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@ictе.uftm.edu.br

Marcelo Firer
Department of Mathematics
State University of Campinas
Campinas - SP, Brazil
Email: mfrir@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 AMDS codes) 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 $\mathbb{P}_{ij} := \Pr[Y = j | X = i]$ defined by:

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

The constant $0 < p < 1/2$ is called the overall error probability of the channel.

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

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

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

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 $x \in \mathbb{F}_q^n$, the support of $x$ is

$$\text{supp}(x) = \{i \in [n] \mid \text{with } x_i \neq 0\}$$

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

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

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

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

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 $\mathcal{A}_1^j = \mathcal{A}_1^j(C)$ the set of all $i$-dimensional linear subcodes $D \subseteq C$ supported by $j$ coordinates, that is,

$$\mathcal{A}_1^j(C) = \{D \subseteq C \mid |\text{supp}(D)| = j \text{ and } \dim(D) = i\}. $$
The cardinality of $A_j^i$ is called the $i$-th generalised spectra with support $j$ of the code $C$ and we denote

$$A_j^i = |A_j^i|.$$ 

We call the matrix $(A_j^i)_{i=0,\ldots,k;j=0,\ldots,n}$ 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,

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

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

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

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

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

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

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

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

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

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, $y \in \mathcal{Y}^n$, $R \subseteq [n]$ and $C$ a linear code, we have that

(i) $|y]_R = \emptyset$ iff $y \notin E_C$;

(ii) $|y]_R = \{ x \in C; x^R = y^R \}$;

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

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

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

D. Error probability for ambiguity and decoding

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

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

$$P_{\text{amb}}(C) = \sum_{y \in \mathcal{Y}^n} \mathbb{P}_{\text{amb}}(y) \mathbb{P}_{\text{receive}}(y)$$

$$= \sum_{y \in E_C} \mathbb{P}_{\text{amb}}(y) \mathbb{P}_{\text{receive}}(y),$$

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

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

$$P_{\text{dec}}(C) = \sum_{y \in \mathcal{Y}^n} \mathbb{P}_{\text{dec}}(y) \mathbb{P}_{\text{receive}}(y)$$

$$= \sum_{y \in E_C} \mathbb{P}_{\text{dec}}(y) \mathbb{P}_{\text{receive}}(y),$$

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

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

$$P_\ast(C) = \sum_{y \in E_C} \mathbb{P}_{\ast}(y) \mathbb{P}_{\text{receive}}(y).$$

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

$$\mathbb{P}_{\text{receive}}(y) = \sum_{x \in C} P(y|x) \mathbb{P}_{\text{send}}(x)$$

$$= \frac{1}{q^k} \sum_{x \in C} P(y|x).$$

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

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

$$= |[0]_R|q^{-k}p^{|R|} (1-p)^{|\bar{R}|}.$$ (3)

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

$$P_\ast(C) = \sum_{y \in E_C} \mathbb{P}_{\ast}(y)|[0]_R|q^{-k}p^{|R|} (1-p)^{|\bar{R}|},$$ (4)

hence we may write (5) as

$$P_\ast(C) = \sum_{R \subseteq [n]} \mathbb{P}_{\ast}(y)|E_R||[0]_R|q^{-k}p^{|R|} (1-p)^{|\bar{R}|}.$$
and, from statement (v) in Proposition 2.1 it follows that
\[ P_s(C) = \sum_{R \leq [n]} P_s(R) p^{[R]} (1 - p)^{|[R]|}. \]  
(6)

We note that we are exchanging \( P_s(y) \) by \( P_s(R) \) and this is possible since those probabilities do not depend on \( y \) but only at what are the erased coordinates of \( y \), that is, on the set
\[ R = R(y) = \{ i \in [n]; y_i = \epsilon \}. \]

Denoting
\[ Q_{s,r} = \sum_{R \leq [n]: |R| = r} P_s(R), \]
we may write (6) as
\[ P_s(C) = \sum_{r=0}^{n} Q_{s,r} p^r (1 - p)^{n-r}. \]  
(8)

We note that
\[ Q_{dec,r} = \sum_{R \subseteq [n]:|R| = r} \left( 1 - \frac{1}{|0|R|} \right), \]  
(9)
\[ Q_{amb,r} = \sum_{R \subseteq [n]:|R| = r} \left[ 1 - \frac{1}{|0|R|} \right]. \]  
(10)
where \([\alpha]\) is the smallest integer greater or equal to \( \alpha \in \mathbb{R} \).

