1
Introdução

Códigos Turbo e o Problema da Codificação de Canal

Em um sistema de comunicação, o objetivo consiste em transmitir uma mensagem através de um canal ruidoso, de modo que o receptor seja capaz de determinar esta mensagem com confiabilidade, diante das adversidades impostas pelo canal.

O problema da codificação de canal consiste em projetar um código $\mathcal{C}$ de taxa R, que viabilize o objetivo descrito acima. As seguintes definições introduzem os conceitos de código e taxa.

Definição 1.1 (Código) Um código $\mathcal{C}$ de comprimento n e cardinalidade $\mathfrak{M}$ sobre um corpo $\mathbb{F}$ é um subconjunto de $\mathbb{F}^n$ com $\mathfrak{M}$ elementos, ou seja

$$\mathcal{C} \triangleq \{\boldsymbol{c}^{[1]}, \ldots, \boldsymbol{c}^{[\mathfrak{M}]}\},\ \boldsymbol{c}^{[i]} \in \mathbb{F}^n,\ 1 \leq i \leq \mathfrak{M} \tag{1-1}$$

onde $\boldsymbol{c}^{[i]}$ é denominada *palavra código*. A *taxa* de um código $\mathcal{C}$ é definida como $R \triangleq 1/n \log_{|\mathbb{F}|} \mathfrak{M}$ símbolos de informação por símbolos codificados. ■

Definição 1.2 (Código linear) Um código $\mathcal{C}$ sobre $\mathbb{F}$ é *linear* se

$$\alpha c + \beta c' \in \mathcal{C}, \quad \forall c, c' \in \mathcal{C} \text{ e } \forall \alpha, \beta \in \mathbb{F} \tag{1-2}$$

i.e., $\mathcal{C}$ é um *subespaço vetorial* do espaço vetorial $\mathbb{F}^n$. A dimensão k do código $\mathcal{C}$ é a dimensão de $\mathcal{C}$ como um espaço vetorial; em particular, $\mathfrak{M} = |\mathbb{F}|^k$. A taxa de um código linear $\mathcal{C}$ é dada por $R = k/n$. ■

No projeto de $\mathcal{C}$, busca-se um compromisso entre cinco parâmetros:

- Taxa do código - R;
- Probabilidade de erro de bit - $P(e_b)$;
- Tamanho do código - n;
- Complexidade da codificação;

– Complexidade da decodificação.

O interesse é maximizar R, transmitindo assim o máximo de informação por símbolo codificado; e minimizar os demais parâmetros, garantindo a maior confiabilidade na transmissão e diminuindo custos de implementação e o atraso que $\mathcal{C}$ introduz.

A teoria da informação surgida em 1948 com o artigo seminal de Claude Shannon [1], estabelece os limitantes teóricos para uma comunicação confiável através de um canal ruidoso.

Nesta teoria, Shannon propôs o teorema da codificação de canal, que garante ser possível realizar transmissões à probabilidades de erro arbitrariamente baixas, desde que a taxa R de codificação seja menor que a capacidade do canal utilizado, e que o comprimento do código empregado seja suficientemente grande ($n \to \infty$). Para um canal AWGN (Aditive White Gaussian Noise), a capacidade de canal, calculada em [1], é

$$C = \frac{1}{2}\log_2\left(1 + 2\frac{RE_b}{\mathcal{N}_0}\right) \quad \text{bits/uso do canal,} \tag{1-3}$$

onde E_b é a energia por bit e $\mathcal{N}_0$ caracteriza a densidade espectral de potência do ruído.

A partir da Eq. (1-3) é possível obter a desigualdade[1] [30], p. 145,

$$\frac{E_b}{\mathcal{N}_0} \leq \frac{2^{2R[1-H_b(P(e_b))]} - 1}{2R} \tag{1-4}$$

onde $P(e_b)$ é a probabilidade de erro de bit, e $H_b(P(e_b))$ a função entropia binária.

