not stated this way in Phelps and LeVan [PL95], but it is proved. Actually, we have this result from Theorem 2.30 and 2.36, where it is shown the construction of these codes using the switching technique.

Theorem 3.7. [PL95] *For all $m \geq 4$, there exists a 1-perfect code of length $n = 2^m - 1$, having rank $n-m+s$ and kernel of dimension $k = 2^{m-s}$ when $s > 1$ and $k = 2^{m-1}-1$ when $s = 1$.*

3.3 Upper bounds

The upper bound on the dimension of the kernel of a 1-perfect code in terms of the rank of the code is a generalization of an argument of Etzion and Vardy [EV98]. We included this argument with Theorem 2.47.

Theorem 3.8. *A 1-perfect code of length $n = 2^m - 1$ with rank $n - m + s$ and a kernel of dimension $n - m - \delta$ fulfills $2^\delta - \delta - 1 \geq s$.*

Proof: A 1-perfect code of length $n = 2^m - 1$ which has rank $n - m + s$ must have that many independent vectors. The kernel contains $n - m - \delta$ independent vectors. Since each coset of the kernel can have at most one additional independent vector, we have that the maximum number of independent vectors will be,

$$n - m - \delta + \frac{2^{n-m}}{2^{n-m-\delta}} - 1 \geq n - m + s$$

which simplifies to $2^\delta - \delta - 1 \geq s$. ∎

Etzion and Vardy [EV98] give a construction of full rank 1-perfect codes (i.e. $s = m$) that achieve this bound when $m \geq 10$. In section 2.5.3 we included this construction proving Theorem 2.47.

The results from [Phe00], that we also included in section 2.5.4, show that this bound is tight for $m = 4$ and $s < m$. Actually, in that section we saw the rank and the dimension of the kernel of all the 1-perfect codes of $m = 4$ (length 15) in [Phe00]. It is showed in [Phe00] it is possible to construct a 1-perfect code of $m = 4$ for any rank $n - m + s$ with $0 \leq s < m$ and for any possible dimension of the kernel between the lower and upper bound. The only open question for length 15 is if there exist full-rank 1-perfect codes with kernel of dimension 6 and 7. Summarizing, for $m = 4$, the following table shows for which pairs $(r(C), k(C))$ there exists a 1-perfect code with these parameters.

$r(C)$	$k(C)$								
11	11								
12		9	8	7					
13			8	7	6	5	4		
14			8	7	6	5	4	3	2
15				?	?	5	4	3	2	1

Now, in this section, we will generalize the previous result to any length. We will see this bound is tight for $m > 4$ and $0 \leq s < m$. The extreme case $s = m$, that is the construction of full-rank 1-perfect codes with maximum dimension of the kernel, will still remain open for $4 \leq m < 10$.

In order to establish this upper bound we will need some results on Hamming codes. Let H_1 and H_2 be two different isomorphic copies of the Hamming code of length $n = 2^m - 1$ (and dimension $2^m - m - 1$). Let T_i denote the subspace generated by the words of weight 3 that have a one in the i^{th} coordinate. The coordinates of the

Hamming code are in one-to-one correspondence with the columns of its parity check matrix which in turn correspond to points in the binary projective space $PG(m-1,2)$. So, we can refer to coordinates as being independent if the corresponding columns (points) are independent.

As we showed in section 2.5.2, Lemma 2.33 and 2.34 [PL95], we have for any i the dimension of T_i is $2^{m-1}-1$ and for any $r \geq 2$ independent coordinates in a Hamming code of length 2^m-1, the dimension of the intersection of corresponding r subspaces T_i is 2^{m-r}. This result is crucial to establishing the next result:

Theorem 3.9. *For any $m-\delta \geq 1$ independent coordinates in a Hamming code of length 2^m-1, the dimension of the subspace spanned by the union of corresponding $m-\delta$ subspaces T_i is $2^m-m-1-(2^\delta-\delta-1)$.*

Proof: Let K be the subspace spanned by the union of these $m-\delta$ subspaces T_i. If $m-\delta=1$, then the result is clear. If $m-\delta \geq 2$, using inclusion -exclusion we have

$$\begin{aligned} dimK &= (m-\delta)(2^{m-1}-1) - \sum_{i=2}^{m-\delta}(-1)^i \binom{m-\delta}{i} 2^{m-i} \\ &= -(m-\delta) - 2^\delta \sum_{i=1}^{m-\delta}(-1)^i \binom{m-\delta}{i} 2^{m-\delta-i} \\ &= -(m-\delta) - 2^\delta(1-2^{m-\delta}) \\ &= 2^m - 1 - m - (2^\delta - \delta - 1) \end{aligned}$$

∎

This leads to the next important Corollary.

Corollary 3.10. *Given Hamming codes H_1, H_2 of length 2^m-1 if*

$$K = < \bigcup_{i \in I} T_i > = H_1 \cap H_2$$

where I is a set of $m-\delta$ independent coordinates, then the dimension of the intersection of the dual codes is

$$dim(H_1^\perp \cap H_2^\perp) = m - (2^\delta - \delta - 1)$$

Proof: We have $dimH_1^\perp = dimH_2^\perp = m$, and

$$dimK^\perp = dim(H_1^\perp \cup H_2^\perp) = m + (2^\delta - \delta - 1).$$

Thus

$$\begin{aligned} dim(H_1^\perp \cap H_2^\perp) &= m + m - dim(H_1^\perp \cup H_2^\perp) \\ &= m - (2^\delta - \delta - 1) \end{aligned}$$

∎

Observe that if $\{i, j, k\}$ is the support for a word of weight 3 in a Hamming code then $T_k \subseteq T_i \cup T_j$. Thus if $S = \{k \mid T_k \subseteq < \bigcup_{i \in I} T_i >\}$ then $|S| = 2^{|I|} - 1 = 2^{m-\delta} - 1$ and the set of coordinates S correspond to a sub Hamming code of this length.

Lemma 3.11. *Let $K = < \bigcup_{i \in I} T_i >$, where I is a set of $m-\delta$ independent coordinates in a Hamming code of length $2^m - 1$. Then, the following vectors are basis for the dual space $K^\perp$*

$$\begin{pmatrix} 0\ldots0 & 1\ldots1 & 0\ldots0 & \cdots & 0\ldots0 \\ 0\ldots0 & 0\ldots0 & 1\ldots1 & \cdots & 0\ldots0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0\ldots0 & 0\ldots0 & 0\ldots0 & \cdots & 1\ldots1 \\ A & A_1^* & A_2^* & \cdots & A_{2^\delta-1}^* \end{pmatrix}$$

where A is a check matrix of a Hamming code of length $2^{m-\delta} - 1$ and A_i^* $\forall i \in \{1, \ldots, 2^\delta - 1\}$ is any matrix $A^* = (0\ A)$ or $A^* + B_j$, where B_j is a matrix with the all-ones vector in the j^{th} row and zeros elsewhere.

Proof: We can assume that the first $2^{m-\delta} - 1$ coordinates are the points of the smallest sub-STS containing the $m-\delta$ independent points and A is the check matrix of the sub Hamming code in these coordinates. We can also order the other coordinates such that each $2^{m-\delta}$ consecutive coordinates plus the first $2^{m-\delta}-1$ form a sub-STS of order $2^{m-\delta+1}-1$ with check matrix for the sub Hamming code $\begin{pmatrix} 0 & 1 & 1 \\ A & 0 & A \end{pmatrix}$. There are $2^\delta - 1$ of these subsystems.

By Theorem 3.9, we know that $dim K^{\perp} = m - \delta + 2^{\delta} - 1$. We have $m - \delta + 2^{\delta} - 1$ linearly independent vectors, thus we only need to see that these vectors are in $K^{\perp}$. We have to prove that any vector $\chi(\{i, j, k\}) \in K$ such that $i \in I$ multiplied by any row is zero. Notice that the coordinates j and k either are both in the first $2^{m-\delta} - 1$ coordinates or are in the same subset of $2^{m-\delta}$ coordinates. Then, it is clear that the first $2^{\delta} - 1$ rows are in $K^{\perp}$ and if the last $m - \delta$ rows are $(A\ A^* \dots\ A^*)$, they are also in $K^{\perp}$. If we change any A^* with $A^* + B_j$ for any $j \in \{1, \dots, m - \delta\}$, then the vectors are still linearly independents and are in $K^{\perp}$. ∎

Theorem 3.12. [EV98] *For each $m \geq 3$ and $s \in \{1, \dots, m\}$, there exist two Hamming codes H_1, H_2 of length $n = 2^m - 1$ such that*

$$dim(H_1^{\perp} \cup H_2^{\perp}) = m + s$$

In fact, in [EV98] this result is stated as Theorem 2.22. We included the proof of this result to show how to construct these two Hamming codes.

We will use the two previous results to prove the next Lemma.

Lemma 3.13. *For each $m \geq 4$ and $s \in \{1, \dots, m\}$, there exist two Hamming codes H_1, H_2 of length $n = 2^m - 1$ such that*

$$H_1^{\perp} \cup H_2^{\perp} \subseteq < \bigcup_{i \in I} T_i >^{\perp} \quad \text{and} \quad dim(H_1^{\perp} \cup H_2^{\perp}) = m + s$$

where I is a set of $m - \delta$ independent coordinates, if $2^{\delta} - \delta - 1 \geq s$ and $\delta < m$.

Proof: Let A be a check matrix of a Hamming code of length $2^{m-\delta} - 1$, and $A^* = (0\ A)$. Let B_j be a matrix with the all-ones vector in the j^{th} row and zeros elsewhere.

If $2^{\delta} - \delta - 1 \geq s$, then $\delta \geq 2$, $\forall s \in \{1, \dots, m\}$.

If $\delta = 2$, then $s = 1$. We can construct the Hamming codes H_1, H_2 defined by the following check matrices

$$\begin{pmatrix} 0 & b_1 \dots b_1 & b_2 \dots b_2 & b_3 \dots b_3 \\ A & A^* & A^* & A^* \end{pmatrix}$$

$$\begin{pmatrix} 0 & b_1 \dots b_1 & b_2 \dots b_2 & b_3 \dots b_3 \\ A & A^* & A^* & A^* + B_j \end{pmatrix}$$

for any $j \in \{1, \dots, m-2\}$, where $B = (b_1\ b_2\ b_3) = \begin{pmatrix} 011 \\ 101 \end{pmatrix}$. In this case, by Lemma 3.11, we know that $H_1^\perp \cup H_2^\perp \subseteq < \bigcup_{i \in I} T_i >^\perp$ and it is easy to see that $dim(H_1^\perp \cup H_2^\perp) = 2 + m - 2 + 1 = m + 1$.

If $\delta \geq 3$ and $s \leq \delta$, then by Theorem 3.12 there exist two Hamming codes $\overline{H}_1$, $\overline{H}_2$ of length $2^\delta - 1$ such that $dim(\overline{H}_1^\perp \cup \overline{H}_2^\perp) = \delta + s\ \forall s \in \{1, \dots \delta\}$. Let $C = (c_1\ c_2 \dots\ c_{2^\delta - 1})$ and $D = (d_1\ d_2 \dots\ d_{2^\delta - 1})$ be the check matrices of $\overline{H}_1$ and $\overline{H}_2$. The Hamming codes H_1, H_2 defined by the following check matrices

$$\begin{pmatrix} 0 & c_1 \dots c_1 & c_2 \dots c_2 & \dots & c_{2^\delta-1} \dots c_{2^\delta-1} \\ A & A^* & A^* & \dots & A^* \end{pmatrix}$$

$$\begin{pmatrix} 0 & d_1 \dots d_1 & d_2 \dots d_2 & \dots & d_{2^\delta-1} \dots d_{2^\delta-1} \\ A & A^* & A^* & \dots & A^* \end{pmatrix}$$

have $dim(H_1^\perp \cup H_2^\perp) = \delta + s + m - \delta = m + s$, $\forall s \in \{1, \dots, \delta\}$.

If $\delta \geq 3$ and $s > \delta$, we can take the following check matrices for the Hamming codes H_1 and H_2

$$\begin{pmatrix} 0 & c_1 \dots c_1 & c_2 \dots c_2 & \dots & c_{2^\delta-1} \dots c_{2^\delta-1} \\ A & A^* & A^* & \dots & A^* \end{pmatrix}$$

$$\begin{pmatrix} 0 & d_1 \dots d_1 & d_2 \dots d_2 & \dots & d_t \dots d_t & d_{t+1} \dots d_{t+1} & \dots & d_{2^\delta-1} \dots d_{2^\delta-1} \\ A & A^* + B_1 & A^* + B_2 & \dots & A^* + B_t & A^* & \dots & A^* \end{pmatrix}$$

where C and D are the check matrices of Hamming codes $\overline{H}_1$ and $\overline{H}_2$ such that $dim(\overline{H}_1^\perp \cup \overline{H}_2^\perp) = 2\delta$. We can assume that the 2δ coordinates that generate the subspace $\overline{H}_1^\perp \cup \overline{H}_2^\perp$ are the last ones. Then, $dim(H_1^\perp \cup H_2^\perp) = 2\delta + m - \delta + t = m + \delta + t$ $\forall t \in \{1, \dots, m - \delta\}$ as long as $2^\delta - 1 \geq 2\delta + t$ which is true because $s = \delta + t \leq 2^\delta - \delta - 1$.

∎

Theorem 3.14. *Given two Hamming codes H_1 and H_2 of length $2^m - 1$ and $s \in \{1, \ldots, m\}$ such that*

$$H_1^\perp \cup H_2^\perp \subseteq < \bigcup_{i \in I} T_i >^\perp \quad \text{and} \quad dim(H_1^\perp \cup H_2^\perp) = m + s$$

there exists a 1-perfect code C of length $n' = 2^{m'} - 1$, where $m' = m + 1$, which has rank $n' - m' + s$ and a kernel of dimension $n' - m' - \delta$ where δ is the minimum integer such that $2^\delta - \delta - 1 \geq s$.

Notice that if $m \geq 4$, $\forall s \in \{1, \ldots, m\}$ there exists at least one δ such that $2^\delta - \delta - 1 \geq s$ and $\delta < m$. So, Lemma 3.13 and Theorem 3.14 lead to the upper bound is tight $\forall m \geq 5$ and $s < m$. In order to prove the previous theorem we need to establish some results on the rank and the kernel of 1-perfect codes constructed with the Doubling construction. In next section, we will develop these results and we will also give the proof of this theorem.

3.4 Doubling construction

In this section, we establish results on the rank and the kernel of 1-perfect codes constructed with the Doubling Construction due to Phelps and Solov'eva and given by Proposition 2.6. We will use these results to prove Theorem 3.14 at the end of this section and also to construct 1-perfect codes of different ranks and dimensions of the kernel in section 3.5.

Let C_1 be a 1-perfect code of length n and C_2^* be an extended 1-perfect code of length $n + 1$. By Proposition 2.6, the code

$$C = (C_1 \oplus C_2^*) \bigcup_{i=1}^{n} (C_1 + e_i \oplus (C_2 + e_{\pi(i)})^*)$$

where π is a permutation on the set $\{1, 2, \ldots, n\}$ is a 1-perfect code of length $2n + 1$.

