Generalized weights and bounds for error probability over erasure channels

Leandro Cruvinel Lemes
Department of Electrical Engineering
Federal University of Triangulo Mineiro
Uberaba - MG, Brazil
Email: leandro@icte.uftm.edu.br

Marcelo Firer
Department of Mathematics
State University of Campinas
Campinas - SP, Brazil
Email: mfirer@ime.unicamp.br

***Abstract*—New upper and lower bounds for the error probability over an erasure channel are provided, making use of Wei's generalized weights, hierarchy and spectra. In many situations the upper and lower bounds coincide and this allows us to improve the existing bounds. Results concerning MDS and AMDS codes are deduced from those bounds.**

I. Introduction

Generalized weights of a linear code were introduced by Victor Wei in [1] and became relevant invariants in Coding Theory, being determined for particular classes of codes [2], [3], [4], [5], [6], [7], [8], [9] and bounded when explicit formulas are not available [10], [11]. However, the importance of those invariants concerning one of the main problems of Coding Theory - estimating the efficiency of a code in terms of errors correction - has not yet been properly explored.

In this work, we consider a q-ary erasure channel and give an expression for the error probability (Proposition 2.2) that separates the variables of the problem (namely, the code and the channel), where for error probability we mean either ambiguity probability or the decoding error's probability. Considering the hierarchy and spectra of generalized weights, we are able to get new bounds for the error probability of linear codes (Theorem 4.4). It turns out that, in many cases, the upper bounds for ambiguity are better then the ones determined by Didier in [12] and the lower bound better then those determined by Fashandi et. al. (in [13], where the authors are concerned mainly with codes over large alphabets). In the last section V we consider separation properties (MDS and generalizations), we show that for MDS and AMDS codes the upper and lower bounds obtained for error probability collapse, becoming hence an exact expression for the error probability, (what was already known to Fashandi et. al [13] in the MDS case) and conclude by showing the minimizing role of MDS and AMDS codes when considering and overall error probability sufficiently small.

II. Basic definitions and notation

A. Erasure Channel

In this work we consider a *Discrete Erasure Channels* (DEC) defined by an input alphabet $\mathcal{X} = \mathbb{F}_q$ (finite field with q elements), an output alphabet $\mathcal{Y} = \mathbb{F}_q \cup \{\epsilon\}$ (where $\epsilon \notin \mathbb{F}_q$ is called the *erasure symbol*) and a probability function $\mathbb{P}_{i|j} := \Pr[Y = j|X = i]$ defined by:

(a) $\mathbb{P}_{j|i} = 0$, for $i \neq j$ and $\{i, j\} \subseteq \mathcal{X}$;
(b) $\mathbb{P}_{i|i} = 1 - \mathrm{p}$, for $0 \leq \pi \leq 1$;
(c) $\mathbb{P}_{\epsilon|i} = \mathrm{p}$, for $i \in \mathcal{X}$,

The constant $0 < \mathrm{p} < 1/2$ is called the *overall error probability* of the channel.

A *Discrete Memoryless Erasure Channels* (DMEC) is obtained by defining

$$P(\mathbf{y}|\mathbf{x}) = \prod_{l=1}^{n} \mathbb{P}_{y_l|x_l}, \tag{1}$$

where, $\mathbf{x} = (x_1, x_2, \cdots, x_n) \in \mathcal{X}^n$ and $\mathbf{y} = (y_1, y_2, \cdots, y_n) \in \mathcal{Y}^n$.

B. Generalized weights

Given integers $r, s \in \mathbb{Z}$ with $r < s$, we denote $[\![r, s]\!] := \{r, r+1, \ldots, s-1, s\}$. For simplicity, we write $[\![n]\!] := [\![1, n]\!]$.

Let $C \subseteq \mathbb{F}_q^n$ be an $[n, k]_q$-linear code. Since in this work we will consider only linear codes, this adjective may be omitted. Given $\mathbf{x} \in \mathbb{F}_q^n$, the *support* of $\mathbf{x}$ is

$$\mathrm{supp}(\mathbf{x}) = \{i \in [\![n]\!]; \text{with } x_i \neq 0\}$$

and the Hamming distance may be expressed as $d(\mathbf{x}, \tilde{\mathbf{x}}) = |\mathrm{supp}(\mathbf{x} - \tilde{\mathbf{x}})|$, where $|A|$ denotes the cardinality of A. Given a subcode $D \subseteq C$, the *support of* D is defined as

$$\mathrm{supp}(D) = \bigcup_{\mathbf{x} \in D} \mathrm{supp}(\mathbf{x})$$

and the *generalized weight* $d_i(C)$ of D is defined as

$$d_i(C) = \min\{|\mathrm{supp}(D)|; D \subseteq C \text{ and } \dim(D) = i\},$$

for $i \in [\![k]\!]$. It is well known (Wei's Theorem [1]) that the generalized weights are strictly increasing

$$d_1(C) < d_2(C) < \cdots < d_k(C)$$

and we call $\{d_1(C), d_2(C), \cdots, d_k(C)\}$ the *weight hierarchy of* C.

We denote by $\mathcal{A}_j^i = \mathcal{A}_j^i(C)$, $i \in [\![k]\!]$ and $j \in [\![n]\!]$, the set of all i-dimensional linear subcodes $D \subseteq C$ supported by j coordinates, that is,

$$\mathcal{A}_j^i(C) = \{D \subseteq C; |\mathrm{supp}(D)| = j \text{ and } \dim(D) = i\}.$$

The cardinality of $\mathcal{A}_j^i$ is called the i-th *generalized spectra with support* j of the code C and we denote

$$A_j^i = |\mathcal{A}_j^i|.$$

We call the matrix $\left(A_j^i\right)_{i=0,\cdots,k;j=0,\cdots n}$ the *spectra-matrix of the code*.

C. Ambiguity

Considering a code $C \subset \mathbb{F}_q^n$ and a DMEC, some messages in $\mathcal{Y}^n$ will never be received. We denote by E_C the subset of messages that may be received, that is,

$$E_C = \{\mathbf{y} \in \mathcal{Y}^n; \mathbb{P}_{\text{receive}}(\mathbf{y}) \neq 0\}$$

and call it the set of *admissible* or *possible messages*, where $\mathbb{P}_{\text{receive}}(\mathbf{y})$ is the probability to receive $\mathbf{y} \in \mathcal{Y}^n$.

Given $\mathbf{x} \in \mathcal{X}^n$, we denote by $\mathbb{P}_{\text{send}}(\mathbf{x})$ the priori probability of $\mathbf{x}$ so that

$$E_C = \{\mathbf{y} \in \mathcal{Y}^n; \exists \mathbf{x} \in C \text{ with } \mathbb{P}_{\text{send}}(\mathbf{x}) \prod_{l=1}^{n} \mathbb{P}_{y_l|x_l} \neq 0\}.$$

Given $\mathbf{y} \in \mathcal{Y}^n$ let $R := R(\mathbf{y}) = \{i \in [\![n]\!]; y_i = \epsilon\}$ and define the *set* $[\mathbf{y}]_R$ *of* R*-ambiguities* of $\mathbf{y}$ as

$$[\mathbf{y}]_R := \{\mathbf{x} \in C; P(\mathbf{y}|\mathbf{x}) \neq 0\}.$$

We note that $[\mathbf{y}]_R$ depends both on $\mathbf{y}$ and C. We remark that, when using a Maximum Likelihood decoder, once the message $\mathbf{y}$ is received, the elements of $[\mathbf{y}]_R$ are the possible choices for decoding $\mathbf{y}$. We say that $\mathbf{y}$ is an *ambiguity* of C if $|[\mathbf{y}]_R| > 1$.

