UNIVERSIDADE ESTADUAL DE CAMPINAS
Instituto de Matemática, Estatística e Computação Científica

CHRISTIANE BUFFO RODRIGUES

Geometria do espaço dos canais binários assimétricos

CAMPINAS
2017

CHRISTIANE BUFFO RODRIGUES

Geometria do espaço dos canais binários assimétricos

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 Doutora em Matemática Aplicada.

Orientador: Prof. Dr. MARCELO FIRER

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELA ALUNA CHRISTIANE BUFFO RODRIGUES E ORIENTADA PELO PROF. DR. MARCELO FIRER.

CAMPINAS
2017

Agência(s) de fomento e nº(s) de processo(s): CNPq, 140368/2015-9; CAPES

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

R618g

Rodrigues, Christiane Buffo, 1983-
Geometria do espaço dos canais binários assimétricos / Christiane Buffo Rodrigues. – Campinas, SP : [s.n.], 2017.

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

1. Canal binário assimétrico. 2. Códigos corretores de erros (Teoria da informação). I. Firer, Marcelo,1961-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Geometry of the space of binary asymmetric channels
Palavras-chave em inglês:
Binary asymmetric channel
Error-correcting codes (Information theory)
Área de concentração: Matemática Aplicada
Titulação: Doutora em Matemática Aplicada
Banca examinadora:
Marcelo Firer [Orientador]
Sueli Irene Rodrigues Costa
Reginaldo Palazzo Junior
Eduardo Brandani da Silva
Giuliano Gadioli La Guardia
Data de defesa: 26-04-2017
Programa de Pós-Graduação: Matemática Aplicada

Tese de Doutorado defendida em 26 de abril de 2017 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). REGINALDO PALAZZO JUNIOR

Prof(a). Dr(a). EDUARDO BRANDANI DA SILVA

Prof(a). Dr(a). GIULIANO GADIOLI LA GUARDIA

A Ata da defesa com as respectivas assinaturas dos membros encontra-se no processo de vida acadêmica da aluna.

DEDICATÓRIA

Aos meus pais, Dimas e Enilze, e ao meu tio Messias (in memoriam) dedico este trabalho como agradecimento por toda a confiança, apoio e incentivo.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus por me dar a calma, a força e a coragem necessárias para seguir em frente sempre que surgiam as dificuldades e os imprevistos da vida. Aos meus pais, Dimas e Enilze, agradeço por todo o apoio, incentivo, compreensão e dedicação para me ajudar a me manter firme em meus objetivos e concluir mais essa etapa.

Aos demais familiares, amigos e colegas agradeço por todo o companheirismo e apoio de sempre.

Agradeço ao meu orientador Marcelo todo o apoio, paciência, confiança e, sobretudo, por sempre cultivar um bom diálogo ao longo destes 4 anos de trabalho. Certamente este período em que convivemos me trouxe muito aprendizado, muitas reflexões e muito amadurecimento pessoal e profissional.

Aos amigos do Laboratório de Matemática Discreta e Códigos, do IMECC-Unicamp, agradeço toda a ajuda, companheirismo e apoio ao longo deste período em que convivemos.

Agradeço ao CNPq e à CAPES, pelas bolsas de estudo concedidas durante o período de doutorado, e agradeço à FAPESP pelo apoio concedido por meio do Projeto Temático FAPESP - Segurança e Confiabilidade da Informação, sob processo de número 2013/25977-7.

RESUMO

Neste trabalho, estudamos a geometria do espaço dos canais binários assimétricos n-dimensionais. Devido à assimetria do problema, não é possível casar uma métrica aditiva a um canal binário assimétrico. No entanto, podemos manter a estrutura aditiva da distância e propor uma função orientada, conhecida na literatura como quasi-métrica. Neste sentido, todo canal binário assimétrico está associado a uma quasi-métrica através de uma relação que compara distâncias entre vetores com as probabilidades de erro do canal. Definimos de modo natural uma relação de equivalência entre canais binários assimétricos e o primeiro passo é a caracterização das classes de equivalência como cones do plano. A caracterização das classes de equivalência nos permitiu iniciar um estudo sobre invariantes quasi-métricos, distância mínima do código e raios de empacotamento e cobertura. Neste sentido, vimos que, para um dado código, estes invariantes quasi-métricos não são constantes e a maioria deles depende não apenas das classes de equivalência de canais e do código em questão, mas também da escolha de palavras código específicas, diferentemente do que ocorre no caso da métrica de Hamming (associada ao canal simétrico) ou qualquer outra métrica invariante por translação. Esta dependência nos leva a definição de sequências de raios de cobertura e empacotamento, que refinam o conceito usual.

Palavras-chave: Canal binário assimétrico. Códigos corretores de erros (Teoria da informação).

ABSTRACT

In this work, we study the geometry of the space of n-dimensional binary asymmetric channels. Since the problem is asymmetric, it is not possible to match an additive metric to a binary asymmetric channel. However, we can preserve the additive structure of the distance and propose an oriented function, known in the literature as quasi-metric. In this sense, every binary asymmetric channel is associated to a quasi-metric through a relation that compares distances between vectors with the channel error probabilities. We define in a natural way an equivalence relation between binary asymmetric channels and the first step is to characterize equivalence classes as cones in the plane. The characterization of the equivalence classes allowed us to initiate a study about quasi-metric invariants, minimum distance of a code, packing and covering radius. In this sense, we have seen that, for a given code, these quasi-metric invariants are not constants and most of them depend not only on the equivalence classes and the code, but also depend on the choice of specific codewords, unlike what happens in the case of Hamming metric (associated to the symmetric channel) or any other metric invariant by translation. This dependence leads us to define sequences of packing and covering radius, which improve the usual concept.

Keywords: Binary asymmetric channel. Error correcting codes (Information theory).

Sumário

Capítulo 1

Introdução

Um canal binário assimétrico sem memória é um canal no qual os símbolos de entrada e saída são binários, mas no qual a probabilidade de erro é distinta para os símbolos 1 e 0. Canais binários assimétricos têm sido utilizados como modelo em diversas situações e aplicações, como por exemplo, na modelagem de memória flash, [1], [2], ou ainda em neurociência, na modelagem de "erros"no acionamento de neurônios específicos mediante estímulos fixos [3]. Apesar do crescente interesse pelo assunto, muito pouco foi dito sobre os canais binários assimétricos como um espaço em sí. Neste trabalho, pretendemos estudar a geometria dos canais binários assimétricos sem memória.

Utilizamos a notação usual de canais binários assimétricos, denotando o par de parâmetros por (p, q), em que p denota a probabilidade de enviar o símbolo 0 e receber o símbolo 1 e q a probabilidade de enviar o símbolo 1 e receber o símbolo 0. Os canais simétricos, são aqueles em que $p = q$ e nestes, do ponto de vista teórico, sob muitos aspectos, é indiferente o valor efetivo de p. Não é esta a situação no caso de canais assimétricos. Mais ainda, o comportamento dos canais depende efetivamente de uma terceira variável, a saber, o comprimento n dos blocos considerados. Assim, denotamos por $BAC^n(p, q)$ o canal binário assimétrico com probabilidades de erro (p, q) e comprimento de bloco n.

Considere dois canais binários assimétricos distintos, $BAC^n(p, q)$ e $BAC^n(p', q')$. Olhando cada um destes canais apenas como um modelo probabilístico, dois tipos de equivalência se impõem de maneira natural a partir de Teoria de Códigos Corretores de Erros.

- **Probabilidade a posteriori:** A primeira delas se refere ao processo de decodificação (a posteriori): dizemos que $BAC^n(p, q)$ e $BAC^n(p', q')$ são equivalentes se para todo código $\mathcal{C} \subseteq \mathbb{F}_2^n$ e para toda palavra recebida $v \in \mathbb{F}_2^n$, a decodificação por máxima verossimilhança (incluindo decodificação por lista) retorna o mesmo resultado para os dois canais.

- **Probabilidade a priori:** Sob o ponto de vista de probabilidade a priori, a relação é distinta: dizemos que $BAC^n(p, q)$ e $BAC^n(p', q')$ são equivalentes se, ao se enviar

uma palavra qualquer $v \in \mathbb{F}_2^n$, e ordenarmos os elementos de $\mathbb{F}_2^n$ de acordo com a probabilidade de serem recebidos (probabilidade que em geral é distinta para $(p,q) \neq (p',q')$) a ordem dos elementos é igual para os dois canais. Para sermos mais precisos, denotemos $z = (p,q), z' = (p',q')$ e seja $\mathbb{P}_z^n(u|v)$ (ou $\mathbb{P}_{z'}^n(u|v)$) a probabilidade (determinada por z (ou z')) de se receber uma mensagem u dado que v tenha sido enviada, em que $u, v \in \mathbb{F}_2^n$. Dizemos que $BAC^n(p,q)$ e $BAC^n(p',q')$ são equivalentes se

$$\mathbb{P}_z^n(w|v) \leq \mathbb{P}_z^n(u|v) \iff \mathbb{P}_{z'}^n(w|v) \leq \mathbb{P}_{z'}^n(u|v),$$

para quaisquer $u, v, w \in \mathbb{F}_2^n$.

Considerando o conjunto de todos os canais ou o conjunto de suas classes de equivalência (em um ou outro sentido, a priori ou a posteriori) temos o que podemos chamar de um espaço de canais , ou seja, um conjunto no qual cada elemento é um canal ou uma classe de equivalência de canais.

A primeira referência que encontramos a respeito deste objeto, citada em [4], se refere a uma questão apresentada em 1967, nas notas de aula de Massey [5] (referência original não encontrada), onde se pergunta sobre a possibilidade de termos uma métrica casada a um canal, no sentido de que a decodificação por máxima verossimilhança (critério a posteriori) coincida com a decodificação por máxima proximidade (critério métrico). Nesse sentido, em 1971, Chiang e Wolf determinaram todos os canais discretos simétricos e sem memória casados com a métrica de Lee, [4]. Em 1980, Séguin resolveu o mesmo problema, para as métricas aditivas e apresentou condições necessárias e suficientes para que um canal discreto e sem memória esteja casado com tais métricas, [6].

O problema foi novamente retomado em um contexto mais genérico em 2016, por Walker e Firer, que definiram a questão para canais genéricos e demonstraram que o canal Z é metrizável, [7]. O caso assimétrico genérico foi estudado por Poplawsky em [8] e resolvido por Qureshi em [9]. Posteriormente, iniciou-se um estudo sobre equivalências entre canais binários assimétricos, sob o ponto de vista da decodificação a posteriori, [10].

O estudo das equivalências entre canais binários assimétricos, sob o ponto de vista de probabilidades a priori, ainda não havia sido explorado e este é o principal objeto de estudo deste trabalho. Claramente, como de modo geral temos que $\mathbb{P}(u|v) \neq \mathbb{P}(v|u)$, não é possível casar uma métrica aditiva a um $BAC^n(p,q)$, a menos que tenhamos o caso simétrico $p = q$. Assim, para casarmos uma medida geométrica a uma medida probabilística do canal, temos duas possibilidades: a primeira é abrir mão do caráter aditivo de distância, conforme foi feito por Firer e Walker em [7], para o canal Z (que é um caso extremo de $BAC^n(p,q)$, com $p = 0$) e por Qureshi, na situação geral, em [9]. Outra possibilidade, que utilizamos aqui, é manter a estrutura aditiva e abrir mão da condição de simetria de uma métrica, obtendo o que é conhecido na literatura como quasi-

métrica (vide *Encyclopedia of Distances*, [11]). A quasi-métrica (também denominada *métrica assimétrica* ou *métrica orientada*) é uma função orientada e que será definida neste trabalho, como uma função que depende das constantes p e q que determinam um $BAC^n(p,q)$.

Se considerarmos a matriz de probabilidades $\mathbb{P}^n_{p,q}$ de um $BAC^n(p,q)$, podemos ordenar as entradas por colunas ou por linhas. Assumimos neste ponto a seguinte convenção: dado que $v \in \mathbb{F}_2^n$ foi enviado, o vetor $u \in \mathbb{F}_2^n$ mais provável de ter sido recebido é aquele que possui a maior probabilidade na *coluna* da matriz $\mathbb{P}^n_{p,q}$, correspondente a v. Esse processo de ordenação da matriz de probabilidades de um canal, por colunas, é um processo diferente do que é feito no processo de decodificação por máxima verossimilhança, em que a matriz de probabilidades é ordenada por linhas, conforme pode ser visto, por exemplo, em [10] e [12].

Temos assim definido o espaço dos canais binários assimétricos de comprimento n e uma relação de equivalência natural: dizemos que dois canais são equivalentes se a ordenação de cada coluna da matriz associada for idêntica. O espaço destas classes de equivalência é o objeto de estudo deste trabalho.

Para lidar com este problema, considerando esta convenção de ordenamento de $\mathbb{P}^n_{p,q}$ por colunas, à cada $BAC^n(p,q)$, associamos uma quasi-métrica aditiva, por uma relação que nos permite comparar as distâncias entre vetores binários de comprimento n, com as probabilidades de erro do canal. Em outras palavras, para $u, v \in \mathbb{F}_2^n$, se a distância de v até u é a menor, dentre todas as distâncias realizáveis a partir de v, então a probabilidade de receber u dado que v foi enviado é a maior dentre todas as probabilidades a priori obtidas a partir de v. Considerando este modelo de distância (quasi-métrica), conseguimos caracterizar de maneira simples as classes de equivalência: cada classe é um cone. Caracterizadas as classes de equivalência, definimos e estudamos os principais parâmetros e invariantes métricos de códigos corretores de erros dentro deste contexto quasi-métrico: distância mínima, raios de empacotamento, raio de cobertura, distribuição de distâncias.

Neste ponto é importante mencionar que o ponto de partida desta tese (ou inspiração original) é o trabalho de Fazelli et. al ([13]) que estuda o limitante de empacotamento de esferas no caso de espaços onde as bolas não têm mesmo volume (ou cardinalidade).

Vale a pena destacar que a principal ferramenta utilizada no estudo de códigos, utilizando os canais binários assimétricos, é a métrica assimétrica proposta em [14], por Constantin e Rao. Para $u, v \in \mathbb{F}_2^n$, a distância assimétrica entre os vetores u e v é definida como sendo $d_a(v,u) = \max\{r,s\}$, em que as quantidades r e s são definidas, respectivamente, por $r = \big|\{i \mid v_i = 1 \text{ e } u_i = 0\}\big|$ e $s = \big|\{i \mid v_i = 0 \text{ e } u_i = 1\}\big|$. Essa métrica é interessante pois determina em qual direção ($0 \to 1$ ou $1 \to 0$) ocorre maior quantidade de erros, fato útil para estimar a quantidade de erros que o canal é capaz de

corrigir. No entanto, esta métrica não reflete adequadamente propriedades importantes do canal em termos de códigos corretores de erros, quais sejam, a equivalência de canais (a posteriori ou a priori), dentre outros motivos porque não dependem dos parâmetros (p, q) que determinam o canal assimétrico.

Este trabalho está organizado da seguinte forma: no Capítulo 2, definimos o espaço dos canais binários assimétricos n-dimensionais e uma quasi-métrica aditiva que será associada a um $BAC^n(p, q)$ pertencente a este espaço. O resultado que caracteriza esta associação é o nosso ponto de partida para desenvolver todo o trabalho. A partir dele, definimos, de maneira natural, uma equivalência de canais e caracterizamos as classes de equivalência como cones convexos do plano. No Capítulo 3, estudamos os invariantes quasi-métricos, distância mínima do código e raios de empacotamento e cobertura. Mostraremos que, para um dado código, estes invariantes não são constantes e a maioria deles depende não somente do código e das classes de equivalência de canais, mas também da escolha das palavras código. Nesse sentido, refinamos o conceito usual e definimos as sequências de raios de empacotamento e cobertura de um código. Encerramos o trabalho elencando algumas considerações finais e perspectivas futuras.

Capítulo 2

Geometria do espaço $\mathcal{P}^n$

Este capítulo tem como principal objetivo apresentar a geometria do espaço $\mathcal{P}^n$. A partir de uma quasi-métrica aditiva, que depende dos parâmetros (p, q) do canal, mostraremos como canal e distância estão associados e, a partir disso, definiremos uma relação de equivalência entre canais que nos permitirá descrever as classes de equivalência como cones convexos do plano.

2.1 Canais binários assimétricos

Neste trabalho consideramos um canal binário assimétrico $BAC(p, q)$, determinado por constantes p, q que representam as probabilidades de erro de símbolo, de modo que $\mathbb{P}(0|0) = 1 - p$, $\mathbb{P}(1|0) = p$, $\mathbb{P}(0|1) = q$ e $\mathbb{P}(1|1) = 1 - q$, para $p, q \in (0, \frac{1}{2})$, conforme podemos ver esquematicamente na Figura 2.1.

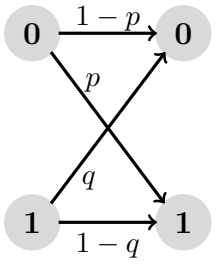


Figura 2.1: Esquema de um canal binário assimétrico $BAC(p, q)$.

Observação 1. *BAC refere-se às iniciais de Binary Asymmetric Channel, em inglês.*

Para $1 \leq n \in \mathbb{N}$, consideramos um canal binário assimétrico n-dimensional,

$$BAC^n(p, q) : V \to V,$$

em que $V = \mathbb{F}_2^n$ e $(p, q) \in (0, \frac{1}{2})^2$. O canal $BAC^n(p, q)$ é considerado sem memória, ou seja, dados $v = (v_1, \ldots, v_n)$ e $u = (u_1, \ldots, u_n)$, com $u, v \in V$, tem-se que

$$\mathbb{P}(u|v) = \prod_{i=1}^{n} \mathbb{P}(u_i|v_i),$$

em que

$$\mathbb{P}(u_i|v_i) = \begin{cases} 1-p, & \text{se} \quad u_i = v_i = 0, \\ p, & \text{se} \quad u_i = 1, v_i = 0, \\ q, & \text{se} \quad u_i = 0, v_i = 1, \\ 1-q, & \text{se} \quad u_i = v_i = 1. \end{cases}$$

Observação 2. *Neste trabalho, $\mathbb{P}(u|v)$ denota a probabilidade de receber um vetor u dado que o vetor v foi enviado, para quaisquer $u, v \in V$.*

Definição 1. *Para $n \in \mathbb{N}$, definimos o conjunto de todos os BACs n-dimensionais por*

$$\mathcal{P}^n = \big\{ BAC^n(p, q) \mid BAC(p, q) \text{ é um BAC} \big\}.$$

Um $BAC^n(p, q)$, como o próprio nome sugere, nos dá uma condição de assimetria para o problema, pois pode-se errar na direção $0 \to 1$ e na direção $1 \to 0$, com probabilidades distintas, diferente do que ocorre com o canal binário simétrico (BSC), [15]. Assim sendo, para esse tipo de canal, devemos tratar os erros de maneira qualitativa e não somente quantitativa, como ocorre no caso simétrico. Note que, anteriormente nos referimos aos tipos de erro do canal, fazendo uso da palavra "direção". Esse termo já sugere como faremos a análise qualitativa dos erros de transmissão deste canal, ou seja, faremos uso de uma distância orientada entre vetores enviados e recebidos, respectivamente. Assim, se por exemplo, enviamos um vetor $v \in V$ e, após a transmissão, recebemos como resposta do canal um vetor $u \in V$, a distância orientada entre os vetores v e u fornecerá a quantidade de erros que ocorreram em cada uma das direções. Note ainda que esta distância será diferente se considerarmos a orientação contrária, ou seja, de u até v.

2.2 A quasi-métrica $\delta_{p,q}^n$

Considere um canal $BAC^n(p, q) \in \mathcal{P}^n$ determinado por um par de probabilidades de erro $(p, q) \in (0, \frac{1}{2})^2$. Suponha que uma mensagem $u \in \mathbb{F}_2^n$ tenha sido enviada pelo canal $BAC^n(p, q)$ e tenhamos recebido uma palavra $v \in \mathbb{F}_2^n$. Então, a transição $u \to v$ pode ser descrita por um grafo bi-orientado e ponderado $G = (V, E)$. O conjunto $V = \mathbb{F}_2^n$ denota o conjunto dos vértices de G e representa todos os possíveis vetores v que podem ser recebidos como resposta do canal ao final da transmissão da mensagem u. O conjunto E é formado por todas as arestas bi-orientadas de G tal que, para todo $u, v \in V$, uma

aresta $uv \in E$ se, e somente se, $d_H(u,v) = 1$, em que d_H denota a *métrica de Hamming*. Vale ressaltar que $uv \in E$ se, e somente se, $vu \in E$, pois d_H é métrica e satisfaz a propriedade simétrica. Além disso, se $uv \in E$, então $\omega_H(u) = \omega_H(v) \pm 1$ (em que ω_H denota o *peso de Hamming* de um vetor), pois u e v diferem em apenas uma coordenada e, nesse caso, $\omega_H(v)$ necessariamente deve ser uma unidade maior ou uma unidade menor que o peso de Hamming de $\omega_H(u)$.

Para cada aresta bi-orientada $uv \in E$ atribuímos um peso, definido de acordo com o tipo de coordenada que foi trocada na transição $u \to v$. O peso de uma aresta $uv \in E$ depende das probabilidades de erro do canal $BAC^n(p,q)$ e do tipo de troca de coordenadas. Assim sendo, o peso atribuído à aresta será em função de q se a aresta foi percorrida na direção $1 \to 0$ e será em função de p, se a aresta foi percorrida na direção inversa, $0 \to 1$, conforme definimos a seguir.

Definição 2. *Seja $G = (V,E)$ um grafo bi-orientado, $V = \mathbb{F}_2^n$ e $uv \in E$ para $u, v \in V$. O peso da aresta uv é definido por*

$$t_{p,q}(uv) = \begin{cases} -\log_2\Big(\dfrac{q}{1-q}\Big) = \log_2\Big(\dfrac{1}{q} - 1\Big), & \text{se} \quad \omega_H(u) = \omega_H(v) + 1; \\ \\ -\log_2\Big(\dfrac{p}{1-p}\Big) = \log_2\Big(\dfrac{1}{p} - 1\Big), & \text{se} \quad \omega_H(u) = \omega_H(v) - 1. \end{cases}$$

Definição 3. *Seja $G = (V,E)$ um grafo bi-orientado, $V = \mathbb{F}_2^n$ e $u, v \in V$. Um **caminho orientado**, com r arestas, ligando o vértice u ao vértice v é uma sequência $\mathbb{V} = (v_i)_{i=0}^r$, onde $v_0 = u$, $v_r = v$ e $v_i v_{i+1} \in E$. O **comprimento (ponderado)** do caminho $\mathbb{V}$ é dado pela soma dos pesos das r arestas de $\mathbb{V}$, ou seja,*

$$l(\mathbb{V}) = \sum_{i=0}^{r-1} t_{p,q}(v_i v_{i+1}).$$

*Um **raio geodésico** é um caminho $\mathbb{V}$ de comprimento mínimo dentre os que ligam o vértice inicial u ao vértice final v. Denotamos por $\delta_{p,q}^n(u,v)$ o comprimento de um raio geodésico unindo u a v.*

Vale observar que como o grafo G é conexo, existem caminhos ligando dois vértices quaisquer e a existência de geodésica ligando dois vértices segue do fato das distâncias serem discretas.

Para um canal $BAC^n(p,q) \in \mathcal{P}^n$ e para um caminho orientado $\mathbb{V}$, ligando o vértice inicial u ao vértice final v, sejam $|e_p|$ a quantidade de arestas na direção $0 \to 1$ e $|e_q|$ a quantidade de arestas na direção $1 \to 0$. Então, o comprimento ponderado de $\mathbb{V}$

pode ser expresso por uma combinação dos pesos das arestas, ou seja,

$$l(\mathbb{V}) = |e_p| \log_2\Big(\frac{1}{p} - 1\Big) + |e_q| \log_2\Big(\frac{1}{q} - 1\Big).$$

Se $\mathbb{V}$ for um raio geodésico de comprimento $\delta^n_{p,q}(u, v)$, a quantidade r de arestas do caminho $\mathbb{V}$ é igual a $r = d_H(u, v)$, conforme mostra a seguinte proposição.

Proposição 1. *Sejam $u, v \in V$. Se $\mathbb{V} = (v_i)_{i=0}^r$ é um raio geodésico ligando o vértice inicial u ao vértice final v, então o caminho $\mathbb{V}$ possui $r = d_H(u, v)$ arestas.*

Demonstração. Sejam $u, w, v \in V$ e $\mathbb{V} = (v_i)_{i=0}^r$ um raio geodésico ligando o vértice inicial $v_0 = u$ ao vértice final $v_r = w$. A demonstração será feita usando o Principio da Indução Finita sobre r.

O caso $r = 1$ é trivial. Assumamos, por hipótese, que o raio geodésico $\mathbb{V}$ possua $r = d_H(u, w)$ arestas, em que $r \geq 1$.

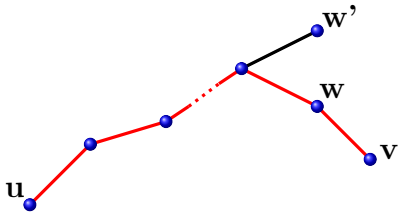


Figura 2.2: Um esquema (em vermelho) para um raio geodésico $\mathbb{V}_1 = \mathbb{V} \cup v$.

Seja $\mathbb{V}_1 = (v_i)_{i=0}^{r+1}$ um raio geodésico ligando o vértice inicial $v_0 = u$ ao vértice final $v_{r+1} = v$. Por hipótese, um raio geodésico unindo $v_0 = u$ a qualquer elemento do conjunto $D = \{w \in V \mid d_H(u, w) = r\}$ possui exatamente r arestas. Como $\mathbb{V}_1$ possui $(r + 1)$ arestas e $\mathbb{V}$ e $\mathbb{V}_1$ têm o mesmo vértice inicial $v_0 = u$, podemos escrever $\mathbb{V}_1$ como $\mathbb{V}_1 = \mathbb{V} \cup v$, conforme ilustra esquematicamente a Figura 2.2, em que $w, w' \in D$. Portanto, existe pelo menos um vetor $w \in D$ tal que $d_H(w, v) = 1$. Nesse caso, a desigualdade triangular aplicada à métrica de Hamming é satisfeita com igualdade, ou seja, $d_H(u, v) = d_H(u, w) + d_H(w, v) = r + 1$ e o resultado está demonstrado. □

O resultado da Proposição 1 é natural pois, se $\mathbb{V}$ é um raio geodésico, com r arestas, ligando o vértice inicial u ao vértice final v, então r representa a menor quantidade necessária de coordenadas trocadas para obter o vetor v a partir da mensagem enviada u. Essa quantidade representa justamente o valor $d_H(u, v)$. Vale ressaltar que a geodésica ligando dois vértices não é necessariamente única.

Adotaremos neste trabalho a definição de quasi-métrica, conforme apresentada em [11].

Definição 4. *Uma função $\delta^n_{p,q} : V^2 \to \mathbb{R}^+$ definida sobre $V = \mathbb{F}_2^n$ é uma quasi-métrica se satisfaz as seguintes condições:*

a) para todo $u, v \in V$, $\delta^n_{p,q}(u,v) \geq 0$ *e* $\delta^n_{p,q}(u,v) = 0 \Leftrightarrow u = v$;

b) para todo $u, v, w \in V$, $\delta^n_{p,q}(u,v) \leq \delta^n_{p,q}(u,w) + \delta^n_{p,q}(w,v)$;

Definição 5. *Uma quasi-métrica* $\delta^n_{p,q} : V^2 \to \mathbb{R}^+$ *definida sobre* $V = \mathbb{F}_2^n$ *é aditiva se*

$$\delta^n_{p,q}(u,v) = \sum_{i=1}^{n} \delta^n_{p,q}(u_i, v_i),$$

para todo $u, v \in V$.

A próxima proposição nos fornece que $\delta^n_{p,q}(\cdot,\cdot)$ é uma quasi-métrica aditiva.