In our case, we have that
\[ \left[ 1 - \frac{1}{|0|R|} \right] = \begin{cases} 0 & \text{if } |0|R| = 1; \\
1 & \text{if } |0|R| > 1, \end{cases} \]
that is, it equals 1 or 0 according if there is more than one or only one (namely \( y \)) admissible messages having \( R \) as a set of ambiguous coordinates.

We define
\[ a_i^s := a_i^s(C) = |\{ R \in [n]; |R| = r \text{ and } \dim (0|R|) = i \}| \]
and
\[ \delta_{s,i} = \begin{cases} 1 - \frac{1}{q^r}, & \text{for } s = \text{dec}; \\
1 - \frac{1}{q^r}, & \text{for } s = \text{amb}. \end{cases} \]

We note that each \( a_i^s \) depends on the code \( C \), since \([0|R|\) is the kernel of the projection \( \pi_R \) restricted to \( C \). We also remark that
\[ \sum_{i=0}^{k} a_i^s = \binom{n}{r}. \]
(12)

With this notation we have that
\[ Q_{s,r} = \sum_{i=0}^{k} a_i^s \delta_{s,i} \]
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
\[ P_s(C) = \delta_s \Lambda \rho^T \]  
(14)
where
\[ \delta_s = (\delta_{s,0}, \ldots, \delta_{s,k}), \]
\[ \rho = ((1-p)^{a_0}, p(1-p)^{a_1}, \ldots, p^n) \]
\[ \rho^T \] is the transpose of the vector \( \rho \) and
\[ \Lambda = \begin{pmatrix} a_0 & a_0 & \ldots & a_0 \\ a_0 & a_0 & \ldots & a_0 \\ \vdots & \vdots & \ddots & \vdots \\ a_0 & a_0 & \ldots & a_0 \end{pmatrix}. \]

We remark that \( \delta_s \) depends only on the the parameters \([n,k]_q \) and on * meaning “decoding” or “ambiguity”; \( \rho \) depends only at the channel not on the code; the matrix \( \Lambda \) depends only on the code \( C \), not on the channel neither on * meaning “decoding” or “ambiguity”. For this reason, since only \( \Lambda \) 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, \( D \in A_1^s(C) \) and \( s \in [k] \). Then, \( D \) contains a set of linearly independent vectors \( \{x^1, \ldots, x^{i-1}\} \subseteq D \) such that \( \pi_s(x^j) = 0 \), for any \( j \in [i-1] \).

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

Let us now assume that \( s \in R \). Since \( R = \text{supp}(D) \), there is \( x \in D \) such that \( \pi_{\{s\}}(x) \neq 0 \). We consider a basis of the subspace \( D \) containing \( x \), let us say \( \{x, u^1, \ldots, u^{i-1}\} \). We define
\[ x^i = u^i - \frac{\pi_i(u^i)}{\pi_s(x)} x \]
and it is immediate to check that \( \{x^1, \ldots, x^{i-1}\} \) is linearly independent and \( \pi_s(x^i) = 0 \), for any \( j \in [i-1] \). \[ \square \]

**Lemma 3.2:** For every \( i \in [k] \) the coefficient \( A_{d_i}^s \) of the spectra-matrix depends on the number of different supports attained by subcodes in \( A_{d_i}^s \), that is,
\[ A_{d_i}^s = |\{ R; R = \text{supp}(D) \text{ and } D \in A_{d_i}^s \}|. \]

**Proof:** It is enough to prove that for \( D_1, D_2 \in A_{d_i}^s \), if \( D_1 \neq D_2 \), then \( \text{supp}(D_1) \neq \text{supp}(D_2) \).

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

Denoting \( \bar{D} = \langle x^1, \ldots, x^i \rangle \) we have that \( \dim(\bar{D}) = i \) and \( \text{supp}(\bar{D}) \subseteq R \setminus \{s\} \), that is, \( \text{supp}(\bar{D}) < d_i \), a contradiction. \( \square \)

We are now able to determine \( d_i^s = 0 \) for \( r \leq d_i \).
But equation (17) implies

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

\[
\dim(\text{Im}(\pi_{\{j\}})) = n - r - 1 \tag{20}
\]

and since \(\dim([0]_{R}) = \dim(\ker(\pi_{R}))\), we have that

\[
\dim(\text{Im}(\pi_{R})) = \dim(C) - \dim(\ker(\pi_{R})) = k - i. \tag{21}
\]

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

\[
\dim(\text{Im}(\pi_{S_j})) \leq \min(k - i, n - r - 1) \tag{22}
\]

and equations (18) and (22) together imply

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

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 \([n,k]\) linear code \(C\) and \(R \subseteq \{0\}_{[R]}\) with \(|R| = r\), then \(|[0]_{R}| \geq q^{k-n+r}\).