A Eq. (1-4) estabelece duas regiões. A região em que o par $(P(e_b), E_b/\mathcal{N}_0)$ é tal que a desigualdade (1-4) é satisfeita, denominada de *região admissível*, ou seja, existe um código de taxa R e desempenho $(P(e_b), E_b/\mathcal{N}_0)$ cujos parâmetros se encontram nesta região. E outra região denominada de *região não-admissível*, na qual não existe um código de taxa R com desempenho $(P(e_b), E_b/\mathcal{N}_0)$ para esta região.

A Eq. (1-4) também informa a mínima razão $E_b/\mathcal{N}_0$, para a qual é possível se transmitir com probabilidade de erro de bit $P(e_b)$, quando a taxa é R. Na Fig. 1.1 estão plotadas as curvas correspondentes a (1-4) para algumas taxas R, estas curvas são conhecidas como limitantes de Shannon para o par $(P(e_b), R)$.

O teorema da codificação de canal é um teorema de existência, que afirma que há códigos que permitem transmissão confiável, mas não diz

[1] A entropia binária é obtida como $H_b(P(e_b)) = -P(e_b)\log_2(P(e_b)) - (1 - P(e_b))\log_2(1 - P(e_b))$.

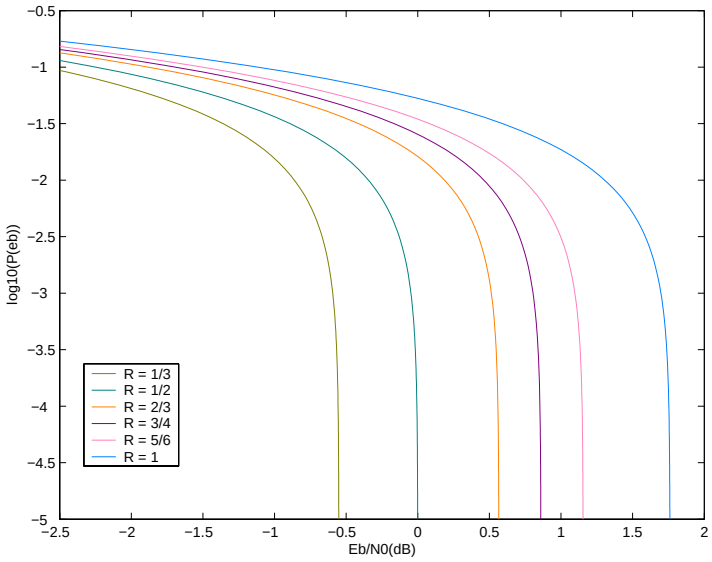

Figura 1.1: Desigualdade em (1-4) para as taxas $R = 1/3, 1/2, 2/3, 3/4, 5/6$.

como encontrá-los. Shannon para prová-lo, utilizou códigos $\mathcal{C}$ escolhidos aleatoriamente e de comprimentos n longos, tendendo a infinito. Entretanto, aumentar o tamanho n para esses códigos, implicava em um nível de complexidade de decodificação que impossibilitava a implementação de $\mathcal{C}$ na prática.

Era necessário, buscar um esquema de menor complexidade. Este fato motivou vários pesquisadores da área e impulsionou a criação de diversos códigos com aplicabilidade prática, mas que no entanto não eram capazes de operar próximo ao limitante de Shannon.

Em 1993, Berrou et. al [4] propuseram um esquema de codificação que produzia palavras códigos longas e decodificação com complexidade que cresce linearmente com o comprimento do código. Esse esquema permite uma comunicação confiável com valores de $E_b/\mathcal{N}_0$ muito próximos do limitante de Shannon. A baixa complexidade e o alto desempenho desse esquema, fizeram com que o mesmo fosse considerado uma solução bastante atrativa para o problema da decodificação de canal. A este esquema de codificação deu-se o nome de códigos turbo.