Proposição 2. *A função* $\delta^n_{p,q} : V^2 \to \mathbb{R}^+$ *define uma quasi métrica aditiva.*

Demonstração. De acordo com a Definição 4 deve-se mostrar que $\delta^n_{p,q}(\cdot,\cdot)$ é uma função não negativa e que satisfaz a Desigualdade Triangular orientada. Assim sendo, sejam $u, v, w \in V$. Tem-se que

a) Para todo $u, v \in V$, o comprimento de um raio geodésico ligando o vértice inicial u ao vértice final v é dado por

$$\delta^n_{p,q}(u,v) = |e_p| \log_2\Big(\frac{1}{p} - 1\Big) + |e_q| \log_2\Big(\frac{1}{q} - 1\Big),$$

com $d_H(u,v) = |e_p| + |e_q|$. Uma vez que $p, q \in (0, \frac{1}{2})$ então valem as seguintes desigualdades: $\log_2(\frac{1}{p} - 1) > 0$, $\log_2(\frac{1}{q} - 1) > 0$ e, portanto, $\delta^n_{p,q}(u,v) > 0$, para todo $u, v \in V$. A igualdade $\delta^n_{p,q}(u,v) = 0$ ocorre se $|e_p| = |e_q| = 0$ e, neste caso, necessariamente $u = v$ para todo $u, v \in V$, pois isso significa que não ocorreram erros ao longo da transmissão da mensagem enviada u, pelo canal $BAC^n(p,q)$. Portanto, $\delta^n_{p,q}$ é não negativa.

b) Sejam $\mathbb{V}_1 = (v_i^1)_{i=0}^{r_1}$ um raio geodésico ligando o vértice inicial $v_0^1 = u$ ao vértice final $v_{r_1}^1 = w$ e $\mathbb{V}_2 = (v_i^2)_{i=0}^{r_2}$ um raio geodésico ligando o vértice inicial $v_0^2 = v_{r_1}^1 = w$ ao vértice final $v_{r_2}^2 = v$. Considere um caminho concatenado, $\mathbb{V} = \mathbb{V}_1 * \mathbb{V}_2$, ligando o vértice inicial u ao vértice final v. Então, pela Proposição 1, temos $d_H(u,w) = r_1$ e $d_H(w,v) = r_2$. Assim sendo, pela desigualdade triangular aplicada à métrica de Hamming, obtemos

$$d_H(u,v) \leq d_H(u,w) + d_H(w,v) = r_1 + r_2.$$

Portanto, um raio geodésico ligando o vértice inicial u ao vértice final v terá uma quantidade de arestas menor que ou igual à quantidade de arestas de $\mathbb{V}$, ou seja, menor que ou igual a $(r_1 + r_2)$. Portanto, necessariamente devemos ter $\delta^n_{p,q}(u,v) \leq \delta^n_{p,q}(u,w) + \delta^n_{p,q}(w,v)$. Portanto, $\delta^n_{p,q}$ satisfaz a Desigualdade Triangular orientada.

Por $a)$ e $b)$ conclui-se que $\delta^n_{p,q}$ é quasi-métrica.

Para mostrar a aditividade de $\delta^n_{p,q}$ sejam $u=(u_1,\ldots,u_n), v=(v_1,\ldots,v_n)\in V$ dois vetores quaisquer e $\mathbb{V}$ um raio geodésico unindo o vértice inicial u ao vértice final v. Então, o comprimento da geodésica $\mathbb{V}$ é dado por $\delta^n_{p,q}(u,v)=|e_p|\log_2(\frac{1}{p}-1)+|e_q|\log_2(\frac{1}{q}-1)$ e, pela Proposição 1, tem-se que $d_H(u,v)=|e_p|+|e_q|$. Portanto, obtém-se imediatamente que

$$\delta^n_{p,q}(u,v)=\sum_{i=1}^{n}\delta^n_{p,q}(u_i,v_i)$$

e, pela Definição 5, conclui-se que $\delta^n_{p,q}$ é quasi-métrica aditiva. □

Observação 3. *Sejam $u,v\in V$. Pela definição de raio geodésico, Definição 3, temos*

$$\delta^n_{p,q}(u,v)=|e_p|\log_2\Big(\frac{1}{p}-1\Big)+|e_q|\log_2\Big(\frac{1}{q}-1\Big)\ \ e$$
$$\delta^n_{p,q}(v,u)=|e_q|\log_2\Big(\frac{1}{p}-1\Big)+|e_p|\log_2\Big(\frac{1}{q}-1\Big).$$

Note que os coeficientes de $\log_2\big(\frac{1}{p}-1\big)$ e $\log_2\big(\frac{1}{q}-1\big)$ estão invertidos devido à troca da orientação no caminho de u a v. Neste caso, temos

$$\delta^n_{p,q}(u,v)\neq\delta^n_{p,q}(v,u)\Longleftrightarrow(|e_p|-|e_q|)\Big[\log_2\Big(\frac{1}{p}-1\Big)-\log_2\Big(\frac{1}{q}-1\Big)\Big]\neq 0\Longleftrightarrow$$
$$|e_p|\neq|e_q|\ \ e\ \log_2\Big(\frac{1}{p}-1\Big)\neq\log_2\Big(\frac{1}{q}-1\Big)\Longleftrightarrow|e_p|\neq|e_q|\ \ e\ \ p\neq q.$$

Portanto, existem $u,v\in V$ tais que $\delta^n_{p,q}(u,v)\neq\delta^n_{p,q}(v,u)$ e, desta forma, não conseguimos garantir a simetria da distância para todo par $u,v\in V$. Logo, a distância $\delta^n_{p,q}$ é assimétrica.

Em [14], Constantin e Rao utilizaram a distância assimétrica

$$d_a(u,v)=\max\{|e_p|,|e_q|\}.$$

Assim sendo, se $p\neq q$ e $|e_p|=|e_q|$, então $d_a(u,v)=|e_p|=|e_q|$. Por outro lado, acabamos de verificar que $\delta^n_{p,q}(u,v)=\delta^n_{p,q}(v,u)\Longleftrightarrow|e_p|=|e_q|$, para $p\neq q$. Segue que

$$\delta^n_{p,q}(u,v)=\delta^n_{p,q}(v,u)\Longleftrightarrow|e_p|=|e_q|=d_a(u,v).$$

Portanto, estas duas distâncias estão relacionadas quando ocorre simetria na quasi-métrica.

Exemplo 1. *Sejam $V=\mathbb{F}_2^3$ e os vetores $u=000, w=101, v=011\in V$. Considere um canal $BAC^3(p,q)\in\mathcal{P}^3$. A Figura 2.3 ilustra o grafo bi-orientado G para o qual o conjunto*

de vértices é V. Pode-se ver que as distâncias entre os pares de vértices (v,u), (u,w) e (w,v) são dadas, respectivamente, por: $\delta^3_{p,q}(u,v) = 2\log_2(\frac{1}{p}-1)$, $\delta^3_{p,q}(u,w) = 2\log_2(\frac{1}{p}-1)$ e $\delta^3_{p,q}(w,v) = \log_2(\frac{1}{p}-1)+\log_2(\frac{1}{q}-1)$. Sabemos que a distância $\delta^3_{p,q}(u,v)$ (comprimento do caminho vermelho no grafo G) é menor que a distância $\delta^3_{p,q}(u,w)+\delta^3_{p,q}(w,v)$ (comprimento dos caminhos em tons de azul no grafo G). Portanto, o caminho vermelho é um raio geodésico, de comprimento $\delta^3_{p,q}(u,v)$, que une o vértice inicial u ao vértice final v.

Além disso, note a assimetria das distâncias quando a orientação dos caminhos vermelho e azul claro são invertidas: $\delta^3_{p,q}(v,u) = \delta^3_{p,q}(w,u) = 2\log_2(\frac{1}{q}-1)$. Por outro lado, para o caminho azul escuro, apesar da inversão na orientação, o comprimento do caminho se mantém igual a $\delta^3_{p,q}(v,w) = \log_2(\frac{1}{q}-1)+\log_2(\frac{1}{p}-1) = \delta^3_{p,q}(w,v)$.

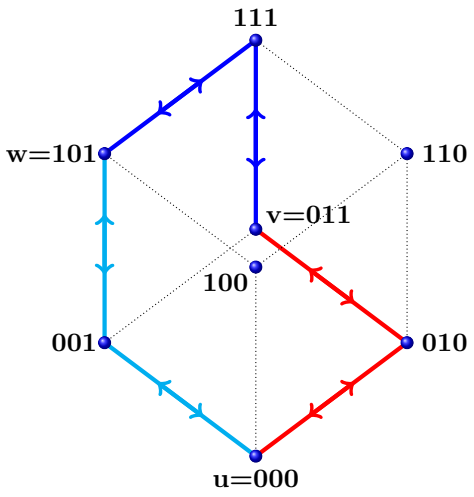


Figura 2.3: Grafo bi-orientado G, correspondente ao espaço V.

2.3 O espectro de $v \in V$

Vimos na Seção 2.2 que, para um dado canal $BAC^n(p,q)$, um raio geodésico $\mathbb{V}$ unindo um vértice inicial u a um vértice final v pode ser descrito por meio de um grafo bi-orientado G. Portanto, cada vez que uma mensagem u é enviada pelo canal $BAC^n(p,q)$, podemos receber como resposta qualquer vetor v, a uma distância $\delta^n_{p,q}(u,v)$ do vértice u. Cada uma dessas distâncias corresponde a um caminho orientado $\mathbb{V}$, no grafo G, que une o vértice inicial u a algum vértice $v \in V$. A seguir, definimos o conjunto $Spec(u)$, formado por todas as distâncias realizáveis a partir de um vértice inicial $u \in V$.

Definição 6. *Seja $u \in V$. O espectro de u é o conjunto de todas as quasi-distâncias que podem ser realizadas a partir de u e de um par de probabilidades de erro (p,q), ou seja,*

$$Spec(u) := \left\{\delta^n_{p,q}(u,v) \mid v \in V\right\}.$$

Conforme visto na Proposição 1, um raio geodésico unindo um vértice inicial u a um vértice final v possui exatamente $d_H(u,v) = |e_p| + |e_q|$ arestas e tem comprimento dado por

$$\delta^n_{p,q}(u,v) = |e_p| \log_2\Big(\frac{1}{p} - 1\Big) + |e_q| \log_2\Big(\frac{1}{q} - 1\Big),$$

com $|e_p| \leq (n - w_H(u))$ e $|e_q| \leq w_H(u)$.

Assim sendo, obter os elementos do conjunto $Spec(u)$ consiste em determinar todos os pares ordenados $(|e_p|, |e_q|) \in \mathbb{N} \times \mathbb{N}$ que são soluções do sistema

$$\textbf{(P)} \begin{cases} |e_p| & + & |e_q| = d_H(u,v) \\ |e_p| & \leq & n - \omega_H(u); \\ |e_q| & \leq & \omega_H(u), \end{cases} \tag{2.1}$$

para $d_H(u,v) \leq n$.

Note que, se $u, v \in V$ são vetores com mesmo peso de Hamming ($\omega_H(u) = \omega_H(v)$), então $Spec(u) = Spec(v)$, já que ambos os conjuntos são determinados pela resolução do Sistema 2.1.

Exemplo 2. *Considere um canal $BAC^3(p,q) \in \mathcal{P}^3$ e $u = 101 \in V$. Uma vez que $\omega_H(u) = 2$ e $n = 3$, obtém-se que*

$$\textbf{(P)} \begin{cases} |e_p| & + & |e_q| = d_H(u,v) \\ |e_p| & \leq & 1; \\ |e_q| & \leq & 2, \end{cases} \tag{2.2}$$

para $r = d_H(u,v) \leq 3$ e todo $v \in V$.

Os pares ordenados que satisfazem o Sistema 2.2 estão ilustrados na Figura 2.4. Cada par ordenado $(|e_p|, |e_q|)$ corresponde a uma distância $\delta^n_{p,q}(u,v)$, para todo $v \in V$, conforme descrito a seguir:

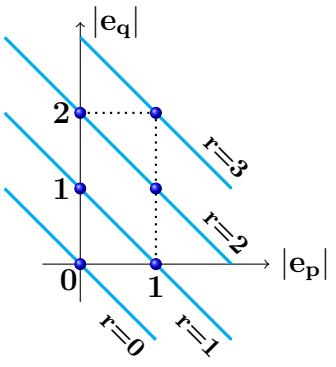


Figura 2.4: Solução do Sistema (2.2). Na figura, r denota a distância de Hamming.

1. $d_H(u,v) = 0$:

   - $(|e_p|, |e_q|) = (0,0) \to \delta^3_{p,q}(v,v) = 0.$

2. $d_H(u,v) = 1$:

   - $\big(|e_p|, |e_q|\big) = (1,0) \to \delta^3_{p,q}(u,v) = \log_2\big(\frac{1}{p} - 1\big)$;
   - $\big(|e_p|, |e_q|\big) = (0,1) \to \delta^3_{p,q}(u,v) = \log_2\big(\frac{1}{q} - 1\big).$

3. $d_H(u,v) = 2$:

   - $\big(|e_p|, |e_q|\big) = (0,2) \to \delta^3_{p,q}(u,v) = 2\log_2\big(\frac{1}{q} - 1\big)$;
   - $\big(|e_p|, |e_q|\big) = (1,1) \to \delta^3_{p,q}(u,v) = \log_2\big(\frac{1}{p} - 1\big) + \log_2\big(\frac{1}{q} - 1\big).$

4. $d_H(u,v) = 3$:

   - $(|e_p|, |e_q|) = (1,2) \to \delta^3_{p,q}(u,v) = \log_2\big(\frac{1}{p} - 1\big) + 2\log_2\big(\frac{1}{q} - 1\big).$

Portanto, temos 6 *distâncias que podem ser realizadas a partir do vértice* u*, ou seja,*

$$Spec(u) = \big\{0, x, y, 2y, x+y, x+2y\big\},$$

com $x = \log_2\big(\frac{1}{p} - 1\big)$ *e* $y = \log_2\big(\frac{1}{q} - 1\big)$.

Uma vez que, para todo $u \in V$, o conjunto $Spec(u)$ está bem definido e caracterizado, mediante a resolução do Sistema (2.1), buscamos encontrar uma expressão que nos fornecesse a cardinalidade deste conjunto, conforme mostramos no próximo teorema.

Teorema 1. *Seja* $u \in V$*. A cardinalidade de* $Spec(u)$ *é dada por*

$$\sigma_u := |Spec(u)| = (\omega_H(u) + 1)(n - \omega_H(u) + 1), \tag{2.3}$$

em que $\omega_H(u)$ *é o peso de Hamming de* u*.*

Demonstração. Seja R o retângulo $(n - \omega) \times \omega$, para $\omega := \omega_H(u)$, conforme ilustrado na Figura 2.5. Para calcular $Spec(u)$ devemos resolver o sistema definido em (2.1), ou seja, precisamos somente contar os pares ordenados $(|e_p|, |e_q|)$ em R. Uma vez que cada par ordenado corresponde a um único elemento de $Spec(u)$, pelo Princípio Multiplicativo obtemos $\sigma_u = (\omega + 1)(n - \omega + 1)$. □

Exemplo 3. *Seja* $v = 101 \in V$*. Então, temos* $\omega_H(v) = 2$ *e, pelo Teorema 1, obtemos* $\sigma_v = 6$*, conforme descrito inicialmente no Exemplo 2.*

Note que σ_v é uma função que depende somente de n e do peso de Hamming de v, para todo $v \in V$. Os corolários a seguir nos fornecem uma condição para que as cardinalidades de σ_v e σ_u coincidam e também os valores máximo e mínimo de σ_v.

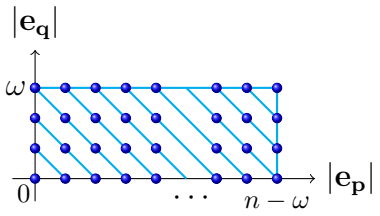


Figura 2.5: Retângulo R.

Corolário 1. *Sejam $u, v \in V$ e $n \in \mathbb{N}$. Então,*

$$\sigma_v = \sigma_u \iff \omega_H(v) = \omega_H(u) \quad ou \quad \omega_H(v) + \omega_H(u) = n.$$

Demonstração. Sejam $u, v \in V$. Pelo Teorema 1, temos:

$$\sigma_v = \sigma_u \iff (\omega_H(v)+1)(n-\omega_H(v)+1) = (\omega_H(u)+1)(n-\omega_H(u)+1).$$

A última igualdade é equivalente a $\big(\omega_H(u) - \omega_H(v)\big)\big(\omega_H(u) + w_H(v) - n\big) = 0$, de onde se obtém que $\omega_H(u) = \omega_H(v)$ ou $\omega_H(u) + \omega_H(v) = n$. □

Corolário 2. *Seja σ_v a cardinalidade do espectro de v, para todo $v \in V$. Então,*

a) $\min\limits_{v\in V} \sigma_v = \sigma_{\mathbf{0}} = \sigma_{\mathbf{1}} = n+1.$

b) $\max\limits_{v\in V} \sigma_v = \begin{cases} (\frac{n+2}{2})^2 & se \quad n \text{ é par e } w_H(v) = \frac{n}{2}; \\ (\frac{n+1}{2})(\frac{n+3}{2}) & se \quad n \text{ é ímpar e } w_H(v) = \lceil \frac{n}{2} \rceil \text{ ou } w_H(v) = \lfloor \frac{n}{2} \rfloor. \end{cases}$

onde $\mathbf{0} = (0, 0, \ldots, 0)$ e $\mathbf{1} = (1, 1, \ldots, 1) \in V$.

Demonstração. Seja $v \in V$.

a) Pelo Teorema 1, tem-se que

$$\sigma_v = (\omega_H(v)+1)(n-\omega_H(v)+1) = (n+1) + \omega_H(v)(n-\omega_H(v)) \geq n+1 = \sigma_{\mathbf{0}} = \sigma_{\mathbf{1}}.$$

Portanto, $\min\limits_{v\in V} \sigma_v = n+1 = \sigma_{\mathbf{0}} = \sigma_{\mathbf{1}}$.

b) Para $n \in \mathbb{N}$ e $v \in V$, σ_v é uma função de $\omega_H(v) := \omega$. Neste caso,

$$\sigma_v = (\omega+1)(n-\omega+1) = -\omega^2 + n\omega + n + 1$$

é uma função do segundo grau definida para os valores inteiros do intervalo fechado $[0, n]$. O máximo absoluto desta função ocorre nos pontos $\omega = \lfloor \frac{n}{2} \rfloor$ e $\omega = \lceil \frac{n}{2} \rceil$, se n é ímpar, e no ponto $\omega = \frac{n}{2}$, se n é par.

Assim sendo, vamos calcular o valor máximo de σ_v para cada um dos casos a seguir:

Caso n par: Se n é par, temos $\omega = \frac{n}{2}$ e, portanto,

$$\sigma_v = (\omega + 1)(n - \omega + 1) = \Big(\frac{n}{2} + 1\Big)^2.$$

Caso ímpar: Se n é ímpar, temos $\omega = \lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$ e $\omega = \lceil \frac{n}{2} \rceil = \frac{n+1}{2}$. Portanto,

$$\sigma_v = (\omega + 1)(n - \omega + 1) = \Big(\frac{n \pm 1}{2} + 1\Big)\Big(n - \frac{n \pm 1}{2} + 1\Big) = \Big(\frac{n+3}{2}\Big)\Big(\frac{n+1}{2}\Big). \quad \square$$

Exemplo 4. *Seja $V = \mathbb{F}_2^3$. Para todo $v \in V$, listamos o conjunto $Spec(v)$, a seguir:*

$$\begin{aligned} Spec(000) =& \{0, x, 2x, 3x\} \\ Spec(100) =& Spec(010) = Spec(001) = \{0, x, y, 2x, x + y, 2x + y\} \\ Spec(110) =& Spec(101) = Spec(011) = \{0, x, y, 2y, x + y, x + 2y\} \\ Spec(111) =& \{0, y, 2y, 3y\}. \end{aligned}$$

Conforme mostra o Corolário 2, uma vez que $n = 3$ é ímpar, os valores máximo e mínimo para σ_v são, respectivamente, 6 e 4. Note ainda que, conforme mostra o Corolário 1, vetores com mesmo peso de Hamming têm o mesmo espectro e, portanto, esses conjuntos têm a mesma cardinalidade. Além disso, pelo mesmo corolário, vemos que os vetores com peso de Hamming iguais a 1 e 2 também têm conjuntos de distâncias com mesma cardinalidade, já que seus correspondentes pesos de Hamming somados resultam em $n = 3$.

2.4 Matriz de probabilidades e matriz de distâncias de um $BAC^n(p, q)$

Considere um $BAC^n(p, q) \in \mathcal{P}^n$. Suponha que uma mensagem $v \in V$ foi enviada e o vetor recebido como resposta é $u \in V$. Então, conforme visto na Seção 2.2, o comprimento de um raio geodésico $\mathbb{V}$ unindo o vértice inicial v ao vértice final u é $\delta^n_{p,q}(v, u) = |e_p| \log_2(\frac{1}{p} - 1) + |e_q| \log_2(\frac{1}{q} - 1)$ e este caminho possui $d_H(v, u) = |e_p| + |e_q|$ arestas. Além disso, como o caminho $\mathbb{V}$ pode ser descrito por um grafo bi-orientado $G = (V, E)$, então podemos dizer que cada aresta percorrida no grafo G, ao longo do caminho $\mathbb{V}$, equivale a um erro na transmissão da mensagem enviada v. Logo, ocorreram $|e_p|$ erros na direção $0 \to 1$ e $|e_q|$ erros na direção $1 \to 0$, ao longo do caminho $\mathbb{V}$.

Pela definição de canal binário assimétrico sem memória, dada na Seção 2.1, a probabilidade de receber o vetor u dado que v foi enviado é dada por

$$\begin{aligned}\mathbb{P}^n_{p,q}(u|v) =& \prod_{i=1}^{n} \mathbb{P}^n_{p,q}(u_i|v_i)\\ =& p^{|e_p|}q^{|e_q|}(1-q)^{\omega_H(v)-|e_q|}(1-p)^{n-\omega_H(v)-|e_p|}\\ =& \Big(\frac{p}{1-p}\Big)^{|e_p|}\Big(\frac{q}{1-q}\Big)^{|e_q|}(1-q)^{\omega_H(v)}(1-p)^{n-\omega_H(v)}. \end{aligned} \tag{2.4}$$

Podemos ainda calcular o erro relativo na transmissão da mensagem v, ou seja,

$$\begin{aligned}\frac{\mathbb{P}^n_{p,q}(u|v)}{\mathbb{P}^n_{p,q}(v|v)} &\overset{(2.4)}{=} \frac{\big(\frac{p}{1-p}\big)^{|e_p|}\big(\frac{q}{1-q}\big)^{|e_q|}(1-q)^{\omega_H(v)}(1-p)^{n-w_H(v)}}{(1-q)^{\omega_H(v)}(1-p)^{n-\omega_H(v)}}\\ &= \Big(\frac{p}{1-p}\Big)^{|e_p|}\Big(\frac{q}{1-q}\Big)^{|e_q|}. \end{aligned} \tag{2.5}$$

Considerando o logaritmo na base 2 dos dois lados da igualdade (2.5), obtemos:

$$\log_2\Big(\frac{\mathbb{P}^n_{p,q}(u|v)}{\mathbb{P}^n_{p,q}(v|v)}\Big) = \log_2\Big[\Big(\frac{p}{1-p}\Big)^{|e_p|}\Big(\frac{q}{1-q}\Big)^{|e_q|}\Big],$$

e daí segue que

$$\log_2\Big(\frac{\mathbb{P}^n_{p,q}(v|v)}{\mathbb{P}^n_{p,q}(u|v)}\Big) = |e_p|\log_2\Big(\frac{1}{p}-1\Big) + |e_q|\log_2\Big(\frac{1}{q}-1\Big),$$

ou seja,

$$\log_2\Big(\frac{\mathbb{P}^n_{p,q}(v|v)}{\mathbb{P}^n_{p,q}(u|v)}\Big) = \delta^n_{p,q}(v,u). \tag{2.6}$$

Portanto, a expressão (2.6) é uma forma alternativa para calcular o comprimento $\delta^n_{p,q}(v,u)$ do raio geodésico $\mathbb{V}$. Note que $\delta^n_{p,q}(v,u)$ depende unicamente da distância de Hamming entre os vértices v e u, do peso de Hamming de v e do par de probabilidades (p,q). Portanto, cada canal $BAC^n(p,q)$ define uma quasi-métrica $\delta^n_{p,q}(\cdot,\cdot)$ e, portanto, dizemos que ***o canal está associado à quasi-métrica***. Mais ainda, para todo $v \in V$, existe uma bijeção

$$\begin{aligned} f_v : Spec(v) &\to \mathbb{P}^n_v\\ : \delta^n_{p,q}(v,u) &\to \mathbb{P}^n_{p,q}(u|v). \end{aligned} \tag{2.7}$$

que leva cada distância $\delta^n_{p,q}(v,u) \in Spec(v)$ a uma probabilidade de transição $\mathbb{P}^n_{p,q}(u|v) \in \mathbb{P}^n_v$, em que $\mathbb{P}^n_v = \{\mathbb{P}(u|v) \mid u \in V\}$.

A próxima proposição é o ponto de partida deste trabalho pois, para um dado canal $BAC^n(p,q)$, o resultado apresentado mostra como a quasi-métrica e a probabilidade

de transição estão relacionadas. Por meio deste resultado consegue-se descrever toda a geometria do espaço de canais, conforme pretendemos.

Proposição 3. *Dado um canal $BAC^n(p,q) \in \mathcal{P}^n$ então*

$$\delta^n_{p,q}(v,u) \leq \delta^n_{p,q}(v,w) \Longleftrightarrow \mathbb{P}^n_{p,q}(w|v) \leq \mathbb{P}^n_{p,q}(u|v),$$

em que $\delta^n_{p,q}(\cdot,\cdot)$ é a quasi-métrica associada ao canal $BAC^n(p,q)$, para todo $v,w,u \in V$.

Demonstração. Considere $\delta^n_{p,q}(\cdot,\cdot)$ a quasi métrica associada ao canal $BAC^n(p,q) \in \mathcal{P}^n$. Então, dados $v,w,u \in V$, sabemos que:

$$\delta^n_{p,q}(v,w) = \log_2\Big(\frac{\mathbb{P}^n_{p,q}(v|v)}{\mathbb{P}^n_{p,q}(w|v)}\Big) \text{ e } \delta^n_{p,q}(v,u) = \log_2\Big(\frac{\mathbb{P}^n_{p,q}(v|v)}{\mathbb{P}^n_{p,q}(u|v)}\Big).$$

Então,

$$\delta^n_{p,q}(v,u) \leq \delta^n_{p,q}(v,w) \Longleftrightarrow \log_2\Big(\frac{\mathbb{P}^n_{p,q}(v|v)}{\mathbb{P}^n_{p,q}(u|v)}\Big) \leq \log_2\Big(\frac{\mathbb{P}^n_{p,q}(v|v)}{\mathbb{P}^n_{p,q}(w|v)}\Big),$$

e, como a função logaritmo é crescente, esta última desigualdade ocorre se, e somente se,

$$\mathbb{P}^n_{p,q}(v|v) \cdot \Big(\frac{1}{\mathbb{P}^n_{p,q}(u|v)} - \frac{1}{\mathbb{P}^n_{p,q}(w|v)}\Big) \leq 0. \tag{2.8}$$

Mas, $\mathbb{P}^n_{p,q}(v|v) > 0$ e, portanto, a desigualdade (2.8) é satisfeita se, e somente se,

$$\big(\frac{1}{\mathbb{P}^n_{p,q}(u|v)} - \frac{1}{\mathbb{P}^n_{p,q}(w|v)}\big) \leq 0,$$

ou seja,

$$\mathbb{P}^n_{p,q}(w|v) \leq \mathbb{P}^n_{p,q}(u|v).$$

□

Definição 7. *Seja M uma matriz quadrada $N \times N$ com coeficientes reais. A forma ordenada, por colunas, da matriz M é a matriz M^* definida pela ordem natural dos números reais, ou seja, $M^*_{ij} = k$, se M_{ij} é o k-ésimo menor elemento da j-ésima coluna de M, para $1 \leq k \leq N$.*

Considere um $BAC^n(p,q) \in \mathcal{P}^n$ cuja matriz de probabilidades é dada por $\mathbb{P}^n_{p,q}$. As colunas dessa matriz são formadas pelos elementos do conjunto $\mathbb{P}^n_v = \big\{\mathbb{P}(u|v) \mid u \in V\big\}$. Note que $\mathbb{P}^n_v$ é o mesmo conjunto definido na bijeção dada na equação 2.7. Conforme a Definição 7 sugere, podemos ordenar a matriz, $\mathbb{P}^n_{p,q}$, por colunas, como mostra a seguinte definição.