We identify $\mathbb{F}_q^n$ with the product $\Pi_{i=1}^n (\mathbb{F}_q)_i$ and, given $R \subseteq [\![n]\!]$, we denote by π_R the projection of $\mathbf{x} = (x_i)_{i \in [\![n]\!]}$ in the coordinates of R: $\pi_R(\mathbf{x}) = (x_i)_{i \in R}$. To shorten the notation we will write $\pi_R(\mathbf{x}) = \mathbf{x}^R$. We also denote by E_R the set of admissible messages that has an erasure on the coordinates in R, that is,

$$E_R = \{\mathbf{y} \in E_C; y_i = \epsilon, \ \forall i \in R\}.$$

Given $R \subseteq [\![n]\!]$ let $\bar{R} := \{i \in [\![n]\!]; i \notin R\}$ be the *complement of* R.

The following proposition consists of a sequence of elementary properties that are stated (without a proof) for future reference.

Proposition 2.1: Considering a DMEC, $\mathbf{y} \in \mathcal{Y}^n$, $R \subseteq [\![n]\!]$ and C a linear code, we have that

(i) $[\mathbf{y}]_R = \emptyset$ *iff* $\mathbf{y} \notin E_C$;

(i) $[\mathbf{y}]_R = \{\mathbf{x} \in C; \mathbf{x}^{\bar{R}} = \mathbf{y}^{\bar{R}}\}$;

(iii) $[\mathbf{0}]_R$ is the kernel of the projection map $\pi_{\bar{R}}$ restricted to the code C;

(iv) For any $\mathbf{y} \in E_C$, $|[\mathbf{y}]_R| = |[\mathbf{0}_R]|$;

(v) $|E_R| = q^k |[\mathbf{0}]_R|^{-1}$.

D. Error probability for ambiguity and decoding

We are considering an DMEC with conditional probabilities defined by (1), with overall error probability $\mathtt{p}$ and prior probabilities identically distributed, that is, $P(i) = q^{-1}, \forall i \in \mathbb{F}_q$.

Given $\mathbf{y} \in \mathcal{Y}^{\mathbf{n}}$ we denote by $\mathbb{P}_{\text{receive}}(\mathbf{y})$ the probability that $\mathbf{y}$ is received and by $\mathbb{P}_{\text{amb}}(\mathbf{y})$ the probability that $\mathbf{y}$ is ambiguous. The *ambiguity probability of* an $[n,k]_q$-code C (or the error probability before decoding procedures) is

$$\begin{aligned} P_{\text{amb}}(C) &= \sum_{\mathbf{y} \in \mathcal{Y}^n} \mathbb{P}_{\text{amb}}(\mathbf{y}) \mathbb{P}_{\text{receive}}(\mathbf{y}) \\ &= \sum_{\mathbf{y} \in E_C} \mathbb{P}_{\text{amb}}(\mathbf{y}) \mathbb{P}_{\text{receive}}(\mathbf{y}), \end{aligned}$$

where the last equality follows from statement (i) in Proposition 2.1.

Considering a maximum likelihood decoding criteria, we denote by $\mathbb{P}_{\text{dec}}(\mathbf{y})$ the probability of $\mathbf{y} \in \mathcal{Y}^n$ being decoded incorrectly and define the *decoding error probability of* an $[n,k]_q$-code C as

$$\begin{aligned} P_{\text{dec}}(C) &= \sum_{\mathbf{y} \in \mathcal{Y}^n} \mathbb{P}_{\text{dec}}(\mathbf{y}) \mathbb{P}_{\text{receive}}(\mathbf{y}) \\ &= \sum_{\mathbf{y} \in E_C} \mathbb{P}_{\text{dec}}(\mathbf{y}) \mathbb{P}_{\text{receive}}(\mathbf{y}), \end{aligned}$$

where the last equality again follows from statement (i) in Proposition 2.1.

We will use $P_*(C)$ to denote either $P_{\text{amb}}(C)$ or $P_{\text{dec}}(C)$, that is, we may consider $*$ to mean either 'dec' or 'amb', so that both the previous expressions may be written as

$$P_*(C) = \sum_{\mathbf{y} \in E_C} \mathbb{P}_*(\mathbf{y}) \mathbb{P}_{\text{receive}}(\mathbf{y}). \tag{2}$$

Since we are assuming that $P(i) = q^{-1}, \forall i \in \mathbb{F}_q$, the probability that a message $\mathbf{y}$ is received is

$$\begin{aligned} \mathbb{P}_{\text{receive}}(\mathbf{y}) &= \sum_{\mathbf{x} \in C} P(\mathbf{y}|\mathbf{x}) \mathbb{P}_{\text{send}}(\mathbf{x}) \\ &= \frac{1}{q^k} \sum_{\mathbf{x} \in C} P(\mathbf{y}|\mathbf{x}). \end{aligned}$$

Considering an admissible message $\mathbf{y} \in E_C$, we have

$$\mathbb{P}_{\text{receive}}(\mathbf{y}) = \sum_{\mathbf{x} \in [\mathbf{0}]_R} q^{-k} \mathtt{p}^{|R|} (1-\mathtt{p})^{|\bar{R}|} \tag{3}$$

$$= |[\mathbf{0}]_R| q^{-k} \mathtt{p}^{|R|} (1-\mathtt{p})^{|\bar{R}|}. \tag{4}$$

Substituting expression (3) into equation (2) we get

$$P_*(C) = \sum_{\mathbf{y} \in E_C} \mathbb{P}_*(\mathbf{y}) |[\mathbf{0}]_R| q^{-k} \mathtt{p}^{|R|} (1-\mathtt{p})^{|\bar{R}|}, \tag{5}$$

hence we may write (5) as

$$P_*(C) = \sum_{R \subseteq [\![n]\!]} \mathbb{P}_*(\mathbf{y}) |E_H| |[\mathbf{0}]_R| q^{-k} \mathtt{p}^{|R|} (1-\mathtt{p})^{|\bar{R}|}$$

and, from statement (v) in Proposition 2.1 it follows that

$$P_*(C) = \sum_{R \subseteq [\![n]\!]} \mathbb{P}_*(R) \mathtt{p}^{|R|} (1-\mathtt{p})^{|\bar{R}|}. \tag{6}$$