Theorem 3.15. *The rank of an 1-perfect code C of length $2n + 1$ constructed with the Doubling construction taking the identity permutation is $2n - r(C_1^\perp \cap C_2^\perp)$.*

Proof: We will see that $r(C^{\perp}) = r(C_1^{\perp} \cap C_2^{\perp}) + 1$. Let $u = (x, y^*)$, where $x = (x_1, \ldots, x_n)$, $y^* = (y, y_{n+1})$ and $y = (y_1, \ldots, y_n)$. By definition, if $u \in C^{\perp}$, then $(x, y^*) \cdot (c + e_i, d^* + e_i + e_{n+1}) = 0$, $\forall c \in C_1$, $d^* \in C_2^*$ and $i \in \{0, 1, \ldots, n\}$. From this we conclude that $x \cdot c = y^* \cdot d^*$ and $x_i = y_i + y_{n+1}$, $\forall i = 1, 2, \ldots, n$. If $z = (y_{n+1}, \ldots, y_{n+1})$, this is equivalent to $(z + y)c = y^* d^*$, $\forall c \in C_1$, $d^* \in C_2^*$. If $y_{n+1} = 0$, then $yc = yd$, $\forall c \in C_1$, $d^* \in C_2^*$, so $u = (y, y, 0)$, where $y \in C_1^{\perp} \cap C_2^{\perp}$. If $y_{n+1} = 1$, it is clear that the vector $u = (\vec{0}, \vec{1}, 1) \in C^{\perp}$. So, we have that $r(C^{\perp}) = r(C_1^{\perp} \cap C_2^{\perp}) + 1$. ∎

Before establish the kernel of the 1-perfect codes of length $2n+1$ constructed with the doubling construction, we will see the following result which give the kernel of a trivial 1-perfect partition of $\mathbb{F}_2^n$.

Proposition 3.16. *Let $C, C + e_1, \ldots, C + e_n$ be a partition of F^n in 1-perfect codes. Then, the kernel of the partition is $K_P = K_C \cup_{i \in I} (K_C + e_i)$, where $I = \{i : T_i \subseteq K_C\}$.*

Proof: It is clear that $K_C \subseteq K_P$. We will see that $K_C + e_i \subseteq K_P$ if $i \in I$. If $x \in K_C + e_i$ for some $i \in I$, $x + e_i \in K_C$, so $x + C + e_i = C$. For each $j \in \{1, \ldots, n\}$, $j \neq i$ exists k, $k \neq i$ and $k \neq j$ such that $e_i + e_j + e_k \in T_i \subseteq K_C$, so $C + e_j = C + e_i + e_k$ and then $x + C + e_j = C + e_k$. Finally, we have $x \in K_P$.

If $x \in K_P$, then $x + C = C$ or $x + C = C + e_i$ for some $i \in \{1, \ldots, n\}$. In the first case $x \in K_C$. We will see that in the second case $x \in K_C + e_i$ where $i \in I$. If $x + C = C + e_i$ then $x + C + e_i = C$. We know that $x \in K_P$, so $\forall j \in \{1, \ldots, n\}$, $j \neq i$ exists k, $k \neq i$ and $k \neq j$ such that $x + C + e_j = C + e_k$, so $C + e_i + e_j + e_k = C$ and $T_i \subseteq K_C$. ∎

Phelps and LeVan [PL95] show that if K_1 and K_2 are the kernels of the codes C_1 and C_2, then the kernel of C is $K_1 \oplus K_2^*$, where

$$C = (C_1 \oplus C_2^*) \bigcup_{i=1}^{n} (C_1 + e_i \oplus (C_2 + e_i)^*)$$

as long as the dimension of K_1 is less than $(n-1)/2$. We can also see this result with Lemma 2.31. Now, we will see which is the kernel of C, in general, without the condition that the dimension of K_1 has to be less than $(n-1)/2$.

Theorem 3.17. *The kernel of the 1-perfect code C of length $2n+1$ constructed with the Doubling construction from 1-perfect codes C_1 and C_2, as above, is*

$$(K_1 \oplus K_2^*) \bigcup_{i \in I} (K_1 + e_i \oplus (K_2 + e_i)^*)$$

where $I = \{i : T_i \subseteq K_1 \cap K_2\}$.

Proof: If $(x, y) \in K_1 \oplus K_2^*$, then it is clear that $(x, y) \in K_C$. If $(x, y) \in K_1 + e_i \oplus K_2^* + e_i + e_{n+1}$, for some $i \in I$ then $(x, y) + (C_1, C_2^*) = (C_1 + e_i, C_2^* + e_i + e_{n+1}) \in C$ and $\forall j \in \{1, \ldots, n\}$, $j \neq i$ $(x, y) + (C_1 + e_j, C_2^* + e_j + e_{n+1}) = (C_1 + e_i + e_j, C_2^* + e_i + e_j) = (C_1 + e_k, C_2^* + e_k + e_{n+1})$ because given i, j $i \neq j$ $\exists k$ such that $e_i + e_j + e_k \in T_i \subseteq K_1$ and $e_i + e_j + e_k \in T_i \subseteq K_2$, and then $C_1 + e_i + e_j = C_1 + e_k$ and $C_2^* + e_i + e_j = C_2^* + e_k + e_{n+1}$. So, we have that $K_1 \oplus K_2^* \cup_{i \in I} (K_1 + e_i \oplus (K_2 + e_i)^*) \subseteq K_C$.

Now, we suppose that $(x, y) \in K_C$. If $(x, y) + (C_1, C_2^*) = (C_1, C_2^*)$ then $(x, y) + (C_1 + e_j, C_2^* + e_j + e_{n+1}) = (C_1 + e_j, C_2^* + e_j + e_{n+1})$, and we have $(x, y) \in K_1 \oplus K_2^*$. If $(x, y) + (C_1, C_2^*) = (C_1 + e_i, C_2^* + e_i + e_{n+1})$ and $\forall j \neq i$ exists $s \neq i$ such that $(x, y) + (C_1 + e_j, C_2^* + e_j + e_{n+1}) = (C_1 + e_s, C_2^* + e_s + e_{n+1})$ then $x \in K_1 + e_i$ and $y \in K_2^* + e_i + e_{n+1}$. If $j = s$ we have $x \in K_1$ and $x \in K_1 + e_i$, but $K_1 \subseteq C_1$, so this is not possible. If $j \neq s$, $x \in K_1 + e_i$ and $x \in K_1 + e_j + e_s$, so $e_i + e_j + e_s \in K_1$ and $T_i \subseteq K_1$. Also, $y \in K_2^* + e_i + e_{n+1}$ and $y \in K_2^* + e_j + e_s$, so $e_i + e_j + e_s \in K_2$ and $T_i \subseteq K_2$. ∎

Now we have the necessary results to prove Theorem 3.14.

Proof: If $dim(H_1^\perp \cup H_2^\perp) = m + s$, then $dim(H_1^\perp \cap H_2^\perp) = 2m - (m + s) = m - s$. By Theorem 3.15 using the Doubling construction with the identity permutation we can construct a 1-perfect code C of length $n' = 2^{m+1} - 1$ such that $r(C) = 2n - dim(H_1^\perp \cap H_2^\perp) = 2n - m + s = n' - m' + s$ $\forall s \in \{1, \ldots, m\}$. We know that $< \bigcup_{i \in I} T_i > \subseteq H_1 \cap H_2$, so by Theorem 3.17 the dimension of the kernel is $k(C) \geq 2(n - m) + m - \delta = n' - m' - \delta$. If $H_1^\perp \cup H_2^\perp \subseteq < \bigcup_{i \in I} T_i >^\perp$, then $dim(H_1^\perp \cup H_2^\perp) \leq dim(< \bigcup_{i \in I} T_i >^\perp)$, so $s \leq 2^\delta - \delta - 1$. If we take the minimum δ such that $s \leq 2^\delta - \delta - 1$ then $k(C) \leq n' - m' - \delta$ by Theorem 3.8. ∎

3.5 Some results near the upper bound

In previous sections, we established the exact lower and upper bounds on the dimension of the kernel, once the rank is fixed, except the exact upper bound for full-rank 1-perfect codes of length $n = 2^m - 1$ if $4 \leq m < 10$. Now, we would like to know if we can construct binary 1-perfect codes with any rank and with kernels of any dimension between the lower and upper bounds.

In this section, we will see that we can construct binary 1-perfect codes of length $n = 2^m - 1$ with rank $r(C) < n$ and with kernels of dimension near the upper bound, that is between the upper bound and $2(n' - m')$, where $n' = 2^{m-1} - 1$ and $m' = m - 1$, or equivalently, with kernels of dimension $k(C) = n - m - \delta$ for any δ such that $2^\delta - \delta - 1 \geq s$ and $\delta < m$ if $r(C) = n - m + s$.

Using the Doubling construction, Lemma 5.6 gives us a construction of Hamming codes which allows us to obtain $\forall s \in \{1, \ldots, m-1\}$ 1-perfect codes of length $n = 2^m - 1$, rank $n - m + s$ and kernel of dimension $n - m - \delta$, where δ is the minimum integer such that $2^\delta - \delta - 1 \geq s$, that is, kernel with maximum dimension. But, in fact, we can prove a stronger result that will allow us to construct in a similar way 1-perfect codes with rank $n - m + s$ $\forall s \in \{2, \ldots, m-1\}$ and dimension of the kernel $n - m - \delta$ for any δ such that $2^\delta - \delta - 1 \geq s$ and $\delta < m$.

Notice that for $s = 1$, in [PL95] it is proved that we can construct 1-perfect codes with any dimension of the kernel between the lower and upper bounds using the Switching construction. We include this result in Lemma 2.37. This result shows that from a Hamming code, H_m, we can make one switch and have a 1-perfect code C, such that the rank is $r(C) = n - m + 1$ and the kernel has any dimension, $(n-1)/2 \leq k(C) \leq n - m - 2$.

Theorem 3.18. *For each $m \geq 3$ and $s \in \{2, \ldots, m\}$, there exist two Hamming codes H_1, H_2 of length $n = 2^m - 1$ such that*

$$dim(H_1^\perp \cup H_2^\perp) = m + s \quad and \quad I = \{i \mid T_i \subseteq H_1 \cap H_2\} = \emptyset$$

Proof: If $s = m$, we can take two different cyclic Hamming codes H_1, H_2. It is easy to see that $dim(H_1^\perp \cup H_2^\perp) = 2m$. In order to see that $I = \emptyset$, we can assume that there is a $T_i \subseteq H_1 \cap H_2$, but then $T_{i+1} \subseteq H_1 \cap H_2$ and we would have $H_1 = H_2$ because $H_1 \cap H_2$ is also a cyclic code.

Assume now $s < m$. Let A be a check matrix of a Hamming code of length $2^{m-s} - 1$. If $s \geq 3$, we can construct the Hamming codes H_1 and H_2 by the following check matrices

$$M_1 = \begin{pmatrix} 0 & b_1 \dots b_1 & b_2 \dots b_2 & \dots & b_{2^s-1} \dots b_{2^s-1} \\ A & 0\ A & 0\ A & \dots & 0\ A \end{pmatrix}$$

$$M_2 = \begin{pmatrix} 0 & c_1 b_1 \dots b_1 & c_2 b_2 \dots b_2 & \dots & c_{2^s-1} b_{2^s-1} \dots b_{2^s-1} \\ A & 0\ A & 0\ A & \dots & 0\ A \end{pmatrix}$$

where $B = (b_1\, b_2 \dots b_{2^s-1})$ and $C = (c_1\, c_2 \dots c_{2^s-1})$ are the check matrices of Hamming codes $\overline{H}_1$ and $\overline{H}_2$ such that $dim(\overline{H}_1^\perp \cup \overline{H}_2^\perp) = 2s$, and $\{i \mid T_i \subseteq \overline{H}_1 \cap \overline{H}_2\} = \emptyset$. In this case, $dim(H_1^\perp \cup H_2^\perp) = m - s + 2s = m + s$. Finally, we will show that $I = \emptyset$. Let $M_1(i)$, $M_2(i)$ denote the i^{th} columns of M_1, M_2 respectively; then it is sufficient to show that for any i there is a j such that columns $M_1(i)$, $M_1(j)$, $M_1(k)$ are dependent but columns $M_2(i)$, $M_2(j)$, $M_2(k)$ are not. We have several cases to consider. If $M_1(i) = \binom{b_r}{a_s}$, or $\binom{0}{a_s}$ then $M_1(i) = M_2(i)$. We can assume that $b_1 \neq c_1$ in which case we pick j such that $M_1(j) = \binom{b_1}{0}$ and $M_2(j) = \binom{c_1}{0}$. If $M_1(i) = \binom{b_r}{0}$ and $M_2(i) = \binom{c_r}{0}$ then by the properties of $\overline{H}_1$, $\overline{H}_2$ (or of B, C) we can pick j such that $M_1(j) = \binom{b_t}{0}$, $M_2(j) = \binom{c_t}{0}$ and b_r, b_t, b_u are dependent but c_r, c_t, c_u are not.

If $s = 2$, we can construct the Hamming codes in the same way, where $B = \begin{pmatrix} 011 \\ 101 \end{pmatrix}$ and $C = \begin{pmatrix} 101 \\ 110 \end{pmatrix}$. In this case $dim(H_1^\perp \cup H_2^\perp) = m + 2$, and we can see that $I = \emptyset$ using a similar argument as before and that the columns between C and D are all different. ∎

Now, we can prove the following result which is stronger than Lemma 3.13, for $s \geq 2$.

Lemma 3.19. *For each $m \geq 3$ and $s \in \{2, \ldots, m\}$, there exist two Hamming codes H_1, H_2 of length $n = 2^m - 1$ such that*

$$< \bigcup_{i \in I} T_i > \subseteq H_1 \cap H_2 \qquad dim(H_1^{\perp} \cup H_2^{\perp}) = m + s$$

and $\{k \mid T_k \subseteq H_1 \cap H_2\} = \{k \mid T_k \subseteq < \bigcup_{i \in I} T_i >\}$, where I is a set of $m - \delta$ independent coordinates, $2^{\delta} - \delta - 1 \geq s$ and $\delta \leq m$.

Proof: If $\delta = m$, $I = \emptyset$ and then $\{k \mid T_k \subseteq < \bigcup_{i \in I} T_i >\} = \emptyset$. In this case, we can take the Hamming codes H_1 and H_2 the same as Theorem 3.18.

If $\delta < m$, then $m \geq 4$ and we can use the same argument as in the proof of Lemma 3.13 but taking the two Hamming codes $\overline{H}_1$ and $\overline{H}_2$ such that $\{i \mid T_i \subseteq \overline{H_1} \cap \overline{H}_2\} = \emptyset$. We can do this, because of Theorem 3.18. ∎

Theorem 3.20. *For each $m \geq 4$ and $s \in \{1, \ldots, m-1\}$, there exists a 1-perfect code C of length $n = 2^m - 1$ with rank $n - m + s$ and a kernel of dimension $n - m - \delta$, where $2^{\delta} - \delta - 1 \geq s$ and $\delta < m$.*

Proof: If $s = 1$, using the Switching construction we have 1-perfect codes with any dimension of the kernel, [PL95].

If $s \geq 2$, using Lemma 3.19 and a similar argument as the proof of Theorem 3.14 we can construct $\forall s \in \{2, \ldots, m-1\}$ a 1-perfect code C of length $n = 2^m - 1$ which has rank $n - m + s$ and a kernel of dimension $n - m - \delta$ as long as $s \leq 2^{\delta} - \delta - 1$ and $\delta \leq m - 1$, because now we know exactly how many T_i there are in $H_1 \cap H_2$. ∎

3.6 Examples

By Theorem 3.20, we can construct $\forall s \in \{2, \ldots, m-1\}$ 1-perfect codes of length $n = 2^m - 1$, rank $n - m + s$ and kernel of dimension $n - m - \delta$, where $2^{\delta} - \delta - 1 \geq s$ and $\delta < m$, that is, with a kernel of any dimension between the upper bound and $2(n' - m')$, where $n' = 2^{m-1} - 1$ and $m' = m - 1$. This is because the maximum δ such

that $\delta < m$ is $m-1$ and in this case the dimension of the kernel is $n-m-(m-1) = n-2m+1 = 2(n'-m')$.