Definição 8. *Considere um $BAC^n(p,q)$. A forma ordenada, por colunas, da matriz $\mathbb{P}^n_{p,q}$ é a matriz $(\mathbb{P}^n_{p,q})^*$ definida por $(\mathbb{P}^n_{ij})^* = \bar{k}$ se $\mathbb{P}^n_{ij}$ é o $\bar{k}$-ésimo menor elemento da j-ésima coluna de $\mathbb{P}^n_{p,q}$, para $1 \leq \bar{k} \leq N$.*

Como probabilidade e distância estão relacionadas pela Proposição 3, definimos a matriz de distâncias associada a um $BAC^n(p,q)$, assim como foi feito com a matriz $\mathbb{P}^n_{p,q}$.

Definição 9. *Considere um $BAC^n(p,q) \in \mathcal{P}^n$. A matriz de distâncias, associada ao $BAC^n(p,q)$ é a matriz $N \times N$ dada por*

$$\mathbb{D}^n_{x,y} = [\mathbb{D}^n_{v_0}\ \mathbb{D}^n_{v_1} \ldots\ \mathbb{D}^n_{v_N}],$$

em que $N = 2^n - 1$, cujas entradas são os elementos $\mathbb{D}^n_{ij} = \delta^n_{p,q}(v_j, v_i)$, para todo $i, j \in \{0, 1, \ldots, N\}$, $x = \log_2(\frac{1}{p} - 1)$ e $y = \log_2(\frac{1}{q} - 1)$. A forma ordenada, por colunas, da matriz $\mathbb{D}^n_{x,y}$ é a matriz $(\mathbb{D}^n_{x,y})^*$ definida por $(\mathbb{D}^n_{ij})^* = k$, em que $\mathbb{D}^n_{ij}$ é o k-ésimo menor elemento da j-ésima coluna de $\mathbb{D}^n_{x,y}$, para $1 \leq k \leq N$ e $N = 2^n$.

Este processo de ordenação de matrizes é similar ao feito em [9] e [12], para o processo de decodificação (probabilidade a posteriori). Nesse caso, a matriz é ordenada por linhas, diferentemente do que fazemos aqui. Para cada uma dessas matrizes, vamos fixar uma ordem para a coluna correspondente ao vetor $v \in V$. Consideraremos a notação binária para representar um inteiro $0 \leq j \leq N$, ou seja, $j = \sum_{i=0}^{n-1} a_i 2^{n-1-i}$, para $a_i \in \{0, 1\}$ e $N = 2^n - 1$. Assim sendo, por exemplo, a coluna $\mathbb{P}^n_v$ corresponde à j-ésima coluna da matriz $\mathbb{P}^n_{p,q}$, em que j é o inteiro cuja representação binária é o vetor v.

Exemplo 5. *Considere $n = 2$ e um canal $BAC^2(p,q) \in \mathcal{P}^2$. Para simplificar, denotaremos $\bar{p} := 1-p$, $\bar{q} := 1-q$, $x = \log_2(\frac{1}{p} - 1)$ e $y = \log_2(\frac{1}{q} - 1)$. As matrizes de probabilidade e distância, associadas ao canal, são dadas, respectivamente, por*

$$\mathbb{P}^2_{p,q} = \left(\begin{array}{c|cccc} u|v & 00 & 01 & 10 & 11 \\ \hline 00 & \bar{p}^2 & q\bar{p} & q\bar{p} & q^2 \\ 01 & p\bar{p} & \bar{p}\bar{q} & pq & q\bar{q} \\ 10 & p\bar{p} & pq & \bar{p}\bar{q} & q\bar{q} \\ 11 & p^2 & p\bar{q} & p\bar{q} & \bar{q}^2 \end{array}\right) \qquad \mathbb{D}^2_{x,y} = \left(\begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & 0 & y & y & 2y \\ 01 & x & 0 & x+y & y \\ 10 & x & x+y & 0 & y \\ 11 & 2x & x & x & 0 \end{array}\right).$$

Sejam $u, v \in \mathbb{F}_2^2$. Então, $\mathbb{P}^2_{p,q}(u|v)$ denota a probabilidade de receber o vetor u dado que o vetor v foi enviado. Assim sendo, uma coluna da matriz $\mathbb{P}^2_{p,q}$ é formada pelos elementos do conjunto $\left\{\mathbb{P}^2_{p,q}(u|v) \mid \text{para todo } u \in \mathbb{F}_2^2\right\}$ em que $v \in \mathbb{F}_2^2$ é o vetor correspondente a esta coluna. Analogamente, uma coluna da matriz $\mathbb{D}^2_{x,y}$ é formada pelos elementos do conjunto $\left\{\delta^2_{p,q}(v,u) \mid \text{para todo } u \in \mathbb{F}_2^2\right\}$ em que $v \in \mathbb{F}_2^2$ é o vetor correspondente a esta coluna.

As formas ordenadas, por colunas, destas matrizes mudam conforme mudamos (p,q) *e serão obtidas considerando-se os dois casos possíveis:* $p>q$ *e* $p<q$*. Consequentemente, a mudança do par de parâmetros* (p,q) *muda o correspondente par* (x,y)*, ou seja, se* $p>q$ *e* $p<q$ *obtém-se, respectivamente, que* $x<y$ *e* $x>y$*. A seguir, vamos analisar cada caso individualmente.*

Para o caso $p>q$*, obtém-se que* $\bar{p}=1-p<\bar{q}=1-q$ *e* $x<y$*. Portanto,*

$$\begin{aligned} pq<q\bar{p}<p\bar{q}<\bar{p}\bar{q} \quad & e \quad 0<x<y<x+y,\\ p^2<p\bar{p}<\bar{p}^2 \quad & e \quad 0<x<2x,\\ q^2<q\bar{q}<\bar{q}^2 \quad & e \quad 0<y<2y. \end{aligned}$$

e as formas ordenadas, por colunas, das matrizes $\mathbb{P}^2_{p,q}$ *e* $\mathbb{D}^2_{x,y}$ *são dadas, respectivamente, por*

$$(\mathbb{P}^2_{p>q})^* = \left(\begin{array}{c|cccc} u|v & 00 & 01 & 10 & 11\\ \hline 00 & 3 & 2 & 2 & 1\\ 01 & 2 & 4 & 1 & 2\\ 10 & 2 & 1 & 4 & 2\\ 11 & 1 & 3 & 3 & 3 \end{array}\right) \qquad (\mathbb{D}^2_{x<y})^* = \left(\begin{array}{c|cccc} & 00 & 01 & 10 & 11\\ \hline 00 & 1 & 3 & 3 & 3\\ 01 & 2 & 1 & 4 & 2\\ 10 & 2 & 4 & 1 & 2\\ 11 & 3 & 2 & 2 & 1 \end{array}\right).$$

Para o caso $p<q$*, obtém-se que* $\bar{q}<\bar{p}$ *e* $x>y$*. Portanto,*

$$\begin{aligned} pq<p\bar{q}<q\bar{p}<\bar{p}\bar{q} \quad & e \quad 0<y<x<x+y,\\ p^2<p\bar{p}<\bar{p}^2 \quad & e \quad 0<x<2x,\\ q^2<q\bar{q}<\bar{q}^2 \quad & e \quad 0<y<2y \end{aligned}$$

e as formas ordenadas, por colunas, das matrizes $\mathbb{P}^2_{p,q}$ *e* $\mathbb{D}^2_{x,y}$ *são dadas, respectivamente, por*

$$(\mathbb{P}^2_{p<q})^* = \left(\begin{array}{c|cccc} u|v & 00 & 01 & 10 & 11\\ \hline 00 & 3 & 3 & 3 & 1\\ 01 & 2 & 4 & 1 & 2\\ 10 & 2 & 1 & 4 & 2\\ 11 & 1 & 2 & 2 & 3 \end{array}\right) \qquad (\mathbb{D}^2_{x>y})^* = \left(\begin{array}{c|cccc} & 00 & 01 & 10 & 11\\ \hline 00 & 1 & 2 & 2 & 3\\ 01 & 2 & 1 & 4 & 2\\ 10 & 2 & 4 & 1 & 2\\ 11 & 3 & 3 & 3 & 1 \end{array}\right).$$

Note que, como consequência da Proposição 3, dados $u,v\in V$, à medida que a distância $\delta^n_{p,q}(v,u)\in Spec(v)$ aumenta, a probabilidade $\mathbb{P}^n_{p,q}(u|v)$ diminui. Neste sentido,

as colunas $(\mathbb{D}_v^n)^*$ e $(\mathbb{P}_v^n)^*$ estão relacionadas, conforme é apresentado na proposição a seguir.

Proposição 4. *Sejam $(\mathbb{D}_{x,y}^n)^*$ e $(\mathbb{P}_{p,q}^n)^*$ as formas ordenadas, respectivamente, das matrizes de distância e probabilidade, associadas a um $BAC^n(p,q) \in \mathcal{P}^n$. Se $(\mathbb{D}_{ij}^n)^* = k$, então $(\mathbb{P}_{ij}^n)^* = \sigma_{v_j} - k + 1$, onde $v_j \in \mathbb{F}_2^n$ é o vetor correspondente à coluna j dessas matrizes e σ_{v_j} denota a cardinalidade de $Spec(v_j)$.*

Demonstração. A demonstração segue imediatamente da ordenação obtida pela Proposição 3. □

Observação 4. *A ordenação $(\mathbb{D}_{x,y}^n)^*$ da matriz de distâncias foi feita por colunas e reflete as probabilidades a priori do canal, ou seja, se transmitimos um vetor v, então*

$$\mathbb{P}_{p,q}^n(\textit{receber } u | \textit{enviado } v) > \mathbb{P}_{p,q}^n(\textit{receber } w | \textit{enviado } v)$$

se e somente se $(\mathbb{D}_{u,v}^n)^* < (\mathbb{D}_{w,v}^n)^*$. Uma questão semelhante, mas distinta, refere-se a probabilidade a posteriori. Em resumo, a partir da matriz de probabilidade $\mathbb{P}_{p,q}^n$, obtemos uma matriz $(\mathbb{P}_{p,q}^n)^\#$ que é obtida ordenando-se em ordem crescente as entradas de cada linha. Assim, obtemos que, dado um código $\mathcal{C} \subseteq \mathbb{F}_2^n$, temos que, recebida uma mensagem u, procuramos na linha u de $(\mathbb{P}_{p,q}^n)^\#$ a maior entrada correspondente a alguma palavra código. Esta foi a abordagem adotada por [12] e [10], o primeiro estudando classes de equivalência de canais em um contexto genérico, o segundo estudando as classes de equivalência de canais binários assimétricos, sob o ponto de vista de decodificação.

2.5 As classes de equivalência de BACs

Nesta seção, iniciamos nosso estudo sobre a equivalência de canais binários assimétricos. Primeiramente, definiremos uma relação de equivalência entre canais assimétricos e, em seguida, faremos uma caracterização das classes de equivalência como cones convexos do plano. Por fim, apresentamos uma expressão fechada que expressa a quantidade de tais classes.

2.5.1 Partição do espaço $(\mathbb{R}^+)^2$ em cones convexos

Sob o ponto de vista da probabilidade a priori, podemos definir naturalmente uma relação de equivalência entre canais binários assimétricos, conforme mostramos a seguir.

Definição 10. *Considere os canais $BAC^n(p,q), BAC^n(p',q') \in \mathcal{P}^n$. Dizemos que esses canais são equivalentes se, para todo $v, w, u \in V$,*

$$\mathbb{P}_{p,q}^n(w|v) \leq \mathbb{P}_{p,q}^n(u|v) \iff \mathbb{P}_{p',q'}^n(w|v) \leq \mathbb{P}_{p',q'}^n(u|v), \tag{2.9}$$

ou, equivalentemente,

$$\delta^n_{p,q}(v,u) \leq \delta^n_{p,q}(v,w) \Longleftrightarrow \delta^n_{p',q'}(v,u) \leq \delta^n_{p',q'}(v,w), \tag{2.10}$$

em que $\delta^n_{p,q}$ e $\delta^n_{p',q'}$ são as quasi-métricas definidas para $BAC^n(p,q)$ e $BAC^n(p',q')$, respectivamente. Denotamos esta relação por $BAC^n(p,q) \sim BAC^n(p',q')$.

Em geral, uma pequena perturbação no par (p,q) não afeta o critério de codificação, ou seja, se considerarmos dois pares $(p,q),(p',q') \in (0,\frac{1}{2})^2$ e que estejam suficientemente próximos, o critério de codificação é o mesmo e então dizemos que $BAC^n(p,q)$ e $BAC^n(p',q')$ são equivalentes. Assim sendo, nosso interesse no estudo das classes de equivalência do espaço $\mathcal{P}^n$ fica justificado pois, uma vez que essas classes de equivalência estão caracterizadas, basta considerar um canal pertencente a cada uma delas para estudar as propriedades que desejamos. Os demais canais pertencentes à mesma classe terão o mesmo comportamento, em termos de codificação.

É simples verificar que a relação $\sim$ é uma relação de equivalência, conforme será demonstrado na proposição a seguir.

Proposição 5. *A relação $\sim$ define uma relação de equivalência no conjunto $\mathcal{P}^n$.*

Demonstração. Sejam $BAC^n(p,q), BAC^n(p',q'), BAC^n(p'',q'') \in \mathcal{P}^n$, canais determinados por pares de probabilidades pertencentes ao espaço $(0,\frac{1}{2})^2$. As propriedades de simetria e reflexão são imediatas e seguem diretamente da Definição 10. A propriedade transitiva segue diretamente da relação (2.9), conforme mostramos a seguir:

Transitividade: Suponha que $BAC^n(p,q) \sim BAC^n(p',q')$ e $BAC^n(p',q') \sim BAC^n(p'',q'')$. Pela Definição 10, temos que, para todo $u,v,w \in V$,

$$BAC^n(p,q) \sim \mathrm{B}AC^n(p',q') \Leftrightarrow \mathbb{P}^n_{p,q}(w|v) \leq \mathbb{P}^n_{p,q}(u|v) \Leftrightarrow \mathbb{P}^n_{p',q'}(w|v) \leq \mathbb{P}^n_{p',q'}(u|v), \tag{2.11}$$

$$BAC^n(p',q') \sim \mathrm{B}AC^n(p'',q'') \Leftrightarrow \mathbb{P}^n_{p',q'}(w|v) \leq \mathbb{P}^n_{p',q'}(u|v) \Leftrightarrow \mathbb{P}^n_{p'',q''}(w|v) \leq \mathbb{P}^n_{p'',q''}(u|v). \tag{2.12}$$

Por (2.11) e (2.12) segue imediatamente que

$$\mathbb{P}^n_{p,q}(w|v) < \mathbb{P}^n_{p,q}(u|v) \Longleftrightarrow \mathbb{P}^n_{p'',q''}(w|v) < \mathbb{P}^n_{p'',q''}(u|v),$$

e, portanto, $BAC^n(p,q) \sim BAC^n(p'',q'')$, para todo $v,w,u \in V$. □

Uma visão geométrica do problema nos mostra que se $BAC^n(p,q) \sim BAC^n(p',q')$ e $\mathbb{V}_{p,q}$ e $\mathbb{V}_{p',q'}$ são dois raios geodésicos que ligam um ponto inicial v a um ponto final u, então $\mathbb{V}_{p,q}$ e $\mathbb{V}_{p',q'}$ são descritos pelo mesmo conjunto de arestas orientadas e ponderadas do grafo $G = (V,E)$, ou seja, ambos os raios geodésicos têm a mesma quantidade de arestas na direção $0 \to 1$ e $1 \to 0$. No entanto, em geral, $\delta^n_{p,q}(v,u) \neq \delta^n_{p',q'}(v,u)$.

Seja $\sim$ a relação de equivalência no conjunto $\mathcal{P}^n$. Denotamos a ***classe de equivalência***, definida por um par de probabilidades (p, q), como sendo

$$[p : q] = \Big\{ BAC^n(p', q') \;\Big|\; BAC^n(p', q') \sim BAC^n(p, q) \Big\},$$

para constantes $p, q \in (0, \frac{1}{2})$. O conjunto das classes de equivalência do espaço $\mathcal{P}^n$, com respeito à relação de equivalência $\sim$, será denotado pelo quociente $\mathcal{P}^n/_{\sim}$.

Esses primeiros resultados e definições nos dão condições necessárias e suficientes para começar a caracterização das classes de equivalência do conjunto $\mathcal{P}^n$.

Primeiramente, considere uma transformação Φ definida por

$$\begin{aligned} \Phi : \big(0, \frac{1}{2}\big)^2 &\longrightarrow \mathfrak{Q} \\ : \ (p, q) \ &\longrightarrow \ \Phi(p, q) = (x, y), \end{aligned} \tag{2.13}$$

com $(x, y) = \Big(\log_2(\frac{1}{p} - 1), \log_2(\frac{1}{q} - 1)\Big)$ e $\mathfrak{Q} := (\mathbb{R}^+)^2$. É fácil verificar que Φ é um homeomorfismo, pois é uma bijeção contínua que admite a transformação inversa,

$$\begin{aligned} \Phi^{-1} : \quad \mathfrak{Q} &\longrightarrow \big(0, \frac{1}{2}\big)^2 \\ : \Phi(p, q) \ &\longrightarrow \Big(\frac{1}{2^x + 1}, \frac{1}{2^y + 1}\Big), \end{aligned}$$

que também é contínua.

Desta forma, o quadrante $\mathfrak{Q}$ é parametrizado pela transformação Φ. Uma vez que a transformação dada na equação (2.13) relaciona cada canal $BAC^n(p, q) \in \mathcal{P}^n$ a um par de números reais não negativos, $(x, y) \in \mathfrak{Q}$, definimos a seguir um conjunto de retas, dependente da dimensão n, que particiona o espaço $\mathfrak{Q}$ em cones convexos. Consequentemente, obtém-se uma partição do espaço $(0, \frac{1}{2})^2$, via transformação Φ^{-1}.

Definição 11. *Para $n \in \mathbb{N}$, definimos os conjuntos*

$$\mathcal{L} = \Big\{ l \;\Big|\; l \text{ é a reta } \ b \cdot y = a \cdot x, \text{ com } (a, b) = 1 \text{ (coprimos) e } a, b \in \mathbb{N} \Big\}$$

$$e$$

$$\mathcal{L}_n = \big\{ l \in \mathcal{L} \;\big|\; a + b \leq n \big\}.$$

Geometricamente, $\mathcal{L}$ representa o conjunto de todas as retas que particionam o quadrante $\mathfrak{Q}$ em cones, enquanto que o conjunto $\mathcal{L}_n$ restringe $\mathcal{L}$ às retas que passam por um ponto (a, b) de um quadrado $[0, n-1] \times [0, n-1]$, com $a + b \leq n$. Portanto, para todo $n \in \mathbb{N}$, o espaço $\mathfrak{Q}$ é particionado em um número finito de cones convexos (ou cones truncados), limitados pelas retas do conjunto $\mathcal{L}_n$.

Exemplo 6. *Para $n = 1$ o conjunto $\mathcal{L}_1$, da Definição 11, é formado pelos eixos coordenados, ou seja,*

$$\mathcal{L}_1 = \{y = 0, x = 0\}$$

e, portanto, todo o espaço $\mathfrak{Q}$ é um cone convexo, como ilustra a Figura 2.6.

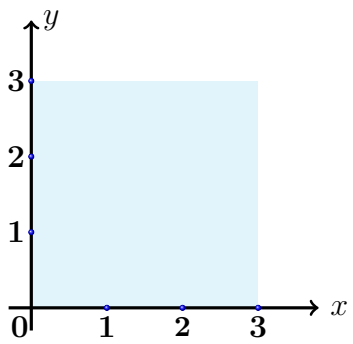


Figura 2.6: Partição do espaço $\mathfrak{Q}$ em cones convexos, para $n = 1$.

Se consideramos $n = 2$, o único par $(a, b) \in \mathbb{N} \times \mathbb{N}$ tal que a e b são coprimos e $a + b = 2$ é o ponto $(1, 1)$ pelo qual passa a reta $y = x$. Os pares $(a, b) \in \mathbb{N} \times \mathbb{N}$ que satisfazem $a + b < 2$ já foram obtidos no caso $n = 1$. Portanto, tem-se

$$\mathcal{L}_2 = \{y = 0, x = 0, y = x\}$$

e o espaço $\mathfrak{Q}$ é particionado em dois cones convexos, como ilustra a Figura 2.7.

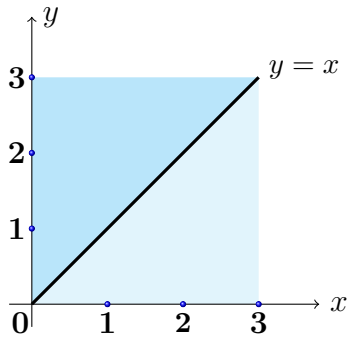


Figura 2.7: Partição do espaço $\mathfrak{Q}$ em cones convexos, para $n = 2$.

Para o caso $n = 3$, os pares $(a, b) \in \mathbb{N}\times\mathbb{N}$ tal que a e b são coprimos e $a+b = 3$ são $(1, 2)$ e $(2, 1)$ pelos quais passam as retas $y = 2x$ e $y = \frac{x}{2}$. Os pares $(a, b) \in \mathbb{N} \times \mathbb{N}$ tais que $a + b < 3$ já foram considerados no caso $n = 2$. Portanto, tem-se que

$$\mathcal{L}_3 = \left\{y = 0, x = 0, y = x, y = 2x, y = \frac{x}{2}\right\}$$

e o espaço $\mathfrak{Q}$ é particionado em quatro cones convexos, como ilustra a Figura 2.8.

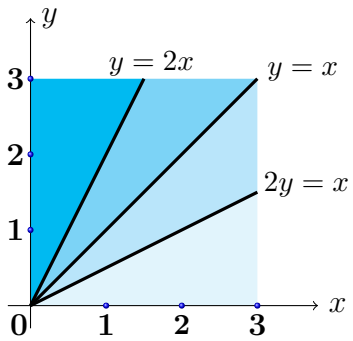


Figura 2.8: Partição do espaço $\mathfrak{Q}$ em cones convexos, para $n = 3$.

A Figura 2.9 reúne as três últimas figuras em uma única representação da partição do espaço $\mathfrak{Q}$ como cones convexos sobrepostos, para $n \leq 3$. Em outras palavras, para cada dimensão $n \leq 3$, o quadrado $n \times n$ contém as retas que correspondem às fronteiras dos cones convexos que particionam o espaço $\mathfrak{Q}$. O prolongamento destas retas é ilustrado com as linhas pontilhadas, para representar todo o cone dentro do espaço. Note que, para $n = 1$, o quadrado 1×1 está colorido com apenas uma cor azul, representando que na dimensão 1 o espaço $\mathfrak{Q}$ é particionado em um único cone convexo. Para $n = 2$, utilizam-se dois tons de azul, significando que na dimensão 2 o espaço $\mathfrak{Q}$ é particionado em dois cones convexos. Para $n = 3$, utilizam-se quatro tons de azul, significando que na dimensão 3 o espaço $\mathfrak{Q}$ é particionado em quatro cones convexos.

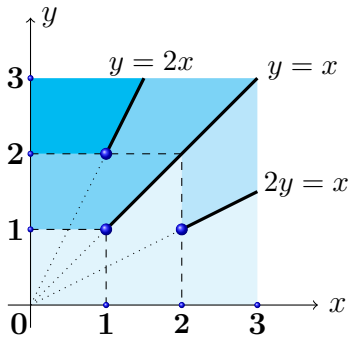


Figura 2.9: Partição do espaço $\mathfrak{Q}$ em cones truncados, para $n \leq 3$.

2.5.2 A condição de fronteira de um cone S

Seja S um cone delimitado pelas retas $r, s \in \mathcal{L}_n$, com $r : b_1 y = a_1 x$ e $s : b_2 y = a_2 x$, conforme ilustrado na Figura 2.10. Sob essas condições, definimos o conjunto de todos os pontos pertencentes a S por

$$S_{r,s} = \left\{ (x, y) \in \mathfrak{Q} \;\middle|\; \frac{a_2}{b_2} x < y < \frac{a_1}{b_1} x \right\},$$

para $x := \log_2(\frac{1}{p} - 1)$ e $y := \log_2(\frac{1}{q} - 1)$.

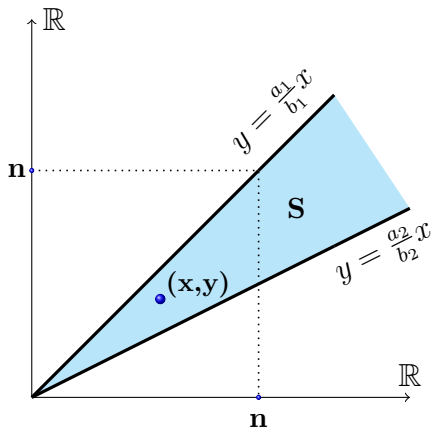


Figura 2.10: O cone S e sua fronteira.

A desigualdade que define o conjunto $S_{r,s}$ pode ser reescrita e dividida em duas partes, cada uma correspondendo a uma desigualdade que compara distâncias (probabilidades) em S, ou seja,

$$\begin{cases} b_1 y < a_1 x & \iff \quad p^{a_1}(1-q)^{b_1} < q^{b_1}(1-p)^{a_1} \\ b_2 y > a_2 x & \iff \quad p^{a_2}(1-q)^{b_2} > q^{b_2}(1-p)^{a_2}. \end{cases} \tag{2.14}$$

Note que a expressão (2.14) age diretamente na ordenação do conjunto $Spec(v)$, para todo $v \in V$, pois estabelece uma ordem para os múltiplos de x e y dentro do espaço S. Além disso, como consequência da Proposição 3, obtemos também uma ordem para as colunas $\mathbb{P}^n_v$ da matriz de probabilidades $\mathbb{P}^n_{p,q}$, associada a um $BAC^n(p,q)$. Logo, as formas ordenadas das matrizes $\mathbb{D}^n_{x,y}$ e $\mathbb{P}^n_{p,q}$, associadas a um $BAC^n(p,q)$, dependem de n e da condição (2.14). A questão que surge neste momento é: a forma ordenada $(\mathbb{D}^n_z)^*$ é única para todos os pontos $z = (x,y) \in S$?

Primeiramente, note que, se o conjunto $\mathcal{L}_n$ particiona o espaço $\mathfrak{Q}$ em cones convexos e se S é um cone desta partição, então S é uma componente conexa de $\mathfrak{Q}\backslash\mathcal{L}_n$. Apesar de estarmos cometendo um abuso na notação, o conjunto $\mathfrak{Q}\backslash\mathcal{L}_n$ significa apenas que excluímos de $\mathfrak{Q}$ todas as retas pertencentes a $\mathcal{L}_n$ e, o interior das regiões formadas por tais retas são as componentes conexas de $\mathfrak{Q}\backslash\mathcal{L}_n$, ou seja, os cones S. Assim sendo, definimos

$$\mathfrak{Q}_n := \big\{ S \;\big|\; S \text{ é componente conexa de } \mathfrak{Q}\backslash\mathcal{L}_n \big\}.$$

Definição 12. *A etapa de um cone $S \in \mathfrak{Q}_n$ é definida por*

$$\eta_S = \min\big\{ n \in \mathbb{N} \;\big|\; S \in \mathfrak{Q}_n \big\},$$

se esse conjunto for diferente de vazio, ou seja, se S existe.