We note that we are exchanging $\mathbb{P}_*(\mathbf{y})$ by $\mathbb{P}_*(R)$ and this is possible since those probabilities do not depend on $\mathbf{y}$ but only at what are the erased coordinates of $\mathbf{y}$, that is, on the set

$$R = R(\mathbf{y}) = \{i \in [\![n]\!]; y_i = \epsilon\}.$$

Denoting

$$Q_{*,r} = \sum_{R;|R|=r} P_*(R), \tag{7}$$

we may write (6) as

$$P_*(C) = \sum_{r=0}^{n} Q_{*,r} \mathtt{p}^r (1-\mathtt{p})^{n-r}. \tag{8}$$

We note that

$$Q_{dec,r} = \sum_{\{R \subseteq [\![n]\!]; |R|=r\}} \left(1 - \frac{1}{|[\mathbf{0}]_R|}\right). \tag{9}$$

$$Q_{amb,r} = \sum_{\{R \subseteq [\![n]\!]; |R|=r\}} \left\lceil 1 - \frac{1}{|[\mathbf{0}]_R|}\right\rceil. \tag{10}$$

where $\lceil \alpha \rceil$ is the smallest integer greater or equal to $\alpha \in \mathbb{R}$. In our case, we have that

$$\left\lceil 1 - \frac{1}{|[\mathbf{0}]_R|}\right\rceil = \begin{cases} 0 & \text{if } |[\mathbf{0}]_R| = 1; \\ 1 & \text{if } |[\mathbf{0}]_R| > 1, \end{cases}$$

that is, it equals 1 or 0 according if there is more then one or only one (namely $\mathbf{y}$) admissible messages having R as a set of ambiguous coordinates.

We define

$$a_r^i := a_r^i(C) = |\{R \in [\![n]\!]; |R| = r \text{ and } \dim([\mathbf{0}]_R) = i\}| \tag{11}$$

and

$$\delta_{*,i} = \begin{cases} 1 - \frac{1}{q^i}, & \text{for } * = \text{dec}; \\ \left\lceil 1 - \frac{1}{q^i}\right\rceil, & \text{for } * = \text{amb}. \end{cases}$$

We note that each a_r^i depends on the code C, since $[\mathbf{0}]_R$ is the kernel of the projection π_R restricted to C. We also remark that

$$\sum_{i=0}^{k} a_r^i = \binom{n}{r}. \tag{12}$$

With this notation we have that

$$Q_{*,r} = \sum_{i=0}^{k} a_r^i \delta_{*,i} \tag{13}$$

so that equation (6) may be expressed in a vectorial form:

Proposition 2.2: The ambiguity probability and the decoding error probability of a linear code may be expressed as the product

$$P_*(C) = \boldsymbol{\delta}_* \Lambda \boldsymbol{\rho}^T \tag{14}$$

where

$$\boldsymbol{\delta}_* = (\delta_{*,0}, \ldots, \delta_{*,k}),$$
$$\boldsymbol{\rho} = \left((1-\mathtt{p})^n, \mathtt{p}(1-\mathtt{p})^{n-1}, \ldots, \mathtt{p}^n\right),$$

$\boldsymbol{\rho}^T$ is the transpose of the vector $\boldsymbol{\rho}$ and

$$\Lambda = \begin{pmatrix} a_0^0 & a_1^0 & \cdots & a_n^0 \\ \vdots & \vdots & & \vdots \\ a_0^k & a_1^k & \cdots & a_n^k \end{pmatrix}. \tag{15}$$

We remark that $\boldsymbol{\delta}_*$ depends only on the the parameters $[n,k]_q$ and on $*$ meaning "decoding" or "ambiguity"; $\boldsymbol{\rho}$ depends only at the channel not on the code; the matrix Λ depends only on the code C, not on the channel neither on $*$ meaning "decoding" or "ambiguity". For this reason, since only Λ depends on the code C, when looking for bounds, we will focus the attention on this matrix, which we call the *support-matrix of* C.

III. Support-matrix and spectra-matrix of a code

In this section and from here on, we will assume that $d_k = n$. We wish to establish a relation between the support-matrix and the spectra-matrix of a code and we start with two simple lemmas.

Lemma 3.1: Let C be a code, $D \in \mathcal{A}_r^i(C)$ and $s \in [\![n]\!]$. Then, D contains a set of linearly independent vectors $\{\mathbf{x}^1, \ldots, \mathbf{x}^{i-1}\} \subset D$ such that $\pi_s(\mathbf{x}^j) = 0$, for any $j \in [\![i-1]\!]$.

Proof: Let $R = supp(D)$ and let us assume first that $s \notin R$. But this implies that $\pi_{\{s\}}(\mathbf{x}) = 0$, for every $\mathbf{x} \in D$ and the result follows from the fact that $\dim(D) = i$.

Let us now assume that $s \in R$. Since $R = supp(D)$, there is $\mathbf{x} \in D$ such that $\pi_{\{s\}}(\mathbf{x}) \neq 0$. We consider a basis of the subspace D containing $\mathbf{x}$, let us say $\{\mathbf{x}, \mathbf{u}^1 \ldots, \mathbf{u}^{i-1}\}$. We define

$$\mathbf{x}^j = \mathbf{u}^j - \frac{\pi_s(\mathbf{u}^j)}{\pi_s(\mathbf{x})}\mathbf{x}$$

and it is immediate to check that $\{\mathbf{x}^1, \ldots, \mathbf{x}^{i-1}\}$ is linearly independent and $\pi_s(\mathbf{x}^j) = 0$, for any $j \in [\![i-1]\!]$. ■

Lemma 3.2: For every $i \in [\![k]\!]$ the coefficient $A_{d_i}^i$ of the spectra-matrix depends on the number of different supports attained by subcodes in $\mathcal{A}_{d_i}^i$, that is,

$$A_{d_i}^i = |\{R; R = \text{supp}\,(D) \text{ and } D \in \mathcal{A}_{d_i}^i\}|.$$

Proof: It is enough to prove that for $D_1, D_2 \in \mathcal{A}_{d_i}^i$, if $D_1 \neq D_2$, then $supp\,(D_1) \neq supp\,(D_2)$.

For $D_1 \neq D_2$ we may assume wlog there is $\mathbf{x} \in D_2 \setminus D_1$. We suppose $supp(D_1) = supp(D_2) = R$ and will show that this leads to a contradiction. Since $\mathbf{x} \in D_2 \setminus D_1$, the subspace $D = \langle \{\mathbf{x}\} \cup D_1 \rangle$ has dimension $i+1$ and since $supp(\mathbf{x}) \subseteq supp(D_1) = R$, we have that $supp(D) = R$ and, from Lemma 3.1, given $s \in R$ there is a linearly independent set $\{\mathbf{x}^1, \ldots, \mathbf{x}^i\} \subseteq D$ such that $\pi_{\{s\}}(\mathbf{x}^j) = 0$, $\forall j \in [\![i]\!]$. Denoting $\tilde{D} = \langle \mathbf{x}^1, \ldots, \mathbf{x}^i \rangle$ we have that $\dim(\tilde{D}) = i$ and $supp(\tilde{D}) \subseteq R \setminus \{s\}$, that is, $|supp(\tilde{D})| < d_i$, a contradiction. ■

