LEANDRO CRUVINEL LEMES

NOVOS LIMITANTES PARA A PROBABILIDADE DE ERRO DE DECODIFICAÇÃO EM CANAIS COM APAGAMENTO

CAMPINAS
2013

UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

LEANDRO CRUVINEL LEMES

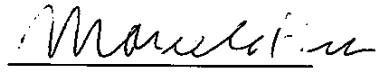
NOVOS LIMITANTES PARA A PROBABILIDADE DE ERRO DE DECODIFICAÇÃO EM CANAIS COM APAGAMENTO

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Matemática.

Orientador: Marcelo Firer

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELO ALUNO LEANDRO CRUVINEL LEMES, E ORIENTADA PELO PROF. DR. MARCELO FIRER

Assinatura do Orientador



CAMPINAS
2013

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

L543n

Lemes, Leandro Cruvinel, 1985-
Novos limitantes para a probabilidade de erro de decodificação em canais com apagamento / Leandro Cruvinel Lemes. – Campinas, SP : [s.n.], 2013.

Orientador: Marcelo Firer.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Peso generalizado de Hamming. 2. Códigos de controle de erros (Teoria da informação). 3. Probabilidade de erro (Matemática). 4. Canal com apagamento. I. Firer, Marcelo. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: New bounds on the decoding error probability over erasure channels
Palavras-chave em inglês:
Generalized Hamming weight
Error-correcting codes (Information theory)
Probability of error (Mathematics)
Erasure channel
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Marcelo Firer [Orientador]
Sueli Irene Rodrigues Costa
Valdemar Cardoso da Rocha Junior
Anderson Clayton Alves Nascimento
Luciano Panek
Data de defesa: 12-09-2013
Programa de Pós-Graduação: Matemática

Tese de Doutorado defendida em 12 de setembro de 2013 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). MARCELO FIRER

Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA

Prof(a). Dr(a). VALDEMAR CARDOSO DA ROCHA JUNIOR

Prof(a). Dr(a). ANDERSON CLAYTON ALVES NASCIMENTO

Prof(a). Dr(a). LUCIANO PANEK

Abstract

Considering an erasure channel, we improve upper and lower bounds for error decoding and ambiguity probabilities of linear error-correcting codes. The given bounds depend on the generalized weight hierarchy and spectrum of a code. We find explicit formulae in the case of AMDS and MDS codes.

Keywords:
MDS codes, AMDS codes, error probabilities, erasure channel, generalized spectrum, generalized Hamming weights

Resumo

Considerando canais discretos, sem memória e com apagamento, obtemos limitantes superiores e inferiores para as probabilidades de erro de decodificação e de ocorrências de ambiguidade de códigos corretores de erro lineares. Os limitantes dependem da hierarquia de pesos e dos espectros generalizados e melhoram os limitantes conhecidos. Encontramos expressões exatas para essas probabilidades nos casos em que o código é AMDS ou MDS.

Palavras-chave:
códigos AMDS, códigos MDS, probabilidade de erro, canais com apagamento, espectros generalizados, pesos generalizados de Hamming

Sumário

Dedicatória

Aos meus amigos e familiares que motivaram a busca e a realização dos meus objetivos, em especial à Angélica Robatino, Carolina Tavares de Oliveira, Cícero Fernandes de Carvalho, Daniel Ribeiro Kacelnik, Matheus Bartolo Guerrero e Rafael Honório Pereira Alves.

Agradecimentos

Agradeço especialmente a Capes e CNPq, pelo apoio econômico que me permitiu culminar com sucesso todo o doutorado.

Lista de Tabelas

Abreviações e siglas

$\mathcal{X}$: Alfabeto de entrada do canal.

$\mathcal{Y}$: Alfabeto de saída do canal.

$p(b|a)$: Probabilidade de receber $b \in \mathcal{Y}$ dado que $a \in \mathcal{X}$ foi transmitido.

$\mathbf{x} = (x_1, \ldots, x_n)$: Palavra de $\mathcal{X}^n$.

$\mathbf{y} = (y_1, \ldots, y_n)$: Palavra de $\mathcal{Y}^n$.

$\mathcal{F}$: Conjunto de palavras de $\mathcal{X}^n$ possíveis de serem enviadas de um canal.

$\mathtt{p}$: Probabilidade de ocorrer erro no canal.

DC : Canal discreto.

DM : Canal sem memória.

DMC : Canal discreto sem memória.

DMSC : Canal discreto simétrico sem memória.

DMEC : Canal discreto de apagamento sem memória.

$\mathbb{F}_q$: Corpo finito com q elementos.

ϵ : Símbolo de erro em um canal com apagamento.

$[\![n]\!]$: Conjunto dos inteiros maiores ou iguais a 1 e menores ou iguais a n.

$[\![r, s]\!]$: Conjunto dos inteiros maiores ou iguais a r e menores ou iguais a s.

$span(B)$: $\mathbb{F}_q$-espaço vetorial gerado por B.

$< B >$: $\mathbb{F}_q$-espaço vetorial gerado por B.

$\langle x_1, \ldots, x_n \rangle$: $\mathbb{F}_q$-espaço vetorial gerado por $\{x_1, \ldots, x_n\}$.

C : Código linear.

c **ou** $\tilde{c}$ **ou** c^i : Palavras do código C.

n : Comprimento do código linear C.

k : Dimensão do código linear C.

$[n, k]_q$**-código** : Código linear de comprimento n e dimensão k.

G : Matriz geradora de C.

$\mathcal{H}$: Matriz de verificação de paridade de C.

$C^{\perp}$: Código dual de C.

$d(C) = d$: Distância mínima do código C.

$[n, k, d]_q$**-código** : Código linear de comprimento n, dimensão k e distância mínima d.

$d_i(C) = d_i$: i-ésimo peso de generalizado de Hamming.

$\mathcal{A}_r^i$: Conjuntos de subcódigos de C de dimensão i e suporte r.

A_r^i : i-ésimo espectro de peso r do código C.

D : Subcódigo de C.

$supp(D)$: Suporte do subcódigo D.

$d(.,.)$: Métrica de Hamming.

$w(\mathbf{x})$: Peso mínimo da palavra $\mathbf{x}$ de $\mathcal{F}_q^n$.

$[n, k, d_1, \ldots, d_k]_q$**-código** : Código com i-ésimo peso de generalizado de Hamming igual a d_i.

MDS : Máxima distância separável.

AMDS : Máxima distância quase separável.

NMDS : Máxima distância próxima de ser separável.

$s(C)$: Defeito de Singleton.

$s_i(C)$: i-ésimo defeito de Singleton generalizado.

α : Decodificador.

MLD : Decodificador de máxima verossimilhança.

NND : Decodificador de máxima proximidade.

$P_{dec}(y)$: Probabilidade de y ser decodificado incorretamente.

$P_{err}(y)$: Probabilidade de y ser uma palavra ambígua.

$p(\mathbf{y})$: Probabilidade de receber $\mathbf{y} \in \mathcal{Y}^n$.

$p(\mathbf{c})$: Probabilidade de uma palavra $c \in C$.

$P_{dec}(C; \mathtt{p}, \alpha)$ **ou** $P_{dec}(C)$: Probabilidade de ocorrer erro de decodificação.

$P_{dec}(C; \mathtt{p})$ **ou** P_{dec} : Probabilidade de ocorrer erro de decodificação.

$P_{err}(C; \mathtt{p})$ **ou** $P_{err}(C)$ **ou** P_{dec} : Probabilidade de ocorrer ambiguidade.

H : Denota um subconjunto de $[\![n]\!]$.

$\bar{H}$: Complementar de H relativo a $[\![n]\!]$.

π_H : Aplicação projeção nas coordenadas de índice em H.

$\mathbf{x}^H$: Imagem de $\mathbf{x}$ pela aplicação π_H.

$\mathcal{E}_H(\mathbf{x})$: Palavra $\mathbf{x}$ com apagamentos nas coordenadas de índice em H.

$supp_{\mathcal{E}}(y)$: Suporte apagado de $\mathbf{y}$.

E_C : Conjunto de apagamentos de C.

$[\mathbf{y}]_H$: Conjunto de ambiguidades de $\mathbf{y}$.

E_H : Conjunto de apagamentos de C com suporte apagado H.

$\lceil l \rceil$: Menor inteiro maior ou igual a l.

$P_*(H)$: $P_*(y)$ quando $supp_{\mathcal{E}}(y) = H$.

$Q_{dec,r}$: r-ésimo coeficiente da parcela do somatório que representa $P_{dec}(C)$.

$Q_{err,r}$: r-ésimo coeficiente da parcela do somatório que representa $P_{err}(C)$.

$P_{FAS}^{inf}(C)$: Limitante inferior em [11] para P_{dec}.

$P_{DID}^{sup}(C)$: Limitante superior em [5] para P_{err}.

$P_{T2,dec}^{inf}$: Limitante inferior obtido do Teorema 4.2.2 para P_{dec}.

$P_{T2,err}^{sup}$: Limitante superior obtido do Teorema 4.2.2 para P_{err}.

$Q_{FAS,r}^{inf}$: r-ésimo coeficiente de $P_{FAS}^{inf}(C)$.

$Q_{DID,r}^{sup}$: r-ésimo coeficiente de $P_{DID}^{sup}(C)$.

$Q_{T2}^{inf}(dec, r)$: r-ésimo coeficiente de $P_{dec}(C)$ obtido do Teorema 4.2.2.

$Q_{T2}^{sup}(err, r)$: r-ésimo coeficiente do limitante para $P_{err}(C)$ obtido do Teorema 4.2.2.

Φ_i : Conjunto dos suportes dos códigos i-dimensionais de peso d_i.

$a_i(r)$: Cardinalidade do conjunto de suportes H com $|H| = r$ e $\dim([0]_H) = i$.

Capítulo 1

Introdução

O principal objeto de estudo desta tese são as funções de probabilidade de erro em um canal com apagamento. Utilizando os pesos generalizados de Hamming e seus espectros, obtemos novos limitantes para estas funções e, com isso, expressões explícitas para códigos que, de algum modo, generalizam a condição conhecida como MDS.

A principal "ferramenta de trabalho"utilizada nesta tese são os pesos generalizados de Hamming de um código, que foram estudados por Wei [28] (vide Seção 2.3) e tornaram-se invariantes importantes na teoria de códigos, sendo estes determinados para diversas famílias de códigos, incluindo os códigos traço [25], de Grassman [14], cíclicos [12], de Goppa [22], Hermitianos [3], produto [13], q-ários de Reed-muller [16], de Golay, Hamming, Reed-Muller de ordem mais alta e MDS [28], códigos de dimensão menor ou igual a 4 [19] e códigos hermitianos de dimensão alta [18]. Quando fórmulas explícitas não foram encontradas, limitantes para os pesos generalizados de Hamming foram também determinados [2, 10]. Um apanhado geral de resultados (limitantes e fórmulas explícitas) até 1995, foi feito por Tsfasman e Vladut [26].

Trabalharemos ainda com generalizações diversas do conceito de códigos MDS, incluindo os conceitos de códigos AMDS (almost-MDS) e os códigos NMDS (near-MDS), estudados por Dodunekov e Landgev [7]. Tais códigos são obtidos por restrições mais fracas do que aquelas que definem os códigos MDS. Dentre os códigos NMDS binários estão o $[7, 4, 3]_2$-código de Hamming e o $[8, 4, 4]_2$-código de Hamming extendido. Dentre os ternários, o $[11, 6, 5]_3$-código de Golay e o $[12, 6, 6]_3$-código de Golay extendido [4]. Todo código NMDS é AMDS. Algumas propriedades dos códigos MDS relacionadas com

a dualidade não são válidas para códigos AMDS; por exemplo, o dual de um código AMDS não é, necessariamente, AMDS. Boer [4] determinou limitantes superiores para o comprimento n tal que existam $[n, n-r-1, r+1]$-códigos e $[n, n-r-1, r+1]$-códigos AMDS. A capacidade de detecção de erros de códigos AMDS e NMDS foi estudada por Dodunekova et al. [9], considerando canais simétricos.

Nosso ambiente de trabalho são os canais de apagamento, que tem sido estudados recentemente devido suas aplicações em redes [11]. Modelos diferentes de canais de apagamento são utilizados no estudo da performace de conexões ponto a ponto via internet [11].

Consideramos códigos q-ários sobre um canal discreto, sem memória e com apagamento. Um dos objetivos dessa tese é obter limitantes, inferiores e superiores, para as probabilidade de ocorrência de ambiguidade e de erro de decodificação por máxima verossimilhança para códigos lineares, mais precisos que os que aparecem na literatura até o momento e determinar códigos que atingem tais limitantes. Compararemos os resultados obtidos com os dois limitantes mais justos (tight) encontrados na literatura. Limitantes superiores para a probabilidade de erro antes da decodificação por máxima verossimilhança para códigos aleatórios em canais com apagamento foram obtidos por Didier [5] como função dos pesos generalizados. Limitantes inferiores para a probabilidade de erro após a decodificação por máxima verossimilhança para códigos aleatórios em função do comprimento, dimensão e distância mínima dos códigos foram obtidos por Fashandi et al.; também foi demonstrado que os códigos MDS atingem tais limitantes [11], fazendo a ressalva que os limitantes apresentados em [11] são feitos para alfabetos grandes.

Os limitantes superiores e inferiores para a probabilidade de ocorrência de ambiguidade e para a probabilidade de erro de decodificação são apresentados no Teorema 4.2.2. Para códigos MDS os limitantes inferiores e superiores coincidem, logo determinam uma expressão explícita e exata para as probabilidades de erro de decodificação de um código MDS (Corolário 5.1.2) reproduzindo a fórmula já conhecida por Fashandi et al. em [11]. Quando a probabilidade de erro do canal é suficientemente pequena, fixados comprimento e dimensão de tal forma que não existem códigos MDS, mas existem códigos AMDS, nestes parâmetros, tais códigos minimizam a probabilidade de erro de decodificação e de ocorrência de ambiguidade. Os códigos NMDS são os melhores códigos AMDS, isto é, de todos os códigos AMDS os códigos NMDS são os que apresentam menor probabilidade de erro de decodificação

(Proposição 5.2.11).

Sobre a organização deste trabalho, no Capítulo 2, as notações e definições são fixadas. No Capítulo 3, uma fórmula que depende apenas das partes do conjunto dos inteiros i tais que $1 \leq i \leq n$, para as probabilidades de erro de decodificação e de ocorrência de ambiguidade (Teorema 3.3.1), é apresentada. No Capítulo 4 novos limitantes inferiores e superiores para ambas as probabilidades, de erro e de ocorrência de ambiguidade, em canais discretos sem memória e com apagamento (Teorema 4.2.2), são obtidos. Vários exemplos, considerando $[7,4]_2$ e $[7,4]_7$-códigos, são estudados afim de ilustras uma maior precisão dos limitantes apresentados no Teorema 4.2.2. No Capítulo 5, é estudada uma série de conseqüências dos resultados estabelecidos no Capítulo 4, no que se refere a códigos AMDS e NMDS. Fianlmente, no Capítulo 6, é feita uma análise da probabilidade de erro de decodificação de códigos em canais com apagamento discreto sem memória quando a probabilidade de apagamento do canal é suficientemente pequena.

Capítulo 2

Conceitos

Neste capítulo são apresentados alguns conceitos básicos da teoria de códigos corretores de erro e, também, ferramentas importantes que são utilizadas para construção dos limitantes, inferiores e superiores, para a probabilidade de erro antes e após a decodificação por máxima verossimilhança de códigos corretores de erro, lineares, em canais com apagamento.

2.1 Canais

Um *canal* é um terna $(\mathcal{X}, \mathcal{Y}, p)$ sendo $\mathcal{X}$ (alfabeto de entrada) e $\mathcal{Y}$ (alfabeto de saída) são conjuntos não vazios e

$$\{p(b|a); a \in \mathcal{X} \text{ e } b \in \mathcal{Y}\}$$

é o conjunto de probabilidades condicionais e $p(b|a)$ denota a probabilidade de receber o símbolo $b \in \mathcal{Y}$ dado que $a \in \mathcal{X}$ foi enviado. Uma *palavra* $\mathbf{x}$ (respectivamente $\mathbf{y}$) é um conjunto ordenado de símbolos do alfabeto $\mathcal{X}$ (respectivamente $\mathcal{Y}$). Uma *fonte* $\mathcal{F}$ de um canal é um conjunto de palavras possíveis de serem enviadas compostas por símbolos do alfabeto de entrada $\mathcal{X}$. Se uma palavra $\mathbf{z}$ tem $n < \infty$ coordenadas, identificamos $\mathbf{z} = (z_1, \ldots, z_n)$, em que z_i são os símbolos que compõem a palavra $\mathbf{z}$ em suas respectivas ordens de envio. O inteiro n é chamado de *comprimento* da palavra $\mathbf{z}$.

Um *canal sem memória* (MC) é caracterizado pela independência de seus eventos, isto é, dados $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{X}^n$ e $\mathbf{y} = (y_1, \ldots, y_n) \in \mathcal{Y}^n$ e denotando por $p(y_m|x_m)$ a probabilidade de receber a m-ésima coordenada de $\mathbf{y}$ dado que a m-ésima coordenada de $\mathbf{x}$ foi transmitida, então $p(y_m|x_m)$ depende

apenas dos m-ésimos termos coordenados de $\mathbf{x}$ e $\mathbf{y}$. Consequentemente se $p(\mathbf{y}|\mathbf{x})$ denota a probabilidade de receber n símbolos ordenados $y_1, \ldots, y_n$ dado que n símbolos, também ordenados, $x_1, \ldots, x_n$ foram recebidos, segue que

$$p(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} p(y_i|x_i), \tag{2.1}$$

no caso de canal sem realimentação.

Um *canal discreto* (DC) sobre $\mathbb{F}_q$ tem alfabeto de entrada $\mathcal{X} = \mathbb{F}_q$, em que $\mathbb{F}_q$ denota um corpo finito com q elementos.

Um *canal simétrico discreto* (DSC) sobre $\mathbb{F}_q$ com probabilidade de erro $\mathtt{p}$ satisfaz

(i) $\mathcal{Y} = \mathbb{F}_q$;

(ii) $p(b|a) = \frac{\mathtt{p}}{q-1}$, se $b \neq a$;

(iii) $p(b|a) = 1 - \mathtt{p}$, se $b = a$;

Um c*anal de apagamento discreto* (DEC) sobre $\mathbb{F}_q$ com probabilidade de erro (apagamento) $\mathtt{p}$ satisfaz

(i) $\mathcal{Y} = \mathbb{F}_q \cup \{\epsilon\}$, com $\epsilon \notin \mathbb{F}_q$;

(ii) $p(b|a) = 1 - \mathtt{p}$, se $a = b$;

(iii) $p(b|a) = 0$, se $a \neq b$ com $a, b \in \mathbb{F}_q$;

(iv) $p(\epsilon|a) = \mathtt{p}$, para todo $a \in \mathbb{F}_q$.

O símbolo $\epsilon \notin \mathbb{F}_q$ é chamado de *símbolo de apagamento do canal*.

Em particular, um canal discreto, sem memória e com apagamentos é denotado pela sigla DMEC (Discrete memoryless erasure channel).

2.2 Códigos

Um $[n, k]_q$-*código linear* C é um $\mathbb{F}_q$-subspaço vetorial de $\mathbb{F}_q^n$. Fixado um canal $(\mathcal{X}, \mathcal{Y}, \mathtt{p})$ com fonte $\mathcal{F}$, se a cardinalidade de $\mathcal{F}$ é q^k podemos identificar $\mathcal{F}$ com $\mathbb{F}_q^k$. Um código linear também pode ser visto como a imagem de uma aplicação linear injetora de $\mathbb{F}_q^k$ em $\mathbb{F}_q^n$, assim, também pode ser identificado

com a fonte do canal. Nesta tese algumas restrições: Todas as fontes terão cardinalidade q^k, todos os códigos serão códigos lineares.

Quando conveniente representamos C como o espaço vetorial gerado por um subconjunto de palavras $B \subseteq \mathbb{F}_q^n$, isto é, C é o conjunto de todas as combinações $\mathbb{F}_q$-lineares das palavras de B. Denotamos

$$C = span(B) = \langle B \rangle .$$

No caso em que $B = \{\mathbf{x_1}, \ldots, \mathbf{x_m}\} \subseteq \mathbb{F}_q^n$, então abusamos da notação omitindo as chaves:

$$C = span(\{\mathbf{x_1}, \ldots, \mathbf{x_m}\}) = \langle \mathbf{x_1}, \ldots, \mathbf{x_m} \rangle = \langle \{\mathbf{x_1}, \ldots, \mathbf{x_m}\} \rangle .$$

Se $C = \langle \mathbf{x_1}, \ldots, \mathbf{x_k} \rangle$ e $D = \{\mathbf{x_1}, \ldots, \mathbf{x_k}\}$ é um subconjunto linearmente independente em $\mathbb{F}_q^n$, então D é uma base para C e a matriz G cujas linhas são dadas pelos vetores $\mathbf{x_1}, \ldots, \mathbf{x_k}$ é uma *matriz geradora* de C. Note que uma matriz geradora G de um código C determina inteiramente os elementos de C, logo um código também pode ser identificado por uma de suas matrizes geradoras. Seja H uma matriz de $n-k$ linhas e n colunas satisfazendo

$$Hc^T = 0, \text{ para todo } c \in C.$$

A matriz H é chamada de *matriz de verificação de paridade* de C. O $[n, n-k]_q$-código $C^\perp$ cuja matriz geradora $G^\perp$ é uma matriz de verificação de paridade de C é chamado de *código dual* de C.

É imediato constatar que

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n; \langle \mathbf{x}, c \rangle = 0, \forall c \in C\}$$

em que $\langle , \rangle$ denota o produto interno formal:

$$\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = \sum_{i=1}^{n} x_i y_i.$$

Denotamos $[\![n]\!] := \{1, 2, \ldots, n\}$. Dados inteiros r e s, com $r < s$, denotamos $[\![r, s]\!] = \{r, r+1, \ldots, s-1, s\}$. Em particular $[\![n]\!] = [\![1, n]\!]$. Denotaremos também por $2^{[\![n]\!]}$ o conjunto das partes de $[\![n]\!]$.