Observamos que $\{S \in \mathfrak{Q}_n \mid \eta_S = \eta\}$ tem mais de um elemento, pois para cada cone S que aparece na etapa η, existe um cone simétrico, na mesma etapa. Para ser mais preciso, se S é um cone que aparece na etapa η e cujas fronteiras são as retas $b_1y = a_1x$ e $b_2y = a_2x$, pertencentes ao conjunto $\mathcal{L}_\eta$, então existe um cone simétrico $\bar{S}$ cujas fronteiras são as retas $a_1y = b_1x$ e $a_2y = b_2x \in \mathcal{L}_\eta$. Se não causar confusão, denotaremos $S := S_\eta$ para indicar que $\eta_S = \eta$.

Definição 13. *Seja $r \in \mathcal{L}_n$ a reta definida por $by = ax$. O conjunto de reordenação é definido por*

$$\mathbb{V}_r^n = \left\{ v \in V \;\middle|\; b \leq \omega_H(v) \leq n - a \right\} \neq \emptyset,$$

para $S \in \mathfrak{Q}_n$.

Sejam $v \in V$, $S \in \mathfrak{Q}_n$ e $z \in S$. Denotaremos a coluna correspondente a v na forma ordenada $(\mathbb{D}_z^n)^*$ por $(\mathbb{D}_v^n)^* = (\mathbb{D}_{1v}\, \mathbb{D}_{2v}\, \ldots\, \mathbb{D}_{Nv})^t$, em que $\mathbb{D}_{iv}$ denota o elemento da i-ésima linha da coluna $(\mathbb{D}_v^n)^*$.

Lema 1. *Sejam $S, \bar{S} \in \mathfrak{Q}_n$ e defina*

$$\mathcal{L}_n(S, \bar{S}) = \left\{ r \in \mathcal{L}_n \;\middle|\; r \text{ separa } S \text{ de } \bar{S} \right\}.$$

Então, $(\mathbb{D}_v^n)^* \neq (\bar{\mathbb{D}}_v^n)^* \iff v \in \mathbb{V}_r^n$, para alguma reta $r \in \mathcal{L}_n(S, \bar{S})$.

Demonstração. Sejam $S, \bar{S} \in \mathfrak{Q}_n$ e uma reta $r \in \mathcal{L}_n(S, \bar{S})$, definida por $by = ax$, com $a + b = n$. Considere um vetor $v \in \mathbb{V}_r^n$ tal que $\omega_H(v) = b$. Então, para $u = 1^n$ e $w = 0^n$, temos $\delta_{p,q}^n(v, u), \delta_{p,q}^n(v, w) \in Spec(v)$, com $\delta_{p,q}^n(v, u) = ax$ e $\delta_{p,q}^n(v, w) = by$. Sob tais condições, temos que

$$\begin{aligned}
(\mathbb{D}_{1v}^n)^* &= \delta_{p,q}^n(v, w) > \delta_{p,q}^n(v, u) = (\mathbb{D}_{Nv}^n)^*, \text{ acima da reta } r, \\
(\bar{\mathbb{D}}_{1v}^n)^* &= \delta_{p,q}^n(v, w) < \delta_{p,q}^n(v, u) = (\bar{\mathbb{D}}_{Nv}^n)^*, \text{ abaixo da reta } r.
\end{aligned}$$

Portanto, necessariamente temos $(\mathbb{D}_v^n)^* \neq (\bar{\mathbb{D}}_v^n)^*$, em que $(\bar{\mathbb{D}}_v^n)^*$ denota a coluna correspondente a v na forma ordenada, por colunas, $(\bar{\mathbb{D}}_z^n)^*$.

Por outro lado, se $(\mathbb{D}_v^n)^* \neq (\bar{\mathbb{D}}_v^n)^*$, é imediato que $v \in \mathbb{V}_r^n$, para alguma reta $r \in \mathcal{L}_n(S, \bar{S})$. □

O Lema 1 nos mostra que, para dois cones $S, \bar{S} \in \mathfrak{Q}_n$, as colunas $(\mathbb{D}_v^n)^*$, correspondentes aos vetores $v \in V_r^n$ são distintas, já que para cada reta r, que separa estes cones, ocorre uma reodenação destas colunas. Logo, as formas ordenadas da matriz de distância, para S e $\bar{S}$ são diferentes. A próxima proposição mostra que a igualdade destas matrizes ocorre quando os cones são iguais, ou seja, cada cone está associado a uma única matriz de distâncias, ordenada por colunas.

Proposição 6. *Sejam $S, \bar{S} \in \mathfrak{Q}_n$ e $z \in S$, $\bar{z} \in \bar{S}$. Então, $(\mathbb{D}_z^n)^* = (\mathbb{D}_{\bar{z}}^n)^* \Leftrightarrow S = \bar{S}$.*

Demonstração. Sejam $S, \bar{S} \in \mathfrak{Q}_n$ e $z \in S$, $\bar{z} \in \bar{S}$. Suponha que $(\mathbb{D}_z^n)^* = (\mathbb{D}_{\bar{z}}^n)^*$ e $S \neq \bar{S}$. Então, existe $r \in \mathcal{L}_n$, que separa S de $\bar{S}$. Mas, pelo Lema 1, concluímos que $(\mathbb{D}_z^n)^* \neq (\mathbb{D}_{\bar{z}}^n)^*$, o que contradiz a hipótese. Logo, $S = \bar{S}$. Por outro lado, se $S = \bar{S}$, não existe $r \in \mathcal{L}_n$ que separa S de $\bar{S}$ e, portanto, $(\mathbb{D}_z^n)^* = (\mathbb{D}_{\bar{z}}^n)^*$. □

Denotaremos por $\mathcal{D}_n$ o conjunto de classes de equivalência do espaço $\mathfrak{Q}$.

Teorema 2. *As classes de equivalência do conjunto $\mathcal{D}_n$ são:*

(a) *Os cones $S \in \mathfrak{Q}_n$;*

(b) *As retas $r \in \mathcal{L}_n$.*

Demonstração. Seja $\mathcal{D}_n$ o conjunto das classes de equivalência de $\mathfrak{Q}$.

(a) Seja $S \in \mathfrak{Q}_n$. Decorre da Proposição 6 que, para quaisquer $z, \bar{z} \in S$, $(\mathbb{D}_z^n)^* = (\mathbb{D}_{\bar{z}}^n)^*$. Segue da Definição 10 que $z \sim \bar{z}$ e, portanto, S é uma classe de equivalência de $\mathcal{D}_n$.

(b) Seja z um ponto qualquer pertencente a uma reta $r \in \mathcal{L}_n$ tal que $r : by = ax$. Então, para todo $u, v \in V$, a distância $\delta_{p,q}^n(v,u) = \alpha x + \beta y$ pode ser escrita como $\delta_{p,q}^n(v,u) = \left(\alpha + \beta\frac{a}{b}\right)x$. Logo, todos os elementos da matriz de distância $\mathbb{D}_z^n$ serão escritos como função de x e, portanto, a forma ordenada por colunas é a mesma para todo $z \in r$. Segue que $r \in \mathcal{L}_n$ é uma classe de equivalência. □

O Teorema 2 nos diz que dois canais z e $\bar{z}$ determinam o mesmo critério de codificação se, e somente se, pertencem a um mesmo cone $S \in \mathfrak{Q}_n$, ou ainda, os cones de $\mathfrak{Q}_n$ são as classes de equivalência do critério de codificação ou $\mathfrak{Q}_n \to \mathcal{D}_n$ por meio da aplicação que, a cada z associa o cone de $\mathfrak{Q}_n$ que o contém. Uma vez que a transformação Φ, definida em (2.13), é uma bijeção contínua tem-se que um cone aberto $S \in \mathfrak{Q}_n$ é uma *classe de equivalência estável* no sentido de que pequenas perturbações em $z \in S$ não afetam o critério de decisão. Cada cone aberto corresponde a uma classe de equivalência estável de $\mathcal{P}^n/_\sim$, por meio da transformação Φ^{-1}. Por outro lado, uma reta $r \in \mathcal{L}_n$ é uma *classe de equivalência instável* que corresponde a uma classe de equivalência instável de $\mathcal{P}^n/_\sim$, via transformação Φ^{-1}.

O próximo exemplo mostra, em detalhes, como calcular as classes de equivalência, as formas ordenadas por colunas e como variam os critérios de codificação à medida que mudamos os cones.

Exemplo 7. *Seja $n = 3$ e considere a Figura 2.8, do Exemplo 6. Então, pelo Teorema 2, cada cone $S \in \mathfrak{Q}_3$ é uma classe de equivalência de $\mathcal{D}_3$ e as correspondentes condições de fronteira são descritas na Tabela 2.1, para cada cone $S \in \mathcal{D}_3$.*

Considerando a condição de fronteira de cada cone, ordenamos $Spec(v)$, para todo $v \in V$, conforme veremos a seguir.

$\mathbf{S_i}$	**Condições de fronteira para** S_i	**Ordenação**
S_1	$0 < y < \frac{x}{2}$	$0 < y < 2y < x$
S_2	$\frac{x}{2} < y < x$	$0 < y < x < 2y$
S_3	$x < y < 2x$	$0 < x < y < 2x$
S_4	$0 < 2x < y$	$0 < x < 2x < y$

Tabela 2.1: Condições de fronteira dos cones S_i, para $n = 3$.

- *Para o cone S_1 a condição de fronteira obtida é $0 < y < \frac{x}{2}$ e, portanto, as correspondentes ordenações de $Spec(v)$ são dadas a seguir, para cada $v \in V$:*

$$\begin{aligned} & Spec(000) : 0 < x < 2x < 3x, \\ Spec(100) = Spec(010) = & Spec(001) : 0 < y < x < x + y < 2x < 2x + y, \\ Spec(110) = Spec(101) = & Spec(011) : 0 < y < 2y < x < x + y < x + 2y, \\ & Spec(111) : 0 < y < 2y < 3y. \end{aligned}$$

A forma ordenada das matrizes de distâncias e probabilidade, associadas ao cone S_1, são dadas respectivamente por

$$(\mathbb{D}^3_{x,y})^* = \left(\begin{array}{c|cccccccc} & 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ \hline 000 & 1 & 2 & 2 & 3 & 2 & 3 & 3 & 4 \\ 001 & 2 & 1 & 4 & 2 & 4 & 2 & 6 & 3 \\ 010 & 2 & 4 & 1 & 2 & 4 & 6 & 2 & 3 \\ 011 & 3 & 3 & 3 & 1 & 6 & 5 & 5 & 2 \\ 100 & 2 & 4 & 4 & 6 & 1 & 2 & 2 & 3 \\ 101 & 3 & 3 & 6 & 5 & 3 & 1 & 5 & 2 \\ 110 & 3 & 6 & 3 & 5 & 3 & 5 & 1 & 2 \\ 111 & 4 & 5 & 5 & 4 & 5 & 4 & 4 & 1 \end{array}\right),$$

e, pela Proposição 4, obtemos

$$(\mathbb{P}^3_{p,q})^* = \left(\begin{array}{c|cccccccc} u|v & 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ \hline 000 & 4 & 5 & 5 & 4 & 5 & 4 & 4 & 1 \\ 001 & 3 & 6 & 3 & 5 & 3 & 5 & 1 & 2 \\ 010 & 3 & 3 & 6 & 5 & 3 & 1 & 5 & 2 \\ 011 & 2 & 4 & 4 & 6 & 1 & 2 & 2 & 3 \\ 100 & 3 & 3 & 3 & 1 & 6 & 5 & 5 & 2 \\ 101 & 2 & 4 & 1 & 2 & 4 & 6 & 2 & 3 \\ 110 & 2 & 1 & 4 & 2 & 4 & 2 & 6 & 3 \\ 111 & 1 & 2 & 2 & 3 & 2 & 3 & 3 & 4 \end{array}\right).$$

- *Para o cone S_2 a condição de fronteira obtida é $\frac{x}{2} < y < x$ e, portanto, as correspondentes ordenações de $Spec(v)$ são dadas a seguir, para cada $v \in V$:*

$$\begin{aligned} & Spec(000) : 0 < x < 2x < 3x, \\ Spec(100) = Spec(010) = & Spec(001) : 0 < y < x < x + y < 2x < 2x + y, \\ Spec(110) = Spec(101) = & Spec(011) : 0 < y < x < 2y < x + y < x + 2y, \\ & Spec(111) : 0 < y < 2y < 3y. \end{aligned}$$

A reta que separa os cones S_1 e S_2 é $r : 2y = x$. Assim sendo, o conjunto de reordenação, na troca do cone S_1 para o cone S_2, é dado por

$$\mathbb{V}_r^3 = \left\{ v \in V \;\middle|\; 2 \leq w_H(v) \leq 2 \right\}.$$

Portanto, pelo Lema 1, somente os vetores com peso de Hamming igual a 2 terão suas colunas reordenadas, na passagem do cone S_1 para o cone S_2. A forma ordenada das matrizes de distâncias e probabilidade, associadas ao cone S_2, são dadas respectivamente por

$$(\mathbb{D}_{x,y}^3)^* = \left(\begin{array}{c|cccccccc} & 000 & 001 & 010 & \mathbf{011} & 100 & \mathbf{101} & \mathbf{110} & 111 \\ \hline 000 & 1 & 2 & 2 & 4 & 2 & 4 & 4 & 4 \\ 001 & 2 & 1 & 4 & 2 & 4 & 2 & 6 & 3 \\ 010 & 2 & 4 & 1 & 2 & 4 & 6 & 2 & 3 \\ 011 & 3 & 3 & 3 & 1 & 6 & 5 & 5 & 2 \\ 100 & 2 & 4 & 4 & 6 & 1 & 2 & 2 & 3 \\ 101 & 3 & 3 & 6 & 5 & 3 & 1 & 5 & 2 \\ 110 & 3 & 6 & 3 & 5 & 3 & 5 & 1 & 2 \\ 111 & 4 & 5 & 5 & 3 & 5 & 3 & 3 & 1 \end{array}\right),$$

e, pela Proposição 4, obtemos

$$(\mathbb{P}_{p,q}^3)^* = \left(\begin{array}{c|cccccccc} u|v & 000 & 001 & 010 & \mathbf{011} & 100 & \mathbf{101} & \mathbf{110} & 111 \\ \hline 000 & 4 & 5 & 5 & 3 & 5 & 3 & 3 & 1 \\ 001 & 3 & 6 & 3 & 5 & 3 & 5 & 1 & 2 \\ 010 & 3 & 3 & 6 & 5 & 3 & 1 & 5 & 2 \\ 011 & 2 & 4 & 4 & 6 & 1 & 2 & 2 & 3 \\ 100 & 3 & 3 & 3 & 1 & 6 & 5 & 5 & 2 \\ 101 & 2 & 4 & 1 & 2 & 4 & 6 & 2 & 3 \\ 110 & 2 & 1 & 4 & 2 & 4 & 2 & 6 & 3 \\ 111 & 1 & 2 & 2 & 4 & 2 & 4 & 4 & 4 \end{array}\right).$$

- *Para o cone S_3 a condição de fronteira obtida é $0 < x < y < 2x$ e, portanto, as correspondentes ordenações de $Spec(v)$ são dadas a seguir, para cada $v \in V$:*

$$\begin{aligned} & Spec(000) : 0 < x < 2x < 3x, \\ Spec(100) = Spec(010) = & Spec(001) : 0 < x < y < 2x < x + y < 2x + y, \\ Spec(110) = Spec(101) = & Spec(011) : 0 < x < y < x + y < 2y < x + 2y, \\ & Spec(111) : 0 < y < 2y < 3y. \end{aligned}$$

A reta que separa os cones S_2 e S_3 é $r : y = x$. Assim sendo, o conjunto de reordenação, na troca do cone S_2 para o cone S_3, é dado por

$$\mathbb{V}_r^3 = \big\{ v \in V \;\big|\; 1 \leq w_H(v) \leq 2 \big\}.$$

Portanto, pelo Lema 1, os vetores com peso de Hamming igual a 1 e 2 terão suas colunas reordenadas, na passagem do cone S_2 para o cone S_3. A forma ordenada das matrizes de distâncias e probabilidade, associadas ao cone S_3, são dadas respectivamente por

$$(\mathbb{D}_{x,y}^3)^* = \left(\begin{array}{c|cccccccc} & 000 & \mathbf{001} & \mathbf{010} & \mathbf{011} & \mathbf{100} & \mathbf{101} & \mathbf{110} & 111 \\ \hline 000 & 1 & 3 & 3 & 5 & 3 & 5 & 5 & 4 \\ 001 & 2 & 1 & 5 & 3 & 5 & 3 & 6 & 3 \\ 010 & 2 & 5 & 1 & 3 & 5 & 6 & 3 & 3 \\ 011 & 3 & 2 & 2 & 1 & 6 & 4 & 4 & 2 \\ 100 & 2 & 5 & 5 & 6 & 1 & 3 & 3 & 3 \\ 101 & 3 & 2 & 6 & 4 & 2 & 1 & 4 & 2 \\ 110 & 3 & 6 & 2 & 4 & 2 & 4 & 1 & 2 \\ 111 & 4 & 4 & 4 & 2 & 4 & 2 & 2 & 1 \end{array}\right),$$

e, pela Proposição 4, obtemos

$$(\mathbb{P}_{p,q}^3)^* = \left(\begin{array}{c|cccccccc} u|v & 000 & \mathbf{001} & \mathbf{010} & \mathbf{011} & \mathbf{100} & \mathbf{101} & \mathbf{110} & 111 \\ \hline 000 & 4 & 4 & 4 & 2 & 4 & 2 & 2 & 1 \\ 001 & 3 & 6 & 2 & 4 & 2 & 4 & 1 & 2 \\ 010 & 3 & 2 & 6 & 4 & 2 & 1 & 4 & 2 \\ 011 & 2 & 5 & 5 & 6 & 1 & 3 & 3 & 3 \\ 100 & 3 & 2 & 2 & 1 & 6 & 4 & 4 & 2 \\ 101 & 2 & 5 & 1 & 3 & 5 & 6 & 3 & 3 \\ 110 & 2 & 1 & 5 & 3 & 5 & 3 & 6 & 3 \\ 111 & 1 & 3 & 3 & 5 & 3 & 5 & 5 & 4 \end{array}\right).$$

- *Para o cone S_4 a condição de fronteira obtida é $0 < x < 2x < y$ e, portanto, as correspondentes ordenações de $Spec(v)$ são dadas a seguir, para cada $v \in V$:*

$$\begin{aligned} & Spec(000) : 0 < x < 2x < 3x, \\ Spec(100) = Spec(010) = & Spec(001) : 0 < x < 2x < y < x + y < 2x + y, \\ Spec(110) = Spec(101) = & Spec(011) : 0 < x < y < x + y < 2y < x + 2y, \\ & Spec(111) : 0 < y < 2y < 3y. \end{aligned}$$

A reta que separa os cones S_3 e S_4 é $r : y = 2x$. Assim sendo, o conjunto de reordenação, na troca do cone S_3 para o cone S_4, é dado por

$$\mathbb{V}_r^3 = \left\{ v \in V \;\middle|\; 1 \leq w_H(v) \leq 1 \right\}.$$

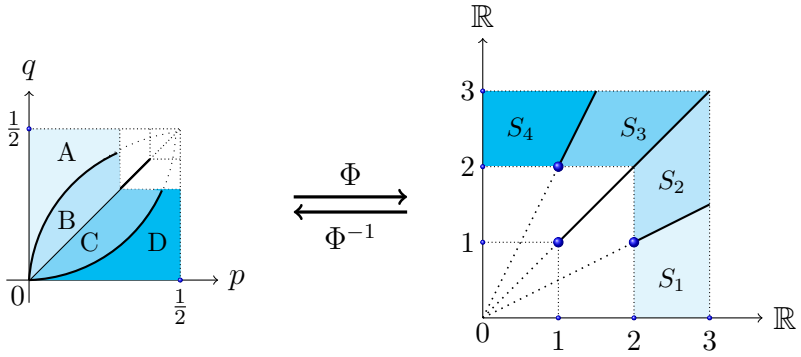
Portanto, pelo Lema 1, somente os vetores com peso de Hamming igual a 1 terão suas colunas reordenadas, na passagem do cone S_3 para o cone S_4. A forma ordenada das matrizes de distâncias e probabilidade, associadas ao cone S_4, são dadas respectivamente por

$$(\mathbb{D}_{x,y}^3)^* = \left(\begin{array}{c|cccccccc} & 000 & \mathbf{001} & \mathbf{010} & 011 & \mathbf{100} & 101 & 110 & 111 \\ \hline 000 & 1 & 4 & 4 & 5 & 4 & 5 & 5 & 4 \\ 001 & 2 & 1 & 5 & 3 & 5 & 3 & 6 & 3 \\ 010 & 2 & 5 & 1 & 3 & 5 & 6 & 3 & 3 \\ 011 & 3 & 2 & 2 & 1 & 6 & 4 & 4 & 2 \\ 100 & 2 & 5 & 5 & 6 & 1 & 3 & 3 & 3 \\ 101 & 3 & 2 & 6 & 4 & 2 & 1 & 4 & 2 \\ 110 & 3 & 6 & 2 & 4 & 2 & 4 & 1 & 2 \\ 111 & 4 & 3 & 3 & 2 & 3 & 2 & 2 & 1 \end{array}\right),$$

e, pela Proposição 4, obtemos

$$(\mathbb{P}_{p,q}^3)^* = \left(\begin{array}{c|cccccccc} u|v & 000 & \mathbf{001} & \mathbf{010} & 011 & \mathbf{100} & 101 & 110 & 111 \\ \hline 000 & 4 & 3 & 3 & 2 & 3 & 2 & 2 & 1 \\ 001 & 3 & 6 & 2 & 4 & 2 & 4 & 1 & 2 \\ 010 & 3 & 2 & 6 & 4 & 2 & 1 & 4 & 2 \\ 011 & 2 & 5 & 5 & 6 & 1 & 3 & 3 & 3 \\ 100 & 3 & 2 & 2 & 1 & 6 & 4 & 4 & 2 \\ 101 & 2 & 5 & 1 & 3 & 5 & 6 & 3 & 3 \\ 110 & 2 & 1 & 5 & 3 & 5 & 3 & 6 & 3 \\ 111 & 1 & 4 & 4 & 5 & 4 & 5 & 5 & 4 \end{array}\right).$$

A Figura 2.11 ilustra o conjunto $\{A, B, C, D\}$ *das classes de equivalência do conjunto* $\mathcal{P}^3/_\sim$.



$$\Phi^{-1}(S_1) = A,\ \Phi^{-1}(S_2) = B,\ \Phi^{-1}(S_3) = C,\ \Phi^{-1}(S_4) = D.$$

Figura 2.11: As classes de equivalência do espaço $\mathcal{P}^3/_\sim$ e do espaço $\mathcal{D}_3$.

A equivalência de canais depende da dimensão n do problema, já que podemos ter canais que são n-equivalentes mas perdem esta propriedade na dimensão $(n+1)$. Assim sendo, passaremos a denotar a equivalência de canais por $BAC^n(p,q) \sim_n BAC^n(p',q')$, para enfatizar a dependência de n, sempre que necessário.

A Figura 2.12 ilustra os cones convexos sobrepostos, para $n \leq 3$. Sejam $z = (x,y), z' = (x',y') \in \mathfrak{Q}$ dois pontos quaisquer, conforme ilustrado na Figura 2.12. Note que z e z' correspondem a canais que são 1-equivalentes e 2-equivalentes mas não são 3-equivalentes.

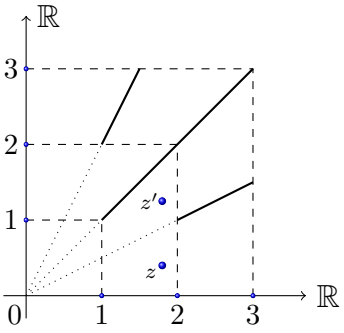


Figura 2.12: Canais n-equivalentes e $(n+1)$-equivalentes, para $n \leq 3$.

Agora que as classes de equivalência de $\mathcal{P}^n/_\sim$ estão caracterizadas como classes de equivalência estáveis e instáveis, podemos calcular a cardinalidade de $\mathcal{P}^n/_\sim$, para um dado n. No próximo teorema, apresentamos essa cardinalidade e mostramos que esta quantidade depende da conhecida *função* φ *de Euler*, cuja definição e propriedades podem ser obtidas em [16].

Teorema 3. *Seja $1 \leq n \in \mathbb{N}$. O conjunto $\mathcal{P}^n/_\sim$ possui exatamente*

a) $\sum_{i=1}^{n} \varphi(i)$ *classes de equivalência estáveis;*

b) $1 + \sum_{i=1}^{n} \varphi(i)$ *classes de equivalência instáveis,*

em que φ é a função phi de Euler.

Demonstração. Seja $1 \leq n \in \mathbb{N}$.

a) Considere que $L_n = |\mathcal{L}_n|$ e $A_n = |\mathcal{A}_n|$ em que

$$\mathcal{A}_n = \big\{(a,b) \in \mathbb{N} \times \mathbb{N} \mid a+b = n,\ m.d.c(a,b) = 1 \text{ e } a,b \leq n\big\}.$$

A quantidade L_n de retas do conjunto $\mathcal{L}_n$ é expressa por uma relação de recorrência não homogênea, dada por:

$$\begin{cases} L_n = L_{n-1} + A_n, \text{ para } n \geq 2 \\ \qquad\qquad\qquad L_1 = 2. \end{cases} \tag{2.15}$$

A próxima etapa consiste em obter uma fórmula fechada para a *Relação de Recorrência* (2.15), ou seja, uma fórmula que não seja recursiva. Seja $L_i = L_{i-1} + A_i$, para $i = 2, \ldots, n$. Então,

$$\begin{aligned} L_i = L_{i-1} + A_i \Longleftrightarrow \sum_{i=2}^{n} L_i &= \sum_{i=2}^{n} L_{i-1} + \sum_{i=2}^{n} A_i \\ \Longleftrightarrow (L_2 + \cdots + L_{n-1} + L_n) &= (L_1 + \cdots + L_{n-1}) + \sum_{i=2}^{n} A_i \\ \Longleftrightarrow L_n &= 2 + \sum_{i=2}^{n} A_i. \end{aligned} \tag{2.16}$$

Mas, a quantidade de classes estáveis é igual a $L_n - 1$ e, por (2.16) segue que, para $n \geq 2$,

$$L_n - 1 = 1 + \sum_{i=2}^{n} A_i. \tag{2.17}$$

Vamos tentar encontrar uma expressão fechada e familiar para a última igualdade obtida em (2.17). Primeiramente, seja $(a,b) \in \mathcal{A}_n$. Então, se existe $q \in \mathbb{N}$ tal que $q|a$ e $q|b$, então $q|n$. Analogamente, se $q|a$ e $q|n$, então $q|b$. Assim sendo, temos:

$$\begin{cases} (a,b) = 1 \;\Rightarrow\; (a,n) = 1 \\ a + b = n \;\Rightarrow\; a < n. \end{cases}$$

Portanto, $a \in \Phi_n$, onde $\Phi_n = \{m \in \mathbb{N} \mid m < n, \text{ e } (m,n) = 1\}$ e $\varphi(n) = |\Phi_n|$.

Por outro lado, seja $a \in \Phi_n$. Então, $a < n$ e $(a,n) = 1$. Mas, $(a,n) = 1$ implica que $(a, n-a) = 1$. Portanto, se considerarmos $b = n - a$, teremos $a + b = n$ e $(a,b) = 1$ de onde concluímos que $(a,b) \in \mathcal{A}_n$.

Assim sendo, para cada elemento $(a,b) \in \mathcal{A}_n$ temos um elemento $a \in \Phi_n$ e, portanto, $A_n = \varphi(n)$, para $n \geq 2$. Segue que

$$L_n - 1 = 1 + \sum_{i=2}^{n} \varphi(i) \overset{\varphi(1)=1}{=} \sum_{i=1}^{n} \varphi(i). \tag{2.18}$$

b) A demonstração deste item é consequência imediata do item a). □

A sequência abaixo denota os valores iniciais da quantidade de classes de equivalências estáveis, para $n \geq 1$:

$$(1, 2, 4, 6, 10, 12, 18, 22, 28, 32, 42, 46, 58, \ldots).$$

Apenas como uma referência, esta sequência pode ser encontrada em [17], como a sequência **M1008** que denota a soma da Função Totient de Euler, de 1 até i.