For $s = 1$ and $m \geq 5$, by Theorem 3.14 we can construct 1-perfect codes with maximum dimension of the kernel. But, in [PL95] it is proved that we can construct 1-perfect codes with any dimension of the kernel between the lower and upper bounds using the Switching construction.

For example, for $n = 31$ and $n = 63$, we have the following tables that show us for each rank the dimensions of the kernel we can get using Theorem 3.20.

$n = 31$ $r(C)$	$k(C)$										
26	26										
27		24	23	22	21	...	15				
28			23	22	?	...	?	8			
29			23	22	?	...	...	?	4		
30			23	22	?	...	...	...	?	2	
31				?	...	...	...	...	...	?	1

$n = 63$ $r(C)$	$k(C)$											
57	57											
58		55	54	53	52	51	...	31				
59			54	53	52	?	...	?	16			
60			54	53	52	?	...	...	?	8		
61			54	53	52	?	...	...	...	?	4	
62				53	52	?	...	...	...	...	?	2
63				?	...	...	...	...	...	...	...	?	1

In this section, we will give some examples of 1-perfect codes of length $n = 31$.

To construct a 1-perfect code of length 31, rank 26+s and a kernel of maximum dimension $26-\delta$, by Theorem 3.14, we need two Hamming codes H_1, H_2 of length 15 such that $dim(H_1^{\perp} \cup H_2^{\perp}) = 4+s$ and $H_1^{\perp} \cup H_2^{\perp} \subseteq < \bigcup_{i \in I} T_i >^{\perp}$, where I is a set of $m-\delta$ independent coordinates and δ is the minimum integer such that $2^{\delta} - \delta - 1 \geq s$.

Example 1: If $s = 1$, the minimum δ such that $2^{\delta} - \delta - 1 \geq 1$ is $\delta = 2$, so $|I| = 2$. By the proof of Lemma 3.13, we can choose the following check matrices for these Hamming codes:

$$\begin{pmatrix} 000 & b_1b_1b_1b_1 & b_2b_2b_2b_2 & b_3b_3b_3b_3 \\ 101 & 0101 & 0101 & 0101 \\ 011 & 0011 & 0011 & 0011 \end{pmatrix}$$

$$\begin{pmatrix} 000 & b_1b_1b_1b_1 & b_2b_2b_2b_2 & b_3b_3b_3b_3 \\ 101 & 0101 & 0101 & 1010 \\ 011 & 0011 & 0011 & 0011 \end{pmatrix}$$

where $B = (b_1\ b_2\ b_3) = \begin{pmatrix} 011 \\ 101 \end{pmatrix}$.

In this case, $dim(H_1^{\perp} \cup H_2^{\perp}) = 5$ and $H_1^{\perp} \cup H_2^{\perp} \subseteq < \bigcup_{i \in I} T_i >^{\perp}$, where $|I| = 2$, so $dim(H_1^{\perp} \cap H_2^{\perp}) = 4+4-5 = 3$, $T_1 \subseteq H_1 \cap H_2$ and $T_2 \subseteq H_1 \cap H_2$. Using the Doubling construction and by Theorem 3.15 and 3.17, we can obtain a 1-perfect code C of length 31, with $r(C) = 2 \cdot 15 - dim(H_1^{\perp} \cap H_2^{\perp}) = 30 - 3 = 27$ and $k(C) = 11 + 11 + 2 = 24$, which is the upper bound for rank 27.

Example 2: If $s = 4$, the minimum δ such that $2^{\delta} - \delta - 1 \geq 4$ is $\delta = 3$, so $|I| = 1$. By the proof of Lemma 3.13, we can choose the following check matrices for these Hamming codes:

$$\begin{pmatrix} 0 & c_1c_1 & c_2c_2 & \dots & c_7c_7 \\ 1 & 0\ 1 & 0\ 1 & \dots & 0\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & d_1d_1 & d_2d_2 & \dots & d_7d_7 \\ 1 & 1\,0 & 0\,1 & \dots & 0\,1 \end{pmatrix}$$

where

$$C = \begin{pmatrix} 1000111 \\ 1011001 \\ 1101010 \end{pmatrix} \quad D = \begin{pmatrix} 1001101 \\ 0011011 \\ 1100011 \end{pmatrix}$$

are check matrices of two Hamming codes $\overline{H}_1$ and $\overline{H}_2$ of length 7 such that $dim(\overline{H}_1^{\perp} \cup \overline{H}_2^{\perp}) = 6$ and the subspace $\overline{H}_1^{\perp} \cup \overline{H}_2^{\perp}$ is generated by the last 6 coordinates.
In this case, $dim(H_1^{\perp} \cup H_2^{\perp}) = 8$ and $H_1^{\perp} \cup H_2^{\perp} \subseteq T_1^{\perp}$. So, using the Doubling construction and by Theorem 3.15 and 3.17, we can get a 1-perfect code C of length 31, with $r(C) = 30$ and $k(C) = 23$, which is the upper bound for rank 30.

It is also possible to construct 1-perfect codes with an allowed kernel not necessary of maximum dimension. Next, we will show an example of a 1-perfect code of length 31, such that its kernel does not have maximum dimension.

Example 3: If we want to construct a 1-perfect code of length 31, rank $r(C) = 26 + 3 = 29$ and kernel of dimension 22, which is not the highest possible, we need two Hamming codes H_1, H_2 of length 15 such that $dim(H_1^{\perp} \cup H_2^{\perp}) = 4 + 3 = 7$ and without any T_i in the intersection $H_1 \cap H_2$, so such that $I = \{i \ : \ T_i \subseteq H_1 \cap H_2\} = \emptyset$, since we want $22 = 31 - 5 - \delta$, $\delta = 4$ and $m - \delta = 0$.
In this case, $s = 3$. By the proof of Theorem 3.18, we can construct the Hamming codes H_1 and H_2 defined by the following check matrices:

$$M_1 = \begin{pmatrix} 0 & b_1b_1 & b_2b_2 & \dots & b_7b_7 \\ 1 & 0\,1 & 0\,1 & \dots & 0\,1 \end{pmatrix}$$

$$M_2 = \begin{pmatrix} 0 & c_1b_1 & c_2b_2 & \dots & c_7b_7 \\ 1 & 0\,1 & 0\,1 & \dots & 0\,1 \end{pmatrix}$$

where

$$B = \begin{pmatrix} 1011100 \\ 0101110 \\ 0010111 \end{pmatrix} \quad C = \begin{pmatrix} 1110100 \\ 0111010 \\ 0011101 \end{pmatrix}$$

are check matrices of two Hamming codes $\overline{H}_1$ and $\overline{H}_2$ of length 7 such that $dim(\overline{H}_1^{\perp} \cup \overline{H}_2^{\perp}) = 6$ and $\{i \ : \ T_i \subseteq \overline{H}_1 \cap \overline{H}_2\} = \emptyset$. We can take $\overline{H}_1$ and $\overline{H}_2$ as two different cyclic Hamming codes generated by the primitive polynomials $g_1(x) = x^3+x+1$ and $g_2(x) = x^3+x^2+1$ respectively. Then, we have $dim(H_1^{\perp} \cup H_2^{\perp}) = 7$, $dim(H_1^{\perp} \cap H_2^{\perp}) = 8-7 = 1$ and $I = \{i \ : \ T_i \subseteq H_1 \cap H_2\} = \emptyset$. Using the Doubling construction and Theorems 3.15 and 3.17, we can obtain a 1-perfect code C of length 31, with $r(C) = 30-1 = 29$ and $k(C) = 11 + 11 = 22$.

3.7 Bulging middle

In this section, we will show how to construct 1-perfect codes with different ranks and different kernel dimensions between the lower and upper bound. In order to do that, we will use the Doubling construction and the results of section 3.4.

We will obtain a large number of cases, but we do not completely settle the question, for what pairs of numbers (r, k) does there exist a binary 1-perfect code C of length $n = 2^m - 1$ having $r(C) = r$ and $k(C) = k$.

Let C_1 be a 1-perfect code of length n and C_2^* be an extended 1-perfect code of length $n + 1$. By Proposition 2.6, the code

$$C = (C_1 \oplus C_2^*) \bigcup_{i=1}^{n} (C_1 + e_i \oplus (C_2 + e_{\pi(i)})^*)$$

where π is a permutation on the set $\{1, 2, \ldots, n\}$ is a 1-perfect code of length $2n + 1$.

By Theorem 3.15, we know the rank of the 1-perfect code C of length $2n + 1$ constructed as above and taking as π the identity permutation is

$$r(C) = 2n - r(C_1^{\perp} \cap C_2^{\perp})$$

So, we are interested in knowing how we can choose the 1-perfect codes C_1 and C_2 to obtain different dimensions of $C_1^\perp \cap C_2^\perp$ and therefore different ranks for the 1-perfect code C. We will compute this dimension in different cases which will also allow us to know the kernel dimension for the 1-perfect code C of length $2n+1$.

In this first case, if we use the following result and Lemma 2.31, we will be able to construct, in a recursive way, 1-perfect codes with all different ranks (except full-rank codes) and with different kernel dimensions, between the lower and upper bound, for a fixed rank. We will show, with some examples ($n = 31$ and $n = 63$), that we can not obtain codes for all the possible kernel dimensions.

Proposition 3.21. *Given two 1-perfect codes of length n, $\overline{C}_1$ and $\overline{C}_2$ such that $r(\overline{C}_2) \leq r(\overline{C}_1)$, we can obtain two 1-perfect codes C_1 and C_2 isomorphic to $\overline{C}_1$ and $\overline{C}_2$ respectively such that $\langle C_2 \rangle \subseteq \langle C_1 \rangle$.*

Proof: If $r(\overline{C}_2) \leq r(\overline{C}_1)$, then $r(\overline{C}_1^\perp) \leq r(\overline{C}_2^\perp)$. Since the dual codes are linear codes and $r(\overline{C}_1^\perp) \leq r(\overline{C}_2^\perp)$, there exist $C_1^\perp$ and $C_2^\perp$ isomorphic codes to $\overline{C}_1^\perp$ and $\overline{C}_2^\perp$ respectively, such that $C_1^\perp \subseteq C_2^\perp$. Using the same permutation, we have codes C_1 and C_2 isomorphic to $\overline{C}_1$ and $\overline{C}_2$ respectively, such that $\langle C_2 \rangle \subseteq \langle C_1 \rangle$. ∎

By Proposition 3.21, given two 1-perfect codes $\overline{C}_1$ and $\overline{C}_2$ of length $n = 2^m - 1$ and ranks $r(\overline{C}_1) = n - m + s$ and $r(\overline{C}_2) = n - m + s'$, where $s, s' \in \{0, 1, \ldots, m\}$ and $s' \leq s$, we can obtain 1-perfect codes C_1 and C_2 isomorphic to $\overline{C}_1$ and $\overline{C}_2$ respectively such that $r(C_1^\perp \cap C_2^\perp) = r(C_1^\perp) = m - s$, since $\langle C_2 \rangle \subseteq \langle C_1 \rangle$. Then, the code C of length $2n+1$ constructed with the Doubling construction and taking the identity permutation has rank $r(C) = 2n - (m - s) = 2^{m+1} - 1 - (m+1) + s$, where $s \in \{0, 1, \ldots, m\}$. Taking codes C_1 of length n with all possible ranks we obtain codes C of length $2n+1$ with all possible ranks except rank $2n+1$, those which are full-rank codes.

By Lemma 2.31, we know the kernel dimension of the 1-perfect code C of length

$2n+1$ constructed using the Doubling construction and taking the identity permutation is $k(C) = k_1 + k_2$, where $k_1 = k(C_1)$ and $k_2 = k(C_2)$ as long as $k_1 < (n-1)/2$.

Next, with some examples, we show for which pairs $(r(C), k(C))$ we can construct a 1-perfect code of rank $r(C)$ and kernel dimension $k(C)$.

Example 1: There exist 1-perfect codes of length 31 for the pairs $(r(C), k(C))$ which correspond to

- 1-perfect codes with the lower and upper bounds of the dimension of the kernel for a fixed rank except full-rank 1-perfect codes with the upper bound if $4 \leq m < 10$ (using the results in sections 3.2 and 3.3).

- 1-perfect codes C of length n with $k(C)$ near the upper bound, exactly with $k(C)$ between the upper bound and $2(n'-m')$, where $n' = 2^{m-1}-1$ and $m' = m-1$, except for full-rank 1-perfect codes (using section 3.5).

- 1-perfect codes C with rank $r(C) = n-m+1$, in this example $r(C) = 27$, and with any dimension of the kernel between the lower and upper bounds. It was proved in [PL95] that from a Hamming code, H_m, we can make one switch and obtain a 1-perfect code C, with rank $r(C) = n-m+1$ and kernel dimension with any value, $(n-1)/2 \leq k(C) \leq n-m-2$, in this example $15 \leq k(C) \leq 24$.

- 1-perfect codes constructed from the above arguments using Proposition 3.21, Lemma 2.31 and the pairs $(r(C), k(C))$ for which it is known there exists a 1-perfect code of length 15 having rank $r(C)$ and kernel of dimension $k(C)$ (see table in page 40).

We summarize all these results in the following table. The question mark sign means that by using the previous results we do not know if there exist 1-perfect codes with these parameters.

$r(C)$	$k(C)$														
26	26														
27		24	23	22	...	...	...	...	...	15					
28			23	22	?	...	?	17	...	...	8				
29			23	22	?	...	?	17	...	...	...	4			
30			23	22	?	...	...	?	16	...	...	...	2		
31				?	...	...	...	...	...	...	...	...	?	1	

Example 2: There exist 1-perfect codes of length 63 for the following pairs of numbers $(r(C), k(C))$ doing the same as before starting from the table of length 31.

$r(C)$	$k(C)$																
57	57																
58		55	54	53	52	...	...	...	...	31							
59			54	53	52	?	...	?	40	...	...	...	16				
60			54	53	52	?	...	?	40	...	...	...	...	8			
61			54	53	52	?	...	?	40	...	...	...	...	...	4		
62				53	52	?	...	...	...	?	27	25	...	...	...	2	
63				?	...	...	...	...	...	...	...	...	...	...	...	?	1

In a more general case, in order to use that by Proposition 3.17, the kernel of C is

$$(K_1 \oplus K_2^*) \bigcup_{i \in I} (K_1 + e_i \oplus (K_2 + e_i)^*)$$

where K_1 and K_2 are the kernels of C_1 and C_2 respectively and $I = \{i : T_i \subseteq K_1 \cap K_2\}$, we are interested in results that will give us how many T_i are in $K_1 \cap K_2$. We will study the case when $I = \emptyset$ and it is possible to know the rank of $C_1^\perp \cap C_2^\perp$. In this case, the kernel dimension of the 1-perfect code C of length $2n+1$ will be $k(C) = k_1 + k_2$, where $k_1 = k(C_1)$ and $k_2 = k(C_2)$, and the rank $r(C) = 2n - r(C_1^\perp \cap C_2^\perp)$.