Dado $D \subseteq \mathbb{F}_q^n$ o *suporte* de D é o conjunto

$$supp(D) = \{i \in [\![n]\!]; \exists \mathbf{x} \in D \text{ com } x_i \neq 0\}.$$

O *suporte de uma palavra* $\mathbf{x} \in \mathbb{F}_q^n$ é dado por

$$supp(\mathbf{x}) = \{i; x_i \neq 0\}$$

Sejam $\mathbf{x} = (x_1, \ldots, x_n)$ e $\mathbf{y} = (y_1, \ldots, y_n)$ palavras de $\mathbb{F}_q^n$. A função $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{N}_0$ definida por

$$d(\mathbf{x}, \mathbf{y}) := |\{i; x_i \neq y_i\}| = |supp(\mathbf{x} - \mathbf{y})|$$

satisfaz os axiomas de métrica em $\mathbb{F}_q^n$ e é chamada de métrica de Hamming. Note que a definição da função d, pode ter domínios mais gerais, por exemplo $\mathcal{X}^n \times \mathcal{X}^n$ ou $\mathcal{Y}^n \times \mathcal{Y}^n$. Usamos a função d dessa forma sem mencionar detalhes.

O *peso de* $\mathbf{x}$ é dado por

$$w(\mathbf{x}) = d(\mathbf{x}, 0) = |\{i; x_i \neq 0\}| = |supp(x)|. \tag{2.2}$$

A *distância mínima de um código* C, denotada por $d(C)$, é a menor distância entre duas palavras distintas do código, isto é,

$$d(C) = \min\{d(\mathbf{x}, \mathbf{y}); \mathbf{x}, \mathbf{y} \in C\}$$

e, no caso de C ser um código linear, temos

$$d(C) = \min\{w(c); c \in C\}.$$

Caso não houver dúvidas sobre qual o código que estamos trabalhando denotamos simplesmente $d = d(C)$. Um $[n, k]_q$-código C de distância mínima d será chamado de $[n, k, d]_q$-*código*.

2.3 Pesos generalizados de Hamming

Nesta seção apresentamos os pesos generalizados de Hamming estudados por Wei em [28]. Um dos objetivos desta tese é relacionar os pesos generalizados com as probabilidades de erro de decodificação e ocorrência de ambiguidades de $[n, k]_q$-códigos lineares.

O *i-ésimo peso generalizado de Hamming* $d_i(C)$, $i \in [\![k]\!]$, é definido por

$$d_i(C) = \min\{|supp(D)|; D \subseteq C \text{ e } \dim(D) = i\}, \tag{2.3}$$

em que $\dim(D)$ denota a dimensão do subcódigo D como $\mathbb{F}_q$-subspaço vetorial.

A *hierarquia de pesos generalizados de* C é o conjunto

$$\{d_i(C); i \in [\![k]\!]\}.$$

Caso não fique confuso qual código estamos trabalhando, podemos omitir C e utilizar a notação mais simplificada $d_i = d_i(C)$, $i \in [\![k]\!]$. Em particular, d_1 é a distância mínima do código.

Um $[n, k, d_1, \ldots, d_k]_q$-código linear é um subspaço linear k-dimensional C de $\mathbb{F}_q^n$ tal que $d_i(C) = d_i$.

O Teorema 2.3.1 será enunciado sem demonstração. A prova para o teorema pode ser encontrada em [17] ou em [28]. Usamos o Teorema 2.3.1 para determinar os pesos generalizados de alguns códigos dos exemplos que aparecem nesta tese.

Teorema 2.3.1 (Monotonicidade, Teorema 1 em [28]) *Seja C um $[n, k]_q$-código linear. Então*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Podemos relacionar os pesos generalizados de Hamming de um código C com os pesos de seu dual $C^\perp$:

Teorema 2.3.2 (Teorema 3 em [28]) *Seja C um $[n, k, d]_q$-código linear e $C^\perp$ seu dual. Então*

$$\{d_i(C); 1 \leq i \leq k\} = [\![n]\!] \setminus \{n + 1 - d_i(C^\perp); 1 \leq i \leq n\}. \tag{2.4}$$

2.4 MDS e propriedades de separação generalizadas

Nesta seção apresentamos conceitos, generalizações naturais e propriedades básicas de códigos que serão estudados nos próximos capítulos.

Um limitante superior para a distância mínima d_1 de um $[n, k]_q$-código bem conhecido na literatura é o *limitante de Singleton* dado por

$$d_1(C) \leq n - k + 1.$$

O *defeito de Singleton* de um $[n, k]_q$-código C é definido por

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

Dizemos que C é um *código separável pela distância máxima* (MDS) se

$$s(C) = 0.$$

Na década de 90 foram introduzidos diversos conceitos que visam mensurar o quanto um código é próximo de ser MDS. O código C é dito *quase (almost) MDS* (AMDS), conforme definido por Boer em [4], se

$$s(C) = 1.$$

Denotando por $C^{\perp}$ o dual de C, dizemos que C é um *código proximamente (near) MDS* (NMDS) se

$$s(C) = s(C^{\perp}).$$

O conceito de códigos NMDS foi introduzido em [7]. Determinar códigos com estas propriedades de separação é um tarefa difícil. Apenas a título de exemplo, em [6], Dodunekov e Landjev determinam o comprimento n máximo que um $[n,k]_q$-código NMDS pode ter fixados k e $q \in \{2,3,4,5\}$.

Considerando os pesos generalizados de Wei, os conceitos de separabilidade de códigos se generalizam de maneira natural:

O i-ésimo defeito generalizado de Singleton de um $[n,k]_q$-código C é definido por

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

Dizemos que C é um *código j-MDS*, terminologia esta adotada por Wei em [28], se

$$s_j(C) = 0.$$

Também C é um *código j-AMDS* se

$$s_j(C) = 1.$$

E, ainda, C é um *código j-NMDS* se

$$s_j(C) = s_j(C^{\perp}).$$

Dizemos que C é um *código $\mathcal{P}_j$-MDS*, vide [15], se C é um código j-MDS próprio, no sentido de que

$$j = \min\{i \in [\![k]\!]; C \text{ é um código } i\text{-MDS}\}.$$

Analogamente, dizemos que C é um *código $\mathcal{P}_j$-AMDS* se

$$j = \min\{i \in [\![k]\!]; C \text{ é um código } i\text{-AMDS}\}$$

e, por fim, que C é um *código $\mathcal{P}_j$-NMDS* se

$$j = \min\{i \in [\![k]\!]; C \text{ é um código } i\text{-NMDS}\}.$$

Mostramos que códigos NMDS, dentre todos os códigos AMDS, são os códigos que minimizam a probabilidade de erro de decodificação 5.2.11, o que torna a busca por códigos NMDS relevante.

2.5 Espectros generalizados

Denotamos $\mathcal{A}_r^i$ o conjunto dos subcódigos i-dimensionais de C que tenham suporte de cardinalidade r, ou seja,

$$\mathcal{A}_r^i = \{D \subseteq C; \dim D = i \text{ e } |supp(D)| = r\}. \tag{2.5}$$

O *i-ésimo espectro generalizado com suporte de cardinalidade r* é definido por

$$A_r^i = |\mathcal{A}_r^i| \tag{2.6}$$

Expressões exatas e limitantes para esses coeficientes podem ser encontrados em [21], [26] e [15]. Em [24] relações dos espectros do código com os espectros de seu dual são obtidas. Em [23], Schaathun mostra como calcular $A_r^i(C)$ para $i \geq k - d_2^\perp + 3$ em que $d_2^\perp$ é o segundo peso generalizado do código dual de C. Limitantes para A_r^1 de códigos com distância mínima d pelo menos 2 e aplicações desses coeficientes para probabilidade de ocorrer ambiguidade aparecem em [20].

O coeficiente binomial de Gauss é definido por

$$\begin{bmatrix} m \\ r \end{bmatrix}_q = \begin{cases} \frac{(1-q^m)(1-q^{m-1})\cdots(1-q^{m-r+1})}{(1-q)(1-q^2)\cdots(1-q^r)}, & \text{se } r \leq m; \\ 0 & \text{se } r > m, \end{cases}$$

com r e m inteiros não negativos.

O teorema a seguir nos permite determinar A_r^i dos códigos MDS.

Teorema 2.5.1 (Teorema 2.5 em [15]) *Seja C um $[n,k]_q$-código $\mathcal{P}_s$-MDS. Então, para todo $s \leq i \leq k$, temos*

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

O Teorema 5.1.1 é demonstrado utilizando o Teorema 2.5.1.

Em [9], Dodunekova et al. determinam limitantes superiores para o número de palavras mínimas $A_{d_1}^1$ de um código NMDS. No Teorema 5.2.8determinamos uma fórmula explícita para a probabilidade de ocorrer ambiguidade em códigos NMDS dependendo de apenas de $A_{d_1}^1$, n e k. Logo, juntamente com os limitantes em [9], obtemos limitantes superiores para a probabilidade de ocorrer ambiguidade em um código NMDS.

2.6 Probabilidades de erro de decodificação e ocorrência de ambiguidade

Em um canal, ao recebermos uma palavra $\mathbf{y} \in \mathcal{Y}^n$, procuramos associar a esta, uma palavra do código C. Um decodificador é uma função $\alpha : \mathcal{Y}^n \to C$ tal que $\alpha(c) = c$, para todo $c \in C$. Neste sentido, dizemos que um decodificador é uma decisão sobre como interpretar uma palavra $\mathbf{y} \in \mathcal{Y}^n$. Os critérios mais naturais de decisão são os critérios de distância (determinado pela métrica de Hamming) e o probabilístico (determinado pelo canal) que apresentamos a seguir:

Dizemos que um decodificador α é um *decodificador por máxima proximidade* (Nearest Neighbor Decoder - NND) se, dado $\mathbf{y} \in \mathcal{Y}^n$

$$d(\alpha(\mathbf{y}), c) \leq d(\tilde{c}, c), \ \forall \tilde{c} \in C,$$

em que $c \in C$ representa a palavra enviada e $\mathbf{y}$ representa a palavra recebida.

Um decodificador α é um *decodificador de máxima verossimilhança* (Maximum Likelihood Decoder - MLD) se, para todo $y \in \mathcal{Y}^n$, temos

$$p(\alpha(\mathbf{y})|c) \geq p(\tilde{c}|c), \ \forall \tilde{c} \in C.$$

No processo de transmissão de uma palavra $c \in C$ e recebimento de uma palavra $\mathbf{y} \in \mathcal{Y}^n$, dizemos que o decodificador α acerta se $\alpha(\mathbf{y}) = c$ e erra se $\alpha(\mathbf{y}) \neq c$.

É fato conhecido que num canal DMEC com $p < \frac{1}{2}$, um decodificador α é de máxima verossimilhança se, e somente se, é de máxima proximidade.

Dado um código C, denotamos por $P_{dec}(C; \mathtt{p}, \alpha)$ a probabilidade de ocorrer erro de decodificação após os processos de transmissão, recebimento e decodificação das palavras do código C considerando sempre um decodificador NND (ou MLD).

A expressão de $P_{dec}(C; \mathtt{p}, \alpha)$ é dada por

$$P_{dec}(C; \mathtt{p}, \alpha) = \sum_{\mathbf{y} \in \mathcal{Y}^n} P_{dec}(\mathbf{y}) p(\mathbf{y}) \tag{2.7}$$

em que $p(\mathbf{y})$ denota a probabilidade de ter recebido $\mathbf{y}$ e $P_{dec}(\mathbf{y})$ denota a probabilidade da palavra enviada ter sido diferente de $\alpha(\mathbf{y})$ dado que $\mathbf{y}$ foi recebido.

Seguindo a notação adotada por Didier em [5], por $P_{err}(C; \mathtt{p})$, denotamos a probabilidade de ocorrer ambiguidade, isto é, de receber uma palavra $\mathbf{y}$ tal que, para tal, existem dois decodificadores $\alpha \neq \tilde{\alpha}$ de máxima verossimilhança tais que $\alpha(\mathbf{y}) \neq \tilde{\alpha}(\mathbf{y})$. Dizer que existem mais do que um decodificador de máxima verossimilhança significa dizer que, para algum $\mathbf{y} \in \mathcal{Y}^n$ existem ao menos duas palavras do código distintas $c_1, c_2 \in C$ tais que

$$p(\mathbf{y}|c_1) = p(\mathbf{y}|c_2) = \max\{p(\mathbf{y}|c); c \in C\}.$$

A expressão para $P_{err}(C; \mathtt{p})$ é dada por

$$P_{err}(C; \mathtt{p}) = \sum_{\mathbf{y} \in \mathcal{Y}^n} P_{err}(\mathbf{y}) p(\mathbf{y}) \tag{2.8}$$

em que $p(\mathbf{y})$ denota a probabilidade de ter recebido $\mathbf{y}$ e $P_{err}(\mathbf{y})$ denota a probabilidade de $\mathbf{y}$ ser uma palavra ambígua.

Quando não houver dúvidas sobre a probabilidade $\mathtt{p}$ do canal e o decodificador α que estão sendo considerados, simplificamos a notação escrevendo

$$P_{dec}(C; \mathtt{p}, \alpha) \quad = P_{dec}(C) = P_{dec}(C; \mathtt{p}) = P_{dec}(C, \alpha)$$

e

$$P_{err}(C; \mathtt{p}) \quad = P_{err}(C).$$

Muitas demonstrações e considerações não dependem da probabilidade ser de ambiguidade ou de erro de decodificação e, portanto, denotamos simplesmente por $P_*(C)$ em que $*$ pode simbolizar tanto err como dec.

Na teoria de códigos corretores de erro, um dos principais problemas é encontrar códigos que minimizem P_{dec} e P_{err}. Determinar $P_*(C)$ é uma tarefa, de um modo geral, intratável simplesmente pelo fato dessa probabilidade depender da distância mínima (ver [27]), pois envolve um número muito grande de operações. Por isso, na prática, usa-se limitantes inferiores e superiores. Na literatura, considerando o canal com apagamento, a atenção tem sido dedicada à probabilidade de ocorrer ambiguidade $P_{err}(C)$, também chamada, por vários autores, de probabilidade de não detectar erros, buscando limitantes para esta. Decidimos tratar de ambas, pois existem códigos distintos C_1 e C_2, tais que $P_{err}(C_1) = P_{err}(C_2)$ e $P_{dec}(C_1) < P_{dec}(C_2)$. Logo, convém escolher C_1 e P_{dec} se torna um invariante importante.

Consideramos apenas códigos sobre DMEC, a probabilidade do canal $\mathtt{p} < \frac{1}{2}$ e a probabilidade $p(c)$ de uma palavra $c \in C$ do código ser transmitida será constante igual a q^{-k}, isto é, todas as palavras têm probabilidades iguais de serem transmitidas.

Nosso objetivo é apresentar novos limitantes inferiores e superiores dependendo dos espectros generalizados com suportes na hierarquia de pesos, relacionar $P_{dec}(C)$ e $P_{err}(C)$, calcular expressões exatas para $P_{dec}(C)$ e $P_{err}(C)$ quando C é um $[n,k]_q$-código cuja hierarquia de peso seja um subconjunto de $[\![n-k,n]\!]$ e apresentar critérios de comparação entre códigos em relação a probabilidade de erro quando a probabilidade de erro do canal seja suficientemente pequena. Consequentemente provamos que, fixados comprimento e dimensão em que não existem códigos MDS, mas existem códigos AMDS, os códigos AMDS com maior d_2 são os melhores, generalizando o que foi feito por Fashandi et al. em [11].

Capítulo 3

Probabilidades de erro em termos das partes de $[\![n]\!]$

Lembramos que a partir de agora estaremos trabalhando somente com canais discretos, sem memória e com apagamento. Neste capítulo apresentamos vários conceitos e notações diferentes das encontradas na literatura. O motivo de adotar notações diferentes é que várias notações distintas para os mesmos conceitos são usadas nos trabalhos de pesquisas atuais [1], [5], [8], [9], [11], [29]. Além disso a notação adotada nesta tese facilita e simplifica as demonstrações de resultados que envolvem simultaneamente a probabilidade de erro de decodificação e de ocorrência de ambiguidade (ver Teorema 3.3.1).

O principal resultado desse capítulo é o Teorema 3.3.1 que apresenta uma fórmula explícita para a probabilidade de erro de decodificação e de ocorrência de ambiguidade de um código. Em [11] e [5], encontramos formulações muito próximas e o Teorema 3.3.1 pode ser facilmente deduzido a partir destes resultados. Não obstante, apenas com o intuito de tornar a leitura desta tese mais auto-contida, e para introduzir uma série de notações e conceitos que serão utilizados adiante, optamos por considerar uma demonstração que não depende de resultados estabelecidos na literatura.

Na Secão 3.1 formalizamos e caracterizamos o conceitos de apagamento e conjunto de apagamentos de um código. Na Seção 3.2 estudamos as ambiguidades, apresentamos várias caracterizações para o conjunto de ambiguidades e mostramos como estas se relacionam com $P_*(C)$ de um $[n,k]_q$-código C. Na Seção 3.3 demonstramos o principal resultado deste capítulo, o Teorema 3.3.1. Ainda nesta seção os Exemplos 3.3.3 e 3.3.4 ilustram aplicações do Teorema 3.3.1.

3.1 Conjunto de apagamentos

Dado $H \subseteq [\![n]\!]$, denotamos por $\bar{H} = [\![n]\!] - H$ o complemento de H em $[\![n]\!]$.

Dados X_i, $i \in [\![n]\!]$, conjuntos arbitrários, denotamos por

$$\mathbf{x} = (x_1, x_2, ..., x_n)$$

um elemento do produto cartesiano $\prod_{i\in[\![n]\!]} X_i$, com $x_i \in X_i$ e por $\mathbf{x}^H$ o elemento de $\prod_{i\in H} X_i$ obtido pela omissão das coordenadas de $\mathbf{x}$ de índices em $\bar{H}$. A projeção

$$\begin{array}{ccc} \prod_{i\in[\![n]\!]} X_i & \longrightarrow & \prod_{i\in H} X_i \\ \mathbf{x} & \longmapsto & \mathbf{x}^H. \end{array}$$

será denotada por π_H.

Em particular, tomando $X_i = \mathbb{F}_q$, para todo $i \in [\![n]\!]$, temos que $\mathbb{F}_q^n = \prod_{i=1}^n X_i$ é um espaço vetorial sobre $\mathbb{F}_q$ e π_H é uma transformação linear. Logo, a imagem $\pi_H(\mathbb{F}_q^n)$ e o núcleo $\ker(\pi_H) = \pi_H^{-1}(\{0\})$ de π_H são subspaços vetoriais sobre $\mathbb{F}_q$.

Vamos agora assumir que $X_i = \mathcal{X} \cup \{\epsilon\} = \mathcal{Y}$ para todo $i \in [\![n]\!]$ e considerar as projeções $\pi_H : \mathcal{Y}^n \longrightarrow \prod_{i\in H} \mathcal{Y}$.

Denotamos por $\mathcal{E}_H(\mathbf{x})$ a palavra de $\mathcal{Y}^n$ satisfazendo as seguintes condições:

1. $\pi_{\{i\}}(\mathcal{E}_H(\mathbf{x})) = \epsilon$, para todo $i \in H$;
2. $\pi_{\{i\}}(\mathcal{E}_H(\mathbf{x})) = x_i$, para todo $i \in \bar{H}$.

A aplicação $\mathbf{x} \longmapsto \mathcal{E}_H(\mathbf{x})$ será denotada por $\mathcal{E}_H$.

O *suporte apagado* de uma palavra $\mathbf{y} \in \mathcal{Y}^n$, denotado por $supp_{\mathcal{E}}(\mathbf{y})$, é o conjunto dos índices de todas as coordenadas apagadas de $\mathbf{y}$, i.e.,

$$supp_{\mathcal{E}}(\mathbf{y}) = \{i \in [\![n]\!]; \pi_{\{i\}}(\mathbf{y}) = \epsilon\}.$$

O *conjunto de apagamentos de* um $[n,k]_q$-código C, denotado por E_C, é o conjunto de todos elementos $\mathbf{y} \in \mathcal{Y}^n$ tais que a probabilidade $p(\mathbf{y}|c)$ de receber $\mathbf{y}$, dado que $c \in C$ foi transmitido, é não nula para algum $c \in C$, isto é,

$$E_C = \{\mathbf{y} \in \mathcal{Y}^n; \exists c \in C \text{ com } p(\mathbf{y}|c) \neq 0\}.$$

A seguir apresentamos outras caracterizações do conjunto de apagamentos de C

Proposição 3.1.1 *Seja E_C o conjunto de apagamentos de um $[n,k]_q$-código C. Então*

$$E_C = \{\mathbf{y} \in \mathcal{Y}^n; \exists c \in C \text{ com } c^{[\![n]\!]\setminus supp_{\mathcal{E}}(\mathbf{y})} = \mathbf{y}^{[\![n]\!]\setminus supp_{\mathcal{E}}(\mathbf{y})}\}.$$

Demonstração
Se $\mathbf{y} \in E_C$, então $p(\mathbf{y}|c) \neq 0$ para algum $c \in C$. Vamos provar que

$$c^{[\![n]\!]\setminus supp_{\mathcal{E}}(\mathbf{y})} = \mathbf{y}^{[\![n]\!]\setminus supp_{\mathcal{E}}(\mathbf{y})}. \tag{3.1}$$

Escrevendo $\mathbf{y} = (y_1, \ldots, y_n)$ e $c = (c_1, \ldots, c_n)$ pela Equação (2.1) temos que

$$p(\mathbf{y}|c) = \prod_{i=1}^{n} p(y_i|c_i) \neq 0,$$

logo $p(y_i|c_i) \neq 0$ para todo $i \in [\![n]\!]$. Como estamos num canal com apagamento, então $p(y_i|c_i) = p$, se $y_i = \epsilon$, e $p(y_i|c_i) = 1 - \mathtt{p}$, se $y_i = c_i$. Logo $y_i = c_i$ para todo $i \in [\![n]\!] \setminus supp_{\mathcal{E}}(\mathbf{y})$, daí vale (3.1).