We are now able to determine $a_r^i = 0$ for $r \leq d_i$:

Proposition 3.3: For any $i = 1, \cdots k$, the coefficients of the support-matrix of a code C satisfy

$$a_r^i = \begin{cases} 0 & \text{for } r < d_i; \\ A_{d_i}^i & \text{for } r = d_i. \end{cases}$$

Proof: We first consider the case $r = d_i$. If we put

$$B = \{R \subseteq [\![n]\!]; \dim([\mathbf{0}]_R) = i \text{ and } |R| = d_i\}.$$

we have, by definition, that $|B| = a_{d_i}^i$. It follows from Lemma 3.2 that we only need to prove that

$$B = |\{R; R = \text{supp}(D) \text{ and } D \in \mathcal{A}_{d_i}^i\}|.$$

Let us consider $R \subseteq [\![n]\!]$ with $\dim([\mathbf{0}]_R) = i$ and $|R| = d_i$ and let us prove that $supp([\mathbf{0}]_R) = R$. We know that $supp([\mathbf{0}]_R) \subseteq R$ and we can not have $|supp([\mathbf{0}]_R)| > |R|$. Since $\dim([\mathbf{0}]_H) = i$ and $|supp([\mathbf{0}]_R)| \leq |R| = d_i$, it follows that $supp([\mathbf{0}]_R) = R$ hence $a_{d_i}^i = A_{d_i}^i$.

We consider now the case $r < d_i$. Given $r < d_i$, suppose that $a_r^i > 0$. This implies there is $R \subseteq [\![n]\!]$ with $|R| = r$ and $\dim([\mathbf{0}]_R) = i$. But $supp([\mathbf{0}]_R) \subseteq R$ and this implies $r = |R| \geq |supp([\mathbf{0}]_R)| \geq d_i$, a contradiction. It follows that $a_r^i = 0$, for all $r < d_i$. ■

We remark that the condition $r = d_i$ is strictly necessary in Proposition 3.3. Considering for example the $[3, 2]_2$-code generated by the vectors $\{(1, 0, 0), (0, 1, 1)\}$ for $r = 2$ and $d_2 = 3$ we have that $A_2^1 = 1$ and $a_2^1 = 3$.

Wei's Monotonicity Theorem states that $i < j$ implies $d_i < d_j$, so Proposition 3.3 ensures the following:

Corollary 3.4: If $j < i$ then $a_{d_j}^i = 0$.

We continue with some results that will be used to produce the expected bounds for the error probability.

Lemma 3.5: Let $R \subsetneq [\![n]\!]$, with $|R| = r$ and $i = \dim([\mathbf{0}]_R)$. Then, for any $j \in [\![n]\!] \setminus R$ we have that

$$\dim([\mathbf{0}]_{R\cup\{j\}}) \geq \max(k + r + 1 - n, i). \tag{16}$$

Proof: Denoting $S_j = R \cup \{j\}$, from item (iii) in Proposition 2.1 we have $[\mathbf{0}]_{S_j} = \ker(\pi_{\bar{S}_j})$. Considering that $\pi_{\bar{S}_j}$ may be expressed as the composition

$$\pi_{\bar{S}_j} = \pi_{\overline{\{j\}}} \circ \pi_{\bar{R}} \tag{17}$$

of the projections

$$\begin{array}{ccccc} C & \xrightarrow{\pi_{\bar{R}}} & \mathbb{F}_q^{n-r} & \xrightarrow{\pi_{\overline{\{j\}}}} & \mathbb{F}_q^{n-r-1} \\ \sum_{s\in[\![n]\!]} c_s \mathbf{e}_s & \longmapsto & \sum_{s\in\bar{R}} c_s \mathbf{e}_s & \longmapsto & \sum_{s\in\bar{S}_j} c_s \mathbf{e}_s, \end{array}$$

the classical Kernel Theorem ensures that

$$\dim(C) = \dim(Im(\pi_{\bar{S}_j})) + \dim(\ker(\pi_{\bar{S}_j})),$$

that is,

$$\dim\left([\mathbf{0}]_{S_j}\right) = k - \dim(Im(\pi_{\bar{S}_j})). \tag{18}$$

But equation (17) implies

$$\dim(Im(\pi_{\bar{S}_j})) \leq \min(\dim(Im(\pi_{\bar{R}})), \dim(Im(\pi_{\overline{\{j\}}}))). \tag{19}$$

Since $\pi_{\overline{\{j\}}}$ determines a projection of an $(n-r)$-dimensional space into an $(n-r-1)$-dimensional one, we have that

$$\dim(Im(\pi_{\overline{\{j\}}})) = n - r - 1 \tag{20}$$

and since $\dim([\mathbf{0}]_R) = \dim(\ker(\pi_{\bar{R}}))$, we have that

$$\dim(Im(\pi_{\bar{R}})) = \dim(C) - \dim(\ker(\pi_{\bar{R}})) = k - i. \tag{21}$$

It follows from (19), (20) and (21) that

$$\dim(Im(\pi_{\bar{S}_j})) \leq \min(k - i, n - r - 1) \tag{22}$$

and equations (18) and (22) together imply

$$\begin{aligned} \dim([\mathbf{0}]_{S_j}) &\geq k - \min(k - i, n - r - 1) \\ &= \max(i, k + r + 1 - n). \end{aligned}$$

■

The next Propositions will be used in the proof of our new bounds in Theorem 4.4 and follows easily from Lemma 3.5.

Corollary 3.6: Given an $[n, k]_q$-linear code C and $R \subseteq [\![n]\!]$ with $|R| = r$, then $|[\mathbf{0}]_R| \geq q^{k-n+r}$.

Proof: The proof is made by induction on $|R|$. For the initial step, $|R| = 0$, the result is satisfied since $R = \emptyset$. Suppose $|[\mathbf{0}]_R| \geq q^{k-n+|R|}$ for every $R \subseteq [\![n]\!]$ with $|R| \leq r$ and let us prove it also holds for $J \subseteq [\![n]\!]$ with $|J| = r + 1$. We write $J = R \cup \{j\}$ with $|R| = r$ and $j \notin R$, and from Lemma 3.5 it follows that

$$\dim([\mathbf{0}]_J) = \dim([\mathbf{0}]_{R\cup\{j\}}) \geq \max(k + r + 1 - n, i)$$

with $i = \dim([\mathbf{0}]_R)$. The induction hypothesis implies that $i \geq k - n + r$ hence

$$\begin{aligned} \dim([\mathbf{0}]_J) &\geq \max(k + r + 1 - n, k - n + r) \\ &= k - n + (r + 1). \end{aligned}$$

■

Proposition 3.7: If $r \geq n - k + i + 1$, then $a_r^i = 0$.