**Proof:** The proof is made by induction on \(|R|\). For the initial step, \(|R| = 0\), the result is satisfied since \(R = 0\).

Suppose \(|[R]| \geq q^{k-n+|R|}\) for every \(R \subseteq \{0\}_{|n|}\) with \(|R| \leq r\) and let us prove it also holds for \(J \subseteq \{0\}_{|n|}\) with \(|J| = r + 1\).

We write \(J = R \cup \{j\}\) with \(|R| = r\) and \(j \not\in R\), and from Lemma 3.5 it follows that

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

with \(i = \dim([0]_{R})\). The induction hypothesis implies that

\[
\dim([0]_{J}) \geq \max(k + r + 1 - n, k - n + r)
\]

\[
= k - n + (r + 1). \tag{23}
\]

**Proposition 3.7:** If \(r \geq n - k + i + 1\), then \(a^{ij}_{i} = 0\).

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

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

We cannot have \(R = \{0\}_{|n|}\), since this would imply \(r = n\) and \(i = k\), contradicting inequality (23). So, let us assume that \(R \subseteq \{0\}_{|n|}\), so there is \(j \in \{0\}_{|n|} \setminus R\). From Lemma 3.5 we have that

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

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

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

It follows there is a subcode \(D \subseteq [0]_{R \cup \{j\}}\) 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 \(\tilde{D} \subseteq [0]_{R}\) and \(\dim([0]_{R}) = i\), a contradiction. It follows that, for \(r \geq n - k + i + 1\), there does not exist \(R \subseteq \{0\}_{|n|}\) such that \(|R| = r\) and \(\dim([0]_{R}) = i\), in other words, \(a^{ij}_{i} = 0\) for \(r \geq n - k + i + 1\).
Corollary 3.8: \(a_{i-1}^n = 0\) for every \(i \neq k-1\) and \(a_{n-1}^{k-1} = n\).

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

\[
\sum_{i=0}^{k} a_{i-1}^n = \binom{n}{n - 1},
\]

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

IV. BOUNDS FOR \(P_s\)

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

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

Proof: Since \(D \subseteq \{0\}_R\), we have that \(|0|_R \geq |D| = q^i\). ■

Lemma 4.2: Let \(C\) be an \([n, k]\)-linear code. If \(R = \text{supp}(D)\) and \(D \in A_{d_i}^1\), then \(|0|_R = q^i\).

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

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

hence

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

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

In the previous lemma we considered a subset \(R \subseteq \{n\}\) that is the support of a subcode \(D \in A_{d_i}^1\) realizing the \(i\)-th weight. In the following proposition we assume that \(|R| = d_i\) but \(R \neq \text{supp}(D)\) for any \(D \in A_{d_i}^1\) realizing the \(i\)-th weight.

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

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

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

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

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

Theorem 4.4 (Bounds for \(P_s(C)\)): Let \(C\) be an \([n, k]\)-linear code. Then,

(a) For every \(i \in \{k\}\), the coefficient \(Q_{\ast, d_i}\) is greater or equal to

\[
A_{d_i}^1 \left(1 - \frac{1}{q^i}\right) + \left(\binom{n}{d_i} - A_{d_i}^1\right) \left(1 - \frac{1}{\max\{1, q^{k-1}\}}\right);
\]

(b) For every \(i \in \{k\}\), the coefficient \(Q_{\ast, d_i}\) is smaller or equal to

\[
A_{d_i}^1 \left(q - 1\right) + \left(\binom{n}{d_i} - A_{d_i}^1\right) \left(1 - \frac{1}{q^{k-1}-1}\right);
\]

(c) For every \(i \in \{2, k\}\), the coefficient \(Q_{\ast, d_i}\) is greater or equal to

\[
A_{d_i}^1 + \left(\binom{n}{d_i} - A_{d_i}^1\right) \left[1 - \frac{1}{\max\{1, q^{k-1} - d_i\}}\right];
\]

(d) \(Q_{\ast, d_i} = A_{d_i}^1\).