Por outro lado, se $\mathbf{y} \in \mathcal{Y}^n$ e existe $c \in C$ satisfazendo (3.1), então, para todo $i \in [\![n]\!] \setminus supp_{\mathcal{E}}(\mathbf{y})$, temos que $c_i = y_i$ e, portanto, $p(y_i|c_i) = 1 - \mathtt{p}$. Se $i \in supp_{\mathcal{E}}(\mathbf{y})$, então $y_i = \epsilon$. Logo, novamente pela Equação (2.1), fazendo $H = supp_{\mathcal{E}}(\mathbf{y})$ temos que

$$p(\mathbf{y}|c) = \prod_{i\in H} p(y_i|c_i) \prod_{i\in \bar{H}} p(y_i|c_i) = \mathtt{p}^{|H|}(1-\mathtt{p})^{|\bar{H}|} \neq 0$$

e temos que $\mathbf{y} \in E_C$. □

Proposição 3.1.2 *Seja E_C o conjunto de apagamentos de um $[n,k]_q$-código C. Então*

$$E_C = \{\mathcal{E}_H(c); c \in C \text{ e } H \subseteq [n]\} = \bigcup_{H\subseteq[n]} \mathcal{E}_H(C). \tag{3.2}$$

Demonstração
É claro que

$$\bigcup_{H\subseteq[\![n]\!]} \mathcal{E}_H(C) \subseteq E_C.$$

Seja agora $\mathbf{y} \in E_C$ e $H = supp_{\mathcal{E}}(\mathbf{y})$. Pela Proposição 3.1.1, existe $c \in C$ tal que $c^{\bar{H}} = \mathbf{y}^{\bar{H}}$. Como $\pi_{\{i\}}(\mathcal{E}_H(c)) = c_i$ para todo $i \in \bar{H}$, então $y_i = \pi_{\{i\}}(\mathcal{E}_H(c))$, para todo $i \in \bar{H}$. Como $H = supp_{\mathcal{E}}(\mathbf{y})$, segue que

$$y_i = \epsilon = \pi_{\{i\}}(\mathcal{E}_H(c)), \text{ para todo } i \in H.$$

e temos que $\mathbf{y} = \mathcal{E}_H(c)$. □

3.2 Conjunto de ambiguidades

Seja $H = supp_{\mathcal{E}}(\mathbf{y})$ o suporte apagado de $\mathbf{y} \in \mathcal{Y}^n$ e seja $[\mathbf{y}]_H$ o conjunto de todas as possíveis palavras de C que poderiam ter sido enviadas dado que $\mathbf{y}$ foi recebido, isto é,

$$[\mathbf{y}]_H = \{c \in C; p(\mathbf{y}|c) \neq 0\}.$$

O conjunto $[\mathbf{y}]_H$ é chamado de *conjunto de ambiguidades* de $\mathbf{y}$. Como é feito em detalhes no Corolário 3.2.4 a existência de ambiguidades, no sentido definido na Seção 2.6 equivale a termos $|[\mathbf{y}]_H| > 1$. De fato, as possíveis decisões de um decodificador por máxima verossimilhaçã para uma palavra com apagamentos nas coordenadas $supp(\mathbf{y}) = H$ são as palavras de $[\mathbf{y}]_H$.

Vamos apresentar agora uma definição equivalente para o conjunto de ambiguidades.

Proposição 3.2.1 *Seja $\mathbf{y} \in \mathcal{Y}^n$, $H = supp_{\mathcal{E}}(\mathbf{y})$ e C um $[n,k]_q$-código linear. Então*

$$[\mathbf{y}]_H = \{c \in C; c^{\bar{H}} = \mathbf{y}^{\bar{H}}\}.$$

Demonstração
Se $c \in [\mathbf{y}]_H$, então $p(\mathbf{y}|c) \neq 0$. Logo, pela Equação (2.1) e relembrando que estamos em um DMEC, $y_i = c_i$, se $i \in \bar{H}$, e $y_i = \epsilon$, se $i \in \bar{H}$. Portanto $\mathbf{y}^{\bar{H}} = c^{\bar{H}}$.

Por outro lado, se $c \in C$ é tal que $c^{\bar{H}} = \mathbf{y}^{\bar{H}}$, então $p(y_i|c_i) = 1 - \mathtt{p}$, para todo $i \in \bar{H}$, e $p(y_i|c_i) = p(\epsilon|c_i) = \mathtt{p}$, para todo $i \in H$. Logo $p(\mathbf{y}|c) \neq 0$ e segue que $c \in [\mathbf{y}]_H$. □

Exemplo 3.2.2 *Seja $C = \langle (1,0,0), (0,1,1) \rangle$ um $[3,2]_2$-código linear. Sejam $\mathbf{y_1} = (\epsilon, 0, 0)$, $\mathbf{y_2} = (1, \epsilon, 0)$, $\mathbf{y_3} = (\epsilon, \epsilon, \epsilon)$ e $\mathbf{y_4} = (0,1,0)$ palavras de $\mathbb{F}_2^3 \cup \{\epsilon\}$ e $H_i = supp_{\mathcal{E}}(\mathbf{y_i})$, $i \in [\![4]\!]$. Então*

(1) $[\mathbf{y_1}]_{H_1} = \{(0,0,0), (1,0,0)\}$;

(2) $[\mathbf{y_2}]_{H_2} = \{(1,0,0)\}$;

(3) $[\mathbf{y_3}]_{H_3} = C$;

(4) $[\mathbf{y_4}]_{H_4} = \varnothing$.

Quando $|[\mathbf{y}]_H| > 1$ dizemos que y é uma *palavra ambígua* ou $\mathbf{y}$ é uma *ambiguidade*. Apenas ambiguidades causam algum problema no que se refere a decodificação. O Lema 3.2.3 será necessário para a demonstração do Teorema 3.3.1 e do Corolário 3.2.4.

Lema 3.2.3 *Sejam* $\mathbf{y} \in E_C$ *com* $supp_{\mathcal{E}}(\mathbf{y}) = H$ *e* C *um* $[n,k]_q$*-código linear. Então*

(i) $p(\mathbf{y}|c) = \mathtt{p}^{|H|}(1-\mathtt{p})^{|\bar{H}|}$*, para todo* $c \in [\mathbf{y}]_H$*;*

(ii) $p(\mathbf{y}|c) = 0$*, para todo* $c \in C \setminus [\mathbf{y}]_H$*.*

Demonstração
Primeiro demonstramos o item (i). Se $c \in [\mathbf{y}]_H$, então $c^{\bar{H}} = \mathbf{y}^{\bar{H}}$. Escrevendo $c = (c_1, \ldots, c_n)$ e $\mathbf{y} = (y_1, \ldots, y_n)$, temos que $c_i = y_i$, para todo $i \in \bar{H}$. Como $H = supp_{\mathcal{E}}(\mathbf{y})$, segue que $y_i = \epsilon$, para todo $i \in H$. Daí, pela Equação (2.1), temos que

$$p(\mathbf{y}|c) = \prod_{i \in H} p(y_i|c_i) \prod_{i \in \bar{H}} p(y_i|c_i) = \mathtt{p}^{|H|}(1-\mathtt{p})^{|\bar{H}|}.$$

A demonstração do item (ii) é trivial, basta observar que, se $c \in C \setminus [\mathbf{y}]_H$, então $p(\mathbf{y}|c) = 0$ pela própria definição de $[\mathbf{y}]_H$. □

O Lema 3.2.3 diz que, dado $\mathbf{y} \in \mathcal{Y}^n$, a probabilidade $p(\mathbf{y}|c)$ de receber $\mathbf{y}$ dado que $c \in C$ foi enviado depende somente de c pertencer ou não a $[\mathbf{y}]_H$ e de H, isto é, não depende de $\mathbf{y}^{\bar{H}}$.

Corolário 3.2.4 *Sejam* C *um* $[n,k]_q$*-código,* $\mathbf{y} \in \mathcal{Y}^n$ *e* $H = supp_{\mathcal{E}}(\mathbf{y})$*. A palavra* $\mathbf{y}$ *é uma ambiguidade se, e somente se, existem dois decodificadores por máxima verossimilhança* α_1 *e* α_2 *tais que* $\alpha_1(\mathbf{y}) \neq \alpha_2(\mathbf{y})$*.*

Demonstração
Se $\mathbf{y} \in \mathcal{Y}^n$ é uma ambiguidade, então $|[\mathbf{y}]_H| > 1$, logo existem $c^1 \neq c^2 \in C$ tais que

$$\pi_{\bar{H}}(c^1) = \pi_{\bar{H}}(c^2) = \pi_{\bar{H}}(\mathbf{y}).$$

Pelo Lema 3.2.3, temos que $p(\mathbf{y}|c) = 0$ ou $p(\mathbf{y}|c) = \mathtt{p}^{|H|}(1-\mathtt{p})^{|\bar{H}|}$. Logo $p(\mathbf{y}|c) \leq p(\mathbf{y}|c^1) = p(\mathbf{y}|c^2)$ e segue que c^1 e c^2 são imagens de $\mathbf{y}$ via decodificadores de máxima verossimilhança. Como $c^1 \neq c^2$, então existem pelo menos dois decodificadores MLD distintos α_1 e α_2 tais que $\alpha_1(\mathbf{y}) = c^1 \neq \alpha_2(\mathbf{y}) = c^2$.

Por outro lado, se α_1 e α_2 são MLD com $\alpha_1(\mathbf{y}) \neq \alpha_2(\mathbf{y})$ para algum $\mathbf{y} \in \mathcal{Y}^n$, então

$$p(\alpha_1(\mathbf{y})|\mathbf{y}) \geq p(c|\mathbf{y}) \text{ e } p(\alpha_2(\mathbf{y})|\mathbf{y}) \geq p(c|\mathbf{y}).$$

Fazendo $c = \alpha_2(\mathbf{y})$ na primeira desigualdade e $c = \alpha_1(\mathbf{y})$ na segunda desigualdade, temos que $p(\alpha_1(\mathbf{y})|\mathbf{y}) = p(\alpha_2(\mathbf{y})|\mathbf{y}) = \lambda$. Pelo Lema 3.2.3, $\lambda = \mathtt{p}^{|H|}(1-\mathtt{p})^{|\bar{H}|}$ ou $\lambda = 0$. Como $\mathbf{y} \in E_C$, existe $c \in C$ tal que $p(\mathbf{y}|c) \neq 0$. Logo $\lambda \neq 0$, pois caso contrário $p(\alpha_1(\mathbf{y})|\mathbf{y}) = p(\alpha_2(\mathbf{y})|\mathbf{y}) \leq p(\mathbf{y}|c)$, contradizendo o fato de α_1 e α_2 serem MLD. Logo $\lambda \neq 0$ e, daí, $\alpha_1(\mathbf{y}) \neq \alpha_2(\mathbf{y}) \in [\mathbf{y}]_H$. Segue que $|[\mathbf{y}]_H| > 1$, isto é, $\mathbf{y}$ é uma ambiguidade. □

Observa-se no Exemplo 3.2.2 que dados $\mathbf{y} \in \mathcal{Y}^n$, $H = supp_{\mathcal{E}}(y)$ e um $[n,k]_q$-código C, então:

- $[\mathbf{y}]_H$ pode conter mais de um elemento e ser distinto de C (Item (1));
- $[\mathbf{y}]_H$ pode conter apenas um único elemento (Item (2));
- $[\mathbf{y}]_H$ pode ser todo o código C (Item (3));
- $[\mathbf{y}]_H$ pode ser vazio (Item (4));
- $[\mathbf{y}]_H$ pode ser ou não um espaço vetorial não trivial.

A seguir é caracterizado cada uma destas situações acima descritas de forma mais geral.

Observe que $supp_{\mathcal{E}}(\mathcal{E}_H(c)) = H$ para todo $c \in C$ e todo $H \subseteq [\![n]\!]$. Logo, simplesmente denotamos $[c]_H \coloneqq [\mathcal{E}_H(c)]_H$.

Corolário 3.2.5 *Sejam C um $[n,k]_q$-código, $\mathbf{y} \in \mathcal{Y}^n$ e $H = supp_{\mathcal{E}}(\mathbf{y})$. O conjunto de ambiguidades $[\mathbf{y}]_H$ é não vazio se, e somente se, $\mathbf{y} \in E_C$.*

Demonstração
Se $[\mathbf{y}]_H \neq \varnothing$, então existe $c \in [\mathbf{y}]_H$. Pelo Lema 3.2.3 $p(\mathbf{y}|c) \neq 0$ e temos que $\mathbf{y} \in E_C$.

Por outro lado, se $\mathbf{y} \in E_C$, então $p(\mathbf{y}|c) \neq 0$ para algum $c \in C$ e, pelo Lema 3.2.3, segue que $c \in [\mathbf{y}]_H$. □

O conjunto de ambiguidades $[0]_H$ de $\mathcal{E}_H(0) \in \mathcal{Y}^n$, com $H \subseteq [\![n]\!]$ é qualquer, tem grande importância para nossos objetivos. Vamos agora descrever e estudar melhor esse conjunto.

Proposição 3.2.6 *Seja $H \subseteq [\![n]\!]$ e C um $[n,k]_q$-código. Então $[0]_H = \ker(\pi_{\bar{H}})$ é um subcódigo de C, considerando uma restrição no domínio de $\pi_{\bar{H}}$ ao conjunto $C \subseteq \mathbb{F}_q^n$.*

Demonstração
Note que $c \in [0]_H$ se, e somente se, $c^{\bar{H}} = 0^{\bar{H}}$, isto é, $\pi_{\bar{H}}(c) = \pi_{\bar{H}}(0) = 0$, pois $\pi_{\bar{H}}$ é uma transformação linear. □

Corolário 3.2.7 *Sejam $H \subseteq [\![n]\!]$ e C um $[n,k]_q$-código linear. Então*

$$|[c]_H| = |[0]_H|, \text{ para todo } c \in C.$$

Conseguentemente, se $y \in E_C$, então $|[y]_H| = |[0]_H|$.

Demonstração
Sejam $\mathbf{y} \in E_C$ com $H = supp_{\mathcal{E}}(\mathbf{y})$, então $[\mathbf{y}]_H \neq \varnothing$. Dado $c_0 \in [\mathbf{y}]_H$, definimos ϕ por

$$\begin{array}{rccc} \phi: & [\mathbf{y}]_H & \longrightarrow & [0]_H \\ & c & \longmapsto & c + (q-1)c_0. \end{array}$$

Note que

$$(c + (q-1)c_0)^{\bar{H}} = c^{\bar{H}} + (q-1)c_0^{\bar{H}} = c_0^{\bar{H}} + (q-1)c_0^{\bar{H}} = 0^{\bar{H}},$$

portanto ϕ está bem definida. Se $\phi(c_1) = \phi(c_2)$, então $c_1 + (q-1)c_0 = c_2 + (q-1)c_0$, logo $c_1 = c_2$, isto é, ϕ é injetora. Seja $c \in [0]_H$, isto é, $c^{\bar{H}} = 0^{\bar{H}}$. Temos que $c_0 + c \in [0]_H$, pois

$$(c_0 + c)^{\bar{H}} = c_0^{\bar{H}} + 0^{\bar{H}} = c_0^{\bar{H}}.$$

Daí,

$$\phi(c + c_0) = c_0 + c + (q-1)c_0 = qc_0 + c = c,$$

portanto ϕ é sobrejetora. Segue então que ϕ é bijetora e $|[y]_H| = |[0]_H|$. □

Podemos agora encontrar uma expressão para a probabilidade $p(\mathbf{y})$ de receber uma palavra $\mathbf{y} \in \mathcal{Y}^n$. Seja $H = supp_{\mathcal{E}}(\mathbf{y})$, então

$$p(\mathbf{y}) = \sum_{c \in [\mathbf{y}]_H} p(\mathbf{y}|c)p(c) + \sum_{c \in C \setminus [\mathbf{y}]_H} p(\mathbf{y}|c)p(c).$$

Pelo Lema 3.2.3, lembrando que estamos considerando $p(c) = q^{-k}$ constante, temos

$$p(\mathbf{y}) = \sum_{c \in [\mathbf{y}]_H} \mathtt{p}^{|H|}(1-\mathtt{p})^{|\bar{H}|}q^{-k},$$

e, pelo Corolário 3.2.7, como $|[\mathbf{y}]_H| = |[0]_H|$, segue que

$$p(\mathbf{y}) = |[0]_H| q^{-k} \mathtt{p}^{|H|} (1-\mathtt{p})^{|H|}. \tag{3.3}$$

Sejam C um $[n,k]_q$-código, E_C o conjunto de apagamentos de C e $H \subseteq [\![n]\!]$. Denotamos por E_H o conjunto de palavras de E_C cujo suporte apagado seja exatamente o conjunto H, isto é,

$$E_H = \{\mathbf{y} \in E_C; supp_{\mathcal{E}}(\mathbf{y}) = H\}.$$

Lema 3.2.8 *Sejam $H \subseteq [\![n]\!]$ e C um $[n,k]_q$-código. Então*

$$|[0]_H||E_H| = q^k.$$

Demonstração
Dados $H \subseteq [\![n]\!]$ e $\mathbf{x}, \mathbf{y} \in E_H$, pelo Coroloário 3.2.7, temos que $|[x]_H| = |[\mathbf{y}]_H|$ e, se $\mathbf{x} \neq \mathbf{y}$, então

$$[\mathbf{x}]_H \cap [\mathbf{y}]_H = \varnothing.$$

Daí, se $c \in C$, então $\mathcal{E}_H(c) \in E_H$, segue que $c \in [c]_H \subseteq \bigcup_{\mathbf{y} \in E_H} [\mathbf{y}]_H$. Daí

$$C = \bigcup_{\mathbf{y} \in E_H} [\mathbf{y}]_H$$

em que a união é disjunta e, portanto,

$$q^k = |C| = \sum_{\mathbf{y} \in E_H} |[\mathbf{y}]_H| = \sum_{\mathbf{y} \in E_H} |[0]_H| = |E_H||[0]_H|.$$

□

Os conjuntos de ambiguidades se relacionam com as probabilidades de erro de decodificação e de ocorrência de ambiguidade do canal. Segue imediatamente das definições de P_{dec} e P_{amb} que: se $\mathbf{y} \in E_C$ é tal que $supp_{\mathcal{E}}(\mathbf{y}) = H$, então

$$P_{dec}(\mathbf{y}) = 1 - \frac{1}{|[0]_H|}. \tag{3.4}$$

A expressão (3.4) é consequência das seguintes igualdades:

$$P_{dec}(\mathbf{y}) = 1 - p(\alpha(\mathbf{y})|\mathbf{y}) = 1 - \frac{p(\mathbf{y}|\alpha(\mathbf{y}))p(\alpha(\mathbf{y}))}{p(\mathbf{y})} =$$

$$1 - \frac{\mathtt{p}^{|H|}(1-\mathtt{p})^{|\bar{H}|}q^{-k}}{|[0]_H|q^{-k}\mathtt{p}^{|H|}(1-\mathtt{p})^{|\bar{H}|}} = 1 - \frac{1}{|[0]_H|}.$$

Observa-se, também, que

$$P_{err}(\mathbf{y}) = \left\lceil 1 - \frac{1}{|[0]_H|} \right\rceil, \tag{3.5}$$

em que $\lceil l \rceil$ denota o menor inteiro maior ou igual a l, no caso, $P_{err}(\mathbf{y}) = 0$, quando $\mathbf{y}$ não for ambiguidade, e $P_{err}(\mathbf{y}) = 1$, quando $\mathbf{y}$ for uma ambiguidade.

3.3 Expressão exata para as probabilidades de erro

Apresentamos uma demonstração simples de como determinar às expressões para P_* encontradas por Didier em [5] e por Fashandi et al em [11] (Teorema 3.3.1). Vemos que a notação adotada permite trabalhar P_{dec} e P_{err} simultaneamente.

Observe que $P_*(\mathbf{y})$ depende somente do conjunto $H = supp_{\mathcal{E}}(\mathbf{y})$, logo denotamos $P_*(H) = P_*(\mathbf{y})$.

Pelo Corolário 3.2.5 temos que $p(\mathbf{y}) = 0$ para todo $\mathbf{y} \in \mathcal{Y}^n \setminus E_C$. Particionando $\mathcal{Y}^n = E_C \cup (\mathcal{Y}^n \backslash E_C)$, obtemos que

$$P_*(C) = \sum_{\mathbf{y} \in E_C} P_*(\mathbf{y}) p(\mathbf{y}). \tag{3.6}$$

Teorema 3.3.1 *Seja C um $[n,k]_q$-código. Então*

$$P_*(C) = \sum_{H \subseteq [\![n]\!]} P_*(H) \mathtt{p}^{|H|}(1-\mathtt{p})^{|\bar{H}|}. \tag{3.7}$$

Demonstração
A seguinte sequência de identidades é válida

$$\begin{aligned}
P_*(C) &\overset{(1)}{=} \sum_{\mathbf{y} \in \mathcal{Y}^n} P_*(y) p(\mathbf{y}) \\
&\overset{(2)}{=} \sum_{\mathbf{y} \in E_C} P_*(H) q^{-k} |[0]_H| p^{|H|} (1-p)^{\bar{H}} \\
&\overset{(3)}{=} \sum_{H \subseteq [\![n]\!]} P_*(H) |E_H| q^{-k} |[0]_H| p^{|H|} (1-p)^{\bar{H}} \\
&\overset{(4)}{=} \sum_{H \subseteq [\![n]\!]} P_*(H) p^{|H|} (1-p)^{\bar{H}}.
\end{aligned}$$

A identidade (1) segue das expressões (2.7) e (2.8). Pelas expressões (3.4) e (3.5), $P_*(\mathbf{y})$ depende apenas de $H(y) = H = supp_{\mathcal{E}}(\mathbf{y})$, isto é $P_*(\mathbf{y}) = P_*(H)$, logo a identidade (2) segue de (3.3), (3.4), (3.5) e (3.6). Somando em $H \subseteq [\![n]\!]$, devemos multiplicar cada parcela do somatório por $|E_H|$, obtendo a identidade (3). Por fim, a identidade (4) segue do Lema 3.2.8. □

Observação 3.3.2 *No Capítulo 4 explicamos em detalhes como as expressões para P_* no Teorema 3.3.1 se relacionam com aquelas apresentadas por Fashandi et al e Didier.*

O trabalho para encontrar limitantes mais refinados reside na obtenção de limitantes para $P_*(H)$ que imediatamente acarretam limitantes para $P_*(C)$.