Proof: Suppose $a_r^i > 0$ for some $r \geq n - k + i + 1$, that is, suppose there is a set $R \subseteq [\![n]\!]$ with $\dim([\mathbf{0}]_R) = i$ and

$$|R| := r \geq n - k + i + 1. \tag{23}$$

We cannot have $R = [\![n]\!]$, since this would imply $r = n$ and $i = k$, contradicting inequality (23). So, let us assume that $R \subsetneq [\![n]\!]$, so there is $j \in [\![n]\!] \setminus R$. From Lemma 3.5 we have that

$$\dim([\mathbf{0}]_{R\cup\{j\}}) \geq \max(k + r + 1 - n, i)$$

and from inequality (23) we have $k + r + 1 - n \geq i + 2 > i$, hence

$$\dim([\mathbf{0}]_{R\cup\{j\}}) \geq i + 2.$$

It follows there is a subcode $D \subseteq [\mathbf{0}]_{R\cup\{j\}}$ with $\dim(D) = i+2$ and Lemma 3.1 ensures the existence of a subcode $\tilde{D} \subseteq D$ such that $\dim(\tilde{D}) = i + 1$ and $supp(\tilde{D}) \subseteq R$. But $\tilde{D} \subseteq [\mathbf{0}]_R$ and $\dim([\mathbf{0}]_R) = i$, a contradiction. It follows that, for $r \geq n-k+i+1$, there does not exist $R \subseteq [\![n]\!]$ such that $|R| = r$ and $\dim([\mathbf{0}]_R) = i$, in other words, $a_r^i = 0$ for $r \geq n - k + i + 1$. ■

Corollary 3.8: $a^i_{n-1} = 0$ for every $i \neq k-1$ and $a^{k-1}_{n-1} = n$.

Proof: Considering $r = n-1 = n-k+(k-1)$ and $i < k-1$, Proposition 3.7 ensures $a^i_{n-1} = 0$. Proposition 3.3 it follows that $a^k_{n-1} = a^k_{d_k-1} = 0$ and as a particular case of expression (12) we have that

$$\sum_{i=0}^{k} a^i_{n-1} = \binom{n}{n-1},$$

and, since a^{k-1}_{n-1} is the only non-zero summand in the equality above, we have $a^{k-1}_{n-1} = \binom{n}{n-1} = n$. ■

IV. Bounds for P_*

In this section, we establish bounds for P_* by founding bounds for the coefficients $Q_{*,r}$ defined in equality (13). We start with three lemmas that give us values and bounds for $|[\mathbf{0}]_R|$.

Lemma 4.1: Let C be an $[n,k]_q$-linear code and let $D \subseteq C$ be an i-dimensional linear subcode of C. If $\text{supp}(D) \subseteq R \subseteq [\![n]\!]$, then $|[\mathbf{0}]_R| \geq q^i$.

Proof: Since $D \subseteq [\mathbf{0}]_R$, we have that $|[\mathbf{0}]_R| \geq |D| = q^i$. ■

Lemma 4.2: Let C be an $[n,k]_q$-linear code. If $R = supp(D)$ and $D \in \mathcal{A}^i_{d_i}$, then $|[\mathbf{0}]_R| = q^i$.

Proof: From item (iii) in Proposition 2.1 we know that $[\mathbf{0}]_R$ is a vector subspace of $\mathbb{F}^n_q$ and hence $|[\mathbf{0}]_R|$ is a power of q. We assume that $|[\mathbf{0}]_R| \geq q^{i+1}$ and this will lead us to a contradiction. But $|[\mathbf{0}]_R| \geq q^{i+1}$ implies $\dim([\mathbf{0}]_R) \geq i+1$ hence there is a subspace $D \subseteq [\mathbf{0}]_R$ with $\dim(D) = i+1$. From $D \subseteq [\mathbf{0}]_R$ it follows that

$$supp(D) \subseteq supp([\mathbf{0}]_R) \subseteq R$$

hence

$$d_{i+1} \leq |supp(D)| \leq |supp([\mathbf{0}]_R)| \leq |H| = d_i.$$

But this contradicts the fact $d_i < d_{i+1}$, ensured by the Monotonicity Theorem (Section II-B). So we have that $|[\mathbf{0}]_R| \leq q^i$ and Lemma 4.1 ensures $|[\mathbf{0}]_R| = q^i$. ■

In the previous lemma we considered a subset $R \subseteq [\![n]\!]$ that is the support of a subcode $D \in \mathcal{A}^i_{d_i}$ realizing the i-th weight. In the following proposition we assume that $|R| = d_i$ but $R \neq supp(D)$ for any D realizing the i-th weight.

Lemma 4.3: Let C be an $[n,k]_q$-linear code. If $R \subseteq [\![n]\!]$ satisfies $|R| = d_i$ but $R \neq supp(D)$ for any $D \in \mathcal{A}^i_{d_i}$, then $|[\mathbf{0}]_R| \leq q^{i-1}$.

Proof: Suppose $|[\mathbf{0}]_R| \geq q^i$, or equivalently, $\dim([\mathbf{0}]_R) \geq i$. In this case, there is an i-dimensional $D \subseteq [\mathbf{0}]_R$ of C such that $supp(D) \subseteq R$ and

$$d_i \leq |supp(D)| \leq |supp([\mathbf{0}]_R)| \leq |R| = d_i,$$

where the first inequality follows from the minimality of d_i. Then we have $supp(D) = R$, $\dim(D) = i$ and $|supp(D)| = d_i$, contradicting the hypothesis that $R \neq supp(D)$ for any $D \in \mathcal{A}^i_{d_i}$. So, $|[\mathbf{0}]_R| < q^i$ and we get $|[\mathbf{0}]_R| \leq q^{i-1}$. ■

Now we are able to establish bounds for $P_*(C)$. This will be done in the next theorem, that actually establish upper and lower bounds for some of the coefficients $Q_{*,j}$ in expression 8.

Theorem 4.4 (Bounds for $P_*(C)$): Let C be an $[n,k]_q$-linear code. Then,

(a) For every $i \in [\![k]\!]$, the coefficient Q_{dec,d_i} is greater or equal to

$$A^i_{d_i}\left(1-\tfrac{1}{q^i}\right) + \left(\tbinom{n}{d_i} - A^i_{d_i}\right)\left(1-\tfrac{1}{\max\{1,q^{k-n+d_i}\}}\right);$$

(b) For every $i \in [\![k]\!]$, the coefficient Q_{dec,d_i} is smaller or equal to

$$A^i_{d_i}\left(\frac{q-1}{q^i}\right) + \binom{n}{d_i}\left(1-\frac{1}{q^{i-1}}\right);$$

(c) For every $i \in [\![2,k]\!]$, the coefficient Q_{amb,d_i} is greater or equal to

$$A^i_{d_i} + \left(\binom{n}{d_i} - A^i_{d_i}\right)\left[1-\frac{1}{\max\{1,q^{k-n+d_i}\}}\right].$$

(d) $Q_{amb,d_1} = A^1_{d_1}$.