Proof:

(a) To simplify the notation we write:

\[
\Phi_i = \{R \subseteq \{n\}; R = \text{supp}(D)\} \text{ with } D \in A_{d_i}^1
\]

and

\[
\Phi_i = \{R \subseteq \{n\}; |R| = d_i\} \setminus \Phi_i.
\]

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

\[
Q_{\ast, d_i} = \sum_{R \in \Phi_i} \left(1 - \frac{1}{|0|_R}\right) + \sum_{R \in \Phi_i} \left(1 - \frac{1}{|0|_R}\right).
\]

Lemma 4.2 ensures that \(R \in \Phi_i\) implies \(|0|_R = q^i\) so

\[
Q_{\ast, d_i} \geq \sum_{R \in \Phi_i} \left(1 - \frac{1}{q^i}\right) + \sum_{R \in \Phi_i} \left(1 - \frac{1}{q^i}\right).
\]

Corollary 3.6 ensures that if \(R \in \Phi_i\) then \(|0|_R \geq q^{k-1} - d_i\), and since we must have \(1 - \frac{1}{|0|_R} \geq 0\) (for it represents a probability), we get that

\[
Q_{\ast, d_i} \geq \sum_{R \in \Phi_i} \left(1 - \frac{1}{q^i}\right) + \sum_{R \in \Phi_i} \left(1 - \frac{1}{\max\{1, q^{k-1} - d_i\}}\right).
\]

From Lemma 3.2 we have that \(|\Phi_i| = |A_{d_i}^1|\) and since the summands do not depend on \(R\) we get that \(Q_{\ast, d_i}\) is greater or equal to

\[
A_{d_i}^1 \left(1 - \frac{1}{q^i}\right) + \left(\binom{n}{d_i} - A_{d_i}^1\right) \left(1 - \frac{1}{\max\{1, q^{k-1} - d_i\}}\right);
\]

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

\[
Q_{\ast, d_i} \leq A_{d_i}^1 \left(q - 1\right) + \left(\binom{n}{d_i} - A_{d_i}^1\right) \left(1 - \frac{1}{q^{k-1}-1}\right);
\]

(c) From Lemma 4.2 we have

\[
1 - \frac{1}{|0|_R} = 1
\]
and, from Corollary 3.6,
\[
\left[1 - \frac{1}{|\mathcal{I}\rangle_{\mathcal{R}}}ight] \geq \left[1 - \max\{1, q^{k-n+d_i}\}\right]. \tag{26}
\]
We write the expression (10) as
\[
Q_{\text{dec},d_i} = \sum_{\mathcal{R} \in \Phi} \left[1 - \frac{1}{|\mathcal{I}\rangle_{\mathcal{R}}}ight] + \sum_{\mathcal{R} \in \bar{\Phi}} \left[1 - \frac{1}{|\mathcal{I}\rangle_{\mathcal{R}}}ight], \tag{27}
\]
an substituting it into (25) and (26) we get
\[
Q_{\text{amb},d_i} \geq A_{d_i}^1 + \left(\binom{n}{q} - A_{d_i}^1\right) \left[1 - \max\{1, q^{k-n+d_i}\}\right]. \tag{28}
\]
(d) From expression (13) we have that
\[
Q_{\text{amb},d_i} = \sum_{i=0}^{k} a_{d_i}^1 \left[1 - q^{-i}\right].
\]
From Corollary 3.4, only two of the summands above are non zero, namely
\[
Q_{\text{amb},d_i} = a_{d_i}^0 \left[1 - q^{-0}\right] + a_{d_i}^1 \left[1 - q^{-1}\right]
\]
and from Proposition 3.3 we have
\[
Q_{\text{amb},d_i} = a_{d_i}^1 = A_{d_i}^1.
\]
\[\blacksquare\]

V. \textit{P}s 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 \textit{P}s(\textit{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 \textit{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 \textit{Maximum Distance Separable} (MDS) if \(s(C) = 0\) and (following Boer in [14]) \(C\) is \textit{Almost Maximum Distance Separable} (AMDS) if \(s(C) = 1\).

Considering the generalized weights, the separability property of a linear code may be expressed 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
\[s_i(C) = n - k + 1 - d_i(C)\]
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 \textit{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 \(P_{2j}\)-AMDS code if
\[j = \min\{i \in [k]; C\text{ is an }i\text{-AMDS code}\}\]

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

We consider the matrix \(\Lambda\) 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 \(\Lambda^T\) are null. Let us write \(\Lambda^T\) explicitly as:
\[
\Lambda^T = \begin{pmatrix}
1 & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
\left(\binom{n}{q} - A_{d_i}^1\right) & 0 & \cdots & 0 & 0 \\
A_{d_i+1}^0 & A_{d_i+1}^1 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
a_{d_{k-1}+1}^0 & a_{d_{k-1}+1}^1 & \cdots & a_{d_{k-1}+1}^{k-1} & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
a_{n-k}^0 & a_{n-k}^1 & \cdots & a_{n-k}^{k-1} & 0 \\
0 & a_{n-k+1}^0 & \cdots & a_{n-k+1}^{k-1} & 0 \\
0 & 0 & \cdots & a_{n-k+2}^{k-1} & 0 \\
0 & 0 & \cdots & 0 & A_{d_k}^k
\end{pmatrix}
\]
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 \(\Lambda^T\) 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 \(\Lambda^T\), 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 \(\Lambda^T\) 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 \(\Lambda\) are expressed in terms of the weight spectra, namely, in terms of A_{d_k}^{d_k}, A_{d_k}^{d_k-1}, \ldots, A_{d_k}^{d_k-k+2}.\)