Exemplo 3.3.3 *Seja $C_1 = \langle (1,1,0),(0,1,1)\rangle$ um $[3,2]_2$-código. Vamos considerar todas as possibilidades para $H \subseteq [\![3]\!]$ e determinar, na tabela a seguir, os valores de $P_{dec}(H)$ e $P_{err}(H)$.*

H	$[0]_H$	$P_{dec}(H)$	$P_{err}(H)$
$\varnothing$	$\{(0,0,0)\}$	*0*	*0*
$\{1\}$	$\{(0,0,0)\}$	*0*	*0*
$\{2\}$	$\{(0,0,0)\}$	*0*	*0*
$\{3\}$	$\{(0,0,0)\}$	*0*	*0*
$\{1,2\}$	$\{(0,0,0),(1,1,0)\}$	$\frac{1}{2}$	*1*
$\{1,3\}$	$\{(0,0,0),(1,0,1)\}$	$\frac{1}{2}$	*1*
$\{2,3\}$	$\{(0,0,0),(0,1,1)\}$	$\frac{1}{2}$	*1*
$\{1,2,3\}$	C_1	$\frac{2}{3}$	*1*

Logo,

$$P_{dec}(C_1) = \frac{3}{2}\mathtt{p}^2(1-\mathtt{p}) + \frac{2}{3}\mathtt{p}^3$$

e

$$P_{err}(C_1) = 3\mathtt{p}^2(1-\mathtt{p}) + \mathtt{p}^3.$$

Exemplo 3.3.4 *Seja $C_2 = \langle (1,0,0),(0,1,1)\rangle$ um $[3,2]_2$-código. Dado $H \subseteq [\![3]\!]$, então*

H	$[0]_H$	$P_{dec}(H)$	$P_{err}(H)$
$\varnothing$	$\{(0,0,0)\}$	*0*	*0*
$\{1\}$	$\{(0,0,0),(1,0,0)\}$	$\frac{1}{2}$	*1*
$\{2\}$	$\{(0,0,0)\}$	*0*	*0*
$\{3\}$	$\{(0,0,0)\}$	*0*	*0*
$\{1,2\}$	$\{(0,0,0),(1,0,0)\}$	$\frac{1}{2}$	*1*
$\{1,3\}$	$\{(0,0,0),(1,0,0)\}$	$\frac{1}{2}$	*1*
$\{2,3\}$	$\{(0,0,0),(0,1,1)\}$	$\frac{1}{2}$	*1*
$\{1,2,3\}$	C_2	$\frac{2}{3}$	*1*

Logo,

$$P_{dec}(C_1) = \frac{1}{2}\mathtt{p}(1-\mathtt{p})^2 + \frac{3}{2}\mathtt{p}^2(1-\mathtt{p}) + \frac{2}{3}\mathtt{p}^3$$

e

$$P_{err}(C_1) = \mathtt{p}(1-\mathtt{p})^2 + 3\mathtt{p}^2(1-\mathtt{p}) + \mathtt{p}^3.$$

Note, nos dois exemplos anteriores, que $P_*(C_2) > P_*(C_1)$ e, portanto, C_1 é um código melhor que C_2 em relação a quantidade de erros de decodificação e de ocorrênci de ambiguidades.

Nos próximos capítulos apresentamos métodos relativamente simples, se comparados à aplicação direta do Teorema 3.3.1, para se comparar dois $[n,k]_q$-códigos C_1 e C_2, restritos a certas condições, em relação às probabilidades de erro e de ocorrência de ambiguidades. Primeiramente estudamos limitantes inferiores e superiores para P_*.

Capítulo 4

Limitantes para P_* em DMEC

Dados $r \in [\![0, n]\!]$ e um $[n, k]_q$-código C, denotamos $Q_{dec,r}(C)$ e $Q_{err,r}(C)$ por

$$Q_{dec,r}(C) = \sum_{\{H \subseteq [n]; |H|=r\}} \left(1 - \frac{1}{|[0]_H|}\right). \tag{4.1}$$

$$Q_{err,r}(C) = \sum_{\{H \subseteq [n]; |H|=r\}} \left\lceil 1 - \frac{1}{|[0]_H|} \right\rceil. \tag{4.2}$$

Da mesma maneira como feito antes, usamos a notação $Q_{*,r}(C)$ quando as afirmações não dependerem de considerar $Q_{dec,r}(C)$ ou $Q_{err,r}(C)$. Pelo Teorema 3.3.1 e pelas notações (4.1) e (4.2) segue que

$$P_*(C) = \sum_{r=0}^{n} Q_{*,r}(C) \mathtt{p}^r (1 - \mathtt{p})^{n-r}. \tag{4.3}$$

Quando não houver dúvidas a respeito de qual código estamos trabalhando, abusamos da notação denotando simplesmente

$$Q_{*,r}(C) = Q_{*,r}$$

para todo $r \in [\![0, n]\!]$.

As expressões (3.7) e (4.3) são conhecidas por diversos outros autores, porém com notações diferentes.

As expressões para P_{dec} encontradas por Fashandi et al em [11], denotada em seu artigo por $P^{\mathcal{C}}_{E,ML}$, é identica a expressão (3.7) fazendo

$$\mathbb{P}(e) = \mathtt{p}^{w(e)} (1 - \mathtt{p})^{n - w(e)}$$

e

$$\mathbb{P}\{e|error\} = P_{dec}(supp(e)),$$

em que $e \in \mathbb{F}_2^n$.

Em [5] a fórmula para $P_{err}(C)$, denotada por $P_{err}(\mathtt{p})$, é a mesma expressão (4.3) fazendo

$$\binom{n}{e} P_{err}(e) = Q_{err,e}$$

em que $e \in \mathbb{F}_2^n$.

Denotamos por $Q_{FAS,r}^{inf}$ o limitante inferior dado em [11] para $Q_{dec,r}$ e por $Q_{DID,r}^{sup}$ o limitante superior dado em [5] pra $Q_{err,r}$, $r \in [\![0, n]\!]$. Isto é

$$Q_{FAS,r}^{inf} = \binom{n}{r}\left(1 - \frac{1}{q^{k-n+r}}\right) \tag{4.4}$$

e

$$Q_{DID,r}^{sup} = \binom{n}{r} \prod_{i=r+1}^{n} \left(\frac{i-d_1}{i}\right) \prod_{i=2}^{k} \left(\frac{d_i}{d_i - d_1}\right). \tag{4.5}$$

Os limitantes para as probabilidades de erro e de ocorrência de ambiguidade decorrentes destas estimativas serão denotados respectivamente por

$$P_{FAS}^{inf}(C) = \sum_{r=d_1}^{n} Q_{FAS,r}^{inf} \mathtt{p}^r (1-\mathtt{p})^{n-r} \tag{4.6}$$

e

$$P_{DID}^{sup}(C) = \sum_{r=d_1}^{n} Q_{DID,r}^{sup} \mathtt{p}^r (1-\mathtt{p})^{n-r}. \tag{4.7}$$

O índice inferior nos somatórios das expressões (4.6) e (4.7) é a distância mínima d_1. Isto se deve ao fato de que $Q_{*,r} = 0$ sempre que $r < d_1$ (Lema 4.2.1).

Note que $P_{DID}^{sup}(C)$ depende apenas de n, k e d_i, $i \in [\![k]\!]$. O Exemplo 4.0.5 a seguir mostra que esses parâmetros não são suficientes para determinar a probabilidade de ocorrer ambiguidade em um código:

Exemplo 4.0.5 *Sejam*

$$\begin{aligned} C_1 &= \langle (1,1,0,0), (0,0,1,1) \rangle; \\ C_2 &= \langle (1,1,0,0), (0,1,1,1) \rangle \end{aligned}$$

dois $[4,2]_2$*-códigos. Temos que*

$$d_1(C_1) = d_1(C_2) = 2;$$
$$d_2(C_1) = d_2(C_2) = 4.$$

Isto é, ambas hierarquias de peso são idênticas, logo $P^{sup}_{DID}(C_1) = P^{sup}_{DID}(C_2)$. *No entanto*

$$P_{err}(C_1) = \quad 2\mathtt{p}^2(1-\mathtt{p})^2 + 4\mathtt{p}^3(1-\mathtt{p}) + \mathtt{p}^4;$$
$$P_{err}(C_2) = \quad \mathtt{p}^2(1-\mathtt{p})^2 + 4\mathtt{p}^3(1-\mathtt{p}) + \mathtt{p}^4.$$

Observamos no Exemplo 4.0.5 que os limitantes superiores em [5] podem ser melhorados, uma vez que os parâmetros dos códigos que aparecem na expressão (4.5) não são suficientes para diferenciar códigos com mesmos parâmetros n, k e d_i, $i \in [\![k]\!]$.

O objetivo desse capítulo é melhorar os limitantes $P^{inf}_{FAS}(C)$ e $P^{sup}_{DID}(C)$ e apresentar também limitantes inferiores para $Q_{err,r}$ e limitantes superiores para $Q_{dec,r}$, quando $r = d_i$, $i \in [\![k]\!]$. Para isso utilizamos os espectros generalizados dos códigos e, em alguns casos, determinamos parcelas exatas para as expressões em (4.1) e (4.2).

Na Seção 4.1 estudamos a cardinalidade do conjunto $[0]_H$ em casos específicos. Na Seção 4.2 apresentamos os novos limitantes. Também, na Seção 4.2 apresentamos várias tabelas comparativas que ilustram o quanto melhor os limitantes apresentados no Teorema 4.2.2 são em relação aos limitantes em [5] e [11].

4.1 Cardinalidade de $[0]_H$

Lembrando que

$$\mathcal{A}^i_r = \{D \subseteq C; \dim(D) = i \text{ e } |supp(D)| = r\},$$

estudamos os suportes dos subcódigos de $\mathcal{A}^i_r$, com $r \in [\![0,n]\!]$ e $i \in [\![k]\!]$.

Lema 4.1.1 *Sejam* C *um código,* $D \in A^i_r(C)$ *e* $s \in [\![n]\!]$. *Então existe um subconjunto* $\{c^1,\ldots,c^{i-1}\} \subset D$ *linearmente independente, tal que* $\pi_s(c^j) = 0$, *para todo* $j \in [\![i-1]\!]$.

Demonstração
Seja $H = supp(D)$. Dividimos a demonstração em dois casos, quando $s \notin H$ e quando $s \in H$. Se $s \notin H$, então $\pi_{\{s\}}(c) = 0$, para todo $c \in D$. Como $\dim(D) = i$, o resultado é imediato.

Seja $s \in H$. Como $H = supp(D)$, existe $c \in D$ tal que $\pi_{\{s\}}(c) \neq 0$. Consideremos uma base de D da forma $\{c, u^1 \ldots, u^{i-1}\}$, isto é, uma base que contenha c. Definimos $c^j := u^j$, se $\pi_{\{s\}}(u^j) = 0$, ou, $c^j = u^j + (q-1)c$, se $\pi_{\{s\}}(u^j) \neq 0$. Então o conjunto $\{c^1, \ldots, c^{i-1}\}$ satisfaz as condições do Lema 4.1.1. □

Ao considerar a função $\mathcal{A}^i_j \to 2^{[\![n]\!]}$, $i \in [\![k]\!]$ e $j \in [\![n]\!]$, que a cada $D \in \mathcal{A}^i_j$ associa $supp(D)$, não podemos, de modo geral, fazer qualquer afirmação sobre esta função. O próximo lema mostra que quando $j = d_i$ esta função é injetora.

Lema 4.1.2 *Sejam $D_1 \neq D_2$ subcódigos de $\mathcal{A}^i_{d_i}$, então*

$$supp(D_1) \neq supp(D_2).$$

Demonstração
Seja $c \in D_2 \setminus D_1$ e suponha por absurdo que $supp(D_1) = supp(D_2) = H$. Como $c \in D_2 \setminus D_1$, então $D = \langle \{c\} \cup D_1 \rangle$ tem dimensão $i+1$. Note que, como $supp(c) \subseteq supp(D_1) = H$, temos que $supp(D) = H$ e, pelo Lema 4.1.1, dado $s \in H$, existe um conjunto linearmente dependente $\{c^1, \ldots, c^i\} \subseteq D$ tal que $\pi_{\{s\}}(c^j) = 0$, $j \in [i]$, isto é, $\tilde{D} = \langle c^1, \ldots, c^i \rangle$ é tal que $\dim(\tilde{D}) = i$ e $supp(\tilde{D}) \subseteq H - \{i\}$, isto é, $|supp(\tilde{D})| < d_i$. Uma contradição, pois $|supp(\tilde{D})| \geq d_i$. □

Observamos que a condição $j = d_i$ é essencial para garantirmos a injetividade da função que a cada $D \in \mathcal{A}^i_j$ associa $supp(D)$. No Exemplo 4.1.3 apresentamos dois subcódigos $D_1, D_2 \in A^i_j$ distintos com $supp(D_1) = supp(D_2)$. Para os cálculos deste exemplo, usamos o Teorema 2.3.1 da Monotonicidade de Wei.

Exemplo 4.1.3 *Seja C o $[5,4]_2$-código cuja matriz geradora é dada por*

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Como $c = (1,0,0,0,0) \in C$, então $d_1 = 1$. Pelo Teorema da Monotonicidade 2.3.1*, $d_2 > d_1 = 1$. Por outro lado, por definição*

$$d_2(C) = \min\{|supp(D)|; D \subseteq C \text{ com } \dim(D) = 2\}. \tag{4.8}$$

Como $D = \langle (1,0,0,0,0), (1,1,0,0,0) \rangle$ *é subcódigo de* C *com* $supp(D) = [\![2]\!]$, $d_2 \leq 2$. *Portanto* $d_2 = 2$. *Os subcódigos*

$$D_1 = \langle (1,1,0,0,0), (0,1,1,0,0) \rangle$$
$$D_2 = \langle (1,0,0,0,0), (0,1,1,0,0) \rangle$$

são subcódigos de C *distintos em* $\mathcal{A}_3^2$ *com mesmo suporte*

$$supp(D_1) = supp(D_2).$$

Denotamos por Φ_i o conjunto de todos os subconjuntos de $[\![n]\!]$ que são suporte de algum subcódigo $D \in \mathcal{A}_{d_i}^i$, isto é,

$$\Phi_i = \{H \subseteq [\![n]\!]; \exists\ D \in \mathcal{A}_{d_i}^i \text{ com } H = \text{supp}(D)\},$$

O Lema 4.1.2 garante que $|\Phi_i| = |\mathcal{A}_{d_i}^i| = A_{d_i}^i$, isto é, para obter $A_{d_i}^i$, basta determinar $|\Phi_i|$.

Lema 4.1.4 *Seja* C *um* $[n,k]_q$*-código linear. Se existe* $D \subseteq C$ *tal que* $\dim(D) = i$ *e* $supp(D) \subseteq H \subseteq [\![n]\!]$, *então* $|[0]_H| \geq q^i$.

Demonstração
Se $c \in D$, então $c \in [0]_H$. Logo $D \subseteq [0]_H$ e $|[0]_H| \geq |D| = q^i$. □

Lema 4.1.5 *Seja* C *um* $[n,k]_q$*-código linear. Se* $H \in \Phi_i$, *então* $|[0]_H| = q^i$.

Demonstração
Pela Proposição 3.2.6 sabemos que $|[0]_H|$ é potência de q uma vez que $[0]_H \subseteq C$ é $\mathbb{F}_q$-subspaço vetorial de dimensão finita. Suponha por absudo que $|[0]_H| \geq q^{i+1}$. Como $[0]_H$ é $\mathbb{F}_q$-subspaço vetorial, então $\dim([0]_H) \geq i+1$. Logo existe um subcódigo $D \subseteq [0]_H$ tal que $\dim(D) = i+1$. Como $D \subseteq [0]_H$, segue

$$supp(D) \subseteq supp([0]_H) \subseteq H$$

e, portanto,

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

Uma contradição, pois $d_i < d_{i+1}$ pelo Teorema da Monotonicidade 2.3.1. Logo $|[0]_H| \leq q^i$ e, pelo Lema 4.1.4, temos $|[0]_H| = q^i$. □

Lema 4.1.6 *Seja C um $[n,k]_q$-código linear. Se $H \subseteq [\![n]\!]$ com $|H| = d_i$ e $H \notin \Phi_i$, então $|[0]_H| \leq q^{i-1}$.*

Demonstração
Suponha que $|[0]_H| \geq q^i$, ou seja, que $\dim([0]_H) \geq i$. Logo existe um subcódigo i-dimensional $D \subseteq [0]_H$ de C tal que $supp(D) \subseteq H$ e

$$d_i \leq |supp(D)| \leq |supp([0]_H)| \leq |H| = d_i,$$

ou seja, $supp(D) = H$, $\dim(D) = i$ e $|supp(D)| = d_i$. Segue que $H \in \Phi_i$, o que contradiz a hipótese. □

Vamos enunciar aqui um resultado com teor similar ao Lema 4.1.4 que será utilizado na próxima seção. Postergamos a demonstração deste resultado para a Seção 5.2, pois este é um caso particular da Proposição 5.2.4.

Proposição 4.1.7 *Seja C um $[n,k]_q$-código linear. Se $H \subseteq [\![n]\!]$ com $|H| = d_i$ e $H \notin \Phi_i$, então $|[0]_H| \geq q^{k-n+d_i}$.*

4.2 Novos limitantes para as probabilidades de erro

Nesta seção determinamos limitantes para P_* a partir de limitantes para $Q_{*,r}$.

Lema 4.2.1 *Seja C um $[n,k,d_1,\ldots,d_k]_q$-código. Se $r < d_1$, então $Q_{*,r} = 0$.*

Demonstração
Dado $r < d_1$, se $c \in [0]_H$ com $|H| = r$, então $supp(c) \subseteq H$, logo $w(c) \leq |H| = r < d_1$. Logo $c = 0$ e $[0]_H = \{0\}$. Pelas expressões (4.1) e (4.2), $Q_{*,r} = 0$. □

Seja $G \in M_{k\times n}(\mathbb{F}_q^n)$ uma matriz geradora de C. O k-ésimo peso generalizado d_k de C é dado pelo números de colunas não nulas de G. Acontece que, se G tem l colunas nulas, excluindo-se essas colunas e denominando a matriz obtida por $\tilde{G}$, temos que $\tilde{G} \in M_{k\times n-l}(\mathbb{F}_q)$ é matriz geradora de um $[d_k,k]$-código $\tilde{C}$ com $P_*(C) = P_*(\tilde{C})$, logo assumimos que $d_k = n$ a partir desse ponto. Pelo Lema 4.2.1 e pela expressão (4.3) temos que

$$P_*(C) = \sum_{i=d_1}^{d_k} Q_{*,i}\mathtt{p}^i(1-\mathtt{p})^{n-i}. \tag{4.9}$$

Lembrando que $|\mathcal{A}_r^i| = A_r^i$, vamos relacionar esse invariante com a dimensão do subcódigo $[0]_H$.

Fixado $d_i \in [\![n]\!]$ e particionando

$$\{H \subseteq [\![n]\!]; |H| = d_i\} = \Phi_i \dot{\bigcup} (\{H \subseteq [\![n]\!]; |H| = d_i\} \setminus \Phi_i)$$

segue que

$$Q_{dec,d_i} = \sum_{H \in \Phi_i} \left(1 - \frac{1}{|[0]_H|}\right) + \sum_{\substack{H \notin \Phi_i \\ |H| = d_i}} \left(1 - \frac{1}{|[0]_H|}\right).$$

Do Lema 4.1.5 temos que

$$Q_{dec,d_i} = \sum_{H \in \Phi_i} \left(1 - \frac{1}{q^i}\right) + \sum_{\substack{H \notin \Phi_i \\ |H| = d_i}} \left(1 - \frac{1}{|[0]_H|}\right). \tag{4.10}$$

Para Q_{err,d_i}, seguindo os mesmo passos, temos

$$Q_{err,d_i} = \sum_{H \in \Phi_i} \left\lceil 1 - \frac{1}{q^i} \right\rceil + \sum_{\substack{H \notin \Phi_i \\ |H| = d_i}} \left\lceil 1 - \frac{1}{|[0]_H|} \right\rceil. \tag{4.11}$$

Em particular, se $i = 1$, dos Lemas 4.1.5, 4.1.6 e da Proposição 4.1.7, obtemos que todos os termos do primeiro somatório acima são constantes iguais a 1 e todos os termos do segundo somatório acima são nulos. Segue que

$$Q_{err,d_1} = |\Phi_1| = A_{d_1}^1.$$

Isto é, Q_{err,d_1} é dado pelo número de palavras de peso mínimo do código C. Em [9] limitantes para $A_{d_1}^1$ foram obtidos para códigos NMDS.