Proof:

(a) To simplify the notation we write:

$$\Phi_i = \{R \subseteq [\![n]\!]; R = supp(D) \text{ with } D \in \mathcal{A}^i_{d_i}\}$$

and

$$\tilde{\Phi}_i = \{R \subseteq [\![n]\!]; |R| = d_i\} \setminus \Phi_i.$$

Using this notation and expression (9), the coefficient Q_{dec,d_i} is expressed as

$$Q_{dec,d_i} = \textstyle\sum_{R\in\Phi_i}\left(1-\frac{1}{|[\mathbf{0}]_R|}\right) + \sum_{R\in\tilde{\Phi}_i}\left(1-\frac{1}{|[\mathbf{0}]_R|}\right). \tag{24}$$

Lemma 4.2 ensures that $R \in \Phi_i$ implies $|[\mathbf{0}]_R| = q^i$ so

$$Q_{dec,d_i} \geq \textstyle\sum_{R\in\Phi_i}\left(1-\frac{1}{q^i}\right) + \sum_{R\in\tilde{\Phi}_i}\left(1-\frac{1}{|[\mathbf{0}]_R|}\right).$$

Corollary 3.6 ensures that if $R \in \tilde{\Phi}_i$ then $|[\mathbf{0}]_R| \geq q^{k-n+d_i}$ and since we must have $1-\frac{1}{|[\mathbf{0}]_R|} \geq 0$ (for it represents a probability), we get that

$$Q_{dec,d_i} \geq \textstyle\sum_{R\in\Phi_i}\left(1-\frac{1}{q^i}\right) + \sum_{R\in\tilde{\Phi}_i}\left(1-\frac{1}{\max\{1,q^{k-n+d_i}\}}\right).$$

From Lemma 3.2 we have that $|\Phi_i| = A^i_{d_i}$ and since the summands do not depend on R we get that Q_{dec,d_i} is greater or equal to

$$A^i_{d_i}\left(1-\tfrac{1}{q^i}\right) + \left(\tbinom{n}{d_i} - A^i_{d_i}\right)\left(1-\tfrac{1}{\max\{1,q^{k-n+d_i}\}}\right).$$

(b) From Lemma 4.3 we can bound $|[\mathbf{0}]_R| \leq q^{i-1}$, for $R \in \tilde{\Phi}_i$, and from Lemma 4.2 we obtain an expression to $|[\mathbf{0}]_R|$, for $R \in \Phi_i$.Substituting those values in expression (24) we get that

$$Q_{dec,d_i} \leq A^i_{d_i}\left(\frac{q-1}{q^i}\right) + \binom{n}{d_i}\left(1-\frac{1}{q^{i-1}}\right).$$

(c) From Lemma 4.2 we have

$$\left[1-\frac{1}{|[\mathbf{0}]_R|}\right] = 1 \tag{25}$$

and, from Corollary 3.6,

$$\left\lceil 1-\frac{1}{|[\mathbf{0}]_R|}\right\rceil \geq \left\lceil 1-\frac{1}{\max\{1,q^{k-n+d_i}\}}\right\rceil. \tag{26}$$

We write the expression (10) as

$$Q_{dec,d_i}=\sum_{R\in\Phi_i}\left\lceil 1-\tfrac{1}{|[\mathbf{0}]_R|}\right\rceil+\sum_{R\in\tilde{\Phi}_i}\left\lceil 1-\tfrac{1}{|[\mathbf{0}]_R|}\right\rceil, \tag{27}$$

an substituting it into (25) and (26) we get

$$Q_{amb,d_i}\geq A^i_{d_i}+\left(\tbinom{n}{d_i}-A^i_{d_i}\right)\left\lceil 1-\tfrac{1}{\max\{1,q^{k-n+d_i}\}}\right\rceil. \tag{28}$$

(d) From expression (13) we have that

$$Q_{amb,d_1}=\sum_{i=0}^{k}a^i_{d_1}\left\lceil 1-q^{-i}\right\rceil.$$

From Corollary 3.4, only two of the summands above are non zero, namely

$$\begin{aligned}Q_{amb,d_1}&=a^0_{d_1}\left\lceil 1-q^{-0}\right\rceil+a^1_{d_1}\left\lceil 1-q^{-1}\right\rceil\\&=a^1_{d_1}\left\lceil 1-q^{-1}\right\rceil\end{aligned}$$

and from Proposition 3.3 we have

$$Q_{amb,d_1}=a^1_{d_1}=A^1_{d_1}.$$

■

V. P_* AND SEPARABILITY PROPERTIES

We start this section presenting some separability properties that generalize the concept of MDS codes and then we will study the behavior of the bounds for $P_*(C)$ expressed in Theorem 4.4 for codes having some of those separability properties.

Using the Singleton bound $d_1(C)\leq n-k+1$ we may define the *Singleton defect* $s(C)$ of an $[n,k]_q$-code C as

$$s(C)=n-k+1-d_1(C).$$

Using the defect, we say that a code C is *Maximum Distance Separable* (MDS) if $s(C)=0$ and (following Boer in [14]) C is *Almost Maximum Distance Separable* (MDS) if $s(C)=1$.

Considering the generalized weights, the separability property of a linear code may be expresses in different but natural ways. Considering the monotonicity of the weight hierarchy, the *i-th Singleton defect* of an $[n,k]_q$-linear code C is defined as

$$s_i(C)=n-k+i-d_i(C).$$

We say (following Wei in [1]) that C is an *j-MDS code* if $s_j(C)=0$ and *j-AMDS code* if $s_j(C)=1$.

We say that C is a *proper j-MDS* code (or just *P_j-MDS*) if it is j-MDS and proper in the sense that

$$j=\min\{i\in[\![k]\!];C \text{ is an } i\text{-MDS code}\}.$$

Similarly, we say C is an *P_j-AMDS code* if

$$j=\min\{i\in[\![k]\!];C \text{ is an } i\text{-AMDS code}\}.$$

A. Expressions for $P_{amb}(C)$ and $P_{dec}(C)$

We consider the matrix Λ used in the vectorial form used (in Proposition 2.2) to express the ambiguity or the decoding error probability. Propositions 3.3 and 3.7 ensures many of the coefficients of Λ^T are null. Let us write Λ^T explicitly as:

.

$$\Lambda^T=\begin{pmatrix}
1 & 0 & \cdots & 0 & 0\\
\vdots & \vdots & & \vdots & \vdots\\
\binom{n}{d_1-1} & 0 & \cdots & 0 & 0\\
\binom{n}{d_1}-A^1_{d_1} & A^1_{d_1} & \cdots & 0 & 0\\
a^0_{d_1+1} & a^1_{d_1+1} & \cdots & 0 & 0\\
\vdots & \vdots & & \vdots & \vdots\\
a^0_{d_{k-1}-1} & a^1_{d_{k-1}-1} & \cdots & 0 & 0\\
a^0_{d_{k-1}} & a^1_{d_{k-1}} & \cdots & A^{k-1}_{d_{k-1}} & 0\\
a^0_{d_{k-1}+1} & a^1_{d_{k-1}+1} & \cdots & a^{k-1}_{d_{k-1}+1} & 0\\
\vdots & \vdots & & \vdots & \vdots\\
a^0_{n-k} & a^1_{n-k} & \cdots & a^{k-1}_{n-k} & 0\\
0 & a^1_{n-k+1} & \cdots & a^{k-1}_{n-k+1} & 0\\
0 & 0 & & a^{k-1}_{n-k+2} & 0\\
0 & 0 & & \vdots & \vdots\\
\vdots & \vdots & \ddots & a^{k-1}_{n-2} & 0\\
0 & 0 & \cdots & n & 0\\
0 & 0 & \cdots & 0 & A^k_{d_k}
\end{pmatrix}$$

In this presentation, the blue values are ensured by Proposition 3.3 and the green entries by Proposition 3.7. Looking at expression (12), we see it is summing over the lines of Λ^T so, in the lines where at most one entry is unknown, we can determine the remaining one using (12): those are the three entries in red.