There is a well known result due to Luc Teirlinck [Tei77] which states that given any two Steiner triple systems (S, B_1), (S, B_2) on the same set of points, S, there

is a permutation π of S such that $B_1 \cap \pi(B_2) = \emptyset$. This means that given any two 1-perfect codes C_1, C_2 there is an isomorphic copy of C_2 such that these codes have no words of weight 3 in common. Using these codes in the Doubling construction would produce a code of length $2n+1$ with $I = \emptyset$, that is, whose kernel is $K_1 \oplus K_2^*$, where K_1 and K_2 are the kernels of C_1 and C_2 respectively. In fact, we do not need the triple systems to be disjoint for this result, a weaker condition will suffice.

Let C_1 and C_2 be two 1-perfect codes of length $n = 2k+1$ and let (S, B_1) and (S, B_2) be the respective triple systems corresponding to the words of weight 3 in each. Let $S = \{\infty, x_1, \ldots, x_k, y_1, \ldots, y_k\}$ and assume that the triples through ∞ are $\{\infty, x_1, y_1\}$, ..., $\{\infty, x_k, y_k\} \in B_1 \cap B_2$. Apply the permutation $\pi = (x_1 \ \ldots \ x_k)$ to B_2 giving a triple system $\pi(B_2)$. Clearly the triples through ∞ are different in B_1 and $\pi(B_2)$. Also for each $x_i \in S$ the triple $\{\infty, x_i, y_i\} \in B_1$ and $\{\infty, x_i, y_{i-1}\} \in \pi(B_2)$; similarly for each $y_i \in S$. Thus $B_1 \cap \pi(B_2)$ does not contain all k triples through any given point. In this case we have $I = \{i : T_i \subseteq K_1 \cap K_2\} = \emptyset$ but it is not easy to know $r(C_1^\perp \cap C_2^\perp)$.

Next, we will prove some results which will allow us to know the structure of the dual code. With these results we will show that given two 1-perfect codes of length $n = 2^m - 1$ with kernels of dimension k_1 and k_2 respectively and ranks $n - r_1$ and $n - r_2$, $r_1 \leq r_2$, then there exists a 1-perfect code C of length $2n+1$ with kernel of dimension $k(C) = k_1 + k_2$ and rank $r(C) = 2n - r_1$ if $r_1 \leq m - 2$.

Lemma 3.22. [KS93] *Let C be a 1-perfect code of length $n = 2^m - 1$ and rank $r(C) = n - m + s$. The set $V = \{i \mid x_i = 0 \ \forall x \in C^\perp\}$ is an $s-1$ flat in the projective space $PG(m-1, 2)$, so $|V| = 2^s - 1$, and*

$$\langle C \rangle = H_m \bigcup_{j \in V} (H_m + e_j)$$

where H_m is a Hamming code of length $n = 2^m - 1$.

Proposition 3.23. *Let C be a 1-perfect code of length $n = 2^m - 1$ and rank $r(C) = n - m + s$. The generator matrix H for the dual code $C^\perp$ is a matrix $(m-s) \times n$ such*

that every nonzero vector of length $m-s$ occurs as a column vector 2^s times and the zero vector occurs 2^s-1 times.

Proof: The dual code $C^\perp$ is a vector space of dimension $m-s$, so the generator matrix H is a $(m-s)\times n$ matrix,

$$H = (h_1\ h_2\ \ldots\ h_n)$$

where h_i are column vectors of length $m-s$. By Lemma 3.22 we know $\langle C\rangle = H_m \cup_{j\in V}(H_m + e_j)$, where H_m is a Hamming code of length $n = 2^m-1$, $V = \{i \mid x_i = 0\ \forall x \in C^\perp\}$ and $|V| = 2^s-1$. Since $H_m \subseteq \langle C\rangle$, the rows of the matrix H are $m-s$ rows of the check matrix of the Hamming code H_m. Since $H_m + e_j \subseteq \langle C\rangle$, the column $h_j = 0\ \forall j \in V$, so the zero vector occurs $|V| = 2^s-1$ times in H. Taking only the $m-s$ rows in the check matrix of the Hamming code H_m such that have zeros in the j^{th} component $\forall j \in V$, every nonzero $m-s$ vector occurs as a column vector equally often 2^s times. ∎

We can always order the column vectors of the generator matrix of $C^\perp$, H, lexigraphically.

It is easy to see that the direct sum of the symmetric group of 2^s-1 symbols, S_{2^s-1}, with $2^{m-s}-1$ copies of S_{2^s} is the group of permutations that fix the generator matrix of $C^\perp$. The perfect code C will have $2^{m-s}-1$ copies of the $STS(2^{s+1}-1)$ all intersecting in the same 2^s-1 coordinates (the zero columns). The other 2^s coordinates in each system correspond to 2^s identical nonzero columns of H.

Example: If C is a 1-perfect code of length 31 and rank $r(C) = n-m+s = 31-5+2 = 28$, a generator matrix H of the dual code $C^\perp$ is the following:

$$H = \begin{pmatrix} 000 & 0000 & 0000 & 0000 & 1111 & 1111 & 1111 & 1111 \\ 000 & 0000 & 1111 & 1111 & 0000 & 0000 & 1111 & 1111 \\ 000 & 1111 & 0000 & 1111 & 0000 & 1111 & 0000 & 1111 \end{pmatrix}$$

The direct sum of the symmetric group of 3 symbols S_3 with 7 copies of S_4 is the group of permutations that fix H. The perfect code C will have 7 copies of the $STS(7)$ all intersecting in the first 3 coordinates. The other 4 coordinates in each system correspond to 4 identical nonzero columns of H.

Proposition 3.24. *If there exist two 1-perfect codes of length $n = 2^m - 1$ with kernels of dimension k_1 and k_2 respectively and ranks $n - r_1$ and $n - r_2$, $0 \leq r_1 \leq r_2 \leq m$, then there exists a 1-perfect code C of length $2n+1$ with kernel of dimension $k(C) = k_1 + k_2$ and rank $r(C) = 2n - r_1$ if $r_1 \leq m - 2$.*

Proof: Let $\overline{C}_1$ and $\overline{C}_2$ be the two 1-perfect codes of length $n = 2^m - 1$ with rank $n - r_1$ and $n - r_2$, $0 \leq r_1 \leq r_2 \leq m$, respectively. Since $n - r_1 \geq n - r_2$, by Proposition 3.21 there exist two 1-perfect codes C_1 and C_2 isomorphic to $\overline{C}_1$ and $\overline{C}_2$ respectively such that $\langle C_2 \rangle \subseteq \langle C_1 \rangle$ or equivalently, $C_1^{\perp} \subseteq C_2^{\perp}$.

By Proposition 3.15, the rank of the 1-perfect code C obtained using the Doubling construction and taking as π the identity permutation is $r(C) = 2n - r_1$, $0 \leq r_1 \leq m$. By Proposition 3.17, the kernel of C is

$$(K_1 \oplus K_2^*) \bigcup_{i \in I} (K_1 + e_i \oplus (K_2 + e_i)^*)$$

where K_1 and K_2 are the kernels of C_1 and C_2 respectively and $I = \{i : T_i \subseteq K_1 \cap K_2\}$. If we find there exist isomorphic copies of C_1 and C_2 such that we still have $C_1^{\perp} \subseteq C_2^{\perp}$ and $I = \emptyset$, the 1-perfect code C would have a kernel of dimension $k(C) = k_1 + k_2$ and rank $r(C) = 2n - r_1$. In order to have $I = \emptyset$, we do not need the triple systems of C_1 and C_2 to be disjoint, we just need they do not contain all triples through any given point.

Let H_1 and H_2 be the generator matrices of $C_1^{\perp}$ and $C_2^{\perp}$ respectively, with the column vectors ordered lexigraphically. If $r_1 = m - s \leq m - 2$, then $s \geq 2$. By Proposition 3.23, in the matrix H_1, every nonzero vector of length $r_1 = m - s$ occurs as a column vector $2^s \geq 4$ times and the zero vector occurs $2^s - 1 \geq 3$ times.

We assume that $I \neq \emptyset$. Let T_i and T_i' denote the subspace generated by the words of weight 3 that have a one in the i^{th} coordinate in C_1 and C_2 respectively. For each $i \in I$, $T_i = T_i' \subseteq K_1 \cap K_2 \subseteq C_1 \cap C_2$, we will see we can make a transposition to C_2 such that fix i, fix the generator matrix H_1 and $T_i \neq T_i'$. If i is one of the first $2^s - 1$ coordinates (the zero columns) in H_1, we choose a subset of 2^s coordinates which correspond to the same column vector in H_1. Notice that in a vector $\chi(\{i, j, k\}) \in T_i$, j and k either are both in the first $2^s - 1$ coordinates or are in the same subset of 2^s coordinates. We can make a transposition of two of these $2^s \geq 4$ coordinates in the same subset such that $T_i \neq T_i'$. If i is in a set of $2^s \geq 4$, we can also make a transposition of two of these $2^s \geq 4$ coordinates in the same subset such that $T_i \neq T_i'$ and fix i. ∎

Next, using Proposition 3.24 instead of Proposition 3.21 and Lemma 2.31 and doing the same as in the examples 1 and 2 (pages 62 and 63), we have the following pairs $(r(C), k(C))$ for which exist 1-perfect codes of length 31 and 63.

$r(C)$	$k(C)$														
26	26														
27		24	23	22	...	...	...	...	...	15					
28			23	22	?	...	?	19	...	...	8				
29			23	22	?	...	?	19	...	...	...	4			
30			23	22	?	...	...	?	16	...	...	...	2		
31				?	...	...	...	...	...	...	...	...	?	1	

$r(C)$	$k(C)$																
57	57																
58		55	54	53	52	...	...	...	...	31							
59			54	53	52	?	...	?	49	...	...	...	16				
60			54	53	52	?	...	?	49	...	...	...	...	8			
61			54	53	52	?	...	?	49	...	...	...	...	...	4		
62				53	52	?	...	...	...	?	27	25	...	...	...	2	
63				?	...	...	...	...	...	...	...	...	...	...	...	?	1

Althought Proposition 3.24 give a stronger result than Proposition 3.21 and Lemma 2.31, since we do not use $k_1 < (n-1)/2$, we still can not obtain all possible pairs $(r(C), k(C))$, 1-perfect codes with all different kernel dimensions between the lower and upper bound for a fixed rank. Even if we knew how to construct full-rank 1-perfect codes for any $k(C)$ and any length, we would not obtain all the others.

Chapter 4

Q-ary perfect codes

In previous chapters, we discussed about binary 1-perfect codes. We gave some known definitions and results in chapter 2 and we proved some new results about the rank and the kernel of these codes in chapter 3. In this chapter, we will give the generalization, to q-ary 1-perfect codes, of definitions and results we can find in the previous chapters for the binary 1-perfect codes. The rank and the kernel of q-ary 1-perfect codes ($q \neq 2$) have not been studied before. The most important result in this chapter is the existence of q-ary 1-perfect codes of length $n = \frac{q^m - 1}{q - 1}$ with any possible rank, $\forall m \geq 4$. On the kernel of q-ary 1-perfect codes we will not give any result in this dissertation.

In section 4.1 we will review some definitions and known properties for q-ary 1-perfect codes. In section 4.2 we will show some known constructions of q-ary 1-perfect codes. In section 4.3, first of all we will generalize an approach of a well-known construction of binary 1-perfect codes, the Switching construction, to obtain q-ary 1-perfect codes. Then, using this construction, we establish the existence of q-ary 1-perfect codes of length $n = \frac{q^m - 1}{q - 1}$ for $m \geq 4$ and rank $r(C) = n - m + s$ for each $s \in \{1, \ldots, m\}$. This is a generalization of the binary case proved by Etzion and Vardy in [EV94]. All the results given in this last section are new and they will be also shown in [PV01b].

4.1 Definitions and Properties

Let $\mathbb{F}_q^n$ be a vector space of dimension n over a Galois Field $\mathbb{F}_q = GF(q)$. The *Hamming distance* between vectors $x,\ y \in \mathbb{F}_q^n$, denoted $d(x,y)$, is the number of coordinates in which x and y differ. The *Hamming weight* of x is given by $wt(x) = d(x,\mathbf{0})$, where $\mathbf{0}$ is the all-zero vector. Obviously, $d(x,y) = wt(x-y)$.

A *q-ary code*, C, of length n is simply a subset of $\mathbb{F}_q^n$. Without loss of generality, we shall assume, unless stated otherwise, that the all-zero vector is in C. The elements of C are called *codewords* and C is called *linear* if it is a linear space over $\mathbb{F}_q$. In other words, if x and y are codewords, then $\lambda x + \mu y$ is contained in the code as well, $\forall \lambda, \mu \in \mathbb{F}_q$. The *minimum distance* of a code is the smallest distance between a pair of codewords.

We shall define an *extended code* of the q-ary code C, denoted by C^*, to be the code resulting from adding an overall parity check digit to each codeword of C, thereby causing all of the codewords $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ to satisfy $\sum_{i=1}^n x_i = 0$ in $\mathbb{F}_q$.

A *monomial matrix* is a matrix with exactly one nonzero entry in each row and column. Two codes $C_1,\ C_2 \subset \mathbb{F}_q^n$, are said to be *isomorphic* if there exists a $n \times n$ monomial matrix A over $\mathbb{F}_q$ such that $C_2 = \{cA \ :\ c \in C_1\}$, [MS77]. They are said to be *equivalent* if there exists a vector v and a $n \times n$ monomial matrix A over $\mathbb{F}_q$ such that $C_2 = \{v + cA \ :\ c \in C_1\}$. There is a more general definition of equivalent codes. Two codes $C_1,\ C_2 \subset \mathbb{F}_q^n$, are said to be *equivalent* if there are n permutations $\tau_1, \ldots, \tau_n$ of the q elements in $\mathbb{F}_q$ and a permutation σ of the n components such that $C_2 = \{\sigma(\tau_1(c_1), \tau_2(c_2), \ldots, \tau_n(c_n)) \ :\ (c_1, c_2, \ldots, c_n) \in C_1\}$, [CHLL97].

A q-ary code C of length n is *perfect* if for some integer $r \geq 0$ every $x \in \mathbb{F}_q^n$ is within distance r from exactly one codeword of C. A q-ary perfect code attains the *sphere-packing* or *Hamming bound*, that is that the spheres of radius r around the codewords partition the whole space $\mathbb{F}_q^n$, or equivalently

$$|C| = \frac{q^n}{\sum_{i=0}^{r} \binom{n}{r}(q-1)^i}$$

where $\sum_{i=0}^{r} \binom{n}{r}(q-1)^i$ is the number of vectors of length n contain in a sphere of radius r around the codewords, [MS77]. We can also define a q-ary perfect code as a q-ary code such that the Hamming bound holds. A q-ary perfect code of length n can correct r errors, so they are also called *perfect r-error correcting codes* or *r-perfect codes*. If $|C| \geq 2$, then the minimum distance of such a code is $d = 2r + 1$.

In [Tie73, ZL73], was proved that the only perfect codes of length n over a prime power alphabet are:

- *trivial q-ary perfect codes* in cases $r = 0$ and $r = n$.
- *binary repetition code* in case $r = (n-1)/2$ with n odd.
- *binary Golay code* in case $r = 3$ with $n = 23$.
- *ternary Golay code* in case $r = 2$ with $n = 11$.
- *q-ary 1-perfect codes* in case $r = 1$ with $n = \dfrac{q^m - 1}{q - 1}$, $m \geq 2$, where q is a prime or prime power.