A busca por uma uma comunicação com $P(e_b)$ tão pequena quanto se queira, vem incentivando a utilização destes códigos em padrões de comunicação atuais, dentre eles estão pradrões de telefonia celular da 3ª geração, de televisão digital e de comunicação via satélites, o que torna importante um estudo detalhado deste código.

Sistema de Comunicação

O modelo teórico utilizado neste trabalho para um sistema de comunicações está ilustrado na Fig. 1.2. Neste modelo, é assumido que a fonte utilizada é binária, e que portanto a mensagem $\boldsymbol{m}$ que se deseja transmitir, consiste de um bloco de bits de tamanho k, representada por

$$\boldsymbol{m} = \begin{pmatrix} m_0 & m_1 & \cdots & m_{k-1} \end{pmatrix} \tag{1-5}$$

onde os bits de $\boldsymbol{m}$ são considerados equiprováveis e independentes entre si.

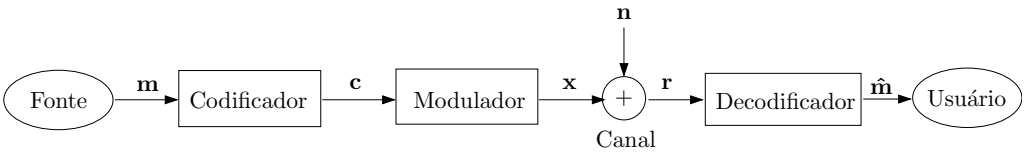

Figura 1.2: Sistema de comunicação simplificado.

A mensagem $\boldsymbol{m}$ é enviada a um *codificador* correspondente a um código $\mathcal{C}$ de comprimento n e taxa $R = k/n$, que a partir de $\boldsymbol{m}$ gera uma palavra código $\boldsymbol{c}$ dada por

$$\boldsymbol{c} = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \end{pmatrix}. \tag{1-6}$$

A cada b bits de $\boldsymbol{c}$, o modulador gera um símbolo modulado x_ℓ, para $\ell = 0, \ldots, M-1$, onde $M = n/b$, através de um mapeamento $x_\ell = \mathcal{M}(c_{\ell b}, c_{\ell b+1}, \ldots, c_{\ell b+(b-1)})$. Para uma constelação b-ária, unidimensional, com $x_\ell \in \mathcal{A}^x = \{\pm 1, \ldots, \pm(2^b - 1)\}$, a seqüência modulada é dada por

$$\boldsymbol{x} = \begin{pmatrix} x_0 & x_1 & \cdots & x_{M-1} \end{pmatrix}. \tag{1-7}$$

Considerando que o canal utilizado seja gaussiano, a seqüência modulada $\boldsymbol{x}$ é corrompida por um ruído aditivo gaussiano branco AWGN, representado pela variável aleatória guassiana n_ℓ, com média zero e variância $\frac{\mathcal{N}_0}{2}$, cuja função densidade de probabilidade é representada pela notação $\mathcal{N}\left(0, \frac{\mathcal{N}_0}{2}\right)$.

Na recepção, a seqüência recebida

$$\boldsymbol{r} = \begin{pmatrix} r_0 & r_1 & \cdots & r_{M-1} \end{pmatrix} \tag{1-8}$$

onde r_ℓ são valores reais obtidos por

$$r_\ell = x_\ell + n_\ell, \tag{1-9}$$

onde $\boldsymbol{r}$ é disponibilizada para o decodificador, e r_ℓ assume valores em um alfabeto $\mathcal{A}^r \subset \mathbb{R}$.

Como pode-se observar na Eq. (1-9), o canal estabelece uma relação probabilística entre $\boldsymbol{x}$ e $\boldsymbol{r}$; e a partir de $\boldsymbol{r}$, o decodificador entrega uma estimação $\hat{\boldsymbol{m}}$ de $\boldsymbol{m}$ para o usuário.