Observação 5. *Na Observação 4 mencionamos a possibilidade de ordenação por linhas da matriz de probabilidades de um $BAC^n(p,q)$, ordenação que define as prioridades de decodificação. Em [10], Qureshi et. al. determinam as classes de equivalência de BAC's sob o ponto de vista de decodificação (probabilidades a posteriori). Em ambos os casos, as classes de equivalência são determinadas pela existência de constantes inteiras a, b, c, d tais que $p^a(1-q)^b = q^c(1-p)^d$ de modo que, não surpreendentemente, o número de classes de equivalências é o mesmo em ambas as instâncias. Uma questão levantada em [10] refere-se a probabilidade de um BAC pertencer a cada uma das classes de equivalência. Esta probabilidade é expressa simplesmente pela área correspondente a cada classe de equivalência, como ilustrado na Figura 2.11. Aparentemente a classe de canais mais próxima do canal simétrico é a mais provável, assim como no caso de probabilidade a posteriori (ordenação da matriz de probabilidades por linhas). Esta é uma constatação heurística, verificada apenas para valores pequenos de n.*

Capítulo 3

Invariantes quasi-métricos

Este capítulo tem como foco o estudo dos invariantes quasi-métricos que são ferramentas importantes para a Teoria dos Códigos Corretores de erros. Começamos este capítulo estudando as bolas quasi-métricas, pois a correção de erros de transmissão está fundamentada no estudo das bolas centradas nas palavras-código de um dado código $\mathcal{C}$. A seguir, apresentamos os invariantes quasi-métricos e mostramos como os mesmos se comportam no caso assimétrico. Na parte final deste capítulo, definimos os polinômios enumeradores de distância e de raios de empacotamento e cobertura.

3.1 Bolas, centros e espectro de distâncias

Na Seção 2.3 definimos o espectro de um elemento $v \in V$. Como consequência direta da Proposição 6, pode-se dizer que se $BAC^n(p,q) \sim BAC^n(p',q')$, então os conjuntos $Spec_{p,q}(v)$ e $Spec_{p',q'}(v)$ são ordenados da mesma forma, no sentido de que $\delta^n_{p,q}(v,u) \leq \delta^n_{p,q}(v,w)$ se, e somente se, $\delta^n_{p',q'}(v,u) \leq \delta^n_{p',q'}(v,w)$, para todos $v,u,w \in V$. Em palavras, dizer que estes conjuntos são ordenados de maneira única significa que, para $(p,q) \sim (p',q')$, a i-ésima distância calculada a partir de v tem valor numérico diferente em cada um dos canais, mas é descrita pelos mesmos parâmetros nos dois canais. Veremos estas afirmações com mais detalhes ao longo desta seção.

Denotaremos por $\delta_i(v)$ a i-ésima distância realizável a partir de v, para todo $v \in V$.

Definição 14. *Sejam $v \in V$ e $BAC^n(p,q) \in \mathcal{P}^n$. A i-ésima bola com centro v e raio $\delta_i(v) \in Spec(v)$ é definida por*

$$B_i^{(p,q)}(v) = \{u \in V \mid \delta^n_{p,q}(v,u) \leq \delta_i(v)\},$$

para $i \in \{0,1,\ldots,\sigma_v - 1\}$, $(p,q) \in (0,\frac{1}{2})^2$ e $\sigma_v := |Spec(v)|$.

Definição 15. *Seja $v \in V$. A esfera de centro v e raio R é definida por*

$$\mathbb{S}^{(p,q)}(v,R) = \{u \in V \mid \delta^n_{p,q}(v,u) = R\}.$$

A i-ésima esfera com centro v e raio $\delta_i(v) \in Spec(v)$ é definida por

$$\mathbb{S}^{(p,q)}_i(v) = \{u \in V \mid \delta^n_{p,q}(v,u) = \delta_i(v)\}.$$

Como já demonstramos no Teorema 2, um cone $S \in \mathcal{D}_n$ é uma classe de equivalência e, portanto, passaremos a denotar a i-ésima bola $B^{(p,q)}_i(v)$ por $B^S_i(v)$. Analogamente, $\mathbb{S}^{(p,q)}_i(v)$ será denotada por $\mathbb{S}^S_i(v)$.

Uma vez que $Spec(v)$ é ordenado de modo único em um cone S, então existe uma única *sequência de bolas encaixadas*, com centro em v,

$$B^S_0(v) \subseteq B^S_1(v) \subseteq B^S_2(v) \subseteq \ldots \subseteq B^S_{\sigma_v - 1}(v), \tag{3.1}$$

para todo $(p,q) \in \Phi^{-1}(S)$. Em palavras, a sequência (3.1) significa que, como conjunto, as i-ésimas bolas centradas em v são iguais, para todo $(p,q) \in \Phi^{-1}(S)$.

Proposição 7. *Sejam $S, \bar{S} \in \mathcal{D}_n$ e $v \in V$. Então, $B^S_i(v) = B^{\bar{S}}_i(v)$, para todo $i > 0$, se, e somente se, $(\mathbb{D}^n_v)^* = (\bar{\mathbb{D}}^n_v)^*$.*

Demonstração. Sejam $S, \bar{S} \in \mathcal{D}_n$ e $v \in V$. Suponha que para todo $i > 0$, tenhamos $B^S_i(v) = B^{\bar{S}}_i(v)$. Então, esta última igualdade ocorre se, e somente se, $\mathbb{S}^S_i(v) = \mathbb{S}^{\bar{S}}_i(v)$, para todo $i > 0$, ou seja, se, e somente se, $(\mathbb{D}^n_v)^* = (\bar{\mathbb{D}}^n_v)^*$. □

Exemplo 8. *Sejam $u = 100, v = 101 \in V$ e os cones $S_1, S_2 \in \mathcal{D}_3$ cujas condições de fronteira são dadas por $S_1 : 0 < y < 2y < x$ e $S_2 : 0 < y < x < 2y$. A ordenação de $Spec(v) = \{0, x, y, x+y, 2y, x+2y\}$ é diferente em cada um dos cones. No cone S_1, ordenamos $Spec(v)$ da seguinte forma*

$$S := S_1 : 0 < y < 2y < x < x + y < x + 2y,$$

enquanto que, no cone S_2, a ordenação é dada por

$$\bar{S} := S_2 : 0 < y < x < 2y < x + y < x + 2y.$$

Note que $B^S_2(v) = \{101, 001, 100, 000\} \neq B^{\bar{S}}_2(v) = \{101, 001, 100, 111\}$ e, portanto, as formas ordenadas, $(\mathbb{D}^3_v)^*$ e $(\bar{\mathbb{D}}^3_v)^*$, correspondentes aos cones S e $\bar{S}$, respectivamente, são diferentes, conforme vemos a seguir:

$$(\mathbb{D}_v^3)^* = \begin{pmatrix} 3 & 2 & 6 & 5 & 2 & 1 & 5 & 4 \end{pmatrix}^t,$$
$$(\bar{\mathbb{D}}_v^3)^* = \begin{pmatrix} 4 & 2 & 6 & 5 & 2 & 1 & 5 & 3 \end{pmatrix}^t.$$

Analogamente, dadas as formas ordenadas $(\mathbb{D}_v^3)^*$ *e* $(\bar{\mathbb{D}}_v^3)^*$*, obtemos diretamente a sequência de bolas encaixadas descrita pelo critério de cada um dos cones.*

Por outro lado, a ordenação de $Spec(u) = \{0, x, y, x+y, 2x, 2x+y\}$ *é a mesma nos dois cones, ou seja,* $0 < y < x < x + y < 2x < 2x + y$*. Então,* $B_i^S(u) = B_i^{\bar{S}}(u)$*, para todo* $i > 0$*, e as formas ordenadas* $(\mathbb{D}_u^3)^*$ *e* $(\bar{\mathbb{D}}_u^3)^*$*, correspondentes aos cone* S *e* $\bar{S}$*, respectivamente, são iguais, conforme vemos a seguir:*

$$(\mathbb{D}_u^3)^* = (\bar{\mathbb{D}}_u^3)^* = \begin{pmatrix} 2 & 4 & 4 & 6 & 1 & 3 & 3 & 5 \end{pmatrix}^t.$$

A proposição anterior nos mostra que para um vetor v fixo e dois cones $S, \bar{S} \in \mathcal{D}_n$, as i-ésimas bolas com centro em v coincidem nestes cones se, e somente se, as formas ordenadas da coluna v, na matriz de distâncias, for a mesma, para S e $\bar{S}$. A proposição a seguir fortalece esta condição de igualdade de bolas quasi-métricas, no sentido de que, se para todo $v \in V$, todas as i-ésimas bolas coincidem, então os cones não podem ser distintos.

Proposição 8. *Sejam* $S, \bar{S} \in \mathcal{D}_n$*. Então,* $B_i^S(v) = B_i^{\bar{S}}(v)$*, para todo* $i \geq 0$ *e todo* $v \in V$*, se, e somente se,* $S = \bar{S}$*.*

Demonstração. Sejam $S, \bar{S} \in \mathcal{D}_n$. Suponha que para todo $v \in V$ e todo $i > 0$, tenhamos $B_i^S(v) = B_i^{\bar{S}}(v)$. Então, a última igualdade ocorre se, e somente se, $\mathbb{S}_i^S(v) = \mathbb{S}_i^{\bar{S}}(v)$, para todo $v \in V$ e todo $i > 0$, ou seja, se, e somente se, $(\mathbb{D}_v^n)^* = (\bar{\mathbb{D}}_v^n)^*$, para todo $v \in V$. Pela Proposição 6, a última igualdade ocorre se, e somente se, $S = \bar{S}$. □

Exemplo 9. *Sejam* $u = 100, v = 101 \in V$ *e considere os cones* $S_1, S_2, S_3, S_4 \in \mathcal{D}_3$*, conforme mostra a Figura 3.1.*

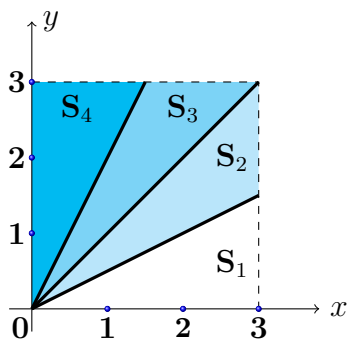


Figura 3.1: Partição do espaço $\mathfrak{Q}$ em cones convexos, para $n = 3$.

Para $x := \log_2(\frac{1}{p} - 1)$ *e* $y := \log_2(\frac{1}{q} - 1)$*, obtemos* $Spec(v)$*, ordenado em cada um dos cones, conforme mostra a Tabela 3.1.*

$Spec(v)$	$\delta_0(v)$	$\delta_1(v)$	$\delta_2(v)$	$\delta_3(v)$	$\delta_4(v)$	$\delta_5(v)$
S_1	0	y	2y	x	x+y	x+2y
S_2	0	y	x	2y	x+y	x+2y
S_3	0	x	y	x+y	2y	x+2y
S_4	0	x	y	x+y	2y	x+2y

Tabela 3.1: Ordenação do espectro de $v = 101$, em cada cone.

A partir da Tabela 3.1, contruímos a Tabela 3.2, que descreve, para cada cone, as i*-ésimas esferas centradas em* v*.*

$\mathbb{S}_j^{S_i}(v)$	$\mathbb{S}_0^{S_i}(v)$	$\mathbb{S}_1^{S_i}(v)$	$\mathbb{S}_2^{S_i}(v)$	$\mathbb{S}_3^{S_i}(v)$	$\mathbb{S}_4^{S_i}(v)$	$\mathbb{S}_5^{S_i}(v)$
S_1	{101}	{001,100}	{000}	{111}	{011,110}	{010}
S_2	{101}	{001,100}	{111}	{000}	{011,110}	{010}
S_3	{101}	{111}	{001,100}	{011,110}	{000}	{010}
S_4	{101}	{111}	{001,100}	{011,110}	{000}	{010}

Tabela 3.2: Ordenação das esferas com centro $v = 101$, em cada cone.

Note que, para $i > 0$*, a distância* $\delta_i(v)$ *pode mudar quando trocamos o cone e, portanto, as bolas quasi-métricas podem variar. Por exemplo,*

$$B_2^{S_1}(v) = \{101, 001, 100, 000\} \neq B_2^{S_2}(v) = \{101, 001, 100, 111\}$$

assim como

$$B_1^{S_2}(v) = \{101, 001, 100\} \neq B_1^{S_3}(v) = \{101, 111\}.$$

Por outro lado, $B_i^{S_3}(v) = B_i^{S_4}(v)$*, para todo* $i \geq 0$*, pois a ordenação de* $Spec(v)$ *é a mesma nos cones* S_3 *e* S_4*. Observe ainda que, apesar de* $Spec(v)$ *ser ordenado de maneira diferente nos cones* S_2 *e* S_3*, temos que* $B_2^{S_2}(v) = B_2^{S_3}(v)$*, ou seja, as bolas, consideradas como conjuntos são iguais embora sejam construídas de modo diferente, como pode ser visto na Tabela 3.2.*

Analogamente, a Tabela 3.3 mostra o conjunto $Spec(u)$*, ordenado em cada um dos cones e a Tabela 3.4 descreve as* i*-ésimas esferas centradas em* u*.*

$Spec(u)$	$\delta_0(u)$	$\delta_1(u)$	$\delta_2(u)$	$\delta_3(u)$	$\delta_4(u)$	$\delta_5(u)$
S_1	0	y	x	x+y	2x	2x+y
S_2	0	y	x	x+y	2x	2x+y
S_3	0	x	y	2x	x+y	2x+y
S_4	0	x	2x	y	x+y	2x+y

Tabela 3.3: Ordenação do espectro de $u = 100$, em cada cone.

$\mathbb{S}_j^{S_i}(v)$	$\mathbb{S}_0^{S_i}(v)$	$\mathbb{S}_1^{S_i}(v)$	$\mathbb{S}_2^{S_i}(v)$	$\mathbb{S}_3^{S_i}(v)$	$\mathbb{S}_4^{S_i}(v)$	$\mathbb{S}_5^{S_i}(v)$
S_1	{100}	{000}	{110,101}	{010,001}	{111}	{011}
S_2	{100}	{000}	{110,101}	{010,001}	{111}	{011}
S_3	{100}	{110,101}	{000}	{111}	{010,001}	{011}
S_4	{100}	{110,101}	{111}	{000}	{010,001}	{011}

Tabela 3.4: Ordenação das esferas com centro $u = 100$, em cada cone.

Seja $S \in \mathcal{D}_3$ um cone fixo. Comparando $B_i^S(u)$ com $B_i^S(v)$, vemos que estas bolas são diferentes para alguns valores de i. Por exemplo, $|\mathbb{S}_1^{S_1}(v)| = 2 \neq 1 = |\mathbb{S}_1^{S_1}(u)|$. Isto mostra claramente como o peso de Hamming do centro de uma bola quasi-métrica interfere na construção desta bola, para $i > 0$, diferente do que ocorre com as bolas de Hamming que sempre têm o mesmo tamanho, a cada etapa i, independente do centro da bola.

Essas considerações são importantes quando discutimos a correção de erros, já que identificamos os erros mais prováveis de acordo com a sequência de raios de uma bola quasi-métrica centrada em v. De modo mais preciso, se $\delta_{p,q}^n(v,u) = \delta_i(v)$ e $\delta_{p,q}^n(v,w) = \delta_j(v)$, temos $\mathbb{P}_{p,q}^n(u|v) \geq \mathbb{P}_{p,q}^n(w|v)$ se, e somente se, $i \leq j$.

Para $v \in V$, a cardinalidade de $Spec(v)$ nos dá a quantidade total de bolas centradas em v e essa quantidade independe do cone S. Nosso objetivo, nesta seção, é caracterizar as bolas quasi-métricas $B_i^S(v)$ a fim de buscar condições para a correção de erros ocorridos a partir de uma mensagem v, transmitida por um $BAC^n(p,q)$.

Lema 2. *Sejam $u, v \in V$ e $\delta_i(v) \in Spec(v)$, para $i \in \{0, 1, \ldots, \sigma_v - 1\}$. Então, para todo $u \in B_i^S(v)$, temos $d_H(v,u) \leq i$.*

Demonstração. Seja $v \in V$ e considere a ordenação de $Spec(v)$

$$\delta_0(v) < \delta_1(v) < \ldots < \delta_i(v) < \delta_{i+1}(v) < \ldots < \delta_{\sigma_v - 1}(v).$$

Usaremos o Princípio de Indução Finita em i, para demonstrar este resultado. Para $i = 0, 1$ não há o que demonstrar.

Suponha que para todo $u \in B_i^S(v)$, vale a desigualdade $d_H(v,u) \leq i$ e considere a bola $B_{i+1}^S(v)$. Então, temos

$$B_i^S(v) \subseteq B_{i+1}^S(v) = B_i^S(v) \cup \mathbb{S}_{i+1}^S(v).$$

Para todo $w \in B_{i+1}^S(v)$, existe $u \in B_i^S(v)$ tal que $d_H(u,w) = 1$. De fato, seja $\delta = (v_i)_{i=0}^l$ um caminho geodésico ligando o ponto inicial v ao ponto final w. Considere

$$j = \max\{k \in \mathbb{N} \mid v_k \in B_i^S(v)\}.$$

Se $j < l-1$, então $j+1 < l$ e

$$\delta_i(v) < \underbrace{\delta^n_{p,q}(v, v_{j+1})}_{\delta_{i+1}(v)} < \delta^n_{p,q}(v, w).$$

Segue que $\delta^n_{p,q}(v,w) \geq \delta_{i+2}(v)$ e, portanto, $w \notin B^S_{i+1}(v)$, o que contradiz a hipótese. Assim sendo, $j = l-1$ e δ é uma geodésica, com $l = d_H(v,w)$ arestas de um grafo bi orientado G. Seja $u = v_{l-1} \in B^S_i(v)$, então $d_H(u,w) = 1$, pois a geodésica δ é descrita sobre as arestas do grafo bi-orientado G. Além disso, $d_H(\cdot,\cdot)$ é uma métrica e, portanto, satisfaz a Desigualdade Triangular da qual obtemos

$$d_H(v,w) \leq d_H(v,u) + d_H(u,w) \leq i+1,$$

o que conclui a demonstração. □

Exemplo 10. *Retomando os resultados obtidos no Exemplo 9, de acordo com a Tabela 3.2, consideramos cada elemento $w \in \mathbb{S}^{S_j}_i(v)$, para $i = 1, 2, \ldots, 5$, e calculamos a distância de Hamming $d_H(v,w)$, em cada cone S_j, com $j = 1, 2, 3, 4$. Os resultados são apresentados na Tabela 3.5.*

	$\mathbb{S}^{S_j}_0(v)$	$\mathbb{S}^{S_j}_1(v)$	$\mathbb{S}^{S_j}_2(v)$	$\mathbb{S}^{S_j}_3(v)$	$\mathbb{S}^{S_j}_4(v)$	$\mathbb{S}^{S_j}_5(v)$
S_1	0	1	2	1	2	3
S_2	0	1	1	2	2	3
S_3	0	1	1	2	2	3
S_4	0	1	1	2	2	3

Tabela 3.5: Distância de Hamming de $w \in \mathbb{S}^{S_j}_i(v)$ até v, em cada cone.

Uma vez que $B^{S_j}_i(v) = \bigcup_{k=0}^{i} \mathbb{S}^{S_j}_k(v)$, para todo $i \geq 0$, pode-se ver na Tabela 3.5 que $d_H(v,w) \leq i$, para todo $w \in B^{S_j}_i(v)$.

Analogamente, para $u = 100$, obtemos a Tabela 3.6 e notamos que $d_H(u,w') \leq i$, para todo $w' \in B^{S_j}_i(u)$. Novamente, note a diferença entre as tabelas, para um cone fixo, refletindo a variação das bolas quasi-métricas centradas em vetores com diferentes pesos de Hamming.

$\mathbb{S}^{S_i}_j(v)$	$\mathbb{S}^{S_i}_0(v)$	$\mathbb{S}^{S_i}_1(v)$	$\mathbb{S}^{S_i}_2(v)$	$\mathbb{S}^{S_i}_3(v)$	$\mathbb{S}^{S_i}_4(v)$	$\mathbb{S}^{S_i}_5(v)$
S_1	0	1	1	2	2	3
S_2	0	1	1	2	2	3
S_3	0	1	1	2	2	3
S_4	0	1	2	1	2	3

Tabela 3.6: Distância de Hamming de $w' \in \mathbb{S}^{S_j}_i(u)$ até u, em cada cone.

Proposição 9. *Sejam $\mathbf{0}^n, \mathbf{1}^n \in V$. Então, para cada $i \geq 0$, tem-se que*

$$|B_i(\mathbf{0}^n)| = |B_i(\mathbf{1}^n)|.$$

Demonstração. Sejam $\mathbf{0}^n, \mathbf{1}^n \in V$ e $B_i(\mathbf{0}^n)$ e $B_i(\mathbf{1}^n)$ as correspondentes i-ésimas bolas com centro $\mathbf{0}^n$ e $\mathbf{1}^n$, respectivamente, com $i \geq 0$. Então, para $x := \log_2(\frac{1}{p}-1)$ e $y := \log_2(\frac{1}{q}-1)$, obtemos $\delta_i(\mathbf{0}^n) = i \cdot x$, $\delta_i(\mathbf{1}^n) = i \cdot y$ e as cardinalidades das correspondentes bolas quasi-métricas são dadas por

$$|B_i(\mathbf{0}^n)| = |B_i(\mathbf{1}^n)| = \sum_{j=0}^{i} \binom{n}{j}.$$

Note que para $\mathbf{v} \in \{\mathbf{0}^n, \mathbf{1}^n\}$, temos $|B_i(\mathbf{v})| = |B_i^H(\mathbf{v})|$, onde $B_i^H(\mathbf{v})$ denota a i-ésima bola de Hamming com centro $\mathbf{v}$. □

Teorema 4. *Seja $v \in V$. A cardinalidade da i-ésima bola com centro v em um cone $S \in \mathcal{D}_n$ é dada por*

$$|B_i^S(v)| = \sum_{j=0}^{i} b_j,$$

onde $b_j = \binom{\omega_H(v)}{|e_q|_j}\binom{n-\omega_H(v)}{|e_p|_j}$, para todo $i \in \{0, 1, \ldots, \sigma_v - 1\}$.

Demonstração. Sejam $S \in \mathcal{D}_n$ e $v \in V$ tal que $\omega := \omega_H(v)$ e $\sigma_v := |Spec(v)|$. Uma vez que

$$B_0^S(v) \subseteq B_1^S(v) \subseteq B_2^S(v) \subseteq \ldots \subseteq B_i^S(v) \subseteq B_{i+1}^S(v),$$

a cardinalidade das bolas define a relação de recorrência dada por

$$\begin{cases} |B_{i+1}^S(v)| &= |B_i^S(v)| + b_{i+1}, \\ |B_0^S(v)| &= 1, \end{cases} \tag{3.2}$$

em que

$$b_{i+1} = \binom{\omega}{|e_q|_{i+1}}\binom{n-\omega}{|e_p|_{i+1}}.$$

representa a quantidade de elementos da esfera $\mathbb{S}_{i+1}^S(v)$ cujo raio é dado por

$$\delta_{i+1}(v) = |e_p|_{i+1} \cdot x + |e_q|_{i+1} \cdot y,$$

para $i \in \{0, 1, \ldots, \sigma_v - 2\}$, $x := \log_2(\frac{1}{p} - 1)$, $y := \log_2(\frac{1}{q} - 1)$ e $|e_p|_{i+1}$, $|e_q|_{i+1}$ denotando a quantidade de arestas na direção $0 \to 1$ e $1 \to 0$, respectivamente, na distância $\delta_{i+1}(v)$.

Então, para $j \in \{0, 1, \ldots, i\}$ consideramos o somatório de $j = 0$ até i, aplicado

à relação (3.2):

$$\sum_{j=0}^{i} |B_{j+1}^{S}(v)| \overset{(3.2)}{=} \sum_{j=0}^{i} |B_{j}^{S}(v)| + \sum_{j=0}^{i} b_{j+1}$$

e obtemos

$$|B_{i+1}(v)| = 1 + \sum_{j=0}^{i} \binom{\omega}{|e_q|_{j+1}} \binom{n-\omega}{|e_p|_{j+1}},$$

para $0 \leq i \leq \sigma_v - 2$ e $B_0^S(v) = 1$. □

Note que a cardinalidade de uma bola $B_i^S(v)$ depende do peso de Hamming de v, da dimensão n e do cone S (pois $|e_p|$ e $|e_q|$ dependem de v e do cone S ao qual (p, q) pertence). Portanto, esta cardinalidade pode mudar quando variamos o cone, conforme mostra o exemplo a seguir.

Exemplo 11. *Seja $v = 101 \in V$ e considere as bolas obtidas no Exemplo 9. A Tabela 3.7 mostra a cardinalidade das i-ésimas esferas, para $i = 0, 1, \ldots, 5$. Uma vez que $|B_i^S(v)| = \sum_{j=0}^{i} |\mathbb{S}_j^S(v)|$, note como varia a cardinalidade da i-ésima bola quando trocamos o cone. Por exemplo, $|B_3^{S_2}(v)| = 5 \neq 6 = |B_3^{S_3}(v)|$.*

$\lvert\mathbb{S}_i^{S_j}(v)\rvert$	$\lvert\mathbb{S}_0^{S_j}(v)\rvert$	$\lvert\mathbb{S}_1^{S_j}(v)\rvert$	$\lvert\mathbb{S}_2^{S_j}(v)\rvert$	$\lvert\mathbb{S}_3^{S_j}(v)\rvert$	$\lvert\mathbb{S}_4^{S_j}(v)\rvert$	$\lvert\mathbb{S}_5^{S_j}(v)\rvert$
S_1	1	2	1	1	2	1
S_2	1	2	1	1	2	1
S_3	1	1	2	2	1	1
S_4	1	1	2	2	1	1

Tabela 3.7: Cardinalidade das esferas com centro $v = 101$, em cada cone.

Considere agora $u = 100 \in V$. Então, novamente obtemos uma Tabela 3.8 com as cardinalidades das i-ésimas esferas centradas em u, para cada cone $S \in \mathcal{D}_3$. Repare que, na Tabela 3.7, a sequência de cardinalidades para todo $S \in \mathcal{D}_3$ difere da sequência apresentada para o mesmo cone, na Tabela 3.8. Este fato decorre do que foi discutido no Exemplo 9 sobre como o peso de Hamming interfere na contrução de uma bola quasi-métrica.

$\lvert\mathbb{S}_i^{S_j}(u)\rvert$	$\lvert\mathbb{S}_0^{S_j}(u)\rvert$	$\lvert\mathbb{S}_1^{S_j}(u)\rvert$	$\lvert\mathbb{S}_2^{S_j}(u)\rvert$	$\lvert\mathbb{S}_3^{S_j}(u)\rvert$	$\lvert\mathbb{S}_4^{S_j}(u)\rvert$	$\lvert\mathbb{S}_5^{S_j}(u)\rvert$
S_1	1	1	2	2	1	1
S_2	1	1	2	2	1	1
S_3	1	2	1	1	2	1
S_4	1	2	1	1	2	1

Tabela 3.8: Cardinalidade das esferas com centro $u = 100$, em cada cone.

Corolário 3. *Sejam $u, v \in V$ e $S \in \mathcal{D}_n$. Se $\omega_H(v) = \omega_H(u)$, então $|B_i^S(v)| = |B_i^S(u)|$, para todo $i \in \{0, 1, \ldots, \sigma - 1\}$, com $\sigma := |Spec(v)| = |Spec(u)|$.*

Demonstração. A demonstração segue imediatamente do Teorema 4 e do fato de $Spec(u) = Spec(v)$. □

A recíproca do último corolário não é verdadeira.