Over an arbitrary alphabet, different to a prime power, the only known perfect codes are the trivial ones. These are the codes containing all vectors of some length over some alphabet which are 0-perfect codes and the codes consisting of only one codeword of length n which are r-perfect codes for each $r \geq n$. In [Bes83], Best showed that in general there are not unknown r-perfect codes over arbitrary alphabets for $r \notin \{1, 2, 6, 8\}$.

The binary and ternary Golay codes are unique up to equivalence, [Ple68, DG75]. The linear q-ary 1-perfect codes are, again, unique up to equivalence, [MS77]. They are the well-known *q-ary Hamming codes* and exist for all $m \geq 2$. Nonlinear q-ary 1-perfect codes also exist for $q = 2, m \geq 4$; $q \geq 3, m \geq 3$, and for q a prime power, $q \neq 4$ or 8, $m \geq 2$, [Vas62], [Sch68], [Lin69]. For $q = 2$, in section 2.3 we have seen some constructions of nonlinear 1-perfect codes. For other q's, constructions of nonlinear 1-perfect codes were presented by Schönheim [Sch68], Lindström [Lin69],

Phelps [Phe84b], Mollard [Mol86] and Etzion [Etz96]. Some of these constructions are outlined in section 4.2.

The q-ary 1-perfect codes have length $n = \dfrac{q^m - 1}{q - 1}$, $m \geq 2$, and $r = 1$. They have q^{n-m} codewords and minimum distance 3.

A *q-ary 1-perfect partition*, as in the binary case, is a partition of the space $\mathbb{F}_q^n$ into $n(q-1)+1$ 1-perfect codes $C_0, C_1, \ldots, C_{n(q-1)}$. We can assume the zero vector is in C_0. Given a q-ary 1-perfect code C of length $n = (q^m - 1)/(q-1)$ we know that there always exists $n(q-1)+1 = q^m$ translates of C, that form a q-ary 1-perfect partition of $\mathbb{F}_q^n$, taking $C + \alpha^j e_i$, $\forall j \in \{1, \ldots, q-1\}$, $i \in \{1, \ldots, n\}$, where α is a primitive element of $\mathbb{F}_q$ and e_i denote the vector of length n having all components equal to zero, except the i^{th} component, which contains a one. We will call this partition the *trivial partition*.

We know that binary 1-perfect codes are distance invariant codes, [SS59] (or see Proposition 2.15). Abdurahmanov [Abd91] showed the same result for any q-ary 1-perfect code.

4.2 Constructions of q-ary 1-perfect codes

In this section, we briefly outline some known constructions of nonlinear q-ary 1-perfect codes. In [CHLL97], we can also find a description of these constructions, which we include now.

The first construction of nonlinear q-ary 1-perfect codes is due to Schönheim [Sch68] and it is a generalization of binary Vasil'ev's construction (Proposition 2.4) to the q-ary case. We do not describe it now, but we will give two constructions, which are generalizations of this construction as well as generalizations to the q-ary case of constructions given by Proposition 2.5, which was itself a generalization of Vasil'ev's construction.

Consider the lexicographical order on the coordinates of any vector $u \in \mathbb{F}_q^{(q-1)n_1n_2}$, $u = (u_{1,1,1}, u_{1,1,2}, \ldots, u_{q-1,n_1,n_2})$. If $s_i = \sum_{h=1}^{q-1} \sum_{j=1}^{n_2} u_{h,i,j}$ and $s'_j = \sum_{h=1}^{q-1} h \sum_{i=1}^{n_1} u_{h,i,j}$, we define $\pi_1(u) \in \mathbb{F}_q^{n_1}$ and $\pi_2(u) \in \mathbb{F}_q^{n_2}$ in the following way:

$$\pi_1(u) = (s_1, s_2, \ldots, s_{n_1})$$
$$\pi_2(u) = (s'_1, s'_2, \ldots, s'_{n_2})$$

Let C_1 and C_2 be two q-ary 1-perfect codes of lengths $n_1 = \dfrac{q^{m_1}-1}{q-1}$ and $n_2 = \dfrac{q^{m_2}-1}{q-1}$ respectively, over $\mathbb{F}_q$. Let $f : C_1 \longrightarrow \mathbb{F}_q^{n_2}$ be an arbitrary mapping.

Proposition 4.1. [Mol86] *The code F defined by*

$$F = \{(u|v_1 + \pi_1(u)|v_2 + \pi_2(u) + f(v_1)) \ : \ u \in \mathbb{F}_q^{(q-1)n_1n_2},\ v_1 \in C_1,\ v_2 \in C_2\}$$

is a q-ary 1-perfect code of length $n = \dfrac{q^{m_1+m_2}-1}{q-1}$.

Note that for $q = 2$ we have Proposition 2.5, for $n_2 = 1$ we would have the generalization of Proposition 2.4, that is the Vasil'ev's construction, to q-ary case, and for $q = 2$ and $n_2 = 1$ we obtain Proposition 2.4.

Next construction is a less straightforward generalization of Proposition 2.4 to the q-ary case, and it is due to Phelps [Phe84b].

Let C_1 and C_2 be two q-ary 1-perfect codes of lengths $n_1 = \dfrac{q^{m_1}-1}{q-1}$ and $n_2 = \dfrac{q^{m_2}-1}{q-1}$ respectively, over $\mathbb{F}_q$. Let C_3 be a q-ary 1-perfect code of length $q+1$ and cardinality q^{q-1}. Let C_4 and C_5 be two q-ary $(n_1+2, q^{n_1+1}, 2)$ and $(n_2+2, q^{n_2+1}, 2)$ codes, respectively. Because they have minimum distances 3, 2 and 2, respectively, the codes C_3, C_4 and C_5 can be expressed as

$$C_3 = \{(x|f_1(x)|f_2(x)) \ : \ x \in \mathbb{F}_q^{q-1}\}$$
$$C_4 = \{(x|f_3(x)) \ : \ x \in \mathbb{F}_q^{n_1+1}\}$$
$$C_5 = \{(x|f_4(x)) \ : \ x \in \mathbb{F}_q^{n_2+1}\}$$

where $f_i(x) \in \mathbb{F}_q$ for $i = 1, 2, 3, 4$ and can be interpreted as a parity function.
For $c = (c_1, c_2, \ldots, c_{n_1}) \in C_1$, $d = (d_1, d_2, \ldots, d_{n_2}) \in C_2$, $u_{i,j} \in \mathbb{F}_q^{q-1}$, for $i = 1, 2, \ldots, n_1$ and $j = 1, 2, \ldots, n_2$, let $a_i = f_4(f_1(u_{i,1}), \ldots, f_1(u_{i,n_2}), c_i)$ and $b_j = f_3(f_2(u_{1,j}), \ldots, f_2(u_{n_1,j}), d_j)$.

Proposition 4.2. [Phe84b] *The code F defined by*

$$F = \{(u_{1,1}|\cdots|u_{i,j}|\cdots|u_{n_1,n_2}|(a_1, a_2, \ldots, a_{n_1}, b_1, b_2, \ldots, b_{n_2})) \ : \\ u_{i,j} \in \mathbb{F}_q^{q-1},\ c \in C_1,\ d \in C_2\}$$

is a q-ary 1-perfect code of length $n = \dfrac{q^{m_1+m_2}-1}{q-1}$.

When $q = 2$, if we take $C_3 = \{(000), (111)\}$, then for $i = 1, 2$ and for $x = 0, 1$, $f_i(x) = x$; the functions f_3 and f_4 can be either the usual binary parity function π or $1 + \pi$. Now for $u_{i,j} \in \mathbb{F}_2$, $a_i = \pi(u_{i,1}, \ldots, u_{i,n_2}, c_i) = \pi(u_{i,1}, \ldots, u_{i,n_2}) + c_i$ and $b_j = \pi(u_{1,j}, \ldots, u_{n_1,j}) + d_j$. So, using the generalized parity functions p_1 and p_2 of construction given by Proposition 2.5 and letting $u = (u_{1,1}|\cdots|u_{i,j}|\cdots|u_{n_1,n_2}) \in \mathbb{F}_2^{n_1 n_2}$, we have

$$F = \{(u|c + p_1(u)|d + p_2(u)) \ : \ u \in F_2^{n_1 n_2},\ c \in C_1,\ d \in C_2\}$$

which is slightly less general than Proposition 2.5.

When $n_2 = 1$, this construction give the generalization of Proposition 2.4, that is the Vasil'ev's construction, to q-ary case. When $n_2 = 1$ and $q = 2$, we have Proposition 2.4 without the mapping f. So, using a mapping $f : C_1 \longrightarrow \mathbb{F}_q^{n_2}$ this construction gives a construction which is truly a generalization of Propositions 2.4 and 2.5.

Next construction uses Zinoviev's generalized concatenated codes [Zin76] to construct q-ary 1-perfect codes.

Let A and B be a $q(A)$-ary $(n(A), |A|, d(A))$ and $q(B)$-ary $(n(B), |B|, d(B))$ codes, respectively, with $|B| = q(A)$. We label the codewords of B from 0 to $q(A) - 1$, $B =$

$\{b(0), \ldots, b(q(A)-1)\}$. For any codeword $a = (a_1, \ldots, a_{n(A)}) \in A$, we construct the vector $a(B) = (b(a_1)|\cdots|b(a_{n(A)}))$. Now $C = \{a(B) : a \in A\}$ is a $q(B)$-ary code with length $n(C) = n(A)n(B)$, size $|C| = |A|$ and minimum distance $d(C) \geq d(A)d(B)$. The codes A, B and C are called, respectively, the *outer*, *inner* and *concatenated codes*.

Assume now that the inner code B is partitioned into q_1 subcodes:

$$B = \bigcup_{i=0}^{q_1-1} B_i$$

where, for $i = 0, 1, \ldots, q_1 - 1$, B_i is a $q(B)$-ary $(n(B), K_1, d_1)$ code.

Assume furthermore that each subcode B_i can be partitioned into q_2 subcodes: for $i = 0, 1, \ldots, q_1 - 1$,

$$B_i = \bigcup_{j=0}^{q_2-1} B_{i,j}$$

where, for $j = 0, 1, \ldots, q_2 - 1$, $B_{i,j}$ is a $q(B)$-ary $(n(B), K_2, d_2)$ code. Now, any codeword $b \in B$ belongs to exactly one $B_{i,j}$ and, if b has index k in $B_{i,j}$, we see that

$$(i, j, k) \in \{0, \ldots, q_1 - 1\} \times \{0, \ldots, q_2 - 1\} \times \{0, \ldots, K_2 - 1\}$$

completely identifies the vector b. We note $b = b(i, j, k)$.

Let $q_3 = K_2$. Consider, for $l = 1, 2, 3$, a q_l-ary $(n(A), |A_l|, d(A_l))$ code A_l and a codeword $a_{i_l} = (a_{i_l,1}, \ldots, a_{i_l,n(A)}) \in A_l$. For any s between 1 and $n(A)$, the triple $(a_{i_1,s}, a_{i_2,s}, a_{i_3,s})$ designates a codeword $b = b(a_{i_1,s}, a_{i_2,s}, a_{i_3,s})$ belonging to B.

Let $C = \{(b(a_{i_1,1}, a_{i_2,1}, a_{i_3,1}|\cdots|b(a_{i_1,n(A)}, a_{i_2,n(A)}, a_{i_3,n(A)}) : a_{i_l} \in A_l, 1 \leq l \leq 3\}$.

Theorem 4.3. [Zin76] *The code C is a $q(B)$-ary code of length $n(C) = n(A)n(B)$, size $|A_1||A_2||A_3|$ and minimum distance $d(C) \geq min\{d(A_1)d(B), d(A_2)d_1, d(A_3)d_2\}$.*

This construction can be extended to more levels of partitioning and more codes A_l, leading to *Zinoviev's generalized concatenated codes*.

Now, to construct q-ary 1-perfect codes using the above construction, we take $B = \mathbb{F}_q^n$, where $q = q(B)$ is a prime power and $n = n(B) = (q^s - 1)/(q - 1)$. Partition

B into q^s cosets B_i of a q-ary Hamming code of length n: each B_i is an $(n, q^{n-s}, 3)$ code and $q_1 = q^s$, $q_2 = q^{n-s}$.

For A_1, take a q_1-ary Hamming $(n(A) = (q_1^m - 1)/(q_1 - 1), q_1^{n(A)-m}, 3)$ code and let $A_2 = \mathbb{F}_{q_2}^{n(A)}$.

Then, with this choice of parameters and by Proposition 4.3, we have the following result:

Proposition 4.4. [Dum98] *The code C is a q-ary 1-perfect code with length*

$$n(C) = n(A)n(B) = (q^{sm} - 1)/(q - 1)$$

Next construction is a generalization of Doubling Construction given by Proposition 2.7 to the q-ary case and it is due to Mollard [Mol84].

For any vector $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$, let $p(v) = \sum_{i=1}^n v_i$ and for any $q - 1$ vectors $v_1, \ldots, v_{q-1}$ in $\mathbb{F}_q^n$, let $p(v_1, \ldots, v_{q-1}) = \sum_{i=1}^{q-1} i \cdot p(v_i)$. Let $n = (q^m - 1)/(q - 1)$, and let $C_0^0 \cup C_1^0 \cup \ldots \cup C_{n(q-1)}^0$ and $C_0^1 \cup C_1^1 \cup \ldots \cup C_{n(q-1)}^1$ be two partitions of $\mathbb{F}_q^n$ into $n(q-1) + 1 = q^m$ q-ary 1-perfect codes of length n.

Proposition 4.5. [Mol84] *The code C defined by*

$$C = \{(v_1|\cdots|v_{q-1}|p(v_1, \ldots, v_{q-1})|v_q) \ : \ v_i \in \mathbb{F}_q^n, \ i = 1, \ldots, q-1, \\ \textstyle\sum_{i=1}^{q-1} v_i \in C_j^0 \Rightarrow v_q \in C_j^1\}$$

is a q-ary 1-perfect code of length $n' = (q^{m+1} - 1)/(q - 1)$.

Note that for $q = 2$, we have

$$C = \{(v_1|p(v_1)|v_2) \ : \ v_1 \in \mathbb{F}_2^n, \ v_1 \in C_j^0 \Rightarrow v_2 \in C_j^1\}$$

which is, up to permutation π, the code defined in Proposition 2.7.

4.3 Ranks of q-ary 1-perfect codes

A structural property of nonlinear codes is the rank. The *rank* of a q-ary code C of length n, $r(C)$, is simply the dimension of the subspace spanned by C. Etzion and Vardy [EV94] established the existence of 1-perfect binary codes of length $n = 2^m - 1$, $m \geq 4$, and rank $r(C) = n - m + s$ for each s, $s \in \{0, 1, \ldots, m\}$. We will generalize this result for q-ary 1-perfect codes. So, we establish the existence of q-ary 1-perfect codes of length $n = \dfrac{q^m - 1}{q - 1}$ for $m \geq 4$ and rank $r(C) = n - m + s$ for each $s \in \{0, 1, \ldots, m\}$. All of these results given in this section are also shown in [PV01b].

First of all, in section 4.3.1, we will generalize an approach of the Switching construction to obtain q-ary 1-perfect codes. Then, in section 4.3.2, since we need to assure that we can make multiple switches, we must know the dimension of the subspaces T_i and the dimension of the intersection of two of these subspaces (see section 2.5.2 or [PL95]). Finally, in section 4.3.3, we prove that we can obtain q-ary 1-perfect codes of length $n = \dfrac{q^m - 1}{q - 1}$ with all the possible different ranks, $\forall m \geq 4$, which it is a generalization of the binary case proved by Etzion and Vardy, but using techniques developed in [PL95] by Phelps and LeVan.