Problema da Decodificação

Para solucionar o problema da decodificação, considera-se que uma palavra código $\boldsymbol{c}$ foi transmitida através de um canal ruidoso e $\boldsymbol{r}$ é a seqüência observada. Dado $\boldsymbol{r}$, o problema da decodificação pode ser formulado de duas maneiras [28]:

1) **Problema da decodificação da palavra código:** é a tarefa de encontrar uma maneira ótima de, observando $\boldsymbol{r}$, inferir qual palavra código $\boldsymbol{c}$ foi transmitida.
2) **Problema da decodificação dos bits transmitidos:** é a tarefa de encontrar uma maneira ótima de, observando $\boldsymbol{r}$, inferir qual bit c_i foi transmitido.

As soluções dos problemas formulados acima, fundamentam-se no teorema de Bayes

$$P(\boldsymbol{c}|\boldsymbol{r}) = \frac{P(\boldsymbol{r}|\boldsymbol{c})P(\boldsymbol{c})}{P(\boldsymbol{r})}, \tag{1-10}$$

onde $P(\boldsymbol{c}|\boldsymbol{r})$ é a probabilidade *a posteriori* da palavra código $\boldsymbol{c}$.

A Eq. (1-10) é composta pelos seguintes fatores:

- $P(\boldsymbol{r}|\boldsymbol{c})$, denominada *verossimilhança* (*likelihood*) da palavra código $\boldsymbol{c}$, é definida pelo modelamento do canal.
- $P(\boldsymbol{c})$, a *probabilidade a priori* de $\boldsymbol{c}$, é geralmente considerada uniforme ao longo de todas as palavras códigos.
- $P(\boldsymbol{r})$ é apenas uma constante de normalização, dada por

$$P(\boldsymbol{r}) = \sum_{\boldsymbol{c}} P(\boldsymbol{r}|\boldsymbol{c})P(\boldsymbol{c}). \tag{1-11}$$

A solução do problema de decodificação seguindo a primeira formulação, busca maximizar a probabilidade *a posteriori* $P(\boldsymbol{c}|\boldsymbol{r})$. Quanto à segunda formulação, a solução otimiza para o i-ésimo bit c_i, marginalizando

a Eq. (1-10) em relação aos outros bits para todas as palavras código, a probabilidade

$$P(c_i|\boldsymbol{r}) = \sum_{\{i \neq i'\}} P(\boldsymbol{c}|\boldsymbol{r}). \tag{1-12}$$

No caso da decodificação turbo, a solução segue a segunda formulação.

Organização do Trabalho

Neste trabalho, abordamos a utilização dos códigos turbo como solução para o problema da codificação de canal. Foi realizada uma revisão da literatura, visando a compreensão dos principais conceitos relacionados à codificação e à decodificação turbo.

O problema da decodificação turbo, em especial, foi explorado segundo duas abordagens denominadas neste trabalho de

Abordagem Convencional: foi introduzida por Berrou et. al [4], esta abordagem é comumente utilizada em vários artigos que abordam códigos turbo. Nela a decodificação turbo é desenvolvida baseada na treliça dos códigos componentes.

Abordagem por Grafo-Fatores: nesta abordagem a decodificação turbo é desenvolvida baseada no grafo-fator [25] que o representa, é uma teoria moderna e que esclarece de forma didática vários aspectos da decodificação turbo.

Foi desenvolvido também um simulador turbo, seguindo a abordagem de grafos-fatores, a fim de se constatar e avaliar, através de simulações, fatores que justificam e influenciam a excelente performance dos códigos turbo.

Esta dissertação está organizada da seguinte maneira: o Capítulo 2 introduz os principais conceitos e fundamentos para a compreensão da codificação turbo; no Capítulo 3, a decodificação turbo é desenvolvida segundo a abordagem convencional; no Capítulo 4 é revisada a teoria de grafos-fatores e a decodificação turbo é discutida detalhadamente segundo essa teoria; no Capítulo 5, os resultados obtidos através do simulador turbo são analisados; e por fim o Capítulo 6 apresenta as conclusões deste trabalho e algumas sugestões de pesquisa para trabalhos futuros.