Exemplo 12. *Sejam $u = 100, v = 101 \in V$. Considere a linha correspondente ao cone S_2 nas Tabelas 3.7 e 3.8, do Exemplo 11. Note que $|B_2^{S_2}(v)| = 4 = |B_2^{S_2}(u)|$, mas $\omega_H(v) = 2 \neq \omega_H(u) = 1$. Portanto, vetores com pesos de Hamming diferentes podem ter suas correspondentes i-ésimas bolas quasi-métricas com mesma cardinalidade.*

Proposição 10. *Seja $v \in V$. A cardinalidade da i-ésima bola em um cone $S \in \mathcal{D}_n$, está limitada por*

$$1 \leq |B_i^S(v)| \leq |B_i(\mathbf{0}^n)| = |B_i(\mathbf{1}^n)|,$$

para todo $i \in \{0, 1, \ldots, \sigma_v - 1\}$, com $\sigma_v = |Spec(v)|$.

Demonstração. Sejam $v \in V$ e um cone $S \in \mathcal{D}_n$. Para $0 \leq i \leq \sigma_v - 1$, é claro que $|B_i^S(v))| \geq 1$ com igualdade para $i = 0$. Seja $u \in B_i^S(v)$. Pelo Lema 2, tem-se que a distância de Hamming $d_H(v, u) \leq i$, ou seja, $\omega_H(v - u) \leq i$. Portanto, para todo $u \in B_i^S(v)$, tem-se que $v - u \in B_i(\mathbf{0}^n)$ o que nos garante que $|B_i(\mathbf{0}^n)| \geq |B_i^S(v)|$. □

3.2 Distância mínima

Seja $\mathcal{C} \subseteq \mathbb{F}_2^n$ um código e $S \in \mathcal{D}_n$. A distância mínima de $\mathcal{C}$, em $z = (x, y) \in S$, é definida por

$$\delta_z^*(\mathcal{C}) = \min_{\substack{c, \bar{c} \in \mathcal{C} \\ i \neq j}} \Big\{ \delta_z^n(c, \bar{c}) \Big\}.$$

Observe que precisamos considerar as distâncias $\delta_z^n(\bar{c}, c)$ e $\delta_z^n(c, \bar{c})$ para calcular a distância mínima entre as palavras código. Se considerarmos $\mathcal{C} \subseteq \mathbb{F}_2^n$ como um código linear, então a estrutura de espaço vetorial sobre $\mathbb{F}_2^n$ nos permite obter uma expressão fechada para $\delta_z^*(\mathcal{C})$, como veremos a seguir.

Observação 6. *Ao longo desta seção, usaremos as definições*

$$x := \log_2(\frac{1}{p} - 1) \ \text{ e } \ y := \log_2(\frac{1}{q} - 1).$$

Lema 3. *Seja $\mathcal{C} \subseteq \mathbb{F}_2^n$ um código linear (com distância mínima de Hamming $d_H^*(\mathcal{C})$) e considere um cone $S \in \mathcal{D}_n$. Então existe $c \in \mathcal{C}$ tal que $\delta_z^n(c, 0) = d_H^*(\mathcal{C}) \cdot y$ e $\delta_z^n(0, c) = d_H^* \cdot x$, para $z \in S$.*

Demonstração. Sejam $\mathcal{C} \subseteq \mathbb{F}_2^n$ um código linear (com distância mínima de Hamming $d_H^*(\mathcal{C})$) e considere um cone $S \in \mathcal{D}_n$. Uma vez que $\mathcal{C}$ é um código linear, existe $c \in \mathcal{C}$ com peso de Hamming $\omega_H(c) = d_H^*$. Daí, segue imediatamente que $\delta_{p,q}^n(c, 0) = d_H^*(\mathcal{C}) \cdot y$ e $\delta_{p,q}^n(0, c) = d_H^*(\mathcal{C}) \cdot x$. □

Teorema 5. *Seja $\mathcal{C} \subseteq \mathbb{F}_2^n$ um código linear (com distância mínima de Hamming $d_H^*(\mathcal{C})$) e $S \in \mathcal{D}_n$. A distância mínima de $\mathcal{C}$, em um canal $z = (x, y) \in S$, é dada por*

$$\delta_z^*(\mathcal{C}) = d_H^*(\mathcal{C}) \cdot \min\{x, y\}.$$

Demonstração. Seja $\mathcal{C}$ um código linear. Então, existe $c_0 \in \mathcal{C}$ com peso de Hamming $\omega_H(c_0) = d_H^*(\mathcal{C})$. Suponha $x < y$. Então, se para $\alpha^*, \beta^* \in \mathbb{N}$ temos $\alpha^* + \beta^* = d_H^*(\mathcal{C})$, a seguinte relação é válida:

$$\delta_z^n(0, c_0) = d_H^*(\mathcal{C}) \cdot x \leq \alpha^* x + \beta^* y \leq d_H^*(\mathcal{C}) \cdot y. \tag{3.3}$$

Sejam $c, \bar{c} \in \mathcal{C}$ tal que $\delta_z^n(c, \bar{c}) = \alpha x + \beta y$ e $\alpha + \beta = d_H(c, \bar{c})$. Uma vez que $d_H^*(\mathcal{C}) \leq d_H(c, \bar{c})$, existem $c_1, c_2 \in \mathcal{C}$ tais que $d_H(c_1, c_2) = d_H^*(\mathcal{C})$ e $\delta_z^n(c_1, c_2) = \alpha^* x + \beta^* y$. Assim sendo, existem $\alpha^*, \beta^* \in \mathbb{N}$, tais que $\alpha^* \leq \alpha$ e $\beta^* \leq \beta$ e, portanto, $\delta_z^n(c_1, c_2) \leq \delta_z^n(c, \bar{c})$, para todo $c, \bar{c} \in \mathcal{C}$. Por (3.3), obtemos que $\delta_z^n(0, c_0) \leq \delta_z^n(c, \bar{c})$, para todo $c, \bar{c} \in \mathcal{C}$.

Analogamente, se $y < x$, $\delta_z^n(c_0, 0) \leq \delta_z^n(c, \bar{c})$, para todo $c, \bar{c} \in \mathcal{C}$. Portanto, a distância mínima do código $\mathcal{C}$ é dada por $\delta_z^*(\mathcal{C}) = d_H^*(\mathcal{C}) \cdot \min\{x, y\}$. □

Note que $\delta_z^*(\mathcal{C})$ é um valor que depende do código linear $\mathcal{C}$ (pois depende da distância mínima de Hamming deste código) e do canal $z = (x, y) \in S$, já que depende do mínimo entre x e y. Assim sendo, dado um código linear $\mathcal{C}$, a distância $\delta_z^*(\mathcal{C})$ é fixa nas curvas determinadas por $\min\{x, y\} = k$, conforme ilustra a Figura 3.2.

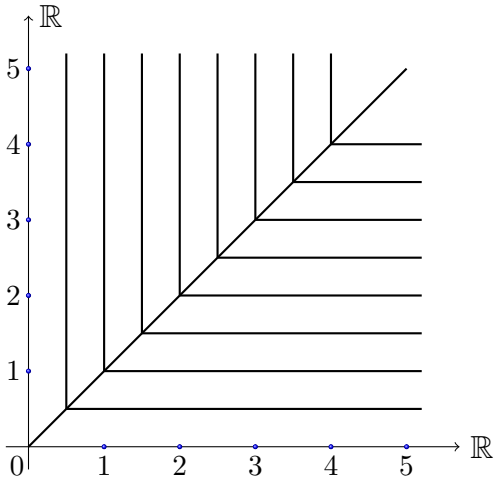


Figura 3.2: As curvas de nível de $\delta_z^*(\mathcal{C})$.

A linearidade do código $\mathcal{C}$ é uma condição necessária para que o último teorema seja válido, caso contrário, não podemos garantir que exista uma palavra $c \in \mathcal{C}$ tal que $\delta_z^n(0,c) = d_H^*(\mathcal{C}) \cdot x$ e $\delta_z^n(c,0) = d_H^*(\mathcal{C}) \cdot y$, conforme vemos no exemplo a seguir.

Exemplo 13. *Seja $\mathcal{C} = \{110, 011, 101\} \subseteq \mathbb{F}_2^3$ um código. Este código é **não** linear, com distância mínima de Hamming $d_H^*(\mathcal{C}) = 2$. Considere o cone $S_1 \in \mathcal{D}_3$. Então, para um canal $z = (x,y) \in S_1$, temos que $\delta_z^3(c,\bar{c}) = x + y$, para todo $c, \bar{c} \in \mathcal{C}$ e*

$$\delta_z^*(\mathcal{C}) = x + y \neq 2 \cdot \min\{x, y\}.$$

Um dos resultados conhecidos na literatura, para códigos lineares, é a *Cota de Singleton*, [15], [18]. Como consequência desse resultado, obtemos um limitante superior para $\delta_z^*(\mathcal{C})$, ou seja, dado um código linear $\mathcal{C} \subseteq \mathbb{F}_2^n$, de dimensão k, temos

$$\delta_z^*(\mathcal{C}) \leq (n - k + 1) \cdot \min\{x, y\},$$

para $z = (x,y) \in S \in \mathcal{D}_n$.

Exemplo 14. *Seja $\mathcal{C} = \{000, 100, 011, 111\} \subseteq \mathbb{F}_2^3$ um código linear e $S \in \mathcal{D}_3$. Então, para um canal $z = (x,y) \in S$, a distância mínima do código é dada por*

$$\delta_z^*(\mathcal{C}) = \min\{y, x, 2y, 2x, 3y, 3x, x + 2y, y + 2x\}$$

e, pela Cota de Singleton, obtemos que $\delta_z^*(\mathcal{C}) \leq 2 \cdot \min\{x, y\}$.

Considerando os critérios de codificação de cada cone $S \in \mathcal{D}_3$, obtemos que

$$\delta_z^*(\mathcal{C}) = \begin{cases} y, & \text{para} \quad z \in S_1 \cup S_2; \\ x, & \text{para} \quad z \in S_3 \cup S_4; \end{cases}$$

Definição 16. *Considere um código $\mathcal{C} \subseteq \mathbb{F}_2^n$ e $S \in \mathcal{D}_n$. Para $z = (x,y) \in S$, a distância mínima de uma palavra código $c \in \mathcal{C}$ é dada por*

$$\delta_{z,\mathcal{C}}^*(c) = \min_{0 \neq \bar{c} \in \mathcal{C}} \left\{ \delta_z^n(c, \bar{c}) \right\}. \tag{3.4}$$

A distância mínima do código $\mathcal{C}$ é dada por $\delta_z^*(\mathcal{C}) = \min_{c \in \mathcal{C}} \left\{ \delta_{z,\mathcal{C}}^*(c) \right\}$.

A Definição 16 é uma medida mais refinada para o código $\mathcal{C}$, pois nos fornece informações sobre a palavra código c, no sentido de permitir uma descrição mais precisa dos tipos de erros que ocorrem a partir do envio de c. Logo, temos mais informação sobre o conjunto de mensagens corrigíveis quando enviamos a palavra código c.

3.3 Raio de empacotamento

Nesta seção apresentamos uma generalização da definição de raio de empacotamento obtida para o caso clássico. Posteriormente, mostraremos que, devido à assimetria do problema, podemos refinar esta medida e definir um raio de empacotamento que depende não somente do canal mas também do cone e da palavra código.

Definição 17. *Considere um código $\mathcal{C} \subseteq \mathbb{F}_2^n$ e $S \in \mathcal{D}_n$. Para um canal $z = (x, y) \in S$, seja $Spec_z = Spec_z(\mathbb{F}_2^n)$. Definimos o raio de empacotamento do código $\mathcal{C}$, por*

$$R_z(\mathcal{C}) = \max\big\{R \in Spec_z \;\big|\; B(c;R) \cap B(\bar{c};R) = \emptyset, \text{ para todo } \bar{c} \in \mathcal{C}\big\}.$$

Proposição 11. *Considere um código linear $\mathcal{C} \subseteq \mathbb{F}_2^n$ e $S \in \mathcal{D}_n$. Para um canal $z = (x, y) \in S$, o raio de empacotamento de $\mathcal{C}$ é dado por*

$$R_z(\mathcal{C}) = \Big[\frac{d_H^*(\mathcal{C}) - 1}{2}\Big] \cdot \min\{x, y\},$$

em que $d_H^*(\mathcal{C})$ denota a distância mínima de Hamming de $\mathcal{C}$.

Demonstração. Seja $\mathcal{C} \subseteq \mathbb{F}_2^n$ um código linear e $S \in \mathcal{D}_n$. Para um canal $z = (x, y) \in S$, considere $R_z(\mathcal{C}) = \left[\frac{d_H^*(\mathcal{C})-1}{2}\right] \cdot \min\{x, y\}$ e suponha que exista $v \in V$ tal que $v \in B\big(c, R_z(\mathcal{C})\big) \cap B\big(\bar{c}; R_z(\mathcal{C})\big)$, para $c, \bar{c} \in \mathcal{C}$. Então, a desigualdade triangular, aplicada à métrica de Hamming, juntamente com a condição de que $m := \min\{x, y\} > 0$, nos fornece a seguinte desigualdade:

$$d_H(c, \bar{c}) \cdot m \leq d_H(c, v) \cdot m + d_H(v, \bar{c}) \cdot m. \tag{3.5}$$

Mas, $d_H(c, \bar{c}) = d_H(c - \bar{c}, 0)$ e, uma vez que o código $\mathcal{C}$ é linear, temos que $c - \bar{c} \in \mathcal{C}$. Portanto, $d_H(c, \bar{c}) \geq d_H^*(\mathcal{C})$.

Além disso, temos que $d_H(c, v) \leq \big[\frac{d_H^*(\mathcal{C})-1}{2}\big]$ e $d_H(\bar{c}, v) \leq \big[\frac{d_H^*(\mathcal{C})-1}{2}\big]$. De fato, se $v \in B(c; R_z(\mathcal{C}))$, então $\delta_z^n(c, v) \leq R_z(\mathcal{C})$ e, portanto,

$$\begin{cases} \delta_z^n(c, v) = & |e_p|x + |e_q|y & \leq R_z(\mathcal{C}) \\ d_H(c, v) = & |e_p| + |e_q|, \end{cases} \tag{3.6}$$

onde $|e_p|$ e $|e_q|$ denotam a quantidade de trocas do tipo $0 \to 1$ e $1 \to 0$, respectivamente. Apenas para simplificar a notação, vamos denotar $R := \big[\frac{d_H^*(\mathcal{C})-1}{2}\big]$. Assim sendo, temos dois casos:

1. Se $m = x$, temos $R_z(\mathcal{C}) = R \cdot x$ e, por (3.6), obtemos $|e_p|x + |e_q|y \leq Rx$ se, e somente se, $(|e_p| - R) \cdot x + |e_q| \cdot y \leq 0$. Como $m = x$, temos $(|e_p| + |e_q| - R) \cdot x \leq 0$. Logo, $(|e_p| + |e_q| - R) \leq 0$, pois $x > 0$ e segue que $d_H(c, v) \leq R$. Portanto, se $v \in B(c; R_z(\mathcal{C}))$, então $d_H(c, v) \leq R$.

2. Se $m = y$, a demonstração é análoga.

Já que $v \in B(\bar{c}; R_z(\mathcal{C}))$, o mesmo vale para v, ou seja, $d_H(\bar{c}, v) \leq R$.
Estes últimos fatos, juntamente com a relação (3.5) nos leva à contradição

$$d_H^*(\mathcal{C}) \cdot m \leq (d_H^*(\mathcal{C}) - 1) \cdot m,$$

Portanto, $B\big(c, R_z(\mathcal{C})\big) \cap B\big(\bar{c}; R_z(\mathcal{C})\big) = \emptyset$ e segue da Definição 17 que $R_z(\mathcal{C})$ é o raio de empacotamento do código $\mathcal{C}$. □

Exemplo 15. *Considere o código linear $\mathcal{C} = \{0000, 1111\}$ e o cone $S_1 \in \mathcal{D}_4$ cujo critério de codificação é dado por $0 < y < 2y < 3y < x < 4y$. Pela Proposição 11, obtemos $R_z(\mathcal{C}) = y$, para um canal $z = (x, y) \in S_1$ e as bolas quasi-métricas, de raio $R_z(\mathcal{C}) = y$, são dadas por:*

$$B(0000; y) = \{0000\}$$
$$B(1111; y) = \{1111, 0111, 1011, 1101, 1110\}.$$

Note que, assim como o canal é assimétrico, a correção de erros também é. De modo mais preciso, vemos que se enviamos $c = 0000$, nenhuma mensagem recebida é corrigível. Por outro lado, se enviamos $\bar{c} = 1111$, o conjunto de mensagens corrigíveis é dado por $\{0111, 1011, 1101, 1110\}$.

O Exemplo 15 sugere que $R_z(\mathcal{C})$ é uma medida grosseira para correção de erros e isto nos motiva à próxima definição.

Definição 18. *Considere um código $\mathcal{C} \subseteq \mathbb{F}_2^n$ e $S \in \mathcal{D}_n$. O raio de empacotamento de uma palavra código $c \in \mathcal{C}$, em um canal $z = (x, y) \in S$, é definido por*

$$\mathcal{R}_{\mathcal{C}}^z(c) = \max_{\delta(c) \in Spec(c)} \Big\{ \delta(c) \;\Big|\; B\big(c; \delta(c)\big) \cap B\big(\bar{c}; \delta(c)\big) = \emptyset, \text{ para todo } c \neq \bar{c} \in \mathcal{C} \Big\}.$$

Neste sentido, o código $\mathcal{C}$ é caracterizado por uma sequência de raios de empacotamento

$$\mathcal{R}_{\mathcal{C}}^z = \big(\mathcal{R}_{\mathcal{C}}^z(c)\big)_{c \in \mathcal{C}}.$$

É imediato ver que a Definição 18 é um refinamento do caso clássico, pois $\mathcal{R}^z(\mathcal{C}) = \min_{c \in \mathcal{C}} \big\{ \mathcal{R}_{\mathcal{C}}^z(c) \big\}$.

Proposição 12. *Considere um código linear $\mathcal{C} \subseteq \mathbb{F}_2^n$ e $S \in \mathcal{D}_n$. Para todo $c \in \mathcal{C}$, o raio de empacotamento $\mathcal{R}_{\mathcal{C}}^z(c)$, em um canal $z = (x, y) \in S$, está limitado por*

$$\mathcal{R}^z(\mathcal{C}) \leq \mathcal{R}_{\mathcal{C}}^z(c) < \delta_{z,\mathcal{C}}^*(c).$$

Demonstração. A demonstração segue diretamente da Definição 18 e da Proposição 11. □

Note que $\mathcal{R}^z_{\mathcal{C}}(c)$ depende do código $\mathcal{C}$, da palavra código $c \in \mathcal{C}$, do canal $z = (x, y) \in S$ e do cone S. De modo mais preciso, dados dois canais $z, \bar{z} \in S$, o raio de empacotamento de c **muda de valor com a mudança do canal**, mas caracteriza os mesmos tipos de erros nos dois canais. Este fato será demonstrado na próxima proposição.

Antes de apresentá-la vamos definir, com um certo abuso de linguagem, que para $c \in \mathcal{C}$ e $z, \bar{z} \in S$, os raios de empacotamento $\mathcal{R}^z_{\mathcal{C}}(c)$ e $\mathcal{R}^{\bar{z}}_{\mathcal{C}}(c)$ são congruentes se, e somente se, estes raios caracterizam os mesmos tipos de erro (α, β), ou seja,

$$\mathcal{R}^z_{\mathcal{C}}(c) \cong \mathcal{R}^{\bar{z}}_{\mathcal{C}}(c) \Longleftrightarrow \mathcal{R}^z_{\mathcal{C}}(c) = \alpha x + \beta y \text{ e } \mathcal{R}^{\bar{z}}_{\mathcal{C}}(c) = \alpha \bar{x} + \beta \bar{y}.$$

Proposição 13. *Sejam $S, \bar{S} \in \mathcal{D}_n$, com $S \neq \bar{S}$.*

(a) *Considere um código linear $\mathcal{C} \subseteq \mathbb{F}_2^n$ e dois canais $z = (x, y), \bar{z} = (\bar{x}, \bar{y}) \in S$. Para todo $c \in \mathcal{C}$, temos $R^z_{\mathcal{C}}(c) \cong R^{\bar{z}}_{\mathcal{C}}(c)$.*

(b) *Se $z = (x, y) \in S$ e $\bar{z} = (\bar{x}, \bar{y}) \in \bar{S}$, então existe código linear $\mathcal{C}$ tal que $R^z_{\mathcal{C}}(c) \ncong R^{\bar{z}}_{\mathcal{C}}(c)$, para algum $c \in \mathcal{C}$.*

Demonstração. Sejam $S, \bar{S} \in \mathcal{D}_n$, com $S \neq \bar{S}$.

(a) Considere um código linear $\mathcal{C} \subseteq \mathbb{F}_2^n$ e dois canais $z = (x, y), \bar{z} = (\bar{x}, \bar{y}) \in S$.

Uma vez que S é classe de equivalência, temos que $z \sim \bar{z}$ e, consequentemente,

$$R^z_{\mathcal{C}}(c) = \alpha x + \beta y \text{ e } R^{\bar{z}}_{\mathcal{C}}(c) = \alpha \bar{x} + \beta \bar{y}.$$

Logo, $\mathcal{R}^z_{\mathcal{C}}(c) \cong \mathcal{R}^{\bar{z}}_{\mathcal{C}}(c)$.

(b) Seja $r \in \mathcal{L}_n(S, \bar{S})$ uma reta que separa os cones S e $\bar{S}$ e definida por $\beta y = \alpha x$, com $\alpha + \beta = n$. Considere o código linear $\mathcal{C} = \{0^n, 1^n\}$. Então, se S é o cone que está abaixo da reta r, dado um canal $z = (x, y) \in S$, temos $\beta y < \alpha x$, de onde obtemos que $\mathcal{R}^{\bar{z}}_{\mathcal{C}}(0^n) = (\alpha - 1)x$ e $\mathcal{R}^{\bar{z}}_{\mathcal{C}}(1^n) = \beta y$. Por outro lado, o cone $\bar{S}$ está acima da reta r e, portanto, dado um canal $\bar{z} = (\bar{x}, \bar{y}) \in \bar{S}$, temos $\alpha \bar{x} < \beta \bar{y}$, de onde obtemos que $\mathcal{R}^{\bar{z}}_{\mathcal{C}}(0^n) = \alpha x$ e $\mathcal{R}^{\bar{z}}_{\mathcal{C}}(1^n) = (\beta - 1)y$.

Logo, $\mathcal{R}^z_{\mathcal{C}}(0^n) \ncong \mathcal{R}^{\bar{z}}_{\mathcal{C}}(0^n)$ e $\mathcal{R}^{\mathcal{C}}_z(1^n) \ncong R^{\mathcal{C}}_{\bar{z}}(1^n)$ o que conclui a demonstração. □

Exemplo 16. *Considere novamente o código do Exemplo 15: $\mathcal{C} = \{0000, 1111\}$ e o cone $S_1 \in \mathcal{D}_4$. Para um canal $z = (x, y) \in S_1$, temos que $\mathcal{R}^z_{\mathcal{C}}(0000) = y$ e $\mathcal{R}^z_{\mathcal{C}}(1111) = 3y$.*

A Figura 3.3 ilustra as bolas quasi-métricas com o raio de empacotamento do código, $\mathcal{R}^z(\mathcal{C}) = y$ e os correspondentes conjunto de mensagens corrigíveis.

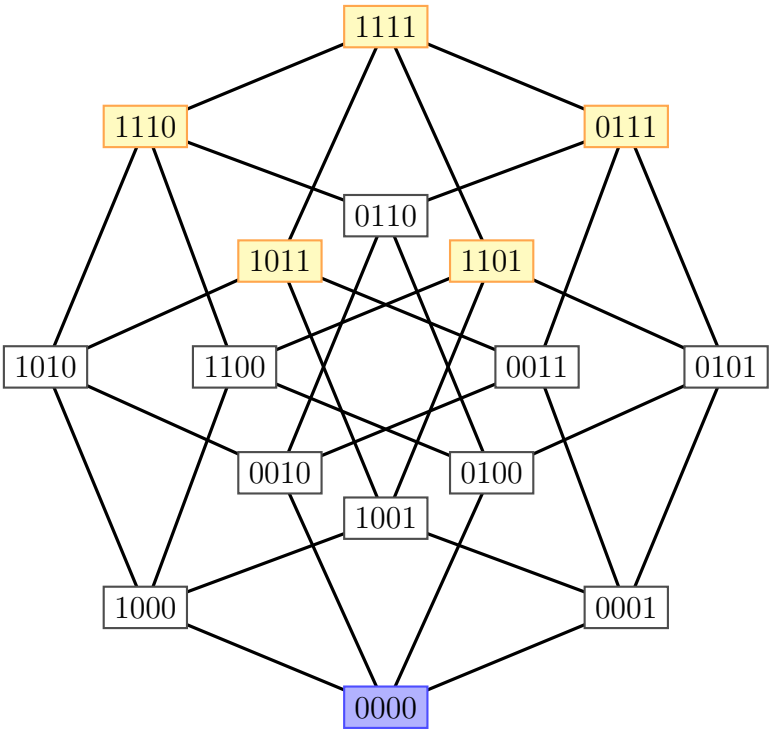


Figura 3.3: Bolas quasi-métricas no cone S_1 com raio de empacotamento do código $\mathcal{C}$.

A Figura 3.4 ilustra as bolas quasi-métricas com o correspondente raio de empacotamento da palavra código, $\mathcal{R}^z_{\mathcal{C}}(c)$. Nesse caso, o conjunto de mensagens corrigíveis é $V = \mathbb{F}_2^4$.

Note que, se enviamos $c = 0000$, nenhuma mensagem recebida é corrigível, mas se enviamos $\bar{c} = 1111$, 14 mensagens possíveis de serem recebidas são corrigíveis.

Observação 7. *Conforme vimos no Exemplo 16, o raio de empacotamento de uma palavra código não é constante, mesmo em se tratando de um código linear. Esta propriedade, à qual não estamos acostumados no contexto de canais simétricos, revelam uma possibilidade que pode ser interessante. Em diversas circunstâncias, trabalha-se com informações de natureza distinta, que demandam proteção desigual de erros. Muitas vezes, a proteção desigual é feita considerando-se proteção desigual de bits, mas por outras vezes, como, por exemplo, na estratégia adotada por Borade, Nakiboglu e Zheng [19], trata-se de proteger desigualmente mensagens diferentes. A variação no raio de empacotamento de palavras códigos sugere uma estratégia natural, com óbvio reflexo no desempenho do código (se este desempenho for medido de algum modo que reflita a importância diferenciada das mensagens): atribuir as informações que demandam mais proteção às palavras códigos que possuem maior raio de empacotamento. Neste sentido, a busca por códigos passa a incluir uma possibilidade adicional a ser considerada, qual seja, não apenas a determinação do $[n, k]_2$-código linear $\mathcal{C}$ mas também o modo como associamos as informações de $\mathbb{F}_2^k$ às palavras códigos.*

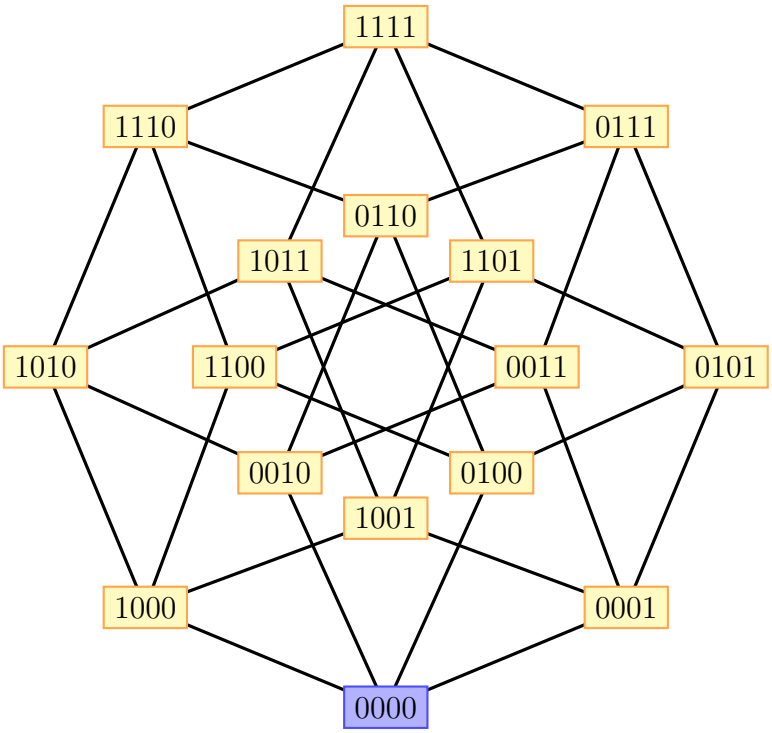


Figura 3.4: Bolas quasi-métricas no cone S_1, descritas pela sequência de raios de empacotamento do código $\mathcal{C}$.