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 \(q\):

\textbf{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
\[
A_{i}^{s}(C) = \begin{cases}
0, & \text{if } 0 \leq r \leq d_i \\
\binom{n}{r} \sum_{t=0}^{s-r} (-1)^t \binom{r}{t} \left[\frac{n-k-i-t}{r+i-d_i-t}\right]_{q}, & \text{if } d_i < r \leq n
\end{cases}
\]

Using those expressions for A_{d_1}^{d_1}, A_{d_2}^{d_2}, \ldots, A_{d_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) $P_{amb}(C) = \sum_{n=0}^{\infty} n^{n-1} \left(\frac{1}{q}\right)^{n-1};$
(b) $P_{dec}(C) = \sum_{n=0}^{\infty} \left(1 - \frac{1}{q}\right)^{n} \left(1 - p\right)^{n}.$

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 $P_s(C)$ depending only on $A_{d_1}$ 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,

$$P_{amb}(C) = A_{1-n}^{-1} P^{-k}(1-p)^k$$
$$+ \sum_{i=1}^{n} \binom{n}{k-i}(1-p)^{k-i}$$
and

$$P_{dec}(C) = \sum_{i=0}^{n-1} A_{n-k+i}^{1-i} \left(\frac{q-1}{q^{n+1}}\right) P^{-k+i}(1-p)^{k-i}$$
$$+ \sum_{i=1}^{k} \binom{n}{k-i}(1-p)^{k-i}.$$

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 $A_{1-n}^{-1}$ and $A_{1-n}^{-1}, A_{1-n}^{-1}, \cdots, A_{1-n}^{-1}$ of the spectrum matrix, respectively. It follows that bounds for the coefficients of the spectrum matrix leads to bounds for $P_s(C).$ In the particular case of an NMDS-code (a code $C$ such that $d_2(C) = n - k$ and $d_2(C) = n - k + 2$), the coefficient $A_{1-n}^{-1}$ determines $P_s(C)$ and an upper bound for this coefficient is provided by Dodunekov et al. in [16]: $A_{1-n}^{-1} = \left(\frac{n}{q-1}\right)^{-1}.$

B. Behavior of $P_s$ for small $p$ and optimality of MDS and AMDS codes

As expected, for small overall error probability $p$, minimizing error probability $P_s(C)$ 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 $P_s(C_1) < P_s(C_2).$

Proof: We prove the proposition we assume $d_1(C_1) > d_1(C_2)$ and show that

$$\lim_{x \to 0} P_s(C_1) = 0.$$ 

But

$$\lim_{x \to 0} P_s(C_1) = \lim_{x \to 0} \sum_{i=1}^{n} \binom{n}{i} Q_*(i) \left(1-p\right)^{n-i}$$
$$= \lim_{x \to 0} \sum_{i=1}^{n} \binom{n}{i} Q_*(i) \left(\frac{p}{1-p}\right)^i.$$

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

$$\lim_{x \to 0} P_s(C_1) = \lim_{x \to 0} \sum_{i=1}^{n} \binom{n}{i} Q_*(i) \left(1-p\right)^{n-i}$$
$$= \lim_{x \to 0} \sum_{i=1}^{n} \binom{n}{i} Q_*(i) \left(\frac{p}{1-p}\right)^i.$$ 

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

$$\lim_{x \to 0} P_s(C_1) = 0 < 1$$

and from continuity of the functions we have that $P_s(C_1) < P_s(C_2), \text{ for every } p$ 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 $P_s$ 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 $P_s(C_1) < P_s(C_2),$ for $p$ sufficiently small.

Proof: From equation (8) we get that

$$\lim_{x \to 0} P_s(C_1) = \lim_{x \to 0} \sum_{i=1}^{n} \binom{n}{i} Q_*,i(C_1) x^i.$$ 

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

$$\lim_{x \to 0} P_s(C_1) = \lim_{x \to 0} Q_*,d_1(C_1) + \sum_{i=1}^{n} \binom{n}{i} Q_*,i(C_1) x^{i-1} - d_1$$
$$= Q_*,d_1(C_1) < Q_*,d_1(C_2) < 1.$$ 

hence $P_s(C_1) < P_s(C_2)$ 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 $P_s(C_1) < P_s(C_2),$ 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