Em termos de limitantes, dos lemas 4.1.5, 4.1.6 e da Proposição 4.1.7, e das expressões (4.10) e (4.11), provamos o seguinte teorema:

Teorema 4.2.2 *Seja C um $[n,k]_q$-código. Então*

$$A_{d_i}^i \left(1 - \frac{1}{q^i}\right) + \left(\binom{n}{d_i} - A_{d_i}^i\right)\left(1 - \frac{1}{\max\{1, q^{k-n+d_i}\}}\right) \leq Q_{dec,d_i}$$

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

para todo $i \in [\![k]\!]$. *De maneira análoga obtemos limitantes para* Q_{err,d_i}, *com* $i \in [\![k]\!]$:

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

para todo $i \in [\![2,k]\!]$.

$$Q_{err,d_1} = |\Phi_1| = A^1_{d_1}.$$

Note que encontramos limitantes para alguns $Q_{*,r}$, a saber, para $r = d_i$, $i \in [\![k]\!]$. Observemos que, se $r < d_1$, então $Q_{*,r} = 0$, de modo que, para calcular limitantes bons para P_*, precisamos estimar $Q_{*,r}$ para todo $r \in [\![d_1, d_k]\!]$ com $r \neq d_i$. Isso não é um problema que pode ser abordado da maneira como feito no Teorema 4.2.2, uma vez que os espectros i-dimensionais com suporte diferente de d_i contêm códigos distintos com mesmo suporte. Nesta tese, estudamos casos particulares, de acordo com as propriedades de separação de um código. De modo mais específico, os casos em que C é MDS e AMDS. Mostramos que os limitantes coincidem para todo $r \in [\![d_s, n]\!]$ quando C é um $[n,k]_q$-código $\mathcal{P}_s$-MDS, para algum $s \in [\![k]\!]$ (Teorema 5.1.1). Como consequência, os limitantes obtidos no Teorema 4.2.2 fornecem fórmulas exatas para códigos MDS (reproduzindo a fórmula exata apresentada em [11]) (ver Corolário 5.1.2). Também mostramos que os limitantes inferiores e superiores dados pelo Teorema 4.2.2 coincidem quando $r = d_1$ ou $r = d_k$ (Lema 5.2.1).

4.3 Comparação de limitantes para o caso de $[7,4]_2$-códigos lineares

Apresentamos agora algumas tabelas e gráficos exemplificando os ganhos em relação aos limitantes conhecidos para o caso de $[7,4]_2$-códigos lineares.

Dizemos que dois $[n,k]_q$-códigos C_1 e C_2 são *equivalentes* se existir uma isometria entre eles, isto é, um isomorfismo de $\mathbb{F}_q$-espaços vetoriais preservando a distância de Hamming. A menos de isomorfismo, existem 22 $[7,4]_2$-códigos distintos (a menos de equivalência). Os códigos $C(4,7,i)$, $i \in [\![22]\!]$, são descritos no anexo deste trabalho pelas suas matrizes geradoras.

A Tabela 4.1 apresenta uma comparação entre o valor obtido de Q_{err,d_1} pelo Teorema 4.2.2 e o valor do limitante superior Q^{sup}_{DID,d_1} para Q_{err,d_1}. Ambos foram divididos por $\binom{n}{d_1}$ para comparações em termos de probabilidade.

Calculamos tais valores para todos os 22 $[7,4]_2$-códigos distintos a menos de equivalência.

Substituindo Q^{sup}_{DID,d_1} por Q_{err,d_1} em (4.7), obtemos um limitante superior para $P_{err}(C;\mathtt{p})$ o qual denotamos por $P^{sup}_{T2,err}(C;\mathtt{p})$.

Seja $\mathtt{p}$ a probabilidade de erro do canal. Para $\mathtt{p} = 0,1$ e $\mathtt{p} = 0,01$, as Tabelas 4.2 e 4.3 apresentam uma comparação entre os limitantes superiores $P^{sup}_{DID}(C;\mathtt{p})$ e $P^{sup}_{T2,err}(C;\mathtt{p})$ para todos os 22 $[7,4]_2$-códigos distintos (a menos de equivalência). Em alguns cálculos, utilizando as fórmulas encontradas em [5], os limitantes $Q^{sup}_{DID,r}$ para $Q_{err,r}$ forneceram valores superiores a $\binom{n}{r}$, o que não é possível pois

$$\frac{Q^{sup}_{DID,r}}{\binom{n}{r}}$$

é um limitante superior para a probabilidade de ocorrer ambiguidade em um canal com quantidade fixa de ambiguidades igual a r (ver [5]), portanto não pode ser superior a um. Logo, quando os limitantes $Q^{sup}_{DID,r}$ eram superiores a $\binom{n}{r}$, consideramos $Q^{sup}_{DID,r} = \binom{n}{r}$ para melhores resultados tanto para $P^{sup}_{DID}(C;\mathtt{p})$ quanto para $P^{sup}_{T2,err}(C;\mathtt{p})$. A última coluna em cada uma destas tabelas apresenta o quociente entre os limitante para a probabilidade de erro e ambiguidade refletindo para valores diferentes de $\mathtt{p}$ o efeito obtido pelo fato do termo $Q^{sup}_{DID,d_1}/Q_{err,d_1} > 1$. Esta influência pode ser visualizada nos Gráficos que seguem as tabelas. A razão representado no eixo y é dada por $P^{sup}_{DID}(C;\mathtt{p})/P^{sup}_{T2}(C;\mathtt{p})$. Alguns gráficos foram omitidos por representarem mesmo traço.

As Proposições 6.0.12 e 6.0.13 mostram que nos casos em que desejamos comparar dois $[n,k]_q$-códigos C_1 e C_2 com $d_1(C_1) = d_2(C_2) = d$, para $\mathtt{p}$ suficientemente pequeno o coeficiente $Q_{*,d_1}(C_j)$, $j \in [\![2]\!]$, é o mais importante, pois determina qual o melhor código em relação a quantidade de erros de decodificação ou de ambiguidades. Observa-se nas Tabelas 4.2 e 4.3 que para valores menores de $\mathtt{p}$ o limitante $P^{sup}_{T2,err}(C;\mathtt{p})$ é bem melhor que o limitante $P^{sup}_{DID}(C;\mathtt{p})$. Este comportamento para $\mathtt{p}$ pequeno será explorado no Capítulo 6.

De fato, a fórmula exata para Q_{err,d_1} dada pelo Teorema 4.2.2 melhora o limitante dado por Didier [5]. Note que os códigos do anexo não possuem mesma distância mínima, quando queremos comparar dois $[n,k]_q$-códigos distintos $C_1 \neq C_2$ com $d_1(C_1) \neq d_1(C_2)$, para $\mathtt{p}$ suficientemente pequeno, se $d_1(C_1) > d_1(C_2)$, então $P_*(C_1) < P_*(C_2)$, o que será mostrado na Proposição 6.0.12. Passamos agora a comparar (para os $[7,4]_2$-código) o desempenho do

limitante inferior que obtivemos no Teorema 4.2.2 com o limitante estabelecido por Fashandi et al.

Para os coeficientes $Q_{err,r}$, com $r = d_i$, $i \notin \{1, k\}$, o limitante superior dado pelo Teorema 4.2.2 é o pior possível. Podemos pensar que o Teorema 4.2.2, na prática, é útil apenas para calcular Q_{err,d_1}, porém isso não é verdade, uma vez que o Teorema 4.2.2 também fornece limitantes superiores e inferiores para $Q_{dec,r}$ e, mais ainda, fornece limitantes inferiores para $Q_{err,r}$, $r = d_i$, $i \in [\![k]\!]$. A partir desses limitantes, também podemos melhorar limitantes inferiores para $P_{dec}(C)$ que aparecem na literatura.

Denotamos por Q^{inf}_{T2,d_i}, $i \in [\![k]\!]$, o limitante inferior para Q_{dec,d_i} dado pelo Teorema 4.2.2.

A Tabelas 4.5 e 4.6 apresentam uma comparação entre os limitantes Q^{inf}_{T2,d_i} para Q_{dec,d_i}, $i \in \{2, 3\}$, obtido pelo Teorema 4.2.2, e o limitante inferior Q^{inf}_{FAS,d_i} para Q_{dec,d_i} encontrado em [11], novamente ambos divididos por $\binom{n}{d_i}$ para comparações em termos de suas probabilidades. Calculamos tais valores para todos os 22 $[7,4]_2$-códigos distintos (a menos de equivalência). Em alguns cálculos utilizando as fórmulas encontradas em [11], os coeficientes $Q^{inf}_{FAS,r}$ forneceram valores negativos, o que não é possível pois

$$\frac{Q^{inf}_{FAS,r}}{\binom{n}{r}}$$

é um limitante inferior para a probabilidade de ocorrer ambiguidade em um canal com quantidade fixa de erros igual a r (ver [11]). Logo, quando os limitantes $Q^{inf}_{FAS,r}$ eram inferiores a zero, optamos por considerar $Q^{inf}_{FAS,r} = 0$ para melhores resultados tanto para $P^{inf}_{FAS}(C; \mathtt{p})$ quanto para $P^{inf}_{T2,dec}(C; \mathtt{p})$. Sendo assim, quando $i = 1$, isto é, $d_i = d_1$ todos os cálculos para $Q^{inf}_{T2,err}$ e para $Q^{inf}_{FAS,err}$ forneceram valores nulos (ver Tabela 4.4) exceto para o $[7,4]_2$-código de Hamming denotado por $C(4, 7, 22)$.

Substituindo os coeficientes Q^{inf}_{FAS,d_i} por Q^{inf}_{T2,d_i} na expressão (4.6), obtemos um limitante inferior, o qual denotamos por $P^{inf}_{T2,dec}(C; \mathtt{p})$ para $P_{dec}(C; \mathtt{p})$. Observamos que os coeficientes $Q_{*,r}$ não dependem da probabilidade de erro do canal. Mais ainda, o fato de termos sempre $Q^{inf}_{FAS,d_i}/Q^{inf}_{T2,d_i} > 1$ implica o limitante $P^{inf}_{T2,dec}(C; \mathtt{p})$ é melhor que o obtidos por Fashandi et al. O quanto melhoramos este limitante, isto depende de $\mathtt{p}$.

Seja $\mathtt{p}$ a probabilidade de erro do canal. Para $\mathtt{p} = 0,1$ e $\mathtt{p} = 0,01$, as Tabelas 4.7 e 4.8 apresentam uma comparação entre os limitantes inferiores

$P^{inf}_{FAS}(C;\mathtt{p})$ e $P^{inf}_{T2,dec}(C;\mathtt{p})$ para todos os 22 $[7,4]_2$-códigos distintos (a menos de equivalência). Note que como acontece ao compararmos $P^{sup}_{T2,err}(C;\mathtt{p})$ com $P^{sup}_{DID}(C;\mathtt{p})$, $P^{inf}_{T2,dec}(C;\mathtt{p})$ é bem melhor que $P^{inf}_{FAS}(C;\mathtt{p})$ quando $\mathtt{p}$ é menor.

Expressões e valores exatos de A^i_r, $i \in [\![k]\!]$, $r \in [\![n]\!]$, para $[n,k]_q$-códigos arbitrátios ainda são problemas em aberto, isso dificulta o cálculo dos limitantes para códigos arbitrários e, ao mesmo tempo, dá uma importância maior para o problema de determinar os coeficientes A^i_r. A melhora dos limitantes é óbvia pelas relações (4.10) e (4.11), uma vez que determinamos o valor exato de algumas parcelas do somatório que aparece nestas relações.

$[7,4]_2$-códigos	$Q^{sup}_{DID,d_1}/\binom{7}{d_1}$	$Q_{err,d_1}/\binom{7}{d_1}$	Q^{sup}_{DID}/Q_{err}
C(4,7,1)	0,5	0,4286	1,1665
C(4,7,2)	0,4444	0,2857	1,5554
C(4,7,3)	0,4444	0,2857	1,5554
C(4,7,4)	0,3333	0,1429	2,3324
C(4,7,5)	0,3333	0,1429	2,3324
C(4,7,6)	0,4	0,2857	1,4001
C(4,7,7)	0,4	0,2857	1,4001
C(4,7,8)	0,3125	0,1429	2,1868
C(4,7,9)	0,3125	0,1429	2,1868
C(4,7,10)	0,3333	0,1905	1,7496
C(4,7,11)	0,3333	0,1905	1,7496
C(4,7,12)	0,3125	0,1429	2,1868
C(4,7,13)	0,3333	0,2381	1,3998
C(4,7,14)	0,2667	0,1429	1,8663
C(4,7,15)	0,2	0,0952	2,1008
C(4,7,16)	0,2	0,1429	1,3996
C(4,7,17)	0,2222	0,1429	1,5549
C(4,7,18)	0,4164	0,2857	1,4575
C(4,7,19)	0,3125	0,1429	2,1868
C(4,7,20)	0,2	0,0476	**4,2017**
C(4,7,21)	0,3333	0,1905	1,7496
C(4,7,22)	0,25	0,2	1,25

Tabela 4.1: Comparação entre Q^{sup}_{DID,d_1} e Q_{err,d_1}

$[7,4]_2$-códigos	$P_{DID}^{sup}(C;0,1)$	$P_{T2,err}^{sup}(C;0,1)$	$P_{DID}^{sup}/P_{T2,err}^{sup}$
C(4,7,1)	0,0332	0,0294	1,1290
C(4,7,2)	0,0296	0,0212	1,3983
C(4,7,3)	0,0296	0,0212	1,3983
C(4,7,4)	0,0224	0,0123	1,8249
C(4,7,5)	0,0224	0,0123	1,8251
C(4,7,6)	0,0031	0,0024	1,2783
C(4,7,7)	0,0031	0,0024	1,2783
C(4,7,8)	0,0210	0,0120	1,7526
C(4,7,9)	0,0210	0,0120	1,7526
C(4,7,10)	0,0027	0,0019	1,4528
C(4,7,11)	0,0027	0,0019	1,4528
C(4,7,12)	0,0210	0,0120	1,7526
C(4,7,13)	0,0027	0,0021	1,2622
C(4,7,14)	0,0179	0,0113	1,5800
C(4,7,15)	0,0017	0,0010	1,5960
C(4,7,16)	0,0017	0,0013	1,2558
C(4,7,17)	0,0018	0,0014	1,3457
C(4,7,18)	0,0278	0,0208	1,3332
C(4,7,19)	0,0210	0,0120	1,7526
C(4,7,20)	0,0017	0,0008	2,1890
C(4,7,21)	0,0027	0,0019	1,4528
C(4,7,22)	0,0002	0,0002	1,1540

Tabela 4.2: Comparação entre $P_{DID}^{sup}(C;0,1)$ e $P_{T2,err}^{sup}(C;0,1)$

$[7,4]_2$-códigos	$P^{sup}_{DID}(C;0,01)$	$P^{sup}_{T2,err}(C;0,01)$	$P^{sup}_{DID}/P^{sup}_{DID}$
C(4,7,1)	0,0048	0,0041	1,1628
C(4,7,2)	0,0043	0,0028	1,5383
C(4,7,3)	0,0043	0,0028	1,5383
C(4,7,4)	0,0032	0,0014	2,2722
C(4,7,5)	0,0032	0,0014	2,2722
C(4,7,6)	3,9E-005	2,8E-005	1,3862
C(4,7,7)	3,9E-005	2,8E-005	1,3862
C(4,7,8)	0,0030	0,0014	2,1365
C(4,7,9)	0,0030	0,0014	2,1365
C(4,7,10)	3,2E-005	1,9E-005	1,7117
C(4,7,11)	3,2E-005	1,9E-005	1,7117
C(4,7,12)	0,0030	0,0014	2,1365
C(4,7,13)	3,2E-005	2,3E-005	1,3834
C(4,7,14)	0,0026	0,0014	1,8349
C(4,7,15)	1,9E-005	9,6E-006	2,0331
C(4,7,16)	1,9E-005	1,4E-005	1,3835
C(4,7,17)	2,1E-005	1,4E-005	1,5300
C(4,7,18)	0,0040	0,0028	1,4442
C(4,7,19)	0,0030	0,0014	2,1365
C(4,7,20)	1,9E-005	5,1E-006	3,8333
C(4,7,21)	3,2E-005	1,9E-005	1,7117
C(4,7,22)	2,4E-007	2,0E-007	1,2379

Tabela 4.3: Comparação entre $P^{sup}_{DID}(C;0,01)$ e $P^{sup}_{T2,err}(C;0,01)$

$[7,4]_2$-códigos	$Q^{inf}_{FAS,d_1}/\binom{7}{d_1}$	$Q^{inf}_{T2,d_1}/\binom{7}{d_1}$	$Q^{inf}_{T2} - Q^{inf}_{FAS}$
C(4,7,i)	0	0	0
C(4,7,22)	0	0,1	0,1

Tabela 4.4: Comparação entre Q^{inf}_{FAS,d_1} e Q^{inf}_{T2,d_1}, $i \in [\![21]\!]$

$[7,4]_2$-códigos	$Q^{inf}_{FAS,d_2}/\binom{7}{d_2}$	$Q^{inf}_{T2,d_2}/\binom{7}{d_2}$	$Q^{inf}_{T2} - Q^{inf}_{FAS}$
C(4,7,1)	0	0	0
C(4,7,2)	0	0	0
C(4,7,3)	0	0	0
C(4,7,4)	0	0,0857	0,0857
C(4,7,5)	0	0,0857	0,0857
C(4,7,6)	0	0,0857	0,0857
C(4,7,7)	0	0,0857	0,0857
C(4,7,8)	0	0,0429	0,0429
C(4,7,9)	0	0,0428	0,0429
C(4,7,10)	0	0,0214	0,0214
C(4,7,11)	0	0,0214	0,0214
C(4,7,12)	0	0,0643	0,0643
C(4,7,13)	0	0,0214	0,0214
C(4,7,14)	0,5	0,5286	0,0286
C(4,7,15)	0,5	0,5214	0,0214
C(4,7,16)	0,5	0,5214	0,0214
C(4,7,17)	0,5	0,55	0,05
C(4,7,18)	0	0	0
C(4,7,19)	0	0,0214	0,0214
C(4,7,20)	0,5	0,5143	0,0143
C(4,7,21)	0	0,0214	0,0214
C(4,7,22)	0,75	0,75	0

Tabela 4.5: Comparação entre Q^{inf}_{FAS,d_2} e Q^{inf}_{T2,d_2}

$[7,4]_2$-códigos	$Q^{inf}_{FAS,d_3}/\binom{7}{d_3}$	$Q^{inf}_{T2,d_3}/\binom{7}{d_3}$	$Q^{inf}_{T2} - Q^{inf}_{FAS}$
C(4,7,1)	0	0,025	0,025
C(4,7,2)	0,5	0,5107	0,0107
C(4,7,3)	0,5	0,5107	0,0107
C(4,7,4)	0,5	0,5107	0,0107
C(4,7,5)	0,5	0,5107	0,0107
C(4,7,6)	0,5	0,5107	0,0107
C(4,7,7)	0,5	0,5107	0,0107
C(4,7,8)	0,75	0,7619	0,0119
C(4,7,9)	0,75	0,7560	0,0060
C(4,7,10)	0,75	0,7560	0,0060
C(4,7,11)	0,75	0,7560	0,0060
C(4,7,12)	0,75	0,7679	0,0179
C(4,7,13)	0,75	0,7619	0,0119
C(4,7,14)	0,875	0,875	0
C(4,7,15)	0,875	0,875	0
C(4,7,16)	0,875	0,875	0
C(4,7,17)	0,75	0,7560	0,0060
C(4,7,18)	0,75	0,7619	0,0119
C(4,7,19)	0,75	0,7619	0,0119
C(4,7,20)	0,875	0,8750	0
C(4,7,21)	0,75	0,7619	0,0119
C(4,7,22)	0,875	0,875	0

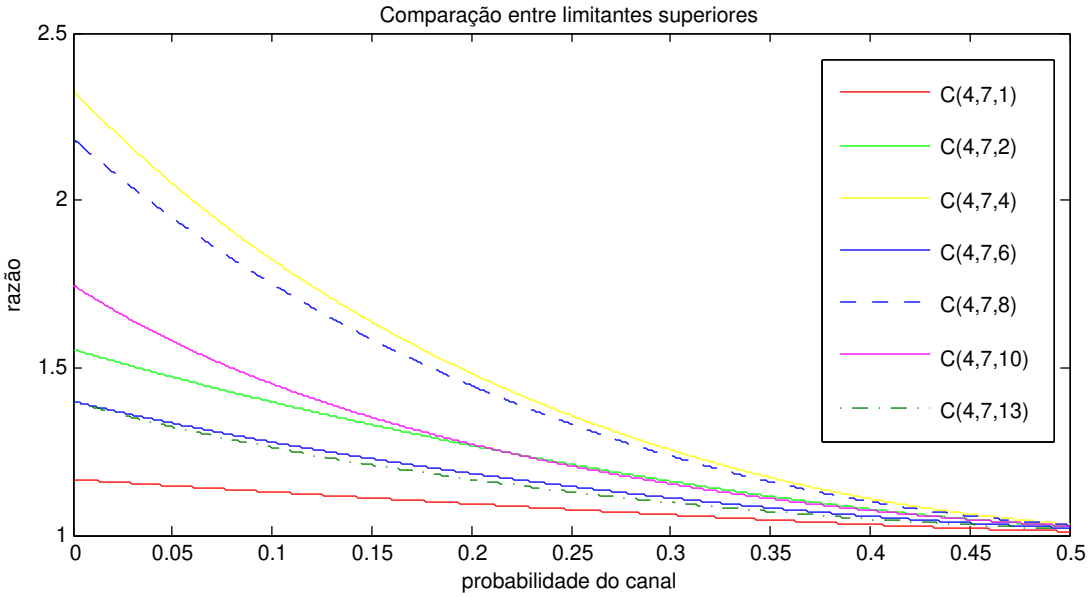
Tabela 4.6: Comparação entre Q^{inf}_{FAS,d_3} e Q^{inf}_{T2,d_3}