4.3.1 Switching construction

The most intuitive approach to constructing nonlinear 1-perfect codes consists of starting with the Hamming code H_m, and *switching* out one specially selected set of codewords $S \subset H_m$ for another set of words S' such that the resulting code

$$C = (H_m \backslash S) \cup S'$$

would still be a 1-perfect code. This idea has been developed from different approaches to construct binary 1-perfect codes, see [AS95], [AS96], [EV94] and [PL99]. In [Etz96], Etzion used one generalization of this technique to construct q-ary 1-perfect codes. In this section we will generalize the approach developed in [PL95] by Phelps and LeVan to construct q-ary 1-perfect codes. They use the switching construction to construct

nonlinear binary 1-perfect codes with kernels of different sizes.

Let $\mathbb{F}_q = \{0, \alpha^0, \alpha, \ldots, \alpha^{q-2}\}$, where α is a primitive element. Let e_i denote the vector of length n having all components equal to zero, except the i^{th} component, which contains a one. Let C be a q-ary 1-perfect code, and let $C + \alpha^j e_i$ be a translate of C. Let T_i will denote the subspace spanned by the triples through the point i. Assume $T_i + x_i \subseteq C$, for some $x_i \in C$. We shall define a *switch* to be the process of the replacing the coset $T_i + x_i$ with the coset $T_i + x_i + \alpha^j e_i$. The resulting code C' can be defined as

$$C' = (C \backslash (T_i + x_i)) \cup (T_i + x_i + \alpha^j e_i)$$

for some $i \in \{1, 2, \ldots, n\}$ and some $j \in \{0, 1, \ldots, q-2\}$.

Proposition 4.6. *Given a q-ary Hamming code H_m of length $n = \dfrac{q^m - 1}{q - 1}$, let T_i, $x_i \in H_m$. Then,*

$$C' = (H_m \backslash (T_i + x_i)) \cup (T_i + x_i + \alpha^j e_i)$$

is a nonlinear q-ary 1-perfect code, $\forall i \in \{1, \ldots, n\}$ and $\forall j \in \{0, 1, \ldots, q-2\}$.

Proof: It's easy to see that C' is not linear.

The code C' has the right number of codewords, so we only need to show that the minimum distance is 3. Assume that $c \in H_m \backslash (T_i + x_i)$ such that $d(c, y) \leq 2$ for some $y \in T_i + x_i + \alpha^j e_i$. Then $d(y - c, 0) \leq 2$, and $y - c \in H_m + \alpha^j e_i$, but this implies that $y - c \in T_i + \alpha^j e_i$ since the words of weight less than or equal to 2 in $H_m + \alpha^j e_i$ are the words $v + \alpha^j e_i$ where v is a triple containing α^j in the component i, or when $v = 0$. Thus, $y \in T_i + \alpha^j e_i + c = T_i + \alpha^j e_i + x_i$. In other words, $c \in T_i + x_i$, but $c \in H_m \backslash (T_i + x_i)$, so the minimum distance is still three. ∎

By the above proposition, once we have made one switch we have another q-ary 1-perfect code. In order to make 1-perfect codes of different ranks, we want to make a series of switches such that we can switch $T_1 + x_1$ with $T_1 + x_1 + \alpha^{j_1} e_1$, $T_2 + x_2$ with $T_2 + x_2 + \alpha^{j_2} e_2$, $\ldots$, $T_m + x_m$ with $T_m + x_m + \alpha^{j_m} e_m$. We can do this if $T_i + x_i$ and $T_k + x_k$ are always disjoint for all $k \neq i$. We will see in the Proposition 4.10 that

this is possible $\forall m \geq 4$. In order to prove this result we need to know the dimension of the subspaces T_i and the dimension of the intersection of two of these subspaces.

4.3.2 Subspaces $\mathbf{T}_i$

Let H_m be a q-ary Hamming code of length $n = \dfrac{q^m - 1}{q - 1}$. The parity check matrix of H_m consist of n pairwise linearly independent columns vectors of length m over $\mathbb{F}_q$. From H_m we can construct a projective space $PG(m-1, q)$ of dimension $m-1$ over $\mathbb{F}_q$, where the points are the columns of the parity check matrix of H_m and three points are in a line if the corresponding columns are linearly dependent (cf [BM75]). Then, the elements of the support of a word of weight 3 are points that are in a line in the projective space. We will say that $\{1, 2, \ldots, k\}$ is a set of independent points if the corresponding columns of the parity check matrix are a set of independent vectors, that is if in the projective space no set of three points are colinear.

Let $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$, then the *support* of x is $supp(x) = \{i \ : \ x_i \neq 0\}$.

Proposition 4.7. *Given a q-ary Hamming code H_m, the dimension of T_i is $q^{m-1} - 1$, $\forall i \in \{1, \ldots, n\}$.*

Proof: If $w \in T_i$ such that $wt(w) = 3$ and the i component is nonzero, then $supp(w)$ are points in one line through the point i of the projective space associated with the q-ary Hamming code. Each line corresponds to a subcode isomorphic to the q-ary code H_2 (of dimension $q-1$). For each line there are $q-1$ linearly independent triples that have their support in that line and generate this subcode. There are $(n-1)/q$ lines through the point i, because in each line there are $q+1$ points. So, the number of linearly independent words that generate T_i is

$$(q-1)\Big(\frac{n-1}{q}\Big) = q^{m-1} - 1.$$

∎

Lemma 4.8. *Given a q-ary Hamming code H_3, the dimension of $T_i \cap T_j$ is $q(q-1)$ $\forall i, j \in \{1, \ldots, n\}$ $i \neq j$.*

Proof: The projective space corresponding to the q-ary Hamming code H_3 is a plane with $n = \dfrac{q^3-1}{q-1} = q^2+q+1$ points. We will see that $T_i \cap T_j$ can be generated by $q(q-1)$ linearly independent vectors, $q-1$ of weight 3 and $(q-1)^2$ of weight 4.

Let L_{ij} be the set of $q+1$ points in the line that contain the points i and j. The triples in $T_i \cap T_j$ have their support in L_{ij}. Since for $m=2$, $n=q+1$ and we know that $T_i \cup T_j = H_2$, $dim(H_2) = dim(T_i) + dim(T_j) - dim(T_i \cap T_j)$ and by Proposition 4.7 $dim(T_i \cap T_j) = q-1+q-1-(q+1-2) = q-1$. So, there are $q-1$ linearly independent triples.

Consider the words of weight 4 in T_i that are generated by two triples that come from different lines containing i. Their support has two components in one line and two components in another line through the point i. In each line we can choose $q-1$ linearly independent triples such that contain i. We can fix one line, so there are $q-1$ different lines without the line L_{ij}. In this way, we can construct $(q-1)^2$ quadruples which are linearly independent vectors in T_i. The supports of these quadruples are quadrangles in a projective plane.

Consider quadrangles in a plane determinated by lines through the points i and j. Let z one of these quadruples. Without loss of generality, we can assume that $supp(z) = \{1,2,3,4\}$ and $\{1,2,i\}$ and $\{3,4,i\}$ are the support of the two triples that generate z. So, we can write $z = (a,b,c,d,0,\ldots,0)$, where $a,b,c,d \in \mathbb{F}_q$. Given the following vectors $(a,0,c,0,\ldots,0)$ and $(0,b,0,d,0,\ldots,0)$, there exist two words of weight 3, $v = (a,0,c,0,x,0,\ldots,0)$ and $w = (0,b,0,d,0,y,0,\ldots,0)$. Since the code is linear, $z-v-w = (0,0,0,0,-x,-y,0,\ldots,0) \in H_3$ and then the component where x and y are must be the same j in the line L_{ij} and $x = -y$. We need to see that the others words in $T_i \cap T_j$ can be generated by triples or quadruples. Suppose we have $w \in T_i \cap T_j$ such that $wt(w) > 4$ with minimum weight. We can suppose that the support of w contain at most one element of L_{ij}, otherwise, if $w = \beta e_k + \gamma e_l + v$, where $\{k,l\} \in L_{ij}$, there exist an unique word $c = \beta e_k + \gamma e_l + \delta e_s$ such that $s \in L_{ij}$ and $c \in T_i \cap T_j$. Then we could take $w' = w - c \in T_i \cap T_j$ and $wt(w') < wt(w)$. Since $wt(w) > 4$, w has at least 4 components that are not in L_{ij}. We know $w \in T_i$, so

the components not in L_{ij} are in pairs in lines through the point i and with at most one pair in each line. Since $w \in T_j$, we can say the same. Then, $w = c + v$, where $c \in T_i \cap T_j$ and $wt(c) = 4$, so we can take $w' = w - c = v \in T_i \cap T_j$ and we will have $wt(w') < wt(w)$. This give us a contradiction since w has minimum weight. ∎

Proposition 4.9. *Given a q-ary Hamming code H_m, the dimension of $T_i \cap T_j$ is $(q-1)q^{m-2}$ $\forall i, j \in \{1, \ldots, n\}$ $i \neq j$.*

Proof: If $m = 2$, then $n = q + 1$ and by the same argument that in the proof of Lemma 4.8, we have that $dim(T_i \cap T_j) = q - 1$.

Let L_{ij} the set of $q + 1$ points in the line that contain the points i and j. By the above argument for $m = 2$, the elements in $T_i \cap T_j$ that have their support on L_{ij} can be generated by $q - 1$ linearly independent vectors. If $m > 2$, the dimension of the projective space is $m - 1 \geq 2$, so it contains planes. The number of planes that contain the line L_{ij} is $\dfrac{n - (q+1)}{q^2}$ since the number of points besides the line L_{ij} is $n - (q + 1)$ and in each plane there are $q^2 + q + 1$, but only q^2 not in L_{ij}. By Lemma 4.8, there are $q(q-1)$ linearly independent vectors such that they have their support on the points of a plane. Since $q-1$ vectors are in the line L_{ij} contained in the plane, we have $(q-1)^2$. So,

$$dim(T_i \cap T_j) = q - 1 + \Big(\frac{n - (q+1)}{q^2}\Big)(q-1)^2 = (q-1)q^{m-2}$$

∎

4.3.3 Q-ary 1-perfect codes with different ranks

Now, as in [PL95] for the binary case, we can prove the following result that allow us to make different switches.

Proposition 4.10. *Let H_m be a q-ary Hamming code of length $n = \dfrac{q^m - 1}{q - 1}$, $m \geq 4$, with $\{1, 2, \ldots, m\}$ as a set of its independent points. Then, there exists $x_1, x_2, \ldots, x_m$ such that $T_i + x_i$ is disjoint from $T_j + x_j$ for all $i, j \in \{1, \ldots, m\}$, and $j \neq i$.*

Proof: The number of cosets of T_i is exactly

$$\frac{|C|}{|T_i|} = \frac{q^{n-m}}{q^{q^{m-1}-1}} = q^{\frac{q^m-1}{q-1}-m-q^{m-1}+1}$$

Each switch affects at most

$$\frac{|T_i|}{|T_i \cap T_j|} = q^{q^{m-1}-1-(q-1)q^{m-2}}$$

of these cosets. Then, if there are m cosets selected, there are at most

$$mq^{q^{m-1}-1-(q-1)q^{m-2}}$$

cosets which intersect these chosen ones. So, we need to prove that

$$mq^{q^{m-1}-1-(q-1)q^{m-2}} << q^{\frac{q^m-1}{q-1}-m-q^{m-1}+1}$$

This can be reduced to the following expression since log_q is an increasing function

$$log_q\ m + q^{m-1} - 1 - (q-1)q^{m-2} << \frac{q^m-1}{q-1} - m - q^{m-1} + 1$$

and by simplifying, we get

$$m + log_q\ m - 2 << \frac{q^{m-2}-1}{q-1}$$

Notice that if $m = 3$, we need that $1 + log_q 3 << 1$, but $log_q 3 > 0$. If $m = 4$, we have to prove that $log_q 4 << q-1$. This is true for $q = 3$ and for $q \geq 4$ since $log_q 4 \leq 1$. For $q = 2$ and $m = 4$, as it is said in [PL95], we can still find a series of switches using a more careful inclusion/exclusion argument or a simple brute force search. If $m > 4$ the former equation is true, since $m + log_q m - 2$ and $\frac{q^{m-2}-1}{q-1} = q^{m-3} + q^{m-4} + \cdots + q + 1$ are increasing functions and $\frac{q^{m-2}-1}{q-1}$ increase quicker than the other one. ∎

Theorem 4.11. *Let H_m be a q-ary Hamming code of length $n = \frac{q^m-1}{q-1}$, $m \geq 4$, with $\{1, 2, \ldots, m\}$ as a set of its independent points. Let*

$$C' = \left(H_m \setminus \bigcup_{i=1}^{s} (T_i + x_i)\right) \cup \bigcup_{i=1}^{s} (T_i + x_i + \alpha^{j_i} e_i)$$

where $j_i \in \{0, 1, \ldots, q-2\}$ $\forall i \in \{1, \ldots, n\}$ and α is a primitive element of $\mathbb{F}_q$. Then $r(C') = n - m + s$, $\forall s \in \{1, \ldots, m\}$.

Proof: If $s = 1$, then $C' = (H_m \backslash (T_1 + x_1) \cup (T_1 + x_1 + \alpha^{j_1} e_1)$. The elements of $T_1 + x_1 + \alpha^{j_1} e_1$ can not be generated by the elements of H_m. Since we need the vector e_1, the rank of C' is $r(C') = n - m + 1$.

Suppose that

$$C' = \left(H_m \backslash \bigcup_{i=1}^{s-1} (T_i + x_i) \right) \cup \bigcup_{i=1}^{s-1} (T_i + x_i + \alpha^{j_i} e_i)$$

$r(C') = n - m + s - 1$ and $\langle C' \rangle$ is generated by the elements of H_m and $e_1, e_2, \ldots, e_{s-1}$. Since $\{1, 2, \ldots, s\}$ is a set of independent points $\forall s \leq m$, there are not any codeword such that its support is a subset of $\{1, 2, \ldots, s\}$, so e_s can not be generated by the elements of H_m and $e_1, e_2, \ldots, e_{s-1}$. Then

$$\begin{aligned} C'' &= (C' \backslash (T_s + x_s)) \cup (T_s + x_s + \alpha^{j_s} e_s) \\ &= \left(H_m \backslash \bigcup_{i=1}^{s} (T_i + x_i) \right) \cup \bigcup_{i=1}^{s} (T_i + x_i + \alpha^{j_i} e_i) \end{aligned}$$

has rank $n - m + s$. ∎

By Theorem 4.11, we proved that starting from the q-ary Hamming code, H_m, of length $n = \dfrac{q^m - 1}{q - 1}$ and using the switching construction we can construct q-ary 1-perfect codes of length $n = \dfrac{q^m - 1}{q - 1}$ for $m \geq 4$ with all possible different ranks.

We know that also exist nonlinear 1-perfect q-ary codes, for $m = 2$ if q is a prime power $q \neq 4$ or 8 and for $m = 3$ if $q \geq 3$, [Vas62], [Sch68], [Lin69]. For these cases and using the ideas developed in this section, we can only construct nonlinear 1-perfect q-ary codes of rank $r(C) = n - m + s$ for some $s \in \{1, \ldots, m\}$. Actually, if $m = 2$ then $H_2 = T_i \ \forall i \in \{1, \ldots, q + 1\}$, since $dim(H_2) = dim(T_i)$ and $T_i \subseteq H_2$. So, we can not use our construction to get nonlinear 1-perfect q-ary codes of length $q + 1$. If $m = 3$, $q \geq 3$, then $T_i \subset H_3$ since $dim(H_3) > dim(T_i)\ \forall q \geq 3$. In this case, we can at least make one switch, $C' = (H_3 \backslash (T_i + x_i)) \cup (T_i + x_i + \alpha^{j_i} e_i)$, so $r(C') = n - m + 1$, but we can not assure that if $\{1, 2, 3\}$ is a set of independent points in H_3, there exist x_1, x_2 or x_1, x_2, x_3 such that $\forall i, j \in \{1, 2, 3\}$ $T_i + x_i$ is disjoint from $T_j + x_j$ for $j \neq i$.