Teorema 6. *Considere um código $\mathcal{C} \subseteq \mathbb{F}_2^n$ e $S \in \mathcal{D}_n$. Para um canal $z = (x, y) \in S$ e $c \in \mathcal{C}$, o raio de empacotamento de c é dado por*

$$\mathcal{R}_{\mathcal{C}}^{z}(c) = \min_{c \neq \bar{c} \in \mathcal{C}} \Big\{ \max \Big\{ \delta_z(c) \;\Big|\; \delta_z(c, \bar{c}) \neq \delta_z(c, v) + \delta_z(v, \bar{c}),\ \textit{para todo } v \in B\big(c, \delta_z(c)\big) \Big\} \Big\}.$$

Demonstração. Seja $\mathcal{C} \subseteq \mathbb{F}_2^n$ um código linear e $S \in \mathcal{D}_n$. Considere $c, \bar{c} \in \mathcal{C}$ e $\delta_z(c) \in Spec(c)$, onde $z = (x, y) \in S$. Suponha que exista $v \in V$ tal que

$$v \in B(c; \delta_z(c)) \cap B(\bar{c}; \delta_z(c)).$$

Então, $\delta_z(c, v) \leq \delta_z(c)$ e $\delta_z(\bar{c}, v) \leq \delta_z(c)$ e, se considerarmos

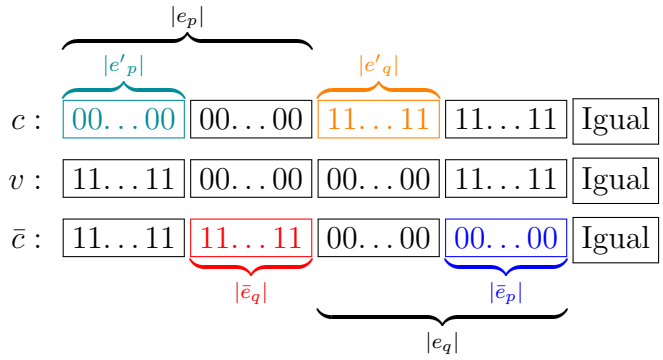
$$\delta_z^n(c, v) = |e'_p|x + |e'_q|y \quad \text{e} \quad \delta_z^n(\bar{c}, v) = |\bar{e}_p|x + |\bar{e}_q|y,$$

obtemos

$$\delta_z^n(c, v) + \delta_z^n(v, \bar{c}) = (|e'_p| + |\bar{e}_q|)x + (|e'_q| + |\bar{e}_p|)y. \tag{3.7}$$

Suponha que $\delta_z^n(c, \bar{c}) = |e_p|x + |e_q|y$, com $d_H(c, \bar{c}) = |e_p| + |e_q|$.

Considere, esquematicamente, e sem perda de generalidade, as distâncias $\delta_z(c, v)$ e $\delta_z(\bar{c}, v)$, representadas da seguinte forma:



Note que v é um vetor com exatamente $(|e'_p| + |e'_q|)$ coordenadas diferentes de c e, ao mesmo tempo, é um vetor com exatamente $(|\bar{e}_p| + |\bar{e}_q|)$ coordenadas diferentes de $\bar{c}$. Mas, c e $\bar{c}$ têm exatamente $(|e_p| + |e_q|)$ coordenadas diferentes entre si e, uma vez que $v \in B\big(c; \delta_z(c)\big) \cap B\big(\bar{c}; \delta_z(c)\big)$, é necessário que tenhamos $|e_p| = |e'_p| + |\bar{e}_q|$ e $|e_q| = |e'_q| + |\bar{e}_p|$, ou seja, é necessário que $d_H(c, \bar{c}) = d_H(c, v) + d_H(v, \bar{c})$.

De fato, se as trocas de coordenadas ocorrerem somente no conjunto Igual, não haverá interseção, pois cada palavra código vai gerar um vetor diferente. Analogamente, se a troca das coordenadas ocorrer parte no conjunto Igual e parte no conjunto de coordenadas diferentes, novamente não haverá interseção pois serão gerados dois vetores distintos, cada um referente a uma palavra código. Portanto, haverá interseção somente quando as trocas de coordenadas ocorrerem no conjunto das $|e_p| + |e_q|$ coordenadas que diferem em c e $\bar{c}$. Portanto, $\delta_z^n(c, v) + \delta_z^n(v, \bar{c}) = \delta_z^n(c, \bar{c})$.

Por outro lado, se $\delta_z^n(c, v) + \delta_z^n(v, \bar{c}) = \delta_{p,q}^n(c, \bar{c})$, considere $\delta_z(c) = \delta_z(c, v)$ e $\delta_z(\bar{c}) = \delta_z(\bar{c}, v)$. Então, temos que $v \in B(c; \delta_z(c))$ e $v \in B(\bar{c}; \delta_z(\bar{c}))$. Resta apenas mostrar que $\delta_z(\bar{c}) \leq \delta_z(c)$. Suponha que $\delta_z(c) < \delta_z(\bar{c})$. Então, $B(\bar{c}; \delta_z(c)) \subseteq B(\bar{c}; \delta_z(\bar{c}))$ e, como assumimos que $\delta_z(c) = \delta_z(c, v)$, então $v \in \mathbb{S}^z(\bar{c}; \delta_z(\bar{c}))$ e $v \notin B(\bar{c}; \delta_z(c))$. Logo, $v \notin B\big(c; \delta_z(c)\big) \cap B\big(\bar{c}; \delta_z(c)\big)$, ou seja, $\delta_z^n(c, \bar{c}) < \delta_z^n(c, v) + \delta_z^n(v, \bar{c})$, e este fato contradiz a hipótese. Portanto, concluímos que $\delta_z(\bar{c}) \leq \delta_z(c)$.

Segue que se $\delta_z^n(c, \bar{c}) \neq \delta_z^n(c, v) + \delta_z^n(v, \bar{c})$, para todo $v \in B(c, \delta_z(c))$, obtemos $B\big(c; \delta_z(c)\big) \cap B\big(\bar{c}; \delta_z(c)\big) = \emptyset$. Assim sendo, o máximo raio $\delta_z(c)$ que satisfaz esta condição será o raio de empacotamento de c relativo à $\bar{c}$. Considerando o mínimo destes raios, sobre todo $c \neq \bar{c} \in \mathcal{C}$, obtemos então o raio de empacotamento de c, ou seja,

$$\mathcal{R}_{\mathcal{C}}^z(c) = \min_{c \neq \bar{c} \in \mathcal{C}} \Big\{ \max \Big\{ \delta_z(c) \;\Big|\; \delta_z(c, \bar{c}) \neq \delta_z(c, v) + \delta_z(v, \bar{c}), \text{ para todo } v \in B\big(c, \delta_z(c)\big) \Big\} \Big\}.$$

□

Observação 8. *É importante notar que $\mathcal{R}_z^{\mathcal{C}}(c)$ não é constante em $c \in \mathcal{C}$, mesmo no caso de termos $\mathcal{C}$ linear. Veremos isto nos exemplos a seguir.*

Exemplo 17. *Considere o código do Exemplo 15:* $\mathcal{C} = \{0000, 1111\}$ *e os cones* $S_i \in \mathcal{D}_4$*, conforme ilustra a Figura 3.5.*

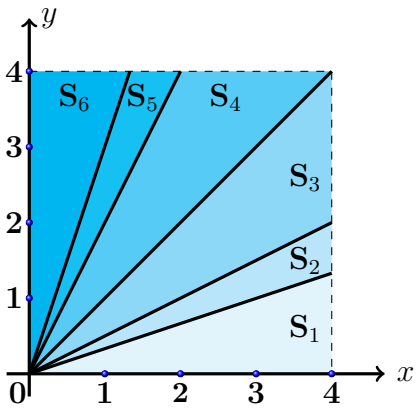


Figura 3.5: Partição do espaço $\mathfrak{Q}$, para $n = 4$.

A Tabela 3.9 mostra os raios de empacotamento em um canal $z = (x, y) \in S$*, para cada* $S \in \mathcal{D}_4$ *e cada* $c \in \mathcal{C}$*.*

	$R^z_{\mathcal{C}}(0000)$	$R^z_{\mathcal{C}}(1111)$
S_1	y	$3y$
S_2	x	$2y$
S_3	x	$2y$
S_4	$2x$	y
S_5	$2x$	y
S_6	$3x$	x

Tabela 3.9: Sequência dos raios de empacotamento $\mathcal{R}^z_{\mathcal{C}}(c)$, para todo $c \in \mathcal{C}$.

Observe que:

1. *Palavras código distintas podem ter raio de empacotamento distintos. Logo, o raio de empacotamento depende da palavra código.*

2. *O valor do raio de empacotamento depende da palavra e do canal.*

3. *O raio de empacotamento é determinado pela palavra código, no cone em questão, ou seja,* $\mathcal{R}^z_{\mathcal{C}}(c) \cong \mathcal{R}^{\bar{z}}_{\mathcal{C}}(c)$*, para* $z, \bar{z}$ *pertencentes ao mesmo cone. Já quando o cone é trocado, esta mesma palavra código pode ter um raio de empacotamento distinto. Observe, por exemplo, o raio de empacotamento de* $c = 0000$ *nos cones* S_3 *e* S_4*.*

4. *O raio de empacotamento máximo não está relacionado com a palavra código de maior peso de Hamming. Por exemplo, para* $z = (x, y) \in S_2$*, o maior raio de empacotamento é* $\mathcal{R}^z_{\mathcal{C}}(0000) = x$ *e* $\omega_H(0000) = 0$*. No entanto,* $\omega_H(1111) = 4$*, mas* $\mathcal{R}^z_{\mathcal{C}}(1111) = 2y < x$*.*

5. *É possível verificar que, para o caso dos canais assimétricos, o código* $\mathcal{C} = \{0000, 1111\}$ *é perfeito, no sentido que*

$$B\big(0000; \mathcal{R}^z_{\mathcal{C}}(0000)\big) \cup B\big(1111; \mathcal{R}^z_{\mathcal{C}}(1111)\big) = \mathbb{F}_2^4.$$

Observe que este é um fato notável visto que, no caso de termos um canal simétrico $(x = y)$*, obtemos* $\mathcal{R}^z_{\mathcal{C}}(0000) = \mathcal{R}^z_{\mathcal{C}}(1111) = x$ *e*

$$B(0000; x) = \{0000, 1000, 0100, 0010, 0001\} = \{v \in \mathbb{F}_2^n \mid \omega_H(v) \leq 1\}$$
$$B(1111; x) = \{1111, 0111, 1011, 1101, 1110\} = \{v \in \mathbb{F}_2^n \mid \omega_H(v) \geq 3\}.$$

Note ainda que, à medida que consideramos cones mais próximos do caso simétrico $(x = y)$*, as bolas quasi-métricas obtidas nestes cones tendem a ficar mais parecidas com as bolas métricas. Por exemplo, considere as primeiras bolas quasi-métricas obtidas para os canais* $z = (x, y) \in S_i$*, coma* $i = 1, 2, 3$*, conforme ilustra a Tabela 3.10.*

Cone S_1			
0	y	$2y$	$3y$
0000	-	-	-
1111	1110, 1101 1011, 0111	1100, 1010, 1001 0110, 0101, 0011	1000, 0100 0010, 0001
Cone S_2			
0	y	$2y$	x
0000	-	-	1000, 0100 0010, 0001
1111	1110, 1101 1011, 0111	1100, 1010, 1001 0110, 0101, 0011	-
Cone S_3			
0	y	x	$2y$
0000	-	1000, 0100 0010, 0001	-
1111	1110, 1101 1011, 0111	-	1100, 1010, 1001 0110, 0101, 0011

Tabela 3.10: Bolas quasi-métricas para os cones S_1, S_2 e S_3.

Repare que, no cone S_1 *as primeiras bolas quasi-métricas não coincidem com as primeiras bolas métricas, já que estamos tratando de canais bem mais assimétricos (quase canais Z) nesta região. Já o cone* S_3 *é o mais próximo do caso simétrico e, portanto, as primeiras bolas quasi-métricas coincidem com as primeiras bolas de Hamming. De fato,* $B(0000; x)$ *e* $B(1111; y)$ *equivalem às bolas métricas de raio igual a* 1 *e a bola quasi-métrica* $B(1111; 2y)$ *equivale à bola métrica* $B(0000; 2) = B(1111; 2)$*.*

O próximo exemplo varia um pouco mais o peso das palavras código e nosso

objetivo novamente é calcular a sequência de raios de empacotamento do código $\mathcal{C}$.

Exemplo 18. *Considere o código linear* $\mathcal{C} = \{0000, 0101, 1011, 1110\}$. *A Tabela 3.11 mostra a sequência de raios de empacotamento do código, em um canal* $z = (x, y) \in S$, *para cada* $S \in \mathcal{D}_4$.

	$R^z_{\mathcal{C}}(0000)$	$R^z_{\mathcal{C}}(0101)$	$R^z_{\mathcal{C}}(1011)$	$R^z_{\mathcal{C}}(1110)$	$\mathcal{E}_{\mathcal{C}}$
S_1	0	y	0	0	6
S_2	0	y	0	0	6
S_3	0	y	0	0	6
S_4	x	x	0	0	10
S_5	x	x	0	0	10
S_6	x	x	0	0	10

Tabela 3.11: Sequência dos raios de empacotamento $\mathcal{R}^z_{\mathcal{C}}(c)$, para todo $c \in \mathcal{C}$.

No que se refere à correção de erros, a última coluna da Tabela 3.11 ilustra a quantidade $\mathcal{E}_{\mathcal{C}} = \big|\bigcup_{c\in\mathcal{C}} B\big(c; \mathcal{R}^z_{\mathcal{C}}(c)\big)\big|$. *Note como esta quantidade varia à medida que trocamos o cone (este fato já é esperado pois os raios de empacotamento podem variar com a troca de cone). Por exemplo, nos* 3 *primeiros cones, se enviarmos as palavras código* 0000, 1011 *ou* 1110, *não conseguimos corrigir qualquer mensagem possível de ser recebida, mas quando enviamos* 0101 *temos condições de corrigir apenas duas mensagens possíveis de serem recebidas.*

Vale observar que, em qualquer dos cones, $\mathcal{E}_{\mathcal{C}}$ *sempre é maior do que a capacidade de correção do código no caso simétrico. De fato, se* $x = y$, *o raio de empacotamento do código é* $\mathcal{R}(\mathcal{C}) = 0$ *e, qualquer palavra código* c *que seja enviada não nos permite corrigir qualquer das mensagens possíveis de serem recebidas, ou seja,* $\big|\bigcup_{c\in\mathcal{C}} B\big(c; 0\big)\big| = 4$.

Como já é conhecido, no caso simétrico o raio de empacotamento do código é igual ao raio de empacotamento de todas as palavras código. Entretanto, quando consideramos canais assimétricos, sabemos que palavras distintas podem ter raios de empacotamento distintos. Mais ainda, o próximo e último exemplo nos mostra que palavras código com mesmo peso de Hamming, podem ter raios de empacotamento distintos.

Exemplo 19. *Considere o código linear* $\mathcal{C} = \{00000, 01100, 10010, 00101, 01001, 11011, 11110, 10111\}$ *e* $S \in \mathcal{D}_5$. *A Tabela 3.12 ilustra a sequência de raios de empacotamento do código, para um canal* $z = (x, y) \in S$, *para cada* S.

Observe que, para $c = 01100$ *e* $\bar{c} = 10010$, *temos* $\omega_H(c) = \omega_H(\bar{c}) = 2$, *mas* $R^z_{\mathcal{C}}(c) \neq R^z_{\mathcal{C}}(\bar{c})$, *para todo* $z \in S$ *e todo cone* S. *Portanto, palavras código com mesmo peso de Hamming não necessariamente têm o mesmo raio de empacotamento.*

$c \in \mathcal{C}$	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}
00000	0	0	0	0	0	x	x	x	x	x
01100	0	0	0	0	0	0	0	0	0	0
10010	y	y	y	y	y	x	x	x	x	x
00101	0	0	0	0	0	0	0	0	0	0
01001	0	0	0	0	0	0	0	0	0	0
11011	0	0	0	0	0	0	0	0	0	0
11110	0	0	0	0	0	0	0	0	0	0
10111	0	0	0	0	0	0	0	0	0	0

Tabela 3.12: Sequências de raios de empacotamento para o código $\mathcal{C}$, em cada cone

3.4 Raio de cobertura

Considere um código $\mathcal{C} \subseteq \mathbb{F}_2^n$ e $S \in \mathcal{D}_n$. Assim como ocorre com o raio de empacotamento (vide Seção 3.3), dado um canal $z = (x, y) \in S$, podemos obter uma sequência de raios de cobertura $\big(\mathfrak{R}^z_{\mathcal{C}}(c)\big)_{c\in\mathcal{C}}$ do código e que depende da palavra código c, para todo $c \in \mathcal{C}$. Essa sequência é um refinamento do raio de cobertura do código $\mathcal{C}$.

Definição 19. *Seja $\mathcal{C} \subseteq \mathbb{F}_2^n$ um código e $S \in \mathcal{D}_n$. Definimos o raio de cobertura do código $\mathcal{C}$, em um canal $z = (x, y) \in S$, como sendo o menor raio $\mathfrak{R}^z(\mathcal{C})$ tal que $\bigcup_{c\in\mathcal{C}} B(c; \mathfrak{R}^z(\mathcal{C})) = \mathbb{F}_2^n$.*

Considerando $\alpha^z(\mathcal{C}) = \sum_{c\in\mathcal{C}} |B(c; \mathfrak{R}^z(\mathcal{C}))|$, existem $\gamma^z(\mathcal{C}) = \alpha^z(\mathcal{C}) - 2^n$ vetores em excesso na cobertura do código $\mathcal{C}$, obtida com o raio $\mathfrak{R}^z(\mathcal{C})$, com $|\mathbb{F}_2^n| = 2^n$. É natural pensar que, se minimizarmos o valor de $\alpha^z(\mathcal{C})$, teremos uma quantidade menor de vetores repetidos nesta cobertura de V.

Definição 20. *Seja $\mathcal{C} \subseteq \mathbb{F}_2^n$ um código e $S \in \mathcal{D}_n$. Para $z = (x, y) \in S$, uma sequência $\mathfrak{R}^z_{\mathcal{C}} = \big(\mathfrak{R}^z_{\mathcal{C}}(c)\big)_{c\in\mathcal{C}}$ é uma **sequência de cobertura** do código $\mathcal{C}$ se*

$$\bigcup_{c\in\mathcal{C}} B(c; \mathfrak{R}^z_{\mathcal{C}}(c)) = \mathbb{F}_2^n \;\; e \;\; \mathcal{R}^z_{\mathcal{C}}(c) \leq \mathfrak{R}^z_{\mathcal{C}}(c) \leq \mathfrak{R}^z(\mathcal{C}),$$

onde $\mathcal{R}^z_{\mathcal{C}}(c)$ denota o raio de empacotamento da palavra código c.

*Uma **sequência de raios de cobertura ótima** é uma sequência de cobertura do código $\mathcal{C}$ cujo valor de $\alpha_{\mathfrak{R}}(\mathcal{C}) = \sum_{c\in\mathcal{C}} \big|B(c; \mathfrak{R}^z_{\mathcal{C}}(c))\big|$ é mínimo.*

*Se a sequência $\mathfrak{R}^z_{\mathcal{C}}$ coincide com a sequência de raios de empacotamento, $\mathcal{R}^z_{\mathcal{C}}$, dizemos que $\mathcal{C}$ é um **código perfeito** .*

A Definição 20 é um refinamento do caso clássico, pois $\mathfrak{R}^z(\mathcal{C}) = \max_{c\in\mathcal{C}}\big\{\mathfrak{R}^z_{\mathcal{C}}(c)\big\}$ e $\alpha_{\mathfrak{R}}(\mathcal{C}) \leq \alpha^z(\mathcal{C})$.

De modo análogo ao que fizemos para a sequência de raios de empacotamento diremos que, para $c \in \mathcal{C}$, os raios de cobertura $\mathfrak{R}^z_{\mathcal{C}}(c)$ e $\mathfrak{R}^{\bar{z}}_{\mathcal{C}}(c)$ são congruentes se, e somente

se, estes raios são descritos pelos mesmos parâmetros (α, β), ou seja,

$$\mathfrak{R}^z_{\mathcal{C}}(c) \cong \mathfrak{R}^{\bar{z}}_{\mathcal{C}}(c) \Longleftrightarrow \mathfrak{R}^z_{\mathcal{C}}(c) = \alpha x + \beta y \text{ e } \mathfrak{R}^{\bar{z}}_{\mathcal{C}}(c) = \alpha \bar{x} + \beta \bar{y}.$$

Proposição 14. *Sejam $S, \bar{S} \in \mathcal{D}_n$, com $S \neq \bar{S}$.*

(a) *Considere um código $\mathcal{C} \subseteq \mathbb{F}_2^n$ e $z, \bar{z} \in S$. Seja $\mathfrak{R}^z_{\mathcal{C}}$ uma sequência de raios de cobertura ótima. Então, para qualquer $c \in \mathcal{C}$, temos $\mathfrak{R}^z_{\mathcal{C}}(c) \cong \mathfrak{R}^{\bar{z}}_{\mathcal{C}}(c)$.*

(b) *Seja $\mathfrak{R}^z_{\mathcal{C}}$ uma sequência de raios de cobertura ótima. Então, para $z \in S$ e $\bar{z} \in \bar{S}$, existe código $\mathcal{C}$ tal que $\mathfrak{R}^z_{\mathcal{C}}(c) \ncong \mathfrak{R}^{\bar{z}}_{\mathcal{C}}(c)$, para algum $c \in \mathcal{C}$.*

Demonstração. Sejam $S, \bar{S} \in \mathcal{D}_n$, com $S \neq \bar{S}$.

(a) Considere um código $\mathcal{C} \subseteq \mathbb{F}_2^n$ e os canais $z, \bar{z} \in S$. Seja $\mathfrak{R}^z_{\mathcal{C}}$ uma sequência de raios de cobertura ótima obtida para $z \in S$ e $\mathfrak{R}^{\bar{z}}_{\mathcal{C}}(c)$ a mesma sequência de raios, determinada por $\bar{z} \in S$.

Uma vez que S é classe de equivalência, temos que $z \sim \bar{z}$ e, consequentemente, $\mathfrak{R}^z_{\mathcal{C}}(c) \cong \mathfrak{R}^{\bar{z}}_{\mathcal{C}}(c)$.

(b) Seja $r \in \mathcal{L}_n(S, \bar{S})$ uma reta que separa os cones S e $\bar{S}$ e definida por $\beta y = \alpha x$, com $\alpha + \beta = n$. Considere o código linear $\mathcal{C} = \{0^n, 1^n\}$. Então, se S é o cone que está abaixo da reta r, dado um canal $z = (x, y) \in S$, temos $\beta y < \alpha x$, de onde obtemos que $\mathfrak{R}^{\bar{z}}_{\mathcal{C}}(0^n) = (\alpha - 1)x$ e $\mathfrak{R}^{\bar{z}}_{\mathcal{C}}(1^n) = \beta y$. Por outro lado, o cone $\bar{S}$ está acima da reta r e, portanto, dado um canal $\bar{z} = (\bar{x}, \bar{y}) \in \bar{S}$, temos $\alpha \bar{x} < \beta \bar{y}$, de onde obtemos que $\mathfrak{R}^{\bar{z}}_{\mathcal{C}}(0^n) = \alpha x$ e $\mathfrak{R}^{\bar{z}}_{\mathcal{C}}(1^n) = (\beta - 1)y$.

Logo, $\mathfrak{R}^z_{\mathcal{C}}(c) \ncong \mathfrak{R}^{\bar{z}}_{\mathcal{C}}(c)$, para $c \in \mathcal{C}$, o que conclui a demonstração. □

Observação 9. *Note que podemos ter mais de uma sequência de raios de cobertura em um mesmo cone S. Neste caso, o próprio código $\mathcal{C}$ já é o exemplo de que $\mathfrak{R}^{\mathcal{C}}_z(c) \ncong \mathfrak{R}^{\mathcal{C}}_{\bar{z}}(c)$, para algum $c \in \mathcal{C}$.*

Assim sendo, se $\mathfrak{R}^z_{\mathcal{C}}$ é uma sequência de raios de cobertura ótima, obtida para $z \in S$, então, o raio de cobertura de c **muda de valor com a mudança do canal**, mas é descrito pelos mesmos parâmetros α e β, nos dois canais, já que $z \sim \bar{z}$. Os próximos exemplos ilustram as sequências de raios de cobertura ótimas, $\mathfrak{R}^z_{\mathcal{C}}$, para um dado código $\mathcal{C}$.

Exemplo 20. *Considere o código linear do Exemplo 17: $\mathcal{C} = \{0000, 1111\}$. A Tabela 3.13 mostra as sequências de raios de cobertura ótimas de $\mathcal{C}$, para $(x, y) \in S$ e cada $S \in \mathcal{D}_4$.*

Conforme já discutido no Exemplo 17, no caso assimétrico, o código $\mathcal{C}$ é perfeito em qualquer dos cones e, portanto, cobre todo o espaço $\mathbb{F}_2^4$ com $\alpha_{\mathfrak{R}}(\mathcal{C}) = 16$. Neste exemplo, cada cone possui uma única sequência de raios de cobertura ótima.

S_1	S_2	S_3	S_4	S_5	S_6
$(y, 3y)$	$(x, 2y)$	$(x, 2y)$	$(2x, y)$	$(2x, y)$	$(3x, x)$

Tabela 3.13: Sequência de raios de cobertura ótima, para cada um canal $(x, y) \in S_i$.

Exemplo 21. *Considere o código linear do Exemplo 18:* $\mathcal{C} = \{0000, 0101, 1011, 1110\}$. *A Tabela 3.14 mostra as sequências de raios de cobertura ótimas de* $\mathcal{C}$, *para* $z = (x, y) \in S$ *e cada* $S \in \mathcal{D}_4$.

	$\mathfrak{R}^z_{\mathcal{C}}(0000)$	$\mathfrak{R}^z_{\mathcal{C}}(0101)$	$\mathfrak{R}^z_{\mathcal{C}}(1011)$	$\mathfrak{R}^z_{\mathcal{C}}(1110)$	$\alpha_{\mathfrak{R}}(\mathcal{C})$
$S_1 \cup S_2$	0	x	x	y	20
	0	x	y	x	
S_3	x	x	x	y	19
	x	x	y	x	
S_4	x	x	y	y	18
$S_5 \cup S_6$	$2x$	x	x	x	17

Tabela 3.14: Sequência dos raios de cobertura $\mathfrak{R}^z_{\mathcal{C}}$ para $\mathcal{C}$, em cada cone S_i.