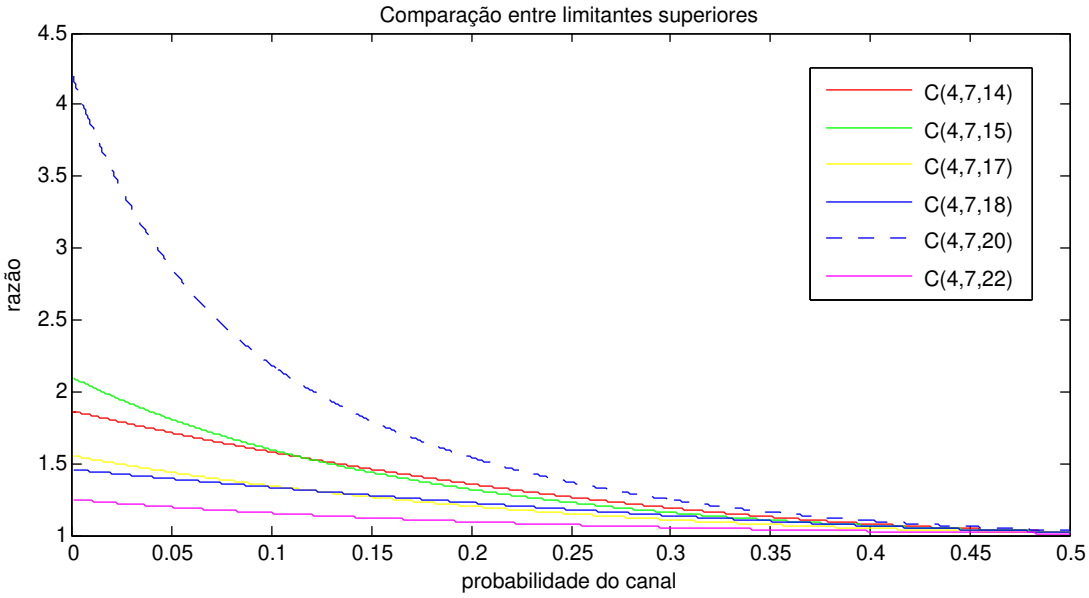
$[7,4]_2$-códigos	$P_{FAS}^{inf}(C;0,1)$	$P_{T2,dec}^{inf}(C;0,1)$	$P_{T2,dec}^{inf}/P_{FAS}^{inf}$
C(4,7,1)	4,3E-005	0,000059815	1,377828966
C(4,7,2)	4,3E-005	4,4193E-005	1,017991856
C(4,7,3)	4,3E-005	4,4193E-005	1,017991856
C(4,7,4)	4,3E-005	0,000100430	2,313405454
C(4,7,5)	4,3E-005	0,000100430	2,313405454
C(4,7,6)	4,3E-005	0,000100430	2,313405454
C(4,7,7)	4,3E-005	0,000100430	2,313405454
C(4,7,8)	4,3E-005	7,1627E-005	1,649928017
C(4,7,9)	4,3E-005	7,1579E-005	1,648817408
C(4,7,10)	4,3E-005	0,00005752	1,324964008
C(4,7,11)	4,3E-005	0,00005752	1,324964008
C(4,7,12)	4,3E-005	0,000085735	1,974892024
C(4,7,13)	4,3E-005	5,7568E-005	1,326074616
C(4,7,14)	4,3E-005	4,5495E-005	1,047978282
C(4,7,15)	4,3E-005	4,4974E-005	1,035983711
C(4,7,16)	4,3E-005	4,4974E-005	1,035983711
C(4,7,17)	4,3E-005	4,7105E-005	1,085072601
C(4,7,18)	4,3E-005	4,3508E-005	1,002221217
C(4,7,19)	4,3E-005	5,7568E-005	1,326074616
C(4,7,20)	4,3E-005	4,4453E-005	1,023989140
C(4,7,21)	4,3E-005	5,7568E-005	1,326074616
C(4,7,22)	4,3E-005	0,000109023	2,511315865

Tabela 4.7: Comparação entre $P_{FAS}^{inf}(C;0,1)$ e $P_{T2,dec}^{inf}(C;0,1)$

$[7,4]_2$-códigos	$P^{inf}_{FAS}(C;0,01)$	$P^{inf}_{T2,dec}(C;0,01)$	$P^{inf}_{T2,dec}/P^{inf}_{FAS}$
C(4,7,1)	4,9E-009	2,8936E-008	5,8770242221
C(4,7,2)	4,9E-009	0,000000005	1,0211082628
C(4,7,3)	4,9E-009	0,000000005	1,0211082628
C(4,7,4)	4,9E-009	8,7356E-008	17,742334164
C(4,7,5)	4,9E-009	8,7356E-008	17,742334164
C(4,7,6)	4,9E-009	8,7356E-008	17,742334164
C(4,7,7)	4,9E-009	8,7356E-008	17,742334164
C(4,7,8)	4,9E-009	4,6089E-008	9,3608499147
C(4,7,9)	4,9E-009	4,6088E-008	9,3607314376
C(4,7,10)	4,9E-009	2,5506E-008	5,1804249476
C(4,7,11)	4,9E-009	2,5506E-008	5,1804249476
C(4,7,12)	4,9E-009	6,6671E-008	13,541274862
C(4,7,13)	4,9E-009	2,5506E-008	5,1805434247
C(4,7,14)	4,9E-009	5,2007E-009	1,0562887008
C(4,7,15)	4,9E-009	5,1314E-009	1,0422165255
C(4,7,16)	4,9E-009	5,1314E-009	1,0422165255
C(4,7,17)	4,9E-009	5,4091E-009	1,0986237034
C(4,7,18)	4,9E-009	4,9247E-009	1,0002369542
C(4,7,19)	4,9E-009	2,5506E-008	5,1805434247
C(4,7,20)	4,9E-009	5,0621E-009	1,0281443504
C(4,7,21)	4,9E-009	2,5506E-008	5,1805434247
C(4,7,22)	4,9E-009	0,000000101	20,508096889

Tabela 4.8: Comparação entre $P^{inf}_{FAS}(C;0,01)$ e $P^{inf}_{T2,dec}(C;0,01)$


Comparação entre limitantes superiores
razão
probabilidade do canal
2.5
2
1.5
1
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
0.5
C(4,7,1)
C(4,7,2)
C(4,7,4)
C(4,7,6)
C(4,7,8)
C(4,7,10)
C(4,7,13)


Comparação entre limitantes superiores
razão
probabilidade do canal
C(4,7,14)
C(4,7,15)
C(4,7,17)
C(4,7,18)
C(4,7,20)
C(4,7,22)
4.5
4
3.5
3
2.5
2
1.5
1
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
0.5

4.4 Comparação de limitantes para o caso de $[7,4]_7$-códigos lineares

No trabalho de Fashandi et al, é feito uma análise do limitante para códigos com alfabeto relativamente grande, isto é, $[n,k]_q$-códigos com $q \geq n$. Como nos parâmetros $n = 7$, $k = 4$ e $q = 7$ fazer um análise de todos os $[n,k]_q$-códigos a menos de equivalência é uma tarefa que requer muito espaço, uma vez que existem vários códigos a menos de equivalência com esses parâmetros, optamos por estudar dez $[7,4]_7$-códigos, escolhido por meio de geradores pseudo aleatório para ilustrar a eficiência dos limitantes dados pelo Teorema 4.2.2.

Considere os $[7,4]_7$-códigos C_i, $i \in [\![10]\!]$, cujas matrizes geradoras G_i, são respectivamente

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 2 & 5 \\ 0 & 1 & 0 & 0 & 5 & 0 & 2 \\ 0 & 0 & 1 & 0 & 3 & 2 & 4 \\ 0 & 0 & 0 & 1 & 6 & 4 & 6 \end{pmatrix},$$

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 4 & 0 & 6 \\ 0 & 1 & 0 & 0 & 0 & 2 & 4 \\ 0 & 0 & 1 & 0 & 3 & 2 & 2 \\ 0 & 0 & 0 & 1 & 4 & 0 & 3 \end{pmatrix},$$

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 2 & 5 \\ 0 & 1 & 0 & 0 & 5 & 6 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 \end{pmatrix},$$

$$G_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 5 & 1 & 3 \\ 0 & 1 & 0 & 0 & 1 & 4 & 4 \\ 0 & 0 & 1 & 0 & 1 & 6 & 0 \\ 0 & 0 & 0 & 1 & 1 & 6 & 6 \end{pmatrix},$$

$$G_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 2 & 2 & 4 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 & 6 & 6 & 3 \end{pmatrix},$$

$$G_6 = \begin{pmatrix} 1 & 0 & 0 & 0 & 6 & 6 & 0 \\ 0 & 1 & 0 & 0 & 5 & 5 & 0 \\ 0 & 0 & 1 & 0 & 0 & 3 & 5 \\ 0 & 0 & 0 & 1 & 6 & 1 & 5 \end{pmatrix},$$

$$G_7 = \begin{pmatrix} 1 & 0 & 0 & 0 & 6 & 3 & 0 \\ 0 & 1 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 1 & 0 & 3 & 0 & 2 \\ 0 & 0 & 0 & 1 & 4 & 1 & 5 \end{pmatrix},$$

$$G_8 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 6 & 0 & 6 \\ 0 & 0 & 1 & 0 & 6 & 1 & 0 \\ 0 & 0 & 0 & 1 & 6 & 3 & 6 \end{pmatrix},$$

$$G_9 = \begin{pmatrix} 1 & 0 & 0 & 0 & 4 & 5 & 3 \\ 0 & 1 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 0 & 6 & 6 & 2 \\ 0 & 0 & 0 & 1 & 1 & 2 & 4 \end{pmatrix}$$

e

$$G_{10} = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 3 & 5 \\ 0 & 1 & 0 & 0 & 6 & 3 & 6 \\ 0 & 0 & 1 & 0 & 6 & 1 & 2 \\ 0 & 0 & 0 & 1 & 2 & 1 & 2 \end{pmatrix}.$$

Considere a matriz T tal que sua i-ésima linha representa os coeficientes do polinômio enumerador de peso de C_i, isto é, $T_{i,j}$ é o número de palavras de peso $j-1$ de C_i. Então a matriz T é dada por

$$T = \begin{pmatrix} 1 & 0 & 0 & 24 & 114 & 522 & 912 & 828 \\ 1 & 0 & 0 & 30 & 132 & 432 & 1014 & 792 \\ 1 & 0 & 18 & 30 & 78 & 414 & 1122 & 738 \\ 1 & 0 & 0 & 18 & 138 & 486 & 936 & 822 \\ 1 & 0 & 12 & 24 & 204 & 426 & 774 & 960 \\ 1 & 0 & 6 & 18 & 120 & 480 & 972 & 804 \\ 1 & 0 & 6 & 30 & 114 & 426 & 1050 & 774 \\ 1 & 0 & 0 & 30 & 90 & 558 & 888 & 834 \\ 1 & 0 & 0 & 12 & 162 & 450 & 960 & 816 \\ 1 & 0 & 6 & 12 & 144 & 444 & 996 & 798 \end{pmatrix}.$$

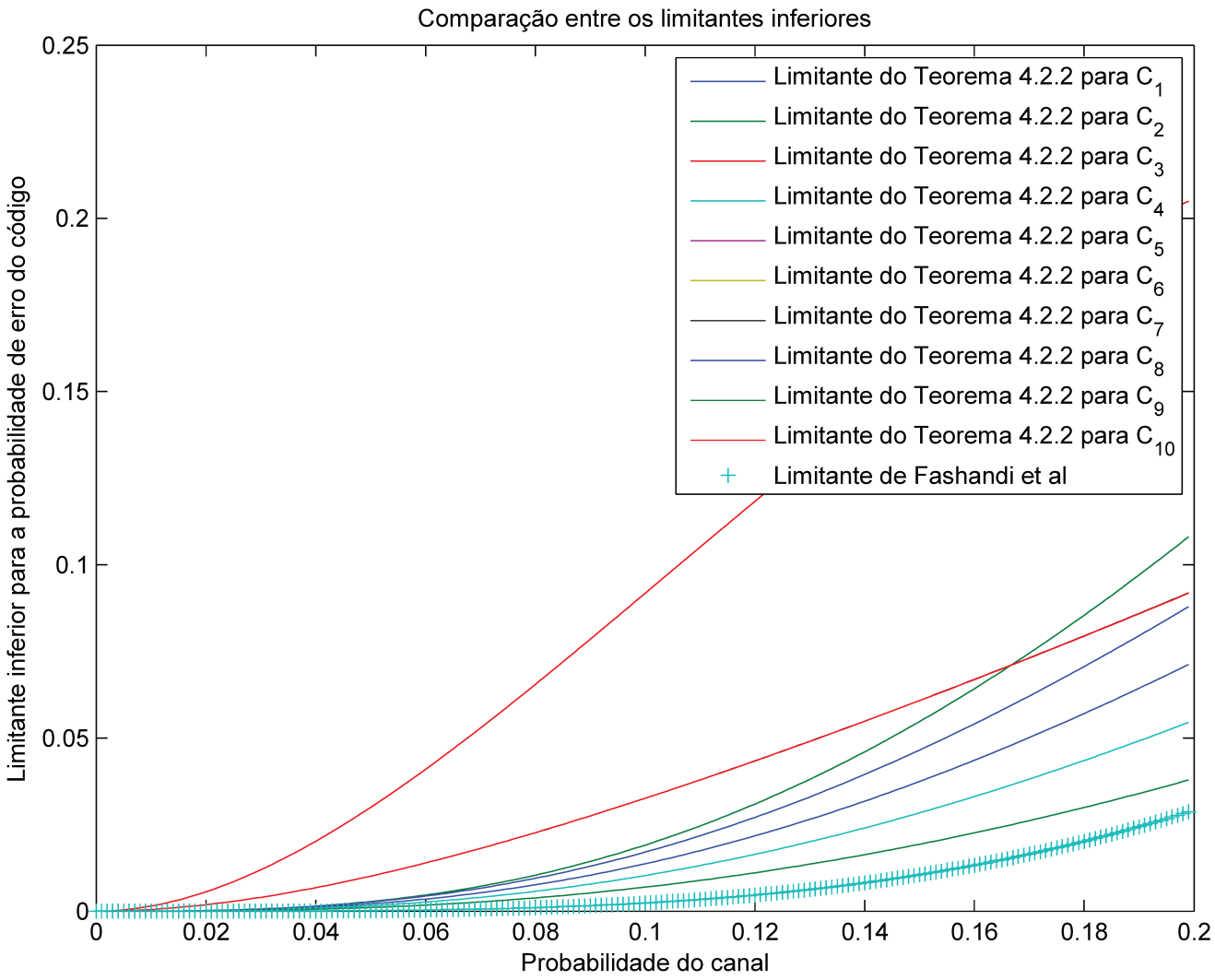
$[7,4]_7$-códigos	$P^{inf}_{T2,dec}(C;0,01)$
C_1	2.00539e-05
C_2	2.49953e-05
C_3	1.46847e-03
C_4	2.00539e-05
C_5	1.01735e-05
C_6	4.89375e-04
C_7	4.89376e-04
C_8	2.49941e-05
C_9	1.01735e-05
C_{10}	4.8937e-04

Tabela 4.9: Comparação entre $P^{inf}_{FAS}(C;0,1)$ e $P^{inf}_{T2,dec}(C;0,1)$ ($q = 7$)

Note que, dentre os dez códigos escolhidos, não há códigos congruentes entre si, pois a matriz T não tem linhas repetidas.

A Tabela ilustra o quão os limitantes inferiores dados pelo Teorema 4.2.2 são mais precisos se comparados aos limitantes de Fashandi et al num canal com probabilidade de erro $\mathtt{p} = 0,01$. Na primeira coluna da Tabela estão os códigos $C_i's$, com $i \in [\![10]\!]$, e na segunda coluna estão os valores dos limitantes para $P_{dec}(C_i)$ dados pelo Teorema 4.2.2. O valor do limitante inferior encontrado em [11] depende apenas do comprimento $n = 7$, da dimensão $k = 4$ e do tamanho do alfabeto $q = 7$ e, portanto, é constante e igual a $P^{inf}_{FAS}(C_i;0,01) = 2.93113e-07$ para todo C_i, $i \in [\![10]\!]$.

A seguir é apresentado o gráfico que compara os limitantes inferiores do Teorema 4.2.2 e os limitantes propostos por Fashandi et al. Nota-se que os limitantes inferiores de Fashandi são menores que os limitantes inferiores do Teorema 4.2.2 para os dez códigos escolhidos.


Comparação entre os limitantes inferiores
Limitante inferior para a probabilidade de erro do código
Probabilidade do canal
0.25
0.2
0.15
0.1
0.05
0
0
0.02
0.04
0.06
0.08
0.1
0.12
0.14
0.16
0.18
0.2
Limitante do Teorema 4.2.2 para C1
Limitante do Teorema 4.2.2 para C2
Limitante do Teorema 4.2.2 para C3
Limitante do Teorema 4.2.2 para C4
Limitante do Teorema 4.2.2 para C5
Limitante do Teorema 4.2.2 para C6
Limitante do Teorema 4.2.2 para C7
Limitante do Teorema 4.2.2 para C8
Limitante do Teorema 4.2.2 para C9
Limitante do Teorema 4.2.2 para C10
Limitante de Fashandi et al

Capítulo 5

Limitantes e propriedades de separação

Na literatura o limitante estabelecido por Fashandi et al [11] determina a expressão exata para a probabilidade de erro de decodificação quando se trata de códigos MDS. Naturalmente, o mesmo ocorre com os limitantes que estabelecemos no Teorema 4.2.2. Neste capítulo utilizamos o resultado obtido para estudar a probabilidade de erro em situações que não são ótimas em termos de separação (MDS), mas que possuem outras propriedades relacionadas: AMDS, NMDS, $\mathcal{P}_s$-MDS, etc.

Na Secão 5.1 determinamos fórmulas exatas para os coeficientes $Q_{*,r}(C)$ de um $[n,k]_q$-código C $\mathcal{P}_s$-MDS para todo $r \in [\![d_s, d_k]\!]$ (ver Teorema 5.1.1). Como consequência direta, determinamos fórmulas exatas para $P_*(C)$ de códigos MDS (ver Corolário 5.1.2). Para calcular tais coeficientes será necessário determinar os i-ésimos espectros generalizados com suporte d_i. Para isso usamos o Teorema 2.5.1 cuja demonstração pode ser encontrada em [15]. Na Seção 5.2 determinamos $P_*(C)$ de um $[n,k]_q$-código C AMDS e apresentamos consequências dos resultados obtidos sobre eficiência de códigos corretores de erros.

5.1 Aplicações dos novos limitantes em códigos MDS

Determinar uma expressão exata para P_* dos códigos MDS é consequência direta do seguinte teorema:

Teorema 5.1.1 *Seja C um $[n,k]_q$-código $\mathcal{P}_s$-MDS. Então*

$$Q_{dec,r} = \binom{n}{r}\left(1 - \frac{1}{q^{r-n+k}}\right) \text{ e } Q_{err,r} = \binom{n}{r},$$

para $d_s \leq r \leq n$.

Demonstração
Seja $d_s \leq r \leq n$. Como C é um código $\mathcal{P}_s$-MDS, $d_s = n-k+s$. Lembrando que $d_k = n$, então temos que a cardinalidade de $[\![d_s, d_k]\!]$ é igual a $k-s+1$. Pelo Teorema da Monotonicidade de Wei, temos que

$$[\![d_s, d_k]\!] = \{d_i; i \in [\![s,k]\!]\},$$

e, logo, $r = d_j = n-k+j$ para algum $j \in [\![s,k]\!]$. Pelo Teorema 2.5.1, temos que

$$A^j_{d_j} = \binom{n}{d_j}, \tag{5.1}$$

para todo $j \in [\![s,k]\!]$. Assim, pelo Teorema 4.2.2 temos

$$A^j_{d_j}\left(1 - \frac{1}{q^j}\right) \leq Q_{dec,d_j} \leq A^j_{d_j}\left(\frac{q-1}{q^j}\right) + \binom{n}{d_j}\left(1 - \frac{1}{q^{j-1}}\right), \tag{5.2}$$

para todo $j \in [\![s,k]\!]$. Substituindo (5.1) em (5.2), temos que os limitantes inferiores e superiores coincidem. Logo obtemos a igualdade

$$Q_{dec,r} = \binom{n}{r}\left(1 - \frac{1}{q^{r-n+k}}\right) \tag{5.3}$$

para todo $r \in [\![d_s, d_k]\!]$. Por outro lado, ainda pelo Teorema 4.2.2

$$A^j_{d_j} \leq Q_{err,d_j} \leq \binom{n}{d_j}, \tag{5.4}$$

para todo $j \in [\![2,k]\!]$. Logo, se $s \geq 2$, substituindo (5.1) em (5.4), novamente os limitantes inferiores e superiores coincidem e, portanto, temos

$$Q_{err,r} = \binom{n}{r}, \tag{5.5}$$

para todo $r \in [\![d_s, d_k]\!]$. Caso $s = 1$, pelo Teorema 4.2.2 e pela expressão (5.1)

$$Q_{err,d_1} = |\Phi_1| = A^1_{d_1} = \binom{n}{d_1}, \tag{5.6}$$

concluindo assim a demonstração. □

O corolário 5.1.2 é conhecido na literatura [11].

Corolário 5.1.2 *Seja C um $[n,k,d_1,\ldots,d_k]_q$-código MDS. Então*

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

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

Demonstração
Pelo Teorema da Monotonicidade de Wei, lembrando que C é um código MDS e, portanto, $d_1(C) = n-k+1$, segue que $d_i = n-k+i$, para todo $i \in [\![k]\!]$, isto é, C é um código $\mathcal{P}_1$-MDS. Da expressão (4.9) e do Teorema 5.1.1 segue o resultado. □

Observe que o item (b) do Corolário 5.1.2 é encontrado em [11].

5.2 Expressões exatas para códigos AMDS

Determinamos nessa seção expressões exatas para as probabilidades de erro de códigos AMDS.