Chapter 5

Conclusions

In this dissertation new results about the rank and the kernel of perfect codes are presented. These two parameters are interesting to study nonlinear perfect codes. We focused on 1-perfect codes over a prime power alphabet, since it is known it is the only one for which there exist nonlinear perfect codes.

In this work several results about binary 1-perfect codes and, in general, about q-ary 1-perfect codes, where q is a prime power are obtained. For binary 1-perfect codes we studied for what pairs of numbers (r, k) does there exist a binary 1-perfect code C of length $n = 2^m - 1$ having $r(C) = r$ and $k(C) = k$. For q-ary 1-perfect codes, we were interested in generalizing previous results about the rank of binary 1-perfect codes proving the existence of q-ary 1-perfect codes of length $n = \frac{q^m - 1}{q - 1}$ with any possible rank.

In this chapter we will summarize the obtained results and we will give the conclusions of this work. Then, we will point out possible future lines of research regarding rank and kernel of perfect codes.

5.1 Results of the dissertation

5.1.1 Binary 1-perfect codes

In chapter 3, we proved the following results on the rank and the kernel of binary 1-perfect codes.

First, in order to give the lower bound on the dimension of the kernel of a binary 1-perfect code in terms of the rank of the code, in section 3.1 some properties on the structure of 1-perfect codes are presented. The first one characterizes 1-perfect codes and the second one describes the subcodes of a 1-perfect code C.

We remember some notation. For any binary code C of length n and minimum distance 3, we defined for each codeword $x \in C$ a *neighborhood triple system*

$$NTS(x) = \{x + y \ : \ y \in C, \ d(x, y) = 3\}$$

Given a subspace D of $\mathbb{F}_2^n$ we defined the set of coordinates

$$S_D = \{i \ : \ c_i = 0 \ \forall (c_1, c_2, \ldots, c_n) \in D\}$$

Given a subset of coordinates $S \subset V = \{1, 2, \ldots, n\}$, and a codeword $y \in C$ we defined

$$C_S(y) = \{x_S \ : \ x \in C, \ x_i = y_i \ \forall i \notin S\}$$

where x_S is the restriction of the codeword x to the subset of coordinates S. The characteristic vector $\chi(S)$ for $S \subset V$ is the binary vector of length n that has 1 in the i^{th} coordinate if and only if $i \in S$.

Theorem 5.1. *A code C of length n and minimum distance 3 is a 1-perfect code if and only if every neighborhood triple system is a Steiner triple system.*

Theorem 5.2. *Given a 1-perfect code C of length $n_m = 2^m - 1$ and its dual code $C^\perp$, then for every subspace $D \subseteq C^\perp$ of dimension $m - s$, $s > 0$, and for every $y \in C$, the subcode $C_{S_D}(y)$ is a 1-perfect code of length $n_s = 2^s - 1$ where S_D is as above, the*

set of coordinates which are zero in every codeword of D. Moreover, when $s > 1$, the characteristic vector $\chi(S_D)$ is in the kernel of C.

From Theorem 5.2, we proved next result which gives the lower bound of the kernel of a 1-perfect code since the rank is fixed.

Theorem 5.3. *Let C be a 1-perfect code of length $n_m = 2^m - 1$, rank $r(C) = n - m + s$ and a kernel of dimension $k(C)$, then*

$$\begin{aligned} k(C) &\geq 2^{m-s} \quad if\ s > 1 \\ k(C) &\geq 2^{m-1} - 1 \quad if\ s = 1 \end{aligned}$$

Phelps and LeVan [PL95] proved the following result, which leads us this bound is the exact lower bound. Actually, we have this result from Theorem 2.30 and 2.36, where it is shown the construction of these codes using the switching technique.

Theorem 5.4. [PL95] *For all $m \geq 4$, there exists a 1-perfect code of length $n = 2^m - 1$, with rank $n - m + s$ and kernel of dimension $k = 2^{m-s}$ when $s > 1$ and $k = 2^{m-1} - 1$ when $s = 1$.*

An upper bound on the dimension of the kernel of a 1-perfect code in terms of the rank was given by the following result, which is a generalization of an argument due to Etzion and Vardy, [EV98].

Theorem 5.5. *A 1-perfect code of length $n = 2^m - 1$ with rank $n - m + s$ and a kernel of dimension $n - m - \delta$ fulfills $2^\delta - \delta - 1 \geq s$.*

For the extreme case $s = m$, Etzion and Vardy [EV98] gave the same upper bound $\forall m \geq 5$ and a construction of full-rank 1-perfect codes that achieve this bound when $m \geq 10$. In section 2.5.3 this construction is included by proving Theorem 2.47. For $s = m = 4$, Theorem 5.5 says the upper bound is 8. In [EV98] it is showed a better upper bound, 7, but it was not proved it were tight.

The table in page 40 shows for which pairs (r, k) there exists a binary 1-perfect code of length 15 ($m = 4$) constructed using the Doubling construction and having $r(C) = r$ and $k(C) = k$, [Phe00]. From this table, we can assure this upper bound is tight for $m = 4$ and $0 \leq s < m$. Actually, from Theorem 5.3 and 5.5, we can also say it is possible to construct a 1-perfect code of length 15 for any rank $11 + s$ with $0 \leq s < 4$ and for any possible dimension of the kernel between the lower and upper bound. The only open remaining question for length 15 is about full-rank 1-perfect codes with kernel of dimension 6 or 7.

In section 3.3, we generalized the previous result to any length showing this bound is tight for $m > 4$ and $0 \leq s < m$. The extreme case $s = m$, that is the construction of full-rank 1-perfect codes with maximum dimension of the kernel, will still remain open for $4 \leq m < 10$. In order to establish this upper bound we proved some results on Hamming codes. Let T_i denote the subspace generated by the words of weight 3 that have a one in the i^{th} coordinate.

Lemma 5.6. *For each $m \geq 4$ and $s \in \{1, \ldots, m\}$, there exist two Hamming codes H_1, H_2 of length $n = 2^m - 1$ such that*

$$H_1^{\perp} \cup H_2^{\perp} \subseteq < \bigcup_{i \in I} T_i >^{\perp} \quad \text{and} \quad dim(H_1^{\perp} \cup H_2^{\perp}) = m + s$$

where I is a set of $m - \delta$ independent coordinates, if $2^{\delta} - \delta - 1 \geq s$ and $\delta < m$.

Theorem 5.7. *Given Hamming codes H_1 and H_2 of length $2^m - 1$ and $s \in \{1, \ldots, m\}$ such that*

$$H_1^{\perp} \cup H_2^{\perp} \subseteq < \bigcup_{i \in I} T_i >^{\perp} \quad \text{and} \quad dim(H_1^{\perp} \cup H_2^{\perp}) = m + s$$

there exists a 1-perfect code C of length $n' = 2^{m'} - 1$, where $m' = m + 1$, which has rank $n' - m' + s$ and a kernel of dimension $n' - m' - \delta$ where δ is the minimum integer such that $2^{\delta} - \delta - 1 \geq s$.

If $m \geq 4$, and $s \in \{1, \ldots, m\}$ there exists at least one δ such that $2^{\delta} - \delta - 1 \geq s$ and $\delta < m$. So, Lemma 5.6 and Theorem 5.7 lead to that the upper bound is tight $\forall m \geq 5$ and $s < m$.

In order to prove the previous theorem we established some results on the rank and the kernel of 1-perfect codes constructed with the Doubling construction due to Phelps and Solov'eva. We also used these results to construct 1-perfect codes of different ranks and dimensions of the kernel. Next we describe again this construction.

Let C_1 be a 1-perfect code of length n and C_2^* be an extended 1-perfect code of length $n+1$. By Proposition 2.6, the code

$$C = (C_1 \oplus C_2^*) \bigcup_{i=1}^{n} (C_1 + e_i \oplus (C_2 + e_{\pi(i)})^*)$$

where π is a permutation on the set $\{1, 2, \ldots, n\}$ is a 1-perfect code of length $2n+1$.

Theorem 5.8. *The rank of an 1-perfect code C of length $2n+1$ constructed with the Doubling construction taking the identity permutation is $2n - r(C_1^{\perp} \cap C_2^{\perp})$.*

Theorem 5.9. *The kernel of an 1-perfect code C of length $2n+1$ constructed with the Doubling construction taking the identity permutation is*

$$(K_1 \oplus K_2^*) \bigcup_{i \in I} (K_1 + e_i \oplus (K_2 + e_i)^*)$$

where K_1 and K_2 are the kernels of C_1 and C_2 respectively and $I = \{i : T_i \subseteq K_1 \cap K_2\}$.

Lemma 5.6 gives a construction of Hamming codes which allows us to obtain $\forall s \in \{1, \ldots, m-1\}$ 1-perfect codes of length $n = 2^m - 1$, rank $n - m + s$ and kernel of dimension $n - m - \delta$, where δ is the minimum integer such that $2^\delta - \delta - 1 \geq s$, that is, kernel with maximum dimension, using the Doubling construction. But, in fact, a stronger result is proved that will allow to construct in a similar way 1-perfect codes with rank $n - m + s$ $\forall s \in \{2, \ldots, m-1\}$ and dimension of the kernel $n - m - \delta$ for any δ such that $2^\delta - \delta - 1 \geq s$ and $\delta < m$.

Lemma 5.10. *For each $m \geq 3$ and $s \in \{2, \ldots, m\}$, there exist two Hamming codes H_1, H_2 of length $n = 2^m - 1$ such that*

$$< \bigcup_{i \in I} T_i > \subseteq H_1 \cap H_2 \qquad dim(H_1^{\perp} \cup H_2^{\perp}) = m + s$$

and $\{k \mid T_k \subseteq H_1 \cap H_2\} = \{k \mid T_k \subseteq < \bigcup_{i \in I} T_i >\}$*, where* I *is a set of* $m - \delta$ *independent coordinates, if* $2^\delta - \delta - 1 \geq s$ *and* $\delta \leq m$*.*

Theorem 5.11. *For each* $m \geq 4$ *and* $s \in \{2, \ldots, m-1\}$*, there exists a 1-perfect code* C *of length* $n = 2^m - 1$ *which has rank* $n - m + s$ *and a kernel of dimension* $n - m - \delta$*, where* $2^\delta - \delta - 1 \geq s$ *and* $\delta < m$*.*

For each $m \geq 4$ and $s \in \{2, \ldots, m-1\}$, in other words the above theorem says that there exists a 1-perfect code C of length $n = 2^m - 1$, with rank $n - m + s$ and a kernel of any dimension between the upper bound and $2(n' - m')$, where $n' = 2^{m-1} - 1$ and $m' = m - 1$. This is because the maximum δ such that $\delta < m$ is $m - 1$ and in this case the dimension of the kernel is $n - m - (m-1) = n - 2m + 1 = 2(n' - m')$.

For $s = 1$, in [PL95] it is proved that we can construct 1-perfect codes with any dimension of the kernel between the lower and upper bounds using the Switching construction. This result shows that from a Hamming code, H_m, we can make one switch and have a 1-perfect code C, such that the rank is $r(C) = n - m + 1$ and the kernel has any dimension, $(n-1)/2 \leq k(C) \leq n - m - 2$.

Using the Doubling construction, we showed how to construct 1-perfect codes with different ranks and different dimensions of the kernel between the lower and upper bound. By Theorem 5.9, since the kernel of C is

$$(K_1 \oplus K_2^*) \bigcup_{i \in I} (K_1 + e_i \oplus (K_2 + e_i)^*)$$

where K_1 and K_2 are the kernels of C_1 and C_2 respectively and $I = \{i : T_i \subseteq K_1 \cap K_2\}$, we were interested in results that will say how many T_i are in $K_1 \cap K_2$. We proved the following result which corresponds to $I = \emptyset$.

Proposition 5.12. *If there exist two 1-perfect codes of length* $n = 2^m - 1$ *with kernels of dimension* k_1 *and* k_2 *respectively and ranks* $n - r_1$ *and* $n - r_2$*,* $r_1 \leq r_2$*, then there exists a 1-perfect code* C *of length* $2n + 1$ *with kernel of dimension* $k(C) = k_1 + k_2$ *and rank* $r(C) = 2n - r_1$ *if* $r_1 \leq m - 2$*.*

Summarizing, in chapter 3, we proved we can construct the following binary 1-perfect codes of length $n = 2^m - 1$, $m \geq 4$.

- 1-perfect codes of length $n = 2^m - 1$ with the lower and upper bounds of the dimension of the kernel for a fixed rank except full-rank 1-perfect codes with the upper bound if $4 \leq m < 10$ (using the results in sections 3.2 and 3.3).

- 1-perfect codes of length $n = 2^m - 1$ with the dimension of the kernel near the upper bound, exactly between $2(n' - m')$, where $n' = 2^{m-1} - 1$ and $m' = m - 1$, and the upper bound except for full-rank 1-perfect codes (using section 3.5).

- 1-perfect codes of length $n = 2^m - 1$ with rank $r(C) = n - m + 1$ and with any dimension of the kernel between the lower and upper bounds. From a Hamming code of length $n = 2^m - 1$, H_m, we can make one switch and obtain a 1-perfect code C, with rank $r(C) = n - m + 1$ and the kernel with any dimension, $(n-1)/2 \leq k(C) \leq n - m - 2$, [PL95].

- 1-perfect codes of length $n = 2^m - 1$ constructed using Proposition 5.12 and the pairs $(r(C), k(C))$ for which it is known there exists a 1-perfect code of length $2^{m-1} - 1$ having rank $r(C)$ and kernel of dimension $k(C)$ (using section 3.7).

For example, for length 31 and 63 we summarize all these results in the following tables. The question mark sign means that by using the previous results we do not know if there exist 1-perfect codes with these parameters.

$r(C)$	$k(C)$														
26	26														
27		24	23	22	...	...	...	...	...	15					
28			23	22	?	...	?	19	...	...	8				
29			23	22	?	...	?	19	...	...	...	4			
30			23	22	?	...	...	?	16	...	...	...	2		
31				?	...	...	...	...	...	...	...	...	?	1	

$r(C)$	$k(C)$																
57	57																
58		55	54	53	52	...	...	...	...	31							
59			54	53	52	?	...	?	49	...	...	...	16				
60			54	53	52	?	...	?	49	...	...	...	...	8			
61			54	53	52	?	...	?	49	...	...	...	...	...	4		
62				53	52	?	...	...	...	?	27	25	...	...	...	2	
63				?	...	...	...	...	...	...	...	...	...	...	...	?	1

The previous tables show we can not obtain 1-perfect codes for all the different dimensions of the kernel between the lower and upper bound for a fixed rank. Even if we knew how to construct full-rank 1-perfect codes for any $k(C)$ and any length, we would not obtain all the others.

5.1.2 Q-ary 1-perfect codes

In chapter 4, we proved the following results on the rank of q-ary 1-perfect codes.