Looking now at the columns of Λ^T, we see that the quantity of undetermined entries at the column j is given by the difference $(n-k+i)-d_i$ and, in an informal way, we can state that "*the more C is separable, the more the entries of Λ^T are known*". In particular, assuming that C is MDS, that is, that $d_1=n-k+1$, the monotonicity of the weights implies that $d_i=n-k+i$ for every $i\in[\![k]\!]$ and in this case, all nonzero entries of Λ are expressed in terms of the weight spectra, namely, in terms of $A^1_{d_1},A^2_{d_2},\cdots,A^k_{d_k}$. But for an MDS code, the following theorem (due to Han, in [11]) gives explicit expressions for those coefficients, depending exclusively on n,k and q:

Theorem 5.1 (Theorem 2.5 in [11]): Let C be an $[n,k]_q$-linear code and suppose that C is P_s-MDS. Then, for $s\leq i\leq k$, we have that

$$A^i_r(C)=\begin{cases}0, & \text{if } 0\leq r\leq d_i\\ \binom{n}{r}\sum_{t=0}^{r-d_i}(-1)^t\binom{r}{t}\begin{bmatrix}r+i-d_i-t\\ i\end{bmatrix}_q, & \text{if } d_i<r\leq n\end{cases}$$

Using those expressions for $A^1_{d_1},A^2_{d_2},\cdots,A^k_{d_k}$ we have an alternative proof of the following Theorem (already proved by Kasami and Lin in [15]):

Theorem 5.2: Let C be an MDS code. Then,

(a) $P_{amb}(C) = \sum_{i=n-k+1}^{n} \binom{n}{i} \mathtt{p}^i (1-\mathtt{p})^{n-i}$;

(b) $P_{dec}(C) = \sum_{i=n-k+1}^{n} \binom{n}{i} \left(1 - \frac{1}{q^i}\right) \mathtt{p}^i (1-\mathtt{p})^i$.

If C is an AMDS code, that is, if $d_1 = n-k$, there is an unique $s := s(C) \leq k$ such that C is P_s-MDS and we can determine an explicit formula for $P_*(C)$ depending only on $A^1_{d_1}$ and s:

Theorem 5.3: Let C be an $[n,k]_q$ AMDS linear code and let $s := s(C) \leq k$ such that C is P_s-MDS. Then,

$$\begin{aligned} P_{amb}(C) =& A^1_{n-k} \mathtt{p}^{n-k} (1-\mathtt{p})^k \\ &+ \sum_{i=1}^{n} \binom{n}{n-k+i} \mathtt{p}^{n-k+i} (1-\mathtt{p})^{k-i} \end{aligned}$$

and

$$\begin{aligned} P_{dec}(C) =& \sum_{i=0}^{s-2} A^{i+1}_{n-k+i} \left(\frac{q-1}{q^{i+1}}\right) \mathtt{p}^{n-k+i} (1-\mathtt{p})^{k-i} \\ &+ \sum_{i=0}^{k} \binom{n}{n-k+i} \left(1 - \frac{1}{q^i}\right) \mathtt{p}^{n-k+i} (1-\mathtt{p})^{k-i}. \end{aligned}$$

Proof: It follows straightforward from the use of the vectorial form (2.2) and Propositions 3.3 and 3.7. ■

We remark that Theorem 5.3 ensures that, for an AMDS code, the error probability $P_{amb}(C)$ and $P_{dec}(C)$ of a code is completely determined by the coefficients A^1_{n-k} and $A^1_{n-k}, \cdots, A^{s-1}_{n-k+s-2}$ of the spectra-matrix, respectively. It follows that bounds for the coefficients of the spectra-matrix leads to bounds for $P_*(C)$. In the particular case of an NMDS-code (a code C such that $d_1(C) = n-k$ and $d_2(C) = n-k+2$), the coefficient A^1_{n-k} fully determines $P_*(C)$ and an upper bound for this coefficient is provided Dodunekov e Landgev, in [16]: $A^1_{n-k} \leq \binom{n}{k-1} \frac{q-1}{k}$.

B. Behavior of P_* for small p *and optimality of MDS and AMDS codes*

As expected, for small overall error probability p, minimizing error probability $P_*(C)$ demands to maximize $d_1(C)$:

Proposition 5.4: Let C_1 and C_2 be two $[n,k]_q$-linear codes. For p sufficiently small, if $d_1(C_1) > d_1(C_2)$ then $P_*(C_1) < P_*(C_2)$.

Proof:

To prove the proposition we assume $d_1(C_1) > d_1(C_2)$ and show that

$$\lim_{\mathtt{p}\to 0} \frac{P_*(C_1)}{P_*(C_2)} = 0.$$

But

$$\begin{aligned} \lim_{\mathtt{p}\to 0} \frac{P_*(C_1)}{P_*(C_2)} &= \lim_{\mathtt{p}\to 0} \frac{\sum_{i=d_1(C_1)}^{n} Q_{*,i}(C_1) \mathtt{p}^i (1-\mathtt{p})^{n-i}}{\sum_{j=d_1(C_2)}^{n} Q_{*,j}(C_2) \mathtt{p}^j (1-\mathtt{p})^{n-j}} \\ &= \lim_{\mathtt{p}\to 0} \frac{\sum_{i=d_1(C_1)}^{n} Q_{*,i}(C_1) \left(\frac{\mathtt{p}}{(1-\mathtt{p})}\right)^i}{\sum_{j=d_1(C_2)}^{n} Q_{*,j}(C_2) \left(\frac{\mathtt{p}}{(1-\mathtt{p})}\right)^j}, \end{aligned}$$

where the first equality follows from equation (8). Denoting $x = \frac{\mathtt{p}}{(1-\mathtt{p})}$ and noting that $\lim_{p\to 0} \frac{\mathtt{p}}{(1-\mathtt{p})} = 0$ we get that

$$\begin{aligned} \lim_{x\to 0} \frac{P_*(C_1)}{P_*(C_2)} &= \lim_{x\to 0} \frac{\sum_{i=d_1(C_1)}^{n} Q_{*,i}(C_1) x^i}{\sum_{j=d_1(C_2)}^{n} Q_{*,j}(C_2) x^j} \\ &= \lim_{x\to 0} \frac{\sum_{i=d_1(C_1)-d_1(C_2)}^{n-d_1(C_2)} Q_{*,i+d_1(C_2)}(C_1) x^i}{\sum_{j=0}^{n-d_1(C_2)} Q_{*,j+d_1(C_2)}(C_2) x^j} \end{aligned}$$

and since we are assuming $d_1(C_1) - d_1(C_2) > 0$, we have that

$$\lim_{x\to 0} \frac{P_*(C_1)}{P_*(C_2)} = 0 < 1$$

and from continuity of the functions we have that $\frac{P_*(C_1)}{P_*(C_2)} < 1$, or equivalently $P_*(C_1) < P_*(C_2)$, for every p sufficiently small. ■

If for a given pair (n,k) there exist an MDS (AMDS) $[n,k]_q$ code, we say that (n,k) is *q-MDS* (*q-AMDS*). As an immediate consequence of Proposition 5.4 we have the following proposition (already known and proved in [13]):

Proposition 5.5: If (n,k) is q-MDS and C is an $[n,k]_q$-code that minimizes the error probability, then C is MDS.