Observe que nos cones S_4, S_5 *e* S_6 *as sequências de raios de cbertura ótimas são únicas. Já para* S_1, S_2 *e* S_3 *obtemos duas sequências de raios de cobertura ótimas, para cada cone. Mas, embora estas sequências sejam diferentes, por definição, ambas determinam o mesmo valor de* $\alpha_{\mathfrak{R}}(\mathcal{C})$ *para o cone.*

A Tabela 3.15 compara os raios de cobertura, $\mathfrak{R}^z(\mathcal{C})$, $\mathfrak{R}^z_{\mathcal{C}}$, *obtidos no caso assimétrico, com o raio de cobertura do caso clássico,* $\mathfrak{R}(\mathcal{C})$. *Note que a sequência* $\mathfrak{R}^z_{\mathcal{C}}$ *sempre cobre o espaço* $\mathbb{F}_2^4$ *com um valor menor de* $\alpha_{\mathfrak{R}}(\mathcal{C})$ *e, portanto, é um refinamento do caso clássico.*

$\mathfrak{R}^z(\mathcal{C})$	$\mathfrak{R}^z_{\mathcal{C}}$	$\mathfrak{R}(\mathcal{C})$
$\alpha(\mathcal{C}) = 29$	$\alpha_{\mathfrak{R}}(\mathcal{C}) = 20$ $\alpha_{\mathfrak{R}}(\mathcal{C}) = 19$ $\alpha_{\mathfrak{R}}(\mathcal{C}) = 18$ $\alpha_{\mathfrak{R}}(\mathcal{C}) = 17$	$\alpha = 20$

Tabela 3.15: Comparativo dos raios $\mathfrak{R}^z(\mathcal{C})$, $\mathfrak{R}^z_{\mathcal{C}}$ com o raio, referente ao caso clássico $\mathfrak{R}(\mathcal{C})$.

3.5 Polinômios enumeradores de distâncias

De acordo com [15], é possível definir polinômios enumeradores que caracterizam a distribuição de pesos e distâncias de um código $\mathcal{C}$. Motivados por esse fato, definiremos nesta seção os polinômios enumeradores de quasi-distâncias, raios de empacotamento e raios de cobertura, para o caso assimétrico, e mostraremos as principais diferenças entre estes polinômios e os do caso clássico.

Considere um código $\mathcal{C} \subseteq \mathbb{F}_2^n$, $S \in \mathcal{D}_n$ e um canal $z = (x, y) \in S$. Um polinômio enumerador de distâncias, para o código $\mathcal{C}$, poderia ser definido como

$$\Lambda_{\mathcal{C}}^{z}(u, r) = \sum_{d=0}^{n} \Big[\sum_{\delta_z \in \mathcal{Q}_{\mathcal{C}}^{z}} \lambda_{\delta_z}^{d} u^{\delta_z} \Big] r^d,$$

em que $\lambda_{\delta_z}^{d} = \Big| \Big\{ (c, \bar{c}) \in \mathcal{C}^2 \;\Big|\; \delta_z = \delta_z^n(c, \bar{c}) \text{ e } d = d_H(c, \bar{c}) \Big\} \Big|$ e $\mathcal{Q}_{\mathcal{C}}^{z}$ denota o conjunto de todas as distâncias entre pares de palavras código $(c, \bar{c}) \in \mathcal{C}^2$.

No entanto, da maneira como foi definido, o polinômio $\Lambda_{\mathcal{C}}^{z}(u, r)$ depende do código $\mathcal{C}$ e do canal $z \in S$. Assim sendo, para $z, \bar{z} \in S$, em geral temos $\Lambda_{\mathcal{C}}^{z}(u, r) \neq \Lambda_{\mathcal{C}}^{\bar{z}}(u, r)$ e, uma vez que estamos trabalhando sempre com invariantes quasi-métricos que dependem do cone, tal polinômio não é interessante, já que não preserva o conceito de equivalência de canais em sua definição. Por esse motivo, redefinimos o polinômio enumerador de distâncias, em termos dos parâmetros α e β que descrevem a distância $\alpha x + \beta y$ entre um par de palavras código $(c, \bar{c}) \in \mathcal{C}^2$. Com isso, podemos obter uma estrutura bem definida para os polinômios enumeradores de canais equivalentes.

De modo análogo e pelo mesmo motivo, definiremos os polinômios enumeradores de raios de empacotamento e cobertura também em função dos parâmetros α e β, conforme veremos a seguir.

Definição 21. *Seja $\mathcal{C} \subseteq \mathbb{F}_2^n$ um código, $S \in \mathcal{D}_n$ e um canal $z = (x, y) \in S$.*

1. *O **polinômio enumerador de parâmetros de distâncias (P.E.D.)** de $\mathcal{C}$ é dado por*

$$\bar{\Lambda}_{\mathcal{C}}(s, t, r) = \sum_{d=0}^{n} \Big[\sum_{(\alpha,\beta) \in \bar{\mathcal{Q}}_{\mathcal{C}}} \lambda_{\alpha\beta}^{d} s^{\alpha} t^{\beta} \Big] r^d,$$

   em que $\lambda_{\alpha\beta}^{d} = \Big| \Big\{ (c, \bar{c}) \in \mathcal{C}^2 \;\Big|\; \delta_z^n(c, \bar{c}) = \alpha x + \beta y \text{ e } d = d_H(c, \bar{c}) = \alpha + \beta \Big\} \Big|$ e $\bar{\mathcal{Q}}_{\mathcal{C}}$ denota o conjunto de todos os pares (α, β) cuja combinação $\alpha x + \beta y$ define uma distância pertencente a $\mathcal{Q}_{\mathcal{C}}^{z}$.

2. *O **polinômio enumerador de parâmetros de raios de empacotamento (P.E.R.E.)** de $\mathcal{C}$ é dado por*

$$\bar{\Gamma}_{\mathcal{C}}^{z}(s, t, r) = \sum_{\omega=0}^{n} \Big[\sum_{(\alpha,\beta) \in \bar{\mathcal{R}}_{\mathcal{C}}} \gamma_{\alpha\beta}^{\omega} s^{\alpha} t^{\beta} \Big] r^{\omega},$$

   em que $\gamma_{\alpha\beta}^{\omega} = \Big| \Big\{ c \in \mathcal{C} \;\Big|\; \mathcal{R}_{\mathcal{C}}^{z}(c) = \alpha x + \beta y \text{ e } \omega_H(c) = \omega \Big\} \Big|$ e $\bar{\mathcal{R}}_{\mathcal{C}}$ denota o conjunto de todos pares (α, β) cuja combinação $\alpha x + \beta y$ define um raio de empacotamento pertencente a $\mathcal{R}_{\mathcal{C}}^{z}$.

3. *O* ***polinômio enumerador de parâmetros de raios de cobertura (P.E.R.C.)*** *de* $\mathcal{C}$ *é dado por*

$$\bar{\Psi}_{\mathcal{C}}^{z}(s,t,r) = \sum_{\omega=0}^{n}\Big[\sum_{(\alpha,\beta)\in\bar{\mathfrak{R}}_{\mathcal{C}}} \psi_{\alpha\beta}^{\omega} s^{\alpha}t^{\beta}\Big] r^{\omega},$$

em que $\psi_{\alpha\beta}^{\omega} = \Big|\big\{c \in \mathcal{C} \mid \mathfrak{R}_{\mathcal{C}}^{z}(c) = \alpha x + \beta y \text{ e } \omega_H(c) = \omega\big\}\Big|$ *e* $\bar{\mathfrak{R}}_{\mathcal{C}}$ *denota o conjunto de todos pares* (α,β) *cuja combinação* $\alpha x + \beta y$ *define um raio de cobertura pertencente a* $\mathfrak{R}_{\mathcal{C}}^{z}$.

A Definição 21 mostra claramente de quais variáveis cada um dos polinômios depende. No que se refere aos polinômios enumeradores de distâncias, vemos que o P.E.D. depende do código $\mathcal{C}$. Já os P.E.R.E. e P.E.R.C. dependem do cone S, do código $\mathcal{C}$ e da palavra código $c \in \mathcal{C}$.

Deve ser observado que a variável r, no P.E.D., pode parecer desnecessária visto que seu expoente denota a soma dos parâmetros α e β que compõe a distância $\alpha x + \beta y$. No entanto, o acréscimo desta variável é justamente para deixar clara que a distância d pode ser decomposta de formas diferentes, como soma dos parâmetros α, β.

Proposição 15. *Considere um código* $\mathcal{C} \subseteq \mathbb{F}_2^n$ *e* $S \in \mathcal{D}_n$. *Para* $z = (x,y) \in S$, *as seguintes identidades são válidas:*

1. $\lambda_{\alpha\beta}^{d} = \lambda_{\beta\alpha}^{d}$ *e* $\lambda_{00}^{d} = |\mathcal{C}|$;
2. $\bar{\Lambda}_{\mathcal{C}}(1,1,1) = |\mathcal{C}|^2$;
3. $\bar{\Gamma}_{\mathcal{C}}(1,1,1) = \bar{\Psi}_{\mathcal{C}}(1,1,1) = |\mathcal{C}|$;

Demonstração. A demonstração segue imediatamente da definição dos polinômios enumeradores. □

Proposição 16. *Sejam* $S, \bar{S} \in \mathcal{D}_n$. *Então,*

(a) *Para qualquer código* $\mathcal{C} \subseteq \mathbb{F}_2^n$ *e quaisquer* $z, \bar{z} \in \mathfrak{Q}_n$, *temos* $\bar{\Lambda}_{\mathcal{C}}^{z}(s,t,r) = \bar{\Lambda}_{\mathcal{C}}^{\bar{z}}(s,t,r)$;

(b) *Para qualquer código* $\mathcal{C} \subseteq \mathbb{F}_2^n$ *e* $z, \bar{z} \in S$, *temos* $\bar{\Gamma}_{\mathcal{C}}^{z}(s,t,r) = \bar{\Gamma}_{\mathcal{C}}^{\bar{z}}(s,t,r)$ *e* $\bar{\Psi}_{\mathcal{C}}^{z}(s,t,r) = \bar{\Psi}_{\mathcal{C}}^{\bar{z}}(s,t,r)$;

(c) *Sejam* $z \in S$ *e* $\bar{z} \in \bar{S}$, *com* $S \neq \bar{S}$. *Então, existe um código* $\mathcal{C} \subseteq \mathbb{F}_2^n$ *tal que* $\bar{\Gamma}_{\mathcal{C}}^{z}(s,t,r) \neq \bar{\Gamma}_{\mathcal{C}}^{\bar{z}}(s,t,r)$ *e* $\bar{\Psi}_{\mathcal{C}}^{z}(s,t,r) \neq \bar{\Psi}_{\mathcal{C}}^{\bar{z}}(s,t,r)$.

Demonstração. Sejam $S, \bar{S} \in \mathcal{D}_n$, com $S \neq \bar{S}$.

(a) Sejam $z, \bar{z} \in \mathfrak{Q}_n$ e um código $\mathcal{C} \subseteq \mathbb{F}_2^n$. Considere $c, \bar{c} \in \mathcal{C}$. Se para $z = (x,y)$ tem-se que $\delta_z^n(c,\bar{c}) = \alpha x + \beta y$, então necessariamente $\delta_{\bar{z}}^n(c,\bar{c}) = \alpha\bar{x} + \beta\bar{y}$, para $\bar{z} = (\bar{x},\bar{y})$.

De fato, a quantidade $\alpha + \beta$ de coordenadas distintas entre c e $\bar{c}$ é a mesma para qualquer canal e, portanto, independe do cone em questão. Portanto, obtemos que $\bar{\Lambda}^z_{\mathcal{C}}(s,t,r) = \bar{\Lambda}^{\bar{z}}_{\mathcal{C}}(s,t,r)$.

(b) Sejam $z, \bar{z} \in S$ e considere um código $\mathcal{C} \subseteq \mathbb{F}_2^n$. Uma vez que S é classe de equivalência, a Proposição 13 nos garante que, para qualquer $c \in \mathcal{C}$, temos $\mathcal{R}^z_{\mathcal{C}}(c) \cong \mathcal{R}^{\bar{z}}_{\mathcal{C}}(c)$, ou seja, ambos os raios de empacotamento de c são descritos pelo mesmo par de parâmetros α e β. Portanto, garantimos a igualdade $\bar{\Gamma}^z_{\mathcal{C}}(s,t,r) = \bar{\Gamma}^{\bar{z}}_{\mathcal{C}}(s,t,r)$.

Analogamente, obtemos que $\bar{\Psi}^z_{\mathcal{C}}(s,t,r) = \bar{\Psi}^{\bar{z}}_{\mathcal{C}}(s,t,r)$.

(c) Sejam $z \in S$ e $\bar{z} \in \bar{S}$. Pela Proposição 13, existe um código $\mathcal{C} \subseteq \mathbb{F}_2^n$ tal que $\mathcal{R}^z_{\mathcal{C}}(c) \ncong \mathcal{R}^{\bar{z}}_{\mathcal{C}}(c)$, para algum $c \in \mathcal{C}$. Portanto, $\bar{\Gamma}^z_{\mathcal{C}}(s,t,r) \neq \bar{\Gamma}^{\bar{z}}_{\mathcal{C}}(s,t,r)$.

Analogamente, obtemos que $\bar{\Psi}^z_{\mathcal{C}}(s,t,r) \neq \bar{\Psi}^{\bar{z}}_{\mathcal{C}}(s,t,r)$. □

Uma vez que os polinômios enumeradores de raios de empacotamento e cobertura são iguais para canais equivalentes, passaremos a denotá-los por

$$\bar{\Psi}^S_{\mathcal{C}}(s,t,r) := \bar{\Psi}^z_{\mathcal{C}}(s,t,r) \quad \text{e} \quad \bar{\Gamma}^S_{\mathcal{C}}(s,t,r) := \bar{\Gamma}^z_{\mathcal{C}}(s,t,r).$$

Por outro lado, o polinômio $\bar{\Lambda}^z_{\mathcal{C}}(s,t,r)$ será denotado apenas por $\bar{\Lambda}_{\mathcal{C}}(s,t,r)$, já que não depende do canal e nem do cone.

Exemplo 22. *Considere o código linear $\mathcal{C} = \{0000, 0101, 1011, 1110\}$, um cone $S \in \mathcal{D}_4$ e $z = (x,y) \in S$.*

O P.E.D. de $\mathcal{C}$, para o canal $z \in S$, é dado por

$$\bar{\Lambda}_{\mathcal{C}}(s,t,r) = 4 + (s^2 + 2st + s^2)r^2 + (2s^3 + 2s^2t + 2st^2 + 2s^3)r^3.$$

Assim sendo, se considerarmos, por exemplo, o termo $2s^2tr^3$, em $\Lambda^z_{\mathcal{C}}(s,t,r)$, isso significa que existem 2 pares de palavras código, $(c,\bar{c}) \in \mathcal{C}^2$, tais que $\delta^4_z(c,\bar{c}) = 2x + y$ e $d_H(c,\bar{c}) = 3$.

O P.E.R.E. de $\mathcal{C}$ é dado por

$$\bar{\Gamma}^z_{\mathcal{C}}(s,t,r) = \begin{cases} 1 + tr^2 + 2r^3 & \textit{para} \quad S_1 \cup S_2 \cup S_3, \\ s + sr^2 + 2r^3 & \textit{para} \quad S_4 \cup S_5 \cup S_6. \end{cases}$$

De modo análogo, se considerarmos, por exemplo, o termo tr^2 do P.E.R.E. de S_1, isso significa que existe somente uma palavra código $c \in \mathcal{C}$ com peso de Hamming $\omega_H(c) = 2$ e raio de empacotamento $\mathcal{R}^z_{\mathcal{C}}(c) = y$.

O P.E.R.C. de $\mathcal{C}$ é dado por

$$\bar{\Psi}^z_{\mathcal{C}}(s,t,r) = \begin{cases} 1 + sr^2 + (s+t)r^3 & para \quad S_1 \cup S_2 \\ s + sr^2 + (s+t)r^3 & para \quad S_3 \\ s + sr^2 + 2tr^3 & para \quad S_4 \\ s^2 + sr^2 + 2sr^3 & para \quad S_5 \cup S_6. \end{cases}$$

Novamente, se considerarmos, por exemplo, o termo tr^3, do P.E.R.C. de S_1, isso significa que somente uma palavra código tem peso de Hamming $\omega_H(c) = 3$ e raio de cobertura $\mathfrak{R}^z_{\mathcal{C}}(c) = y$.

No caso simétrico, esses mesmos tipos de polinômios são reduzidos a uma variável r. De fato, o código $\mathcal{C}$ tem raios de empacotamento e cobertura constantes e dados, respectivamente, por $\mathcal{R} = 0$ e $\mathfrak{R} = 1$. Assim sendo, não é necessário descrever quantas palavras código com peso de Hamming ω têm raio de empacotamento (cobertura) igual a i, pois toda palavra código tem o mesmo raio. Neste caso, os polinômios enumeradores estão restritos à distribuição de peso do código linear $\mathcal{C}$ e são dados por:

$$\begin{aligned} \Lambda_{\mathcal{C}}(r) &= 4 \cdot (1 + r^2 + 2r^3) \\ \Gamma_{\mathcal{C}}(r) &= 1 + r^2 + 2r^3 \\ \Psi_{\mathcal{C}}(r) &= 1 + r^2 + 2r^3. \end{aligned}$$

Considere os polinômios enumeradores de raios do caso assimétrico e seus correspondentes, no caso simétrico. Observe que, para todo i, o coeficiente A_i do caso simétrico, corresponde à soma dos coeficientes dos termos $s^\alpha t^\beta r^i$, do caso assimétrico.

No caso dos polinômios $\bar{\Lambda}_{\mathcal{C}}(s,t,r)$ e $\Lambda_{\mathcal{C}}(r)$, repare ainda que, o expoente do termo r^i, no caso simétrico, corresponde à soma dos parâmetros α, β do termo $s^\alpha t^\beta r^i$, no caso assimétrico. De fato, podemos escrever d como composições de duas partes, ou seja, $d = 0 + i = \ldots = \alpha + \beta = \ldots = i + 0$, gerando as correspondentes distâncias $\delta_z = iy, \ldots, \alpha x + \beta y, \ldots, ix$, com $\alpha + \beta = i$. Isto justifica a necessidade de contruir polinômios com mais variáveis, no caso assimétrico.

Proposição 17. *Considere um código $\mathcal{C} \subseteq \mathbb{F}_2^n$ e $S \in \mathcal{D}_n$. Para $z \in S$, as seguintes identidades são válidas:*

1. *$\bar{\Lambda}_{\mathcal{C}}(1,1,r) = \mathcal{D}_{\mathcal{C}}(r)$, onde $\mathcal{D}_{\mathcal{C}}(r)$ denota o **polinômio enumerador de distâncias** do código $\mathcal{C}$, no caso clássico, [15];*

2. *$\bar{\Gamma}_{\mathcal{C}}(1,1,r) = \bar{\Psi}_{\mathcal{C}}(1,1,r) = \mathcal{W}_{\mathcal{C}}(r)$, onde $\mathcal{W}_{\mathcal{C}}(r)$ denota o **polinômio enumerador de pesos** do código $\mathcal{C}$, no caso clássico, [15].*

Se $\mathcal{C}$ for um código linear, obtemos que $\frac{1}{|\mathcal{C}|} \cdot \bar{\Lambda}_{\mathcal{C}}(1,1,r) = \bar{\Gamma}_{\mathcal{C}}(1,1,r) = \bar{\Psi}_{\mathcal{C}}(1,1,r)$.

Demonstração. Considere um código $\mathcal{C} \subseteq \mathbb{F}_2^n$ e $z \in S \in \mathcal{D}_n$.

1. Por definição, temos que

$$\bar{\Lambda}_{\mathcal{C}}(1,1,r) = \sum_{d=0}^{n} \Big[\sum_{(\alpha,\beta)\in\bar{\mathcal{Q}}_{\mathcal{C}}} \lambda_{\alpha\beta}^{d} \Big] r^d = \sum_{d=0}^{n} \Big[\sum_{\substack{(\alpha,\beta):\\ \alpha+\beta=d}} \lambda_{\alpha\beta}^{d} \Big] r^d.$$

   Mas, para $0 \leq d \leq n$, o termo $\Big[\sum_{\substack{(\alpha,\beta):\\ \alpha+\beta=d}} \lambda_{\alpha\beta}^{d}\Big] r^d$ é equivalente ao termo $A_d r^d$ do polinômio enumerador de distâncias, $\mathcal{D}_{\mathcal{C}}(r)$. Daí segue a igualdade $\bar{\Lambda}_{\mathcal{C}}(1,1,r) = \mathcal{D}_{\mathcal{C}}(r)$.

2. Por definição, temos que

$$\bar{\Gamma}_{\mathcal{C}}^{z}(1,1,r) = \sum_{\omega=0}^{n} \Big[\sum_{(\alpha,\beta)\in\bar{\mathcal{R}}_{\mathcal{C}}} \gamma_{\alpha\beta}^{\omega} \Big] r^{\omega}.$$

   Mas, o termo $\Big[\sum_{(\alpha,\beta)\in\bar{\mathcal{R}}_{\mathcal{C}}} \gamma_{\alpha\beta}^{\omega}\Big] r^{\omega}$ é equivalente ao termo $A_{\omega} r^{\omega}$ do polinômio enumerador de pesos $\mathcal{W}_{\mathcal{C}}(r)$. Daí, segue imediatamente que $\bar{\Gamma}_{\mathcal{C}}(1,1,r) = \mathcal{W}_{\mathcal{C}}(r)$. A demonstração é análoga para o polinômio $\bar{\Psi}_{\mathcal{C}}^{z}(s,t,r)$. □

Capítulo 4

Considerações finais

Finalizamos este trabalho elencando brevemente três pontos ainda a serem explorados.

1. Buscar condições para determinar em que medida o desempenho relativo de dois códigos (*código A é "melhor"que código B*) depende do canal ou de sua classe de equivalência. Em um primeiro momento, buscamos comparar as probabilidades de erro de dois códigos em canais distintos de um mesmo cone $S \in \mathcal{D}_n$. Esperávamos que pudesse ser uma boa figura de mérito para comparar a eficiência de dois códigos. No entanto, percebemos que ao tomarmos dois canais $z, \bar{z} \in S$, em regiões distintas de S, um canal pode ser melhor que o outro em z, mas pior que o mesmo canal em $\bar{z}$. Logo, esta não é uma boa estratégia para encontrar o melhor código corretor de erros. A figura de mérito adequada ainda está por ser encontrada.

2. A busca de uma identidade do tipo MacWilliams para distâncias e raios de empacotamento. A necessidade de se considerar três variáveis na definição do Polinômio Enumerador de Distâncias $\bar{\Lambda}_{\mathcal{C}}(s,t,r)$ ou raios de empacotamento $\bar{\Gamma}_{\mathcal{C}}(s,t,r)$ se deve à busca de uma identidade do tipo MacWilliams. É fácil ver que essas três variáveis são estritamente necessárias visto que duas delas (s e t) são variáveis indicadoras dos parâmetros α e β que determinam uma distância e a terceira variável r denota a distância de Hamming d. Esta última variável pode parecer menos importante; entretanto, como foi mencionado anteriormente, tal variável pode ser decomposta de diversas maneiras no código $\mathcal{C}$. Neste sentido, esta foi acrescentada ao polinômio justamente para enfatizar a decomposição. Pensando nesta decomposição de d e na busca por uma identidade do tipo de MacWilliams, que relacione o código $\mathcal{C}$ com seu dual, gostaríamos de mostrar que se dois códigos lineares $\mathcal{C}$ e $\bar{\mathcal{C}}$ têm o mesmo polinômio enumerador de distâncias, então, seus correspondentes duais $\mathcal{C}^{\perp}$ e $\bar{\mathcal{C}}^{\perp}$ também são descritos por um mesmo polinômio enumerador de distâncias. No decorrer desta tentativa de demonstração, utiliza-se a Identidade de MacWilliams,

que relaciona os pesos do código com os pesos do seu respectivo dual (vide [18]) e, como os códigos $\mathcal{C}$ e $\bar{\mathcal{C}}$ são lineares, garantimos imediatamente que os duais terão a mesma distribuição de distâncias de Hamming. No entanto, não conseguimos garantir que uma distância de Hamming d é decomposta da mesma forma nestes dois códigos duais e isso impede que consigamos concluir a demonstração da igualdade desejada. Todos os exemplos trabalhados até o momento (casos $n = 2, 3$ e 4) sugerem que estas variáveis sejam suficientes para garantir uma relação entre $\bar{\Lambda}_{\mathcal{C}}(s,t,r)$ e $\bar{\Lambda}_{\mathcal{C}^\perp}(s,t,r)$, mas infelizmente não foi possível demonstrar a questão. Um problema similar ocorre quando tentamos demonstrar esta mesma relação para os raios de empacotamento do código. Esta questão, aparentemente, demanda algum salto de entendimento para poder ser abordada de maneira sistemática, haja vista que os recursos tradicionais utilizados por MacWilliams (caracteres) tornam-se de trato muito difícil ao se considerar mais variáveis.

3. A última questão se refere às possibilidades de ganho de desempenho ao se explorar a assimetria dos canais para proteção desigual de erros. Apesar da possibilidade de ganho ser evidente, a quantificação deste ganho é algo a ser estudado, por métodos de simulação, em instâncias específicas.

Índice Remissivo

Referências Bibliográficas

[1] Y. Cassuto, M. Schwartz, V. Bohossian, J. Bruck, *Codes for asymmetric limited-magnitude errors with application to multi-level Flash memories*, IEEE Transaction on Information Theory, vol. 56, nº4, 1582-1595, 2010;

[2] E. Yaakobi, P. H. Siegel, A. Vardy, J. K. Wolf, *On codes that correct asymmetric errors with graded magnitude distribution*, IEEE ISIT, St Peterburgh, Russia, 2011;

[3] C. Curto, V. Itskov, K. Morrison, Z. Roth, J. L. Walker, *Combinatorial neural codes from a mathematical coding theory perspective*, Neural Computation, vol. 25, nº7, 1891-1925, 2013;

[4] J. C.-Y. Chiang, J. K. Wolf, *On channels and codes for the Lee metric*, Information and Control, Vol. 19, 159-173, Sep 1971;

[5] J. L. Massey, *Notes on Coding Theory*, class notes for course 6.575 (spring), M.I.T., Cambridge, Mass, 1967;

[6] G. Séguin, *On metrics matched to the discrete memoryless channel*, J. Franklin Inst., Vol. 309, nº3, 179-189, Mar 1980;

[7] M. Firer, J. L. Walker, *Matched metrics and channels*, IEEE Transactions on Information Theory, Vol. 62, nº3, March 2016;

[8] A. Poplawsky, *On matched metric and channel problem*, arXiv:1606.02763v1, 2017;

[9] C. M. Qureshi *Matched metrics to the binary asymmetric channels*, arXiv: 1606.09494v1, 2016;

[10] C. Qureshi, S. I. R. Costa, C. B. Rodrigues e M. Firer, *Maximum likelihood criteria for binary asymmetric channels*, arXiv:1611.10268, 2016;

[11] M. M. Deza, E. Deza, *Encyclopedia of Distances*, 3th edition, Springer, 2014;

[12] R. G. L. D'Oliveira, M.Firer, *Channel metrization*, arXiv:1510.03104v2, 2016;

[13] A. Fazeli, A. Vardy, E. Yaakobi, *Generalized sphere packing bound*, IEEE Transactions on Information Theory, Vol. 61, nº5, 2313-2334, May 2015;

[14] S. D. Constantin e T. R. N. Rao, *On the theory of binary asymmetric error correcting codes*, Information and Control, Vol. 40, 20-36, 1979;

[15] F. J. Macwilliams, N. J. A. Sloane, *The Theory of Error-correcting Codes*, North-Holland, 1977;

[16] J. P. O. Santos, *Introdução à Teoria dos Números*, terceira edição, Coleção Matemática Universitária, IMPA, 2003;

[17] N. J. A. Sloane, S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, 1995;

[18] V. Pless *Introduction to the Theory of Error-Correcting Codes*, 3th edition, Wiley-Interscience, 1998;

[19] S. Borade, B Nakiboğlu and L. Zheng - *Unequal error protection: an information-theoretic perspective* - IEEE Transactions on Information Theory (2009), vol. 55, No. 12, 5511-5539;

[20] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, 2nd edition, Wiley-Interscience, 2006;

[21] D. B. West, *Introduction to Graph Theory*, 2nd edition, Prentice Hall, 2001;

[22] S. Ross, *A first Course in Probability*, eight edition, Prentice Hall, 2010;

[23] J. P. O. Santos, M. P. Melo, *Introdução à Análise Combinatória*, 4ª ediçao revista, editora Ciência Moderna, 2007.