First, we generalized an approach of the Switching construction to construct q-ary 1-perfect codes. We remember that T_i denote the subspace of $\mathbb{F}_q^n$ generated by the words of weight 3 that have a one in the i^{th} coordinate.

Proposition 5.13. *Given a q-ary Hamming code H_m of length $n = \dfrac{q^m - 1}{q - 1}$, let T_i, $x_i \in H_m$. Then,*

$$C' = (H_m \backslash (T_i + x_i)) \cup (T_i + x_i + \alpha^j e_i)$$

is a nonlinear q-ary 1-perfect code, $\forall i \in \{1, \ldots, n\}$ and $\forall j \in \{0, 1, \ldots, q-2\}$.

By the above proposition, once we have made one switch we have another q-ary 1-perfect code. In order to make 1-perfect codes of different ranks, we want to make a series of switches such that we can switch $T_1 + x_1$ with $T_1 + x_1 + \alpha^{j_1} e_1$, $T_2 + x_2$ with $T_2 + x_2 + \alpha^{j_2} e_2$, $\ldots$, $T_m + x_m$ with $T_m + x_m + \alpha^{j_m} e_m$. We saw we can do this $\forall m \geq 4$ because we can choose $x_1, x_2, \ldots x_m$ such that $T_i + x_i$ and $T_k + x_k$ are always

disjoint for all $k \neq i$. In order to prove this result, the dimension of the subspaces T_i and the dimension of the intersection of two of these subspaces are computed.

Finally, on the rank of q-ary 1-perfect codes, the existence of q-ary 1-perfect codes of length $n = \dfrac{q^m - 1}{q - 1}$ with any possible rank, $\forall m \geq 4$ is established. This is a generalization of Theorem 2.23, due to Etzion and Vardy [EV98], but using techniques developed by Phelps and LeVan [PL95].

Theorem 5.14. *Let H_m be a q-ary Hamming code of length $n = \dfrac{q^m - 1}{q - 1}$, $m \geq 4$, with $\{1, 2, \ldots, m\}$ as a set of its independent points. Let*

$$C' = \Big(H_m \setminus \bigcup_{i=1}^{s} (T_i + x_i)\Big) \cup \bigcup_{i=1}^{s} (T_i + x_i + \alpha^{j_i} e_i)$$

where $j_i \in \{0, 1, \ldots, q-2\}$ $\forall i \in \{1, \ldots, n\}$ and α is a primitive element of $\mathbb{F}_q$. Then $r(C') = n - m + s$, $\forall s \in \{1, \ldots, m\}$.

We know that also exist nonlinear 1-perfect q-ary codes, for $m = 2$ if q is a prime power $q \neq 4$ or 8 and for $m = 3$ if $q \geq 3$, [Vas62], [Sch68], [Lin69]. For these cases and using the ideas developed in section 4.3, we can only construct nonlinear 1-perfect q-ary codes of rank $r(C) = n - m + s$ for some $s \in \{1, \ldots, m\}$. Actually, if $m = 2$ then $H_2 = T_i$ $\forall i \in \{1, \ldots, q+1\}$, since $dim(H_2) = dim(T_i)$ and $T_i \subseteq H_2$. So, we can not use our construction to get nonlinear 1-perfect q-ary codes of length $q + 1$. If $m = 3$, $q \geq 3$, then $T_i \subset H_3$ since $dim(H_3) > dim(T_i)$ $\forall q \geq 3$. In this case, at least we can make one switch, $C' = (H_3 \setminus (T_i + x_i)) \cup (T_i + x_i + \alpha^{j_i} e_i)$, so $r(C') = n - m + 1$, but we can not assure that if $\{1, 2, 3\}$ is a set of independent points in H_3, there exist x_1, x_2 or x_1, x_2, x_3 such that $\forall i, j \in \{1, 2, 3\}$ $T_i + x_i$ is disjoint from $T_j + x_j$ for $j \neq i$.

5.2 Future research

Since there are still some open questions in our work, in this section we would like to point out some possible lines for pursuing future research.

For binary 1-perfect codes:

- We established the exact upper and lower bounds on the dimension of the kernel of binary 1-perfect codes of length $n = 2^m - 1$, once the rank is fixed, except for one case. It would be nice to solve this case, that is to know the exact upper bound of the dimension of the kernel for full-rank binary 1-perfect codes of length $n = 2^m - 1$, $4 \leq m < 10$.

- Although we have obtained a large number of binary 1-perfect codes with different ranks and different dimensions of the kernel we did not completely settle the question for what pairs of numbers (r, k) does there exist a binary 1-perfect code C of length $n = 2^m - 1$ having $r(C) = r$ and $k(C) = k$. We think it is possible to look into this problem proving some results using the Doubling and Switching construction.

- It would be also interesting to completely settle the question for length 15. In this case the only open question is whether there exist full-rank 1-perfect codes with kernel of dimension 6 and 7. As we saw in section 2.5.3, this problem is equivalent to the existence of a full-rank tiling of $\mathbb{F}_2^n$ for $n = 8$ and 9.

- In order to obtain whether there exist binary 1-perfect codes of length $n = 2^m - 1$ with any rank and any dimension of the kernel between the lower and the upper bound, it would be useful to know how to construct full-rank 1-perfect codes of length $n = 2^{m-1} - 1$ with different kernels.

For q-ary 1-perfect codes:

- We established the existence of q-ary 1-perfect codes of length $n = \dfrac{q^m - 1}{q - 1}$ with any possible rank, $\forall m \geq 4$. Actually, we know that also exist nonlinear 1-perfect q-ary codes, for $m = 2$ if q is a prime power $q \neq 4$ or 8 and for $m = 3$ if $q \geq 3$. It would be interesting to construct q-ary 1-perfect codes with any possible rank for these cases.

- The kernel of q-ary 1-perfect codes has not been studied before. It would be nice to generalize Theorem 2.24 which establishes the existence of binary 1-perfect codes with kernels of all possible sizes, to q-ary 1-perfect codes.

Bibliography

[Abd91] J. K. Abdurahmanov. *On geometrical structure of codes correcting errors.* PhD thesis, Tashkent, Usbekiston, 1991.

[AS95] S. V. Avgustinovich and F. I. Solov'eva. On projections of perfect binary codes. In *Proc. Seventh Joint Swedish-Russian Int. Workshop on Inform. Theory*, pages 25–26, St. Petersburg, Russia, 1995.

[AS96] S. V. Avgustinovich and F. I. Solov'eva. On non-systematic perfect binary codes. *Problems of Information Transmission*, 32(3):258–261, 1996.

[AS97] S. V. Avgustinovich and F. I. Solov'eva. Construction of perfect binary codes by sequential translations of $\tilde{\alpha}$-components. *Probl. Inform. Transmission*, 33(3):202–207, 1997.

[Bes83] M. R. Best. Perfect codes hardly exist. *IEEE Trans. Inform. Theory*, 29(3):349–351, 1983.

[BGH83] H. Bauer, B. Ganter, and F. Hergert. Algebraic techniques for nonlinear codes. *Combinatorica*, 3:21–33, 1983.

[BM75] I. F. Blake and R. C. Mullin. *The Mathematical Theory of Coding.* Academic Press, New York, 1975.

[Bon84] A. Bonisoli. Every equidistant linear code is a sequence of dual hamming codes. *Ars Combin.*, 18:181–186, 1984.

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

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

[CLVZ96] G. D. Cohen, S. Litsyn, A. Vardy, and G. Zémor. Tilings of binary spaces. *SIAM J. Discrete Mathematics*, 9:393–412, 1996.

[Dej01] I. J. Dejter. STS-Graphical invariant for perfect codes. *The Journal of Combinatorial Mathematics and Combinatorial Computing*, 36:65–82, 2001.

[DG75] P. Delsarte and J. M. Goethals. Unrestricted codes with the Golay parameters are unique. *Discrete Math.*, 12:211–224, 1975.

[DHV78] J. Doyen, X. Hubaut, and M. Vandensavel. Ranks of incidence matrices of steiner triple systems. *Math. Z.*, 163:251–259, 1978.

[DSd85] I. Diener, E. Schmitt, and H. L. deVries. All 80 Steiner triple system on 15 elements are derived. *Discrete Math.*, 55:13–19, 1985.

[Dum98] I. I. Dumer. Concatenated codes and their multilevel generalizations. In *Handbook of Coding Theory*, pages 1911–1988. Huffman and Pless, 1998.

[Etz96] T. Etzion. Nonequivalent q-ary perfect codes. *SIAM J. Discrete Mathematics*, 9(3):413–423, 1996.

[EV94] T. Etzion and A. Vardy. Perfect binary codes: Constructions, properties and enumeration. *IEEE Trans. Inform. Theory*, 40:754–763, 1994.

[EV98] T. Etzion and A. Vardy. On perfect codes and tiling: problems and solutions. *SIAM J. Discrete Math.*, 11:205–223, 1998.

[Gib76] P. D. Gibbons. *Computing Techniques for the construction and analysis of block designs*. PhD thesis, University of Toronto, 1976.

[GvT75] J. M. Goethals and H. C. A. van Tilborg. Uniformly packed codes. *Philips Research*, 30:9–36, 1975.

[Hed77] O. Heden. A new construction of group and nongroup perfect codes. *Inform. and Control*, 34:314–323, 1977.

[Hed94] O. Heden. A binary perfect code of length 15 and codimension 0. *Designs, Codes and Cryptography*, 4:213–220, 1994.

[Her82] F. Hergert. The equivalence classes of the Vasil'ev codes of length 15. In *Proceedings of Ravishholzhausen Konfoenz*, volume 963 of *Springer Lecture Notes Series*, 1982.

[Her85] F. Hergert. *Algebraische Methoden Fur nichtlineare Codes*. PhD thesis, Technischen Hochschule Darmstadt, 1985.

[HP85] D. R. Hughes and F. C. Piper. *Design Theory*. Cambridge Univ. Press, 1985.

[Kir47] T. P. Kirkman. On a problem in combinations. *Cambridge and Dublin Math. Journal*, 2:191–204, 1847.

[KS93] J. D. Key and F. E. Sullivan. Codes of Steiner triple and quadruple systems. *Designs, Codes and Cryptography*, 3(2):117–125, 1993.

[LeV95] J. M. LeVan. *Designs and Codes*. PhD thesis, Auburn University, 1995.

[Lin69] B. Lindström. On group and nongroup perfect codes in q symbols. *Math. Scand.*, 25:149–158, 1969.

[LR97] C. C. Lindner and C. A. Rodger. *Design Theory*. CRC Press LLC, 1997.

[LZ97] A. C. Lobstein and V. A. Zinov'ev. On new perfect binary nonlinear codes. *Applicable Algebra in Engineering, Communication and Computing*, 8:415–420, 1997.

[Mol84] M. Mollard. Une nouvelle famille de 3-codes parfaits sur $gf(q)$. *Discrete Methematics*, 49:209–212, 1984.

[Mol86] M. Mollard. A generalized parity function and its use in the construction of perfect codes. *SIAM J. Algebraic Discrete Methods*, 7:113–115, 1986.

[MS77] F. J. MacWilliams and N. J. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, New York, 1977.

[Phe83] K. T. Phelps. A combinatorial construction of perfect codes. *SIAM J. Algebraic Discrete Methods*, 4:398–403, 1983.

[Phe84a] K. T. Phelps. A general product construction for error-correcting codes. *SIAM J. Algebraic Discrete Methods*, 5:224–228, 1984.

[Phe84b] K. T. Phelps. A product construction for perfect codes over arbitrary alphabets. *IEEE Trans. Inform. Theory*, 30:769–771, 1984.

[Phe00] K. T. Phelps. An enumeration of 1-perfect binary codes of length 15. *Australasian Journal of Combinatorics*, 21:287–298, 2000.

[PL95] K. T. Phelps and M. LeVan. Kernels of nonlinear Hamming codes. *Designs, Codes and Cryptography*, 6:247–257, 1995.

[PL99] K. T. Phelps and J. M. LeVan. Switching equivalence classes of perfect codes. *Designs, Codes and Cryptography*, 16:179–184, 1999.

[Ple68] V. Pless. On the uniqueness of the Golay codes. *J. Combin. Theory*, 5:215–228, 1968.

[PV01a] K. T. Phelps and M. Villanueva. Perfect codes: rank and kernel. to appear in Designs, Codes and Crytography, 2001.

[PV01b] K. T. Phelps and M. Villanueva. Ranks of q-ary 1-perfect codes. to appear in Designs, Codes and Crytography, 2001.

[Rif99] J. Rifà. Well-ordered Steiner triple systems and 1-perfect partitions of the n-cube. *SIAM J. Discrete Math.*, 12:35–47, 1999.

[RP97] J. Rifà and J. Pujol. Translation-invariant propelinear codes. *IEEE Trans. Inform. Theory*, 43(2):590–598, 1997.

[Sch68] J. Schönheim. On linear and nonlinear single-error-correcting q-nary perfect codes. *Inform. and Control*, 12:23–26, 1968.

[Sno73] S. L. Snover. *The Uniqueness of the Nordstrom-Robinson and the Golay binary codes*. PhD thesis, Dept. of Mathematics, Michigan State Univ., 1973.

[Sol81] F. I. Solov'eva. On binary nongroup codes. *Methody Discretnogo Analiza*, 37:65–76, 1981. (in Russian).

[Sol88] F. I. Solov'eva. Factorization of code-generating disjunctive normal forms. *Methody Discretnogo Analiza*, 47:66–88, 1988. (in Russian).

[Sol00a] F. I. Solov'eva. Perfect binary codes: bounds and properties. *Discrete Mathematics*, 213:283–290, 2000.

[Sol00b] F. I. Solov'eva. Switching and perfect codes. In *Numbers, Information and Complexity*, pages 311–324. Kluwer Academic Publishers, 2000.

[SS59] G. S. Shapiro and D. L. Slotnik. On the mathematical theory of error correcting codes. *IBM J. Res. and Develop.*, 3(1):25–34, 1959.

[Tei77] L. Teirlinck. On making two steiner triple systems disjoint. *J. Combinatorial Theory*, 23:349–350, 1977.

[Tei80] L. Teirlinck. On projective and affine hyperplanes. *J. Combinatorial Theory*, 28:290–306, 1980.

[Tie73] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. *SIAM J. Appl. Math.*, 24:88–96, 1973.

[Til76] H. C. A. Tilborg. *Uniformly packed codes*. PhD thesis, Univ. of Techn. Eindhover, 1976.

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

[VS95] Y. L. Vasil'ev and F. I. Solov'eva. Interdependence between perfect binary codes and their projections. In *Proceedings of the 6th Joint Swedish-Russian Workshop on Information Thery*, pages 239–242, St. Petersburg, Russia, June 1995.

[WCC19] H. S. White, F. N. Cole, and L. D. Cummings. Complete classification of triad systems of fifteen elements. In *Mem. Mat. Acad. Sci.*, volume 14 of *2nd memoir*, pages 1–89, USA, 1919.

[Zin76] V. A. Zinov'ev. Generalized cascade codes. *Problems of Infrom. Transmi.*, 12(1):2–9, 1976.

[Zin88] V. A. Zinov'ev. *Combinatorial properties, analysis and constructions of nonlinear block codes*. PhD thesis, Computer Center of Russian Academy of Science, Moscow, 1988. (in Russian).

[ZL73] V. A. Zinov'ev and V. K. Leont'ev. The nonexistence of perfect codes over Galois fields. *Probl. Control and Inform. Theory*, 2:123–132, 1973. (in Russian).

Mercè Villanueva i Gay

Bellaterra, July 2001