Pairs that are q-MDS are not very frequent . For $q = 2$, for example, it is well known that MDS-codes are rather trivial and the unique 2-MDS pairs are the pairs (n,n), $(n,1)$, $(n,0)$, $(n,n-1)$. Considering AMDS codes, those are not classified, but there are many constructions of particular families of AMDS codes and results ensuring the existences of such codes with parameters n and k (see for example [14]). In all those cases, when the pair (n,k) is AMDS but not MDS, for p sufficiently small, a code that minimizes P_* should be an AMDS code.

From Proposition 5.4 we know that, for p sufficiently small, we should look for codes having maximal minimal distance. Among all those codes, which should perform better? A partial answer is given by the next two results and can be summarized as follows: maximize the minimal distance and then minimize the corresponding value in the spectra.

Proposition 5.6: Let C_1 and C_2 be two $[n,k]_q$-linear codes with $d_1(C_1) = d_1(C_2)$. If $Q_{*,d_1(C_1)} < Q_{*,d_1(C_2)}$, then $P_*(C_1) < P_*(C_2)$, for p sufficiently small.

Proof: From equation (8) we get that

$$\lim_{x\to 0} \frac{P_*(C_1)}{P_*(C_2)} = \lim_{x\to 0} \frac{\sum_{i=d_1(C_1)}^{n} Q_{*,i}(C_1) x^i}{\sum_{i=d_1(C_2)}^{n} Q_{*,i}(C_2) x^i}.$$

We write $d_1 = d_1(C_1) = d_1(C_2)$ and cancel x^d from the right side we get

$$\begin{aligned} \lim_{x\to 0} \frac{P_*(C_1)}{P_*(C_2)} &= \lim_{x\to 0} \frac{Q_{*,d_1}(C_1) + \sum_{i=d_1+1}^{n} Q_{*,i}(C_1) x^{i-d_1}}{Q_{*,d_1}(C_2) + \sum_{i=d_1+1}^{n} Q_{*,i}(C_2) x^{i-d_1}} \\ &= \frac{Q_{*,d_1}(C_1)}{Q_{*,d_1}(C_2)} < 1. \end{aligned}$$

hence $P_*(C_1) < P_*(C_2)$ for every p sufficiently small. ■

Proposition 5.7: Let C_1 and C_2 be two $[n,k]_q$-linear codes with $d_1(C_1) = d_1(C_2)$. If $A^1_{d_1}(C_1) < A^1_{d_1}(C_2)$, then $P_*(C_1) < P_*(C_2)$, for p sufficiently small.

Proof: It follows straightforward from Proposition 5.6 and items *(b)* and *(d)* of Theorem 4.4. ■

VI. Conclusion

In this work we used the generalized weights and spectra to set new bounds for the error probability over an erasure channel. Further work may be done exploring the situation when two codes have the same minimal distance and this is attained by the same number of vectors. The role of generalized weights and spectra for the error probability still needs to be explained for other channels.

Acknowledgment

This work was partially supported by CAPES and FAPESP grants 2007/56052-8 and 2013/09493-0.

References

[1] V. K. Wei, "Generalized hamming weights for linear codes," *Information Theory, IEEE Transactions on*, vol. 37, no. 5, pp. 1412–1418, 1991.

[2] H. Stichtenoth and C. Voss, "Generalized hamming weights of trace codes," *Information Theory, IEEE Transactions on*, vol. 40, no. 2, pp. 554–558, 1994.

[3] G. Feng, K. Tzeng, and V. Wei, "On the generalized hamming weights of several classes of cyclic codes," *Information Theory, IEEE Transactions on*, vol. 38, no. 3, pp. 1125–1130, 1992.

[4] C. Munuera, "On the generalized hamming weights of geometric goppa codes," *Information Theory, IEEE Transactions on*, vol. 40, no. 6, pp. 2092–2099, 1994.

[5] A. Barbero and C. Munuera, "The weight hierarchy of hermitian codes," *SIAM Journal on Discrete Mathematics*, vol. 13, no. 1, pp. 79–104, 2000. [Online]. Available: http://epubs.siam.org/doi/abs/10.1137/S089548019834342X

[6] H. Georg Schaathun, "The weight hierarchy of product codes," *Information Theory, IEEE Transactions on*, vol. 46, no. 7, pp. 2648–2651, 2000.

[7] P. Heijnen and R. Pellikaan, "Generalized hamming weights of q-ary reed-muller codes," *Information Theory, IEEE Transactions on*, vol. 44, no. 1, pp. 181–196, 1998.

[8] T. Klove, "Weight hierarchies of binary linear codes of dimension 4," in *Information Theory, 1993. Proceedings. 1993 IEEE International Symposium on*, 1993, pp. 147–147.

[9] J. Hirschfeld, M. Tsfasman, and S. Vladut, "The weight hierarchy of higher dimensional hermitian codes," *Information Theory, IEEE Transactions on*, vol. 40, no. 1, pp. 275–278, 1994.

[10] A. Ashikhmin, A. Barg, and S. Litsyn, "New upper bounds on generalized weights," *Information Theory, IEEE Transactions on*, vol. 45, no. 4, pp. 1258–1263, 1999.

[11] S. T. D. S. Han, "Higher weights and generalized mds codes," *J. Korean Math. Soc.*, vol. 47, no. 6, pp. 1167–1182, 2010.

[12] F. Didier, "A new upper bound on the block error probability after decoding over the erasure channel," *Information Theory, IEEE Transactions on*, vol. 52, no. 10, pp. 4496–4503, 2006.

[13] S. Fashandi, S. Gharan, and A. Khandani, "Coding over an erasure channel with a large alphabet size," in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, 2008, pp. 1053–1057.

[14] M. A. de Boer, "Almost mds codes," *Designs, Codes and Cryptography*, vol. 9, no. 2, pp. 143–155, 1996.

[15] T. Kasami and S. Lin, "On the probability of undetected error for the maximum distance separable codes," *Communications, IEEE Transactions on*, vol. 32, no. 9, pp. 998–1006, 1984.

[16] S. Dodunekov and I. Landgev, "On near-mds codes," *Journal of Geometry*, vol. 54, no. 1-2, pp. 30–43, 1995. [Online]. Available: http://dx.doi.org/10.1007/BF01222850