Lema 5.2.1 *Seja C um $[n,k]_q$-código. Então*

$$\begin{aligned} Q_{dec,d_k} &= 1 - \frac{1}{q^k}; \\ Q_{err,d_k} &= 1; \\ Q_{dec,d_1} &= A^1_{d_1}\left(1 - \frac{1}{q}, \right); \\ Q_{err,d_1} &= A^1_{d_1}. \end{aligned}$$

Demonstração
Como $d_k = n$, temos que $A^k_{d_k} = 1$. Pelo Teorema 4.2.2, $Q_{dec,d_k} = 1 - q^{-k}$ e $Q_{err,d_k} = 1$, pois os limitantes superiores e inferiores coincidem $i = k$. Para calcular Q_{dec,d_1} basta substituir $i = 1$ nos limitantes inferiores e superiores dados pelo Teorema 4.2.2 e notar que eles também coincidem. □

Denotamos por

$$a_i(r) = |\{H \subseteq [\![n]\!]; \dim([0]_H) = i \text{ e } |H| = r\}|. \tag{5.7}$$

Podemos então reescrever os coeficientes $Q_{*,r}$ como se segue

$$Q_{dec,r} = \sum_{i=0}^{k} a_i(r)\left(1 - \frac{1}{q^i}\right) \tag{5.8}$$

e

$$Q_{err,r} = \sum_{i=1}^{k} a_i(r). \tag{5.9}$$

Assim, estudamos $Q_{*,r}$ a partir dos coeficientes $a_i(r)$. Observamos antes de tudo que

$$\sum_{i=0}^{k} a_i(r) = \binom{n}{r}. \tag{5.10}$$

Lema 5.2.2 *Seja C um $[n,k]_q$-código. Então $a_i(r) = 0$, para todo $r < d_i$, e $a_i(d_i) = A^i_{d_i}$.*

Demonstração
Pelo Lema 4.1.2 temos que $|\Phi_i| = A^i_{d_i}$. Seja

$$B = \{H \subseteq [\![n]\!]; \dim [0]_H = i \text{ e } |H| = d_i\}.$$

Observe que $|B| = a_i(d_i)$. Vamos demonstrar que $B = \Phi_i$. tal Seja $H \subseteq [\![n]\!]$ com $\dim([0]_H) = i$ e $|H| = d_i$. Basta provar que $supp([0]_H) = H$. Sabemos que $supp([0]_H) \subseteq H$. Suponha por absurdo que $|supp([0]_H)| < |H|$, então $\dim([0]_H) = i$ e $|supp([0]_H)| < |H| \leq d_i - 1$, uma contradição. Logo $supp([0]_H) = H$ e, portanto, $a_i(d_i) = A^i_{d_i}$.

Suponha por aburdo agora $t > 0$. Se, por absurdo, $a_i(d_i - t) > 0$, temos que existe $H \subseteq [\![n]\!]$ com $|H| = d_i - t$ e $\dim([0]_H) = i$. Mas $supp([0]_H) \subseteq H$ e, portanto, $d_i - t = |H| \geq |supp([0]_H)| \geq d_i$. Absudo. Portanto $a_i(d_i - t) = 0$, ou seja, $a_i(r) = 0$, para $r < d_i$. □

Continuamos a estudar os coeficientes $a_i(r)$. Para uma melhor visualização dos resultados que se seguem, consideramos a matriz $(n+1) \times (k+1)$ em que a entrada na i-ésima coluna e r-ésima linha é dada por $a_{i-1}(r-1)$.

O Lema 5.2.2 diz que todos os elementos acima das posições (i, d_i), $i \in [\![k]\!]$ da matriz $a_i(r)$ também são nulos e $a_i(d_i) = A^i_{d_i}$. As entradas em azul da matriz $a_i(r)$ abaixo foram calculadas utilizando o Lema 5.2.2.

Na matriz abaixo, as entradas em verde foram estabelecidas utilizando o Lema 5.2.5.

A soma das entradas da j-ésima linha da matriz $a_i(r)$ é igual a $\binom{n}{j-1}$ pela expressão (5.10). Logo as entradas em vermelho são completamente determinadas por essa expressão.

Note que quanto maior d_1, menor a parte a ser determinada da matriz $a_i(r)$.

$$\begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
\binom{n}{d_1-1} & 0 & 0 & \cdots & 0 & 0 & 0 \\
\binom{n}{d_1} - A^1_{d_1} & A^1_{d_1} & 0 & \cdots & 0 & 0 & 0 \\
a_0(d_1+1) & a_1(d_1+1) & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
a_0(d_2-1) & a_1(d_2-1) & 0 & \cdots & 0 & 0 & 0 \\
a_0(d_2) & a_1(d_2) & A^2_{d_2} & \cdots & 0 & 0 & 0 \\
a_0(d_2+1) & a_1(d_2+1) & a_2(d_2+1) & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
a_0(d_{k-2}-1) & a_1(d_{k-2}-1) & a_2(d_{k-2}-1) & \cdots & 0 & 0 & 0 \\
a_0(d_{k-2}) & a_1(d_{k-2}) & a_2(d_{k-2}) & \cdots & A^{k-2}_{d_{k-2}} & 0 & 0 \\
a_0(d_{k-2}+1) & a_1(d_{k-2}+1) & a_2(d_{k-2}+1) & \cdots & a_{k-2}(d_{k-2}+1) & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
a_0(d_{k-1}-1) & a_1(d_{k-1}-1) & a_2(d_{k-1}-1) & \cdots & a_{k-2}(d_{k-1}-1) & 0 & 0 \\
a_0(d_{k-1}) & a_1(d_{k-1}) & a_2(d_{k-1}) & \cdots & a_{k-2}(d_{k-1}) & A^{k-1}_{d_{k-1}} & 0 \\
a_0(d_{k-1}+1) & a_1(d_{k-1}+1) & a_2(d_{k-1}+1) & \cdots & a_{k-2}(d_{k-1}+1) & a_{k-1}(d_{k-1}+1) & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
a_0(n-k) & a_1(n-k) & a_2(n-k) & \cdots & a_{k-2}(n-k) & a_{k-1}(n-k) & 0 \\
0 & a_1(n-k+1) & a_2(n-k+1) & \cdots & a_{k-2}(n-k+1) & a_{k-1}(n-k+1) & 0 \\
0 & 0 & a_2(n-k+2) & & a_{k-2}(n-k+2) & a_{k-1}(n-k+2) & 0 \\
0 & 0 & 0 & & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & a_{k-2}(n-2) & a_{k-1}(n-2) & 0 \\
0 & 0 & 0 & \cdots & 0 & n & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & A^k_{d_k}
\end{pmatrix}$$

O Lema 5.2.5 será consequência da seguinte da próxima posição.

Proposição 5.2.3 *Seja C um $[n,k]_q$-código, $H \subsetneq [\![n]\!]$ com cardinalidade r e $i = \dim([0]_H)$. Então*

$$\dim([0]_{H\cup\{j\}}) \geq \max(k+r+1-n, i), \tag{5.11}$$

para todo $j \in [\![n]\!] \setminus H$.

Demonstração
Denotamos $R = H \cup \{j\}$. Pela Proposição 3.2.6, $[0]_R = \ker(\pi_{\bar{R}})$. Identificando

$$\pi_{\bar{R}} = \pi_{\{\bar{j}\}} \circ \pi_{\bar{H}} \tag{5.12}$$

considerando a composição de funções

$$\begin{array}{ccccc}
C & \xrightarrow{\pi_{\bar{H}}} & \mathbb{F}_q^{n-r} & \xrightarrow{\pi_{\{\bar{j}\}}} & \mathbb{F}_q^{n-r-1} \\
\sum_{s\in[n]} c_s e_s & \longmapsto & \sum_{s\in\bar{H}} c_s e_s & \longmapsto & \sum_{s\in\bar{R}} c_s e_s,
\end{array}$$

pelo Teorema do Núcleo e Imagem segue

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

isto é,

$$\dim[0]_R = k - \dim(Im(\pi_{\bar{R}})). \tag{5.13}$$

Mas, pela expressão (5.12)

$$\dim(Im(\pi_{\bar{R}})) \leq \min(\dim(Im(\pi_{\bar{H}})), \dim(Im(\pi_{\{\bar{j}\}}))). \tag{5.14}$$

Como $\pi_{\{\bar{j}\}}$ é a projeção de $\mathbb{F}_q^{n-r}$ em $\mathbb{F}_q^{n-r-1}$ coordenadas,

$$\dim(Im(\pi_{\{\bar{j}\}})) = n - r - 1 \tag{5.15}$$

e, como $\dim([0]_H) = \dim(\ker(\pi_{\bar{H}}))$, temos que

$$\dim(Im(\pi_{\bar{H}})) = \dim(C) - \dim(\ker(\pi_{\bar{H}})) = k - i. \tag{5.16}$$

Segue de (5.14), (5.15) e (5.16) que

$$\dim(Im(\pi_{\bar{R}})) \leq \min(k - i, n - r - 1). \tag{5.17}$$

De (5.13) e (5.17) temos

$$\dim([0]_R) \geq k - \min(k - i, n - r - 1) = \max(i, k + r + 1 - n). \tag{5.18}$$

□

Proposição 5.2.4 *Seja C um $[n,k]_q$-código linear. Se $H \subseteq [\![n]\!]$ com $|H| = r$, então $|[0]_H| \geq q^{k-n+r}$.*

Demonstração
Se $|H| = 0$, o resultado é trivial. Suponha que o resultado vale para $H \subseteq [\![n]\!]$ com $|H| \leq r$. Vamos mostrar que também vale para $J \subseteq [\![n]\!]$ com $|J| = r + 1$. Escrevendo $J = H \cup \{j\}$ com $|H| = r$ e $j \notin H$, pela Proposição 5.2.3 temos que

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

em que $i = \dim([0]_H)$. Mas pela hipótese de indução $i \geq k - n + r$, logo

$$\dim([0]_J) \geq \max(k + r + 1 - n, k - n + r) = k - n + (r + 1).$$

□

Lema 5.2.5 *Dado um $[n,k]_q$-código C, então $a_i(r) = 0$, sempre que $r \geq n-k+i+1$.*

Demonstração
Suponha por absurdo que exista $H \subseteq [\![n]\!]$ com $|H| = r$, $\dim([0]_H) = i$ e $r \geq n-k+i+1$. Se $H = [\![n]\!]$, então temos $r = n$ e $i = k$, não satisfazendo a hipótese. Logo, $H \subsetneq [\![n]\!]$. Seja $j \in [\![n]\!] \setminus H$. Pela Proposição 5.2.3

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

Como $r \geq n-k+i+1$, então $r+k+1-n \geq i+2 > i$. Assim

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

Daí, $[0]_{H\cup\{j\}}$ contém um subconjunto D de dimensão $i+2$. Pelo Lema 4.1.1 existe um subcódigo $\tilde{D} \subseteq D$ tal que $\dim(\tilde{D}) = i+1$ e $supp(\tilde{D}) \subseteq H$. Mas $\tilde{D} \subseteq [0]_H$ e $\dim([0]_H) = i$, uma contradição. Portanto não existe $H \subseteq [\![n]\!]$ tal que $|H| = r$ e $\dim([0]_H) = i$. Segue que $a_i(r) = 0$. □

Corolário 5.2.6 *Seja C um $[n,k]_q$-código. Então os coeficientes $a_i(n-1)$ são todos nulos, para $i \neq k-1$, e $a_{k-1}(n-1) = n$.*

Demonstração
Pelo Lema 5.2.5, tomando $r = n-1 = n-k+(k-1)$, se $i < k-1$, então $a_i(n-1) = 0$. Também, pelo Lema 5.2.2, temos $a_k(n-1) = a_k(d_k - 1) = 0$. Pela expressão (5.10)

$$\sum_{i=0}^{k} a_i(n-1) = \binom{n}{n-1},$$

e, portanto, temos que $a_{k-1}(n-1) = n$, pois esta é a única parcela não nula do somatório acima. □

Códigos AMDS tem a probabilidade de erro de decodificação e de ocorrência de ambiguidade inteiramente determinadas pelos Lemas 5.2.2 e 5.2.5. O Exemplo 5.2.7 ilustra a aplicação desses lemas para o $[7,4]_2$-código de Hamming.

Exemplo 5.2.7 *Consideremos o código $C = HAM(7,4)_2$, isto é, o código $C \subseteq \mathbb{F}_2^n$ de matriz geradora G dada por*

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

Temos que a hierarquia de pesos de C é

d_1	d_2	d_3	d_4
3	*5*	*6*	*7*

Pelo Teorema 2.5.1*, calculamos $A^i_{d_i}$, para $i = 2, 3, 4$. Por ser um código de dimensão pequena $A^1_{d_1}$ pode ser calculado simplesmente contando as palavras de peso d_1 de C. Assim*

A^0_0	$A^1_{d_1}$	$A^2_{d_2}$	$A^3_{d_3}$	$A^4_{d_4}$
1	*7*	*21*	*7*	*1*

Dispondo os coeficientes $a_i(r)$ em um matriz na forma

$$a_i(r) = \begin{pmatrix} a_0(0) & a_1(0) & a_2(0) & a_3(0) & a_4(0) \\ a_0(1) & a_1(1) & a_2(1) & a_3(1) & a_4(1) \\ a_0(2) & a_1(2) & a_2(2) & a_3(2) & a_4(2) \\ a_0(3) & a_1(3) & a_2(3) & a_3(3) & a_4(3) \\ a_0(4) & a_1(4) & a_2(4) & a_3(4) & a_4(4) \\ a_0(5) & a_1(5) & a_2(5) & a_3(5) & a_4(5) \\ a_0(6) & a_1(6) & a_2(6) & a_3(6) & a_4(6) \\ a_0(7) & a_1(7) & a_2(7) & a_3(7) & a_1(7) \end{pmatrix}.$$

Pelos Lemas 5.2.2 *e* 5.2.5*, tendo em mente que a Hierarquia de pesos de C é $\{3, 5, 6, 7\}$ temos*

$$a_i(r) = \begin{pmatrix} a_0(0) & 0 & 0 & 0 & 0 \\ a_0(1) & 0 & 0 & 0 & 0 \\ a_0(2) & 0 & 0 & 0 & 0 \\ a_0(3) & A^1_3 & 0 & 0 & 0 \\ 0 & a_1(4) & 0 & 0 & 0 \\ 0 & 0 & A^5_2 & 0 & 0 \\ 0 & 0 & 0 & A^3_6 & 0 \\ 0 & 0 & 0 & 0 & A^4_7 \end{pmatrix}.$$

Note que a soma dos coeficientes da j-ésima linha da matriz $a_i(r)$ é $\binom{n}{j-1}$ e $A^1_3 = 7$. Assim, obtemos todos os coeficientes $a_i(r)$ para $i \in [\![0, 4]\!]$ e $r \in [\![0, 7]\!]$, a saber

$$a_i(r) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 7 & 0 & 0 & 0 & 0 \\ 21 & 0 & 0 & 0 & 0 \\ 28 & 7 & 0 & 0 & 0 \\ 0 & 35 & 0 & 0 & 0 \\ 0 & 0 & 21 & 0 & 0 \\ 0 & 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Mas, como

$$\begin{aligned} Q_{dec,r} &= \sum_{i=0}^{k} a_i(r)\left(1-\frac{1}{q^i}\right); \\ Q_{err,r} &= \sum_{i=1}^{k} a_i(r). \end{aligned}$$

e $P_*(C) = \sum_{r=0}^{n} Q_{*,r}\mathrm{p}^r(1-\mathrm{p})^{n-r}$, *temos que*

$$P_{err}(C) = 7\mathrm{p}^3(1-\mathrm{p})^4 + 35\mathrm{p}^4(1-\mathrm{p})^3 + 21\mathrm{p}^5(1-\mathrm{p})^2 + 7\mathrm{p}^6(1-\mathrm{p})^1 + \mathrm{p}^7.$$

e

$$\begin{aligned} P_{dec}(C) &= 7\left(1-\frac{1}{2}\right)\mathrm{p}^3(1-\mathrm{p})^4 + 35\left(1-\frac{1}{2}\right)\mathrm{p}^4(1-\mathrm{p})^3 \\ &+ 21\left(1-\frac{1}{4}\right)\mathrm{p}^5(1-\mathrm{p})^2 + 7\left(1-\frac{1}{8}\right)\mathrm{p}^6(1-\mathrm{p})^1 + \left(1-\frac{1}{16}\right)\mathrm{p}^7. \end{aligned}$$

Note que no caso do Exemplo 5.2.7 os resultados obtidos determinam a probabilidade de erro exata do código. Mostramos que podemos sempre obter exatamente P_* se C é um $[n,k]_q$-código com $\{d_i; i \in [\![k]\!]\} \subseteq [\![n-k, n]\!]$, isto é, C é um código MDS ou um código quase MDS. A prova desta afirmação é consequência direta do Corolário 5.1.2 e do Teorema 5.2.8.

A idéia da demonstração do Teorema 5.2.8 é a mesma usada para calcular $P_*(C)$ no Exemplo 5.2.7. A demonstração do caso geral, no entanto, é extensa e técnica, porém, tendo em mente a representação matricial dos coeficientes $a_i(r)$, podemos acompanhar facilmente todos os passos.

Teorema 5.2.8 *Dado um* $[n,k]_q$*-código* C *com* $d_1 = n-k$, *então*

$$P_{err}(C) = A^1_{n-k}\mathrm{p}^{n-k}(1-\mathrm{p})^k + \sum_{i=1}^{n}\binom{n}{n-k+i}\mathrm{p}^{n-k+i}(1-\mathrm{p})^{k-i} \quad (5.19)\ (5.20)$$

e

$$P_{dec}(C) = \sum_{i=0}^{s-2} A_{n-k+i}^{i+1} \left(\frac{q-1}{q^{i+1}}\right) \mathtt{p}^{n-k+i}(1-\mathtt{p})^{k-i} + \sum_{i=0}^{k} \binom{n}{n-k+i} \left(1-\frac{1}{q^i}\right) \mathtt{p}^{n-k+i}(1-\mathtt{p})^{k-i}, \tag{5.21}$$

em que $s \in [\![k]\!]$ é tomado de forma que C seja $\mathcal{P}_s$-MDS.

Demonstração
Seja $s \in [\![k]\!]$ tal que C seja um código $\mathcal{P}_s$-MDS. Note que, como $d_1 \neq n-k+1$, então C não é 1-MDS. Logo $s > 1$.

O Teorema 5.1.1 determina $Q_{*,r}$, para todo $r \in [\![d_s, n]\!]$, a saber

$$Q_{err,r} = \binom{n}{r} \tag{5.22}$$

e

$$Q_{dec,r} = \binom{n}{r}\left(1-\frac{1}{q^{r-n-k}}\right) \tag{5.23}$$

Vamos determinar esses coeficientes para $r \in [\![0, d_s-1]\!]$. Pelo Lema 4.2.1,

$$Q_{*,r} = 0, \text{ para todo } r \in [\![0, d_1-1]\!]. \tag{5.24}$$

Dessa forma precisamos apenas dos coeficientes $Q_{*,r}$ com $r \in [\![d_1, d_s-1]\!]$.

1º Caso: $r = d_s - 1$

Fixe $r = d_s - 1$. Então $Q_{*,r}$ dependem dos coeficientes $a_i(r)$, para todo $i \in [\![0,k]\!]$. Pelo Teorema da Monotonicidade de Wei, como $d_1 = n-k$, segue que

$$d_i = n-k+i-1, \text{ se } i \in [\![1, s-1]\!]$$

e

$$d_i = n-k+i, \text{ se } i \in [\![s,k]\!].$$

Se $r = d_s - 1$, temos que $r < n-k+s \leq n-k+i = d_i$, para todo $i \geq s$. Pelo Lema 5.2.2 temos que

$$a_i(d_s-1) = 0, \text{ para todo } i \geq s. \tag{5.25}$$

Por outro lado, se $r = d_s - 1$, então $r = n-k+s-1 \geq n-k+i+1$, para todo $i \leq s-2$. Pelo Lema 5.2.5 segue que

$$a_i(d_s-1) = 0, \text{ para todo } i \leq s-2. \tag{5.26}$$

Pelas expressões (5.10), (5.25) e (5.26), temos que

$$a_{s-1}(d_s-1)=\binom{n}{d_s-1} \text{ e } a_i(d_s-1)=0,\ \forall i\neq s-1.$$

e, das expressões (5.9) e (5.8), segue que

$$Q_{err,d_s-1}=\binom{n}{d_s-1} \tag{5.27}$$

e

$$Q_{dec,d_s-1}=\binom{n}{d_s-1}\left(1-\frac{1}{q^{s-1}}\right). \tag{5.28}$$

2º Caso: $r\in[\![d_1,d_s-2]\!]$

Como $d_1=n-k$ e $d_s-2=d_{s-1}$, então

$$|[\![d_1,d_s-2]\!]|=(n-k+s-2)-(n-k)+1=s-1. \tag{5.29}$$

Logo pela equação (5.29) e, novamente, pelo Teorema da Monotonicidade de Wei, temos

$$[\![d_1,d_s-2]\!]=\{d_i;i\in[\![s-1]\!]\}.$$

Daí, se $r\in[\![d_1,d_s-2]\!]$, então $r=d_t$, para algum $t\in[\![s-1]\!]$. Seja $r=d_t$, com $t\in[\![s-1]\!]$. Vamos agora determinar $a_i(r)=a_i(d_t)$ para todo $i\in[\![k]\!]$. Para isso dividimos em subcasos:

1º Subcaso do 2º Caso: $i\geq t+1$.

Pelo Teorema da monotonicidade de Wei $d_i>d_t=r$, para todo $i\in[\![t+1,k]\!]$. Logo, pelo Lema 5.2.2, segue que

$$a_i(r)=0 \text{ para todo } i\in[\![t+1,k]\!]. \tag{5.30}$$

2º Subcaso do 2º Caso: $i\leq t-2$.

Se $i\in[\![t-2]\!]$, então $i\leq t-2$, logo $d_i\leq d_{t-2}=d_t-2=r-2$. Segue que $r\geq d_i+2$, isto é, $r\geq n-k+i+1$. Logo, temos que

$$a_i(r)=0,\ \text{para todo } i\in[\![t-2]\!]. \tag{5.31}$$

3º Subcaso do 2º Caso: $i=t$.

Se $r=d_t$ e $i=t$, para algum $t\in[\![s-1]\!]$, pelo Lema 5.2.2 segue que

$$a_i(r)=A^t_{d_t},\ i=t. \tag{5.32}$$

4º Subcaso do 2º Caso: $i = t-1$.

Pelo somatório (5.10) e pelas expressões (5.30), (5.31) e (5.32) temos que

$$a_{t-1}(d_t) = \binom{n}{d_t} - A^t_{d_t}, \text{ para todo } t \in [\![t-1]\!]. \tag{5.33}$$

Se $r \in [\![d_1, d_s - 2]\!]$, das expressões (5.9) e (5.8), substituindo $r = d_t = n-k+t-1$ nas expressões (5.30), (5.31), (5.32) e (5.33), segue que

$$Q_{err,r} = \binom{n}{r}, \text{ se } r \in [\![d_1+1, d_s-2[\![\tag{5.34}$$

e

$$Q_{err,r} = A^1_{d_1}, \text{ se } r = d_1 \tag{5.35}$$

e

$$Q_{dec,r} = A^{r-n+k+1}_r \left(1 - \frac{1}{q^{r-n+k+1}}\right) + \left(\binom{n}{r} - A^{r-n+k+1}_r\right)\left(1 - \frac{1}{q^{r-n+k}}\right). \tag{5.36}$$

que reescrita fica

$$Q_{dec,r} = A^{r-n+k+1}_r \frac{q-1}{q^{r-n+k+1}} + \binom{n}{r}\left(1 - \frac{1}{q^{r-n+k}}\right). \tag{5.37}$$

As expressões (5.24), (5.22), (5.23), (5.27), (5.28), (5.34), (5.35) e (5.37) são resumidas nas tabelas a seguir

r	$Q_{err,r}$	Equação
$[\![0, d_1-1]\!]$	0	(5.24)
d_1	A^1_{n-k}	(5.34)
$[\![d_1+1, d_s-2]\!]$	$\binom{n}{r}$	(5.35)
d_s-1	$\binom{n}{r}$	(5.27)
$[\![d_s, n]\!]$	$\binom{n}{r}$	(5.22)

e

r	$Q_{dec,r}$	Equação
$[\![0, d_1-1]\!]$	0	(5.24)
$[\![d_1, d_s-2]\!]$	$A^{r-n+k+1}_r \frac{q-1}{q^{r-n+k+1}} + \binom{n}{r}\left(1 - \frac{1}{q^{r-n+k}}\right)$	(5.37)
d_s-1	$\binom{n}{r}\left(1 - \frac{1}{q^{s-1}}\right)$	(5.28)
$[\![d_s, n]\!]$	$\binom{n}{r}\left(1 - \frac{1}{q^{r-n+k}}\right)$	(5.23)

Reescrevendo a expressão (4.3) como segue

$$\begin{aligned} P_{dec}(C) = \quad & \textstyle\sum_{r=0}^{d_1-1} Q_{dec,r}\mathtt{p}^r(1-\mathtt{p})^{n-r} + \\ & \textstyle\sum_{r=d_1}^{d_s-2} Q_{dec,r}\mathtt{p}^r(1-\mathtt{p})^{n-r} + \\ & Q_{dec,d_s-1}\mathtt{p}^{d_s-1}(1-\mathtt{p})^{n-d_s+1} + \\ & \textstyle\sum_{r=d_s}^{d_k} Q_{dec,r}\mathtt{p}^r(1-\mathtt{p})^{n-r}. \end{aligned}$$

Lembrando que $d_s - 1 = n - k + s - 1$ e substituindo os valores apresentados na segunda tabela temos

$$\begin{aligned} P_{dec}(C) = \quad & \textstyle\sum_{r=d_1}^{n-k+s-2} A_r^{r-n+k+1}\left(\frac{q-1}{q^{r-n+k+1}}\right)\mathtt{p}^r(1-\mathtt{p})^{n-r} + \\ & \textstyle\sum_{r=d_1}^{n-k+s-2}\binom{n}{r}\left(1-\frac{1}{q^{r-n+k}}\right)\mathtt{p}^r(1-\mathtt{p})^{n-r} + \\ & \textstyle\binom{n}{n-k+s-1}\left(1-\frac{1}{q^{s-1}}\right)\mathtt{p}^{n-k+s-1}(1-\mathtt{p})^{k-s+1} + \\ & \textstyle\sum_{r=d_s}^{d_k}\binom{n}{r}\left(1-\frac{1}{q^{r-n+k}}\right)\mathtt{p}^r(1-\mathtt{p})^{n-r}. \end{aligned}$$

Fazendo a mudança de índice $i = r - d_1 = r - n + k$ temos

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

que, após um agrupamento de termos, temos

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

Analogamente, para determinar P_{err}, escrevemos a expressão (4.3) da seguinte forma

$$\begin{aligned} P_{err}(C) = \quad & \textstyle\sum_{r=0}^{d_1-1} Q_{err,r}\mathtt{p}^r(1-\mathtt{p})^{n-r} + \\ & Q_{err,d_1}\mathtt{p}^{d_1}(1-\mathtt{p})^{n-d_1} + \\ & \textstyle\sum_{r=d_1+1}^{n} Q_{err,r}\mathtt{p}^r(1-\mathtt{p})^{n-r}. \end{aligned}$$

Substituindo os valores da segunda tabela que aparece na demonstração deste teorema obtemos

$$\begin{aligned} P_{err}(C) = \quad & A^1_{n-k}\mathtt{p}^{n-k}(1-\mathtt{p})^k + \\ & \textstyle\sum_{r=d_1+1}^{n}\binom{n}{r}\mathtt{p}^r(1-\mathtt{p})^{n-r}. \end{aligned}$$

Fazendo a mudança de índices $i = r - d_1$ segue que

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

como no enunciado. □

Vamos agora estudar as fórmulas obtidas no Teorema 5.2.8.

Corolário 5.2.9 *Sejam C_1 e C_2 dois $[n,k]_q$-códigos AMDS e suponha $A^1_{d_1}(C_1) = A^1_{d_1}(C_2)$. Então, temos que $P_{err}(C_1) = P_{err}(C_2)$.*

Demonstração
A expressão (5.19) do Teorema 5.2.8 depende apenas de n, k e $A^1_{d_1}$, portanto $P_{err}(C_1) = P_{err}(C_2)$. □

Corolário 5.2.10 *Sejam C_1 e C_2 dois $[n,k]_q$-códigos satisfazendo $d_1(C_1) = d_1(C_2) = n-k$ e $A^1_{d_1}(C_1) > A^1_{d_1}(C_2)$. Então, temos que $P_{err}(C_1) > P_{err}(C_2)$.*

Demonstração
Segue direto da expressão (5.19) do Teorema 5.2.8. □

Proposição 5.2.11 *Sejam C_1 e C_2 $[n,k]_q$-códigos com $d_i(C_1) = d_i(C_2) = n-k+i-1$ e $A^i_{d_i}(C_1) = A^i_{d_i}(C_2)$ para todo $i \in [\![s-1]\!]$. Se C_1 é $\mathcal{P}_s$-MDS e C_2 é $\mathcal{P}_{s+1}$-MDS, então $P_{dec}(C_1) < P_{dec}(C_2)$.*

Demonstração
Da expressão (5.21) temos que

$$\begin{aligned} P_{dec}(C_2) - P_{dec}(C_1) = \quad & A^s_{d_s}(C_2)\left(1-\tfrac{1}{q^s}\right)\mathtt{p}^{d_s}(1-\mathtt{p})^{n-d_s} \\ & -A^s_{d_s}(C_2)\left(1-\tfrac{1}{q^{s-1}}\right)\mathtt{p}^{d_s}(1-\mathtt{p})^{n-d_s}, \end{aligned}$$

que podemos reescrever da forma

$$P_{dec}(C_2) - P_{dec}(C_1) = A^s_{d_s}(C_2)\left(\frac{q-1}{q^s}\right)\mathtt{p}^{d_s}(1-\mathtt{p})^{n-d_s} > 0.$$

□

Da Proposição 5.2.11, conclui-se que, dentre todos os $[n,k]_q$-códigos AMDS com mesmo $A^1_{d_1}$, os NMDS são os com menor probabilidade de erro de decodificação.

Consequentemente, o segundo peso generalizado de Hamming tem uma importância fundamental quando buscamos encontrar códigos que minimizam a probabilidade de erro de decodificação.

Capítulo 6

P_* para $\mathtt{p}$ suficientemente pequeno

Em [11], Fashandi, Gharan e Khandani provaram que os códigos MDS atingem as probabilidades de erro de decodificação mínimas, fixados parâmetros nos quais existam tais códigos. Nessa seção, mostramos que fixados comprimento n e dimensão k nos quais existam $[n,k]_q$-códigos AMDS, mas não existam $[n,k]_q$-códigos MDS, os AMDS atigem as probabilidades mínimas de erro de decodificação e ocorrêcia de ambiguidade para $\mathtt{p}$ suficientemente pequeno. Os $[n,k]_q$-códigos AMDS com primeiro espectro generalizado de suporte d_1 mínimo, minimizam P_*. Se existirem mais de um $[n,k]_q$-código AMDS satisfazendo essa condição de minimalidade os códigos AMDS com maior segundo peso generalizado minimizam P_* para $\mathtt{p}$ é suficientemente pequeno. Os resultados aqui apresentados seguem imediatamente das proposições do Capítulo 5 considerando limites quando $\mathtt{p}$ tende a zero e utilizando argumentos padrões de continuidade.

Proposição 6.0.12 *Sejam C_1 e C_2 $[n,k]_q$-códigos. Se $d_1(C_1) > d_1(C_2)$, então $P_*(C_1) < P_*(C_2)$ para $\mathtt{p}$ suficientemente pequeno.*

Demonstração

Vamos calcular o limite

$$\lim_{\mathtt{p}\to 0} \frac{P_*(C_1)}{P_*(C_2)} = \lim_{\mathtt{p}\to 0} \frac{\sum_{i=d_1(C_1)}^{n} Q_{*,i}(C_1)\mathtt{p}^i(1-\mathtt{p})^{n-i}}{\sum_{i=d_1(C_2)}^{n} Q_{*,i}(C_2)\mathtt{p}^i(1-\mathtt{p})^{n-i}}.$$

Colocando $(1-\mathtt{p})^n$ em evidência em ambos somatórios temos

$$\lim_{\mathtt{p}\to 0}\frac{P_*(C_1)}{P_*(C_2)}=\lim_{\mathtt{p}\to 0}\frac{(1-\mathtt{p})^n\sum_{i=d_1(C_1)}^{n}Q_{*,i}(C_1)\mathtt{p}^i(1-\mathtt{p})^{-i}}{(1-\mathtt{p})^n\sum_{i=d_1(C_2)}^{n}Q_{*,i}(C_2)\mathtt{p}^i(1-\mathtt{p})^{-i}},$$

dividindo numerador e denominador por $(1-\mathtt{p})^n$ obtemos

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

Fazendo a mudança de variável $x=\frac{\mathtt{p}}{(1-\mathtt{p})}$ e observando que, como $\mathtt{p}$ tende a zero, x tende a zero, obtemos

$$\lim_{x\to 0}\frac{P_*(C_1)}{P_*(C_2)}=\lim_{x\to 0}\frac{\sum_{i=d_1(C_1)}^{n}Q_{*,i}(C_1)x^i}{\sum_{i=d_1(C_2)}^{n}Q_{*,i}(C_2)x^i}. \tag{6.1}$$

Por hipótese, $d_1(C_1)>d_1(C_2)$, dividindo o numerador e o denominador por $x^{d_1(C_2)}$ e aplicando o limite, temos

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

Segue que $P_*(C_1)<P_*(C_2)$ para $\mathtt{p}$ suficientemente pequeno. □

A Proposição 6.0.12 garante que para $\mathtt{p}$ suficientemente pequeno, o primeiro peso é o que determina a probabilidade de erro.

Dessa forma dados comprimento n e dimensão k em que existam códigos MDS, se C é um $[n,k]_q$-código que minimiza P_*, então C é MDS. Obtemos como consequência uma nova demonstração para o fato já conhecido e demonstrado em [11]. Observamos no entanto que são raros os parâmetros $[n,k]$ sobre os quais existem códigos MDS. Por exemplo, se $q=2$ e C é um $[n,k]_q$-código MDS, então C é trivial, isto é, ou C é o espaço todo, ou C é código de Repetição, isto é, $C=\langle(1,1,\ldots,1\rangle$, ou C é um dual destes dois códigos.

Assim em parâmetros nos quais não existem códigos MDS nos interessa procurar por códigos AMDS. Embora não exista classificação dos códigos AMDS, é possível encontrar na literatura diversos resultados que apresentam códigos AMDS ou parâmetros que garantem sua existência (ver por exemplo

[4]). Como estamos procurando códigos ótimos, pela Proposição 6.0.12, a distância mínima d_1 tem que ser a máxima possível, em outras palavras, buscamos $[n,k]_q$-códigos AMDS.

O teorema a seguir estabelece um critério de comparação entre códigos com mesma distância mínima.

Proposição 6.0.13 *Sejam C_1 e C_2 $[n,k]_q$-códigos, $k \neq 0$, com $d_1(C_1) = d_1(C_2)$. Se $Q_{*,d_1(C_1)} < Q_{*,d_1(C_2)}$, então $P_*(C_1) < P_*(C_2)$, para $\mathtt{p}$ suficientemente pequeno.*

Demonstração
Pela expressão (6.1), vimos que

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

Dividindo numerador e denominador por $x^{d_1(C_1)} = x^{d_1(C_2)}$ obtemos

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

logo

$$\lim_{x\to 0} \frac{P_*(C_1)}{P_*(C_2)} = \frac{Q_{*,d_1(C_1)}}{Q_{*,d_1(C_2)}} < 1.$$

e segue que $P_*(C_1) < P_*(C_2)$ para $\mathtt{p}$ suficientemente pequeno. □

Corolário 6.0.14 *Sejam C_1 e C_2 dois $[n,k]_q$-códigos com $d_1(C_1) = d_1(C_2)$. Então, para $\mathtt{p}$ suficientemente pequeno, temos que $P_*(C_1) < P_*(C_2)$ sempre que $A^1_{d_1}(C_1) < A^1_{d_1}(C_2)$.*

Demonstração
Segue diretamente do Lema 5.2.1 e da Proposição 6.0.13. □

Para finalizar, apenas a título de exemplo, utilizamos a Proposição 6.0.13 para determinar o $[7,3]_2$-código linear C que minimiza a probabilidade de ocorrência de ambiguidade $P_{err}(C)$ para $\mathtt{p}$ suficientemente pequeno.

Seja C um $[7,3]_2$-código linear que minimiza a probabilidade de ocorrência de ambiguidade $P_{err}(C)$ para $\mathtt{p}$ suficientemente pequeno. Pela Proposição 6.0.12, para encontrar C, primeiramente devemos maximizar d_1. Não é difícil ver que com esses parâmetros a máxima distância mínima possível é $d_1 = 3$.

Sejam respectivamente C_1, C_2 e C_3 os $[7,3,3]_2$-códigos lineares gerados pelas matrizes

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix},$$

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

e

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Então, a menos de equivalência, estes são os únicos $[7,3,3]_2$-códigos lineares que existem. Como $A^1_{d_1}(C_1) = 3$, $A^1_{d_1}(C_2) = 3$ e $A^1_{d_1}(C_3) = 2$, pelo Corolário 6.0.14, temos que C_3 é o melhor $[7,3]_2$-código, ou seja, C_3 minimiza $P_*(.)$ fixados comprimento $n = 7$, dimensão $k = 3$ e cardinalidade do alfabeto $q = 2$ para $\mathtt{p}$ suficientemente pequeno.

Em resumo, para obter $[n,k]_q$-códigos ótimos, isto é, $[n,k]_q$-códigos que minimizem as probabilidades de erro de decodificação e de ocorrência de ambiguidade, quando $\mathtt{p}$ é suficientemente pequeno, primeiro selecionamos todos $[n,k]_q$-códigos com a maior distância mínima possível, depois, dentre estes códigos, selecionamos os que possuem o menor número possível de palavras de peso mínimo.

Capítulo 7

Conclusões e perspectivas futuras

Considerando os invariantes, pesos generalizados e espectros generalizados, dos códigos lineares, melhora-se os limitantes conhecidos na literatura. Para isso, substitue-se os limitantes dados pelo Teorema 4.2.2 na expressão (4.3).

Os coeficientes $a_i(r)$ definidos na expressão (5.7) determinam completamente as probabilidades de erro de decodificação e de ocorrência de ambiguidade e, mais ainda, não dependem da probabilidade de erro do canal. Ao determinar limitantes ou expressões exatas para estes coeficientes, determinamos limitantes ou expressão exatas para as duas probabilidades P_{dec} e P_{amb} simultaneamente.

No Capítulo 6, é demonstrado que os coeficientes $Q_{*,r}$ de menor índice r na expressão 4.3 são os de maior peso no cálculo de P_* quando a probabilidade $\mathtt{p}$ do canal é suficientemente pequena. Portanto, maximizar a distância mínima reduz a probabilidade de erro de decodificação e de ocorrência de ambiguidade.

7.1 Perspectivas futuras

Listamos abaixo possíveis estudos que podem dar continuadade ao trabalho apresentado nesta tese:

(i) Generalizar o que foi feito (limitantes e expressões para as probabilidades de erro) considerando outros canais como, por exemplo, simétricos;

(ii) Caracterizar as probabilidades de erro de outros canais em termos da matriz dos coeficientes $a_i(r)$;

(iii) Encontrar limitantes para a probabilidade de erro de decodificação quando o decodificador não é MLD considerando os espectros e os pesos generalizados dos códigos;

(iv) Determinar relações entre a probabilidade $P_*(C)$ de um $[n,k]_q$-código em termos dos invariantes do código $C^\perp$ dual de C;

(vi) Determinar limitantes para os coeficientes $Q_{*,r}$ com $r \neq d_i$, $i \in [\![k]\!]$, para as probabilidades de erros de decodificação e de ocorrência de ambiguidade em canais de apagamento e outros canais.;

Anexo

Existem vinte e dois $[7,4]_2$-códigos a menos de equilavência com $d_4 = 7$. Abaixo representamos tais códigos pelas matrizes geradoras e os rotulamos para futuras referências:

$$C(7,4,1) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad C(7,4,5) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$C(7,4,2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad C(7,4,6) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$C(7,4,3) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad C(7,4,7) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$C(7,4,4) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad C(7,4,8) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$C(7,4,9) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad C(7,4,16) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$C(7,4,10) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \quad C(7,4,17) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$C(7,4,11) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad C(7,4,18) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$C(7,4,12) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad C(7,4,19) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$C(7,4,13) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad C(7,4,20) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$C(7,4,14) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \quad C(7,4,21) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$C(7,4,15) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \quad C(7,4,22) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Referências Bibliográficas

[1] K. A S Abdel-Ghaffar, *A lower bound on the undetected error probability of block codes*, Information Theory, 1995. Proceedings., 1995 IEEE International Symposium on, 1995, pp. 341–.

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

[3] A. Barbero and C. Munuera, *The weight hierarchy of hermitian codes*, SIAM Journal on Discrete Mathematics **13** (2000), no. 1, 79–104.

[4] Mario A. de Boer, *Almost mds codes*, Designs, Codes and Cryptography **9** (1996), no. 2, 143–155 (English).

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

[6] S.M Dodunekov and I.N Landjev, *Near-mds codes over some small fields*, Discrete Mathematics **213** (2000), no. 1-3, 55 – 65.

[7] Stefan Dodunekov and Ivan Landgev, *On near-mds codes*, Journal of Geometry **54** (1995), no. 1-2, 30–43 (English).

[8] R. Dodunekova and S.M. Dodunekov, *The mmd codes are proper for error detection*, Information Theory, IEEE Transactions on **48** (2002), no. 12, 3109–3111.

[9] R. Dodunekova, S.M. Dodunekov, and T. Klove, *Almost-mds and near-mds codes for error detection*, Information Theory, IEEE Transactions on **43** (1997), no. 1, 285–290.

[10] Steven T. Dougherty and T.Aaron Gulliver, *Higher weights and binary self-dual codes*, Electronic Notes in Discrete Mathematics **6** (2001), no. 0, 469 – 480, WCC2001, International Workshop on Coding and Cryptography.

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

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

[13] Hans Georg Schaathun, *The weight hierarchy of product codes*, Information Theory, IEEE Transactions on **46** (2000), no. 7, 2648–2651.

[14] Sudhir R. Ghorpade and Gilles Lachaud, *Higher weights of grassmann codes*, Coding Theory, Cryptography and Related Areas (Johannes Buchmann, Tom Hoholdt, Henning Stichtenoth, and Horacio Tapia-Recillas, eds.), Springer Berlin Heidelberg, 2000, pp. 122–131 (English).

[15] S. T. Douguerty; S. Han, *Higher weights and generalized mds codes*, J. Korean Math. Soc. **47** (2010), no. 6, 1167–1182.

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

[17] Tor Helleseth, Torleiv Kove, and Johannes Mykkeltveit, *The weight distribution of irreducible cyclic codes with block lengths n1((q1-1)n)*, Discrete Mathematics **18** (1977), no. 2, 179 – 211.

[18] J.W.P. Hirschfeld, M.A. Tsfasman, and S.G. Vladut, *The weight hierarchy of higher dimensional hermitian codes*, Information Theory, IEEE Transactions on **40** (1994), no. 1, 275–278.

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

[20] T. Klove and Jinquan Luo, *Upper bounds on the weight distribution function for some classes of linear codes*, Information Theory, IEEE Transactions on **58** (2012), no. 8, 5512–5521.

[21] Torleiv Klove, *Support weight distribution of linear codes*, Discrete Mathematics **106 - 107** (1992), no. 0, 311 – 316.

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

[23] H.G. Schaathun, *Duality and support weight distributions*, Information Theory, IEEE Transactions on **50** (2004), no. 5, 862–867.

[24] Juriaan Simonis, *The effective length of subcodes*, Applicable Algebra in Engineering, Communication and Computing **5** (1994), no. 6, 371–377 (English).

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

[26] M. Tsfasman and S. Vladut, *Geometric approach to higher weights*, Information Theory, IEEE Transactions on **41** (1995), no. 6, 1564–1588.

[27] A. Vardy, *The intractability of computing the minimum distance of a code*, Information Theory, IEEE Transactions on **43** (1997), no. 6, 1757–1766.

[28] V. K. Wei, *Generalized hamming weights for linear codes*, Information Theory, IEEE Transactions on **37** (1991), no. 5, 1412–1418.

[29] J.K. Wolf, A. Michelson, and A.H. Levesque, *On the probability of undetected error for linear block codes*, Communications, IEEE Transactions on **30** (1982), no. 2, 317–325.